

IBM Aspera On Cloud



Tables of Contents

IBM Aspera on Cloud	3
Admin	3
Get started	4
Try Aspera on Cloud for free	4
Get to know Aspera on Cloud	4
What is IBM Aspera on Cloud?	5
What is a transfer?	5
What is a package?	6
Applications: Overview	7
What is a workspace?	8
What is a shared inbox?	8
What is IBM Aspera Connect?	9
Should I send or share?	9
Key elements and roles in Aspera on Cloud	11
Multi-session transfers	14
Prerequisites	15
System requirements and browser support	15
Firewall requirements	16
Access security and content security	17
Primary access keys and sub-access keys	18
Secure the access credentials for your built-in node	18
Configuring authentication methods for your organization	18
Content security overview	19
Data logging and retention	20
Customize for your use case	21
Define your use case	21
Collaboration: Open or closed?	22
Configuration best practices	24
Integrating Aspera products	24
Give users access to local or cloud storage	24
Set up your organization	24
Organization: Overview	25
Accelerate setup using inherited settings	26
Select a transfer method	27
Transfer with Aspera HTTP Gateway instead of Aspera Connect	28
Configure technical support for your users	28
Customize your organization URL, name, and logo	29
Configure the user login page	30
Give users access to local or cloud storage	24
Share a node folder with a workspace	31
Add users: Overview	32
Delegate to a workspace manager	32
Set the default storage location for your organization	33
Session and token duration	33
Configure email notifications for your organization	34
Customize email notification templates	34
Email template inheritance in Aspera on Cloud	36
Email template variables	37
Control email notification delivery	37
Storage and workspace configuration scenarios	38
Configuration scenario: Sharing with external colleagues	38
Configuration scenario: Workspace members sharing a file repository	46
Access security and credentials	51
Session and token duration	33
Access keys	52
Primary access keys and sub-access keys	18
Create a sub-access key to a workspace	53
Create a sub-access key to a shared folder	53
Create a sub-access key to a cloud storage folder	54
Tracking your node access credentials	55
FASP security: Aspera Connect transfer client authorized keys and aspsell	56
Access key to your built-in node	57
Secure the access credentials for your built-in node	18
Identify your built-in node	57
Access your built-in node	58
Access issues	58
Trouble creating a new access key	58
Can't find the access credentials to your built-in node	
Tracking your node access credentials	55

Content security	65
Session and token duration	33
Content security overview	19
Encryption	67
Content encryption: In flight and at rest	67
Require encryption at rest	68
Rotate keys for your Azure storage	68
Use Aspera-managed keys for server-side encryption at rest	69
Bring your own key for server-side encryption at rest	69
Permissions	72
Sharing Permissions	72
Sending Permissions	74
Collaboration: Open or closed?	22
Watermarking: Integrate your Irdeto service	76
Antivirus scanning	79
Authentication	80
Configuring authentication methods for your organization	18
Configure the user login page	30
SAML	81
Configuring SAML: Overview	81
Configuring SAML: Procedures	83
Configuring SAML SSO using OKTA	84
IBMid	85
Configure IBMid	85
Require multifactor authentication for IBMid users	86
Avoid lockout when disabling IBMid	86
Configuring Google authentication	86
Subscription usage and billing	87
Understanding your subscription usage and billing	87
Feature and usage tiers	88
Try Aspera on Cloud for free	4
Manage transfer volume in your subscription	89
Manage egress in your subscription	92
Manage storage in your subscription	96
Required configuration for your tethered node	96
Aspera Connect transfer client	97
What is IBM Aspera Connect?	9
Aspera Connect for Outside Users	97
Monitor transfers	98
Installation	98
Installing Aspera Connect	99
Adding the Chrome browser extension for Connect	100
Adding the Firefox browser extension for Connect	102
Adding the Safari browser extension for Connect	102
Adding the Microsoft Edge browser extension for Connect	103
Installation troubleshooting	104
Overview: Aspera Connect installation troubleshooting	105
Windows OS: Error when installing with a non-admin account	105
Windows OS: Connectivity issues	107
MacOS X: Connectivity issues	107
Linux: AppArmor prevents access to Connect	108
Linux: Connectivity issues	108
Other Connect troubleshooting	108
IBM Aspera Connect common issues	109
Connect prompt continues to appear	110
Disable IBM Aspera Connect	110
Attach cloud and local storage	110
Node and storage basics	111
Cloud platforms and regions supported	111
Share a node folder with a workspace	31
Managing storage usage	113
Creating network policies	116
Creating node configuration policies	117
Deleting a node	118
Node types in Aspera on Cloud	118
Identifying a node type	119
Attach your own Aspera HSTS node	119
Tether Your Aspera Transfer Server to Aspera on Cloud	120
Installing SSL certificates for tethered nodes	121
Firewall requirements for tethered nodes	122
Using an HTTPS proxy for outgoing ALEE and AEJD traffic from your tethered node	124
Configure your transfer server as a tethered node	125

Configure Nginx reverse proxy and server certificates	126
Create the transfer user for your tethered node	127
Configure the HA Redis backend for a tethered node cluster	129
Tether your HSTS node to Aspera on Cloud	129
Mark remote storage attached to your tethered node as mount points	132
Configure monitoring and metering for your tethered node	133
Backing up and restoring a tethered node database	134
Attach your existing cloud storage	135
Firewall requirements for ATS and cloud storage	135
Share a node folder with a workspace	31
Attach your IBM Cloud storage	137
Attach your Google storage	138
Attach your Azure Blob storage	139
Attach your Azure Files storage	140
Attach an AWS S3 bucket	141
Create an AWS S3 IAM role and policy	145
Attach a KMS-encrypted AWS bucket	146
Sample IAM Policies for AWS S3	150
Creating AWS IAM roles for transfer service nodes	151
Installing File preview	152
File preview supported file types	154
Attaching storage troubleshooting	156
Trouble creating a new access key	58
Tracking your node access credentials	55
Workspaces	162
What is a workspace?	8
Create a new workspace	163
Create workspace distribution lists	165
Delegate to a workspace manager	32
Share a node folder with a workspace	31
Which folders are shared with a workspace?	166
Delete a workspace	167
Users and groups	167
Users, groups, and roles	167
User roles and types	167
Create and manage users	169
Create and manage groups	170
Assign the organization administrator role	171
Assign the ATS administrator role	171
Assign the workspace manager role	172
Manage inactive users	172
Content access: User permissions and memberships	173
Content permissions	173
Direct and inherited memberships	175
Manage workspace memberships and roles	176
Manage shared folder memberships	177
Manage shared inbox memberships	178
Manage application memberships	178
Manage group memberships and roles	179
Membership Troubleshooting	179
Removed member still has access	180
Packages app: Send and receive files and folders	180
Packages app basics	180
What is the Packages app?	180
What is a submission link?	181
Accelerate Packages app setup through inheritable settings	181
Content security in the Packages app	182
Package expiration policies for storage management	182
Configuration options	183
Set package expiration policies	184
Send files to external users	184
Request files from external users	185
Require external users to log in	185
Control content distribution in the workspace	186
Disable package sending	186
Require encryption at rest	68
Configure link styles for requesting digital packages	187
Protect privacy in the workspace	187
Creating JSON sidecar files for digital packages	188
Give all workspace members access to all sent packages	188
Shared inboxes	189
Shared inboxes overview	189

Accelerate shared inbox setup through inheritance	190
Manage shared inbox memberships	178
Create a new shared inbox	191
Configure shared inbox settings	192
Add metadata fields to a shared inbox	192
Allow self-registration for a shared inbox	192
Use shared inboxes for external collaboration	194
Troubleshooting: Sending files and folders	194
Email notifications	194
Resending "Draft" packages	195
Files App: Using a shared file repository	195
Files app basics	195
What is the Files app?	195
Content permissions	173
Content security in the Files app	197
File deletion policies for storage management	198
Accelerate Files app setup through inheritable settings	198
Configuration options	199
Share a node folder with a workspace	31
Share folders using public links	200
Share folders with external users	201
Control content sharing in the workspace	201
Configure public and authenticated link styles for sharing folders	201
Sharing strategies	202
Control and monitor usage in the Files app	203
Unshare a folder	204
Configuration scenario: Sharing with external colleagues	38
Configuration scenario: Workspace members sharing a file repository	46
Troubleshooting: Sharing files and folders	217
Can't access a shared folder	217
User still has access to unshared folder	217
Activity app: Monitor events, activity, and usage in your organization	218
Overview	218
Enabling the Activity app and adding members	218
Aspera Activity App API	218
Architecture and components of the activity app	219
Reporting activity and usage	219
Data retention	220
Monitoring	220
Monitor bandwidth usage	220
Monitor volume usage	221
Monitor application events	222
Use cases	223
Example use cases for monitoring transfer activity	223
Example use cases for monitoring volume usage	224
Example use cases for monitoring file access	224
Example use cases for monitoring application events	224
Automation app: Automate your transfer workflows	225
Get started	225
Automation app: Overview	225
Prerequisites	227
Enabling the Automation app and adding members	227
Resources for developers	228
Create and manage automated workflows	228
Tutorial: Create a simple workflow that transfers a package	228
Workflow actions and their attributes	229
Workflow triggers and their attributes	232
Managing workflows and jobs	233
Use substitution variables in workflow actions	234
Configuring API callback	234
Troubleshooting	235
Failure notification types and locations	235
Get current status information for Aspera on Cloud	236
Transfer issues	236
Select a transfer method	27
Retry the transfer	237
Resending "Draft" packages	195
Node-to-node transfer issues	237
Slow transfer speeds	238
Specific transfer failures	239
More transfer troubleshooting resources	240
Access, notifications, and other issues	240

Can't find the access credentials to your built-in node	
Email notifications	194
Trouble creating a new access key	58
Can't access a shared folder	217
User still has access to unshared folder	217
Stored report not available in Activity app	246
Delete large files and folders	246
Rename large folders	247
Irdeto watermarking integration	247
Aspera Connect installation issues	248
Overview: Aspera Connect installation troubleshooting	105
Select a transfer method	27
Connect prompt continues to appear	110
Windows OS: Error when installing with a non-admin account	105
Windows OS: Connectivity issues	107
MacOS X: Connectivity issues	107
Linux: AppArmor prevents access to Connect	108
Linux: Connectivity issues	108
Specific error messages	253
Get IBM technical assistance	253
Who is eligible for technical assistance?	254
Register for technical assistance	254
Open a case	254
Subscribe to notifications	254
Resources	255
Error code reference	255
Integration and APIs	255
Registering an API client	255
Watermarking: Integrate your Irdeto service	76
Bring your own key for server-side encryption at rest	69
Transfer Clients	263
Desktop access to AoC using IBM Aspera for desktop	263
IBM Aspera mobile app	263
Command Line Interface (CLI)	264
Transfer to cloud with Desktop Client, HST Server, or HST Endpoint GUI	264
Transfer Servers	265
Transfer to cloud with Desktop Client, HST Server, or HST Endpoint GUI	264
Aspera APIs	266
Notifications and announcements	266
Deprecation notices	267
Important updates	267
New and Coming Soon	268
What's new in Aspera on Cloud	268
Coming soon to Aspera on Cloud	280
Legal Notice	280
User	281
Get started	281
Get to know Aspera on Cloud	4
What is IBM Aspera on Cloud?	5
What is a transfer?	282
What is a workspace?	8
What is IBM Aspera Connect?	9
Should I send or share?	9
Quick start	285
Before you begin	286
Quick start: Send files and folders	286
Quick start: Share a folder from your Files app repo	286
Uploads and downloads	287
Monitor transfers	98
File preview supported file types	154
Set your account preferences	290
Set your default language	291
Set your default items per page	291
Set your default app	291
Set your default workspace	291
Set your default download location	291
Add your public key	291
Subscribe to email notifications	292
Disable IBM Aspera Connect	110
Packages app: Send and receive files and folders	292
Get started sending files and folders	292
What is a package?	6

- Should I send or share?
- Save packages as drafts
- Schedule packages to send later
- Quick start: Send files and folders
- Quick start: Request a file
- Send files and folders in a digital package
 - Sending: Detailed procedure
 - Save packages directly to your Files app repo
 - Download from the Packages app
 - Sending: Become an expert
 - Create a personal distribution list
 - Forward a package
 - Add recipients to a sent package
 - Recall a package
 - Resend packages in the Drafts folder
 - Delete a package you sent
 - Verify whether a package has been downloaded
- Request files and folders
 - What is a submission link?
 - Request a package to My inbox
 - Request a package to a shared inbox
 - Customize submission links
 - Manage submission links
- Shared inboxes
 - What is a shared inbox?
 - Send to a shared inbox
 - Request a package to a shared inbox
- Files app: Sharing folders
 - Get started sharing folders
 - Should I send or share?
 - Quick start: Share a folder from your Files app repo
 - Unshare a folder
 - Upload files and folders to the Files app
 - Download from the Files app
 - Sharing permissions
 - Which permissions do I have?
- Sharing folders
 - Determine who has shared access
 - Change permissions to a folder you shared
 - Understand "Size" and "Last Updated" data
 - Set notifications for new content in a shared folder
 - Move or copy content in your Files app
 - Manage your shared links
 - Mark favorites in the Files app
 - Create a new folder
 - Delete files and folders
 - Rename folders in your Files app
- Share with outside users
 - What is a public link?
 - Share with external users
 - Share with unauthenticated recipients using public links
- Sharing problems
 - Delete large files and folders
 - Rename large folders
 - Can't access a shared folder
 - User still has access to unshared folder
- Aspera Connect transfer client
 - What is IBM Aspera Connect?
 - Aspera Connect for Outside Users
 - Installation
 - Installing Aspera Connect
 - Adding the Firefox Connect Browser Extension
 - Adding the Chrome browser extension for Connect
 - Adding the Safari browser extension for Connect
 - Adding the Microsoft Edge browser extension for Connect
 - Installation troubleshooting
 - Overview: Aspera Connect installation troubleshooting
 - Connect prompt continues to appear
 - Windows OS: Error when installing with a non-admin account
 - Windows OS: Connectivity issues
 - MacOS X: Connectivity issues
 - Linux: AppArmor prevents access to Connect

- Linux: Connectivity issues
- Aspera for desktop transfer client
 - What is IBM Aspera for desktop?
- Troubleshooting
 - Failure notification types and locations
 - Transfer issues
 - IBM Aspera Connect common issues
 - Connect prompt continues to appear
 - Retry the transfer
 - Resending "Draft" packages
 - Node-to-node transfer issues
 - Slow transfer speeds
 - Specific transfer failures
 - More transfer troubleshooting resources
- Other Issues
 - Email notifications
 - Connect prompt continues to appear
 - Can't access a shared folder
 - Delete large files and folders
 - Rename large folders
 - Specific error messages
- New and Coming Soon
 - Coming soon to Aspera on Cloud
 - What's new in Aspera on Cloud
- Legal Notice

IBM Aspera on Cloud

Welcome to Aspera on Cloud.

- [Admin](#)
- [User](#)

Getting started

- [What is IBM Aspera on Cloud?](#)
- [What's New in Aspera on Cloud](#)
- [Getting Started](#)
- [System Requirements, Firewall Settings, and Browser Support](#)
- [Planning Your Aspera on Cloud Implementation](#)

Common tasks

- [Secure the Access Credentials for your Built-in Node](#)
- [Installing Aspera Connect](#)
- [Sending Files and Folders](#)
- [Sharing Folders](#)
- [Sharing a Folder from a Node to Workspace Members](#)

Troubleshooting and support

- [Troubleshooting](#)
- [Coming Soon to Aspera on Cloud](#)

© Copyright IBM Corporation 2020

Admin

- [Get started](#)

Welcome to IBM Aspera on Cloud (AoC). Use articles in this section to build foundational knowledge of key aspects of AoC like workspaces, applications, shared inboxes, user roles, and much more. Understand prerequisites including firewall configuration. Learn how AoC protects your content using standards-based authorization, access keys, encryption, and configuration options in each application. Get guidance on how to set up and customize your organization, including event notifications and attaching storage.
- [Access security and credentials](#)

Set token duration, configure primary and sub-access keys to grant and control access to content, track and manage the credentials to your built-in IBM Cloud storage, and troubleshoot access issues.
- [Content security](#)

This section includes an overview of the numerous content security configuration options in Aspera on Cloud. Other articles describe how to configure both server-side and client-side encryption, including a detailed procedure for bringing your own key (BYOK) by integrating your IBM Key Protect KMS. Another detailed procedure describes how to configure watermarking by integrating your Irdeto watermarking service.
- [Authentication](#)

Configure the appropriate authentication method for your organization. Articles detail setting up SAML, IBMid (enabled by default), and Google authentication methods. Implement multifactor authentication for IBMid. Avoid admin lockout when disabling IBMid for another authentication method. Learn how to configure the login page to guide users to the proper authentication method.
- [Subscription usage and billing](#)

Understand your subscription and its features. Learn how to manage your storage usage, transfer volume, and egress, and how your billing reflects your usage.
- [Aspera Connect transfer client](#)

Learn how to install the IBM Aspera Connect transfer client, how to help outside users install Connect, and how to troubleshoot installation problems.
- [Attach cloud and local storage](#)

Understand how to give your AoC users access to content in your cloud and on-prem servers by connecting them as *nodes* to Aspera on Cloud. Review supported cloud providers and regions. Learn strategies to manage storage available to your users in the Files and Packages apps. Create network policies to manage node access for enhanced security. Create node policies to set encryption ciphers, default target rates, event logging, recursive counts, and more.
- [Workspaces](#)

Workspaces are a key organizational unit in Aspera on Cloud. Depending on your AoC subscription, you can configure each workspace with specific security, access, and collaboration settings, add specific members, provide access to specific storage, and enable specific apps like Files and Packages. Delegate specific local admin tasks to a workspace manager. Share specific content from your storage to specific workspace members.
- [Users and groups](#)

Understand and assign user types and roles. Create and manage users and groups. Manage memberships in workspaces, shared folders, shared inboxes, and more. Troubleshoot membership issues.
- [Packages app: Send and receive files and folders](#)

The Aspera on Cloud Packages app lets users send and receive digital "packages", collections of files, folders, images, and video. Learn how to configure collaboration rules that govern content exchange within and beyond the workspace. Configure and manage shared inboxes that allow all inbox members to access content sent to the inbox, enhancing and accelerating team activities. Troubleshoot issues related to sending digital packages.
- [Files App: Using a shared file repository](#)

The AoC Files app allows users to share access to a file repo. Learn how to share content from your cloud or local storage with Files app members. Configure collaboration rules that govern how and with whom members can share content. Understand content permissions and security. Troubleshoot shared folder access issues.
- [Activity app: Monitor events, activity, and usage in your organization](#)

The AoC Activity app gives detailed insight into activity and usage in your Aspera on Cloud organization. Learn how to monitor transfer activity, volume usage, and

application events. Create detailed reports to export or download. Customers can ingest Activity API events like application and security events, volume usage and transfer details into their analytics tool of choice.

- **[Automation app: Automate your transfer workflows](#)**

Review Automation app highlights, key concepts, and prerequisites. Enable the app and add users. Link to the Automation app API. Understand and configure workflows triggers, actions, and jobs.

- **[Troubleshooting](#)**

Address issues with transfers, access, notifications, and more. Subscribe to app status information, maintenance schedules, and new features announcements. Get access to IBM Support.

- **[Integration and APIs](#)**

Integrate your AoC organization with other Aspera products like transfer clients and servers. Integrate your IBM Key Protect KMS or your Irdeto watermarking service. Register an API client to build your own integration.

- **[Notifications and announcements](#)**

Important notifications and announcements for IBM Aspera on Cloud.

- **[New and Coming Soon](#)**

As a SaaS solution, IBM Aspera on Cloud receives frequent updates to deliver new features, functionality, and bug fixes. Get previews into upcoming new features and get insights into enhancements and features as they are released, including links to details user documentation.

- **[Legal Notice](#)**

Get started

Welcome to IBM Aspera on Cloud (AoC). Use articles in this section to build foundational knowledge of key aspects of AoC like workspaces, applications, shared inboxes, user roles, and much more. Understand prerequisites including firewall configuration. Learn how AoC protects your content using standards-based authorization, access keys, encryption, and configuration options in each application. Get guidance on how to set up and customize your organization, including event notifications and attaching storage.

- **[Try Aspera on Cloud for free](#)**

You can try Aspera on Cloud for free. You can use your Aspera on Cloud trial for 14 days or for 50 Gb of transfer volume, whichever happens first. Your trial subscription is the Standard Plus edition; you can change to a different edition when you convert to a paid subscription if you wish; note that some features are not available in the Essentials and Pay/Go editions.

- **[Get to know Aspera on Cloud](#)**

This section answers some fundamental questions about Aspera on Cloud. What is this app? What is a transfer? What is a workspace? And what is Aspera Connect, the transfer client that drives desktop-based uploads and downloads? Aspera on Cloud allows you to send files and to share them; understand the difference and when to use which in these brief introductory articles.

- **[Prerequisites](#)**

Understand system requirements, minimum software versions, browser support, and requirements for SSL certificates and firewall configuration.

- **[Access security and content security](#)**

These articles describe security measures including the various access keys that protect storage; the authorization options available to protect app access; and the many content security controls available to administrators. This section also describes data logging and retention, including content storage durations and treatment of personally identifiable information (PII).

- **[Customize for your use case](#)**

Define your own use case so that you can maximize the value of this very flexible application. Consider and configure the controls available to protect user privacy and define how app members collaborate with each other and with outside users. Articles in this section also introduce options to integrate AoC with other IBM products and options to allow users and groups to access content in your local and cloud storage.

- **[Set up your organization](#)**

This section guides your initial setup and how to accelerate configuration. Articles describe how to brand your organization, provide login guidance for your users, and give users access to specific content in your storage. Also discussed are how to add users, delegate management tasks, configure default storage locations, and configure session and token durations.

- **[Configure email notifications for your organization](#)**

Aspera on Cloud provides numerous user notification options, including for events like being invited to join the organization, receiving a package, being invited to send a package, and many more. These articles describe how to use and customize the default notification templates provided, and how to control which events generate notifications.

- **[Storage and workspace configuration scenarios](#)**

This section provides detailed, step-by-step configuration guidance for some typical usage scenarios, including configuring workspaces, users and groups, collaboration scenarios, and related notifications, designed to be adapted to the specifics of your use case.

Try Aspera on Cloud for free

You can try Aspera on Cloud for free. You can use your Aspera on Cloud trial for 14 days or for 50 Gb of transfer volume, whichever happens first. Your trial subscription is the Standard Plus edition; you can change to a different edition when you convert to a paid subscription if you wish; note that some features are not available in the Essentials and Pay/Go editions.

For a free trial of Aspera on Cloud or to convert to a paid subscription, go to <https://www.ibm.com/cloud/aspera/pricing>.

To set up your new trial organization, see [Set up your organization](#).

Keep in mind that your trial subscription gives you the Standard Plus edition; if you convert to a different paid edition, available features and volumes will change.

Important: Sending packages to external users is not available in the trial. To test this feature, contact the support team or your IBM sales representative. Alternatively, you can add the recipient as a user in your instance and send them the package directly.

Get to know Aspera on Cloud

This section answers some fundamental questions about Aspera on Cloud. What is this app? What is a transfer? What is a workspace? And what is Aspera Connect, the transfer client that drives desktop-based uploads and downloads? Aspera on Cloud allows you to send files and to share them; understand the difference and when to use which in these brief introductory articles.

- **[What is IBM Aspera on Cloud?](#)**
Aspera on Cloud is IBM's on-demand SaaS offering for global content transfer and exchange. The service enables organizations to move large files and data sets – securely and reliably – across on-premises and multi-cloud environments at unrivaled speed.
- **[What is a transfer?](#)**
A transfer moves files and folders from one storage location to another (examples of storage locations include your own local machine, a remote server, public or private cloud storage).
- **[What is a package?](#)**
In the Packages app, a package (also called a digital package) is a collection of digital assets (files, folders, video, images, etc.) that you gather to send to one or more individuals or user groups, or to an Aspera on Cloud shared inbox. When you send a package, Aspera on Cloud creates copies of the content you attach for each recipient; the source content remains unchanged.
- **[Applications: Overview](#)**
An Aspera on Cloud application is a self-contained service with its own memberships and configuration settings.
- **[What is a workspace?](#)**
The workspace is a collection of Aspera on Cloud users working together—on a project perhaps, or in a department or division. Users in a given workspace can freely collaborate with other members of the same workspace.
- **[What is a shared inbox?](#)**
An Aspera on Cloud Packages app shared inbox is an optional workspace feature similar to a drop box: you can send content directly and simultaneously to all members of the shared inbox without having to address it to particular users or user groups.
- **[What is IBM Aspera Connect?](#)**
Aspera on Cloud requires one of two transfer methods to power high-speed transfers between user desktops and Aspera transfer servers. Users can either download and install Aspera Connect, a free, lightweight, install-on-demand software program; or you can configure the IBM Aspera HTTP Gateway and attach it to your Aspera on Cloud organization.
- **[Should I send or share?](#)**
Sending files and folders using the Packages app and sharing folders in your Files app both initiate a FASP (fast, adaptable, secure, predictable) transfer. However, there are important distinctions between sending content and sharing content using Aspera on Cloud.
- **[Key elements and roles in Aspera on Cloud](#)**
This article describes the elements of your Aspera on Cloud organization, including workspaces and applications, along with key roles like organization admin, ATS admin, standard and limited users, and so on.
- **[Multi-session transfers](#)**
Multi-session transfers simultaneously transfer large files dividing them into smaller segments through multiple sessions. Instead of relying on a single transfer session, you can distribute the workload across several parallel sessions. This process takes advantage of the combined bandwidth from multiple connections.
- **[What is a transfer?](#)**
A transfer moves files and folders from one storage location to another (examples of storage locations include your own local machine, a remote server, public or private cloud storage).

What is IBM Aspera on Cloud?

Aspera on Cloud is IBM's on-demand SaaS offering for global content transfer and exchange. The service enables organizations to move large files and data sets – securely and reliably – across on-premises and multi-cloud environments at unrivaled speed.

Using Aspera on Cloud, organizations can store and readily access files and folders in multiple cloud-based and on-premises storage systems. Sharing among users is as easy as browsing or dragging-and-dropping – regardless of where the files are located – freeing collaboration from traditional boundaries among colleagues in both local and remote locations.

Aspera on Cloud uses IBM Aspera's FASP protocol, which overcomes the limitations of other file-transfer technologies. By moving large data sets at maximum speed, reliably and securely – regardless of network conditions, physical distance between sites, and file size, type, or number – Aspera technology enables a new world of collaboration, sharing, and content delivery.

Aspera on Cloud highlights include the following:

- Domain security within the application
 - Intuitive file management tools
 - Multiple permission or access levels for individual files and folders, configurable per user or group
 - Ability to send content to multiple recipients using an intuitive, email-like interface
 - Simple sharing of files and folders
 - Configurable permissions to share with and send to outside users who do not have an Aspera on Cloud account
 - Comprehensive administrative console
 - Support for IBM Aspera transfer service, enabling automated self-scaling of transfer capacity to maximize performance while minimizing cost
 - RESTful Platform API (including users, permissions, transfers, and reporting)
- For AoC API documentation, see [IBM API Hub](#). For more information about integrations and related APIs, see [Integration and APIs](#).

What is a transfer?

A transfer moves files and folders from one storage location to another (examples of storage locations include your own local machine, a remote server, public or private cloud storage).

Aspera's FASP® transfer technology allows Aspera on Cloud users to share and send files and folders quickly, easily, securely – overcoming the traditional problems and bottlenecks of other transfer technologies.

For example, these are some of the operations you may perform that initiate a FASP transfer:

- Send or receive a [digital package](#) in your Packages app

- Download content you receive in a package
- Move files and folders from a package to your Files app
- Move files and folders from one directory to another directory within the Files app

The transfer may be a copy-and-paste action to the new location, leaving the source content intact in the original location. Or it may be a copy-and-delete operation, pasting the content to the new location while deleting the original content in the source location.

You can monitor active transfers and review completed transfers in the [transfer monitor](#).

There are four transfer types in Aspera on Cloud:

- These two transfer types require either the [IBM Aspera Connect](#) app and browser extension or [Aspera HTTP Gateway](#):
 - **Upload:** Uploading content from your local machine or from a local or remote storage location into an Aspera on Cloud workspace. This is typically a copy/paste operation, leaving the source content intact in the original location. Most Send operations are also uploads, copying the content to an interim location on a transfer server accessible to the recipient for download.
 - **Download:** Downloading content from the Aspera on Cloud workspace to your local machine, or to a local or remote storage location. This is also typically a copy/paste operation, leaving the source content in Aspera on Cloud intact while duplicating it in the target location.
- These two transfers types do *not* use Aspera Connect or Aspera HTTP Gateway; these are FASP-native transfers:
 - **Node-to-node:** Also called **share-to-share**. Moving content from one Aspera transfer server to another. This may be the case when moving files and folders from one location to another in your Aspera on Cloud workspace – for example, when you move files or folders from a package you received in your Packages app to a location in your Files app. Moving content from one location to another within your Files app may also be a transfer, depending on the source and destination locations. Such a move can be a copy or a move operation; hold the Alt key while you drag to change the default action (the default action varies based on the source or destination location; see also [Move or copy content in your Files app](#)).
 - **Intra-node:** Moving content from one location on an Aspera transfer server to another location on the same server. This may be the case when moving files and folders from one location to another in your Aspera on Cloud workspace. For example, when you move files or folders from a package you received in your Packages app to a location in your Files app; or when you move items from one directory to another within the Files app.

What is a package?

In the Packages app, a package (also called a digital package) is a collection of digital assets (files, folders, video, images, etc.) that you gather to send to one or more individuals or user groups, or to an Aspera on Cloud shared inbox. When you send a package, Aspera on Cloud creates copies of the content you attach for each recipient; the source content remains unchanged.

Introduction

For a procedure, see [Quick start: Send files and folders](#).

Aspera on Cloud allows you to use your Finder or Explorer to browse your local desktop, hard drive, or a remote source to select content to add to the package. You can also drag and drop content from any of these sources to the package as you construct it.

You can also attach files and folders in your Files app as you create a digital package in the Packages app; simply right-click the items in your Files app to include in the package and select the option to send. You can add content to a package you initiate from the Files app.

Once you are satisfied with the contents of the package, you can send it to the recipients you designate. Recipients can be:

- One or more of the following:
 - Aspera on Cloud users or groups in your workspace
 - All members of your Aspera on Cloud workspace (depending on settings configured by your admin)
 - Aspera on Cloud users outside your workspace, or users who do not have an Aspera on Cloud account (depending on settings configured by your admin)
- An Aspera on Cloud shared inbox (depending on settings configured by your admin)

Once you have sent the package, you must [recall](#) it to add, change, or remove the content in it. Your recipients can view, move, download, change or delete the copies of the content you send them without affecting the source content. For more information, see [Should I send or share?](#)

Monitor package transfer

Sending a package initiates a [FASP transfer](#); if desired, you can monitor the transfer in the [transfer panel](#) . You can also view statistics for recent, completed transfers.

Your Inbox and Sent folders

When the transfer completes, Aspera on Cloud displays the package in your recipient's Inbox and in your Sent folders. From that location, you and your recipient can do the following:

- Open the package to view its contents, along with summary details about the transfer, including status, size, average rate, duration, whether the package has been downloaded by recipients, and other information.
- Download all or part of the content to your local machine or to a remote storage location.
- Move package contents directly into your Files app.

Drafts folder

When a package transfer fails to start, AoC displays a toast message and moves the package to the Drafts folder in your Packages app. You must resend the Draft package with the intended content. See [Resending "Draft" packages](#).

Package details panel

You can click any package row to display the package contents and the package details panel. Click More detail to see package info like size, date, and contents (except archived and deleted packages), average transfer speed, package metadata if applicable, package recipients, and which recipients have downloaded all or part of the package.

Applications: Overview

An Aspera on Cloud application is a self-contained service with its own memberships and configuration settings.

What is an Aspera on Cloud application?

Each application can be configured at the global, organization level and at the [workspace](#) level. Organization-level settings are inherited by each workspace. The administrator (or, with proper permissions, the workspace manager) can override the inherited settings and customize them for a given workspace.

Aspera on Cloud supports the following apps:

- Packages app: sending and receiving digital packages:
 - Can be enabled or disabled for the organization.
 - When enabled for the org, can be turned on or off for each workspace.
 - When turned on for a workspace, all workspace members automatically become Packages app members; org admin or workspace managers (with proper permissions) can remove individual workspace members from the Packages app.
 - Configured globally; global settings inherited by each workspace; inherited settings can be overridden and customized at each workspace.
- Files app: sharing folders
 - Can be enabled or disabled for the organization.
 - When enabled for the org, can be turned on or off for each workspace.
 - When turned on for a workspace, all workspace members automatically become Packages app members; org admin or workspace managers (with proper permissions) can remove individual workspace members from the Packages app.
 - Configured globally; global settings inherited by each workspace; inherited settings can be overridden and customized at each workspace.
- Activity: monitoring transfer activity, volume usage, events:
 - Can be enabled or disabled for the organization.
 - Not specific to a given workspace.
 - When enabled, an org admin can add users as members of the Activity app.
- Automation app: automating workflows:
 - Can be enabled or disabled for the organization.
 - Not specific to a given workspace.
 - When enabled, an org admin can add users as members of the Automation app.
- Admin: configuring users, nodes, apps, workspaces, and so on:
 - Always enabled; accessible to all organization administrators.
 - Portions of the Admin app are available to workspace managers, depending on permissions granted to them.

The Packages application

Members of the Packages application use it to [send and receive digital packages](#). A [package](#) is a collection of digital assets (files, folders, video, images, and so on) that you gather to send to one or more individuals or user groups, or to an Aspera on Cloud shared inbox. When you send a package, Aspera on Cloud creates copies of the content you attach for each recipient; the source content remains unchanged.

The Packages app also allows users to [invite other people to send](#) files and folders back to them or to a shared inbox.

By default, Packages app members can collaborate freely with external users. Org administrators can gradually restrict external collaboration, all the way to eliminating it.

For configuration procedures, see [Packages app: Send and receive files and folders](#).

The Files application

Members of the Files app use it to [share folders](#) in a workspace with one or more individuals or user groups. When you share, you assign [access permissions](#) for each folder to each recipient you share with. When you share folders, Aspera on Cloud does not create a separate copy, but grants the recipients access to the exact same materials you have access to. For configuration procedures, see [Configuration options](#).

By default, Files app members can collaborate freely with external users. Org administrators can gradually restrict external collaboration, all the way to eliminating it.

For more information, see [Should I send or share?](#).

The Activity application

The Activity application provides analysis and visualization of performance, history, and usage for file transfers made within Aspera on Cloud. The responsive engine automatically feeds real-time logs to the Activity server for output in the UI, so that you can easily associate the log data with user data and transfer statistics.

See [Activity app: Monitor events, activity, and usage in your organization](#) and related topics.

The Automation application

The Automation app lets you to create automated workflows that initiate file transfers, make calls to an API, and send notifications to users.

Automation monitors your file storage system for event triggers; for example, a specific date and time can initiate a transfer, and a file upload to a shared folder can trigger an email notification.

See [Automation app: Automate your transfer workflows](#) and related topics.

The Admin application

The Admin app provides all the controls to configure organization branding, workspaces, collaboration rules, users, nodes, content, and more. Organization administrators can delegate certain tasks to workspace managers. For these administrative tasks in the designated workspaces, managers use the Admin app.

What is a workspace?

The workspace is a collection of Aspera on Cloud users working together—on a project perhaps, or in a department or division. Users in a given workspace can freely collaborate with other members of the same workspace.

You need specific permissions, configured by the organization administrator or workspace manager, to collaborate with users outside the workspace.

The users, packages, files, and folders in one workspace are completely separate from those in another workspace.

The workspace name displays in the upper left corner, immediately below the app name (Files or Packages apps).

Membership in multiple workspaces

You may be a member of more than one workspace. You may have different permissions and access in one workspace than you do in another.

If you are a member of multiple workspaces, you can display them by clicking the caret beside the workspace name, then selecting the intended workspace to switch to it. If you have membership in more than five workspaces, you can pin one or more to keep them at the top of your list for convenient access.

Note: Multiple workspaces are available depending on your subscription edition. To see your edition, click the User icon and see Account settings > Account > IBM Aspera on Cloud Edition.

Workspaces in the Packages app

As a workspace member in the Packages app, you send and receive [digital packages](#). You can access your personal inbox ("My Inbox"), which contains the packages sent to you as an individual. You can also access your sent, archived, and deleted or expired packages.

Optional Permissions

You may also have the following capabilities in your Packages workspace:

- Sending to people who are not members of your workspace.
- Sending a [file request](#) to someone outside your workspace, inviting them to send you a digital package.
- Membership in one or more [shared inboxes](#).

Note: Shared inboxes are available depending on your subscription edition.

Workspaces in the Files app

As a workspace member in the Files app, you have access to a collection of folders shared with you by your administrator and by other members of your workspace. When others share a folder, they may share it with you only, or they may share it with multiple people. Your collection of folders may be very different than the collection of another user in the same workspace, though you may share some of the same folders.

The person sharing also grants various [permission levels](#) to these folders and their contents (for example: view, download, delete, and several others); your permission to one folder may be different than your permission to another folder. Similarly, your permission to a folder may be different than the permission another user has to that folder.

Even when folders are shared with multiple members of your workspace, you can move and rename folders without affecting the location and naming of those same shared folders in other users' applications. However, for important conditions regarding deleting shared folders and files from your Files app, see [Delete files and folders](#).

You can share folders in your workspace with other members of your workspace; you may also be able to share folders with people outside your workspace.

Note: In rare circumstances, folders in your workspace may display in red, indicating that they are currently unavailable; contact your administrator or workspace manager for assistance.

Optional permissions

You may also have the following capabilities in your Files app:

- [Uploading](#) files and folders into your Files app workspace; the content you upload remains private to you until you share it with others.
- [Creating new folders](#) in your workspace.
- [Sharing](#) a folder with someone outside your workspace.

What is a shared inbox?

An Aspera on Cloud Packages app shared inbox is an optional workspace feature similar to a drop box: you can send content directly and simultaneously to all members of the shared inbox without having to address it to particular users or user groups.

An Aspera on Cloud administrator or workspace manager creates the shared inbox, then designates members of the shared inbox from among the workspace members; each member has specific permissions to the inbox.

You as an individual user in the workspace may have membership in one or more shared inboxes, or in none. You may have different permissions in each shared inbox. Your permissions may be different than the permissions of other shared inbox members.

Am I a member of a shared inbox?

Find your shared inboxes, if any, as follows:

- For inboxes to which you have Receive or Add users permission:
 - Click Inboxes in the left panel. Any inboxes in the list that are not labeled My Inbox are your shared inboxes. Click the shared inbox name to display the content in that shared inbox only.
 - Click Send files, then click in the To field of the form to display all shared inboxes to which you can send packages.
- For inboxes to which you have only Send permission, click Send Files, then click the Recipient field of the form to display the list of shared inboxes to which you can send packages.

When you send a [digital package](#) to a shared inbox, you send to all members of that shared inbox simultaneously; each shared inbox member receives their own copy of the content you included in the package. As with all package sending in Aspera on Cloud, sending content to a shared inbox initiates a [transfer](#), which you can monitor in the [Transfer monitor](#) if you wish.

Metadata

The Aspera on Cloud administrator or workspace manager can configure metadata fields for each shared inbox, and can make these fields either optional or required. When present, these fields allow senders to apply metadata tags to packages they send to a shared inbox; these tags provide information about package contents without requiring the recipient to open the package, and allow shared inbox members to search and sort packages easily. If any metadata data fields are required, you cannot send the package without addressing the required field.

Permissions

Shared inbox members may have one or more access permissions (configured by the Aspera on Cloud administrator or the workspace manager) to a given shared inbox; users see the shared inboxes they have at least one permission to in the list of all inboxes on the left side panel.

- **Send:** Members with Send permission can send packages to the shared inbox.
 - Click Send files; in the form that displays, click the To field to display a list of shared inboxes to which you have Send permission.
 - See [Sending: Detailed procedure](#).
 - Members with only Send permission cannot see contents or receive packages from this shared inbox.
- **Receive:** These members can access packages sent to the shared inbox.
 - In the list of all inboxes on the left side panel, click the shared inbox name; packages in the shared inbox display.
 - Members with only Receive permission cannot send a package (upload files or folders) to the shared inbox.
- **Add users:** These members can invite others to send packages to the shared inbox.
 - In the list of all inboxes on the left side panel, click the shared inbox name.
 - In the Collaboration panel on the right, look for the Add button; if present, this member has Add permission to this shared inbox.
 - See [Request a package to a shared inbox](#) for details.

What is IBM Aspera Connect?

Aspera on Cloud requires one of two transfer methods to power high-speed transfers between user desktops and Aspera transfer servers. Users can either download and install Aspera Connect, a free, lightweight, install-on-demand software program; or you can configure the IBM Aspera HTTP Gateway and attach it to your Aspera on Cloud organization.

Aspera Connect is the default transfer method for Aspera on Cloud and other Aspera web app. However, if your deployment of Aspera on Cloud does not permit the download and installation of client software, the admin can [configure](#) an alternative transfer method: the [IBM Aspera HTTP Gateway](#). Otherwise, all users must install the Aspera Connect transfer client and the Connect browser extension to complete high-speed transfers.

Once installed, Connect runs automatically when you transfer content using one of the Aspera web apps. In Aspera on Cloud, Connect typically runs in the background rather than on screen as in many of the other Aspera web applications.

Important: Connect comprises an app and a browser extension; you must install both as follows:

- You must install the Connect app once on your computer.
See [Installing Aspera Connect](#).
- You must install the Connect extension for each browser (except Internet Explorer) you'll use to access Aspera on Cloud.
See the appropriate article:
 - [Adding the Chrome browser extension for Connect](#).
 - [Adding the Firefox Connect Browser Extension](#).
 - [Adding the Safari browser extension for Connect](#).
 - [Adding the Microsoft Edge browser extension for Connect](#).

If required, you can configure Connect to change default settings for download location, transfer bandwidth, and various network and security settings. Configure Connect settings with the guidance of your Aspera administrator. Note that the Connect Transfers window displays all your recent transfers, whether through Aspera on Cloud or another Aspera product.

After each successful login, Aspera on Cloud checks to see whether the most recent version of Connect is running on your machine. If a Connect upgrade is available, Aspera on Cloud prompts you through the upgrade process.

If you have any issues with Aspera Connect performance, run the [IBM Aspera Connect Diagnostic Tool](#). See also [Installation troubleshooting](#) and [IBM Aspera Connect common issues](#). For more details, see the [IBM Aspera Connect product documentation](#).

Should I send or share?

Sending files and folders using the Packages app and sharing folders in your Files app both initiate a FASP (fast, adaptable, secure, predictable) transfer. However, there are important distinctions between sending content and sharing content using Aspera on Cloud.

If you are an admin, remember that in any organization or workspace, you can allow users to send, or share, or both. You can configure transfer options based on what your team is used to or on how you want your team to perform transfer tasks.

Introduction

Send: Like sending an email with attachments

Sending files and folders using the Aspera on Cloud *Packages app* is very much like sending an email with attachments. Senders use a simple form to address recipients and attach content. Recipients receive a copy of the content and can download it to use however they want.

Share: Like collaborating in a shared file repo

Sharing folders using the Aspera on Cloud *Files app* is like collaborating using a shared file repository. Each user has access to certain folders in the repo, with specific permissions to each folder and its contents. Files app users can share their folders with others, assigning content permissions to each recipient. Keep in mind that when you upload to your Files app, no one sees your folder until you share it with them.

Send: Send a copy of files and folders using the Packages app

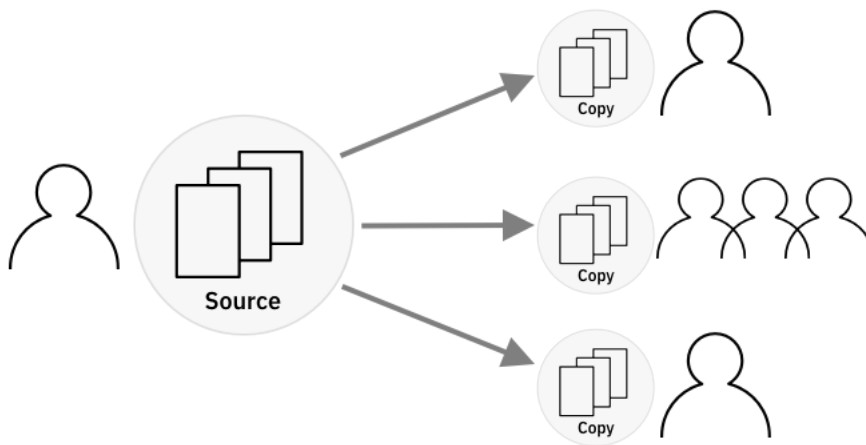
Use the AoC Packages app to send, receive, and request files and folders.

When you send files and folders, you send a *copy* of the source content to your recipients.

- You cannot modify the copy once you send it. Changes you make to the source content do not affect the copy you sent.
- Changes the recipient makes to the copy do not affect your source.
- Your recipient can act in any way on their copy of the content you send. Unlike sharing, you do not assign permissions to content you send.

You can send files and folders from any connected source: your own computer, an attached drive, share, or cloud storage, your Files app, and so on.

To request files, send a [submission link](#), also called a *file request*. Such a link enables another user to send files and folders to you.



Who can send to whom?

By default, any workspace member with access to the Packages app can send files to and request files from anyone else. Workspace members may also be able to send to users and groups outside the workspace.

As an admin, you can protect content security by using any of several options to restrict valid recipients outside the workspace. If necessary, you can keep all Packages app exchanges within the realm of the workspace. For details, see [Collaboration: Open or closed?](#) and [Content security in the Packages app](#).

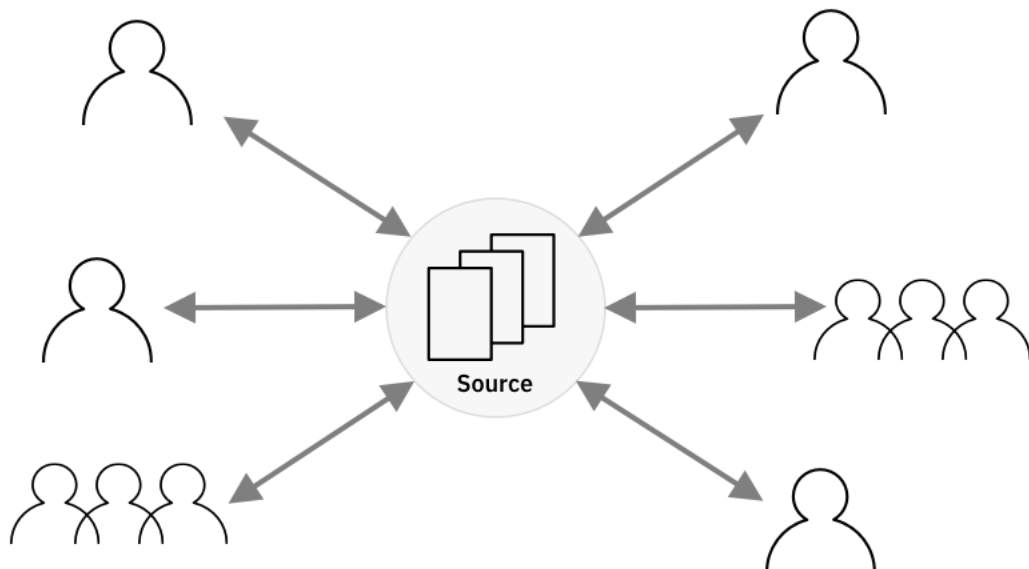
Share: Give others access to your *source* content using the Files app

Use the AoC Files app to share folders.

When you share a folder, you give others access to your *source* content. The folder content is *live*: all users with shared access can update folder contents and see the updates others make. You assign access permissions to the folder for each person you share with. These permissions determine what that person can do with the folder you share.

The folder to share must be in your AoC environment. There are three ways to get content into your Files app:

- You can upload a folder to your Files app and share it. Other members of your workspace won't be able to see the folder you upload until you share it. You can also upload a file, but you can only share a folder. To share a file, place it in a folder and share the folder.
- When someone shares a folder with you, it appears in your Files app. You can share a folder that has been shared with you.
- You can move files and folders from your Packages app to your Files app. Once in the Files app, you can share it.



Who can share with whom?

By default, any workspace member with access to the Files app can share folders with anyone else. As an admin, you can protect content security by using any of several options to restrict valid recipients outside the workspace. If necessary, you can keep all Files app exchanges within the realm of the workspace. For details, see [Collaboration: Open or closed?](#) and [Content security in the Files app](#). For configuration procedures, see [Files App: Using a shared file repository](#).

Shared content permissions

When you upload a folder to your Files app, you have all permissions to it. When someone shares a folder with you, you have the permissions they assign to you.

Permissions may include:

- Browse (View)
- Preview
- Rename
- Upload to
- Download
- Delete
- Create a new folder in

When you share a folder, you assign permissions to each user you share with. You can assign, at most, only the permissions that you yourself have to the folder; you can also share a folder and grant fewer permissions than you have to it.

For example, if a colleague shared a folder with you, giving you Browse, Preview, and Delete permissions, you can share that folder with another person, giving them the same Browse, Preview, and Delete permissions that you have. You can also share the that folder with only Browse permission. But you cannot share the folder with Download permission, since you don't have that permission to the folder. For a full discussion, refer to [Content permissions](#).

Key elements and roles in Aspera on Cloud

This article describes the elements of your Aspera on Cloud organization, including workspaces and applications, along with key roles like organization admin, ATS admin, standard and limited users, and so on.

Key elements

The following table summarizes the key elements of IBM Aspera on Cloud (AoC).

Element	Definition
Subscription	Each subscription has one owner. A subscription may contain one or more organizations. A subscription is a billing/business entity rather than a logical software entity.
Organization	One or more per subscription. The organization is the primary container and administrative unit. An org contains one or more workspaces; a workspace is the primary element in which users collaborate. Certain configurable settings at the organization level are inherited by workspaces; for example: branding (logos, etc.), email templates.

Element	Definition
Applications	Applications in Aspera on Cloud are: • Admin • Files • Packages • Activity • Automation Admin app The Admin app is automatically enabled for every organization admin. Relevant portions of the Admin app are automatically available to users who have been granted workspace manager privileges. Files and Packages apps Files and Packages apps can be individually enabled/disabled for the organization by the organization administrator. The org admin can also configure these apps at the global level. Global settings are inherited at each workspace in the org; inherited settings can be customized at each workspace. See 'Hierarchy and Inheritance' below. Each app enabled at the org level can be enabled and configured at the individual workspace level. Applications enabled for a given workspace are available for all workspace members. A new member of the workspace automatically gains access to the apps enabled in that workspace. Activity app When the Activity app is enabled in the organization, it can be enabled for specific users. Until you add organization members as members of the Activity app specifically, they cannot see or access the Activity app. Automation app When the Automation app is enabled in the organization, it can be enabled for specific users. Until you add organization members as members of the Automation app specifically, they cannot see or access the Automation app.
Workspace	One or more per Aspera on Cloud organization. A workspace is the digital space in which teammates collaborate. The workspace contains a team of AoC users working together -- on a given project, for example, or perhaps in a department or division -- along with their files, folders, and packages. Users in a workspace can freely collaborate with other members of the same workspace. However, they need specific permissions to collaborate with users outside the workspace. See 'Collaboration: Open or Closed?', below. The packages, files, and folders in one workspace are completely separate from those in another workspace. An individual user may have membership in more than one workspace, and may have different permissions and access in one workspace compared to another. However, they cannot move files and folders from one workspace to another. The org admin can delegate certain workspace-level administrative tasks to a workspace manager. See 'Delegating to a Workspace Manager' below.
Packages app	The Packages app enables app members in a workspace to send digital packages (collections of files and folders) to other people using an intuitive, email-like interface. Files and folders to send can reside on any connected local, remote, or cloud storage, including files and folders in the Files app. A Packages app member in a workspace can freely send packages to other workspace members. With proper permissions, the member can send packages to AoC users outside the workspace, or to people who do not have an AoC account. A Packages app member in a workspace can also send a digital package to a shared inbox in the workspace, provided that the member has 'Send' permission to the shared inbox. The Packages app also provides a 'file request' capability, which allows members to send an email inviting the recipient to send a digital package. The email contains a link (called a submission link) that allows the recipient to use IBM Aspera's high-speed transfer technology to send the folders and files requested. Admins can enable or disable this feature based on user type (workspace member or workspace manager). The Packages app provides each app member several sortable, filterable lists of packages: • <i>My Inbox</i> presents packages received by the user as an individual, as opposed to packages sent to a shared inbox. • <i>Sent</i> presents packages sent by the user. • <i>Archived</i> presents received packages that the user has moved from the Inbox. • <i>Deleted/Expired</i> is the listing of (1) sent packages that the sender later deleted, (2) packages that expired due to an applied policy. In both cases, the contents of the package are no longer available, although package details and transfer statistics are still viewable by clicking the package row. • A Packages app member may be a member of one or more shared inboxes in the workspace; the shared inbox listing presents packages sent to the shared inbox. See 'Shared inbox' below for more details.
Digital package	A feature of the Packages app, a digital package is composed of one or more files and folders, collected by a user to send to someone else. Once sent, the package is an immutable 'master' copy of the transfer, enabling an auditable trail of senders, recipients, and content.

Element	Definition
Shared inbox	A optional feature of the Packages app in a given workspace, a shared inbox is a collection of users with shared access to the digital packages sent to the shared inbox. A shared inbox allows users to send content directly and simultaneously to all members of the shared inbox without having to address it to particular users or user groups. A shared inbox is similar to an email distribution list, and includes an easily accessible, filtered listing of packages sent to the inbox. A shared inbox is created by the AoC administrator or workspace manager, who designates members of the shared inbox from among the workspace members, then assigns each member one or more permissions to the inbox. Shared inbox permissions include: • Send: can send packages to the shared inbox. • Receive: can browse and download all packages sent to the inbox. • Add users: can add a new member to the inbox, granting them Send permission only. Each shared inbox member can have one or more permissions to the inbox. An individual user in the workspace may have membership in one or more shared inboxes, or in none; may have different permissions in each shared inbox, and permissions may be different than the permissions of other shared inbox members. A workspace member with 'Add users' permission to a shared inbox can invite a user from other workspaces or from outside the organization to become a member of the shared inbox. The invited user has 'Send' permission only to the shared inbox. The invited user is not a member of the workspace, but only a member of the shared inbox. This user becomes a limited member of the organization.
Files app	The AoC Files app allows users in a workspace to access a collection of folders. Folders in the Files app may be added by: • The administrator, who can make folders from a transfer server available to Files app users in a given workspace. • Files app users with permission to upload, who can share their folders with others. • Folders shared by other users. A workspace member with access to the Files app can freely share folders within the app with other workspace members. With proper permissions, the member can share folders with AoC users outside the workspace, or with people who do not have an AoC account. Files app members with proper permission can upload files and folders from any connected source to the app. and from there share the folder with others. Until the folder is shared, it is visible and accessible only to the user who uploaded it (and to the administrator). When users share folders with others, they grant each recipient specific permissions to act on the folder and its contents. Permissions presets bundle the atomic content permissions most often used together: • Edit (This is the highest level of permission and gives a user full control over the item, it contains all other permissions.) • Download (browse folder content, preview supported movie file types, download the folder or its contents) • Preview (browse and preview) • Upload (create and upload folders and upload files) Atomic custom permissions are also available: • Browse folder contents • Upload files and folders to the folder • Create or upload an empty folder in the shared folder • Download the folder or its contents • Rename the folder • Preview the movie files in the folder (thumbnail previews of supported image types are always available) • Delete or overwrite files and folders in the folder Users who receive shared access to a folder can in turn share it with others, according to their permission in the workspace and to their permissions to the specific folder. When re-sharing a shared folder, they can grant only the access they have to the folder, or less. Files app users can save content they receive in a package in the Packages app directly to their Files app (assuming they are member of both apps in the same workspace).
Shared folder	A feature of the Files app. Files app users with appropriate permissions can upload a folder from their own local or remote storage and share it freely with other Files app members in the same workspace, granting access permissions to each recipient as required. The recipients of the shared folder can then access it according to the permissions granted, and in turn share the folder with others, granting the same access permissions they have (or fewer) to their recipients. With proper permissions, the workspace member can also share the folder with AoC users outside the workspace, or with people who do not have an AoC account -- again, granting to their recipients the same access permissions they have (or fewer). With proper permissions, workspace members can use a public link to share a folder with outside users, which allows recipients to access the folder without having to log in. Org administrators or workspace managers can share folders directly from a node or storage to workspace members, sharing with all members or with specific members, and granting access permissions to each recipient as required. Such administratively-shared folders can be controlled by anyone with admin credentials.
Activity app	The Activity app gives app users deep insights into real-time and historical transfer usage and activities. Users can filter and display data along a number of axes: transfer usage per org, per workspace, per node, per user. App users can monitor transfer activity in real time, collect historical data to identify trends, monitor events and user activity to enhance security, and export reports for all of the above.
Automation app	The Automation app in Aspera on Cloud lets you to create automated workflows that initiate file transfers, integrate with external web services via API calls, and send event-driven email notifications to users. Automation monitors your file storage system for event triggers; for example, a specific date and time can initiate a transfer, and a file upload to a shared folder can trigger an email notification. The Job Queue page in the Automation app allows you to easily monitor all running and completed workflow jobs.

Key roles

The following table summarizes the key roles in IBM Aspera on Cloud.

Role	Definition
Subscription Owner	Responsible for all the usage charges incurred within the subscription.
Organization administrator	The master role in the organization; one or more per org. For the organization: • Configures all security, authorization, branding, notifications; registers API clients. • Enables and configures apps. • Creates and configures workspaces. May delegate certain configuration responsibilities for a given workspace to a workspace manager, whose responsibilities and privileges are applicable to that workspace only. • Monitors, manages, and reports on usage and transfer activities. • Configures existing transfer servers to support the AoC organization. May delegate these responsibilities to the infrastructure administrator (future). For users: • Creates and configures users and groups; user membership in groups, workspaces, and shared inboxes; user access to enabled apps; assigns user roles. May delegate some responsibilities to the workspace manager. For applications: • Enables and disables apps for the org and for individual workspaces; configures app settings globally and for workspaces; manages app members in each workspace. May delegate some of these responsibilities in a given workspace to a workspace manager. For workspaces: • Configures branding; members; security; event notifications; usage monitoring. May delegate these responsibilities in a given workspace to the workspace managers. • Enables and configures apps for each workspace. May delegate these responsibilities in a given workspace to the workspace managers. For shared inboxes (if any) in the Packages app in a workspace: • Configures membership and access permissions; metadata fields, collaboration settings; package expiration policies; notifications. May delegate these responsibilities to the workspace manager.
Transfer service administrator (ATS admin)	An organization administrator with additional privileges that enable the following activities: • Create a transfer service node. • Convert a trial subscription to a paid subscription. This role is automatically granted to the user account that first registers for a trial subscription to Aspera on Cloud. An existing ATS administrator in the organization can add transfer service admin privileges to an organization admin.
Workspace manager	Optional role created by the organization administrator. For a workspace, configures branding; manages members (including groups); configures and controls event notifications; monitors usage. For Files and Packages apps in the workspace, configures collaboration settings and URL styles. For Packages app, manages shared inboxes and members, package expiration policies, package security. For Files app, manages shared content. An organization admin can allow or disallow workspace managers' ability to change certain collaboration settings.
User	A standard user is a member of the AoC organization. This user has membership in at least one workspace in the organization.
Limited user	Limited users are not members of the AoC organization, although they do have login credentials to the org. AoC creates a limited user when a standard user sends an authenticated file request (also called a submission link) to an outside user, inviting that outside user to submit a digital package to a shared inbox. The invited user must create an account and log in to AoC to respond to the invitation; this user becomes a limited user in the organization, with authenticated access to that shared inbox only, without workspace membership. In addition, an organization admin creates a limited user when configuring any org member with no workspace membership.

Multi-session transfers

Multi-session transfers simultaneously transfer large files dividing them into smaller segments through multiple sessions. Instead of relying on a single transfer session, you can distribute the workload across several parallel sessions. This process takes advantage of the combined bandwidth from multiple connections.

Upload and download settings

To edit the multi-session transfer settings for uploads and downloads from local machines:

1. Open the Transfer monitor and click the three dot menu.
2. Click Multi-session transfer settings.
3. Click Open transfer client and modify the settings as needed in your transfer client.

Move and copy transfers settings

To edit the multi-session transfer settings for move and copy transfers:

1. Open the Transfer monitor and click the three dot menu.

2. Click Multi-session transfer settings.
3. Modify the settings in the Multi-session transfer size and Number of sessions fields as needed.

Multi-session transfer size

You can specify the minimum total transfer size (default is set to 5GB) that triggers the multi-session transfers. To do this, define the minimum file size in the Multi-session transfer size field. Increase or decrease the transfer size, and select the unit measurement you want to use (available options are Megabytes (**MB**), Gigabytes (**GB**), and Terabytes (**TB**)).

Number of sessions

By default, the number of sessions to be started per transfer is set to three. You can select a different option in the Number of sessions drop-down.

Prerequisites

Understand system requirements, minimum software versions, browser support, and requirements for SSL certificates and firewall configuration.

- [System requirements and browser support](#)
This article describes the very simple requirements for Aspera on Cloud. You must use a supported browser/version. If your organization includes users who cannot use the default transfer method, you must configure an alternative method. Depending on your network configuration, you may need to configure your firewall.
- [Firewall requirements](#)
Depending on your network, you may have to configure your firewalls to use Aspera on Cloud. This article describes how to allow traffic from your network to Aspera on Cloud and to and from any Aspera High-Speed Transfer Servers (HSTS) and cloud storage you attach to your AoC organization.

System requirements and browser support

This article describes the very simple requirements for Aspera on Cloud. You must use a supported browser/version. If your organization includes users who cannot use the default transfer method, you must configure an alternative method. Depending on your network configuration, you may need to configure your firewall.

Select an IBM Aspera transfer method

All transfers between Aspera on Cloud and a user desktop require one of these two transfer methods:

- **IBM Aspera Connect transfer client**
As the typical transfer method, Aspera Connect is a free, lightweight, install-on-demand software program that powers high-speed transfers between desktops and Aspera servers. Users must download and install the Connect client and, for most browsers, install a browser extension. The guided, in-app installation is quick and easy. For details, see [What is IBM Aspera Connect?](#)

Important: If you are using MacOS 10.12 or earlier, you must upgrade your OS or use Aspera Connect v3.11.
- **IBM Aspera HTTP Gateway**
The Aspera HTTP Gateway is a standalone product that uses both HTTP/S and Aspera FASP to complete file transfers. This transfer option does not require users to download and install a client.

Once you configure your Aspera HTTP Gateway, you can point your Aspera on Cloud organization to it. For details, see [Transfer with Aspera HTTP Gateway instead of Aspera Connect](#).

Transfers between nodes (node-to-node transfers) in your Aspera transfer network do not require Aspera Connect or Aspera HTTP Gateway.

Minimum software version for tethered nodes

If you have your own IBM Aspera High-Speed Transfer Server (HSTS), you can attach or "tether" it to your Aspera on Cloud organization. Tethering enables you to give users in your AoC organization access to content on your HSTS.

If you tether your HSTS node to Aspera on Cloud, IBM highly recommends that you **always use the most recently released version of** [Aspera transfer server software](#) (IBM Aspera High-Speed Transfer Service) for user-managed (tethered) nodes attached to Aspera on Cloud.

Aspera transfer servers tethered to Aspera on Cloud **must** run software version 3.9.3 or higher.

Certificates for tethered nodes

To configure an Aspera High-Speed Transfer Server (HST Server) with an SSL certificate, you must have:

- the key
- the signed root certificate, or a certificate bundle (root certificate plus intermediate certificates)

The key and certificate files must be in `.pem` or `.crt` format.

Note: The key and certificate (or certificate bundle) must be provided by an authorized, globally trusted Certificate Authority (CA) included in the [Mozilla CA bundle](#). You cannot use a self-generated SSL certificate.

Minimum MacOS version

If you are using MacOS 10.12 or earlier, you must upgrade your OS or use Aspera Connect v3.11.

Browser support

Firewall requirements

Depending on your network, you may have to configure your firewalls to use Aspera on Cloud. This article describes how to allow traffic from your network to Aspera on Cloud and to and from any Aspera High-Speed Transfer Servers (HSTS) and cloud storage you attach to your AoC organization.

Note: For Aspera IP addresses, only a few of those in the listed subnet ranges will be active at any given time. However, you should allow the entire set of ranges below to ensure continuous service in the event of a failover. (To determine the set of active IP addresses, check what `api.ibmaspera.com` resolves to using a tool such as **dig** or **nslookup**.)

Allowing traffic from your network to Aspera on Cloud

To use AoC APIs, AoC web interfaces, or Aspera Connect clients on your network with Aspera on Cloud, and to connect to the Aspera metering system (ALEE), configure and allowlist your firewall as follows:

- For all AoC clients, and for users of the AoC API, allow traffic on TCP/443 to the DNS name `api.ibmaspera.com`.
- Allow traffic on TCP/443.
- For Aspera Connect clients and nodes (ATS, user-managed, and so on), also allow traffic on UDP/33001 and TCP/33001.

Allowing traffic from Aspera on Cloud to user-managed transfer servers (tethered nodes)

To use your own transfer server with Aspera on Cloud (as a *tethered node*), you configure your firewall as follows:

- Allow traffic on TCP/443.
- For Aspera Connect clients, also allow traffic on UDP/33001 and TCP/33001.
- Provide *ingress* access for the following AoC service IP addresses:

IP Address
169.46.4.68/31
169.46.4.70/31
169.48.106.192/26
169.48.226.120/31
169.48.236.50/31
169.48.249.64/26
169.60.129.66/31
169.60.151.232/31
169.60.197.0/26
169.61.233.80/29
169.61.54.112/29

Allowing traffic to Aspera transfer service (ATS) nodes

You must also allow access for any transfer service nodes. Transfer service nodes typically use the `aspera.io` domain.

To retrieve the public IP addresses and ports for the transfer service for allowing in your firewall rules, do the following:

- Go to Nodes and Storage > Nodes.
- In the list of nodes, scan for nodes NOT listed as Hosted by Aspera = Aspera.
- Click the node row and enter the node secret to view details.
- In the Node URL field, note the URL. The node URL contains the service provider region.
- Use a curl request or your browser to access the following endpoints:
 - IBM Cloud: <https://ats.aspera.io/pub/v1/servers/softlayer>
 - Amazon S3: <https://ats.aspera.io/pub/v1/servers/AWS>
 - Microsoft Azure: <https://ats.aspera.io/pub/v1/servers/AZURE>
 - Google Cloud: <https://ats.aspera.io/pub/v1/servers/Google>
- Search for the region you noted in step 4. Note all IP addresses associated with that region, along with the port found in the `transfer_setup_url` field.
- Enter these IP addresses and ports in your firewall allowlist rules.

From	To		
	Service name	Service IP address	Service port
Aspera on Cloud API client or front-end web client	ATS transfer server	ATS IP address range	TCP/443
Aspera Connect clients	ATS transfer server	ATS IP address range	UDP/33001, TCP33001
Aspera Connect browser	ATS transfer server	ATS IP address range	UDP/33001, TCP33001

Allowing traffic using IBMId authentication

If your AoC authentication methods include IBMId, you must allowlist the following URLs:

From	To	
	Service name	Service FQDN + Port =TCP/443

From	To	
	Service name	Service FQDN + Port =TCP/443
Aspera on Cloud front-end web client	IBM Cloud	- iam.cloud.ibm.com - identity-?.*.iam.cloud.ibm.com/identity/authorize Where: ? = one character * = one region name (no deeper subdomain allowed) For example: https://identity-2.us-south.iam.cloud.ibm.com/identity/authorize

Allowing traffic to CloudFront

To ensure seamless access to CloudFront, configure your network to allow traffic to the following domains:

Aspera URLs

URL	Port	Protocol	Usage
api.ibmaspera.com	443	TCP	Aspera on Cloud API
<your_org_subdomain>.ibmaspera.com	443	TCP	Aspera on Cloud Front-end Portal, organization specific
aspera.pub	443	TCP	Short URL service for file sharing
downloads.ibmaspera.com	443	TCP	Provides distributions for IBM Aspera for desktop

IBM id specific URLs

URL	Port	Protocol	Usage
login.ibm.com	443	TCP	Login with IBM ID
iam.cloud.ibm.com	443	TCP	IBM Cloud Identity and Access Management (IAM) authentication
identity-1.us-south.iam.cloud.ibm.com	443	TCP	IAM authentication in US South region
identity-2.us-south.iam.cloud.ibm.com	443	TCP	IAM authentication redundancy for US South
identity-3.us-south.iam.cloud.ibm.com	443	TCP	IAM authentication redundancy for US South
identity-1.uk-south.iam.cloud.ibm.com	443	TCP	IAM authentication in UK South region
identity-2.uk-south.iam.cloud.ibm.com	443	TCP	IAM authentication redundancy for UK South
identity-3.uk-south.iam.cloud.ibm.com	443	TCP	IAM authentication redundancy for UK South
identity-1.eu-central.iam.cloud.ibm.com	443	TCP	IAM authentication in EU Central region
identity-2.eu-central.iam.cloud.ibm.com	443	TCP	IAM authentication redundancy for EU Central
identity-3.eu-central.iam.cloud.ibm.com	443	TCP	IAM authentication redundancy for EU Central
identity-1.ap-south.iam.cloud.ibm.com	443	TCP	IAM authentication in AP South region
identity-2.ap-south.iam.cloud.ibm.com	443	TCP	IAM authentication redundancy for AP South
identity-3.ap-south.iam.cloud.ibm.com	443	TCP	IAM authentication redundancy for AP South
identity-1.ap-north.iam.cloud.ibm.com	443	TCP	IAM authentication in AP North region
identity-2.ap-north.iam.cloud.ibm.com	443	TCP	IAM authentication redundancy for AP North

Telemetry (Used by IBM Aspera SRE to monitor the application)

URL	Port	Protocol	Usage
sentry.asperasoft.com	443	TCP	Application exception monitoring
eum-coral-saas.instana.io	443	TCP	Application performance monitoring

For additional information regarding CloudFront edge server locations and best practices, refer to the official [AWS documentation](#).

Access security and content security

These articles describe security measures including the various access keys that protect storage; the authorization options available to protect app access; and the many content security controls available to administrators. This section also describes data logging and retention, including content storage durations and treatment of personally identifiable information (PII).

- [Primary access keys and sub-access keys](#)

You must use a primary access key to share transfer access *outside* your AoC organization, such as with a vendor or other collaborator, or with a downstream on-prem application like Aspera Faspex, Shares, or Console. Use a sub-access key to share transfer access *inside* your AoC org, such as when delegating access and management tasks to a workspace manager.

- [Secure the access credentials for your built-in node](#)

Each Aspera on Cloud subscription includes one built-in, Aspera-managed transfer server (ATS) node with storage in IBM Cloud Object Storage. The access credentials (or access key) for this transfer server are automatically delivered to the administrator who first created the AoC organization. Find these credentials in a digital package from Tech Support in the Packages app. It's very important to track and store these credentials securely so that you can access and manage content on this node.

- [Configuring authentication methods for your organization](#)

Configure one or more authentication methods for your AoC users, including IBMid, Google OAuth, and one or more SAML providers. Once configured, you can apply one or more of these methods to users and groups in your organization.

- [Content security overview](#)

In addition to secure access controls, protecting content directly ensures that digital assets retain their value even as Aspera on Cloud users collaborate to develop,

exchange, and deliver content. This article collects several Aspera on Cloud content security settings and strategies, and provides links to configuration procedures.

- [Data logging and retention](#)

This article describes retention duration for data in Aspera on Cloud.

Primary access keys and sub-access keys

You must use a primary access key to share transfer access *outside* your AoC organization, such as with a vendor or other collaborator, or with a downstream on-prem application like Aspera Faspex, Shares, or Console. Use a sub-access key to share transfer access *inside* your AoC org, such as when delegating access and management tasks to a workspace manager.

Primary access keys

Use a primary access key to give a user or application *outside* Aspera on Cloud transfer credentials to access the content assets on that node.

An Aspera on Cloud *superadmin* (an administrator who knows the Aspera transfer user name and password) can create a primary access key in two ways:

- Using the Node API; see the `/access_keys` endpoint in the [IBM Aspera Node API](#) documentation on IBM API hub.
- Using the Aspera on Cloud application, when attaching a new transfer node to the AoC organization. The new node may be a [customer-managed Aspera HSTS node or cluster](#), or it may be an [ATS node that attaches the customer's cloud object storage](#).

Sub-access keys

Use a sub-access key to delegate certain administrative tasks and contextual content access to another AoC admin or to a workspace manager without having to distribute the primary access key. You can create a sub-access key only on a sub-directory of another access key.

Important: To maintain tenant privacy and content separation, do not use a sub-access key outside the context of the Aspera on Cloud organization.

An Aspera on Cloud administrator can use the primary access key to create either of two sub-access key types, using the Aspera on Cloud application.

- A *client* sub-access key (also called a *workspace* access key) gives an admin or workspace manager contextual access and management rights within the *root folder* of a given workspace on the node.
- A *folder* sub-access key gives an admin or workspace manager access and management rights in a [folder in cloud storage](#) or in an [administratively shared folder](#). Note that a folder sub-access key is a different access credential than the sharing permissions set on a shared folder. *Access through a folder sub-access key is full access to folder contents*; such access is not restricted to the actions allowed through sharing permissions.

Secure the access credentials for your built-in node

Each Aspera on Cloud subscription includes one built-in, Aspera-managed transfer server (ATS) node with storage in IBM Cloud Object Storage. The access credentials (or access key) for this transfer server are automatically delivered to the administrator who first created the AoC organization. Find these credentials in a digital package from Tech Support in the Packages app. It's very important to track and store these credentials securely so that you can access and manage content on this node.

To retrieve the credentials for your built-in, Aspera-managed node, do the following:

Attention: You must be the administrator who first configured the Aspera on Cloud organization.

1. Go to the Packages app. If necessary, click the app switcher  and select Packages.
2. In the left-side gray panel, click My inbox.
3. In the packages list, click the row of the package from IBM Aspera Tech Support called "Access key information". This package contains a text file listing the key and secret.
4. Review the message included with the package.
5. Right-click the text file and select Download to...
6. In the Finder or Explorer window that opens, select the location for this download.
7. Click Open or Done.
8. Aspera highly recommends you rename the file to make it easier to track. Track and protect the text file with the key and secret according to your local site security practices. Note that IBM Aspera does not keep a copy of the access key secret.

Note: Selecting Download to... affects *only this download*. To change your *default* download location, open Aspera Connect from your system tray or launcher; go to Preferences > Transfers. In the Downloads location field, enter the default location for your downloads.

Configuring authentication methods for your organization

Configure one or more authentication methods for your AoC users, including IBMid, Google OAuth, and one or more SAML providers. Once configured, you can apply one or more of these methods to users and groups in your organization.

Once you configure one or more of these authentication methods, you can assign one of them to each user in your organization, either during new user creation or by modifying an existing user record. You can also allow individual users to log in using any configured auth provider for which they have credentials; in this scenario, the user can log in at one time using one configured auth provider, and another time using a different configured auth provider. For details, see [Create and manage users](#).

The authentication methods you configure for your organization appear as buttons on your organization login page. For each auth method, you can configure the label on the button to help guide your users to the login method you intend for them; go to Admin > Authentication > *your_identity_provider*.

The following table provides an overview of different authentication types supported in Aspera on Cloud:

Authentication Type	Description
IBMid	IBMid is enabled by default for all Aspera on Cloud organizations; no configuration is required. IBMid is the ID-as-a-Service (IDaaS) from IBM. It is available for anyone using IBM cloud and many IBM cloud services, including Aspera on Cloud. You can enable multifactor authentication for users who log in with IBMid. You can also enable a special access option for specific admins to avoid being locked out of Aspera on Cloud when you disable IBMid. For details and procedures, see the articles under IBMid .
SAML	You can enable one or more SAML IdPs for your organization. To allow your users to log in through multiple SAML providers, set the Authentication method to Any . For details and procedures, see the articles under SAML .
Google OAuth	You can enable authentication by Google, which allows users to access Aspera on Cloud based on authentication into Google. In this scenario, the user in essence logs in to Google using a dialog presented by Aspera on Cloud; Google then passes that authentication to Aspera on Cloud, and Aspera on Cloud accepts that authentication to allow Aspera on Cloud access. Such authentication populates user accounts in Aspera on Cloud based on Google-verified identity. For details and a procedure, see Configuring Google authentication .

Content security overview

In addition to secure access controls, protecting content directly ensures that digital assets retain their value even as Aspera on Cloud users collaborate to develop, exchange, and deliver content. This article collects several Aspera on Cloud content security settings and strategies, and provides links to configuration procedures.

Aspera security considerations

If your business security requirements include restrictions for uploads and transfers by file extension type, you must use the Aspera Node API on each transfer server to configure exclusion rules.

Content encryption in Aspera on Cloud

- [Content encryption at rest and in flight](#)
- [Require encryption at rest](#)

Server-side encryption

- [Use Aspera-managed keys for server-side encryption at rest](#)
- [Bring your own key for server-side encryption at rest](#)

Security in multi-tenant organizations

In a multi-tenant or reseller organization, you must ensure strict separation between workspaces to protect tenant privacy.

By default, the auto-complete function in Aspera on Cloud shows workspace managers all users and groups in the entire organization, along with the personal contacts of all users. Instead, you can configure your org such that workspace managers can see only users and groups from the workspaces in which they are members, along with their own personal contacts in any workspace and with outside users.

For details, see [Assign the workspace manager role](#).

Files app content security

Admin controls

By default, collaboration in the Files app is unrestricted. But as an admin, you can apply increasingly restrictive controls to sharing actions available to Files app members.

Global: Admin > Applications > Files

Workspace: Admin > Workspaces > *workspaceName* > Applications > Files

- Prevent app users from sharing with unauthenticated recipients; restrict the use of [public links](#): Who can share folders via public links
- [Prevent](#) app users from sharing with non-workspace members: Who can share folders with external users
- Allow sharing with [designated non-workspace members only](#); list specific external users as the only valid recipients: Who are eligible external users
- Prevent accidental sharing with the entire workspace: Who can share folders with the entire workspace
- [Require](#) external users to create an AoC account and log in to receive a package

User controls

As an admin, you can establish workflows that guide your workspace members how to use these additional content security measures:

- Apply [content permissions](#) to shared content
- Require a password to access content shared using a [public link](#)
- [Unshare](#) a folder

Packages app content security

Admin controls

Global: Admin > Applications > Packages

Workspace: Admin > Workspaces > *workspaceName* > Applications > Packages

- Prevent app users from requesting packages from non-workspace members: Who can send submission links
- Prevent app users from sending packages to non-workspace members: Who can send packages to external users
- Require non-workspace recipients to create an account and log in to receive a package: Require external users to log in when receiving packages
- Prevent accidental sending to the entire workspace: Who can send packages to the entire workspace
- Require encryption at rest for all send packages: Automatically apply encryption at rest to all packages

Global: Integrations > Watermarking

- If you [integrate your Irdeto forensic watermarking service with Aspera on Cloud](#), you can *allow* or *require* workspace members of the Packages app to apply a watermark to all packages they send.

User controls

As an admin, you can establish workflows that guide your workspace members how to use these additional content security measures:

- Require package recipients to apply a password
- Apply watermarking when sending a package

Content security caveats

Members of the Automation and Activity apps are not limited to acting on, monitoring, or reporting on content in workspaces where they are members. No matter their workspace membership:

- Automation app members can configure and manage automated workflows on any workspace in your org.
- Activity app members can monitor and report on content in all workspaces in your org.

For these reasons, Automation and Activity app members are typically org admins.

Public links

Public link expiration

Global: Admin > Applications > Packages/Files

Workspace: Admin > Workspaces > *workspaceName* > Applications > Packages/Files

Select the check box next to the Links expire after (days) option in the Public and authenticated links section, and set the desired value for the link expiration.

- The administrator can set a default expiration for all public links.
- An individual user can reduce the expiration set by the administrator, but cannot extend it.

Public link password

Global: Admin > Applications > Packages/Files

Workspace: Admin > Workspaces > *workspaceName* > Applications > Packages/Files

Select the check box next to the Make password required for new links option in the Public and authenticated links section.

- The administrator can enforce the password requirement when creating the public links.
- Passwords won't be set by default, users must set the password when creating a new public link.

Disallow encryption-at-rest during package send operations

Global: Admin > Applications > Packages

Workspace: Admin > Workspaces > *workspaceName* > Applications > Packages

Select the option Disabled from the drop-down list in the Client-side encryption at rest section.

- Administrators can disable the application of client-side encryption-at-rest to packages in all workspaces or in specific workspaces.
- Senders can't apply EAR to individual packages.

Data logging and retention

This article describes retention duration for data in Aspera on Cloud.

General

- All personally identifiable information (PII) is deleted from the active backend databases no more than 60 days after the subscription ends.
- Database backups are deleted after 270 days.

Retention policy for data in the Admin app

Data in the Admin app Activity page (Admin > Organization > Activity) are retained as follows:

- Volume usage is retained indefinitely for the length of the subscription.
 - The most recent three months of data are searchable in the web UI.
 - The AoC API allows access to historical volume usage data.
- Package activity is retained indefinitely for the length of the subscription.
- Application events are retained for one year.

Retention policy for data in the Activity app

Data in the Activity app are retained for five years. See also [Data retention](#).

Backend logging and audit data

Application logs are collected for debugging purposes and not exposed to end users. These data are retained for 366 days.

Stored file transaction attributes

The following attributes are stored according to the retention policies.

- Organization
- User workspace
- Data package name
- Sender user ID
- Receiver user ID
- File ID
- File name
- File size
- File transfer timestamp
- File transfer source IP address
- Server IP address
- Transfer size
- Transfer rate

Customize for your use case

Define your own use case so that you can maximize the value of this very flexible application. Consider and configure the controls available to protect user privacy and define how app members collaborate with each other and with outside users. Articles in this section also introduce options to integrate AoC with other IBM products and options to allow users and groups to access content in your local and cloud storage.

- [Define your use case](#)
For a successful implementation, take the time to consider your enterprise requirements, then to plan and design which Aspera on Cloud resources and strategies will achieve your goals.
- [Collaboration: Open or closed?](#)
Default collaboration settings tend to be open. Administrators can make collaboration options increasingly strict as required.
- [Configuration best practices](#)
Aspera on Cloud is an incredibly flexible and adaptable application. While this is surely a strength of the product, it also present challenges to administrators planning their AoC implementation. Best practices articles help you to zero in on effective configuration decisions that lead to an organization that is most apt for achieving corporate goals.
- [Integrating Aspera products](#)
Depending on your use case, you may wish to integrate other IBM and IBM Aspera products with your Aspera on Cloud organization.
- [Give users access to local or cloud storage](#)
Typically, an organization has existing storage that your Aspera on Cloud users need to access. To enable this access, you *attach* or add a node to your AoC organization. A node can be your own Aspera High-Speed Transfer Server, or can be storage in a cloud provider region. The nodes or storage you attach are in addition to the built-in storage in IBM Cloud that is an automatic part of your Aspera on Cloud subscription.

Define your use case

For a successful implementation, take the time to consider your enterprise requirements, then to plan and design which Aspera on Cloud resources and strategies will achieve your goals.

Consider the following questions.

- Are you creating a multi-tenant implementation, in which the various entities that will be using Aspera on Cloud are completely separate from each other, and require maximum compartmentalization and privacy?
- Is there need for collaboration among various teams, or only within teams?
- Is there need for organization members to collaborate with people outside the organization? If yes, how much control or freedom do you want your users to have in collaborating with outside users?
- Is the scenario predominantly to ingest files?
- Will users be collaborating iteratively on content in shared folders in a repository?
- Are you expecting that various and diverse users will be submitting files for further processing or publication?

Ingest from multiple collaborators

If your Aspera on Cloud usage is focused on ingest of files and folders from multiple collaborators, use a single workspace, enable the Packages app, and configure multiple shared inboxes. Shared inboxes provide separation of projects, assets, and participants. Grant membership in specific shared inboxes to specific workspace members, configuring one or more inbox permissions as required for each user:

- Send: Can send packages to the shared inbox
- Receive: Can browse and download packages sent to the inbox
- Add users: Can add a new member to the inbox, granting Send only permission to the new member

With Add users permission, shared inbox members can invite users outside the workspace or outside the organization to become members of the inbox with Send only privilege for a 'blind drop' to the inbox.

Each shared inbox can have discrete or overlapping membership, discrete branding, collaboration settings, metadata fields, workflows, and notifications, and can be tailored for various uses:

- Ingest for a specific project or project phase
- Ingest from a specific client
- Ingest from a specific user
- Ingest from internal users
- Ingest from external users

Using the Packages app to send and receive digital packages creates an traceable trail of delivery, contents, and recipients, since each package is an immutable, original record of the transfer.

Delivering and accessing content using a shared folder structure

If your users need to collaborate iteratively on a structured set of content items, you can use the Files app, configure the required folders, and share them with your users. Collaboration conventions among team members can mean that the latest version of certain content is always available in a given location. This structure can also be used to distribute files and folders to users in diverse locations, who can be granted browse and download permission to the required folders. Email notifications alert users when new content is available.

Distributing assets to large groups of recipients

Similar to the ingest scenario, use a single workspace, enable the Packages app, and configure multiple, uniquely branded shared inboxes. Give asset creators Submit permission to the shared inbox; give the recipient list Receive permission. Asset creators submit immutable digital packages containing any number of assets of any size, from any source or location; each recipient receives a separate copy of the package to download for further processing or distribution.

Alternatively, add aligned recipients into groups; asset creators can address digital packages to these groups. Addressing groups can provide additional simplicity to content delivery since senders can address multiple groups and multiple individual recipients in the same send operation, whereas senders to a shared inbox cannot address additional recipients or groups in the same send operation.

Collaborating with users with limited storage access

You may find a need to collaborate with users who have access only to certain storage locations or types. In this scenario, you can use the Files app to create a folder structure on the appropriate storage, posting the shared content to the required portion of the folder structure. The intended recipients receive email notification that new or revised content is available in the location they can access.

Collaboration: Open or closed?

Default collaboration settings tend to be open. Administrators can make collaboration options increasingly strict as required.

Administrators can configure a number of settings that govern users' ability to collaborate with others. These settings include which users can collaborate outside the workspace, with whom, who can invite new users to the app or to a shared inbox, and other settings.

Administrators can configure collaboration settings at the global level for the Files and Packages apps independently. Global app settings are inherited at the workspace level; inherited settings can be overridden and customized for each app in each workspace. Therefore, collaboration permissions can vary from workspace to workspace and from app to app, allowing admins to customize Aspera on Cloud for maximum usability and content security.

In the Files application

Workspace members with access to the Files application can share folders freely with other members of the same workspace. This is a fundamental privilege of workspace membership and cannot be curtailed.

By default, all workspace members can also share with people outside the workspace. However, administrators or workspace managers can control which user types, if any, can share folders outside the workspace, and how.

There are two options for sharing outside the workspace: authenticated and unauthenticated; you can control these capabilities independently.

To configure the Files app globally, go to Applications > Files.

To customize the settings inherited from global app configuration for a given workspace, go to Workspaces > *workspaceName* > Applications > Files.

For details, see [Files App: Using a shared file repository](#).

Authenticated sharing outside the workspace

In the AoC UI, this is the setting labeled Who can share folders with external users.

The workspace member shares a folder with someone outside the workspace, either with an AoC member of a different workspace, or with a person who is not an AoC member at all. In both cases, the recipient of the share receives an email notification containing a link that allows them to access the shared folder.

- The AoC user in another workspace gets access to this shared folder through a limited workspace experience. They do not gain access to any content in the workspace except the folder specifically shared with them.
- For a person outside AoC entirely, the link in the email leads to an account creation flow; the recipient then logs in to access the shared folder through an AoC portal. This user does not have access to other content in the workspace or to any other functions of the app; only to folders that have been specifically shared with them. This means that folders you as administrator have shared with the entire workspace remain hidden and inaccessible to these users.
- You can control which user types in this workspace have authenticated sharing capability:
 - All members of the workspace (default).
 - Workspace managers only.
 - No one; you can disable this capability for all workspace members.
- If you enable sharing outside the workspace, you can list specific external users with whom those enabled users can share; configure this at the workspace level (Workspaces > *intended workspace* > Profile > Collaboration > Who are eligible external users).

Unauthenticated sharing outside the workspace

Unauthenticated sharing uses a public link. In the AoC UI, this is the setting labeled Who can share folder via public links.

- This recipient does not create an account or log in to AoC. They access the shared folder through an AoC portal.
- A public link is truly public: the public link recipient can forward the link to another user, who can then use the link to access the shared folder.
- You can control which user types in this workspace have unauthenticated sharing capability:
 - All members of the workspace (default).
 - Workspace managers only.
 - No one; you can disable this capability for all workspace members.
- If you enable sharing outside the workspace, you can designate specific external users that are valid recipients; workspace members can share only with those designated outside users. Configure this at the workspace level (Workspaces > *intended workspace* > Profile > Collaboration > Who are eligible external users).

In the Packages application

Workspace members with access to the Packages application can send packages freely to other members of the same workspace. This is a fundamental privilege of workspace membership and cannot be curtailed.

By default, all workspace members can also send packages to people outside the workspace. However, administrators or workspace managers can control which user types, if any, can send and request packages outside the workspace.

By default, workspace members can also request packages from others in the workspace or from outside users by sending a submission link; however, the administrator can restrict or disable the package request function.

To configure the Packages app globally, go to Applications > Packages.

To customize the settings inherited from global app configuration for a given workspace, go to Workspaces > *workspaceName* > Applications > Packages.

For details, see [Packages app: Send and receive files and folders](#).

Sending outside the workspace, with or without requiring recipients to log in

In the AoC UI, this is the setting labeled Who can send packages to external users.

The workspace member can send a package to someone outside the workspace, either to an AoC member of a different workspace, or with a person who is not an AoC member at all. In both cases, the package recipient receives an email notification containing a link that allows them to access the package.

- The AoC user in another workspace accesses the package in a limited workspace experience. They do not gain access to other workspace content.
- For a person outside AoC entirely, the link in the email opens an AoC portal that provides access to the package. This recipient does not have access to other content in the workspace or to any other functions of the application, only to packages that have been sent to them specifically. This means that packages sent to the entire workspace are not available to this recipient.
 - By default, the outside recipient does not need to create an AoC account and log in. However, you can require that; select the check box labeled Require external users to log in when receiving packages. When you require external users to log in, the link in the email notification leads the user through an account creation flow; the recipient then logs in to access the shared package through an AoC portal. This recipient does not gain access to any other content in the workspace or functions of the Packages application.
- You can control which user types in the workspace have outside sending capability:
 - All members of the workspace (default).
 - Workspace managers only.
 - No one; you can disable outside package sending entirely.
- If you enable sending outside the workspace, you can list eligible recipients to whom those enabled users can send; configure this at the workspace level: go to Workspaces > *workspace_name* > Collaboration > Who are eligible external users.

Requesting packages to My inbox

Note: The request packages permission described in this section applies only to requests to send to an individual user (send to My inbox) as opposed to sending to a shared inbox. See the following section for details on shared inbox requests.

In the AoC UI, this is the setting labeled Who can request packages by sharing submission links.

Workspace members request packages by sending a [submission link](#). AoC sends an email notification that contains the submission link, which enables the recipient to open an AoC portal; the portal allows the recipient to create a digital package and send it to the My inbox of the AoC user who sent the submission link.

You can control which user types in the workspace can request packages from others:

- All members of the workspace.
- Workspace managers only.
- No one; you can disable package requests entirely for all users of this workspace.

Unlike many of the other collaboration settings, when this setting is enabled for either members or managers, those enabled users can request packages from anyone, inside or outside the workspace, or outside AoC entirely.

Requesting packages to a shared inbox

Members of a workspace [shared inbox](#) who have *Add users* permission can send a [submission link](#) to anyone inside or outside AoC. AoC sends an email notification that contains the submission link, which enables the recipient to open an AoC portal; the portal allows the recipient to create a digital package and send it to the shared inbox from which the submission link was sent. The package is then available to all members of the shared inbox who have Receive permission to that inbox.

The user with *Add users* permission can send a submission link to another member of the shared inbox, or to someone who is not a member of the shared inbox.

In the workspace

By default, when you enable collaboration with outside users in either or both the Files and Packages applications for workspace members, those enabled users can collaborate with any user outside the workspace or outside AoC. But you can restrict collaboration to specific users or groups if required.

Go to Workspaces > *workspace_name* > Applications > Files/Packages > Collaboration > Who are eligible external users. You can configure the following, for the Packages app and for the Files app independently:

- Any email address (default).
- Any email plus the following groups.
- Only the following emails and groups.

Configuration best practices

Aspera on Cloud is an incredibly flexible and adaptable application. While this is surely a strength of the product, it also presents challenges to administrators planning their AoC implementation. Best practices articles help you to zero in on effective configuration decisions that lead to an organization that is most apt for achieving corporate goals.

Configuration best practices guides

This document now contains two articles documenting best practices for common use cases focused on exchanging content using a shared folder repo: the Files app. In the near future, you will find articles documenting best practices using the Packages app.

See the articles in this section: [Storage and workspace configuration scenarios](#).

Other deployment strategy resources

- [Content security overview](#)
- [Collaboration: Open or closed?](#)
- [Primary access keys and sub-access keys](#)
- [Accelerate setup using inherited settings](#)
- [Managing storage usage](#)

Integrating Aspera products

Depending on your use case, you may wish to integrate other IBM and IBM Aspera products with your Aspera on Cloud organization.

Whether integrating an API client embedded in your corporate internet, your Irdeto watermarking service, your IBM Key Protect KMS, the IBM Aspera mobile app, or another IBM Aspera product, refer to the articles in this section: [Integration and APIs](#).

Give users access to local or cloud storage

Typically, an organization has existing storage that your Aspera on Cloud users need to access. To enable this access, you *attach* or add a node to your AoC organization. A node can be your own Aspera High-Speed Transfer Server, or can be storage in a cloud provider region. The nodes or storage you attach are in addition to the built-in storage in IBM Cloud that is an automatic part of your Aspera on Cloud subscription.

Once you attach the node, you must make the intended content on the node available to users in the Files or Packages app in a workspace in your org. You do this by *administratively sharing* a folder on the node to workspace members. When you share as an admin, all admins in your org can manage access and permissions to the folder. This is generally preferable to sharing a folder as a user; in this case, only the user who shared the folder can manage the contents and permissions.

To attach your own HSTS node (org admin credentials required), go to [Tether Your Aspera Transfer Server to Aspera on Cloud](#).

To attach your existing cloud storage (ATS admin credentials required), go to [Attach your existing cloud storage](#).

You can also create one or more access keys to allow access to attached nodes and storage to allow access as follows: For access key details and procedures, see [Access keys](#).

- You can allow other admins or workspace managers to access and manage specific content on your attached node.
- You can allow an API client or other integration to access specific content on your attached node.

See [this article](#) for more information on your built-in IBM Cloud storage.

Set up your organization

This section guides your initial setup and how to accelerate configuration. Articles describe how to brand your organization, provide login guidance for your users, and give users access to specific content in your storage. Also discussed are how to add users, delegate management tasks, configure default storage locations, and configure session and token durations.

- [Organization: Overview](#)
The Aspera on Cloud organization is the primary administrative container. By default, an org contains at least one workspace, which is the primary container for user collaboration.
- [Accelerate setup using inherited settings](#)
Certain aspects of the Aspera on Cloud structure are hierarchical, allowing administrators to speed deployment.
- [Select a transfer method](#)
Aspera on Cloud requires one of two transfer methods to power high-speed transfers between user desktops and Aspera transfer servers. Users can either download and install Aspera Connect, a free, lightweight, install-on-demand software program; or an admin can configure the IBM Aspera HTTP Gateway and attach it to your Aspera on Cloud organization.
- [Transfer with Aspera HTTP Gateway instead of Aspera Connect](#)
You can use your IBM Aspera HTTP Gateway as a transfer client for Aspera on Cloud. This configuration supports users who cannot install the IBM Aspera Connect transfer client. Use this procedure to configure your Aspera on Cloud organization to use your Aspera HTTP Gateway.
- [Configure technical support for your users](#)
Some Aspera on Cloud users are eligible to register on the IBM Technical Support site. For users who are not eligible, your organization must provide local technical support. You can configure a pop-up message with local support instructions when a non-eligible user clicks the Help icon in the Aspera on Cloud banner.
- [Customize your organization URL, name, and logo](#)
Highlight your organization brand by configuring the name and subdomain of your AoC organization, and by importing logos or other graphics that display to your users and convey your brand. You can also configure the login buttons and instructions on the user login page.
- [Configure the user login page](#)
You can configure a splash message to communicate any information your users may need; for example, a welcome message, an upcoming maintenance window, a configuration change, and so on. You can also provide login guidance to your users by configuring the login buttons and associated instructions on the login page.
- [Give users access to local or cloud storage](#)
Typically, an organization has existing storage that your Aspera on Cloud users need to access. To enable this access, you *attach* or add a node to your AoC organization. A node can be your own Aspera High-Speed Transfer Server, or can be storage in a cloud provider region. The nodes or storage you attach are in addition to the built-in storage in IBM Cloud that is an automatic part of your Aspera on Cloud subscription.
- [Share a node folder with a workspace](#)
To allow the members of a workspace to use the content in a node attached to your org, an admin must give them access to the content. When you *administratively share* a folder with users, as described in this procedure, all admins in your org can manage the folder access. This shared management ability is typically preferable to having one admin user share a folder as an individual user; in such case, only that individual admin can revoke or change access permissions.
- [Add users: Overview](#)
As a productivity and collaboration tool, Aspera on Cloud assumes a diverse user base. There are multiple user types and roles that you can assign to maximize the effectiveness of your org members. There are also multiple ways to add users, both in bulk (IBMid, SAML) and individually.
- [Delegate to a workspace manager](#)
If desired, you can grant workspace manager privileges to one or more members in a workspace. A workspace manager can take over certain management tasks in that workspace.
- [Set the default storage location for your organization](#)
The organization *default node* automatically stores the files, folders, and packages of any new workspaces you create. The system default node is the built-in node in IBM Cloud that comes with your subscription. If you attach additional nodes or storage attached to your Aspera on Cloud organization, you can select a different node as the default.
- [Session and token duration](#)
You can configure settings for your organization that govern session duration and security token behaviors.

Organization: Overview

The Aspera on Cloud organization is the primary administrative container. By default, an org contains at least one workspace, which is the primary container for user collaboration.

Some org-level settings apply throughout your org. Other org-level settings are inherited by all workspaces, but can be overridden as necessary to customize each workspace. See also [Key elements and roles in Aspera on Cloud](#).

You can configure several **organization**-level settings, which are inherited by all workspaces in the org. You can override many inherited settings in any workspace as required:

Org-only settings

The configurations in this section apply to your org as a whole. These settings are not specifically inherited by workspaces nor customizable in workspaces.

Authentication

You can enable one or multiple authentication methods for your org, including SAML, IBMid, and Google OAuth. Then you can assign one or more auth methods to each org member. See [Authentication](#).

Access to content in storage

You can [attach your existing cloud storage](#) as a *node* to your aspera on Cloud organization. Once the node is attached to the org, you can make specific content in that storage available to specific workspace members through the Files app. The same applies for your own [Aspera High-Speed Transfer Server](#), if you have one.

Technical support

You must configure the tech support method for your organization. Go to Organization > Advanced settings > Support contact. For details and a procedure, see [Configure technical support for your users](#).

Multi-tenant privacy

When admins and workspace managers add users to workspaces and apps within the workspace, the auto-fill function in the *Add users* field lists potential matches. By default, workspace managers can see auto-fill entries from all users in the organization. But you can restrict the auto-fill list to display only the members of workspaces in which the manager is already a member. This restriction is particularly useful in a multi-tenant organization in which complete compartmentalization and privacy between tenants is required. Go to **Organization > Advanced settings**. See [Delegate to a workspace manager](#).

Security

You can customize the default settings for session and token duration. Go to **Organization > Security**. See [Session and token duration](#).

Aspera HTTP Gateway

You can attach your own [Aspera HTTP Gateway](#) to provide an alternative to Aspera Connect, the default transfer method. Aspera HTTP Gateway enables high-speed, FASP-based transfers for users who cannot download the Aspera Connect transfer client.

Org/workspace settings

The configuration in this section propagate from the org level to the workspace level.

Email templates

Accept the defaults, or configure email appearance and contents using Markup and custom variables. Global email templates and delivery settings are inherited by workspaces in your org. Go to **Organization > Email settings**. You can override global settings for a given workspace. Go to Workspaces > *workspaceName* > Notifications. See [Configure email notifications for your organization](#).

Applications

By default, the *Files* and *Packages* apps are enabled for the org and in each workspace. You can disable either of them in any workspace. If you disable them at the org, you cannot enable them in any workspace. You can configure certain behaviors (for example, collaboration settings, link configuration, and so on) at the org level and those setting propagate to each workspace. You can override inherited settings at each workspace to customize as required. For global configuration, go to Applications > Files or Applications > Packages. For workspace configuration, go to Workspaces > *workspaceName* > Applications > Files or Packages. See [Files App: Using a shared file repository](#) and [Packages app: Send and receive files and folders](#).

The *Activity* app is also enabled by default. This app is a global app rather than a workspace app like Files and Packages. The Activity app reports data for your entire org, though you can of course filter by workspace and by many other parameters to get granular activity data. Because of this org-wide data access, the typical Activity app member is an org admin. Go to Applications > Activity. See [Activity app: Monitor events, activity, and usage in your organization](#).

The *Automation* app is available only for Standard Plus and Premium subscriptions. Like the Activity app, it is a global app with org-wide data access. However, you must enable it for your org; then you can add members (typically other admins) who can access it. Go to Applications > Automation. See [Automation app: Automate your transfer workflows](#).

Accelerate setup using inherited settings

Certain aspects of the Aspera on Cloud structure are hierarchical, allowing administrators to speed deployment.

For example, you can take advantage of:

- Sensible defaults for ready-to-use ease.
- An inheritance scheme to accelerate implementation and simplify customization.
- Granular configuration options for highly-customizable control.

The tables below describes the features and elements of Aspera on Cloud that are hierarchical and inheritable.

Application access

You can configure which workspaces have access to each AoC application.

Hierarchical Level	Inheritance and Customization	Configuration Location
Organization	Files and Packages apps enabled by default. Can disable either or both. Activity and Automation apps are not associated with a specific workspace. The Activity app is enabled at the org level by default. Enable the Activity app at the org (Automation available only with Standard Plus and Premium subscriptions.)	Applications
Workspace	For Files and Packages apps, inherited from organization; When enabled at the org, can disable at a given workspace. When disabled at the org, no access at any workspace.	Workspaces > <i>workspaceName</i> > Applications

Packages app settings

There are several settings for the Packages app that you can configure at the global app level. Global app settings are inherited by the Packages app in each workspace in the org. Shared inboxes in the workspace inherit the workspace-level app settings. These settings include:

- Collaboration
- Public and authenticated link styles
- Security
- Package expiration
- JSON "sidecar" metadata file

Hierarchical Level	Inheritance and Customization	Configuration Location
Organization: Packages app	Can customize defaults.	Applications > Packages

Hierarchical Level	Inheritance and Customization	Configuration Location
Workspace: Packages app	Default: Inherit from global app settings. Can override inheritance and customize.	Workspaces > <i>workspaceName</i> > Applications > Packages
Workspace: Packages app: Shared inboxes	Default: Use workspace setting. Can override inheritance and customize.	Workspaces > <i>workspaceName</i> > Applications > Packages > Shared inboxes > <i>sharedInboxName</i>

Files app settings

There are several settings for the Files app that you can configure at the global app level. Global app settings are inherited by the Files app in each workspace in the org. These settings include:

- Collaboration
- Public and authenticated link styles
- Restrict usage (workspace level only; can exempt individual users and groups from the restriction)

Hierarchical Level	Inheritance and Customization	Configuration Location
Organization: Files app	Can customize defaults.	Applications > Files
Workspace: Files app	Default: Inherit from global app settings. Can override inheritance and customize.	Workspaces > <i>workspaceName</i> > Applications > Files

Email notifications: templates and delivery

You can configure templates that govern the content and appearance of the various email notifications that Aspera on Cloud generates; see [Customize email notification templates](#). You can also control whether or not email notifications for specific events are delivered, and customize these settings for the organization, for individual workspaces, and for individual shared inboxes; see [Control email notification delivery](#).

Note also that individual users can subscribe to specific notifications: User menu > Account settings > Notification settings.

Hierarchical Level	Inheritance and Customization	Configuration Location
Organization	Defaults; can customize.	Organization > Email templates
Workspace	Inherited from organization; can customize.	Workspaces > <i>workspaceName</i> > Email templates and Workspaces > <i>workspaceName</i> > Notifications
Workspace: Packages app: Shared inboxes	Inherited from workspace; can customize.	Workspaces > <i>workspaceName</i> > Applications > Packages > Shared inboxes > <i>sharedInboxName</i> > Email settings

Branding

You can import graphics that display to your users and convey your brand. Workspaces in your organization inherit the graphic you import. Or you can override the inheritance and customize the graphic for a given workspace.

For details, see [Customize your organization URL, name, and logo](#) and [Create a new workspace](#).

Hierarchical Level	Inheritance and Customization	Configuration Location
Organization	Can import a graphic logo.	Organization > Profile and branding
Workspace	Default: Inherit from org logo. Can override inheritance and customize.	Workspaces > <i>workspaceName</i> > Profile

Users and groups

Users can inherit memberships and other settings from groups they belong to. These settings include:

- Workspace membership
- Group membership
- Application membership

For details, see [Users and groups](#).

Hierarchical Level	Inheritance and Customization	Configuration Location
Groups	Can customize defaults.	Groups > Members/Managers/Workspace memberships
Users	Inherit from group settings. Cannot override group settings; instead, remove user from group.	n/a

Select a transfer method

Aspera on Cloud requires one of two transfer methods to power high-speed transfers between user desktops and Aspera transfer servers. Users can either download and install Aspera Connect, a free, lightweight, install-on-demand software program; or an admin can configure the IBM Aspera HTTP Gateway and attach it to your Aspera on Cloud organization.

Aspera Connect is the default transfer method for Aspera on Cloud and other Aspera web apps. However, if your deployment of Aspera on Cloud does not allow users to download and install client software, you can configure an alternative transfer method: the [IBM Aspera HTTP Gateway](#). The Aspera HTTP Gateway is a standalone product that uses both HTTP/S and Aspera FASP to complete file transfers.

For details about Aspera Connect, see [Aspera Connect transfer client](#).

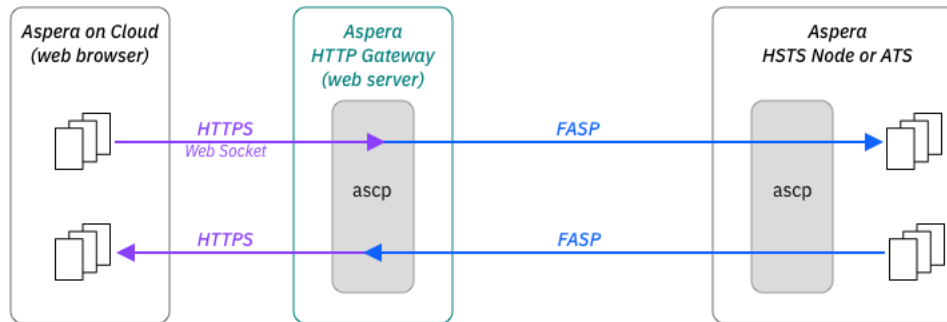
Transfer with Aspera HTTP Gateway instead of Aspera Connect

You can use your IBM Aspera HTTP Gateway as a transfer client for Aspera on Cloud. This configuration supports users who cannot install the IBM Aspera Connect transfer client. Use this procedure to configure your Aspera on Cloud organization to use your Aspera HTTP Gateway.

Users who can install [Aspera Connect](#) can and should continue to use it, even as others in the organization use the HTTP Gateway for transfers. Aspera Connect transfers are typically faster than Aspera HTTP Gateway transfers.

The Aspera HTTP Gateway is a standalone product that uses both HTTP/S and Aspera FASP to complete file transfers. To install and configure the Aspera HTTP Gateway, see the [IBM Aspera HTTP Gateway Admin Guide](#).

Once you configure your Aspera HTTP Gateway, you can point your Aspera on Cloud organization to it. Enabling the Gateway ensures that all Aspera on Cloud users can transfer.



Best practices and limitations

Best practices

- IBM Aspera highly recommends deploying HTTP Gateway as close as possible to end users. Gateway proximity mitigates the speed degradation inherent in HTTP/HTTPS transfers over distance.
- Users who can install and use the Aspera Connect transfer client should do so. Transfers using Aspera Connect are generally faster, so Connect remains the preferred transfer method.

Limitations

For transfers using the HTTP Gateway:

- To upload a folder, you must either:
 - Archive the folder as a .zip or other archive file type.
 - Open the folder and upload the files in it.When you try to upload a folder, Aspera on Cloud displays an explanatory notice, then opens your Finder or Explorer so you can select one or more files for upload.
- When you download a folder or download multiple files in a single transfer, Aspera on Cloud automatically archives the folder or the files as a .zip file and then downloads the .zip file.
- Aspera on Cloud does not show HTTP Gateway transfers in the Transfer monitor. Use your browser download manager to track downloads.
- Do not close the Aspera on Cloud application browser tab until the upload completes. You can open a new tab or switch to a different open tab on your browser.
- You cannot resume an interrupted HTTP Gateway transfer. You must start the transfer over.
- You cannot upload empty files or folders.
- You cannot download empty folders.

Enable Aspera HTTP Gateway

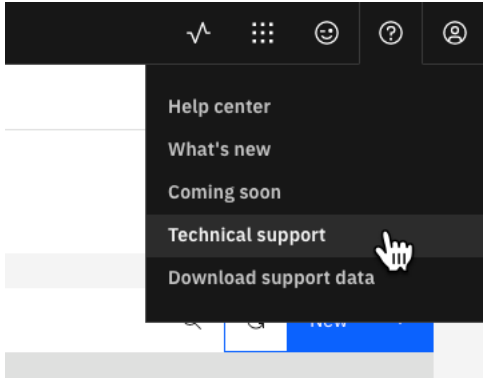
1. Go to Admin > Organization > Aspera HTTP Gateway > Configuration.
2. Set the Enable toggle to On.
3. Paste the URL of your Aspera HTTP Gateway into the following field.
For example, `https://http-gateway.mycompany.com/aspera/http-gwy/v1`.
4. Click Test connection.
A success notification displays when the connection is established.
If the connection test fails, check the URL for accuracy and verify proper network configuration. Then click Test connection again.
5. Click Save.
6. For users who cannot install Aspera Connect, disable Connect and the Connect installation prompt:
 - a. Click Aspera Connect configuration.
 - b. Select the users and groups who cannot install Aspera Connect; Aspera on Cloud disables Connect for these users and will not prompt them to install Connect.
Individual users can disable Aspera Connect by using the toggle at the bottom of the transfer monitor panel; the user setting overrides the Admin setting.

Configure technical support for your users

Some Aspera on Cloud users are eligible to register on the IBM Technical Support site. For users who are not eligible, your organization must provide local technical support. You can configure a pop-up message with local support instructions when a non-eligible user clicks the Help icon in the Aspera on Cloud banner.

Users who are registered can go to the IBM Support portal. If you are a registered user and open a support ticket, include the file available from Help > Download support data.

Other users can click the **Help** icon  on the right side of the upper black banner and select the **Technical support** menu option.



For these users, you can configure one of two behaviors:

- Redirect users to the URL of a web page your company uses to provide technical support.
- Display a brief pop-up notification that you compose with contact info for your own internal Support team.

To configure the technical support behavior for your users, do the following:

1. Go to **Organization > Advanced settings > Support contact**.
2. Select one of the following:
 - a. **Display popup message**
Select this option to compose a message to your users that pops up when they select the **Technical support** menu option. The Technical support message field that displays contains a sample of a message to your users with a Support contact. Edit the message to your users as desired, including the correct contact info. Use Markdown to format your message.
 - b. **Redirect to your company support URL**
Select this option to redirect users to your internal Support page when they select the **Technical support** menu option. In the following field, enter the URL.
3. Click Save.

Customize your organization URL, name, and logo

Highlight your organization brand by configuring the name and subdomain of your AoC organization, and by importing logos or other graphics that display to your users and convey your brand. You can also configure the login buttons and instructions on the user login page.

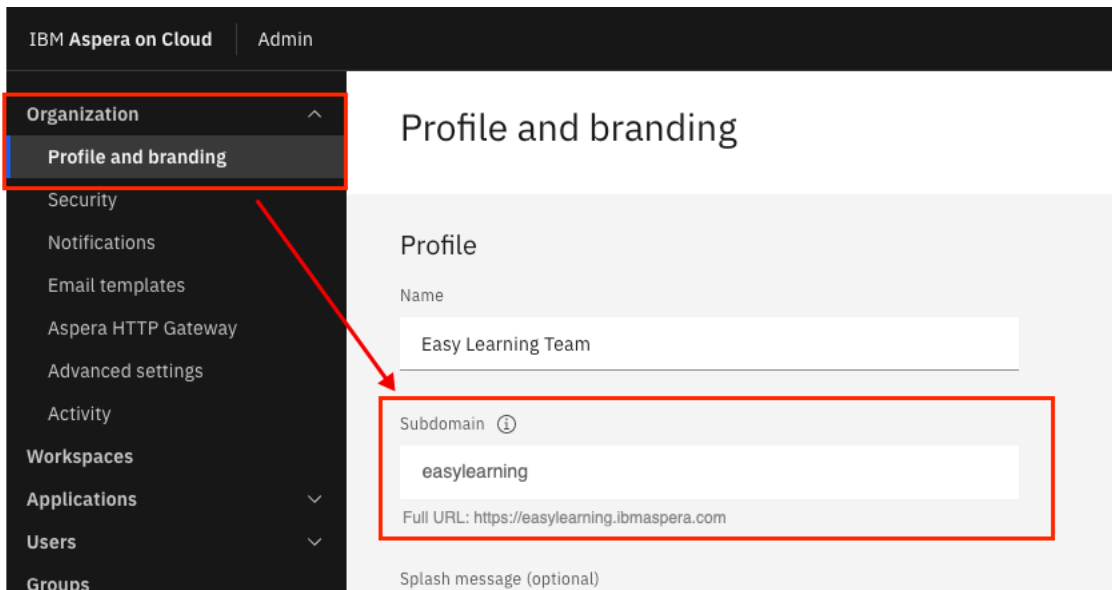
You can configure the following; find a detailed procedure later in this article.

- Edit the name of your organization. The name displays on the user login page.
- Configure the subdomain of your AoC org URL. This one-time configuration persists as the subdomain in your organization web address (for example: `https://<my_subdomain>.ibmaspera.com`).
Note: Use care when selecting this URL; once you configure it you cannot change it.
- Import a logo or other graphic that displays on the user login page and in the top left of your AoC org interface. The graphic you import replaces the default "IBM Aspera on Cloud" logo that appears in the upper left of the interface by default. This graphic must be square and less than 512 kb in size.
- Import a graphic that displays as a background image on the org login page. This graphic must be 16:9 aspect ratio and be less than 2 Mb in size.
- Configure a message that displays at the top of the login page. This message can welcome users, announce upcoming changes or maintenance windows, and so on.
- You can further configure the login page as follows:
 - To edit button labels and add instructions for users that appear with the login button; see [Configuring authentication methods for your organization](#).
 - If you present more than one login method (for example, IBMid and Google OAuth), you can reorder the buttons; see [Configure the user login page](#).

To brand your organization, do the following:

1. Go to **Organization > Profile and branding > Profile**.
2. To change the name of your organization, update the text in the Name field.
3. To set your organization subdomain, enter it as a string in the Subdomain name field.
The initial subdomain of a new organization is an automatically generated string (for example, 34029priibi). You can customize this automated string once; once customized, you cannot change it.
 - Valid characters: a – z; 0 – 9; hyphen (-) allowed, but not at start or end of the string.
 - No spaces.
 - Maximum length: 63 characters.
 - Do not include ".ibmaspera.com" in the field.

In the example in the screenshot below, the organization subdomain will display as `http://easylearning.ibmaspera.com`.



4. To configure an optional message that appears to users at the top of the login page, enter text in the Splash message field. Clear the field when the message is no longer relevant.
5. Click Save.

To customize your login page's logo and background image go to Organization > Profile and branding > Login page

6. To add a logo or other image that displays in the upper left corner of the Aspera on Cloud interface of both Admin and User views, click Add file to browse, or drag and drop the image in the field.
Use a square graphic up to 500 Kb in size.
7. To configure an image that displays in the background of your organization landing page, scroll to Custom background image, click Add file to browse, or drag and drop the image in the field.
Use a 16:9 graphic up to 4 Mb in size.
8. Click Save.

To customize the logo that will be displayed on the UI header, go to Organization > Profile and branding > Logo

9. (Default, Custom text logo, Custom image logo, and Custom text and image). Click Add file to browse. Use a square image up to 500 Kb in size. To customize your text logo, update the text in the Custom text logo field.
10. Click Save.

To customize your theme, font, and UI header text go to Organization > Profile and branding > Theme editor

11. To set a custom theme to use in other IBM Aspera apps or systems, you can choose to import or export one. Under Theme editor choose the appropriate option for your customization option.
 - Set to default: Sets the current theme as the default one. You will be prompted to refresh the page to apply your changes.
 - Export current settings: Downloads your current theme as a JSON file.
 - Import: Upload a new theme, files must be in JSON format with the '.json' extension.
12. To change the theme of the application between light or dark, scroll to Themes and select the desired option. You can also lock the application to a single custom theme by turning the Enable light and dark custom themes slider off.
13. To customize the UI font, go to Font and select a new one from the drop down.
14. You can customize the color of several items of the header (scroll down to Header), left navigation (scroll down to Left navigation), and buttons (scroll down to Buttons). Each option allows you to modify the color of different areas such as backgrounds, borders, texts, and more.
15. To change all UI design tokens, scroll down to Advanced design tokens. You can modify the color of different areas. For more information see the Carbon Design System documentation (Guidelines > Color > Tokens).
16. Click Save.

Configure the user login page

You can configure a splash message to communicate any information your users may need; for example, a welcome message, an upcoming maintenance window, a configuration change, and so on. You can also provide login guidance to your users by configuring the login buttons and associated instructions on the login page.

These configuration options are in addition to your ability to [brand](#) the login page with your logo and a background image.

Configure the login button and label and associated instructions on Admin > Authentication. See [Configuring authentication methods for your organization](#) for details and a procedure.

To configure the login page button labels, button instructions, button order and a splash message, do the following:

1. Go to Organization > Profile and branding.
2. To configure a login page splash message to your users, enter the message in the text box in the Organization > Profile and branding > Profile > Splash message field. Use Markdown to format the message as required. To delete the message, simply remove the text from the text box.
3. To configure the login button labels, along with instructions (if needed) that display with the login button, go to Authentication > OAuth, or to Authentication > SAML instance > Profile.
4. To configure the order of the button display on the login page, scroll to the Organization > Profile and branding > Login options area. Click the arrows or drag each button to display them in your intended order.

5. Click Save.

Give users access to local or cloud storage

Typically, an organization has existing storage that your Aspera on Cloud users need to access. To enable this access, you *attach* or add a node to your AoC organization. A node can be your own Aspera High-Speed Transfer Server, or can be storage in a cloud provider region. The nodes or storage you attach are in addition to the built-in storage in IBM Cloud that is an automatic part of your Aspera on Cloud subscription.

Once you attach the node, you must make the intended content on the node available to users in the Files or Packages app in a workspace in your org. You do this by *administratively sharing* a folder on the node to workspace members. When you share as an admin, all admins in your org can manage access and permissions to the folder. This is generally preferable to sharing a folder as a user; in this case, only the user who shared the folder can manage the contents and permissions.

To attach your own HSTS node (org admin credentials required), go to [Tether Your Aspera Transfer Server to Aspera on Cloud](#).

To attach your existing cloud storage (ATS admins credentials required), go to [Attach your existing cloud storage](#).

You can also create one or more access keys to allow access to attached nodes and storage to allow access as follows: For access key details and procedures, see [Access keys](#).

- You can allow other admins or workspace managers to access and manage specific content on your attached node.
- You can allow an API client or other integration to access specific content on your attached node.

See [this article](#) for more information on your built-in IBM Cloud storage.

Share a node folder with a workspace

To allow the members of a workspace to use the content in a node attached to your org, an admin must give them access to the content. When you *administratively share* a folder with users, as described in this procedure, all admins in your org can manage the folder access. This shared management ability is typically preferable to having one admin user share a folder as an individual user; in such case, only that individual admin can revoke or change access permissions.

Use this procedure to give users in the Files application:

- Shared access to content in your cloud or on-prem storage.
- A folder in which they can collaborate on content according the permissions you set.

Once you share the folder using this procedure, users see it on the top level of their Files app.

For each folder you share, you set permissions for each user and group you share with. These permissions determine the actions that users can take on the folder contents. For details, see [Content Permissions](#).

This procedure allows you to share one folder at a time with one or more members of a single workspace. To share multiple folders, or to share a folder with users in multiple workspaces, repeat the procedure

Procedure

Note: To complete this procedure, you need the secret of the node containing the folder you want to share.

1. Go to Workspaces > *workspaceName* > Applications > Files app > Shared folders > Create new.
2. Do one of the following:
 - Enter the node secret and click Log in.
 - If you have a different access key for this node, click **Use custom access key**, enter the key and associated secret, then click **Log in**.
3. (Optional) To create a new folder on the node, do the following:
 - a. Click Create folder.
 - b. Enter a name for the new folder and click Create.
4. From the list of folders that displays, select the folder to share by clicking the option button on the folder row.
If required, you can click a folder name to drill into it. Go back up a level using the breadcrumb list at the top of the modal.
5. (Optional) To display a different name for the folder to the workspace users (perhaps a name that may be most meaningful to them), enter the desired name in the Display name text box.
6. Click Submit.
7. To give all members of the workspace access to this folder, click Add all workspace members.
 - a. Set the access permission level for these users.
 - b. If desired, add other members you want to access this folder at the permission level you set.
 - c. Click Add.
8. To give specific workspace members access to this folder, click Add member.
 - a. Set the access permission level for these users.
 - b. Enter the names of workspace members which whom to share this folder at this permission level.
 - c. Click Add.
9. To change a user's access to the shared folder, click the user row to open the record, adjust permissions as required, then click Save.
10. To remove a user's access to the shared folder, select the check box to the left of the user row and click Delete.

Note:

When new members join the workspace Files app, they can see and access shared folders as follows:

- Folders shared with the entire workspace.
- Folders shared with the new member as an individual or as a group member.

Add a member to an existing shared folder

1. Go to **Workspaces > workspaceName > Applications > Files app > Shared folders**.
2. Right-click the intended folder to see the current member list.
3. Do one of the following:
 - Enter the node secret and click Log in.
 - If you have a different access key for this node, click **Use custom access key**, enter the key and associated secret, then click **Log in**.
4. Click Add member.
5. Select the access permission for this new member.
6. Enter the member name.
7. Repeat steps 5 and 6 for additional new members.
8. Click Add.

Node access for workspace managers

1. Go to Workspaces > workspaceName > Profile > Node access for workspace managers.
2. Click Add.
3. In the Name drop down, select the node you want to give access to.
4. In the Access key field, enter the access key provided by your administrator.
5. In the Secret field, enter the secret associated with the access key.
Click the eye icon to show or hide the secret as you type.
6. From the Node owners drop down, select who can manage the node:
 - a. Only ATS admins: Only ATS administrators can manage the node.
 - b. All admins: All administrators can manage the node.

Note: Node owners can browse and manage this node without the need of an access key.
7. Click Log in to save the configuration and establish node access.
8. Click Cancel if you do not want to save the configuration and exit.

Add users: Overview

As a productivity and collaboration tool, Aspera on Cloud assumes a diverse user base. There are multiple user types and roles that you can assign to maximize the effectiveness of your org members. There are also multiple ways to add users, both in bulk (IBMid, SAML) and individually.

For detailed procedures, see articles in the following sections:

- [Authentication](#)
- [Users and groups](#)
- [User roles and types](#)

Delegate to a workspace manager

If desired, you can grant workspace manager privileges to one or more members in a workspace. A workspace manager can take over certain management tasks in that workspace.

For example:

- Adding and removing workspace members.
- Creating and managing groups.
- Granting and revoking workspace manager privileges to other users in the same workspace.
- Manage email notification templates and delivery options.
- Manage the settings of the Files app in the workspace.
- Manage the settings of the Packages app in the workspace, including shared inboxes.

The workspace manager role is optional, since organization administrators can manage every aspect of all workspaces. The workspace manager must be a member of the workspace.

Access keys

You can [generate an access key and secret](#) to a folder on a transfer node that you have shared to a workspace ("administratively shared folder"). You can give this key pair to a workspace manager to allow them to manage content in this shared folder without giving the manager access to other content on the node.

Privacy in a multi-tenant organization

In a multi-tenant organization, when strict privacy between workspaces is required, you can ensure that workspace managers cannot see organization members beyond those in the groups they are enabled to manage. Otherwise, workspace managers can see the users and groups across the entire organization during operations like adding a member to a shared inbox, to a group, or to a workspace. Control this privacy setting at Organization > Advanced settings > Workspace manager privileges. The setting you configure here applies to all workspace managers in the entire organization.

For more information, see [Assign the workspace manager role](#).

Delegate app and email configuration

To delegate configuration of the Packages and Files apps and of email notifications in a specific workspace, do the following.

1. Go to Workspaces > *workspaceName* > Settings.
2. Select checkboxes for these settings:
 - a. To allow workspace managers to configure the email templates and delivery options for the workspaces they manage, allowing them to override the email settings inherited from the global org settings, select the box labeled Workspace managers can edit email settings.
 - b. To allow workspace manager to configure the Files app in the workspaces they manage, allowing them to override the Files app settings inherited from the global org settings, select the box labeled Workspace managers can edit the settings of the Files application.
 - c. To allow workspace manager to configure the Packages app in the workspaces they manage, allowing them to override the Files app settings inherited from the global org settings, select the box labeled Workspace managers can edit the settings of the Packages application.
3. Click Save.

To reserve these configuration responsibilities for org admins, clear the checkboxes.

Set the default storage location for your organization

The organization *default node* automatically stores the files, folders, and packages of any new workspaces you create. The system default node is the built-in node in IBM Cloud that comes with your subscription. If you attach additional nodes or storage attached to your Aspera on Cloud organization, you can select a different node as the default.

For whichever node you select as default, the default storage paths are as follows:

- For content in the Packages app: `/workspace/workspace_id/packages`.
- For content in the Files app: `/workspaces/workspace_id/home`.

Every workspace in your organization inherits the default node for the organization. But you can override the organization default for a new workspace and assign a different node for workspace storage. For details, see [Create a new workspace](#).

To set the default node for your organization, do the following:

1. Go to Nodes and storage > Settings.
2. In the Default node field, select the intended node.
3. Click Save.

Session and token duration

You can configure settings for your organization that govern session duration and security token behaviors.

Parameters and definitions follow the procedure below.

Note: Administrator session duration parameters are not configurable.

Note: Numeric entries cannot begin with zero (0).

You can configure user session duration using the parameters in this section. Aspera on Cloud manages sessions using three types of tokens: a login token (also called an access token), a refresh token, and a transfer node token.

To configure settings for your organization, do the following:

1. Go to Organization > Security.
2. To enable a setting, select the checkbox; to disable a setting, clear the checkbox.
3. Enter the intended duration.
4. Click Save.

Access (login) token expiration

The login token expiration defines the maximum duration of an active session unless the refresh token duration (see previous parameter) is configured to extend the session. Unless refresh tokens are configured, users must re-authenticate when the login token expires.

- Default duration is 1 hour.
- Valid durations are 15 minutes to 24 hours.

Refresh token rotation

The refresh token defines the maximum duration that an active login session can be extended. This option is disabled by default for new organizations.

When a user logs in, Aspera on Cloud grants the user a login token (see the following parameter) and a refresh token. The refresh token provides an active user with subsequent login tokens, extending their active session for the duration you configure for this parameter.

- When enabled, the user session is extended, in increments equal to the login token duration, for the duration you configure for this parameter. For example, if the login token expiration is set to 1 hour and the refresh token expiration is set to 1 day, Aspera on Cloud issues new login tokens to an active user each hour for 24 hours. Then the session expires and the user must reauthenticate.
 - Recommended duration is 7 days.
 - Valid durations are 1 day to 365 days.

Inactive session logout

You can configure a maximum duration for inactive sessions. This option is disabled by default for new organizations.

- When enabled, an inactive session is automatically logged out after the duration you configure.

- Recommended duration is 1 hour.
- Valid durations are 15 minutes to 7 days.
- When disabled, user sessions are never logged out due to inactivity.

Transfer token expiration

The transfer node token expiration defines the maximum duration of authorized activity on the transfer node. This token, with the duration you configure here, is issued/reissued automatically when the login token is issued/reissued.

Note: You must set the transfer node token expiration duration longer than the login token expiration duration. Set the transfer node token duration to match your organization's longest transfer durations.

- Default duration is 12 hours.
- Valid durations are 1 hour to 14 days.

Configure email notifications for your organization

Aspera on Cloud provides numerous user notification options, including for events like being invited to join the organization, receiving a package, being invited to send a package, and many more. These articles describe how to use and customize the default notification templates provided, and how to control which events generate notifications.

- [Customize email notification templates](#)
Aspera on Cloud supports email notifications for various user and admin events, including invitations to an organization, workspace, or shared inbox, package and folder sharing events, user account deactivation, and many more.
- [Email template inheritance in Aspera on Cloud](#)
The Aspera on Cloud email template inheritance scheme accelerates and simplifies email customization.
- [Email template variables](#)
For most templates, you can select variables, such as `{workspace_name}`, `{sender_name}`, `{package_name}`, to use in editable fields.
- [Control email notification delivery](#)
As an administrator, you can control which events generate email notifications to your users.

Customize email notification templates

Aspera on Cloud supports email notifications for various user and admin events, including invitations to an organization, workspace, or shared inbox, package and folder sharing events, user account deactivation, and many more.

As an administrator or workspace manager, you can configure templates that govern the content and appearance of the various email notifications that Aspera on Cloud (AoC) generates. The AoC email template schema provides:

- Sensible defaults for ready-to-use ease.
- An inheritance scheme to accelerate and simplify customization.
- Granular configuration options for highly-customizable control of notifications.

Templates function on three levels:

- Organization (organization administrators only; not accessible to workspace managers)
- Workspace
- Shared inbox

AoC provides two types of templates you can customize:

- Base template: Customize the fields that are common to all event-driven notification templates; these include the From field and a logo, among others.
- Event-driven notification templates: Customize the fields in notifications for specific events; for example, the notification to a user who has received a package, or to a user receiving an invitation to join the AoC organization.

For each level, you can configure separate templates for the following user types:

- Members: AoC users who are standard or limited members of the given workspace.
- External users: Users who are not members of the given workspace.

For details on the inheritance scheme and configuration options, see [Email template inheritance in Aspera on Cloud](#) and [Email template variables](#).

You can also control whether or not email notifications for specific events are delivered, customizing these settings for the organization, for individual workspaces, and for individual shared inboxes; see [Control email notification delivery](#).

Note: To troubleshoot email notification issues, see [Email notifications](#) in the "Troubleshooting and support" section.

Configure organization-level email templates

Note: Only organization administrators can configure organization-level templates.

You can allow organization templates to remain at their system default settings, or you can customize them for your organization.

Keep the following behaviors in mind:

- The settings for the organization base template:
 - Propagate to all event-driven templates in the organization.
 - Are inherited by all workspace base templates in the organization.

- The settings for a given organization-level event-driven template are inherited by the corresponding template in each workspace.

To use organization default settings, select Organization > Email templates > Use default settings > On.

Otherwise, to customize email templates at the organization level, do the following:

1. Go to Organization > Email templates.
2. Click the toggle labeled Use default settings to Off.
3. To configure different email templates for members than for external users, select the checkbox labeled Enable external user templates.
4. Click to select the template to configure (for example, Base > Base external or Packages > Package uploaded).
5. Configure each template as follows:
 - a. Enter text as required in each field.
 - b. To use variables, click Use variables; from the list that is displayed, copy the desired variable and paste it into the appropriate template field.
 - c. (Base template only) Select the desired logo to be included in the email heading: either the default Aspera on Cloud logo or the organization logo (configured at Organization > Profile and branding)
 - d. (Base template only) The logo you select above appears in a header. Select the header color (black or white) to provide a contrasting or complementing background for your logo.
6. To revert to default and inherited settings, click Reset.
7. To save the configuration, click Save.

Configure workspace-level email templates

By default, workspace templates inherit configurations from the organization templates. But you can customize templates for individual workspaces.

Keep the following behaviors in mind:

- Base template
 - Pre-existing base template settings for a workspace are inherited from the organization base template.
 - The settings for the workspace base template:
 - Propagate to all event-driven templates in the workspace.
 - Are inherited by the base templates in all shared inboxes in the workspace.
- Event-driven templates
 - Pre-existing event-driven template settings for a workspace are inherited from the corresponding organization template.
 - The settings for a given workspace-level event-driven template are inherited by the corresponding template in each shared inbox in the workspace.

To use settings inherited from the organization, select Workspaces > *workspaceName* > Email templates > Use organization settings > On. For more information about inheritance, see [Email template inheritance in Aspera on Cloud](#).

Otherwise, to customize email templates at the workspace level, do the following:

1. Go to Workspaces > *workspaceName* > Email templates.
2. Click the toggle labeled Use default settings to Off.
3. To configure different email templates for members than for external users, select the checkbox labeled Enable external user templates.
4. Click to select the template to configure (for example, Base > Base template or Packages > Package received).
5. Configure each template as follows:
 - a. Enter text as required in each field.
 - b. To use variables, click Use variables; from the list that is displayed, copy the desired variable and paste it into the appropriate template field.
 - c. (Base template only) Select the desired logo to be included in the email heading: choose the default Aspera on Cloud logo, or the organization logo, or the workspace logo (configured at Workspaces > *workspaceName* > Profile > Name).
 - d. (Base template only) Select the header color (black or white) to provide a contrasting or complementing background for your logo.
6. To revert to inherited settings, click Reset.
7. To save the configuration, click Save.

Configure shared inbox-level email templates

By defaults, shared inbox templates inherit the workspace templates. You can customize them for individual shared inboxes.

Keep the following behaviors in mind:

- Base template
 - Pre-existing shared inbox base template settings are inherited from the workspace base template.
 - Settings for the shared inbox base template propagate to all event-driven templates in the shared inbox.
- Event-driven templates: existing settings are inherited from the corresponding workspace template.

To customize email templates at the shared inbox level, do the following:

1. Go to the Templates settings for the shared inbox:
 - In the Admin app, go to Workspaces > *workspaceName* > Applications > Packages > Shared inboxes > *sharedInboxName* > Email templates.
 - In the Packages app, click Manage shared inboxes in the left-side panel, then click *sharedInboxName* > Email templates.
2. To use settings inherited from the workspace, set the toggle labeled Use workspace settings to On.
3. To customize settings for this shared inbox, set the toggle labeled Use workspace settings to Off.
4. To configure different email templates for members than for external users, select the checkbox labeled Enable external user templates.
5. Click to select the template to configure (for example, Base > Base Template or Packages > Package received).
6. Configure each template as follows:
 - a. Enter text as required in each field.
 - b. To use variables, click Use variables; from the list that is displayed, copy the desired variable and paste it into the appropriate template field.
 - c. (Base template only) Select the desired logo to be included in the email heading: choose the default Aspera on Cloud logo, or the organization logo, or the workspace logo, or the shared inbox logo (configured at Workspaces > *workspaceName* > Applications > Packages > Shared inboxes > *inboxName* > Profile).
 - d. (Base template only) Select the header color (black or white) to provide a contrasting or complementing background for your logo.
7. To revert to inherited settings, click Reset.
8. To save the configuration, click Save.
9. If you enabled different templates for external users, repeat steps 4 through 7 to configure each external user template.

Revert to inherited template

For each individual template, you can revert to the settings inherited from the base template and from the parent template. For example, if you are configuring a shared inbox-level template and click "Reset", that specific template will use configurations inherited from the shared inbox base template and from the corresponding workspace-level template.

For more information about inheritance, see [Email template inheritance in Aspera on Cloud](#).

Email template inheritance in Aspera on Cloud

The Aspera on Cloud email template inheritance scheme accelerates and simplifies email customization.

There are two types of inheritance that interact with each other in the AoC email template customization schema:

- Inheritance from the base template
- Inheritance from parent template to child template (applies to base templates and to event-driven templates)

Note: To troubleshoot email notification issues, see [Email notifications](#) in the "Troubleshooting and support" section.

Base template inheritance

At each of the three template levels (organization, workspace, and shared inbox) you can configure a base template. The base template allows you to customize the fields that are common to all event-driven templates. You can customize the following fields only by configuring them at the base template:

- Subject prefix (for example, if you configure this field to read 'Urgent: ', the Subject line of each notification generated will begin with 'Urgent: ', followed by the subject entered by the sender)
- From
- Email logo (supported file types:.jpg,.png; maximum size: 512 kb; recommended dimension: square; see [Customize your organization URL, name, and logo](#))
- Email title
- Footer

Note: To customize fields not in the base template, go to the individual event-driven templates.

In addition to the base template for the organization, each workspace in the organization has its own base template. Further, each shared inbox in each workspace has its own base template.

Base templates influence related templates in two ways simultaneously:

- Settings in the base template propagate to event-driven templates at the same level.
- Settings from parent base templates are inherited by child base templates.

Propagation of settings from base templates to event-driven templates

The settings you configure for base template fields propagate to all the event-driven templates at that level. For example, when you customize the 'Subject-prefix' field in the base template at the organization level, that customized 'Subject-prefix' setting propagates to all the email templates at the organization level (for example, the 'Welcome to Aspera on Cloud' notification, the 'Package Received' notification, the 'Folder Shared' notification, etc.).

Similarly, settings you configure at the workspace base template propagate to all workspace-level event-driven templates. And settings from a shared inbox base template propagate to all shared inbox event-driven templates.

Inheritance from parent base template to child base template

Settings configured in the parent base template are inherited by the child base template: from organization base template to the base template in each workspace; and from workspace base template to the base template in each shared inbox in each workspace.

If you configure only the organization base template, those settings will:

- Be inherited by child base templates in workspaces and shared inbox
- Propagate through all event-driven templates in the organization.

However, each workspace has its own base template that you can customize to override the inheritance from the organization base template. If you do not override the settings inherited from the organization base template, the workspace templates display the settings configured at the organization base template.

Similarly, these workspace base template settings are inherited by each shared inbox base template (and in turn by the event-driven templates at the shared inbox level). Again, for each shared inbox, you can override the settings inherited from the workspace base template and configure customized shared inbox base template settings; again, the settings you configure at the shared inbox base template propagate to all the event-driven templates for that shared inbox.

Parent-to-child inheritance

For both base templates and event-driven templates, templates at each level inherit the configuration of templates at the parent level: shared inbox templates inherit from workspace templates; workspace templates inherit from organization templates.

However, you can override the inheritance for many configurable fields.

If you don't configure the templates at the workspace level, workspace-level notifications reflect the settings at the organization level. Similarly, if you don't configure the templates at the shared inbox level, shared inbox-level notifications reflect the settings at the workspace level (which may in fact inherit from the organization).

At any level, you can configure none, some, or all configurable fields. A configurable field that you don't configure inherits the configuration from the parent level.

Unique templates for internal and external users

If desired, you can configure unique templates for external users. External users are not members of your AoC organization, but when allowed by the AoC administrator, members of a given workspace can send to, share with, and request files from these external members.

For external user templates, both base and event-driven templates follow a parallel inheritance path to member templates. External user templates do not inherit from member templates.

Email template variables

For most templates, you can select variables, such as `{workspace_name}`, `{sender_name}`, `{package_name}`, to use in editable fields.

Select the template to edit, then click Use variables to display the variables available for the current template. Copy the variable you want from the list on the right of the template into the intended field. When AoC generates a notification, it substitutes the actual data indicated for the variable.

The variables available depend on the specific template you are editing.

For example, user John Doe, member of the Marketing workspace, sends a package named 'New Package' to Jane Smith with the following template:

```
Hello {recipient_name}. You've received the package "{package_name}" from {sender_name}. Log in to your AoC organization in the {workspace_name} workspace to view and download the content.
```

The generated notification might be the following:

```
Hello Jane Smith. You've received the package "New Package" from John Doe. Log in to your AoC organization in the Marketing workspace to view and download the content.
```

Note: To troubleshoot email notification issues, see [Email notifications](#) in the "Troubleshooting and support" section.

Control email notification delivery

As an administrator, you can control which events generate email notifications to your users.

You can control notifications at the organization, workspace, and shared inbox levels, using the inbuilt inheritance scheme to accelerate and simplify customization. See [Customize email notification templates](#) for related information and procedures.

Note: To troubleshoot email notification issues, see [Email notifications](#) in the "Troubleshooting and support" section.

Configure organization-level notification delivery

Note: Only organization administrators can configure organization-level settings.

Keep the following behaviors in mind:

- By default, all notifications are enabled. For your organization, you can do one of the following:
 - Allow notification delivery settings to remain at their system default settings (all notifications enabled).
 - Disable all notifications.
 - Customize which notifications are delivered.
- Settings at the organization level are inherited by all workspaces in the organization to become workspace-level default settings (which can be modified for individual workspaces).

To control email notification delivery at the organization level, do the following:

1. Go to Organization > Notifications.
2. To disable all notifications for this organization, click **Toggle all notifications**. Skip to step 4.
3. To customize notification settings for this organization, click the toggle for each notification as required.
4. Click Save.

Configure workspace-level notification delivery

By default, workspace notification delivery settings are inherited from the organization settings. You can customize the settings for individual workspaces.

Keep the following behaviors in mind:

- Pre-existing settings in each workspace are inherited from the organization settings. You can override these for each individual workspace if desired.
- Settings for a given workspace are inherited by each shared inbox in the workspace.

To control email notification delivery at the workspace level, do the following:

1. Go to Workspaces > *workspace_name* > Notifications.
2. To override the settings inherited from the organization, click the toggle labeled Use organization settings to Off.
3. Click the toggle for each notification as required.
4. Click Save.

Configure shared inbox-level notification delivery

By default, shared inbox notification delivery settings are inherited from the workspace settings. You can customize the settings for individual shared inboxes.

By default, the notifications you select go to all shared inbox members. But if desired you can limit notification delivery to members you specify (this setting applies to notifications for shared inbox events only, not to workspace- or org-level notifications).

Keep in mind that the pre-existing settings in each shared inbox are inherited from the workspace settings.

To control email notification delivery at the shared inbox level, do the following:

1. You can configure email notifications from the Admin or Packages app:
 - In the Admin app, go to Workspaces > *workspace_name* > Applications > Packages > Shared inboxes > *sharedInboxName* > Notifications.
 - In the Packages app, click Manage in the left-side navigation panel, then click *sharedInboxName* > Notifications.
2. To override the settings inherited from the workspace, click the toggle labeled Use workspace settings to Off.
3. Click the toggle for each notification as required.
4. To specify individual recipients for these notifications, click the toggle labeled Send to custom recipients to On. Select recipients from the existing members of the shared inbox. If you don't specify individual recipients, all shared inbox members receive notifications.
5. Click Save.

Storage and workspace configuration scenarios

This section provides detailed, step-by-step configuration guidance for some typical usage scenarios, including configuring workspaces, users and groups, collaboration scenarios, and related notifications, designed to be adapted to the specifics of your use case.

- **Configuration scenario: Sharing with external colleagues**
If your team collaborates with vendors, contractors, or other colleagues in a different company by sharing access to a repository of files and folders, use this article to configure your organization. You'll use the Aspera on Cloud Files app to enable secure and permission-based sharing of folders among designated collaborators.
- **Configuration scenario: Workspace members sharing a file repository**
If your team shares access to files and folders in a common repository, use this article to configure your organization. You'll use the Aspera on Cloud Files app to enable secure and permission-based sharing of folders among collaborators.

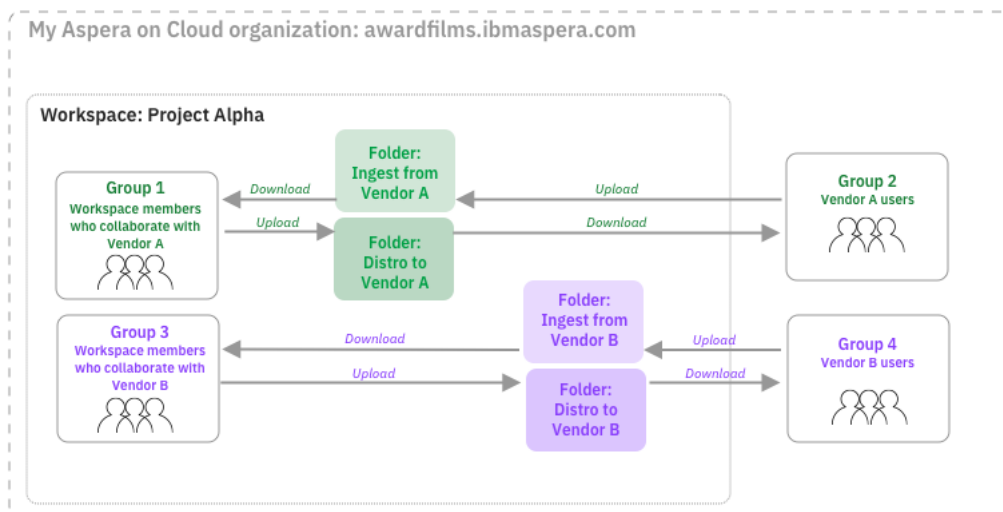
Configuration scenario: Sharing with external colleagues

If your team collaborates with vendors, contractors, or other colleagues in a different company by sharing access to a repository of files and folders, use this article to configure your organization. You'll use the Aspera on Cloud Files app to enable secure and permission-based sharing of folders among designated collaborators.

For example, perhaps your team is:

- A news organization receiving files from dispersed reporters and content providers.
- A production company distributing files to theaters in diverse locations.
- A team of scientists collaborating with researchers at a distant university to study the feasibility of exploratory mining in a given site.
- Part of a production company sharing assets with vendors who provide coloration or other services.
- A medical research group sharing large sets of genomic data files with scientific collaborators at remote sites.

Aspera proposes a workspace like this. This setup is flexible of course, and you can adapt it for your specific needs.



Your AoC organization: Overview

Your Aspera on Cloud (AoC) organization is the primary container and administrative unit in your AoC subscription.

Customize your URL to brand your org

You can name your org and configure the subdomain of the URL that users will browse to access your org. For example, if your company name is Award Films, you can choose to use the URL `awardfilms.ibmaspera.com`. For details on this one-time-only configuration, see [Customize your organization URL, name, and logo](#).

Your users collaborate in a workspace

A workspace is a digital space where designated members can collaborate. Each workspace is a collection of specific users, files and folders, access permissions, and collaboration rules. The users, files, and folders in one workspace are completely separate from those in another workspace. You'll configure a workspace in Procedure 2

below.

Users in a given workspace can collaborate freely with other members of the same workspace. By default, workspace members can also collaborate with users outside the workspace. But the admin can restrict that privilege if necessary; see Procedure 3 below.

Your files and folders are in IBM Cloud storage

Each Aspera on Cloud subscription includes one built-in, [Aspera-managed auto-scale transfer cluster](#) attached to storage in IBM Cloud.

This Aspera transfer cluster (also called ATS, Aspera transfer service; sometimes called a *node*) is the engine that AoC uses to upload and download your files and folders to and from your built-in IBM Cloud storage. ATS is hosted and managed by IBM Aspera.

The built-in IBM Cloud storage hosts your organization workspace, including the content your users upload and share using the Files app. As an admin, you can also upload content directly to this storage and then make that content available to your users. (Storage capacity depends on your AoC subscription tier.) See procedure 4 below.

The access credentials (access key and secret) for this transfer cluster and storage are delivered to the administrator who first created the AoC organization. You should [retrieve and securely store the access credentials](#); they allow you to access and manage your IBM Cloud storage.

Note: You can attach your own local or cloud storage to Aspera on Cloud and then share storage contents with workspace users, but that process is not covered in this document; see articles in the Nodes section of this Help Center.

- To attach your existing cloud storage to AoC, see [Attach your existing cloud storage](#).
- To attach your own Aspera HSTS server, see [Tether Your Aspera Transfer Server to Aspera on Cloud](#).

Process overview

These are the high-level steps required to configure the scenario shown in the graphic in the opening section of this article; detailed procedures follow. Adapt as needed for your own requirements.

Use the AoC Admin app to:

1. Create groups of users, both internal and external, to simplify and accelerate user management.
2. Configure the workspace in which your groups will collaborate. Add your internal user groups as workspace members.
3. (Optional) Configure the Files app to allow your workspace members to collaborate with your designated external groups only. This configuration is by no means required, but provides content security for your proprietary assets.
4. Create the folders in which your internal and external groups will collaborate; share the folders with your groups, assigning specific permissions to allow them access while preserving content security.
5. (Optional) Configure notifications to alert internal users when new content appears in their folders.

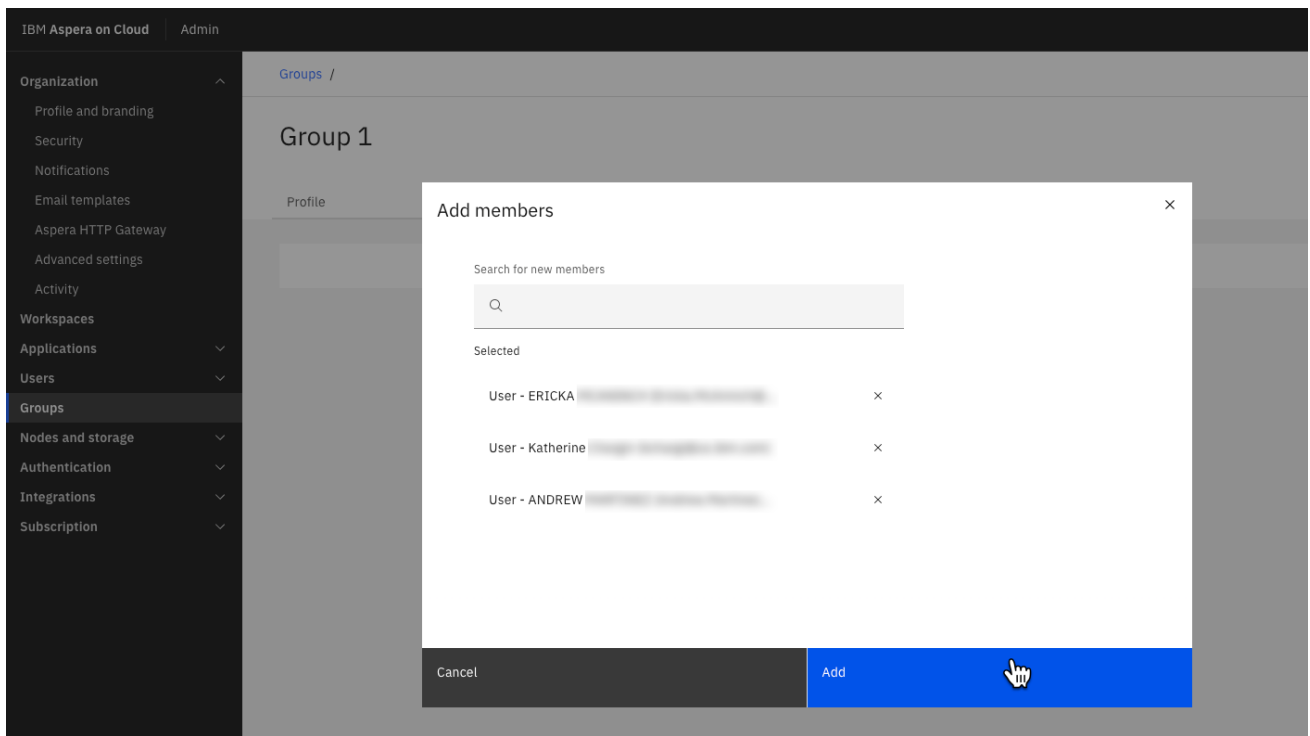
Important: As an admin, you must provide a transfer method for your users. You can do either of the following:

- Notify your users that they will be prompted to download and install [IBM Aspera Connect](#), the free, lightweight client app that enables high-speed transfers between the AoC app and the user desktop. For most browsers, users must also install a browser extension on each browser they use to access Aspera on Cloud. See [Installation](#).
- Configure the [IBM Aspera HTTP Gateway](#), then attach it to Aspera on Cloud. This transfer method does not require users to download and install the Aspera Connect client.

1. Create groups to accelerate user management

Use the AoC Admin app to create groups and add members to each group. You can add group members as follows:

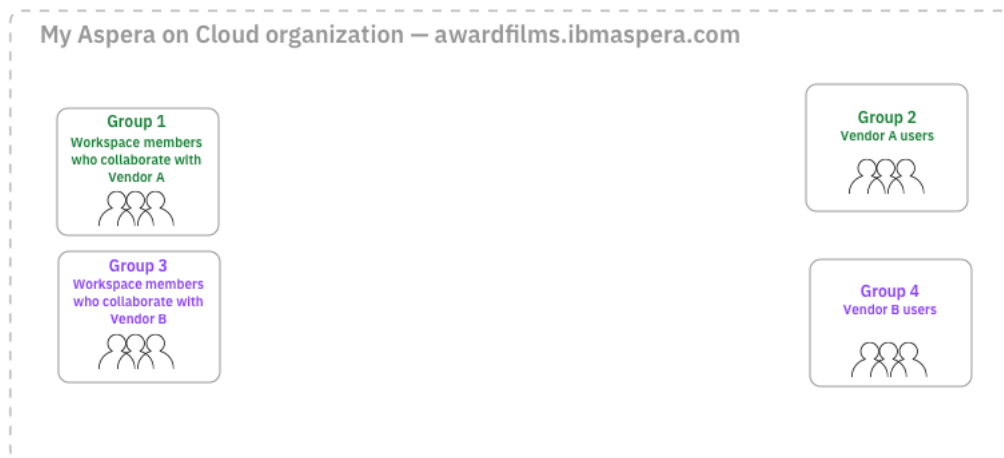
- Add users who are already members of your AoC organization. You'll see their names or email addresses auto-filling in the *Add members* dialog.
 - Add users who are not part of your AoC org. When you add new users to a group, you simultaneously add them as members of the organization.
1. Go to the Admin app by clicking the app switcher  and selecting Admin.
 2. Go to Groups > Create new.
 3. Give the group a name; for example, Group 1.
 4. Click Save.
You have created the group; now add members to it.
 5. Click Members > Add members.
 6. Enter user names or email addresses for these group members and click Add. You can add multiple members in one operation.



7. Repeat this procedure for the additional groups:

- Group 2 (external group: Vendor A users)
- Group 3 (internal users who collaborate with Vendor B)
- Group 4 (external group: Vendor B users)

After you create the four groups, your Aspera on Cloud org looks like this:



2. Configure the workspace for user collaboration

Now set up the workspace and make your internal groups workspace members.

Every AoC subscription is configured with one default [workspace](#). Aspera recommends that you rename and use your default workspace. Depending on your [subscription](#), you may be able to create a new workspace.

1. Go to **Workspaces > Default workspace**.
2. Give this workspace a name that clearly indicates its purpose; for example, Project Alpha.
3. Click Save.
4. Click Members > Add member.
5. In the Search for new members field, enter the names of your *internal* user groups; for example: Group 1, Group 3.

Note: Add yourself as a workspace member so you can verify correct workspace configuration. You can revoke your membership later if desired.

Important: Do *not* enter the names of the external groups.

These external users become [limited users](#) in your AoC org. Limited users have no access to workspace content beyond what you specifically share with them; this limited access enhances security for the content in the workspace.

6. Click Add.

You now have a workspace with your internal groups as members.



2a. Disable the Packages app in your workspace (optional)

Both the Files and Packages apps are enabled by default. This workspace uses only the Files app, so disable the Packages app. You can re-enable it at any time.

Important: Before you perform this procedure, be sure that you have [retrieved the access key for your built-in node and storage](#); the admin who created the AoC organization received the credentials in a digital package from Aspera Tech Support. You can re-enable the Packages app any time.

1. If necessary, open your new workspace: Workspaces > Project Alpha.
2. Click Applications > Packages.
3. Clear the checkbox labeled Use global app settings.
4. Clear the checkbox labeled Enable application.
5. Click Save.

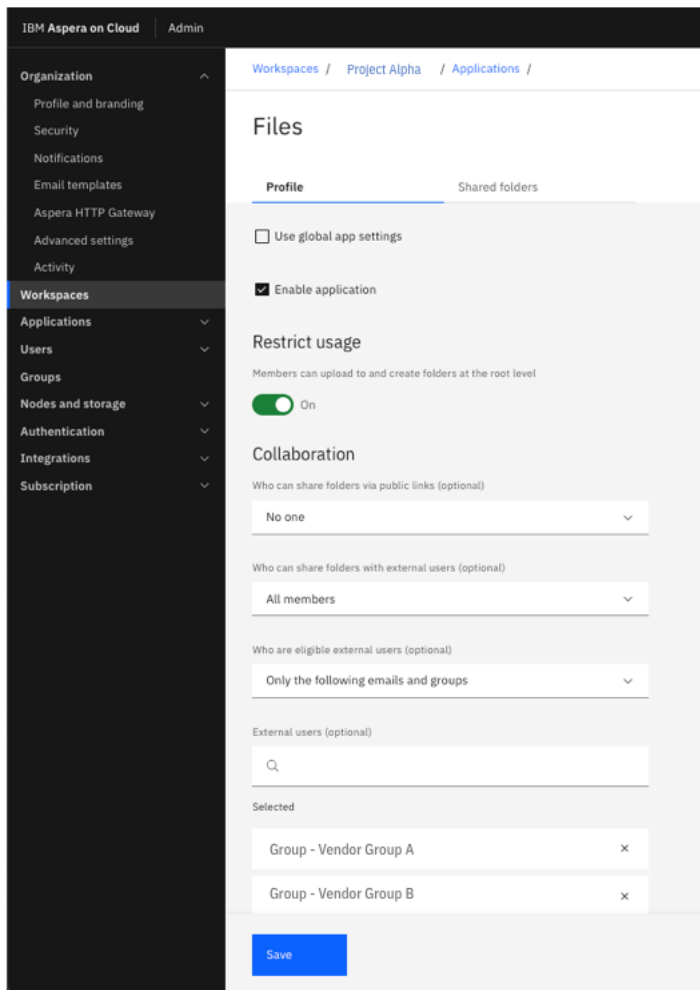
3. Configure the workspace Files app for secure collaboration (optional)

In this optional procedure, you'll configure the following specific collaboration capabilities for your workspace members. If you don't need these additional controls and security, skip this procedure.

- Allow workspace members to upload content *only* into the folders you designate. This configuration makes it easy for you to monitor storage usage and transfer volume.
- Designate your external groups (Group 2 and Group 4) as the *only* external users your workspace members can share with. This configuration ensures content security.

Configure the Files app:

1. Go to Workspaces > Project Alpha > Applications > Files.
2. Clear the checkbox labeled Use global app settings.
3. In Restrict usage, click the toggle labeled Members can upload to and create folders on their home folder to On.
The home folder is the root level of the Files app. By preventing uploads to this root level, you ensure that users upload content only into the folders you create on the built-in IBM Cloud storage and share with the workspace (see Procedure 4); these are folders you can readily monitor. For details, see [Managing storage usage](#).
4. In Collaboration, do the following:
 - a. Set Who can share folders via public links to No one.
This setting prevents members from sharing folders with public users.
 - b. Set Who are eligible external users to Only the following emails and groups.
 - c. Click the Search field and enter the external vendor groups; for example, Group 2 and Group 4.
This configuration ensures that workspace members can share folders only with each other and with your two external vendor groups.
5. Click Save.

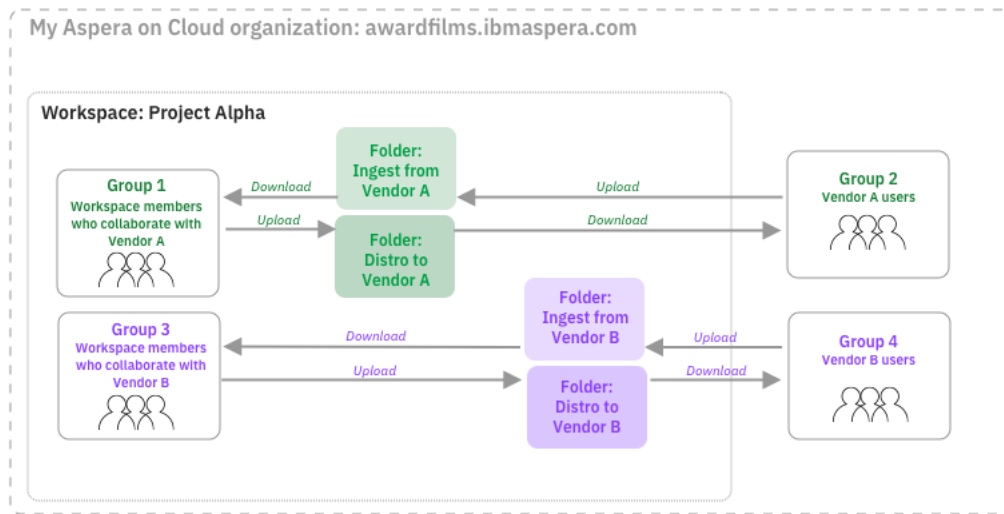


4. Create and share the collaboration folders with the groups

Now set up folders on your IBM Cloud storage and share them with your groups, giving them the spaces to collaborate in. You'll give access and the required permissions to each group. Then you can upload the desired content to the folders, or allow the users with "Upload" permission to populate the folder content.

You'll need the node secret for this procedure. To find the secret, see Important note in procedure 2a.

Recall that this is the configuration goal:



Folder permissions

As you share, you'll assign permissions to each folder based on the group and their access needs. Aspera recommends the following permissions matrix. Adjust for your own situation and goals.

skip this table and simplify the following procedure to omit assigning permissions. For details, see [Content permissions](#).

Folders	Permissions			
	Group 1	Group 2	Group 3	Group4
Ingest from Vendor A	• Browse • Download • Delete • Preview	• Browse • Upload files • Create directory	n/a	n/a
Distro to Vendor A	• Browse • Upload files • Create directory	• Browse • Download • Delete • Preview	n/a	n/a
Ingest from Vendor B	n/a	n/a	• Browse • Download • Delete • Preview	• Browse • Upload files • Create directory
Distro to Vendor B	n/a	n/a	• Browse • Upload files • Create directory	• Browse • Download • Delete • Preview

To create and share folders, do the following:

1. Go to Workspaces > *Project Alpha* > Applications > Files > Shared folders > Create new.
2. In the *Node access* dialog that opens, select the intended node, enter your node secret, and click Log in.
3. Create a folder for Group 1 to upload content for Group 2 to download:
 - a. In the *Choose folder to share* dialog that opens, click Create folder.
 - b. Name the folder "Distro to Vendor A", then click OK. The new folder appears in the list.
 - c. Click to select this new folder, then click Submit. This action makes the folder a shared folder.

Choose folder to share

Display name (optional)

Enter the name that members see. Leave blank to use the current folder name.

[Root](#)

Create folder

	Name	Size	Last updated
☐		—	—
☒	Distro to Vendor A	—	—
☐		4 MB	1/31/19 3:45 PM

Cancel

Submit

- d.
- e.
4. Share the folder "Distro to Vendor A" with Group 1, giving your internal users permission to upload to this folder:
 - a. Click the folder row to open it, then click Add member.
 - b. Click the field that displays Can edit to display permission options.
 - c. Select permissions for Browse, Upload, Create folders. Then click off the permission list to close it. The field displays "Custom."

Permissions to "Distro to Vendor A" for Group 1 (workspace members who collaborate with Vendor A).

Add members

×

Select permissions

Custom

▼

☒ Browse
 ☐ Download
 ☒ Upload files
 ☐ Delete
 ☒ Create directory
 ☐ Rename
 ☐ Preview

Choose new members to add

🔍

Search for users or groups

Selected

Group - Group 1

×

Cancel

Add

- d.
 - e. In the field that displays Search for users or groups, enter Group 1.
 - f. Click Add.
 5. Share the folder "Distro to Vendor A" with Group 2, giving your users from Vendor A permission to download from this folder.
 - a. Click Add member.
 - b. Click the field that displays Can edit to open the permission options.
 - c. Select permissions for Browse, Download, Delete, and Preview. Then click off the permission list to close it. The field displays "Custom."
- Permissions to "Distro to Vendor A" for Group 2 (the users from Vendor A).**

Add members

×

Select permissions

Custom

▼

☒ Browse
 ☒ Download
 ☐ Upload files
 ☒ Delete
 ☐ Create directory
 ☐ Rename
 ☒ Preview

Choose new members to add

🔍

Search for users or groups

Selected

Group - Group 2

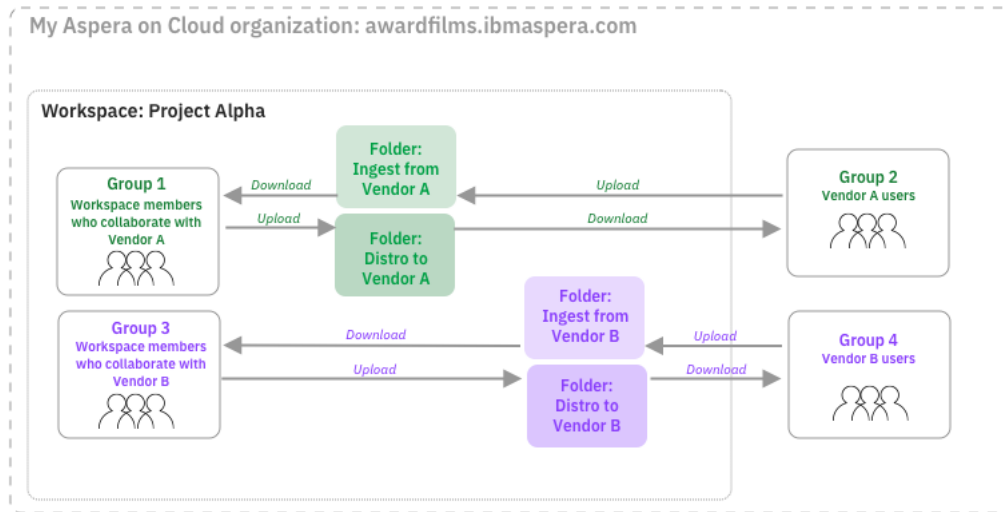
×

Cancel

Add

- d. In the field that displays Search for new members, enter Group 2.
6. Repeat the previous steps to create the folder "Ingest from Vendor A" with Group 1 and Group 2, reversing the permissions as shown in the permissions matrix.
7. Repeat these steps to create and share two more folders for collaboration with Vendor B, giving access and permissions to Group 3 and Group 4. Refer to the table in the section "Folder permissions".

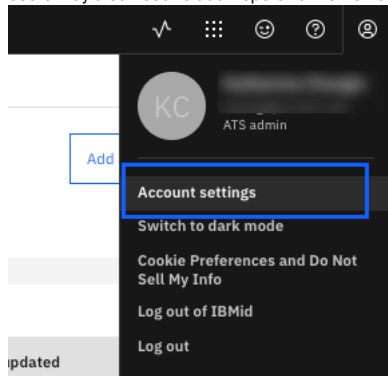
Result: Your internal and external groups can see the folders you created, and access folder content according to the permissions you assigned. Users must go to the workspace you set up in Procedure 2, and access the Files app in that workspace.



5. Configure notifications

By default, AoC sends email notifications to all users when they receive access to a shared folder. This means that the users in your internal and external groups receive an email with a link to access each folder you share.

Note: If internal users don't see the notifications, ask them to verify that they've enabled receipt of notifications in their Account Settings page. Both internal and external users may also need to add Aspera to their email contacts. See also ["Troubleshooting Email Notifications"](#).



You can also allow your internal users to configure a notification when content is added to a folder they need to monitor.

1. Go to Workspaces > Project Alpha > Notifications.
2. Click the toggle labeled Use organization settings to Off.
3. Click the toggle labeled Allow users to turn on notifications for new shared folder content to On.
4. Click Save.

Your internal users can now set notifications for themselves when new content is added to the folders they need to monitor. For a user procedure, see [Set notifications for new content in a shared folder](#).

Results

Your configuration work is done.

- Members of your internal groups are members of your org and the workspace Project Alpha. Each member of each internal group receives four email notifications.
 - The first contains a link allowing them to join the organization by logging in and creating an account.
 - The second email contains a link to join the workspace. These are *standard* users in your org.
 - The third and fourth emails contain links to the two folders you shared with them.
- In the workspace, your internal groups see two folders in their Files app. They can browse and upload content to the Distro folder, and browse, download, preview and delete content from the Ingest folder.
- Members of your external groups receive two email notifications, each with a link to one of the two folders you shared with them. When they click the link, an AoC portal opens to allow them access to the folder according to the permissions you set.
- The external group members do not see the workspace or any content beyond what has been shared with them. These are *limited* users in your org.

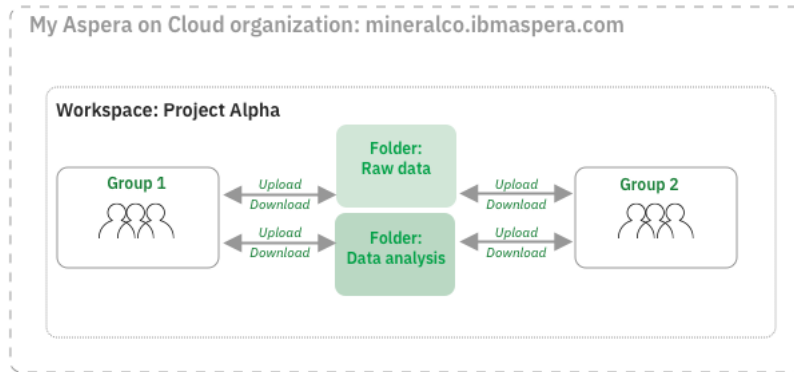
Configuration scenario: Workspace members sharing a file repository

If your team shares access to files and folders in a common repository, use this article to configure your organization. You'll use the Aspera on Cloud Files app to enable secure and permission-based sharing of folders among collaborators.

For example, perhaps your team is:

- A video production company developing a film through ideation, production, and editing.
- A team of geologists studying the feasibility of exploratory mining in a given site.
- Part of a production company sharing assets among internal teams who provide coloration, titles, or other services.

Aspera proposes a workspace like this. This setup is flexible of course, and you can adapt it for your specific needs.



Your AoC organization: Overview

Your Aspera on Cloud (AoC) organization is the primary container and administrative unit in your IBM Aspera subscription.

Customize your URL to brand your org

You can name your org and configure the subdomain of the URL that users will browse to access your org. For example, if your company name is American Mineral Company, you can choose to use the URL `mineralco.ibmaspera.com`. For details on this one-time-only configuration, see [Customize your organization URL, name, and logo](#).

Your users collaborate in a workspace

A workspace is a digital space where designated members can collaborate. Each workspace is a collection of specific users, files and folders, access permissions, and collaboration rules. The users, files, and folders in one workspace are completely separate from those in another workspace. You'll configure a workspace in Procedure 2 below.

Users in a given workspace can collaborate freely with other members of the same workspace. By default, workspace members can also collaborate with users outside the workspace. But the admin can restrict that privilege if necessary; see Procedure 3 below.

Your files and folders are in IBM Cloud storage

Each Aspera on Cloud subscription includes one built-in, [Aspera-managed auto-scale transfer cluster](#) attached to storage in IBM Cloud.

This Aspera transfer cluster (also called ATS, Aspera transfer service; sometimes called a *node*) is the engine that AoC uses to upload and download your files and folders to and from your built-in IBM Cloud storage. ATS is hosted and managed by IBM Aspera.

The built-in IBM Cloud storage hosts your organization workspace, including the content your users upload and share using the Files app. As an admin, you can also upload content directly to this storage and then make that content available to your users. (Storage capacity depends on your AoC subscription tier.) See procedure 4 below.

The access credentials (access key and secret) for this transfer cluster and storage are delivered to the administrator who first created the AoC organization. You should see [Secure the access credentials for your built-in node](#) retrieve and securely store the access credentials; they allow you to access and manage your IBM Cloud storage.

Note: If desired, you can attach your own local or cloud storage to Aspera on Cloud and then share storage contents with workspace users, but that process is not covered in this document; see articles in the Nodes section of this Help Center.

- To attach your existing cloud storage to AoC, see [Attach your existing cloud storage](#).
- To attach your own Aspera HSTS server, see [Tether Your Aspera Transfer Server to Aspera on Cloud](#).

Process overview

These are the high-level steps required to configure the scenario shown in the graphic in the opening section of this article; detailed procedures follow. Adapt as needed for your own requirements.

Use the AoC Admin app to:

1. Create groups of users to simplify and accelerate user management.
2. Configure the workspace in which your groups will collaborate. Add your user groups as workspace members.
3. (Optional) Configure the Files app to allow your workspace members to collaborate only within the workspace. This configuration is by no means required, but it allows you greater control over access to your proprietary assets.

4. In your built-in IBM Cloud storage, create the folders in which your groups will collaborate; share the folders with your groups, assigning specific permissions to allow access while preserving content security.
5. (Optional) Configure notifications to alert internal users when new content appears in their folders.

Important: As an admin, you must provide a transfer method for your users. You can do either of the following:

- Notify your users that they will be prompted to download and install [IBM Aspera Connect](#), the free, lightweight client app that enables high-speed transfers between the AoC app and the user desktop. For most browsers, users must also install a browser extension on each browser they use to access Aspera on Cloud. See [Installation](#).
- Configure the [IBM Aspera HTTP Gateway](#), then attach it to Aspera on Cloud. This transfer method does not require users to download and install the Aspera Connect client.

1. Create groups to accelerate user management

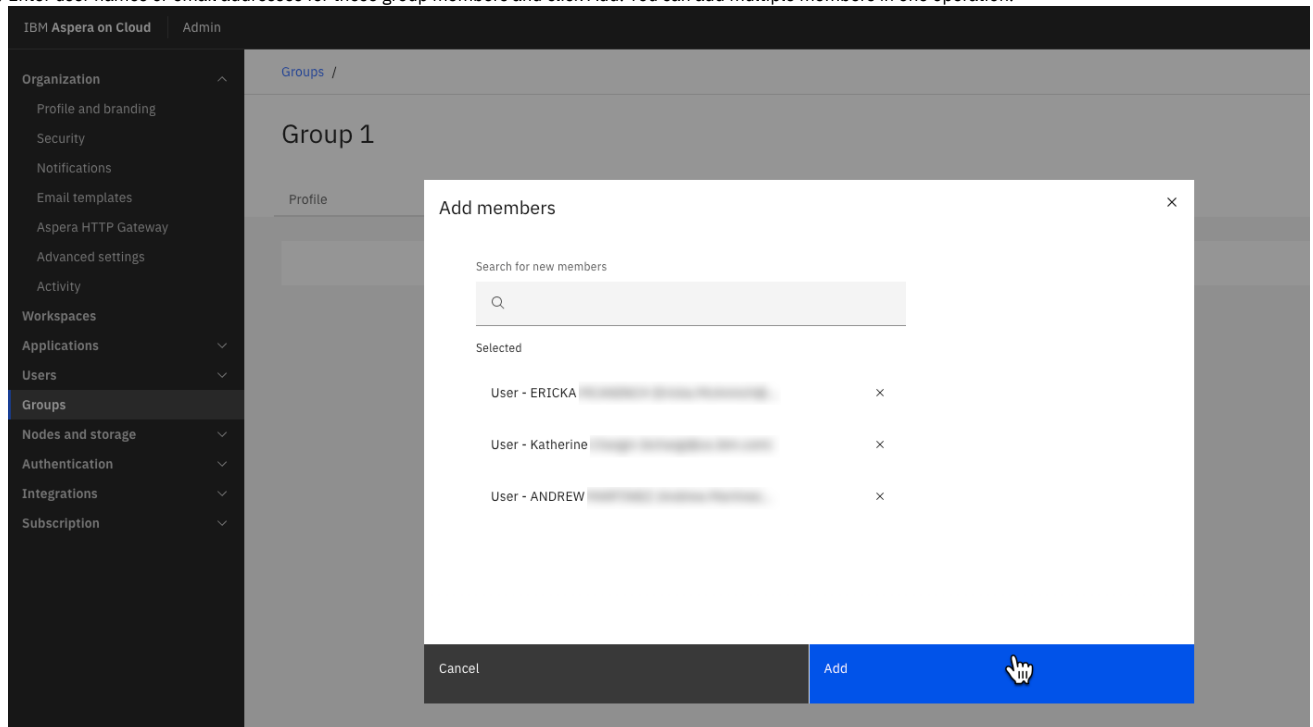
Use the AoC Admin app to create groups and add members to each group. You can add group members as follows:

- Add users who are already members of your AoC organization. You'll see their names or email addresses auto-filling in the *Add members* dialog.
- Add users who are not part of your AoC org. When you add new users to a group, you simultaneously add them as members of the organization.

1. Go to the Admin app by clicking the app switcher and selecting Admin.
2. Go to Groups > Create new.
3. Give the group a name; for example, Group 1.
4. Click Save.

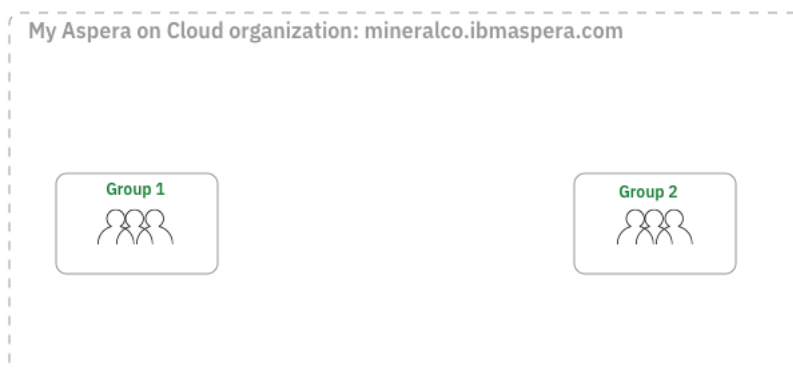
You have created the group; now add members to it.

5. Click Members > Add members.
6. Enter user names or email addresses for these group members and click Add. You can add multiple members in one operation.



7. Repeat this procedure for Group 2 (other internal users who collaborate with Group 1)

After you create the two groups, your Aspera on Cloud org looks like this:



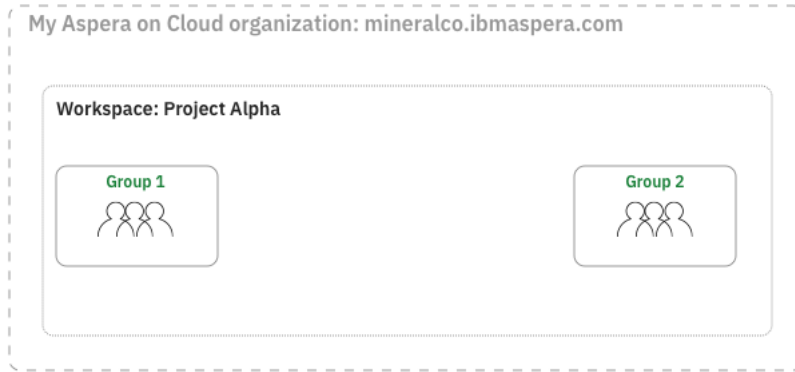
2. Configure the workspace for collaboration

Now set up the workspace and add your groups as members of the workspace.

Every AoC subscription is configured with one default [workspace](#). Aspera recommends that you rename and use your default workspace. (Depending on your [subscription](#), you may be able to create a new workspace).

1. Go to **Workspaces > Default workspace**.
2. Give this workspace a name that clearly indicates its purpose; for example, Project Alpha.
3. Click Save.
4. Click Members > Add member.
5. In the Search for new members field, enter the names of your user groups.
Note: Add yourself as a workspace member so you can verify correct workspace configuration. You can revoke your membership later if desired.
6. Click Add.

You now have a workspace with your groups as members.



2a. Disable the Packages app in your workspace (optional)

Both the Files and Packages apps are enabled by default. This workspace uses only the Files app, so disable the Packages app. You can re-enable it at any time.

Important: Before you perform this procedure, be sure that you have [retrieved the access key for your built-in node](#) and storage; the admin who created the AoC organization received the credentials in a digital package from Aspera Tech Support. You can re-enable the Packages app any time.

1. If necessary, open your new workspace: Workspaces > Project Alpha.
2. Click Applications > Packages.
3. Clear the checkbox labeled Use global app settings.
4. Clear the checkbox labeled Enable application.
5. Click Save.

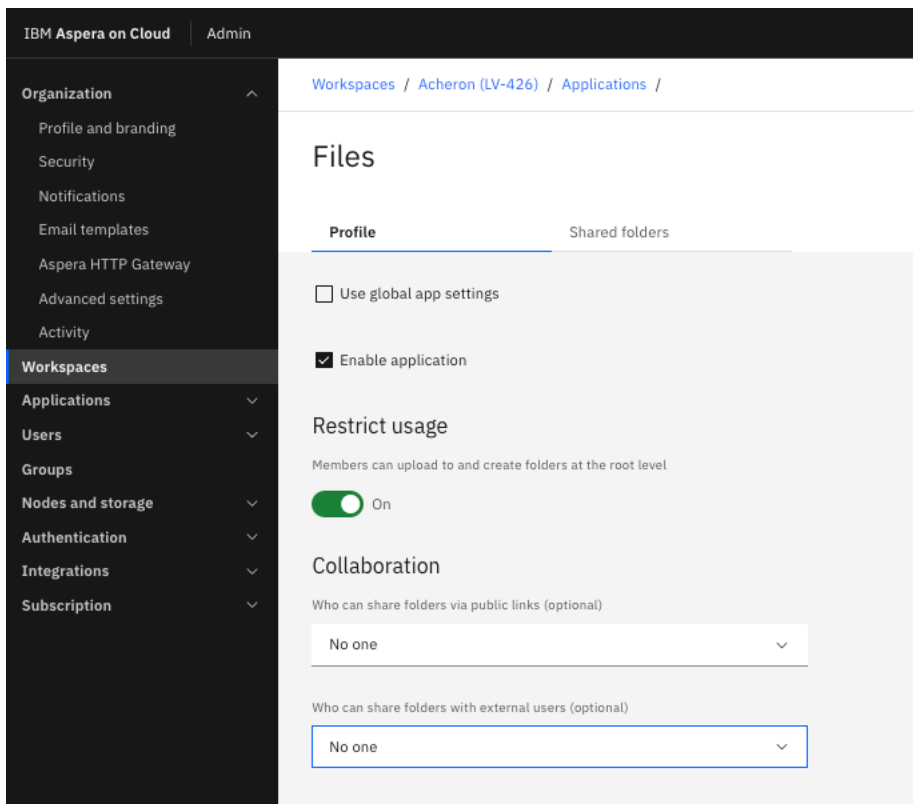
3. Configure the workspace Files app for secure collaboration (optional)

In this optional procedure, you'll configure the following specific collaboration capabilities for your workspace members. If you don't need these additional controls and security, skip this procedure.

- Allow workspace members to upload content *only* into the folders you designate. This configuration makes it easy for you to monitor storage usage and transfer volume.
- Restrict sharing to workspace members only. This means that workspace members can share with other members of the workspace only; they cannot share with anyone outside the workspace or outside the AoC organization.

Configure the Files app:

1. Go to Workspaces > Project Alpha > Applications > Files.
2. In Custom application settings, clear the checkbox labeled Use global app settings.
3. In Restrict usage, click the toggle labeled Members cannot upload to or create folders on their home folder to On.
The home folder is the root level of the Files app. By preventing uploads to this root level, you ensure that users upload content only into the folders you create on the built-in IBM Cloud storage and share with the workspace (see Procedure 4); these are folders you can readily monitor. For details, see [Managing storage usage](#).
4. In Collaboration, do the following:
 - a. Set Who can share folders via public links to No one.
This setting prevents members from sending a public link to share folders with people outside the workspace or organization.
 - b. Set Who can share folders with external users to No one.
This setting ensure that members can share only with each other.
5. Click Save.

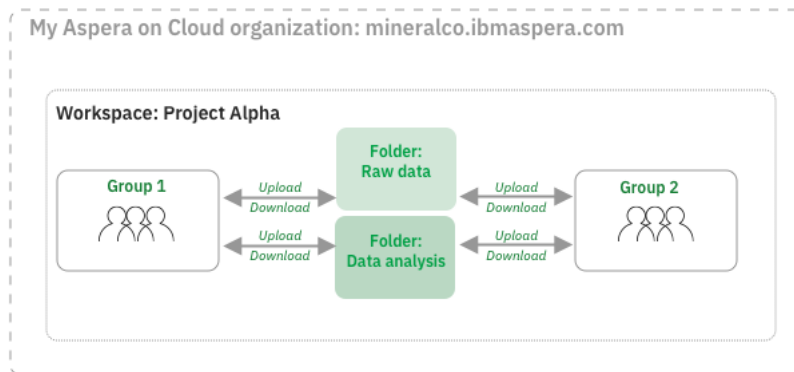


4. Create and share the collaboration folders with the groups

Now set up folders on your IBM Cloud storage and share them with your groups, giving them the spaces to collaborate in. You'll give access and the required permissions to each group. Then you can upload the desired content to the folders, or allow the users with "Upload" permission to populate the folder content.

You'll need the node secret for this procedure. To find the secret, see Important note in procedure 2a.

Recall that this is the configuration goal:



To create and share folders, do the following:

1. Go to Workspaces > *Project Alpha* > Applications > Files > Shared folders > Create new.
2. In the *Node access* dialog that opens, select the intended node, enter your node secret, and click Log in.
3. Create the first folder for your groups to collaborate in:
 - a. In the *Choose folder to share* dialog that opens, click Create folder.
 - b. Name the folder "Raw data", then click OK. The new folder appears in the list.
 - c. Click to select this new folder, then click Submit. This action makes the folder a shared folder.

Choose folder to share ×

Display name (optional)

Enter the name that members see. Leave blank to use the current folder name.

Root

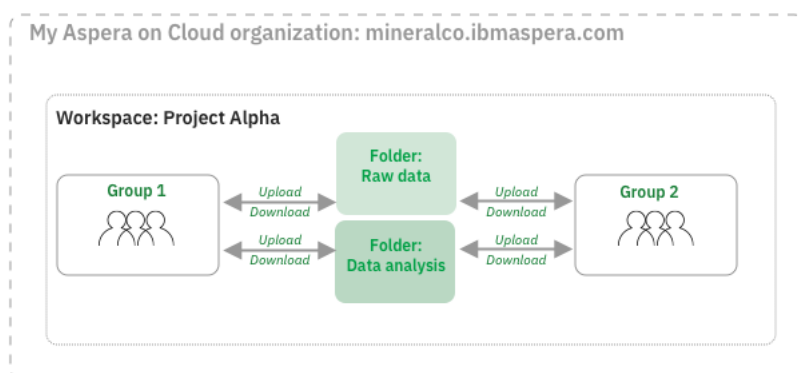
Create folder

	Name	Size	Last updated
☐		—	—
☒	Raw data	—	—
☐		4 MB	1/31/19 3:45 PM

Cancel
Submit

4. Share the folder "Raw data" with Group 1 and Group 2, giving both user groups Edit permission to this folder:
 - a. Click the folder row to open it, then click Add member.
 - b. In the field that displays Search for new members, enter Group 1 and Group 2.
The default permission setting is **Can edit**. This permission allows members full access to folder contents, including **Delete**. Click **Custom** to apply only specific permission.
 - c. Click Add.
5. Repeat the previous steps to create the folder "Data analysis", then add Group 1 and Group 2 as members with **Can edit** permission.

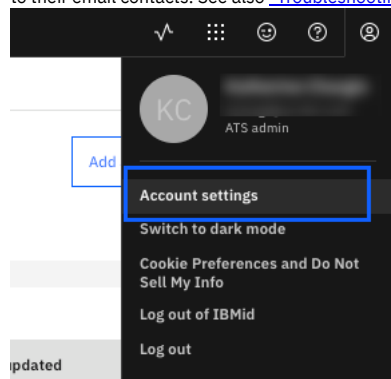
When you complete this procedure, your users can see the folders you created and can access folder content according to the permissions you assigned. Users must go to the workspace you set up in Procedure 2, and access the Files app in that workspace.



5. Configure notifications (optional)

By default, AoC sends email notifications to all users when they receive access to a shared folder. This means that the users in your groups receive an email with a link to access each folder you share.

Note: If users don't see the notifications, ask them to verify that they've enabled receipt of notifications in their Account settings page. They may also need to add Aspera to their email contacts. See also "[Troubleshooting Email Notifications](#)".



You can also allow your users to configure a notification when content is added to a folder they need to monitor.

1. Go to Workspaces > Project Alpha > Notifications.
2. Click the toggle labeled Use organization settings to Off.

3. Click the toggle labeled Allow users to turn on notifications for new shared folder content to On.
4. Click Save.

Your users can now set notifications for themselves when new content is added to the folders they need to monitor. For a user procedure, see .

Results

Your configuration work is done.

- Your groups are members of your org and the workspace Project Alpha. Each member receives four email notifications.
 - The first contains a link allowing them to join the organization by logging in and creating an account.
 - The second email contains a link to join the workspace. These are *standard* users in your org.
 - The third and fourth emails contain links to the two folders you shared with them.
- In the workspace, your groups see and can access the two folders you created in their Files app.

Access security and credentials

Set token duration, configure primary and sub-access keys to grant and control access to content, track and manage the credentials to your built-in IBM Cloud storage, and troubleshoot access issues.

- [Session and token duration](#)
You can configure settings for your organization that govern session duration and security token behaviors.
- [Access keys](#)
These procedures cover the creation of primary and sub-access keys that allow you to assign access to and delegate management of content in your organization workspaces, shared folders, and cloud storage. Also in this section, learn about "SSH bypass keys" that are delivered with Aspera Connect, the transfer client that powers transfers between user desktops and storage.
- [Access key to your built-in node](#)
Each Aspera on Cloud organization comes with built-in storage in IBM Cloud. Learn how to secure and track the credentials for this storage, and how to use these credentials to access the storage.
- [Access issues](#)
This section contains troubleshooting procedures for creating and tracking node access keys.

Session and token duration

You can configure settings for your organization that govern session duration and security token behaviors.

Parameters and definitions follow the procedure below.

Note: Administrator session duration parameters are not configurable.

Note: Numeric entries cannot begin with zero (0).

You can configure user session duration using the parameters in this section. Aspera on Cloud manages sessions using three types of tokens: a login token (also called an access token), a refresh token, and a transfer node token.

To configure settings for your organization, do the following:

1. Go to Organization > Security.
2. To enable a setting, select the checkbox; to disable a setting, clear the checkbox.
3. Enter the intended duration.
4. Click Save.

Access (login) token expiration

The login token expiration defines the maximum duration of an active session unless the refresh token duration (see previous parameter) is configured to extend the session. Unless refresh tokens are configured, users must re-authenticate when the login token expires.

- Default duration is 1 hour.
- Valid durations are 15 minutes to 24 hours.

Refresh token rotation

The refresh token defines the maximum duration that an active login session can be extended. This option is disabled by default for new organizations.

When a user logs in, Aspera on Cloud grants the user a login token (see the following parameter) and a refresh token. The refresh token provides an active user with subsequent login tokens, extending their active session for the duration you configure for this parameter.

- When enabled, the user session is extended, in increments equal to the login token duration, for the duration you configure for this parameter. For example, if the login token expiration is set to 1 hour and the refresh token expiration is set to 1 day, Aspera on Cloud issues new login tokens to an active user each hour for 24 hours. Then the session expires and the user must reauthenticate.
 - Recommended duration is 7 days.
 - Valid durations are 1 day to 365 days.

Inactive session logout

You can configure a maximum duration for inactive sessions. This option is disabled by default for new organizations.

- When enabled, an inactive session is automatically logged out after the duration you configure.
 - Recommended duration is 1 hour.
 - Valid durations are 15 minutes to 7 days.
- When disabled, user sessions are never logged out due to inactivity.

Transfer token expiration

The transfer node token expiration defines the maximum duration of authorized activity on the transfer node. This token, with the duration you configure here, is issued/reissued automatically when the login token is issued/reissued.

Note: You must set the transfer node token expiration duration longer than the login token expiration duration. Set the transfer node token duration to match your organization's longest transfer durations.

- Default duration is 12 hours.
- Valid durations are 1 hour to 14 days.

Access keys

These procedures cover the creation of primary and sub-access keys that allow you to assign access to and delegate management of content in your organization workspaces, shared folders, and cloud storage. Also in this section, learn about "SSH bypass keys" that are delivered with Aspera Connect, the transfer client that powers transfers between user desktops and storage.

- **Primary access keys and sub-access keys**
You must use a primary access key to share transfer access *outside* your AoC organization, such as with a vendor or other collaborator, or with a downstream on-prem application like Aspera Faspex, Shares, or Console. Use a sub-access key to share transfer access *inside* your AoC org, such as when delegating access and management tasks to a workspace manager.
- **Create a sub-access key to a workspace**
As an administrator with the primary access key, you can generate sub-access key/secret pairs to use as transfer and access credentials for a folder in your cloud storage.
- **Create a sub-access key to a shared folder**
As an administrator with the primary access key, you can generate sub-access key/secret pairs to use as transfer and access credentials for a folder in your cloud storage.
- **Create a sub-access key to a cloud storage folder**
As an administrator with the primary access key, you can generate sub-access key/secret pairs to use as transfer and access credentials for a folder in your cloud storage.
- **Tracking your node access credentials**
Logging in to a transfer server node with access credentials gives the user full access to the content there. AoC never stores the credentials, so it is imperative that you track and store them according to your site's established security practices.
- **FASP security: Aspera Connect transfer client authorized keys and aspsell**
Aspera Connect client uses "SSH bypass" keys. Those keys are delivered with the Aspera Connect client. They allow the client to start a FASP session without requiring a password, while security is implemented on protocol level with a security "token". The associated public keys are enhanced with OpenSSH specific stanza that forces the use of a compatible secure environment: aspsell and token authorization. This article explains how it works.

Primary access keys and sub-access keys

You must use a primary access key to share transfer access *outside* your AoC organization, such as with a vendor or other collaborator, or with a downstream on-prem application like Aspera Faspex, Shares, or Console. Use a sub-access key to share transfer access *inside* your AoC org, such as when delegating access and management tasks to a workspace manager.

Primary access keys

Use a primary access key to give a user or application *outside* Aspera on Cloud transfer credentials to access the content assets on that node.

An Aspera on Cloud *superadmin* (an administrator who knows the Aspera transfer user name and password) can create a primary access key in two ways:

- Using the Node API; see the `/access_keys` endpoint in the [IBM Aspera Node API](#) documentation on IBM API hub.
- Using the Aspera on Cloud application, when attaching a new transfer node to the AoC organization. The new node may be a [customer-managed Aspera HSTS node or cluster](#), or it may be an [ATS node that attaches the customer's cloud object storage](#).

Sub-access keys

Use a sub-access key to delegate certain administrative tasks and contextual content access to another AoC admin or to a workspace manager without having to distribute the primary access key. You can create a sub-access key only on a sub-directory of another access key.

Important: To maintain tenant privacy and content separation, do not use a sub-access key outside the context of the Aspera on Cloud organization. An Aspera on Cloud administrator can use the primary access key to create either of two sub-access key types, using the Aspera on Cloud application.

- A *client* sub-access key (also called a *workspace* access key) gives an admin or workspace manager contextual access and management rights within the *root folder* of a given workspace on the node.
- A *folder* sub-access key gives an admin or workspace manager access and management rights in a [folder in cloud storage](#) or in an [administratively shared folder](#). Note that a folder sub-access key is a different access credential than the sharing permissions set on a shared folder. *Access through a folder sub-access key is full access to folder contents*; such access is not restricted to the actions allowed through sharing permissions.

Create a sub-access key to a workspace

As an administrator with the primary access key, you can generate sub-access key/secret pairs to use as transfer and access credentials for a folder in your cloud storage.

Use sub-access keys to delegate certain administrative tasks and contextual content access to another AoC admin or to a workspace manager without having to distribute the primary access key.

Note that the sub-access keys you create using the procedure in this article are for use only within Aspera on Cloud. Be sure to use the proper key type to avoid security implications. For details see [Primary access keys and sub-access keys](#).

To complete this procedure, you need either the secret to the node hosting the shared folder or a valid custom access key and secret.

To create a sub-access key for a workspace, also sometimes called a client sub-access key, do the following:

1. Go to Nodes and storage > Nodes > *nodeName*.
2. Provide access credentials and log in, using either of the following methods:
 - Enter the secret for the node hosting this shared folder and click Log in.
 - Click Use custom access key, enter the custom access key and secret, and click Log in.AoC creates the new access key for the shared folder.
3. Click Workspaces.
4. On the row of the intended workspace, right-click and select Workspace keys.
5. Click Create new.
6. Give this key a name and provide notes to add a description, purpose, expected use, or other info that will be useful to those using this key.
This step is optional but highly recommended to make key management and use easier. If you add a name and notes, they'll be included in the file you download in a following step.
7. Save the access key by doing one of the following:
 - Click Download. AoC generates the file **KeySecretPair.txt**, containing the key and secret. Aspera recommends you rename the file to make it easier to track.
 - Click Copy for both key and secret.

Note: Note that Aspera on Cloud does not store the secret. Once you click OK in the following step, you can no longer retrieve the secret. Store the key and secret in a secure and accessible location according to local site security practices.
8. Click OK.
9. Name the key pair file and click Save.

Delete a workspace sub-access key

1. Go to Nodes and storage > Nodes > *nodeName*.
2. Provide access credentials and log in, using either of the following methods:
 - Enter the secret for the node hosting this workspace and click Log in.
 - Click Use custom access key, enter the custom access key and secret, and click Log in.AoC creates the new access key for the workspace.
3. Click Workspaces.
4. On the row of the intended workspace, right-click and select Workspace keys.
5. On the row of the intended key, right-click Delete, then confirm.

Create a sub-access key to a shared folder

As an administrator with the primary access key, you can generate sub-access key/secret pairs to use as transfer and access credentials for a folder in your cloud storage.

Use sub-access keys to delegate certain administrative tasks and contextual content access to another AoC admin or to a workspace manager without having to distribute the primary access key.

Note that the sub-access keys you create using the procedure in this article are for use only *within* Aspera on Cloud. Be sure to use the proper key type to avoid security implications. For details see [Primary access keys and sub-access keys](#).

Note also that a folder sub-access key is a different access credential than the sharing permissions set on a shared folder. *Access through a folder sub-access key is full access to folder contents*; such access is not restricted to the actions allowed through sharing permissions.

To complete this procedure, you need either the secret to the node hosting the shared folder or a valid custom access key and secret.

To create a sub-access key for a shared folder, do the following:

1. Go to Workspaces > *workspaceName* > Applications > Files > Shared folders.
2. On the row of the shared folder, right-click and select Client access keys > Create new.
3. Provide access credentials and log in using one of the following methods:
 - Enter the secret for the node hosting this shared folder and click Log in.
 - Click Use custom access key, enter the custom access key and secret, and click Log in.AoC creates the new sub-access key for the shared folder.
4. Give this key a name and provide notes to add a description, purpose, expected use, or other info that will be useful to those using this key.
This step is optional but highly recommended to make key management and use easier. If you add a name and notes, they'll be included in the file you download in a following step.
5. Save the sub-access key by doing one of the following:
 - Click Download. AoC generates the file **KeySecretPair.txt**, containing the key and secret. Aspera recommends you rename the file to make it easier to track, and save it to a secure and accessible location.

- Click Copy for both key and secret, saving them to a secure and accessible location.

Store the key and secret in a secure and accessible location according to local site security practices. Aspera on Cloud does not store the secret. Once you click OK in the following step, you can no longer retrieve the secret.

6. Click OK.
7. Name the key pair file and click Save.

To use this key to set up a connection to this folder in the Aspera GUI client, do the following:

1. Note the node URL.
2. Deliver the key pair file to the user of the GUI client according to your local site security practice.
3. In the Aspera GUI client, create a new connection, and enter data in the fields as follows:
 - Host: Enter the URL of the node hosting the shared folder.
 - User: Enter the access key.
 - Password: Enter the secret.

Refer to the [IBM Aspera High-Speed Transfer Server Admin Guide](#) for more information.

Delete a sub-access key to a shared folder

To delete an existing sub-access key to a shared folder, do the following:

1. Go to Workspaces > *workspaceName* > Applications > Files > Shared folders.
2. On the row of the shared folder, right-click and select Client access keys.
3. Right-click Delete, then confirm.

Create a sub-access key to a cloud storage folder

As an administrator with the primary access key, you can generate sub-access key/secret pairs to use as transfer and access credentials for a folder in your cloud storage.

Use sub-access keys to delegate certain administrative tasks and contextual content access to another AoC admin or to a workspace manager without having to distribute the primary access key.

Note that these credentials are a separate access method from the permission you set on a shared folder. The permissions you set on a shared folder do not restrict actions on folder content when using the access key.

Also note that the sub-access keys you create using the procedure in this article are for use only *within* Aspera on Cloud. Be sure to use the proper key type to avoid security implications. For details see [Primary access keys and sub-access keys](#).

1. Go to Nodes and storage > Nodes > *nodeName*
2. Provide access credentials and log in, using either of these methods:
 - Enter the secret for the node hosting this shared folder and click Log in.
 - If you have a custom access key, click Use custom access key, enter the custom access key and secret, and click Log in.

AoC creates the new access key for the shared folder.
3. Click Folder access keys > Create new.
4. Select the intended folder:
 - a. Click any folder to drill into it.
 - b. Click Create folder at any location to make a new folder; name the folder, choosing a name that will be descriptive enough for those who will need to access it. Click OK.
 - c. Use the gray bar near the folder list to navigate up and down the folder hierarchy.
 - d. Click to select the option button to the left of the folder row, then click Create.
5. Give this key a name and provide notes to add a description, purpose, expected use, or other info that will be useful to those using this key.
This step is optional but highly recommended to make key management and use easier. If you add a name and notes, they'll be included in the file you download in a following step. If you are creating multiple access keys to the same storage for different users or groups of users, make the name descriptive enough to tell them apart.
6. Save the access key by doing one of the following:
 - Click Download. AoC generates the file **KeySecretPair.txt**, containing the key and secret. Aspera recommends you rename the file to make it easier to track, and save it to a secure and accessible location.
 - Click Copy for both key and secret, saving them to a secure and accessible location.

Note: Aspera on Cloud does not store the secret. Once you click OK in the following step, you can no longer retrieve the secret. Store the key and secret in a secure and accessible location according to local site security practices.
7. Click OK.
8. Name the key pair file and click Save.
9. To use this key to set up a connection to this folder in the Aspera GUI client, note the node URL.
10. Deliver the key pair file to the user of the client according to your local site security practice.

Delete a folder sub-access key

To delete a sub-access key to a folder in cloud storage, do the following:

1. Go to Nodes and storage > Nodes > *nodeName*.
2. Provide access credentials and log in, using either of these methods:
 - Enter the secret for the node hosting this shared folder and click Log in.
 - If you have a custom access key, click Use custom access key, enter the custom access key and secret, and click Log in.

AoC creates the new access key for the shared folder.
3. Click Folder access keys.
4. Right-click the row of the intended folder and select Manage access keys.

5. Right-click Delete, then confirm deletion.

Tracking your node access credentials

Logging in to a transfer server node with access credentials gives the user full access to the content there. AoC never stores the credentials, so it is imperative that you track and store them according to your site's established security practices.

AoC access credentials take the form of access keys, each of which is composed of two parts:

- Key ID. For example, N26Y-pfC33hcsOw24keUlzSR
- Secret. For example, Yppsv_iXH5pyFBKe5cvA2nTiaXStd4NYpgjxWA0239_3

Built-in node access credentials

The credentials for the built-in node that is included with your initial AoC subscription are delivered in a digital package to the AoC admin who first created the AoC organization, as described in [Secure the access credentials for your built-in node](#).

Additional access credentials

Over the course of your AoC subscription, you may have reason to create several access keys. For example, you may want to:

- Give a workspace manager access only to specific content on the transfer server rather than all content.
- Give an API client access to specific folders on the transfer server.
- Attach your existing cloud storage to your AoC organization and allow AoC users to access content in it.
- Attach an Aspera server that you manage to your AoC organization and allow AoC users to access content in it.

For procedures, see [Access keys](#).

Recommended practices

Each time you create an access key, you have the option to name it and add descriptive notes. This step is optional but highly recommended to make key management and use easier. If you add a name and notes, they'll be included in the file you download in a following step.

You can add or edit a name and notes for your existing keys. To edit both name and notes, click the node row to open the key details. To edit notes only, right-click the key row and select Edit.

Each time you create an access key, AoC requires you to *download or copy* it to complete the creation process. When you download the key, AoC generates a text file that is always called `KeySecretPair.txt`.

IBM Aspera recommends that you rename this file with a meaningful label and save it to a secure and accessible location according to your local site security practices. Important: Once you close the window that displays your key and secret, you can no longer retrieve the secret. Be sure to save the key and secret in a secure and accessible location according to local site security practices. Aspera on Cloud does not store the secret.

Recovering a lost key

If however, you do not rename the file, you may have to search for the file by the default name. If you've created multiple access credentials without renaming them, you may need to rely on the timestamp to identify each file, doing your best to recall which credentials you created on which days and times. You can combine the timestamp information with the key ID that displays in the AoC interface when you right-click the row of the transfer server, shared folder, etc., and select View access key.

☐	Name	Storage provider	Hosted by
☐	files-prod-es-tor03.a...	Amazon S3	IBM Aspera
☐	Files Internal Dallas ...		IBM Aspera
☐	ATS AWS East		Other
☐	Japan ATS Demo	Amazon S3	Other
☐	https://ats-aws-us-e...	Other storage	Other

Simply cannot find your credentials?

If you cannot locate your credentials after a thorough search as described in this article, try the following, based on the type of node.

- For a transfer server that you manage, use your node user name and password to change the secret; see [Tether Your Aspera Transfer Server to Aspera on Cloud](#).
- For cloud storage that you have attached to your AoC organization, use the storage credentials to create a new access key; see [Attach your existing cloud storage](#).

FASP security: Aspera Connect transfer client authorized keys and aspsell

Aspera Connect client uses "SSH bypass" keys. Those keys are delivered with the Aspera Connect client. They allow the client to start a FASP session without requiring a password, while security is implemented on protocol level with a security "token". The associated public keys are enhanced with OpenSSH specific stanza that forces the use of a compatible secure environment: aspsell and token authorization. This article explains how it works.

Important: Depending on the version of Aspera client you are using, the client may only support DSA keys for SSH authentication, or include a DSA key in addition to the RSA key. DSA keys are deprecated and the transfer servers won't be supporting this type of keys in the future.

Keys on Aspera Connect client

Aspera Connect client comes with the following key (SSH bypass keys):

1. aspera_tokenauth_id_rsa

Item 1 is a RSA private key, protected by a passphrase.

When Aspera Connect client starts a transfer, it provides the key on `ascp` command line (-i), and the passphrase with the `ASPERA_SCP_PASS` env var.

Keys on Aspera High-Speed Transfer Server (HSTS)

HSTS includes an SSH private key in `<installdir>/var`:

- **aspera_tokenauth_id_rsa** (RSA,newer)

This key is used by asperanoded to start node-to-node transfers, and it is passphrase-protected.

The public key is provided in the following file:

- **aspera_tokenauth_id_rsa.pub**

The file uses the OpenSSH format for authorized_keys. This format can be consulted in the man page of [sshd\(8\)](#) in section "AUTHORIZED_KEYS FILE FORMAT".

When configuring a "transfer user" (that is, a user known by the SSH daemon on the server) for use with web applications (Faspex and others), the content of **aspera_tokenauth_id_rsa.pub** must be added to the transfer user's **authorized_keys** file (see the [IBM Aspera Connect User Guide](#)). This file contains:

```
command="/bin/aspsell -t",no-agent-forwarding,no-port-forwarding,no-X11-forwarding,no-pty ssh-dss AA<content cut>Ko= Aspera public
command="/bin/aspsell -t",no-agent-forwarding,no-port-forwarding,no-X11-forwarding,no-pty ssh-rsa AA<content cut>zQ= Aspera publi
```

Security considerations

Note that some additional options are added before the actual public key. Those keys (public and private) are "well known": private keys are directly delivered with the Aspera Connect client.

The security of the connection using SSH for FASP in web applications using those keys relies on three items:

- SSH shall allow transfers only, not execution of any other commands: This is enforced by setting the SHELL of the transfer user to `/bin/aspsell`.
- The transfer shall be allowed by an authentication token.
This is enforced by setting the parameters "authorization_transfer_in_value" and "authorization_transfer_out_value" to "token" in `aspera.conf`.
- It shall not be possible to "browse" using FASP (that is, using `ascmd`).
This is enforced by using aspsell in "loose" mode (see below, option "-r").

Moreover, the **sshd** daemon shall be configured to disallow some features, such as port forwarding at least for the transfer users.

On Linux, the administrator shall take care of setting the shell appropriately. On Windows, the `asconfigurator` command will set the shell to aspsell if the docroot of the user is not empty. In both cases, this can be checked in the "passwd" file.

The aspsell provides a loose mode (also known as a restricted mode); this is enforced by calling it with option "-r". For ease of configuration, aspsell can also be called with the name "aspsell-r" which is equivalent to calling with the -r option.

The aspsell is a shell that allows execution of only some commands. For instance, on Linux, those commands can be listed like this:

```
# strings /bin/aspsell|grep -E '^[^as[cy][^i][a-z0-9]* ( [^,]+)?$'
ascp -S. -V1
ascp4 -S.
async -q -S -s-
!ascmd
!ascmd -V2
ascp --no-mgmt-port-files -M %d -S. -V1 %ls
```

The lines starting with "!" are not allowed in loose mode. The first line allows legacy ascp transfers (server side). The second line allows ascp4 transfers. The third line allows the use of async. The ascmd lines are used by Desktop client GUI, Console, and Orchestrator to list files under the docroot (and other operations). The last line is the command used by async for file transfers.

Authentication token use is enforced by setting the transfer's users parameters in `aspera.conf` with commands like (see the manuals):

```
asconfigurator -x "set_user_data;user_name,faspex;authorization_transfer_in_value,token;authorization_transfer_out_value,token"
```

If those configurations are not properly made, then the server is at risk of either getting malicious SSH connections in a standard shell (bash), or having files browsable and downloadable without using the web applications authorization.

Enforcement directly in authorized_keys

It was noted that the lines added to the transfer user's authorized_keys files for OpenSSH begin with:

```
command="/bin/aspshell -t",no-agent-forwarding,no-port-forwarding,no-X11-forwarding,no-pty
```

This actually enforces most of the items listed previously: Instead of executing the command provided in the SSH connection (normally "**ascp -S -v1**", but a malicious user may try to execute another command), OpenSSH will execute "**/bin/aspshell -t**" and place the actual command in an envvar (SSH_ORIGINAL_COMMAND). The "-t" option will do the following:

- Enforce the "loose mode" (restricted mode, no ascmd)
- Set an envvar: ASPERA_AUTH_TOKEN=TOKEN
- Validate that the command in SSH_ORIGINAL_COMMAND is allowed (**ascp**, same as regular aspshe11 invocation)

When **ascp** is invoked, if the envvar ASPERA_AUTH_TOKEN is set to TOKEN, it will override the values of the parameters **authorization_transfer_in_value** and **authorization_transfer_out_value** to "token" (even if those values were set to "allow" in *aspera.conf*).

So, even if the basic security configuration was overlooked by the administrator (aspshe11-r and token auth), those parameters in the authorized_keys file will effectively enforce the security.

Note that this is specific to OpenSSH, and care shall be taken with other SSH servers (bitwise and others)

Access key to your built-in node

Each Aspera on Cloud organization comes with built-in storage in IBM Cloud. Learn how to secure and track the credentials for this storage, and how to use these credentials to access the storage.

- [Secure the access credentials for your built-in node](#)

Each Aspera on Cloud subscription includes one built-in, Aspera-managed transfer server (ATS) node with storage in IBM Cloud Object Storage. The access credentials (or access key) for this transfer server are automatically delivered to the administrator who first created the AoC organization. Find these credentials in a digital package from Tech Support in the Packages app. It's very important to track and store these credentials securely so that you can access and manage content on this node.

- [Identify your built-in node](#)

In Aspera on Cloud, transfer server are called nodes. Since you can attach multiple transfer server nodes and cloud storage to your organization, your list of nodes may have multiple entries. Use the procedure in this article to identify the built-in node that comes with your subscription.

- [Access your built-in node](#)

The transfer server included in your subscription is hosted by IBM Aspera. Use this built-in transfer server to store your user workspaces, including the content they upload and share using the Files app and the packages they send and receive using the Packages app. As admin, you can also upload content directly to this transfer server and then make that content available to your users.

Secure the access credentials for your built-in node

Each Aspera on Cloud subscription includes one built-in, Aspera-managed transfer server (ATS) node with storage in IBM Cloud Object Storage. The access credentials (or access key) for this transfer server are automatically delivered to the administrator who first created the AoC organization. Find these credentials in a digital package from Tech Support in the Packages app. It's very important to track and store these credentials securely so that you can access and manage content on this node.

To retrieve the credentials for your built-in, Aspera-managed node, do the following:

Attention: You must be the administrator who first configured the Aspera on Cloud organization.

1. Go to the Packages app. If necessary, click the app switcher  and select Packages.
2. In the left-side gray panel, click My inbox.
3. In the packages list, click the row of the package from IBM Aspera Tech Support called "Access key information". This package contains a text file listing the key and secret.
4. Review the message included with the package.
5. Right-click the text file and select Download to...
6. In the Finder or Explorer window that opens, select the location for this download.
7. Click Open or Done.
8. Aspera highly recommends you rename the file to make it easier to track. Track and protect the text file with the key and secret according to your local site security practices. Note that IBM Aspera does not keep a copy of the access key secret.

Note: Selecting Download to... affects *only this download*. To change your *default* download location, open Aspera Connect from your system tray or launcher; go to Preferences > Transfers. In the Downloads location field, enter the default location for your downloads.

Identify your built-in node

In Aspera on Cloud, transfer server are called nodes. Since you can attach multiple transfer server nodes and cloud storage to your organization, your list of nodes may have multiple entries. Use the procedure in this article to identify the built-in node that comes with your subscription.

1. Go to **Nodes and storage > Nodes**.
2. Check the **Hosted by** column for a node that is hosted by IBM Aspera. Of nodes hosted by Aspera, the initial node typically has a URL that contains `asperafiles.com`.

3. For further validation, match the key ID in [the file you downloaded](#) to the key ID of the node in the node listing. To find the key ID for a node, right-click the node row and select **View access key**.

Access your built-in node

The transfer server included in your subscription is hosted by IBM Aspera. Use this built-in transfer server to store your user workspaces, including the content they upload and share using the Files app and the packages they send and receive using the Packages app. As admin, you can also upload content directly to this transfer server and then make that content available to your users.

Access this transfer server in **Nodes and storage > Nodes**.

Note: You can access this built-in node only through Aspera Node API and Aspera FASP protocol, using any of the following:

- Aspera on Cloud web UI and [Aspera Connect](#) client
- Aspera [Node API](#) and [Transfer SDK](#)

Use an access key

Transfer server or node access credentials take the form of an access key. An access key is composed of two parts:

- Key ID. For example, N26Y-pfC33hcsOw24keUlzSR
- Secret. For example, Yppsv_iXH5pyFBKe5cvA2nTiaXStd4NYpgjxWA0239_3

Use the access key as follows:

- To [browse, add, remove](#), and share files and folders on this node.
- To apply [network policies](#) and [configuration policies](#) to this node.
- To create and manage [folder-level access keys and client access keys](#).
- To manage files and folders in your users' Files and Packages apps for workspaces that are hosted on this node.

Access issues

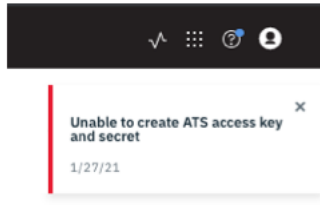
This section contains troubleshooting procedures for creating and tracking node access keys.

- [Trouble creating a new access key](#)
To create a new node and attach storage to your Aspera on Cloud organization, you must create a new access key. Review this procedure if you encounter errors.
- [Can't find the access credentials to your built-in node](#)
Each Aspera on Cloud subscription includes one built-in, Aspera-managed transfer server node with storage in IBM Cloud Object Storage. The access credentials (or access key) for this transfer server are delivered to the administrator who first created the AoC organization in a digital package from Tech Support in the Packages app. It's very important to track and store these credentials securely.
- [Tracking your node access credentials](#)
Logging in to a transfer server node with access credentials gives the user full access to the content there. AoC never stores the credentials, so it is imperative that you track and store them according to your site's established security practices.

Trouble creating a new access key

To create a new node and attach storage to your Aspera on Cloud organization, you must create a new access key. Review this procedure if you encounter errors.

If Aspera on Cloud displays the error message "Unable to create ATS access key and secret", verify that the data you entered into each configuration field is accurate. Often this error indicates no more than a typo when entering your storage configuration settings.



This article highlights the fields to verify for each supported storage type.

For all node types, go to Nodes > Create new > Attach my cloud storage.

IBM Cloud

Verify content in the highlighted fields. Ensure there are no typos and that cloud configuration settings are copied accurately.

IBM Aspera on Cloud

Admin

Access key

Storage

IBM COS

Region

Choose an option

Access key ID

Access key secret

Bucket

Path

AWS (Amazon Web Services)

Verify content in the highlighted fields. Ensure there are no typos and that cloud configuration settings are copied accurately.

IBM Aspera on Cloud

Admin

Storage

Amazon S3

Region

us-east-1

Storage class

Standard

Amazon S3 Server-Side Encryption (optional)

None

Select the Amazon S3 encryption-at-rest method. Note: Nodes with server-side encryption enabled do not support watermarking.

Trust relationship policy

```
{
  "Version": "2012-10-17",
  "Statement": [
```

IAM role ARN

arn:aws:iam:123:role/mine

Session name (optional)

Bucket

Path

Microsoft Azure Blob

Verify content in the highlighted fields. Ensure there are no typos and that cloud configuration settings are copied accurately.

IBM Aspera on Cloud

Admin

Storage

Microsoft Azure Blob

Region

eastus

API type

Block

Storage credentials

Key

Storage account

Key

Container

Path

Microsoft Azure Files

Verify content in the highlighted fields. Ensure there are no typos and that cloud configuration settings are copied accurately.

IBM Aspera on Cloud

Admin

Storage

Microsoft Azure Files

Region

eastus

API type

Block

Storage account

Password

Path

GCS (Google Cloud Service)

Verify content in the highlighted fields. Ensure there are no typos and that cloud configuration settings are copied accurately.

The screenshot shows the 'Admin' section of the 'IBM Aspera on Cloud' interface. The 'Storage' section is active, showing a dropdown menu for 'Google Cloud'. Below this, a blue rectangular box highlights several configuration fields: 'Region' (dropdown menu showing 'us-west1'), 'Authentication' (dropdown menu showing 'Private key'), 'Project ID' (text input field), 'Client email' (text input field showing 'client_id@gserviceaccount.com'), 'Private key ID' (text input field), 'Private key' (text input field), and 'Path' (text input field).

Can't find the access credentials to your built-in node

Each Aspera on Cloud subscription includes one built-in, Aspera-managed transfer server node with storage in IBM Cloud Object Storage. The access credentials (or access key) for this transfer server are delivered to the administrator who first created the AoC organization in a digital package from Tech Support in the Packages app. It's very important to track and store these credentials securely.

To retrieve the credentials for your built-in, Aspera-managed node, do the following:

Attention: You must be the administrator who first configured the Aspera on Cloud organization.

1. Go to the Packages app. If necessary, click the app switcher  and select Packages.
2. In the left-side gray panel, click My inbox.
3. In the packages list, click the row of the package from IBM Aspera Tech Support called "Access key information". This package contains a text file listing the key and secret.
4. Review the message included with the package.
5. Right-click the text file and select Download to...
6. In the Finder or Explorer window that opens, select the location for this download.
7. Click Open or Done.
8. Aspera highly recommends you rename the file to make it easier to track. Track and protect the text file with the key and secret according to your local site security practices. Note that IBM Aspera does not keep a copy of the access key secret.

Note: Selecting Download to... affects *only this download*. To change your *default* download location, open Aspera Connect from your system tray or launcher; go to Preferences > Transfers. In the Downloads location field, enter the default location for your downloads.

Tracking your node access credentials

Logging in to a transfer server node with access credentials gives the user full access to the content there. AoC never stores the credentials, so it is imperative that you track and store them according to your site's established security practices.

AoC access credentials take the form of access keys, each of which is composed of two parts:

- Key ID. For example, N26Y-pfC33hcsOw24keUlzSR
- Secret. For example, Yppsv_iXH5pyFBKe5cvA2nTiAXStd4NYpgjxWA0239_3

Built-in node access credentials

The credentials for the built-in node that is included with your initial AoC subscription are delivered in a digital package to the AoC admin who first created the AoC organization, as described in [Secure the access credentials for your built-in node](#).

Additional access credentials

Over the course of your AoC subscription, you may have reason to create several access keys. For example, you may want to:

- Give a workspace manager access only to specific content on the transfer server rather than all content.
- Give an API client access to specific folders on the transfer server.
- Attach your existing cloud storage to your AoC organization and allow AoC users to access content in it.
- Attach an Aspera server that you manage to your AoC organization and allow AoC users to access content in it.

For procedures, see [Access keys](#).

Recommended practices

Each time you create an access key, you have the option to name it and add descriptive notes. This step is optional but highly recommended to make key management and use easier. If you add a name and notes, they'll be included in the file you download in a following step.

You can add or edit a name and notes for your existing keys. To edit both name and notes, click the node row to open the key details. To edit notes only, right-click the key row and select Edit.

Each time you create an access key, AoC requires you to *download or copy* it to complete the creation process. When you download the key, AoC generates a text file that is always called `KeySecretPair.txt`.

IBM Aspera recommends that you rename this file with a meaningful label and save it to a secure and accessible location according to your local site security practices. Important: Once you close the window that displays your key and secret, you can no longer retrieve the secret. Be sure to save the key and secret in a secure and accessible location according to local site security practices. Aspera on Cloud does not store the secret.

Recovering a lost key

If however, you do not rename the file, you may have to search for the file by the default name. If you've created multiple access credentials without renaming them, you may need to rely on the timestamp to identify each file, doing your best to recall which credentials you created on which days and times. You can combine the timestamp information with the key ID that displays in the AoC interface when you right-click the row of the transfer server, shared folder, etc., and select View access key.

The screenshot shows the IBM Aspera on Cloud Admin interface. On the left is a navigation menu with options: Organization, Workspaces, Applications, Users, Groups, Nodes and storage (expanded), Nodes (selected), Network policies, Configuration policies, Settings, Authentication, Integrations, and Subscription. The main area is titled 'Nodes' and contains a table with columns: Name, Storage provider, and Hosted by. The table lists several nodes, including 'files-prod-es-tor03.a...', 'Files Internal Dallas ...', 'ATS AWS East', 'Japan ATS Demo', and 'https://ats-aws-us-e...'. A context menu is open for the 'Files Internal Dallas ...' node, showing options: View access key (highlighted with a red box), Update status, and Delete.

☐	Name	Storage provider	Hosted by
☐	files-prod-es-tor03.a...	Amazon S3	IBM Aspera
☐	Files Internal Dallas ...		IBM Aspera
☐	ATS AWS East		Other
☐	Japan ATS Demo	Amazon S3	Other
☐	https://ats-aws-us-e...	Other storage	Other

Simply cannot find your credentials?

If you cannot locate your credentials after a thorough search as described in this article, try the following, based on the type of node.

- For a transfer server that you manage, use your node user name and password to change the secret; see [Tether Your Aspera Transfer Server to Aspera on Cloud](#).
- For cloud storage that you have attached to your AoC organization, use the storage credentials to create a new access key; see [Attach your existing cloud storage](#).

Content security

This section includes an overview of the numerous content security configuration options in Aspera on Cloud. Other articles describe how to configure both server-side and client-side encryption, including a detailed procedure for bringing your own key (BYOK) by integrating your IBM Key Protect KMS. Another detailed procedure describes how to configure watermarking by integrating your Irdeto watermarking service.

- [Session and token duration](#)
You can configure settings for your organization that govern session duration and security token behaviors.
- [Content security overview](#)
In addition to secure access controls, protecting content directly ensures that digital assets retain their value even as Aspera on Cloud users collaborate to develop, exchange, and deliver content. This article collects several Aspera on Cloud content security settings and strategies, and provides links to configuration procedures.
- [Encryption](#)
All Aspera transfers are encrypted in flight. You can also configure encryption at rest. Learn about key rotation for Azure storage. Get detailed guidance on both client-side and server-side encryption, including how to bring your own key (BYOK), integrating your IBM Key Protect KMS.
- [Permissions](#)
This section describes the options for configuring content sending permission in the Packages app and content sharing permission in the Files app. Another article discusses strategies for configuring the appropriate level of collaboration at the global, workspace, and shared-inbox levels.
- [Watermarking: Integrate your Irdeto service](#)
Forensic watermarking is an anti-piracy solution to prevent and trace illegal content redistribution and security breaches. This article describes how to integrate your Irdeto watermarking service with Aspera on Cloud. After integration, Packages app users can apply watermarking when sending digital packages.
- [Antivirus scanning](#)
This document outlines the steps to create a new antivirus configuration.

Session and token duration

You can configure settings for your organization that govern session duration and security token behaviors.

Parameters and definitions follow the procedure below.

Note: Administrator session duration parameters are not configurable.

Note: Numeric entries cannot begin with zero (0).

You can configure user session duration using the parameters in this section. Aspera on Cloud manages sessions using three types of tokens: a login token (also called an access token), a refresh token, and a transfer node token.

To configure settings for your organization, do the following:

1. Go to Organization > Security.
2. To enable a setting, select the checkbox; to disable a setting, clear the checkbox.
3. Enter the intended duration.
4. Click Save.

Access (login) token expiration

The login token expiration defines the maximum duration of an active session unless the refresh token duration (see previous parameter) is configured to extend the session. Unless refresh tokens are configured, users must re-authenticate when the login token expires.

- Default duration is 1 hour.
- Valid durations are 15 minutes to 24 hours.

Refresh token rotation

The refresh token defines the maximum duration that an active login session can be extended. This option is disabled by default for new organizations.

When a user logs in, Aspera on Cloud grants the user a login token (see the following parameter) and a refresh token. The refresh token provides an active user with subsequent login tokens, extending their active session for the duration you configure for this parameter.

- When enabled, the user session is extended, in increments equal to the login token duration, for the duration you configure for this parameter. For example, if the login token expiration is set to 1 hour and the refresh token expiration is set to 1 day, Aspera on Cloud issues new login tokens to an active user each hour for 24 hours. Then the session expires and the user must reauthenticate.
 - Recommended duration is 7 days.
 - Valid durations are 1 day to 365 days.

Inactive session logout

You can configure a maximum duration for inactive sessions. This option is disabled by default for new organizations.

- When enabled, an inactive session is automatically logged out after the duration you configure.
 - Recommended duration is 1 hour.
 - Valid durations are 15 minutes to 7 days.
- When disabled, user sessions are never logged out due to inactivity.

Transfer token expiration

The transfer node token expiration defines the maximum duration of authorized activity on the transfer node. This token, with the duration you configure here, is issued/reissued automatically when the login token is issued/reissued.

Note: You must set the transfer node token expiration duration longer than the login token expiration duration. Set the transfer node token duration to match your organization's longest transfer durations.

- Default duration is 12 hours.
- Valid durations are 1 hour to 14 days.

Content security overview

In addition to secure access controls, protecting content directly ensures that digital assets retain their value even as Aspera on Cloud users collaborate to develop, exchange, and deliver content. This article collects several Aspera on Cloud content security settings and strategies, and provides links to configuration procedures.

Aspera security considerations

If your business security requirements include restrictions for uploads and transfers by file extension type, you must use the Aspera Node API on each transfer server to configure exclusion rules.

Content encryption in Aspera on Cloud

- [Content encryption at rest and in flight](#)
- [Require encryption at rest](#)

Server-side encryption

- [Use Aspera-managed keys for server-side encryption at rest](#)
- [Bring your own key for server-side encryption at rest](#)

Security in multi-tenant organizations

In a multi-tenant or reseller organization, you must ensure strict separation between workspaces to protect tenant privacy.

By default, the auto-complete function in Aspera on Cloud shows workspace managers all users and groups in the entire organization, along with the personal contacts of all users. Instead, you can configure your org such that workspace managers can see only users and groups from the workspaces in which they are members, along with their own personal contacts in any workspace and with outside users.

For details, see [Assign the workspace manager role](#).

Files app content security

Admin controls

By default, collaboration in the Files app is unrestricted. But as an admin, you can apply increasingly restrictive controls to sharing actions available to Files app members.

Global: Admin > Applications > Files

Workspace: Admin > Workspaces > *workspaceName* > Applications > Files

- Prevent app users from sharing with unauthenticated recipients; restrict the use of [public links](#): Who can share folders via public links
- [Prevent](#) app users from sharing with non-workspace members: Who can share folders with external users
- Allow sharing with [designated non-workspace members only](#); list specific external users as the only valid recipients: Who are eligible external users
- Prevent accidental sharing with the entire workspace: Who can share folders with the entire workspace
- [Require](#) external users to create an AoC account and log in to receive a package

User controls

As an admin, you can establish workflows that guide your workspace members how to use these additional content security measures:

- Apply [content permissions](#) to shared content
- Require a password to access content shared using a [public link](#)
- [Unshare](#) a folder

Packages app content security

Admin controls

Global: Admin > Applications > Packages

Workspace: Admin > Workspaces > *workspaceName* > Applications > Packages

- Prevent app users from requesting packages from non-workspace members: Who can send submission links
- Prevent app users from sending packages to non-workspace members: Who can send packages to external users
- Require non-workspace recipients to create an account and log in to receive a package: Require external users to log in when receiving packages
- Prevent accidental sending to the entire workspace: Who can send packages to the entire workspace
- Require encryption at rest for all send packages: Automatically apply encryption at rest to all packages

Global: Integrations > Watermarking

- If you [integrate your Irdeto forensic watermarking service with Aspera on Cloud](#), you can *allow* or *require* workspace members of the Packages app to apply a watermark to all packages they send.

User controls

As an admin, you can establish workflows that guide your workspace members how to use these additional content security measures:

- Require package recipients to apply a password
- Apply watermarking when sending a package

Content security caveats

Members of the Automation and Activity apps are not limited to acting on, monitoring, or reporting on content in workspaces where they are members. No matter their workspace membership:

- Automation app members can configure and manage automated workflows on any workspace in your org.
- Activity app members can monitor and report on content in all workspaces in your org.

For these reasons, Automation and Activity app members are typically org admins.

Public links

Public link expiration

Global: Admin > Applications > Packages/Files

Workspace: Admin > Workspaces > *workspaceName* > Applications > Packages/Files

Select the check box next to the Links expire after (days) option in the Public and authenticated links section, and set the desired value for the link expiration.

- The administrator can set a default expiration for all public links.
- An individual user can reduce the expiration set by the administrator, but cannot extend it.

Public link password

Global: Admin > Applications > Packages/Files

Workspace: Admin > Workspaces > *workspaceName* > Applications > Packages/Files

Select the check box next to the Make password required for new links option in the Public and authenticated links section.

- The administrator can enforce the password requirement when creating the public links.
- Passwords won't be set by default, users must set the password when creating a new public link.

Disallow encryption-at-rest during package send operations

Global: Admin > Applications > Packages

Workspace: Admin > Workspaces > *workspaceName* > Applications > Packages

Select the option Disabled from the drop-down list in the Client-side encryption at rest section.

- Administrators can disable the application of client-side encryption-at-rest to packages in all workspaces or in specific workspaces.
- Senders can't apply EAR to individual packages.

Encryption

All Aspera transfers are encrypted in flight. You can also configure encryption at rest. Learn about key rotation for Azure storage. Get detailed guidance on both client-side and server-side encryption, including how to bring your own key (BYOK), integrating your IBM Key Protect KMS.

- **Content encryption: In flight and at rest**
Aspera on Cloud offers two forms of encryption for contents of digital packages. Encryption in flight protects contents in transit. Encryption at rest maintains protection at the remote destination until the recipient applies the proper passphrase.
- **Require encryption at rest**
You can configure an organization-level setting requiring that all packages sent in the organization automatically have encryption at rest (EAR) applied. Sending with EAR applied ensures that package contents remain encrypted at the receiving end, even after the recipient downloads the files and folders in the packages.
- **Rotate keys for your Azure storage**
To support key rotation for Azure storage, you can update your attached Azure node with new storage credentials.
- **Use Aspera-managed keys for server-side encryption at rest**
You can apply Aspera two-tier AES encryption to secure your data in storage attached to your AoC organization. This article describes the AoC-native key-management capability and how to apply it to secure your data.
- **Bring your own key for server-side encryption at rest**
You can bring your own key to protect your data in storage attached to your AoC organization. This article describes how to bring your own key by integrating your key-management service (KMS) with AoC.

Content encryption: In flight and at rest

Aspera on Cloud offers two forms of encryption for contents of digital packages. Encryption in flight protects contents in transit. Encryption at rest maintains protection at the remote destination until the recipient applies the proper passphrase.

The Aspera on Cloud Packages app automatically applies in-flight encryption to every package sent by every user of the app; this in-flight encryption protects content 'over the wire' during the transfer.

Users can apply an additional 'at-rest' security measure that applies encryption to the package at the destination. Even after download on the receiving end, the package remains encrypted until the recipient applies the password associated with the package.

There are two ways to apply password protection to a package:

- The sender can apply password protection at the time of sending. The sender creates a password for the package in the Send Files form, then delivers the password to the recipients according to local site security practice. For a procedure, see [Sending Files and Folders](#).
- The administrator can require that all sent packages have password protection automatically applied. Again, the sender must create and confirm the password to apply to the package, and deliver the password to recipients according to local site security practice. See [Require encryption at rest](#).

Encryption in Flight

Every time you transfer content using any Aspera web app, the underlying FASP protocol uses the Cipher Feedback with Checksum mechanism to ensure the security and integrity of data in flight.

Each packet sent in a session is encrypted independently. Transport encryption uses two symmetric 128-bit AES session keys, randomly generated at session initiation. Dual-key encryption and decryption allows packet-by-packet verification at the remote end, and non-conforming packets are discarded.

Encryption at Rest (Password Protection)

When you choose to apply encryption at rest (password protection), you are applying an additional layer of security. A 128-bit AES key used for each session is generated at random, and then is itself encrypted and stored along with the encrypted file.

At the remote end, the session key is extracted by decrypting with a secure hash of the password, which you apply to the package when you send it. Security depends on the length and complexity of the password you apply; for most uses, five normal words in unfamiliar order is sufficient.

The recipient must apply the same password to decrypt the package content. Until that password is applied, the content is secure and inaccessible.

Require encryption at rest

You can configure an organization-level setting requiring that all packages sent in the organization automatically have encryption at rest (EAR) applied. Sending with EAR applied ensures that package contents remain encrypted at the receiving end, even after the recipient downloads the files and folders in the packages.

Senders must enter and confirm a passphrase for every package they send with EAR applied, then must deliver the passphrase to the recipient according to local site security practices. The recipient must apply that passphrase to decrypt the downloaded package.

Every workspace inherits the organization setting, but the administrator can override the inherited setting and either apply or remove EAR for packages sent in the workspace.

When you require EAR at the workspace, senders cannot send a package without EAR. However, even if you do not require EAR at the workspace, senders have the option to apply EAR to individual packages. In the Send files panel of the Packages user view, EAR is called 'Password protection'.

1. To configure the global Packages app, go to Applications > Packages > Security.
2. Check or clear the box labeled Automatically apply encryption at rest to all packages.
3. Click Save.

The setting you choose here is inherited by all workspaces in the organization. To override this inherited setting for a given workspace, go to the next step.

4. To configure the Packages app setting for a given workspace, do the following:
 - a. Go to Workspaces > *workspaceName* > Applications > Packages > Profile.
 - b. Clear the checkbox labeled Use global app settings.
 - c. Select or clear the checkbox labeled Automatically apply encryption at rest to all packages.
5. Click Save.

Note: This setting is not available for an individual shared inbox. All shared inboxes in the workspace inherit the workspace configuration.

Rotate keys for your Azure storage

To support key rotation for Azure storage, you can update your attached Azure node with new storage credentials.

To complete this procedure, you need the following:

- From your Azure storage, the new storage credentials applicable after key rotation.
- The Aspera node name and Aspera secret for your Azure storage attached to Aspera on Cloud.

To update your Azure storage credentials, do the following:

1. In your Azure storage management portal, update the credentials for the storage attached to Aspera on Cloud. Capture the new credentials to apply in Aspera on Cloud.
2. In Aspera on Cloud, go to **Nodes and storage > Nodes**; click the row of your Azure node. Enter the Aspera node key and secret.
3. Click **Update storage credentials**.
4. In the modal that appears, enter the new credentials from your Azure storage.

5. Click **Save**.

Result: You have updated the storage credentials for your Azure node in your Aspera on Cloud organization. The Aspera on Cloud node access key and secret remain unchanged.

Use Aspera-managed keys for server-side encryption at rest

You can apply Aspera two-tier AES encryption to secure your data in storage attached to your AoC organization. This article describes the AoC-native key-management capability and how to apply it to secure your data.

When you apply Aspera's server-side encryption at rest (SSEAR), you can choose either of two key-management strategies. You can use Aspera's native key-management function, or you can [integrate a key-management service](#) to manage your own encryption key. In both cases, Aspera protects your data using a two-tier, AES-based encryption hierarchy.

Using Aspera-managed keys

This is an overview of the encryption process when you choose to use Aspera-managed keys.

- You create a secret passphrase (also called the content protection secret).
- Aspera uses a randomly-generated data encryption key (DEK) to encrypt your data using the AES algorithm.
- Aspera combines your passphrase with other unique data and uses the AES algorithm to encrypt the DEK.
- Aspera saves the encrypted DEK in a metadata file, along with the encrypted customer data, in the customer's cloud storage.
- After encryption, Aspera securely discards the unencrypted DEK. Unencrypted keys are never stored in AoC, on the node, or in the storage.
- To decrypt, Aspera uses unique data combined with metadata from the metadata file to decrypt the DEK, then uses the DEK to decrypt customer data.

Important: It is your responsibility to manage your secret passphrase. You may need it to access your content in storage directly, rather than through Aspera on Cloud.

Implementation notes

- Supported cloud platforms:
 - [IBM Cloud](#)
 - [AWS S3](#)
 - [Google Cloud Services](#)
 - Microsoft Azure [Blob](#) or [Files](#)
- Supported Aspera [node types](#):
 - Customer-managed tethered nodes
 - Aspera-managed auto-scale clusters (ATS)
- You must store and manage the secret passphrase (step 6 in the following procedure) according to your local site security practices. You may need it to access your data outside AoC.
- You can apply Aspera SSEAR in addition to or instead of encryption options offered by your cloud provider.
- You can enable encryption only on nodes that are not configured for watermarking. This applies to both Aspera SSEAR and cloud-provider encryption. See [this article](#) for details.

Procedure

Use this procedure for each node to encrypt.

Note: To complete this procedure on an existing node, you need the access key secret for the node.

To apply Aspera SSEAR to an existing node using Aspera-managed keys, do the following:

1. Go to Admin > Nodes and storage > Nodes.
2. Select the intended node by clicking the node row.
3. Enter the access key secret and click Log in.
4. In the Details tab, go to Aspera encryption at rest.
5. In the Key management method field, select Use Aspera-managed keys.
6. In the next field, enter your secret passphrase.
Note: Save this passphrase according to your local site security practices.
7. Click **Save**.

Your data on this node is protected using Aspera's two-tier encryption hierarchy and Aspera-managed keys.

Note: Once you apply encryption at rest, you cannot remove or change it.

Note: Encryption applies only to new data that you upload after you apply encryption. Data that exists on the node before you encrypt remains unencrypted.

Bring your own key for server-side encryption at rest

You can bring your own key to protect your data in storage attached to your AoC organization. This article describes how to bring your own key by integrating your key-management service (KMS) with AoC.

When you apply Aspera's server-side encryption at rest (SSEAR), you can choose either of two key-management strategies. You can use [Aspera's native key-management](#) function, or you can manage your own key by integrating a key-management service with AoC. In both cases, Aspera protects your data using a two-tier, AES-based encryption hierarchy.

When you bring your own key, it remains under your independent management the entire time. You use your KMS to protect and control your key, perform key rotation, key deletion, all other key-management functions. Your own key is never accessible to Aspera.

To bring your own key, you integrate your KMS with AoC by creating a KMS profile in AoC. Then you associate the profile with a node attached to your AoC organization.

Envelope encryption

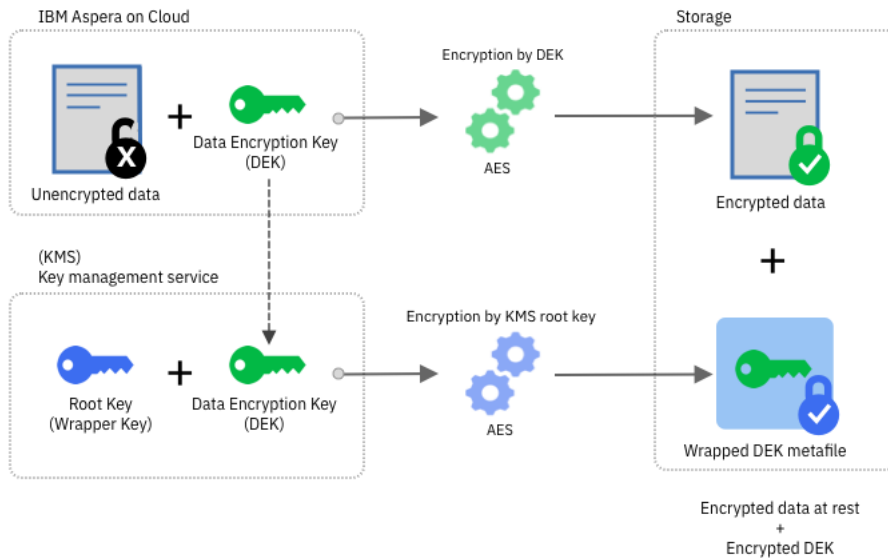
Aspera SSEAR uses *envelope encryption* to protect your content. Envelope encryption is the practice of encrypting data with a *data encryption key*, and then encrypting the data encryption key with a highly secure *key-wrapping key*.

The key you bring is key-wrapping key, also called the root key. The root key is independently managed by you using your KMS. The root key is never available to or under the control of Aspera.

When you apply envelope encryption using your own key, Aspera stores your encrypted data and the encrypted DEK in your cloud storage. Aspera never stores unencrypted DEKs and never has access to your root key in your KMS.

This double-encryption model combines the strengths of the AES algorithm with the inherent separation of key-management roles required for high-quality security.

Envelope encryption

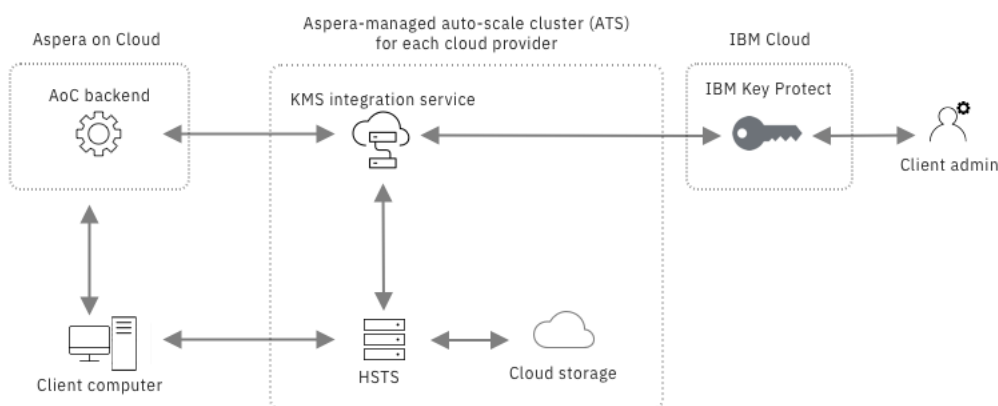


Using Your KMS with Aspera on Cloud

You can integrate your IBM Key Protect key-management service with Aspera on Cloud so that you can "bring your own key" for envelope encryption.

The following drawing is a schematic representation of the AoC/KMS integration architecture integration with IBM Key Protect.

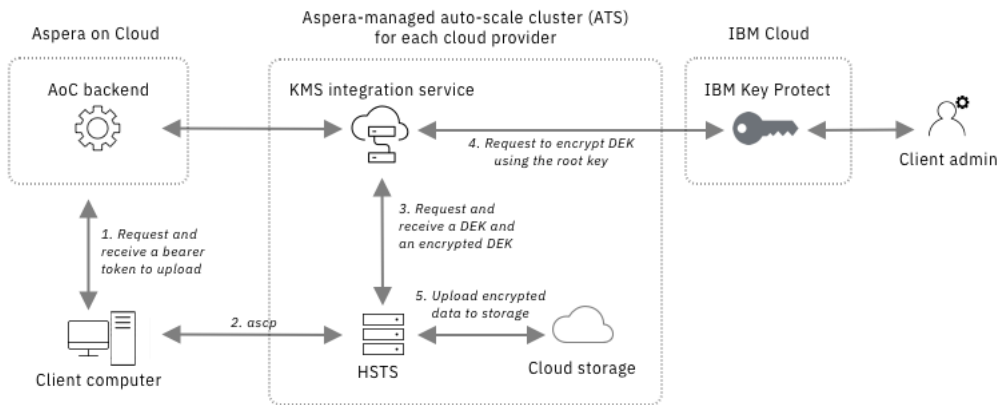
Architecture



The new Aspera KMS integration service interacts with both the AoC backend and the HST server in the Aspera-managed auto-scale cluster (ATS). It also interacts with your IBM Key Protect account using your IBM IAM with a service ID API key in the IBM Cloud. The following drawings show the upload and download workflows, illustrating the specific interactions among all these elements.

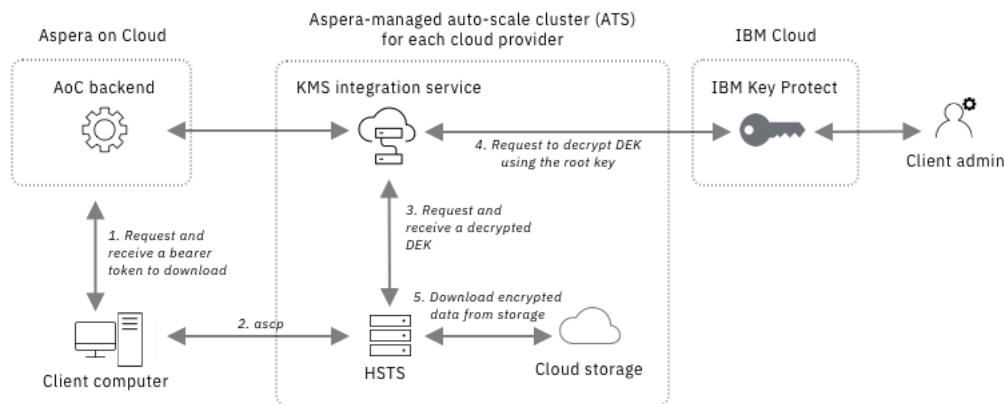
This drawing shows the end-to-end upload workflow.

Upload workflow



The download workflow reverses the process, as shown in the next diagram.

Download workflow



Implementation notes

- Supported KMS: [IBM Key Protect](#).
- Support for KMS key rotation.
- Supported storage types:
 - [IBM Cloud](#)
 - [AWS S3](#)
 - [Microsoft Azure](#)
 - [Google Cloud Storage](#)
- Supported Aspera node type: Aspera-managed auto-scale clusters (ATS).
- You can apply Aspera SSEAR in addition to or instead of encryption options offered by your cloud provider.
- You can enable encryption only on nodes that are not configured for watermarking. This applies to both Aspera SSEAR and cloud-provider encryption. See [this article](#) for details.

Prerequisites

- IBM Key Protect instance. Set the "Allowed network policy" to public-and-private (this is the default setting).
- IBM IAM authentication using Service ID API Key.

KMS provider specifications

To complete this task, you need the following information from your IBM Key Protect account.

Value	Definition	Example
KMS endpoint	The Key Protect service endpoint. The API endpoint to use when you connect to the Key Protect API.	<code>https://us-east.kms.cloud.ibm.com</code>
Key Protect Instance ID	The unique identifier assigned to your Key Protect service instance.	<code>ra385699-3d6f-47d4-8239-56b7890e5f73</code>
Root key ID	The unique identifier for the root key to use for encrypting and decrypting (wrapping and unwrapping) the DEK.	<code>41aed334-923f-4b6d-8d67-13e1f6c019b3</code>
API key	The key that AoC submits to Key Protect to be authenticated and be granted access. Aspera recommends that you use <i>Service ID API keys</i> . Aspera also supports <i>User API keys</i> .	<code>8uEy9TUDVtUHUGXpsMlpTb4rp8B_ZEfjU28ujik_nyw</code>

Procedures

To encrypt content using the root key in your KMS you must create at least one AoC KMS profile. Then you must associate the profile with a node attached to your organization. You can associate a profile with an existing attached node as long as you have not previously applied Aspera encryption-at-rest to it. You can also associate a profile with a new node during node creation.

KMS profile configuration notes

- Give each profile a unique name.
- You can associate any given profile with multiple nodes. Any given node can have only one KMS profile associated with it.
- You can update an existing profile by changing the profile name and API key, but you cannot update other profile settings.
- To protect your access to existing encrypted data, you cannot delete a KMS profile if you have associated it with any nodes. You must first [delete the associated nodes](#). Then you can delete the profile. Right-click a profile row and select Delete.

To complete this procedure on an existing attached node, you need the access key secret. You can also create a new access key. See

1. Create a KMS profile.
 - a. Go to Admin > Integrations > Third-party > Key-management services.
 - b. Click Create new to open the Key-management service profile page.
 - c. Give this profile a unique name.
 - d. Select your KMS provider.
 - e. Enter the required data into the form, according to the specifications of your KMS provider.
 - f. Click Save.
2. Apply the KMS profile to the node to encrypt.
 - a. Go to Admin > Nodes and storage > Nodes.
 - b. Select the intended node by clicking the node row.
 - c. Enter the access key secret and click Log in.
 - d. In the Details tab, go to Aspera encryption at rest.
 - e. In the Key-management method field, select Use my Key-management service.
 - f. In the following field, select the KMS profile to apply.
 - g. Click Save.

Once you complete these procedures successfully, all data you upload to this node will be protected using envelope encryption.

Note: Once you apply encryption at rest, you cannot remove or change it.

Note: Encryption applies only to new data that you upload after you apply encryption. Data that exists on the node before you encrypt remains unencrypted.

Permissions

This section describes the options for configuring content sending permission in the Packages app and content sharing permission in the Files app. Another article discusses strategies for configuring the appropriate level of collaboration at the global, workspace, and shared-inbox levels.

- [Sharing Permissions](#)
This article describes the various permissions in the AoC Files app. Using the Files app, workspace members *share* folders with others. The member who shares grants specific permissions to the person they share with. These permissions govern how the person shared with can act upon the content in the folder.
- [Sending Permissions](#)
This article describes the various permissions in the AoC Packages app. Using the Packages app, workspace members *send* files and folders to others. *Sending* in the Packages app is similar to sending an email with attachments.
- [Collaboration: Open or closed?](#)
Default collaboration settings tend to be open. Administrators can make collaboration options increasingly strict as required.

Sharing Permissions

This article describes the various permissions in the AoC Files app. Using the Files app, workspace members *share* folders with others. The member who shares grants specific permissions to the person they share with. These permissions govern how the person shared with can act upon the content in the folder.

Note:

Your ability to share folders in your workspace depends upon:

- The settings configured for your workspace and organization.
- The permissions granted to you for a specific folder.

For a change in permissions or settings, contact your Aspera on Cloud administrator or the person who shared the content with you.

Sharing Permissions

See also "Content Permissions" below and the topics available in [Sharing folders](#).

When you share a folder, you grant your recipient one or more specific permissions to it (for a list, see "Content Permissions" below). The permissions you can grant to your recipient for that shared folder depend on the permissions you have to the folder: you can grant the same permissions you have, or fewer; but you cannot grant permissions you do not have.

For example, if you have Browse, Preview, and Download permissions to a folder, you can grant all three of those permissions, or any two, or any one of those permissions, but you cannot grant Upload files or Delete permission.

- You can always share any folder in your Files app with fellow workspace members, including groups that are workspace members. To share this way, right-click the folder row and select Share.

- If enabled for members of your workspace, you can also share any folder in your Files app with AoC users outside your workspace and with people who do not have an AoC account at all.

Only you change the permission level for people you shared with (unless you are an admin that used the [admin sharing procedure](#)).

For details and strategies, see [Sharing folders](#). To share as an administrator, see [Share a node folder with a workspace](#).

Revoking Shared Permissions ("Unsharing" Content)

This applies to users of the Files app.

Only you can revoke shared access for the people you shared with.

Note: When an administrator uses the [admin procedure](#) to share a folder from attached storage to one or more workspace members, any admin can change access and permissions.

Changing Content Permissions

Only you change the permission level for people you shared with. You can grant any or all of the permissions that you have to the folder, but you cannot grant permissions that you do not have.

Note: When an administrator uses the [admin procedure to share a folder](#) from attached storage to one or more workspace members, any admin can change access and permissions.

Uploading Content in the Files app

- You can upload content to any folder to which you have Edit or Upload Files permission.
- You automatically have Edit permission to content you have placed (either by uploading or by moving from a package) into the Files application.
- By default you can upload to the **Home folder** area of your Files app. However, the admin can restrict that ability.

For more information on uploading, see [Upload files and folders to the Files app](#).

Content Permissions

You have a specific permission or access level for each file or folder in your Files app. Check your permission to a given folder by right-clicking and selecting Info.

There are four preset or composite permissions and seven custom permissions for content in your Files app:

- Preset or Composite permissions:
 - **Edit** (also called *Can Edit*)

This is the highest level of permission and gives a user full control over the item; it contains all other permissions.
 - **View** (also called *Download Only*)

Includes *Browse*, *Download*, and *Preview* permissions.
 - **Upload**

Includes *Create/Upload folders* and *Upload files*
 - **Preview**

Includes *Browse* and *Preview*
- Custom permissions (content must reside on a transfer server with node software at version 3.7.4 or higher; see the "Package Information" section of the IBM Aspera High-Speed Transfer Service [Release Notes](#) for specific build numbers for your platform):
 - **Create/Upload folders**

Create or upload an empty folder; to upload folders containing files, enable this permission along with *Upload files*.
 - **Rename**

Rename files and folders.
 - **Upload files**

Upload files and folders; to upload folders containing files, enable this permission along with *Create/Upload folders* permission -- or use *Upload* composite permission. See *Delete* below for uploading a file with the same name as an existing file (overwrite or replace). You need *Upload* permission to a folder to move or copy content to it.
 - **Download**

Download the folder or file in the folder.
 - **Preview**

Preview movie files in the folder. Thumbnail previews of supported image tiles are always available.
 - **Browse**

Browse folder content; if this setting is not enabled, you can see the folder but cannot view folder contents.

- **Delete**

Delete or overwrite folder contents.

Internal and other permissions

An administrator or workspace manager may see a shared item identified as having an "Internal" or "Other" permission. This identification can indicate a number of different scenarios, as follows:

- **Internal permission: workspace folder**
This permission was created by the system to display and track shared folders in Aspera on Cloud.
- **Internal permission: application**
This permission was created by the system for internal purposes.
- **Other permission: node or other app**
This permission was created by an admin on an attached node, by an API user, or by a user of another app like Aspera Drive. Use caution and investigate carefully before deleting these permissions.

Sending Permissions

This article describes the various permissions in the AoC Packages app. Using the Packages app, workspace members *send* files and folders to others. *Sending* in the Packages app is similar to sending an email with attachments.

Sending Permissions

Sending is different than sharing in that you do not set permission on content you send. Your recipient has full access to content you send.

You can always send to fellow workspace users or groups.

If enabled for members of your workspace, you can send to Aspera on Cloud users in outside your workspace and to people who do not have an Aspera on Cloud account. When you send files and folders to such individuals, you have two options:

- You can simply send the package. Aspera on Cloud delivers an email notification that enables the recipient to open an Aspera on Cloud portal that provides access to the package you send.
- You can invite the recipient to become a member of the workspace as you send. Aspera on Cloud delivers an email notification containing a link that enables the user to log in to the workspace to receive the package you sent. The content you sent is available to them in their Packages app inbox, along with any content they are entitled to as a workspace member. That person is now a full member of the workspace, with normal workspace privileges.

If enabled by your administrator, you can send content to a [shared inbox](#).

For more information, see the topic in [Packages app: Send and receive files and folders](#).

Inviting Other Users to Send Content

If enabled by your administrator, you can send a [submission link](#), which generates an email message inviting your recipient to send you content. You can invite the recipient to send to you in either of two ways:

- To yourself as an individual Aspera on Cloud user.
See [Request a package to My inbox](#).
- To a [shared inbox](#) for which you have 'Add users' permission.
See [Request a package to a shared inbox](#).

Shared Inbox Permissions

Shared inboxes are a feature of the Packages app.

You may have one or more of the following permissions to any given [shared inbox](#):

- **Send:** You can send packages to that shared inbox. Simply click the To field of the Send files form to see a list of shared inboxes to which you have Send permission. If you are not a member of the workspace that hosts the shared inbox, you send to the shared inbox using the AoC submission portal. Access the portal by clicking the link in the email notification the you receive from and AoC user inviting you to send files.
- **Receive:** You can receive packages sent to that shared inbox. You see the shared inbox in the left panel of the Packages app in your workspace. Click the inbox name to see the packages listing. If you have Receive permission only, you cannot send a package (upload files and folders) to this shared inbox.
- **Add users:** You can add members to the shared inbox. When you enter the shared inbox by clicking it in the left panel, you see the **Add** button in the right panel.
 - You can invite people (workspace members, Aspera on Cloud users who are not workspace members, people who do not have an Aspera on Cloud account) to submit content to shared inbox. Refer also to [submission link](#)
 - You can add users to the shared inbox, granting them the appropriate permissions to it. Adding users to a shared inbox does not make them a member of the associated workspace. If these users do not already have membership in a workspace, they are considered limited users, and are listed as such in the organization user listing.

Collaboration: Open or closed?

Default collaboration settings tend to be open. Administrators can make collaboration options increasingly strict as required.

Administrators can configure a number of settings that govern users' ability to collaborate with others. These settings include which users can collaborate outside the workspace, with whom, who can invite new users to the app or to a shared inbox, and other settings.

Administrators can configure collaboration settings at the global level for the Files and Packages apps independently. Global app settings are inherited at the workspace level; inherited settings can be overridden and customized for each app in each workspace. Therefore, collaboration permissions can vary from workspace to workspace and from app to app, allowing admins to customize Aspera on Cloud for maximum usability and content security.

In the Files application

Workspace members with access to the Files application can share folders freely with other members of the same workspace. This is a fundamental privilege of workspace membership and cannot be curtailed.

By default, all workspace members can also share with people outside the workspace. However, administrators or workspace managers can control which user types, if any, can share folders outside the workspace, and how.

There are two options for sharing outside the workspace: authenticated and unauthenticated; you can control these capabilities independently.

To configure the Files app globally, go to Applications > Files.

To customize the settings inherited from global app configuration for a given workspace, go to Workspaces > *workspaceName* > Applications > Files.

For details, see [Files App: Using a shared file repository](#).

Authenticated sharing outside the workspace

In the AoC UI, this is the setting labeled Who can share folders with external users.

The workspace member shares a folder with someone outside the workspace, either with an AoC member of a different workspace, or with a person who is not an AoC member at all. In both cases, the recipient of the share receives an email notification containing a link that allows them to access the shared folder.

- The AoC user in another workspace gets access to this shared folder through a limited workspace experience. They do not gain access to any content in the workspace except the folder specifically shared with them.
- For a person outside AoC entirely, the link in the email leads to an account creation flow; the recipient then logs in to access the shared folder through an AoC portal. This user does not have access to other content in the workspace or to any other functions of the app; only to folders that have been specifically shared with them. This means that folders you as administrator have shared with the entire workspace remain hidden and inaccessible to these users.
- You can control which user types in this workspace have authenticated sharing capability:
 - All members of the workspace (default).
 - Workspace managers only.
 - No one; you can disable this capability for all workspace members.
- If you enable sharing outside the workspace, you can list specific external users with whom those enabled users can share; configure this at the workspace level (Workspaces > *intended workspace* > Profile > Collaboration > Who are eligible external users).

Unauthenticated sharing outside the workspace

Unauthenticated sharing uses a public link. In the AoC UI, this is the setting labeled Who can share folder via public links.

- This recipient does not create an account or log in to AoC. They access the shared folder through an AoC portal.
- A public link is truly public: the public link recipient can forward the link to another user, who can then use the link to access the shared folder.
- You can control which user types in this workspace have unauthenticated sharing capability:
 - All members of the workspace (default).
 - Workspace managers only.
 - No one; you can disable this capability for all workspace members.
- If you enable sharing outside the workspace, you can designate specific external users that are valid recipients; workspace members can share only with those designated outside users. Configure this at the workspace level (Workspaces > *intended workspace* > Profile > Collaboration > Who are eligible external users).

In the Packages application

Workspace members with access to the Packages application can send packages freely to other members of the same workspace. This is a fundamental privilege of workspace membership and cannot be curtailed.

By default, all workspace members can also send packages to people outside the workspace. However, administrators or workspace managers can control which user types, if any, can send and request packages outside the workspace.

By default, workspace members can also request packages from others in the workspace or from outside users by sending a submission link; however, the administrator can restrict or disable the package request function.

To configure the Packages app globally, go to Applications > Packages.

To customize the settings inherited from global app configuration for a given workspace, go to Workspaces > *workspaceName* > Applications > Packages.

For details, see [Packages app: Send and receive files and folders](#).

Sending outside the workspace, with or without requiring recipients to log in

In the AoC UI, this is the setting labeled Who can send packages to external users.

The workspace member can send a package to someone outside the workspace, either to an AoC member of a different workspace, or with a person who is not an AoC member at all. In both cases, the package recipient receives an email notification containing a link that allows them to access the package.

- The AoC user in another workspace accesses the package in a limited workspace experience. They do not gain access to other workspace content.
- For a person outside AoC entirely, the link in the email opens an AoC portal that provides access to the package. This recipient does not have access to other content in the workspace or to any other functions of the application, only to packages that have been sent to them specifically. This means that packages sent to the entire workspace are not available to this recipient.

- By default, the outside recipient does not need to create an AoC account and log in. However, you can require that; select the check box labeled Require external users to log in when receiving packages. When you require external users to log in, the link in the email notification leads the user through an account creation flow; the recipient then logs in to access the shared package through an AoC portal. This recipient does not gain access to any other content in the workspace or functions of the Packages application.
- You can control which user types in the workspace have outside sending capability:
 - All members of the workspace (default).
 - Workspace managers only.
 - No one; you can disable outside package sending entirely.
- If you enable sending outside the workspace, you can list eligible recipients to whom those enabled users can send; configure this at the workspace level: go to Workspaces > *workspace_name* > Collaboration > Who are eligible external users.

Requesting packages to My inbox

Note: The request packages permission described in this section applies only to requests to send to an individual user (send to My inbox) as opposed to sending to a shared inbox. See the following section for details on shared inbox requests.

In the AoC UI, this is the setting labeled Who can request packages by sharing submission links.

Workspace members request packages by sending a [submission link](#). AoC sends an email notification that contains the submission link, which enables the recipient to open an AoC portal; the portal allows the recipient to create a digital package and send it to the My inbox of the AoC user who sent the submission link.

You can control which user types in the workspace can request packages from others:

- All members of the workspace.
- Workspace managers only.
- No one; you can disable package requests entirely for all users of this workspace.

Unlike many of the other collaboration settings, when this setting is enabled for either members or managers, those enabled users can request packages from anyone, inside or outside the workspace, or outside AoC entirely.

Requesting packages to a shared inbox

Members of a workspace [shared inbox](#) who have *Add users* permission can send a [submission link](#) to anyone inside or outside AoC. AoC sends an email notification that contains the submission link, which enables the recipient to open an AoC portal; the portal allows the recipient to create a digital package and send it to the shared inbox from which the submission link was sent. The package is then available to all members of the shared inbox who have Receive permission to that inbox.

The user with *Add users* permission can send a submission link to another member of the shared inbox, or to someone who is not a member of the shared inbox.

In the workspace

By default, when you enable collaboration with outside users in either or both the Files and Packages applications for workspace members, those enabled users can collaborate with any user outside the workspace or outside AoC. But you can restrict collaboration to specific users or groups if required.

Go to Workspaces > *workspace_name* > Applications > Files/Packages > Collaboration > Who are eligible external users. You can configure the following, for the Packages app and for the Files app independently:

- Any email address (default).
- Any email plus the following groups.
- Only the following emails and groups.

Watermarking: Integrate your Irdeto service

Forensic watermarking is an anti-piracy solution to prevent and trace illegal content redistribution and security breaches. This article describes how to integrate your Irdeto watermarking service with Aspera on Cloud. After integration, Packages app users can apply watermarking when sending digital packages.

It's important that you work with your Irdeto representative to set up proper access between your Irdeto service and your AoC nodes. Aspera cannot validate that you have configured your Irdeto service correctly.

Once that access is properly configured, use the Aspera on Cloud Admin app to configure watermarking for your organization and for the specific workspaces in which you want watermarked packages. The Admin app UI flow accomplishes these actions:

1. Create a watermarking profile.
 - Name the profile that maps your Irdeto service to AoC.
2. Associate the watermarking profile with a [node](#) attached to your organization.
 - You can attach any watermarking profile to one or more nodes. (A node is your cloud storage bucket that you've attached to your AoC org.)
3. Enable watermarking for the AoC Packages application in each workspace where you want watermarking available.
 - Once enabled, you can make watermarking required for every package sent from that workspace, or you can allow workspace members to choose whether to apply watermarking to individual packages they send.
 - For the Packages app user procedure showing how senders can apply watermarking, see [Sending: Detailed procedure](#). For a more in-depth treatment, see the relevant section in [Sending: Become an expert](#).

For step-by-step instructions, see "Configure watermarking in Aspera on Cloud" later in this article.

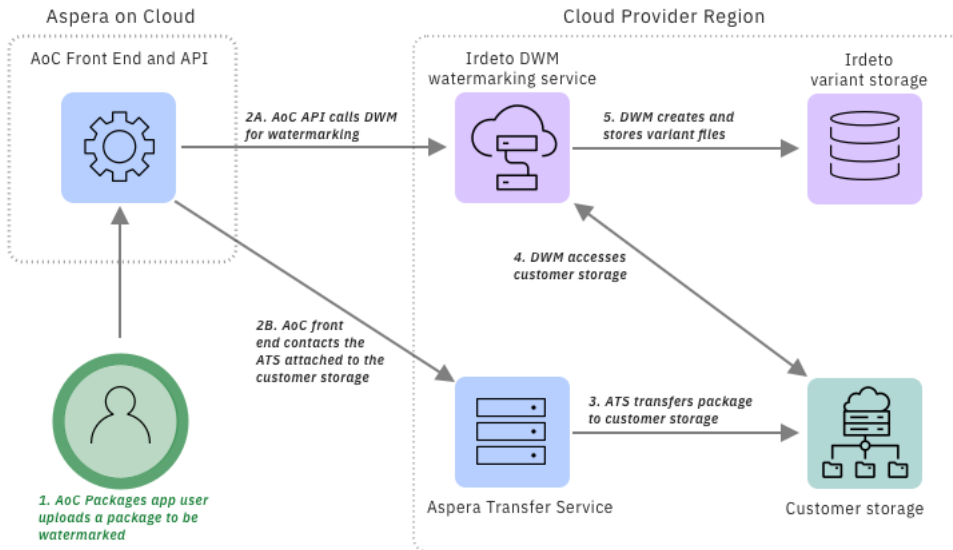
Watermarking with Irdeto in Aspera on Cloud

Watermarking combats piracy by applying an invisible yet traceable 'signature' on digital files. The watermark allows you to track that asset through the development and distribution process.

Each time an AoC user downloads a watermarked file, Irdeto updates the watermark to indicate the specific user who downloaded it. If a user who downloads a watermarked file then forwards the file using some mechanism other than AoC, the file retains the watermark identifying the user who downloaded it.

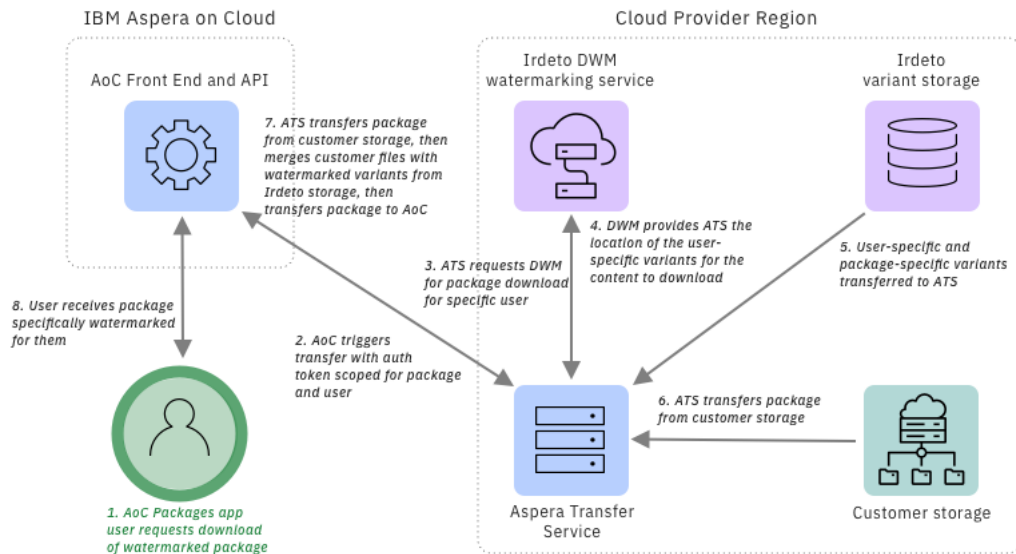
The following drawing is a schematic representation of the package upload workflow for your integration of Irdeto with AoC.

Upload a package for watermarking



The following drawing is a schematic representation of the package download workflow for your integration of Irdeto with AoC.

Download a watermarked package



Prerequisites

Work with your Irdeto representative to establish the following:

- The DWM (distributed watermarking) service API endpoint address(es) that are local to your cloud storage location(s).
- The tenant ID for your organization.
- Read-only access permissions from Irdeto to your storage.

Important: AoC cannot validate that your Irdeto service is configured correctly. You must work with Irdeto to validate your Irdeto implementation.

Cloud and node support

This section details support and constraints for Irdeto watermarking in Aspera on Cloud.

- Supported cloud platforms
 - AWS S3
 - N. Virginia (us-east-1); Oregon (us-west-2); N. California (us-west-1)
 - Sao Paulo (sa-east-1)
 - Ireland (eu-west-1); London (eu-west-2); Frankfurt (eu-central-1)
 - Tokyo (ap-northeast-1); Singapore (ap-southeast-1); Sydney (ap-southeast-2)

- GCS
 - us-central1

Note: Your Irdeto account and your associated cloud storage must be in same provider region. See [Irdeto documentation](#) for more information.

- Supported [Aspera node type](#): Aspera-managed auto-scale clusters (ATS).
- You can enable watermarking only on nodes that do *not* have encryption at rest (EAR) applied.
 - This EAR constraint includes both cloud-provider server-side encryption and Aspera-provided encryption-at-rest (whether Aspera or your own KMS manages the root key).
 - If you are unsure whether a node is enabled for encryption at rest, Aspera recommends creating one or more new nodes to support your organization's watermarking needs.
 - For supporting documentation, see [Use Aspera-managed keys for server-side encryption at rest](#); [Bring your own key for server-side encryption at rest](#).

Using watermarking in Aspera on Cloud

This section describes how Packages app users can work with the watermarking capabilities you configure.

Watermarking applies to content in the AoC Packages app only.

Receiving a watermarked package

Recipients of watermarked packages must log in to retrieve the package. Traceability using forensic watermarking requires that users in the content workflow be authenticated. Therefore, recipients cannot download a watermarked package from a public link.

Recipients must download watermarked packages using the Aspera on Cloud Packages app with [IBM Aspera Connect](#).

File types and profiles supported

In a watermarked package, watermarking applies only to files that conform to supported profiles. Profiles comprise not only the supported file types (.ts; .ps; .mpg; .mpeg; .mov; .mxf; .mp4), but codecs, dimensions, and more; see the [Irdeto watermarking service documentation](#) for requirements.

GCS caveat

Ensure that watermarked packages do not contain files from Google Cloud Storage (GCS) that have special characters in file names.

Package actions

- [Recalled packages](#): You cannot recall a watermarked package.
- [Forward packages](#): You cannot forward a watermarked package.
- [Save to Files app](#): You cannot use the Actions menu to save a watermarked package to the Files app.
- [Add recipients to a package](#): When you add recipients to a watermarked package, the new recipients receive packages with their watermark. Adding recipients generates an immediate notification to the new recipients.
- [Draft packages](#): If a transfer fails to start, AoC moves the package to the Drafts folder. You cannot change the watermarking setting for a package in the Drafts folder.

Configure watermarking in Aspera on Cloud

To complete this procedure, you need the following:

- The name of the workspace in which you want members to send watermarked packages.
- The node secret for the node that contains the workspace in which you want members to send watermarked packages.
- These parameters from your Irdeto account:
 - Storage provider
 - Storage provider region
 - DWM API endpoint
 - Tenant ID

1. Create a watermarking profile.
 - a. In the Admin app, go to Integrations > Watermarking > Create new.
 - b. Give this profile a name and add a description if you wish.
 - c. In the following fields, select your cloud provider and region, then enter your Irdeto DWM API endpoint and Tenant ID.
 - d. Click Create.

AoC displays a list of nodes available to use with the Irdeto account you specified in the profile.
2. Associate the profile with a node.
 - a. From the list of nodes, select the node hosting the workspace in which you want members to send watermarked packages.
 - b. Enter the [node secret](#), then click OK.

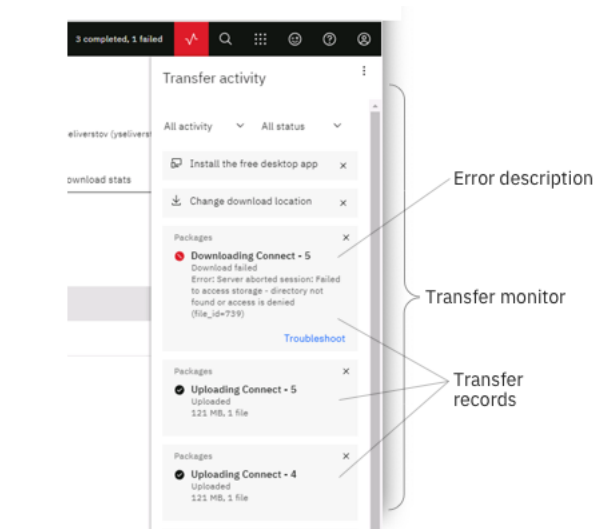
The list of available workspaces on that node appears.
3. Enable watermarking for Packages in a workspace.
 - a. In the list of workspaces that appears, click the intended workspace to display a configuration window.
 - b. Set the toggle labeled Watermarking enabled to On.
 - c. Set the toggle labeled Watermarking required.

Select Yes to make watermarking automatic for every package sent from this workspace.
 Select No if you want workspaces members to choose whether to apply watermarking to a given package as they send it.

Note: As noted previously in this article, recipients of a watermarked package *must* log in to AoC to download the package. Does this workspace allow members to send to external users? If yes, and you select Required, you must also check the Packages app setting Require external users to log in when receiving packages. An external user who does not log in cannot download watermarked package contents. See [Require external users to log in](#).
4. Click Save.

Troubleshooting

Errors that may occur for the transfer of watermarked packages appear in the AoC transfer monitor, on the individual transfer record.



The table below lists watermarking-related errors that may occur. For troubleshooting procedures, see the [Irdeto documentation](#).

Error code	Error message
106	Service: Could not embed enough watermarks for proper detection
130	Service: Failed bits per sample validity check
131	Service: Failed Resolution validity check
132	Service: Failed Framerate validity check
133	Service: Failed Bitrate validity check
134	Service: Unsupported input file codec
165	Service: Task processing retries attempted but still failed
1001	Watermark: Invalid parameter value received
1002	Watermark: Embedder was forcefully interrupted
1003	Watermark: Not implemented
1007	Watermark: Input file not found
1008	Watermark: General IO error
1009	Watermark: Unsupported input format
1011	Watermark: No permissions to read input file
1013	Watermark: Corrupted stream
1014	Watermark: Cannot write variant file
3000	Unknown system error

Antivirus scanning

This document outlines the steps to create a new antivirus configuration.

Create a new antivirus scanning configuration

Follow these steps to set up a new antivirus configuration:

1. Select the Admin application.
2. From the left-hand navigation panel, go to Integrations > Antivirus scanning.
3. Click Create new to begin setting up a new antivirus profile.
Important: Access to your AWS account and configuration of your Trend Micro instance are required to set up your antivirus scanning.
4. Fill in the following fields:
 - Name: Enter a unique name for your antivirus configuration.
 - Description (optional): Add a brief description to help identify the configuration later.
5. Under Storage provider, select Amazon S3 from the drop-down menu.
6. Copy the JSON snippet from the Trust relationship policy box. In your AWS Management Console, create a new IAM role and paste the trust policy into the AWS IAM trust relationship configuration. This policy is required to establish secure communication between IBM Aspera and your AWS environment. For more information about creating IAM roles, refer to the [official AWS documentation](#).

AWS settings configuration

1. **Create an IAM role:** Ensure that the IAM role has permissions to access the SQS queue. Note the role's Amazon Resource Name (ARN). For example:

```
arn:aws:iam::<account-id>:role/<role-name>
```

2. **Create or identify an SQS queue:** In the Amazon SQS console, create a new queue that will be used for antivirus scanning notifications. Note the queue's URL. For example:

```
https://sqs.<region>.amazonaws.com/<12-digit-account>/<queue-name>
```

- For more information about creating and configuring SQS queues, refer to the [official AWS documentation](#).
3. **Associate the IAM role with the SQS queue:** Update the IAM role policies to allow sending and receiving messages from the SQS queue. For more information about managing permissions for SQS, refer to the [official AWS documentation](#).
 4. After creating the IAM role and SQS Queue URL, select the I have created the IAM role with the provided trust policy, and am ready to proceed box.

Finalize the antivirus configuration

1. In the antivirus profile setup screen, enter the following values:
 - IAM role ARN: Provide the full ARN of the IAM role you created.
 - SQS Queue URL: Provide the URL of the SQS queue that will be used for antivirus scanning notifications.
2. Specify the name of the Amazon S3 bucket associated with this configuration in the Bucket name field.
3. Copy the JSON snippet from the Permission Policy box. In your AWS Management Console, open the SQS console, edit the queue's Access policy, and paste the provided JSON. This grants the IAM role permission to send and receive messages from the queue.
4. After you successfully complete the process in the AWS dashboard, select the I have saved the permission policy in my AWS dashboard box.
5. Click Create to save the configuration.

Authentication

Configure the appropriate authentication method for your organization. Articles detail setting up SAML, IBMid (enabled by default), and Google authentication methods. Implement multifactor authentication for IBMid. Avoid admin logout when disabling IBMid for another authentication method. Learn how to configure the login page to guide users to the proper authentication method.

- [Configuring authentication methods for your organization](#)
Configure one or more authentication methods for your AoC users, including IBMid, Google OAuth, and one or more SAML providers. Once configured, you can apply one or more of these methods to users and groups in your organization.
- [Configure the user login page](#)
You can configure a splash message to communicate any information your users may need; for example, a welcome message, an upcoming maintenance window, a configuration change, and so on. You can also provide login guidance to your users by configuring the login buttons and associated instructions on the login page.
- [SAML](#)
This section provides a detailed overview of Aspera on Cloud SAML support. It also contains step-by-step procedures to integrate your SAML SSO into AoC. For those using the OKTA IdP, find here a procedure to configure OKTA to provide SAML-based user authentication for Aspera on Cloud.
- [IBMid](#)
IBMid is enabled by default, and supports multifactor authentication (MFA). You can disable IBMid if required, but consider enabling a special access option to avoid administrator logout.
- [Configuring Google authentication](#)
You can enable authentication by Google, which allows users to access Aspera on Cloud based on authentication into Google.

Configuring authentication methods for your organization

Configure one or more authentication methods for your AoC users, including IBMid, Google OAuth, and one or more SAML providers. Once configured, you can apply one or more of these methods to users and groups in your organization.

Once you configure one or more of these authentication methods, you can assign one of them to each user in your organization, either during new user creation or by modifying an existing user record. You can also allow individual users to log in using any configured auth provider for which they have credentials; in this scenario, the user can log in at one time using one configured auth provider, and another time using a different configured auth provider. For details, see [Create and manage users](#).

The authentication methods you configure for your organization appear as buttons on your organization login page. For each auth method, you can configure the label on the button to help guide your users to the login method you intend for them; go to Admin > Authentication > *your_identity_provider*.

The following table provides an overview of different authentication types supported in Aspera on Cloud:

Authentication Type	Description
IBMid	IBMid is enabled by default for all Aspera on Cloud organizations; no configuration is required. IBMid is the ID-as-a-Service (IDaaS) from IBM. It is available for anyone using IBM cloud and many IBM cloud services, including Aspera on Cloud. You can enable multifactor authentication for users who log in with IBMid. You can also enable a special access option for specific admins to avoid being locked out of Aspera on Cloud when you disable IBMid. For details and procedures, see the articles under IBMid .
SAML	You can enable one or more SAML IdPs for your organization. To allow your users to log in through multiple SAML providers, set the Authentication method to Any . For details and procedures, see the articles under SAML .
Google OAuth	You can enable authentication by Google, which allows users to access Aspera on Cloud based on authentication into Google. In this scenario, the user in essence logs in to Google using a dialog presented by Aspera on Cloud; Google then passes that authentication to Aspera on Cloud, and Aspera on Cloud accepts that authentication to allow Aspera on Cloud access. Such authentication populates user accounts in Aspera on Cloud based on Google-verified identity. For details and a procedure, see Configuring Google authentication .

Configure the user login page

You can configure a splash message to communicate any information your users may need; for example, a welcome message, an upcoming maintenance window, a configuration change, and so on. You can also provide login guidance to your users by configuring the login buttons and associated instructions on the login page.

These configuration options are in addition to your ability to [brand](#) the login page with your logo and a background image.

Configure the login button and label and associated instructions on Admin > Authentication. See [Configuring authentication methods for your organization](#) for details and a procedure.

To configure the login page button labels, button instructions, button order and a splash message, do the following:

1. Go to Organization > Profile and branding.
2. To configure a login page splash message to your users, enter the message in the text box in the Organization > Profile and branding > Profile > Splash message field. Use Markdown to format the message as required. To delete the message, simply remove the text from the text box.
3. To configure the login button labels, along with instructions (if needed) that display with the login button, go to Authentication > OAuth, or to Authentication > SAML instance > Profile.
4. To configure the order of the button display on the login page, scroll to the Organization > Profile and branding > Login options area. Click the arrows or drag each button to display them in your intended order.
5. Click Save.

SAML

This section provides a detailed overview of Aspera on Cloud SAML support. It also contains step-by-step procedures to integrate your SAML SSO into AoC. For those using the OKTA IdP, find here a procedure to configure OKTA to provide SAML-based user authentication for Aspera on Cloud.

- [Configuring SAML: Overview](#)
Aspera on Cloud administrators can configure Aspera on Cloud to support SAML (Security Assertion Markup Language) 2.0 authentication for your users. When a user attempts to sign in to Aspera on Cloud using SAML, Aspera on Cloud redirects the user to the identity provider (IdP) sign-on URL. The user signs in to the IdP with their SAML credentials, and the IdP sends a SAML assertion to Aspera on Cloud; Aspera on Cloud then grants access to the SAML user.
- [Configuring SAML: Procedures](#)
This article contains step-by-step procedures for configuring SAML authentication for your organization, including default SAML workspaces and shared inboxes, SAML metadata on the IdP, and SAML groups. Also included is how to configure the AoC login page with specific instructions to guide SAML users and avoid improper login actions.
- [Configuring SAML SSO using OKTA](#)
OKTA is an identity provider (IdP) that supports SAML; an AoC administrator can configure OKTA to provide SAML-based user authentication for Aspera on Cloud.

Configuring SAML: Overview

Aspera on Cloud administrators can configure Aspera on Cloud to support SAML (Security Assertion Markup Language) 2.0 authentication for your users. When a user attempts to sign in to Aspera on Cloud using SAML, Aspera on Cloud redirects the user to the identity provider (IdP) sign-on URL. The user signs in to the IdP with their SAML credentials, and the IdP sends a SAML assertion to Aspera on Cloud; Aspera on Cloud then grants access to the SAML user.

Aspera on Cloud supports multiple SAML IdPs.

For detailed procedures, see [Configuring SAML authentication: Procedures](#).

Note: When you use SAML, you may consider disabling IBMid as an authentication method. Before you do, review the information in [Avoid lockout when disabling IBMid](#).

Process overview

1. Configure your SAML Identity Provider.
2. Configure SAML for Aspera on Cloud. Configure an Aspera on Cloud default SAML workspace, including shared inbox access and permissions, if desired.
Note: Configuring SAML default workspaces is optional if you prefer to assign user access and permissions using Aspera on Cloud SAML groups.
3. Apply the Aspera on Cloud-generated SAML metadata to the IdP.
4. Configure SAML groups in Aspera on Cloud, using the IdP group Distinguished Name (DN) to map an Aspera on Cloud SAML group to an IdP SAML group.
Note: Configuring mapped SAML groups is optional if you prefer to assign user access and permissions using SAML default workspaces.
5. Customize the label on the SAML button that users click on the user login page.
6. Grant additional access and permissions beyond those defined in default SAML workspaces or SAML groups.

IdP requirements

To use SAML with Aspera on Cloud, you must already have an identity provider (IdP) that meets the following requirements:

- Supports SAML 2.0
- Able to use an HTTP POST binding
- Generates fingerprints using the SHA-1 algorithm
- Not configured to use pseudonyms
- Can return assertions to Aspera on Cloud that include the entire contents of the signing certificate
- If prompted, set to sign the SAML response (signing the SAML assertion is optional)

Certificate or fingerprint

To configure SAML on Aspera on Cloud, you can use either the IdP certificate or the fingerprint. If you use an IdP fingerprint, it must be encrypted using the SHA-1 algorithm.

IdP metadata

The following formats are required for IdP configuration with Aspera on Cloud:

Tag	Format
NameID	urn:oasis:names:tc:saml:1.1:nameid-format:unspecified

Tag	Format
EntityID	https://api.ibmaspera.com/api/v1/oauth2/<your_org_subdomain>/saml/<saml_id>/metadata
Binding	urn:oasis:names:tc:saml:2.0:bindings:HTTP-POST
Callback URL	https://api.ibmaspera.com/api/v1/oauth2/<your_org_subdomain>/saml/<saml_id>/callback

Once you complete SAML configuration in Aspera on Cloud, Aspera on Cloud generates XML metadata that you can copy and apply to your IdP. For more details, see "Configuring SAML metadata on the IdP" in [Configuring SAML authentication: Procedures](#).

SAML assertion

Aspera on Cloud expects the assertion from the IdP to contain the following elements:

Aspera on Cloud Attribute Mapping Field	Required or Optional
Email	Required
First Name	Optional
Last Name	Optional
Member Of	Required to map Aspera on Cloud SAML groups to existing groups in the IdP database

Default SAML workspaces

In the SAML configuration interface (**Organization > Authentication > SAML**), you can configure one or more existing Aspera on Cloud workspaces as default SAML workspaces. Each SAML user gains automatic membership in each default SAML workspace you configure.

In each default SAML workspace, you can configure SAML-user access and permissions to existing shared inboxes. Each SAML user has automatic membership and access permissions in the group inboxes you designate in default SAML workspaces.

Note: SAML default workspace configuration is optional. If you do not configure a default SAML workspace, you must configure at least one Aspera on Cloud SAML group that is mapped to an IdP group (see "SAML groups" below). Granting access using SAML groups can provide more flexible access control.

Default SAML workspaces and shared inboxes must already exist

You must create a workspace (and any shared inboxes in it) as a separate operation before you can designate a workspace as a default SAML workspace (see [Creating a new workspace](#) and [Creating a new shared inbox](#)). Once the workspaces and shared inboxes exist, you can designate workspaces as SAML defaults, assigning shared inbox access and permissions in the same operation (see "Configuring SAML authentication" in [Configuring SAML authentication: Procedures](#)).

SAML user access and permissions

SAML members gain access to all files and folders shared to the default workspaces, even if they were shared before the SAML member's initial login. In addition, SAML users gain access to shared inbox packages in the shared inboxes you designate, according to the permissions you configure, even if that package was sent before the SAML user first logged in.

If you add or remove default SAML workspaces, SAML users gain or lose membership in the workspaces automatically. The same applies to changes you make to shared inbox access and permissions in a default SAML workspace.

If desired, you can add further access and permissions for an individual SAML user account, but you cannot restrict permissions beyond those configured in the user's default SAML workspaces or SAML groups.

Important:

- Access and permission changes are applied only when a user logs in. Changes you make while a given SAML user is logged in to Aspera on Cloud will not affect the user until they log out and back in.
- If you update the email address for a SAML user, the user will receive AoC notifications at the new address. However, the user must continue to log in to AoC using their *original* email address.

SAML groups

You can create an Aspera on Cloud group, mark that group as a SAML group, then map that Aspera on Cloud SAML group to an IdP group using the group Distinguished Name (DN); be sure to enter the DN in the AoC UI exactly as configured at the IdP. Aspera on Cloud grants new SAML users membership in Aspera on Cloud SAML groups based on the IdP group membership data contained in the IdP response messages. This grant requires accurate mapping of the AoC **Member of** attribute mapping field (Organization > Authentication > SAML > Create new/<existing_SAML_config_name>) to the DN of the IdP group in the SAML assertion (see "SAML assertion" above).

You can restrict login to members of IdP-mapped Aspera on Cloud groups. With this restriction in place, users without membership in an IdP group mapped to an Aspera on Cloud SAML group cannot log in to Aspera on Cloud. Without that restriction in place, a SAML user who is not a member of any IdP groups can log in to Aspera on Cloud, but will not gain membership in any Aspera on Cloud SAML group. However, such a user gains membership in configured default SAML workspaces, if any exist. To configure this restriction, see "Configuring SAML Authentication" in [Configuring SAML authentication: Procedures](#).

With one exception, you can manage Aspera on Cloud SAML groups just like any other group, including adding an Aspera on Cloud SAML group to a non-SAML group. The exception is that you cannot manually add users to or remove users from an Aspera on Cloud SAML group. Aspera on Cloud SAML group membership is granted upon login to a user who is a member of an IdP group that is mapped to a corresponding Aspera on Cloud SAML group.

You can convert a SAML group to a standard group, and vice versa. See "Configuring Aspera on Cloud SAML Groups" in [Configuring SAML authentication: Procedures](#).

SAML users

SAML users can log in to Aspera on Cloud through membership in a configured default SAML workspace, or through their membership in an IdP group that has a corresponding mapped Aspera on Cloud SAML group, or both.

There is no need to configure SAML users in Aspera on Cloud. When a SAML user logs in to Aspera on Cloud for the first time, Aspera on Cloud automatically generates an account for that user based on the information provided in the SAML response. If the SAML response includes group membership information, Aspera on Cloud gives the SAML user membership in the corresponding Aspera on Cloud group (if it exists), which is mapped to the IdP group using the group Distinguished Name (DN). If your

Aspera on Cloud SAML configuration includes default SAML workspaces, the user gains membership in these workspaces and any shared inboxes in these workspaces that you designated, according to the permissions you selected during SAML configuration.

Once a SAML user has established an Aspera on Cloud account, you can manage that user in the same ways you can manage non-SAML users.

Important:

- When you delete a SAML user from the IdP database, you should manually delete the corresponding Aspera on Cloud user account.
- If you update the email address for a SAML user, the user will receive AoC notifications at the new address. However, the user must continue to log in to AoC using their *original* email address.

Adding access and permissions

If desired, you can update a SAML user account to grant additional access and permissions, but you cannot restrict permissions beyond those configured in the default SAML workspaces or the user's SAML groups. For example:

- If default SAML Workspace1 includes access to SharedInboxA with Can Send and Can Receive permission, you can update an individual SAML user account to add Can Invite permission to SharedInboxA. You cannot remove Can Send or Can Receive permission, because those are configured at the default workspace level.
- If a SAML user is a member of mapped Aspera on Cloud SAML GroupA that has membership in Workspace2, you cannot remove the SAML user's membership in Workspace2 without removing the user from SAML GroupA.
- You can grant access to an existing SharedInboxB in default Workspace1 that is not included in default workspace configuration.
- You can grant access to workspaces not included in the configured SAML default workspaces.
- You can add SAML users to non-SAML groups.

Users with preexisting AoC accounts

When a SAML user logs in to Aspera on Cloud for the first time, Aspera on Cloud checks for a preexisting Aspera on Cloud account with the same email address. If an account with a matching email address already exists, Aspera on Cloud merges the preexisting account with the new SAML account, resulting in one SAML user account.

In this way, a preexisting user who logs in through SAML becomes a SAML user; the new SAML user loses access to Aspera on Cloud via the preexisting account. However, the user's preexisting access and permissions are retained, in addition to the access and permissions granted with their SAML account. If such a user is deleted from the IdP database, they lose all access to Aspera on Cloud, the same as any other Aspera on Cloud SAML user.

Login restrictions

If desired, you can restrict user login for certain domains:

- **Include domains:** List domains from which users **can** log in. For example, if you select Include domains and list abc.com and xyz.com, only users with email addresses from those two domains are allowed to log in. Users from all other domains than those listed are not allowed to log in.
- **Exclude domains:** List domains from which users **cannot** log in. For example, if you select Exclude domains and list rst.com and bgt.com, users with email addresses from those two domains are not allowed to log in. Users from all other domains than those listed are allowed to log in.

You can also restrict login to users who are members in Aspera on Cloud groups that are mapped to SAML groups. See "SAML groups" above.

Configuring SAML: Procedures

This article contains step-by-step procedures for configuring SAML authentication for your organization, including default SAML workspaces and shared inboxes, SAML metadata on the IdP, and SAML groups. Also included is how to configure the AoC login page with specific instructions to guide SAML users and avoid improper login actions.

For an overview of SAML authentication in Aspera on Cloud, including IdP requirements and details on default SAML workspaces, SAML groups, and SAML users, refer to [Configuring SAML authentication: Overview](#).

Note: When you use SAML, you may consider disabling IBMId as an authentication method. Before you do, review the information in [Avoid lockout when disabling IBMId](#).

Configuring SAML authentication

To configure SAML authentication for your Aspera on Cloud organization, do the following:

1. In the Admin Management console, select **Admin > Authentication > SAML**.
2. Click Create new.
3. Select the checkbox labeled Enable SAML authentication.
4. In the Name field, enter a name for this SAML configuration. The name you configure here appears in the Type column for individual SAML users (Users & Groups > Users). The name is also used in the label for the login button presented to users when they log in; see "Labeling the user login button" below.
5. In the SSO target URL field, enter your IdP single sign-on URL.
6. In the SAML login button label field, enter the button label to display to users on the login page.
7. In the Instructions field, if desired, enter text to help your users select the proper login method, or any other useful message.
8. In the allowable clock drift field, enter the maximum allowable drift, in seconds, between Aspera on Cloud and the SAML IdP.
If the actual drift exceeds the configured value, Aspera on Cloud does not accept the SAML response and does not execute the operations attempted by SAML users.
9. Select Fingerprint or **Certificate**; only one is required to authenticate with the SAML IdP.
 - a. If you select Fingerprint, enter the fingerprint of the IdP.
Note: The fingerprint must be generated from the certificate using the SHA-1 algorithm.
 - b. If you select Certificate, enter the certificate of the IdP.
10. To prevent users who are not assigned to a mapped SAML group from logging in to your Aspera on Cloud organization, select **Restrict login to mapped SAML group members**.
11. To apply domain-based login restrictions, do the following in the Login restrictions area of the window (for details on login restrictions, see [Configuring SAML: Overview](#)):
 - a. Select Exclude domains or Include domains from the Login restrictions menu.
 - b. In the field that displays, enter one or more domains (example.com).

- c. To remove a domain from the restriction list, click X on the domain row.
12. In the Attribute mapping fields, enter the IdP attribute labels that correspond to the Aspera on Cloud field labels. For example, in the First Name field, enter **given_name** if your IdP uses that label for the user first name attribute. **Note:** These fields are not optional, even if the IdP labels are identical with Aspera on Cloud labels.
 - a. In the Email field, enter your IdP attribute label for user email addresses.
 - b. In the First name field, enter your IdP attribute label for user first or given name.
 - c. In the Last name field, enter your IdP attribute label for user last name or surname.
 - d. In the Member of field, enter your IdP attribute label for user SAML group membership.
13. Click Create.

Configuring default SAML workspaces and shared inboxes

After the SAML instance is created you can configure workspaces and shared inboxes for your SAML users.

1. Click the row of the SAML instance to open the record, then click Workspace memberships > Add workspaces.
2. Select the role for these SAML users in this workspace: Member or Workspace manager.
3. Enter the workspace name.
4. Click Add.
5. To add a shared inbox, do the following:
 - a. Click the row of the workspace.
 - b. Select the intended shared inboxes.
 - c. Click Add.

Configuring SAML metadata on the IdP

Once SAML authentication configuration is complete, Aspera on Cloud generates the SAML metadata and displays it in the SAML Metadata panel. You must copy this metadata and apply it to your SAML IdP. Once the metadata generated by Aspera on Cloud is applied to the IdP, Aspera on Cloud and the IdP negotiate a trusted relationship. Only then can SAML users authenticate at their IdP to gain login access to Aspera on Cloud.

Configuring Aspera on Cloud SAML groups

To configure an Aspera on Cloud SAML group, do the following:

1. Go to Groups > Create new.
2. Enter a group name and optional description.
3. Select Make this group a SAML group.
4. Enter the Distinguished Name (DN) of the IdP group, exactly as defined at the IdP, to map to this Aspera on Cloud group.
5. Click Create.

Labeling the user login button

Once you complete SAML configuration, a button for your SAML instance displays on the Aspera on Cloud login page. You can configure the label for that button to ensure users authenticate against the proper authentication instance.

By default, the login button for your SAML instance displays the text "Sign in with <saml_instance_name>". To customize this label, do the following:

1. Go to Admin > Authentication > SAML, then click the row of the intended SAML instance.
2. In the SAML login button label field, customize the label as desired.
3. To provide additional guidance to users about this login method, enter text in the Instructions field.

To change the order of authentication options presented on the login page, go to Organization > Profile and branding > Login options.
4. Click Save.

Configuring SAML SSO using OKTA

OKTA is an identity provider (IdP) that supports SAML; an AoC administrator can configure OKTA to provide SAML-based user authentication for Aspera on Cloud.

Enabling the trusted relationship between OKTA and AoC that allows your SAML users to log in to AoC requires that you perform a multi-step process. Assuming that you have migrated from Aspera Files to Aspera on Cloud, configure a new SAML instance for OKTA.

- In OKTA, create a new SSO connection, entering the desired clock drift and SAML attributes.
- In Aspera on Cloud, create a new SAML instance, using the SSO URL and SSH fingerprint or certificate generated by OKTA.
- In OKTA, complete the configuration, using the SAML metadata generated by AoC.

Detailed procedures follow; refer also to your [OKTA user documentation](#).

Create the SSO connection in OKTA

In OKTA, create new SSO connection. Completing this procedure generates the following data, which are required for the configuration in Aspera on Cloud.

- SSO URL
- SSH fingerprint or SSH certificate, whichever you configured

In the Attribute Statements panel, configure the following:

Name	Value
email	user.email

Name	Value
given_name	user.firstName
surname	user.lastName

Create the new SAML instance in Aspera on Cloud

In Aspera on Cloud, do the following:

1. Go to Organization > Authentication > SAML > Create new.
2. Create the new SAML instance, using the SSO URL and SSH fingerprint or certificate generated from OKTA, as described in [Configuring SAML for AoC](#).

When you save the new SAML configuration, AoC generates the SAML metadata, which you must add to your OKTA configuration for AoC.

To find the SAML metadata, go to Organization > Authentication > SAML > your SAML instance > Profile. Scroll down to find the SAML metadata entry; copy it and return to OKTA to complete the configuration.

Enter the SAML metadata in OKTA

In OKTA, do the following:

1. In the AoC SSO connection, go to the Configure SAML tab.
2. In the Single sign on URL field, enter the Callback URL for the AoC SAML configuration (called 'Location' in the AoC SAML metadata).
3. Select the check box labeled **Use this for Recipient URL and Destination URL**.
4. In the Audience URI field, enter the AoC metadata URL (called 'entity ID' in the AoC SAML metadata).
5. In the Name ID format field, leave the entry unspecified.
6. In the Application username field, enter the OKTA username.

IBMid

IBMid is enabled by default, and supports multifactor authentication (MFA). You can disable IBMId if required, but consider enabling a special access option to avoid administrator lockout.

- **Configure IBMId**
IBMid is automatically enabled for your organization; you do not need to configure it. You can disable it if required.
- **Require multifactor authentication for IBMId users**
You can require multifactor authentication (MFA) for all Aspera on Cloud organization members who log in with IBMId. Once enabled, users who enter their IBMId credentials (the first factor) see a page that requires them to enter a verification code (the second factor). The second factor can be delivered in either of two ways.
- **Avoid lockout when disabling IBMId**
When you disable IBMId for your organization, you can minimize the possibility of being locked out of Aspera on Cloud by enabling *special access*.

Configure IBMId

IBMid is automatically enabled for your organization; you do not need to configure it. You can disable it if required.

IBMid is the ID-as-a-Service (IDaaS) from IBM. It is available for anyone using IBM cloud and many IBM cloud services, including Aspera on Cloud.

The authentication methods you configure for your organization appear as configurable buttons on your organization login page.

You can configure the label on the IBMId login button. You can also configure instructions that display next to the login button, helping users to select the appropriate authentication method when more than one is available.

You can [require multifactor authentication \(MFA\)](#) for all Aspera on Cloud organization members who log in with IBMId. You can also enable a [special access option](#) for specific admins to avoid being locked out of Aspera on Cloud when you disable IBMId.

To configure the IBMId button and provide instructions, do the following:

1. Go to **Authentication > OAuth > IBMId**.
2. Select the check box labeled **Enable IBMId** (enabled by default).
3. To require users to enter a verification code sent to their IBMId email or authentication app, select the checkbox labeled Require multifactor authentication. For details, see [this article](#).
4. In the field labeled **IBMId login button label**, enter the label you want your users to see on the login button.
5. If desired, in the field labeled **Instructions to display with the login button**, enter a message to users.
6. Click **Save**.

Allow traffic using IBMId authentication

You must allow (allowlist/whitelist) the following URLs:

From	To	
	Service name	Service FQDN + Port =TCP/443

From	To	
	Service name	Service FQDN + Port =TCP/443
Aspera on Cloud front-end web client	IBM Cloud	- iam.cloud.ibm.com - identity-?*.iam.cloud.ibm.com/identity/authorize Where: ? = one character * = one region name (no deeper subdomain allowed) For example: https://identity-2.us-south.iam.cloud.ibm.com/identity/authorize

Require multifactor authentication for IBMid users

You can require multifactor authentication (MFA) for all Aspera on Cloud organization members who log in with IBMid. Once enabled, users who enter their IBMid credentials (the first factor) see a page that requires them to enter a verification code (the second factor). The second factor can be delivered in either of two ways.

- By default, users receive a verification code in their IBMid email account.
- Users who prefer to use an authenticator app can configure this in their IBMid account. Log in to www.ibm.com with IBMid credentials; go to Profile > ID and password > TOTP for configuration guidance. Users can download the authenticator app of their choice to their smart phone or tablet; for example, IBM Verify or Google Authenticator.

Before you begin

Keep the following in mind when considering whether and when to enable MFA for your Aspera on Cloud organization.

- Enabling MFA affects all your organization members who log in with IBMid.
- MFA for your organization applies to the AoC web app login for IBMid users. API keys for users and service IDs continue to work after you enable MFA.
- Plan a communication and support strategy for users in your organization:
 - Choose a date and time to enable MFA that results in the least impact to your business.
 - Notify your account users that you will be enabling MFA, and provide them with information on what to expect and how to prepare.

Enabling MFA

Enabling MFA does not affect users that are already logged in; MFA takes effect only at new logins.

- Go to Authentication > OAuth > IBMid.
- Select the checkbox labeled Require multifactor authentication.
- Click Save.

Upon their next log in attempt, your IBMid users receive the second-factor authentication request according to their IBMid profile.

Avoid lockout when disabling IBMid

When you disable IBMid for your organization, you can minimize the possibility of being locked out of Aspera on Cloud by enabling *special access*.

Consider this scenario: suppose that you disable IBMid and OAuth, and configure a single SAML provider as the single authentication method for your organization. If the SAML server becomes unavailable, all users would be locked out of your organization.

Special access allows org admins whose **Authentication type** is set to **Any access provider** to log in at a restricted URL using their IBMid.

With special access enabled, these admins can access a restricted login page by entering this URL: https://<your_org_subdomain>.ibmaspera.com/ibmid. When the admin enters valid IBMid credentials on this page, they can access Aspera on Cloud.

To configure the required **Authentication type** for organization administrators, see [Create and manage users](#).

To disable IBMid as an authentication method, do the following:

- Go to **Authentication > OAuth > IBMid**.
- Deselect the check box labeled **IBMid**.
- If desired, select the check box labeled **Enable special access**.
- Click **Yes**.

Configuring Google authentication

You can enable authentication by Google, which allows users to access Aspera on Cloud based on authentication into Google.

In this scenario, the user in essence logs in to Google using a dialog presented by Aspera on Cloud; Google then passes that authentication to Aspera on Cloud, and Aspera on Cloud accepts that authentication to allow Aspera on Cloud access. Such authentication populates user accounts in Aspera on Cloud based on Google-verified identity.

Note: When you use Google OAuth, you may consider disabling IBMid as an authentication method. Before you do, consider the information in [Avoid lockout when disabling IBMid](#).

Login restrictions

You can restrict user login for certain domains:

- **Include domains:** List domains from which users *can* log in.
For example, if you select *Include* and list abc.com and xyz.com, only users with email addresses from those two domains are allowed to log in. Users from all other domains are not allowed to log in.
- **Exclude domains:** List domains from which users *cannot* log in.
For example, if you select *Exclude* and list rst.com and bgt.com, users with email addresses from those two domains are not allowed to log in. Users from all other domains are allowed to log in.

Enable Google OAuth

To enable authentication by Google, do the following:

1. Go to **Authentication > OAuth > Google OAuth**.
2. Select the check box labeled **Enable Google OAuth**.
3. In the field labeled **Google login button label**, enter the label you want your users to see on this button on the login page.
4. If desired, in the field labeled **Instructions to display with the login button**, enter a message to users.
5. To apply login restrictions, do the following:
 - a. Select either **Include Domains** or **Exclude Domains** from the **Login restrictions** drop-down menu (for details, see "Login Restrictions").
 - **Include Domains:** List domains from which users *can* log in.
 - **Exclude Domains:** List domains from which users *cannot* log in.
 - b. In the field that displays, enter one or more domains (example.com).
 - c. To remove a domain from the restriction list, click the **X** on the domain row.
6. Click **Save**.

Subscription usage and billing

Understand your subscription and its features. Learn how to manage your storage usage, transfer volume, and egress, and how your billing reflects your usage.

- [Understanding your subscription usage and billing](#)
The Subscription Management page shows your actual historical, monthly, and cumulative usage as reflected on your bill. Use this data to monitor usage, identify usage patterns, control budget, project expenses, and reconcile billing statements.
- [Feature and usage tiers](#)
IBM Aspera on Cloud customers can select from among several editions when subscribing to the service. All subscription pricing is based on the volume of data transferred using the service.
- [Try Aspera on Cloud for free](#)
You can try Aspera on Cloud for free. You can use your Aspera on Cloud trial for 14 days or for 50 Gb of transfer volume, whichever happens first. Your trial subscription is the Standard Plus edition; you can change to a different edition when you convert to a paid subscription if you wish; note that some features are not available in the Essentials and Pay/Go editions.
- [Manage transfer volume in your subscription](#)
This value measures the volume of all transfers *into and out of* storage when you use an *entitlement*-enabled Aspera transfer server.
- [Manage egress in your subscription](#)
Egress is the fee that a cloud provider charges when you move data out of their cloud. When you download data directly from your cloud storage, your storage provider bills you for egress directly. When you use Aspera on Cloud to download from cloud storage, the cloud provider charges IBM Aspera for egress; IBM Aspera then passes these egress charges on to your subscription.
- [Manage storage in your subscription](#)
Each AoC subscription includes storage in IBM Cloud—this storage is *built in* to your AoC subscription. "Storage" is the volume of your data in your built-in IBM Cloud storage each month.
- [Required configuration for your tethered node](#)
When you tether (or attach) your own Aspera HSTS node or cluster to Aspera on Cloud, you must configure it specifically for monitoring in the Activity app and for usage metering on your subscription. This procedure is not required when you attach your own existing cloud storage.

Understanding your subscription usage and billing

The Subscription Management page shows your actual historical, monthly, and cumulative usage as reflected on your bill. Use this data to monitor usage, identify usage patterns, control budget, project expenses, and reconcile billing statements.

To access this page, click Subscription management in the left panel (**Admin > Subscription management**). There are two tabs, each providing key information.

- The Account page states your subscription edition (Essentials, Advanced, and so on) and summarizes the features and volume allowances of your AoC plan. This page also describes your subscription term, making it easy to know when renewal date approaches.
This tab includes your pre-paid volume for the three key usage components: transfer volume, egress, and storage. These volumes include your original in-plan allowance plus any additional allowance you added since the term began. (Pay-as-You-Go subscriptions do not have pre-paid volumes.)
- The Subscription page, available to administrators of paid editions, displays historical and current monthly usage. In graphs and tables, you can see monthly and cumulative usage (when applicable) compared to your plan allowances or pre-committed maximums for each value. This page is available to administrators of all paid editions. For more access details, see "Availability" near the end of this article.

For details on AoC subscription editions, pricing, and available terms, or to start a free trial, see <https://www.ibm.com/cloud/aspera/pricing>. To discuss a current AoC subscription, contact your IBM Sales Representative.

Note: If you are the initial admin in your org, you also have access to the Aspera Usage Portal at <https://usage.asperasoft.com/login>. The Usage Portal provides data on transfer usage only, and allows you to download CSV reports of transfer usage. Additional admins can request access to the Usage Portal by emailing aspera-

Trial subscriptions

Admins of trial subscriptions can access the Account summary page only. Trial subscriptions are the Advanced edition.

For a free trial of Aspera on Cloud, go to <https://www.ibm.com/cloud/aspera/pricing>.

Convert from trial to paid subscription: Contact IBM Sales

To convert from a free trial to a paid subscription, go to <https://www.ibm.com/cloud/aspera/pricing>, then click the Let's talk button to contact an IBM Sales Rep. Keep in mind that your trial subscription gives you the Advanced edition; if you convert to a different paid edition, available features and volumes will change.

Metric definitions

The Subscription management page shows your actual usage as reflected on your bill. See also the [IBM Aspera on Cloud Service Description](#).

Subscription versions

Revisions to the Aspera on Cloud service description have changed some metric definitions. The content in this and related articles reflects the newest service description. Following are a few examples of these service description changes. There are other service description changes, including certain pricing details and tethered node limits, that do not impact these articles.

In the new service description:

- Pay-as-You-Go editions do not have pre-paid storage; all your storage in use at the time of the monthly snapshot is billed to you.
- Pay-as-You-Go editions no longer see a separately line item for egress. Instead, egress charges are included in transfer volume charges.
- All editions allow unlimited users.
- The Activity app is available to all editions.

Transfer volume

Your subscription accumulates transfer volume when you use any Aspera transfer server that is enabled by an *entitlement* to transfer files or folders. Your subscription does *not* accumulate transfer volume when you use a transfer server that is enabled by a *license*, which is bandwidth-based rather than consumption-based.

Your pre-paid subscription includes a pre-paid amount of transfer volume. If you exceed that pre-paid maximum, you'll receive a bill for the excess volume, billed at pay-per-use (overage) rates.

Pay-as-You-Go subscriptions do not have pre-paid transfer volume. As a Pay/Go subscriber, you are billed for all outbound and inbound transfers enabled by an entitlement.

For details, see [Manage transfer volume in your subscription](#).

Egress

Egress measures the volume of data transferred *out* of your attached cloud storage using an Aspera-managed transfer server.

Your pre-paid subscription includes a pre-paid amount of egress. If you exceed that pre-paid maximum, you'll receive a bill for the excess volume, billed at pay-per-use (overage) rates.

Pay-as-You-Go subscriptions do not pay egress; egress fees are included in transfer volume fees.

For details, see [Manage egress in your subscription](#).

Storage

This value is the volume of data that your organization places in your built-in IBM Cloud storage each month.

Your pre-paid subscription includes a pre-paid amount of storage. If you exceed that pre-paid maximum, you'll receive a bill for the excess volume, billed at pay-per-use (overage) rates.

Pay-as-You-Go subscriptions do not have pre-paid storage. As a Pay/Go subscriber, you are billed for all storage in your built-in IBM Cloud storage. For details, see [Manage storage in your subscription](#).

Availability

The Subscription management page provides two views: Account and Usage. These views are available to AoC admins according to the table below.

Note: The Subscription management page is not currently available to customers with multiple AoC organizations.

For any questions about availability of the Subscription management page, contact your IBM Sales Representative: go to <https://www.ibm.com/cloud/aspera/pricing>, then click **Let's Talk**; an IBM Sales professional will come online to assist you.

View	Trial	Pay/Go	Essentials	Standard Plus	Premium
Account	✓	✓	✓	✓	✓
Usage	—	✓	✓	✓	✓

Feature and usage tiers

IBM Aspera on Cloud customers can select from among several editions when subscribing to the service. All subscription pricing is based on the volume of data transferred using the service.

Aspera's FASP transfer technology is incorporated into each edition, and offers:

- High-speed data transfer across hybrid-cloud environments
- Reliable transfer of any size or number of files
- Built-in clustering delivering unlimited scalability
- Use of any storage location
- Encryption in transit and at rest
- Data integrity verification

Note: [Aspera on Cloud trial](#) organizations use the Standard plus edition. Converting from a trial to a Pay/Go or Essentials edition subscription results in some features of the trial being unavailable.

The editions build upon each other to offer robust collaboration, management, branding, and security capabilities. For details, see [IBM Aspera on Cloud: Pricing](#).

To confirm your subscription level, click the user menu icon and select Account settings > IBM Aspera on Cloud edition.

To change your subscription level, contact your IBM Sales representative.

Features	Subscription tiers			
	Pay as You Go	Essentials	Standard Plus	Premium
	Ideal for lean teams with simple, one-off file-sharing use cases	Great for small organizations delivering simple, fixed-volume projects to multiple locations	Best for mid-size companies in need of multiple workspaces and simple automation	For enterprises continuously working on high-volume projects & advanced workflow acceleration
IBM Aspera Proxy			●	●
Minimum transfer volume commitment (TB)	No transfer volume commitment	1	6	30
Included storage (TB)	Storage not included. Storage charged as USD 0.03 per GB	1	10	20
Included egress (TB)	Egress pass-through provider costs included as part of the per-GB price	10	100	500
Custom URLs	0	1	1	5
Concurrent automated workflows	0	0	5	10
Workspaces	1	1	100	Unlimited
High-speed transfer server installs	1	1	Unlimited	Unlimited
File deletion policies	0	1	5	150
Unlimited users		●	●	●
Uncapped bandwidth		●	●	●
Advanced monitoring and insights		●	●	●
HTTPs Gateway			●	●
SSO with SAML			●	●
Shared inboxes			Unlimited	Unlimited
Access to IBM Aspera Enterprise software suite				●
File preview (self-managed)				●
Antivirus scanning integration			●	●

Try Aspera on Cloud for free

You can try Aspera on Cloud for free. You can use your Aspera on Cloud trial for 14 days or for 50 Gb of transfer volume, whichever happens first. Your trial subscription is the Standard Plus edition; you can change to a different edition when you convert to a paid subscription if you wish; note that some features are not available in the Essentials and Pay/Go editions.

For a free trial of Aspera on Cloud or to convert to a paid subscription, go to <https://www.ibm.com/cloud/aspera/pricing>.

To set up your new trial organization, see [Set up your organization](#).

Keep in mind that your trial subscription gives you the Standard Plus edition; if you convert to a different paid edition, available features and volumes will change.

Important: Sending packages to external users is not available in the trial. To test this feature, contact the support team or your IBM sales representative. Alternatively, you can add the recipient as a user in your instance and send them the package directly.

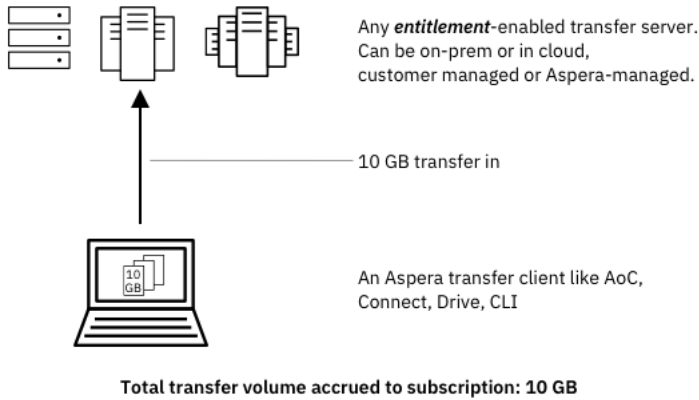
Manage transfer volume in your subscription

This value measures the volume of all transfers *into and out of* storage when you use an *entitlement*-enabled Aspera transfer server.

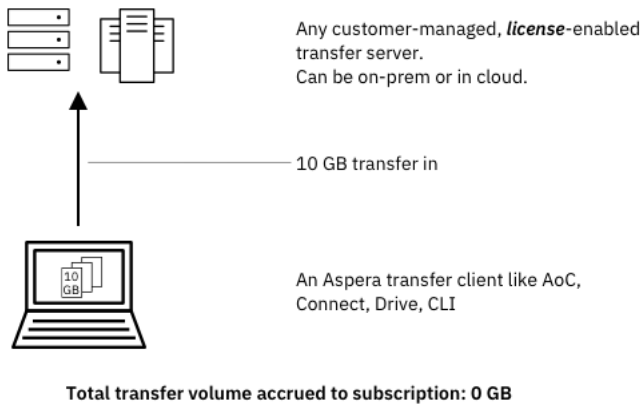
Which transfers accrue to your subscription?

Your subscription accumulates transfer volume when you use any Aspera transfer server that is enabled by an *entitlement* to transfer files or folders. Your subscription does *not* accumulate transfer volume when you use a transfer server that is enabled by a *license*, which is bandwidth-based rather than consumption-based.

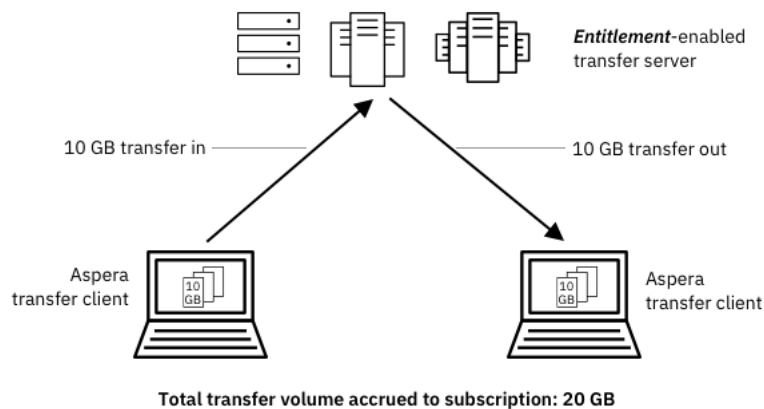
Using an *entitled* server, upload from desktop: A simple upload of a 10 GB folder to an *entitlement*-enabled transfer server accrues 10 GB of transfer volume in your subscription. The same would apply for a download of a 10 GB file from an entitlement-enabled transfer server.



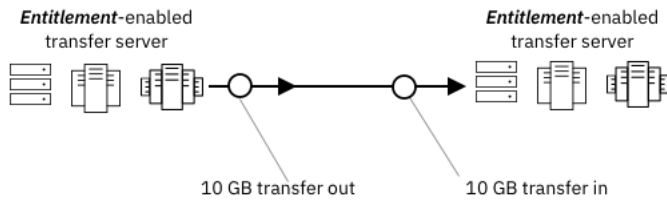
Using a *licensed* server, upload from desktop: A simple upload of a 10 GB folder to a *license*-enabled transfer server does not accrue transfer volume in your subscription. The same would apply for a download of a 10 GB file from a license-enabled transfer server.



Using an *entitled* server, send files from one person to another: This operation combines an upload and a download of a 10 GB file for a total of 20 GB transfer volume.

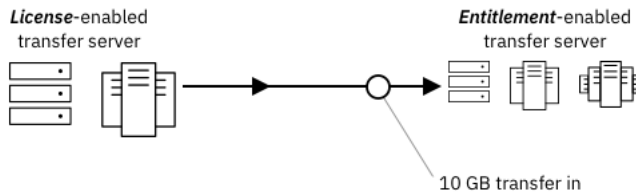


Between *entitled* servers, transfer from Node to node/Region to region/Cloud to cloud: When you transfer from one *entitlement*-enabled server to another, the transfer is metered on both the send and receiving systems. In this example, the transfer of a 10 GB file from one region to another results in 20 GB of total transfer volume. This type of transfer volume may accrue when you move files or folders from one location to another in your AoC Files app.



Total transfer volume accrued to subscription: 20 GB

Between a *licensed* and an *entitled* server, transfer from Node to node/Region to region/Cloud to cloud: When you transfer between a *license*-enabled server and an entitlement-enabled server, the transfer is metered only at the entitled system. In this example, the transfer of a 10 GB file from one region to another results in 10 GB of total transfer volume. This type of transfer volume may accrue when you move files or folders from one location to another in your AoC Files app.



Total transfer volume accrued to subscription: 10 GB

What causes transfer volume overages?

Your pre-paid subscription includes a pre-paid transfer volume. You have the entire term of your subscription to use that volume. Once you exceed the pre-paid volume, your subscription incurs overage charges for further transfers; you move into a pay-per-use status for transfer volume.

You remain in pay-per-use status and continue to be billed overage fees for additional transfer volume until either you increase your pre-paid volume in negotiation with IBM, or the term expires and your transfer volume accumulation begins again.

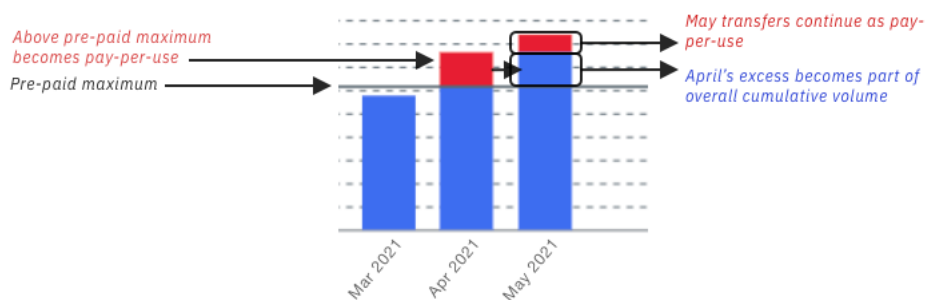
AoC does not limit your ability to transfer data even if you exceed your pre-paid transfer volume.

Pay-as-You-Go subscriptions do not have pre-paid transfer volume. As a Pay/Go subscriber, you are billed for all outbound and inbound transfers enabled by an entitlement.

Example

In the screenshot below, taken from the Subscription management page (**Admin > Subscription > Usage > Transfer volume**), your transfer volume exceeds your pre-paid max in April. The excess volume is shown in red in April. IBM Aspera bills you for the excess volume at pay-per-use rates.

In May, April's excess volume, already billed to you, shows as part of the overall cumulative transfer volume you've used so far. IBM Aspera bills you for the transfers you make in May at pay-per-use rates, since you continue to be in excess of your pre-paid max.



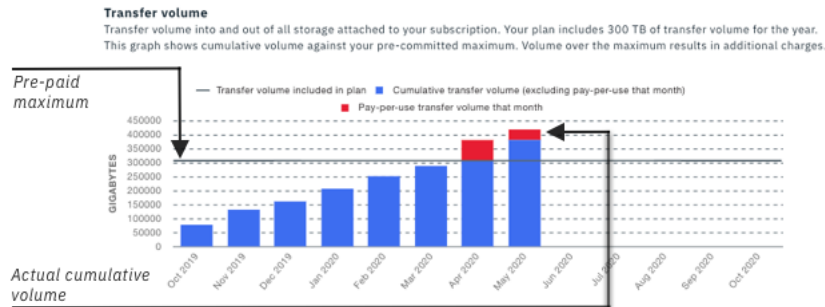
Interpret the graph and table

Transfer volume accumulates over the term of your subscription.

Reminder: Your subscription does not meter or charge for volume usage on your own bandwidth-based, licensed Aspera HSTS nodes or clusters tethered to Aspera on Cloud.

Graph

Consider a sample graph for transfer volume.



- You'll see that the actual cumulative transfer volume to date is shown by the height of the last bar to the right, which is the current month.
- The in-plan allowance or pre-committed maximum is the heavy horizontal line on the graph.

Table

If your subscription includes multiple entitlements, you can filter the table view. When you filter by month, the table shows a different view of the same data shown in the graph. If you filter by entitlement, you see usage depicted by entitlement.

Each monthly row shows transfer volume used, the total for the month, and the total cumulative volume used per date. Monthly usage is broken down into your pre-paid volume and pay-per-use volume. As long as your cumulative volume remains below your pre-paid max, you are not billed for pay-per-use fees (also called overage fees). Once you exceed your pre-paid max, all subsequent monthly transfer volume is pay-per use or overage.

Month	In-plan transfer volume used	Pay-per-use transfer volume used	Total monthly transfer volume	Total transfer volume used to date

As an example, suppose transfer volume exceeds the in-plan allowance during the month of April. Consider these columns in the April row. The third column shows that the total transfer volume used in the month was 93,072.9 GB. This total monthly volume is split between 19,096.7 GB (left column) as the last of the pre-paid volume, plus 73,976.2 GB (second column) additional transfer volume that month, to be billed as pay-per-use.

April 2020	Pre-paid volume 19,096.7 GB	+ Pay-per-use volume 73,976.2 GB	= Total monthly volume 93,072.9 GB	Term cumulative volume 381,176.2 GB

Now consider the last two columns for two adjacent months. The value in the last column ("Total transfer volume used to date") for October, plus the value in the second-to-the-last column ("Total monthly transfer volume") for November, equals the value in the last column for November. In other words, the *Month1 cumulative* volume plus *Month2 monthly* volume equals *Month2 cumulative* volume.

Month	In-plan transfer volume used	Pay-per-use transfer volume used	Total monthly transfer volume	Total transfer volume used to date
October 2019	77,143.6 GB	0 GB	77,143.6 GB	1 77,143.6 GB
November 2019	54,250.8 GB	0 GB	2 54,250.8 GB	3 131,394.4 GB

1 + 2 = 3

Manage egress in your subscription

Egress is the fee that a cloud provider charges when you move data out of their cloud. When you download data directly from your cloud storage, your storage provider bills you for egress directly. When you use Aspera on Cloud to download from cloud storage, the cloud provider charges IBM Aspera for egress; IBM Aspera then passes these egress charges on to your subscription.

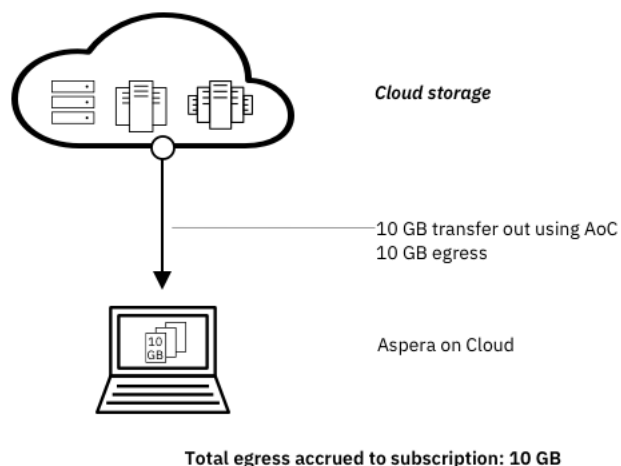
Which transfers accrue egress?

Your pre-paid subscription accumulates egress charges when you use AoC to transfer data out of any cloud storage. Your subscription does *not* accumulate egress when you *don't* use AoC to transfer data from cloud storage, nor when you use AoC to transfer data from an on-premises, non-cloud storage.

Note that IBM Aspera does not bill Pay-as-You-Go subscriptions for egress as a separate line item; egress fees are included in transfer volume fees.

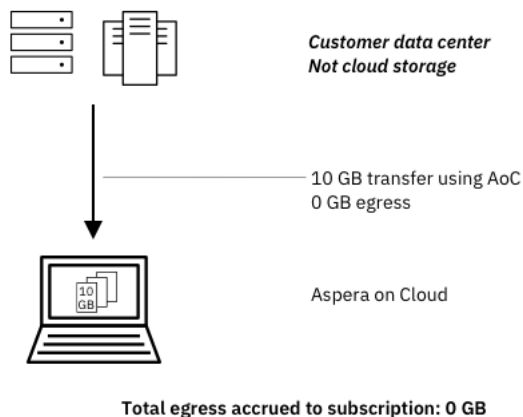
From cloud storage, download using AoC

When you use AoC to download, the cloud provider charges IBM Aspera for egress; Aspera passes those charges on to you.



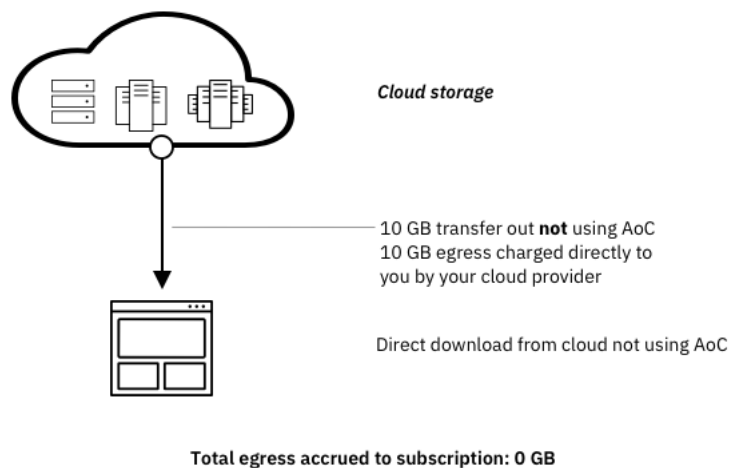
From your data center, download using AoC:

If the data you download is not in the cloud, no egress charges occur.



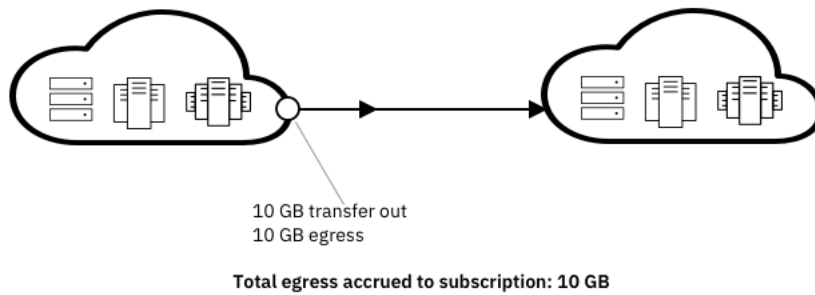
From cloud storage, download directly without AoC

If you download using some other tool rather than using AoC, your cloud provider charges you directly for egress; no egress accrues to your subscription.



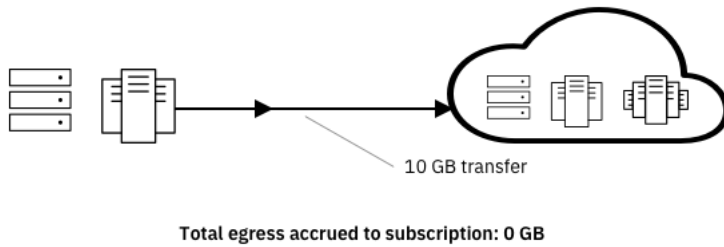
From cloud storage, transfer to another cloud or region using AoC

Using AoC to transfer data from one cloud to another results in egress charges to IBM Aspera; IBM Aspera passes those charges to your subscription.



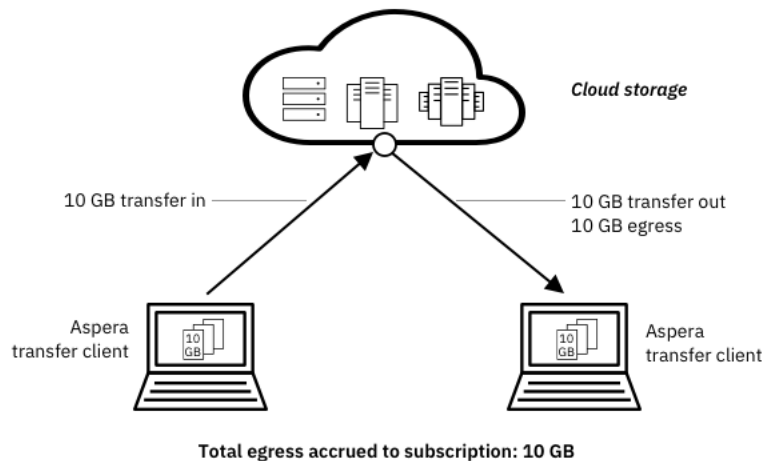
From a data center, transfer to cloud storage using AoC

This transfer does not cause egress charges since the data is not moving out of any cloud storage.



Send files from one person to another

This operation combines an upload and a download of a 10 GB file. Since the transfer used the cloud, egress of 10 GB accrues to your subscription.



What causes egress overages?

Your subscription includes a pre-paid egress volume. You have the entire term of your subscription to use that egress volume. Once you exceed the pre-paid volume, your subscription incurs overage charges for further egress; you move into a pay-per-use status for egress.

You remain in pay-per-use status and continue to be billed overage fees for additional egress until either you increase your pre-paid volume in negotiation with IBM, or the term expires and your egress accumulation begins again.

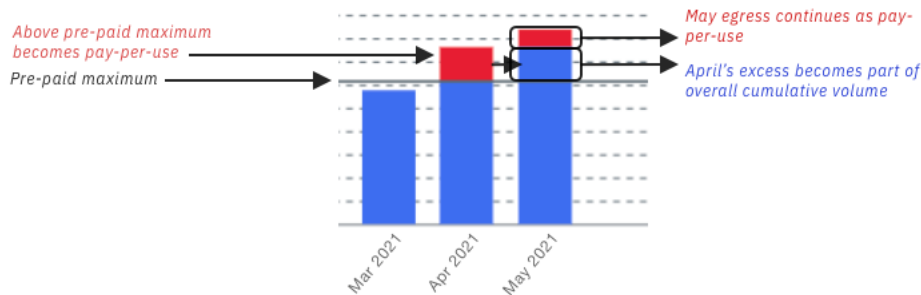
AoC does not limit your ability to move your data from cloud storage even if you exceed your pre-paid egress volume.

If you subscribed to a Pay-as-You-Go (Pay/Go) plan, the term of your subscription is one month and there is no pre-paid maximum allowance for egress.

Example

In the screenshot below, your egress volume exceeds your pre-paid max in April. The excess egress is shown in red in April. IBM Aspera bills you for the excess egress at pay-per-use rates.

In May, April's excess egress, already billed to you, shows as part of the overall cumulative egress you've used so far. The egress you use in May continues to be billed at pay-per-use rates, since you continue to be in excess of your pre-paid max.

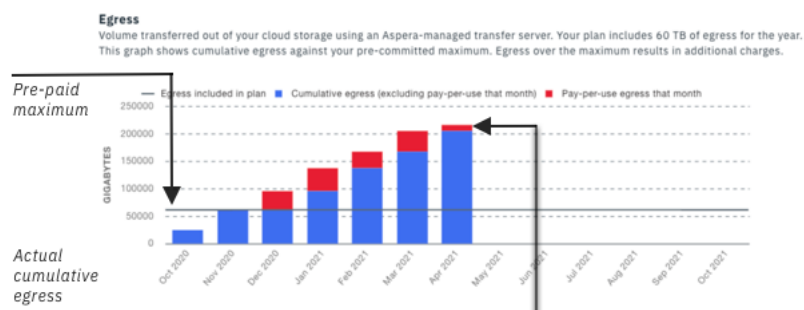


Interpret the graph and table

Egress usage accumulates over the term of your subscription. Your subscription includes a pre-paid, in-plan egress volume.

Graph

Consider a sample graph for egress.



It's easy to see your current egress usage compared to your pre-paid egress allowance.

- The height of the last bar to the right, which is the current month, is the actual cumulative egress to date.
- The heavy horizontal line shows pre-committed maximum or pre-paid allowance for egress.

Table

If your subscription includes multiple entitlements, you can filter the table view. When you filter by month, the table shows a different view of the same data shown in the graph. If you filter by entitlement, you see usage depicted by entitlement.

Below each graph is a tabular representation of the same data. Each month shows egress used, the total for the month, and the total cumulative egress used per date. Monthly usage is broken down into your in-plan volume and pay-per-use volume. As long as your cumulative egress remains below your in-plan max, you incur no pay-per-use fees. Once you exceed your in-plan max, all subsequent egress is pay-per use.

Month	In-plan egress used	Pay-per-use egress used	Total monthly egress	Total egress used to date

As an example, suppose egress exceeds the in-plan allowance during the month of April. Consider these columns in the April row. The right column shows that the total egress used in the month was 93,072.9 GB. This total monthly egress is split between 19,096.7 GB (left column) as the last of the pre-committed, in-plan egress, plus 73,976.2 GB (center column) additional egress that month, to be billed as pay-per-use.

April 2020	Pre-paid volume 19,096.7 GB	+	Pay-per-use volume 73,976.2 GB	=	Total monthly volume 93,072.9 GB	Term cumulative volume 381,176.2 GB

Now consider the last two columns for two adjacent months. The value in the last column ("Total egress used to date") for October, plus the value in the second-to-the-last column ("Total monthly egress") for November, equals the value in the last column for November. In other words, the Month1 cumulative egress plus Month2 monthly egress equals Month2 cumulative egress.

Month	In-plan egress used	Pay-per-use egress used	Total monthly egress	Total egress used to date
October 2020	24,661.6 GB	0 GB	24,661.6 GB	1 24,661.6 GB
November 2020	36,387.2 GB	0 GB	2 36,387.2 GB	3 61,048.8 GB

1 + 2 = 3

Manage storage in your subscription

Each AoC subscription includes storage in IBM Cloud—this storage is *built in* to your AoC subscription. "Storage" is the volume of your data in your built-in IBM Cloud storage each month.

You can also [add your own existing storage](#) in any [supported cloud provider](#) to your Aspera on Cloud application; your subscription does not bill for storage in your own cloud provider since your pay your provider directly.

What counts as storage?

All data in your built-in IBM Cloud storage at the time of the monthly snapshot counts in your AoC storage metric.

Data in any other storage attached to your AoC organization in not counted in your AoC subscription, no matter whether that storage is on-premises, remote, or in the cloud, no matter which cloud provider. You pay those storage costs directly to the storage provider.

What causes storage overage charges?

Unlike egress and transfer volume, the AoC storage metric is not a cumulative measure of storage used over your term; rather, storage is calculated as a monthly snapshot.

For example, if, at the time of the monthly snapshot in May, data in your built-in storage exceeds your pre-paid storage volume, you are billed an overage charge for the excess storage that month. But if your built-in storage volume at the June monthly snapshot does not exceed your pre-paid volume, you do not receive a storage overage charge in June.

IBM Aspera does not limit the amount of data you can place in your built-in storage, even if you exceed your pre-paid amount.

Pay-as-You-Go Subscriptions

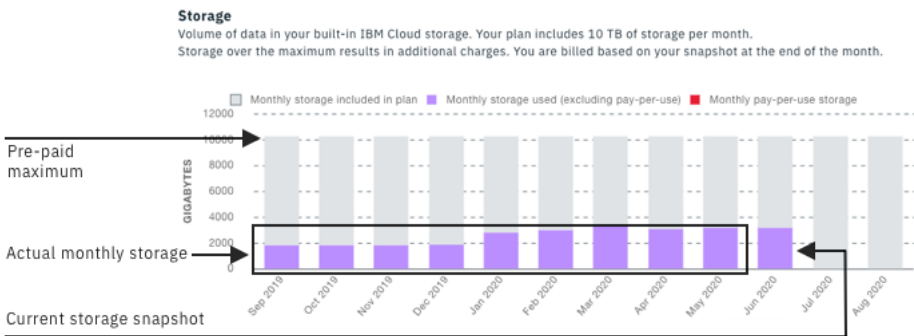
Pay-as-You-Go subscriptions do not have pre-paid storage. As a Pay/Go subscriber, you are billed for all storage in your built-in IBM Cloud storage at the time of the monthly snapshot.

Interpret the graph and table

Storage is not tracked or billed as cumulative volumes but rather as monthly usage values.

Graph

Consider a sample graph for storage.



The height of each monthly column shows the pre-paid storage maximum. In any given month, storage can be higher or lower than the previous month since storage is not calculated cumulatively over the term of your subscription. If you exceed your pre-paid maximum storage in a given month, IBM Aspera bills you for overage at pay-per-use rates. In the next month, your storage may again be below the pre-paid threshold and you won't receive a bill for overage.

Table

Below each graph is a tabular representation of the same data. Each month shows storage used. As long as the monthly total remains below your pre-paid max, you incur no pay-per-use fees. If a monthly total exceeds your pre-paid maximum for any given month, you are billed for pay-per use fees for that month.

The monthly in-plan allowance plus any monthly pay-per-use volume equals the total monthly storage volume.

Month	Monthly storage used (excluding pay-per-use)	Monthly pay-per-use storage	Total monthly storage
June 2020	149.9 GB 1	0 GB 2	149.9 GB 3
1 + 2 = 3			

Required configuration for your tethered node

When you tether (or attach) your own Aspera HSTS node or cluster to Aspera on Cloud, you must configure it specifically for monitoring in the Activity app and for usage metering on your subscription. This procedure is not required when you attach your own existing cloud storage.

Note: Linux servers are the only ones that can be used as a tethered node.

To attach your own user-managed High-Speed Transfer Server (HSTS) to Aspera on Cloud, you must configure it as a *tethered node*. For an overview of this procedure, see [Tether Your Aspera Transfer Server to Aspera on Cloud](#).

To configure your tethered node for monitoring and metering, see [Configure monitoring and metering for your tethered node](#). Without this configuration, you cannot transfer to or from your tethered node.

Aspera Connect transfer client

Learn how to install the IBM Aspera Connect transfer client, how to help outside users install Connect, and how to troubleshoot installation problems.

- [What is IBM Aspera Connect?](#)
Aspera on Cloud requires one of two transfer methods to power high-speed transfers between user desktops and Aspera transfer servers. Users can either download and install Aspera Connect, a free, lightweight, install-on-demand software program; or you can configure the IBM Aspera HTTP Gateway and attach it to your Aspera on Cloud organization.
- [Aspera Connect for Outside Users](#)
Aspera Connect is a free, lightweight, install-on-demand software program that powers high-speed transfers between desktops and Aspera servers.
- [Monitor transfers](#)
You can review your attempted and completed transfers and monitor your active, in-progress transfers using the transfer monitor. This in-app monitor reflects the transfer activity that you perform using the Aspera on Cloud app, including transfers that use the IBM Aspera Connect transfer client; the IBM Aspera HTTP Gateway; and direct node-to-node FASP transfers. To view transfer activity and usage for the entire organization, use the Aspera on Cloud Activity app.
- [Installation](#)
This section gives step-by-step instructions for installing the IBM Aspera Connect transfer client. Also included are instructions for installing the Connect browser extension in each supported browser.
- [Installation troubleshooting](#)
Find troubleshooting procedures addressing Aspera Connect installation-specific issues.
- [Other Connect troubleshooting](#)
Address the most common issues with Aspera Connect using the articles in this section, including the Connect prompt reappearing, disabling Connect when Aspera HTTP Gateway is enabled, and more.

What is IBM Aspera Connect?

Aspera on Cloud requires one of two transfer methods to power high-speed transfers between user desktops and Aspera transfer servers. Users can either download and install Aspera Connect, a free, lightweight, install-on-demand software program; or you can configure the IBM Aspera HTTP Gateway and attach it to your Aspera on Cloud organization.

Aspera Connect is the default transfer method for Aspera on Cloud and other Aspera web app. However, if your deployment of Aspera on Cloud does not permit the download and installation of client software, the admin can [configure](#) an alternative transfer method: the [IBM Aspera HTTP Gateway](#). Otherwise, all users must install the Aspera Connect transfer client and the Connect browser extension to complete high-speed transfers.

Once installed, Connect runs automatically when you transfer content using one of the Aspera web apps. In Aspera on Cloud, Connect typically runs in the background rather than on screen as in many of the other Aspera web applications.

Important: Connect comprises an app and a browser extension; you must install both as follows:

- You must install the Connect app once on your computer.
See [Installing Aspera Connect](#).
- You must install the Connect extension for each browser (except Internet Explorer) you'll use to access Aspera on Cloud.
See the appropriate article:
 - [Adding the Chrome browser extension for Connect](#).
 - [Adding the Firefox Connect Browser Extension](#).
 - [Adding the Safari browser extension for Connect](#).
 - [Adding the Microsoft Edge browser extension for Connect](#).

If required, you can configure Connect to change default settings for download location, transfer bandwidth, and various network and security settings. Configure Connect settings with the guidance of your Aspera administrator. Note that the Connect Transfers window displays all your recent transfers, whether through Aspera on Cloud or another Aspera product.

After each successful login, Aspera on Cloud checks to see whether the most recent version of Connect is running on your machine. If a Connect upgrade is available, Aspera on Cloud prompts you through the upgrade process.

If you have any issues with Aspera Connect performance, run the [IBM Aspera Connect Diagnostic Tool](#). See also [Installation troubleshooting](#) and [IBM Aspera Connect common issues](#). For more details, see the [IBM Aspera Connect product documentation](#).

Aspera Connect for Outside Users

Aspera Connect is a free, lightweight, install-on-demand software program that powers high-speed transfers between desktops and Aspera servers.

Aspera on Cloud provides several ways for you to collaborate with outside users; an *outside user* is an Aspera on Cloud user outside your workspace, or a user without a Aspera on Cloud account. Depending on the permissions configured, you can:

- Send files and folders to an outside user.

- Share folders with an outside user.
- Invite an outside user to send files and folders to you or to an Aspera on Cloud shared inbox.

When the outside user attempts to access content you've sent or shared, or to send content to you, Aspera on Cloud prompts them to download and install Aspera Connect—the same software your computer uses to transfer content between your local machine and another location. Aspera on Cloud supports Connect on both Windows and Mac OS, and in the most common browsers for each platform.

The download and installation are quick and simple, and Aspera on Cloud guides users through the process. See the procedures in [Installation](#).

Important: You may need to remind your colleague that they must install the Connect app once on their computer, but they must install the Connect extension for each browser (except Safari and Internet Explorer) they'll use to access Aspera on Cloud.

If they still have problems, direct them to [Overview: Aspera Connect installation troubleshooting](#) and the related browser-specific topics. If problems persist, contact your Technical Support provider.

Monitor transfers

You can review your attempted and completed transfers and monitor your active, in-progress transfers using the transfer monitor. This in-app monitor reflects the transfer activity that you perform using the Aspera on Cloud app, including transfers that use the IBM Aspera Connect transfer client; the IBM Aspera HTTP Gateway; and direct node-to-node FASP transfers. To view transfer activity and usage for the entire organization, use the Aspera on Cloud Activity app.

Transfer monitor

To open the transfer monitor, click the Transfers icon . You can filter the list of transfers by activity type (all, upload, download) or by transfer status (all, failed, stopped, running).

Note these aspects of the transfer monitor:

- For each transfer:
 - Label indicates whether the transfer occurred in the Packages app or in the Files app
 - Main label indicates package name (for transfers in the Packages app) or file/folder path/name (for transfers in the Files app)
 - Check mark indicates successful completion
 - Progress bar indicates active, in-progress transfer
 - "x" icon indicates failed transfer
 - Statistics labels indicate transfer size and date, transfer status (Downloaded, Uploaded, Error, Stopped, InProgress)
 - Access the activity modal by clicking the information icon. You can adjust the target rate of desktop transfers that were started using the Aspera clients. This modal displays real-time insights including transfer rate, percent completion, and more.
 - Click View local folder to jump to the finder/explorer location of the content on the local machine or remote storage
 - Location path displays near transfer statistics
- For active transfers:
 - Click the Pause or Play icon to the right to pause or resume the transfer
 - Text labels indicate transfer progress, rate, and items remaining
 - Animated progress bar indicates transfer progress

Entries in the transfer monitor

Note that a single user transfer operation may generate multiple transfer entries in the transfer monitor.

For example, suppose a single package contains content from multiple sources. Content from a local or remote source is a separate transfer from content that already resides on an Aspera transfer server. In this case, it is possible for one transfer to succeed and another to fail, even though both transfers are initiated from sending a single package.

What starts a transfer?

Aspera on Cloud initiates a transfer when you perform any of the following actions:

- Upload content into your Files app
- Download content from your Files app
- Move content from one location in your Files app to another
- Save content from a package to a location in your Files app
- Send a digital package in the Packages app
- Send a package to a shared inbox
- Download content from a package (including a shared inbox submission)

In addition, Aspera on Cloud also initiates a transfer during these operations:

- When an outside user sends you content
- When an outside user submits content to a shared inbox
- When an outside user you've shared content with downloads it
- When an outside user you've sent content to downloads it

Installation

This section gives step-by-step instructions for installing the IBM Aspera Connect transfer client. Also included are instructions for installing the Connect browser extension in each supported browser.

- [Installing Aspera Connect](#)

IBM Aspera Connect is the free, lightweight app that powers Aspera high-speed transfers. Aspera Connect is one of the two transfer methods that enable high-

speed transfers to and from user desktops. Once installed, Connect runs automatically in the background. Installing Connect is fast and easy, with a built-in installation wizard that provides step-by-step guidance.

- [Adding the Chrome browser extension for Connect](#)

This topic explains how to obtain and add the required IBM Aspera Connect extension to your Chrome browser. The extension is required in each browser you use to interact with Aspera on Cloud.

- [Adding the Firefox browser extension for Connect](#)

This topic explains how to obtain and add the required IBM Aspera Connect extension to your Firefox browser. The extension is required in each browser you use to interact with Aspera on Cloud.

- [Adding the Safari browser extension for Connect](#)

This topic explains how to obtain and add the required IBM Aspera Connect extension to your Safari browser. The extension is required in each browser you use to interact with Aspera on Cloud.

- [Adding the Microsoft Edge browser extension for Connect](#)

This topic explains how to obtain and add the required IBM Aspera Connect extension to your Edge browser. The extension is required in each browser you use to interact with Aspera on Cloud.

- [Adding the Firefox Connect Browser Extension](#)

This topic explains how to obtain and add the required IBM Aspera Connect extension to your Firefox browser. The extension is required in each browser you use to interact with Aspera on Cloud.

Installing Aspera Connect

IBM Aspera Connect is the free, lightweight app that powers Aspera high-speed transfers. Aspera Connect is one of the two transfer methods that enable high-speed transfers to and from user desktops. Once installed, Connect runs automatically in the background. Installing Connect is fast and easy, with a built-in installation wizard that provides step-by-step guidance.

Note: If you are unable to download software to your computer, see [Select a transfer method](#) and talk to your administrator.

Shortly after you log into Aspera on Cloud for the first time, you'll see an on-screen message prompting you to download and install Aspera Connect. A similar message displays when AoC detects that your local machine is not running the current version of Connect.

IBM Aspera recommends that you always use the latest version of Connect.

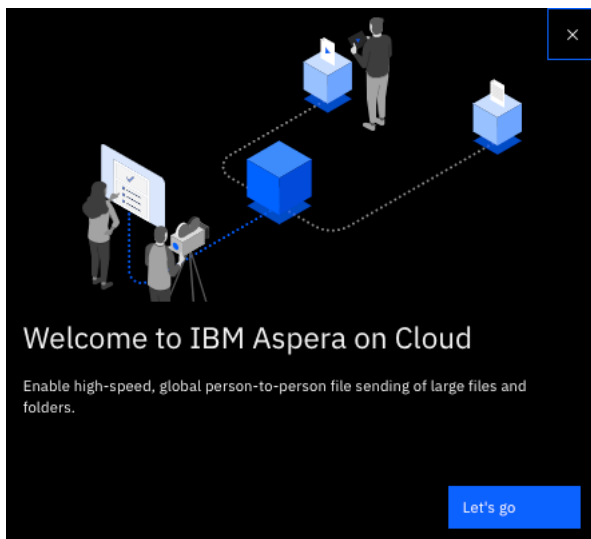
The procedure for installing IBM Aspera Connect requires enabling a browser extension for Connect in addition to installing the Connect application itself.

Important

- You must install the Connect app once on your computer. You must install the Connect extension for each browser (except Safari and Internet Explorer) you'll use to access Aspera on Cloud.
- Before performing a system-wide installation (all users of the machine), uninstall any per user installations. For details on uninstalling, see the [Connect user documentation](#).
- Remove all previous Connect installers before downloading the new installer.
- Connect works better when your browser's local storage is enabled; however, this is not a requirement.

Guided installation

When you log in to Aspera on Cloud for the first time, click Let's go on the Welcome screen.



Depending on your browser/platform combination, the screens shown in these instructions may vary.

1. In the Get started now screen, click Install extension and confirm to add the extension. Your browser's page for the Connect extension opens. See the instructions for your browser in [Installation](#). If successful, you'll see the message confirming the extension has been added.
2. The Get started now screen next prompts you to install Connect; click Install Connect:

Get started now — install the IBM Aspera Connect transfer client.

Install the [IBM Aspera Connect](#) client and the Aspera Connect browser plug-in to enable our signature high-speed file transfer technology.

☒ Install extension
Pre-requisite to install Connect

Install extension

☐ Install Connect client
Essential desktop app to make the transfer fast

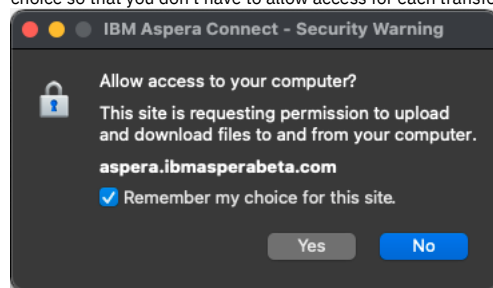
Install Connect

If you skip installing, you will be able to use IBM Aspera HTTP Gateway for transfers; for faster transfers come back and install Connect.

[I'll skip for now](#)

3. Once the Connect installation completes, refresh your browser.

Note: When you upload from or download to your computer, Connect requests access to your computer. IBM Aspera recommends you click the box to remember your choice so that you don't have to allow access for each transfer. Click Yes.



For more details, see the [Connect user documentation](#).

Adding the Chrome browser extension for Connect

This topic explains how to obtain and add the required IBM Aspera Connect extension to your Chrome browser. The extension is required in each browser you use to interact with Aspera on Cloud.

The Connect extensions are specific to the browser; the procedure for adding an extension to a browser is the same regardless of which OS platform that browser is running on. With a guided install, clicking **Install Extension** opens the extension link for the browser you are using. With a manual install, be sure to download the extension for the browser you intend to use with Connect.

Important: You must install the Connect app once on your computer. You must install the Connect extension for each browser (except Internet Explorer) you use to access Aspera on Cloud.

To obtain and install the Connect extension for Chrome, follow the procedure below:

1. When you see the Get started now screen, click Install Extension.

Get started now — install the IBM Aspera Connect transfer client.

Install the [IBM Aspera Connect](#) client and the Aspera Connect browser plug-in to enable our signature high-speed file transfer technology.

☒ Install extension
Pre-requisite to install Connect

Install extension

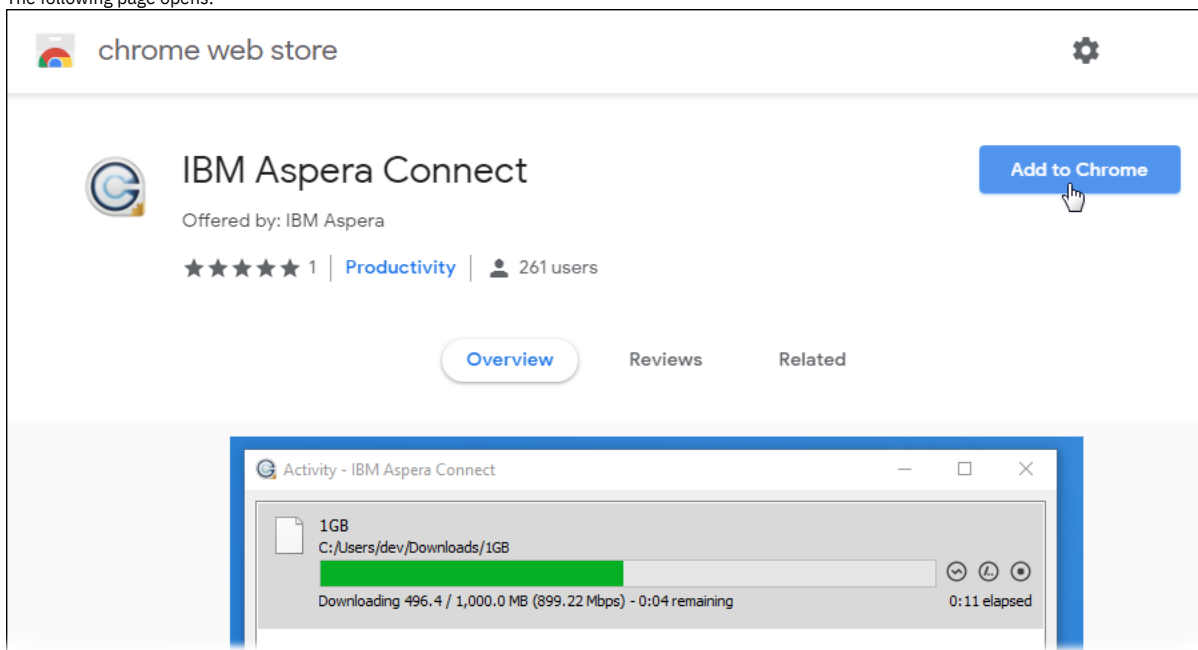
☐ Install Connect client
Essential desktop app to make the transfer fast

Install Connect

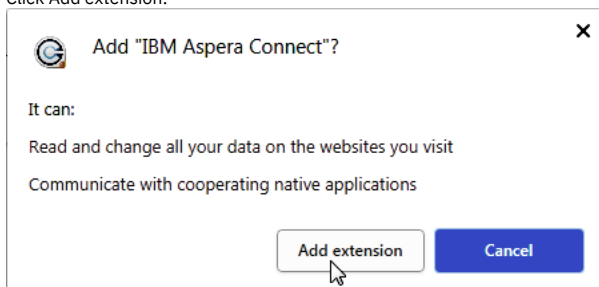
If you skip installing, you will be able to use IBM Aspera HTTP Gateway for transfers; for faster transfers come back and install Connect.

[I'll skip for now](#)

The following page opens:

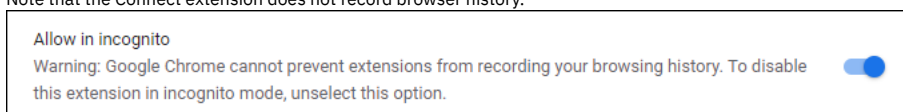


- Click Add to Chrome. The Add "IBM Aspera Connect"? dialog appears.
- Click Add extension.



If successful, you'll see the message "IBM Aspera Connect has been added to Chrome."

Note: By default, the Connect extension is disabled in Chrome's incognito mode. To enable the Connect extension, right-click the small Connect icon in the upper-right corner of your browser page. Then open Manage extensions and scroll down to the heading **Allow in incognito**. Then set the switch to ON as shown below. Note that the Connect extension does not record browser history.



Adding the Firefox browser extension for Connect

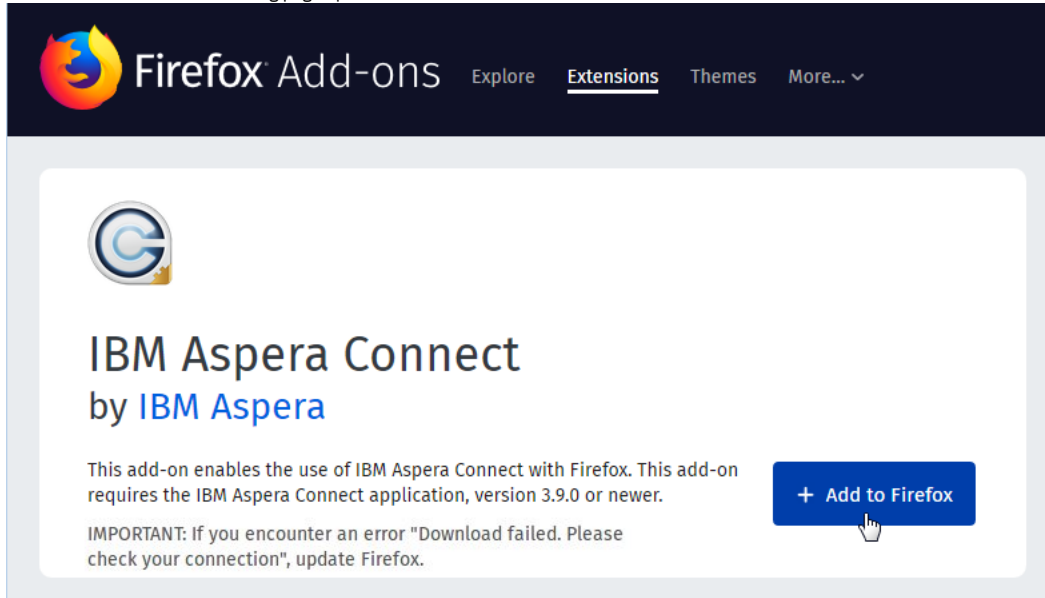
This topic explains how to obtain and add the required IBM Aspera Connect extension to your Firefox browser. The extension is required in each browser you use to interact with Aspera on Cloud.

The Connect extensions are specific to the browser; the procedure for adding an extension to a browser is the same regardless of which OS platform that browser is running on. With a guided install, clicking **Install Extension** opens the extension link for the browser you are using. With a manual install, be sure to download the extension for the browser you intend to use with Connect.

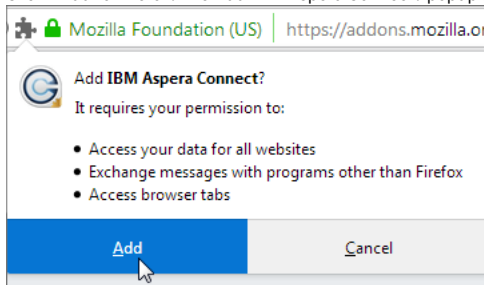
Important: You must install the Connect app once on your computer. You must install the Connect extension for each browser (except Internet Explorer) you use to access Aspera on Cloud.

To obtain and install the Connect extension for Firefox, follow the procedure below:

1. Click Add extension. The following page opens:



2. Click +Add to Firefox. The Add IBM Aspera Connect? popup appears.



3. Click Add.
If successful, you'll see the message "IBM Aspera Connect has been added to Firefox".

Adding the Safari browser extension for Connect

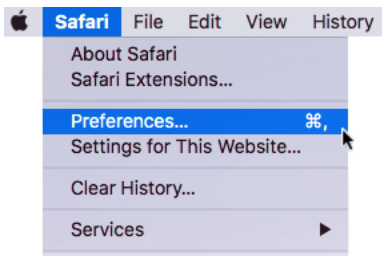
This topic explains how to obtain and add the required IBM Aspera Connect extension to your Safari browser. The extension is required in each browser you use to interact with Aspera on Cloud.

The Connect extensions are specific to the browser; the procedure for adding an extension to a browser is the same regardless of which OS platform that browser is running on. With a guided install, clicking **Install Extension** opens the extension link for the browser you are using. With a manual install, be sure to download the extension for the browser you intend to use with Connect.

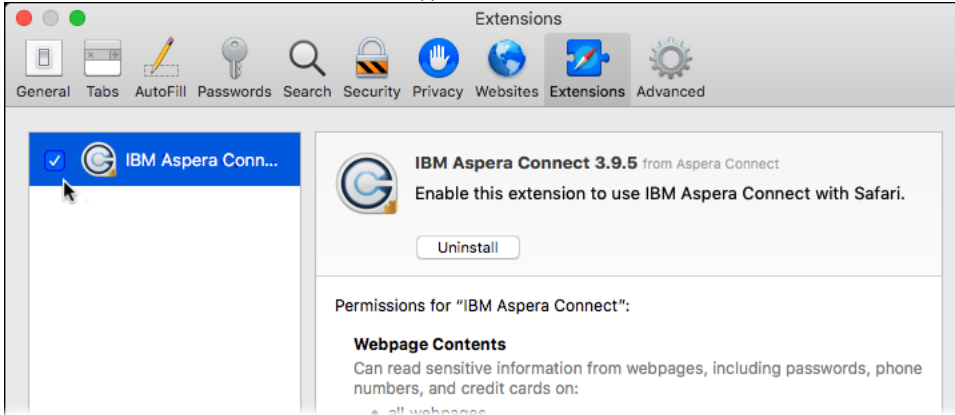
Important: You must install the Connect app once on your computer. You must install the Connect extension for each browser (except Safari and Internet Explorer) you use to access Aspera on Cloud.

The Connect browser extension for Safari is provided with the macOS installer for Connect. For this reason, the extension cannot be added to Safari until after the installer has been run. Once Connect is installed, add the Connect extension to Safari as follows:

1. Open **Safari > Preferences** (not Safari Extensions):



2. Select the **Extensions** tab. The Extensions window appears.



3. Look for the IBM Aspera Connect extension listed in the left panel, and click the check box to select it.
4. Close the dialog. The Connect extension has been added to your browser.

Adding the Microsoft Edge browser extension for Connect

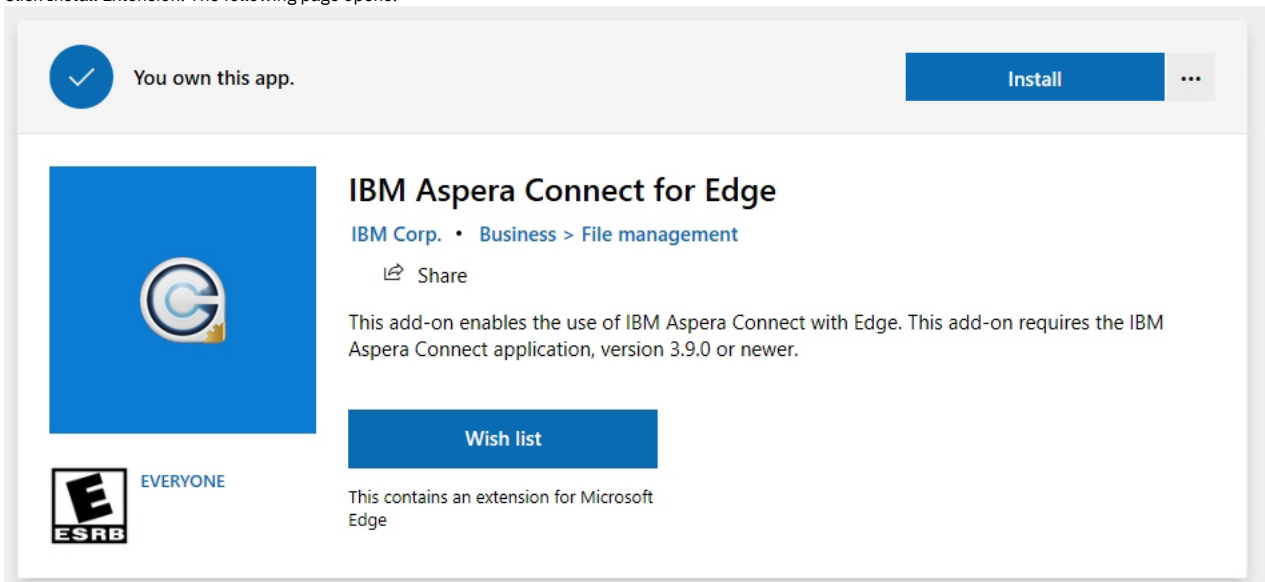
This topic explains how to obtain and add the required IBM Aspera Connect extension to your Edge browser. The extension is required in each browser you use to interact with Aspera on Cloud.

The Connect extensions are specific to the browser; the procedure for adding an extension to a browser is the same regardless of which OS platform that browser is running on. With a guided install, clicking Install Extension opens the extension link for the browser you are using. With a manual install, be sure to download the extension for the browser you intend to use with Connect.

Important: You must install the Connect app once on your computer. You must install the Connect extension for each browser (except Internet Explorer) you use to access Aspera on Cloud.

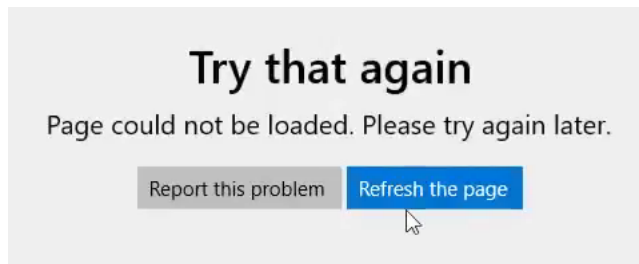
To obtain and install the Connect extension for Edge, follow the procedure below:

1. Click Install Extension. The following page opens:

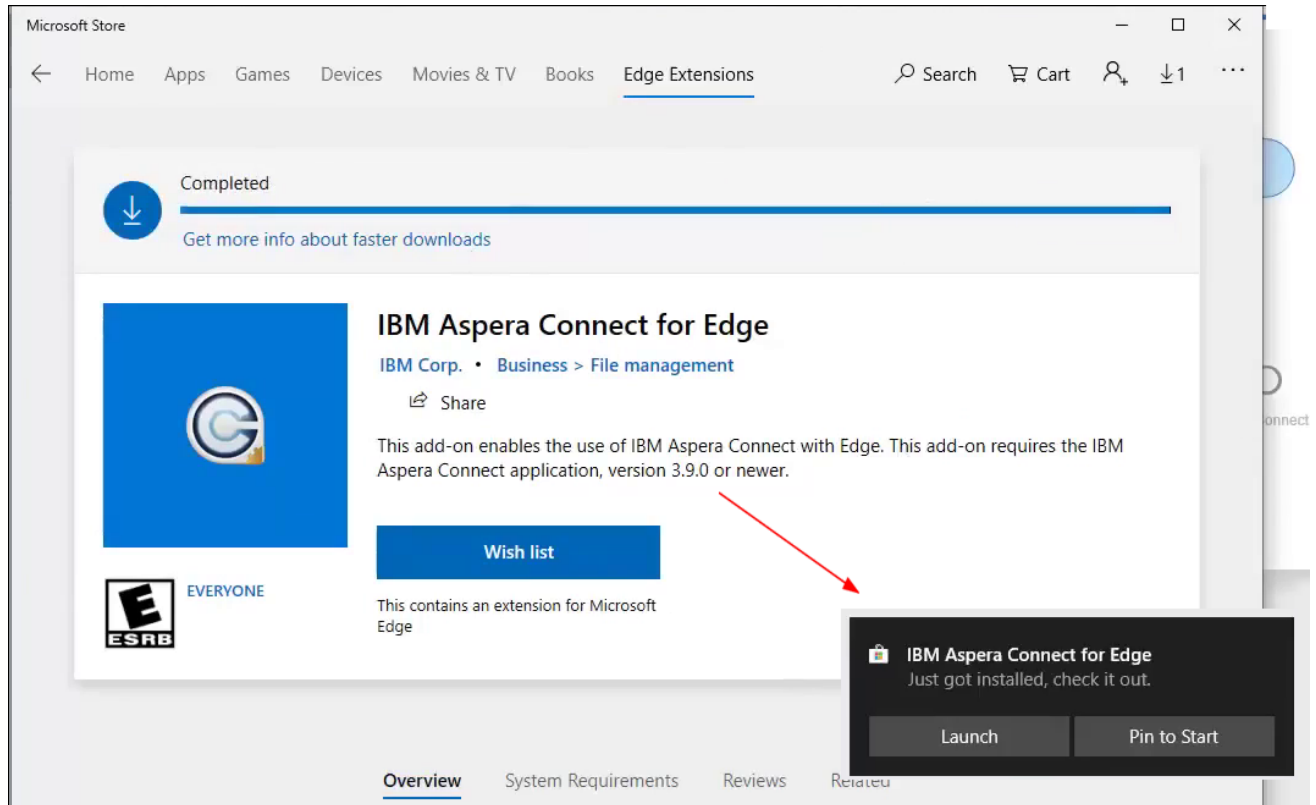


If you are prompted to sign in, you can dismiss the dialog; you are not required to sign in.

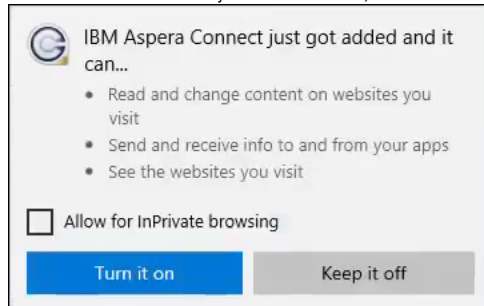
2. Click Install.
If the message below appears, click **Refresh the page**.



A dialog appears indicating the extension is installed.



3. Click Launch. This returns you to the browser, and the following dialog appears:



4. Click Turn it on.

Note: If the Connect extension for Edge is disabled, and you try to use a web app, the launch bar asks you to install the extension. Clicking Install Extension opens the Microsoft app store and shows a Launch button—however, the Launch button will *not* enable the extension. Enable the extension in the settings for Edge.

Installation troubleshooting

Find troubleshooting procedures addressing Aspera Connect installation-specific issues.

- [Overview: Aspera Connect installation troubleshooting](#)
Use this topic to start troubleshooting issues with installing or running IBM Aspera Connect.
- [Windows OS: Error when installing with a non-admin account](#)
Use this procedure to troubleshoot an Aspera Connect installation on a Windows machine when you have a non-admin account.
- [Windows OS: Connectivity issues](#)
Use this procedure to troubleshoot an Aspera Connect installation on a Windows machine when you have connectivity issues.

- [MacOS X: Connectivity issues](#)

Use this procedure to troubleshoot an IBM Aspera Connect installation on MacOS.

- [Linux: AppArmor prevents access to Connect](#)

AppArmor is a Linux security module that uses mandatory access control (MAC) to restrict some applications' system access. It may prevent Connect from running correctly on some Linux systems.

- [Linux: Connectivity issues](#)

Use this topic to troubleshoot connectivity issues for Connect on Linux.

- [Connect prompt continues to appear](#)

Once you download and install IBM Aspera Connect, the Connect installation prompt should no longer appear. However, there are two circumstances in which you may continue to see the installation dialog even though you've already installed Connect.

Overview: Aspera Connect installation troubleshooting

Use this topic to start troubleshooting issues with installing or running IBM Aspera Connect.

For your reference, the Connect installation process performs the following tasks:

- Installs the Connect browser extension.
- Downloads the Connect app.
- Installs the Connect app.

Before troubleshooting, make sure your Connect installation meets the requirements specified in the IBM Aspera Connect [user documentation and release notes](#), particularly with regard to the supported versions of operating systems, browsers, and (if Linux) OpenSSL.

In all cases, the first troubleshooting step is to run Aspera's web-based [Connect diagnostic tool](#) to get a preliminary assessment of your Connect installation. This diagnostic tool does the following:

- Reports the version number of your current Connect installation, if installed.
- Indicates whether your installed version is up to date.
- Checks whether Connect is running.
- Verifies whether your current version of Connect is compatible with your current browser.
- Tests your ports.
- Attempts to perform a test transfer.
- Generates a summary report that you can download and send to IBM Aspera support, if necessary.

Use the other topics in this section to further troubleshoot your Connect installation, according to the OS of your local machine. See also [IBM Aspera Connect common issues](#).

Windows OS: Error when installing with a non-admin account

Use this procedure to troubleshoot an Aspera Connect installation on a Windows machine when you have a non-admin account.

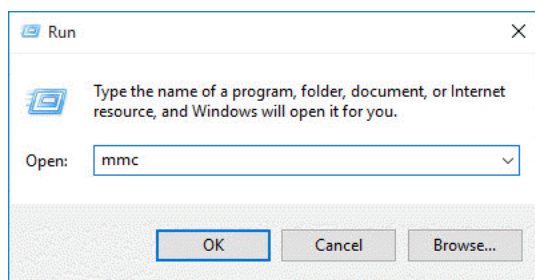
You may encounter an error such as the following (or with similar wording) if you are not an Administrator when executing the MSI installer file.

The system administrator has set policies to prevent this installation.

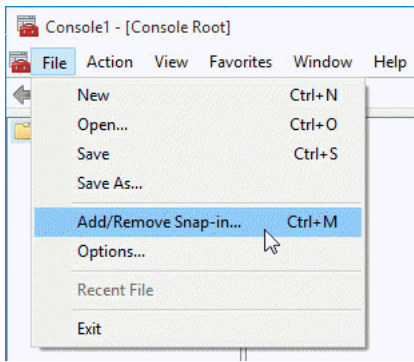
These error messages are due to not having permissions to install an MSI package as a non-admin account. Other than logging in as an administrator to install Connect, you may also ask that your Administrator grant the group policy access for non-admin users to install applications.

The following example shows you how to grant group policy access for non-admins to install software on Windows 2016:

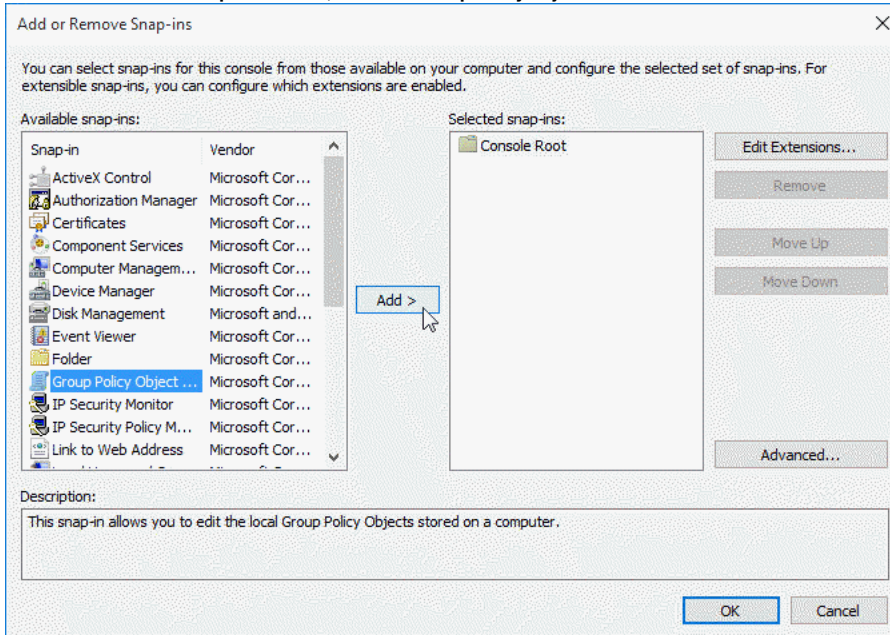
1. Launch the Microsoft Management Console (MMC).
Go to **Start menu > Run**. Enter **mmc** and click **OK** to launch it.



2. Add the Group Policy Object Editor Snap-in.
 - a. In the MMC, go to the toolbar and select **File > Add/Remove Snap-in**:



b. In the **Add or Remove Snap-ins** window, select the **Group Policy Object Editor** and click **Add**:

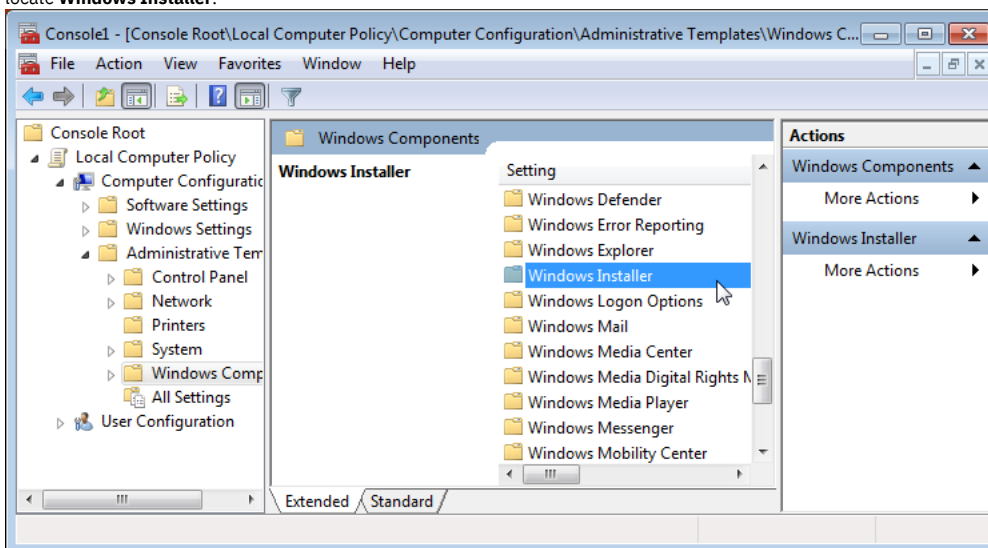


c. In the Select Group Policy Object window (wizard), under Group Policy Object, click **Browse** and select either **This Computer** or specify another computer. When done, click **OK** to return to the wizard window.

d. In the wizard window, click **Finish**. When you are returned to the **Add/Remove Snap-ins** window, click **OK** to save the changes.

3. Grant the Windows installation group policy.

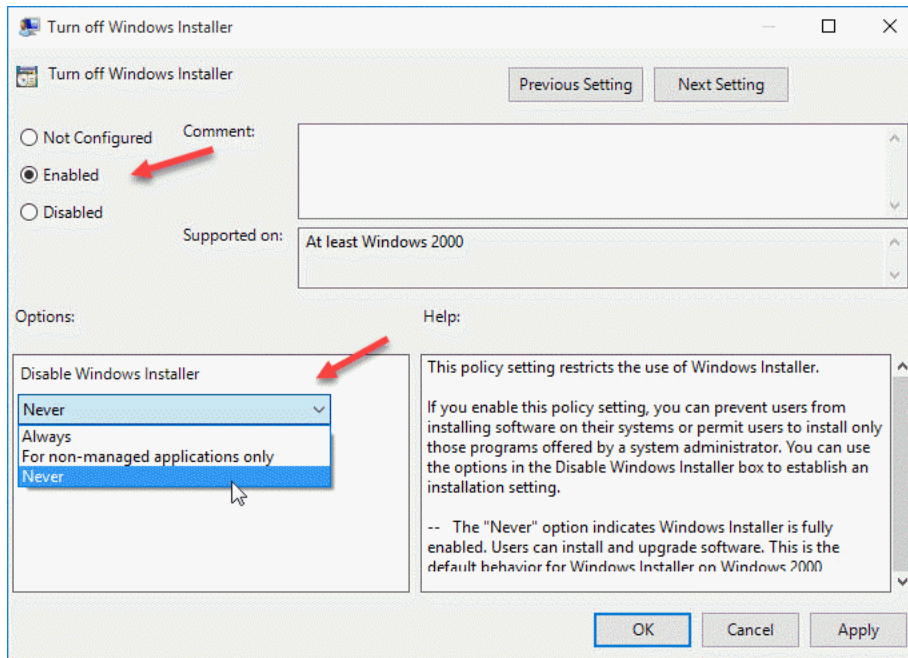
a. In the MMC, navigate into **Console Root > Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components** and locate **Windows Installer**:



b. Double-click **Windows Installer**.

c. In the list that appears, locate **Turn off Windows Installer** and double-click it. The Turn Off Windows Installer window opens.

d. Under the Turn off Windows Installer heading, select **Enabled**. In the Disable Windows Installer box, open the pull-down and select **Never**. When finished, click **OK**:



e. To close the MMC, click **File > Exit**.

f. When prompted to save console settings, click **Yes** to save the settings to a file. When prompted for a .msc filename, click **Save**.

g. Reboot the computer to apply the changes, or execute the following command at a command prompt:

```
> gpupdate /force
```

Windows OS: Connectivity issues

Use this procedure to troubleshoot an Aspera Connect installation on a Windows machine when you have connectivity issues.

SSH connectivity errors: "Timeout establishing connection"

If you receive the error "Timeout establishing connection," the TCP connection between Connect and the server is blocked (error codes 13, 15, or 40 in the log files). To determine the cause, open a Terminal or a Command prompt on the client machine (where Connect is installed). Use **telnet** to test the connection to the server:

```
> telnet server-ip-address 33001
```

where *server-ip-address* is the IP address of the Aspera server (for example, 10.0.1.1) on TCP port 33001 (or the configured TCP port, if other than 33001).

You will receive one of the following errors and can take the appropriate action:

- **"Connection refused"**: The Aspera server is not running the SSHD service. Have your server administrator review the server's SSH service status.
- **"Timeout"**: The client-side firewall is disallowing outbound TCP traffic. Ensure that the client-side firewall allows outbound TCP traffic on port 33001 (or the configured TCP port).

UDP connectivity errors: "Data transfer timeout"

If Connect appears to successfully connect to the server but:

- The transfer progress reads 0%.
- Files appear to be transferred to the destination but are 0 bytes.
- You eventually receive the error "Data transfer timeout."

UDP connectivity is blocked, likely by the firewall configuration (error codes 14, 15, and 18 in the log files). Ensure that the client-side firewall allows outbound traffic on the FASP UDP port (33001, by default) and the server firewall allows inbound traffic on UDP port 33001.

IBM Aspera Connect diagnostic tool

Aspera provides a web-based diagnostic tool that can be useful for identifying connection issues. You can access the tool here:

<https://test-connect.asperasoft.com/>

MacOS X: Connectivity issues

Use this procedure to troubleshoot an IBM Aspera Connect installation on MacOS.

SSH connectivity errors: "Timeout establishing connection"

If you receive the error "Timeout establishing connection," the TCP connection between Connect and the server is blocked (error codes 13, 15, or 40 in the log files). To determine the cause, open a Terminal or a Command prompt on the client machine (where Connect is installed). Use **telnet** to test the connection to the server:


```
$ telnet server-ip-address 33001
```

where *server-ip-address* is the IP address of the Aspera server (for example, 10.0.1.1) on TCP port 33001 (or the configured TCP port, if other than 33001).

You will receive one of the following errors and can take the appropriate action:

- **"Connection refused":** The Aspera server is not running the SSHD service. Have your server administrator review the server's SSH service status.
- **"Timeout":** The client-side firewall is disallowing outbound TCP traffic. Ensure that the client-side firewall allows outbound TCP traffic on port 33001 (or the configured TCP port).

UDP connectivity errors: "Data transfer timeout"

If Connect appears to connect successfully to the server but:

- The transfer progress reads 0%.
- Files appear to be transferred to the destination but are 0 bytes.
- You eventually receive the error "Data transfer timeout."

UDP connectivity is blocked, likely by the firewall configuration (error codes 14, 15, and 18 in the log files). Ensure that the client-side firewall allows outbound traffic on the FASP UDP port (33001, by default) and the server firewall allows inbound traffic on UDP port 33001.

IBM Aspera Connect diagnostic tool

Aspera provides a web-based diagnostic tool that can be useful for identifying connection issues. You can access the tool here:

<https://test-connect.asperasoft.com/>

Linux: AppArmor prevents access to Connect

AppArmor is a Linux security module that uses mandatory access control (MAC) to restrict some applications' system access. It may prevent Connect from running correctly on some Linux systems.

To disable AppArmor, enter the following commands on the affected computer:

```
# /etc/init.d/apparmor stop
# update-rc.d -f apparmor remove
```

Linux: Connectivity issues

Use this topic to troubleshoot connectivity issues for Connect on Linux.

SSH connectivity errors: "Timeout establishing connection"

If you receive the error "Timeout establishing connection," the TCP connection between Connect and the server is blocked (error codes 13, 15, or 40 in the log files). To determine the cause, open a Terminal or a Command prompt on the client machine (where Connect is installed). Use **telnet** to test the connection to the server:

```
# telnet server-ip-address 33001
```

where *server-ip-address* is the IP address of the Aspera server (for example, 10.0.1.1) on TCP port 33001 (or the configured TCP port, if other than 33001).

You will receive one of the following errors and can take the appropriate action:

- **"Connection refused":** The Aspera server is not running the SSHD service. Have your server administrator review the server's SSH service status.
- **"Timeout":** The client-side firewall is disallowing outbound TCP traffic. Ensure that the client-side firewall allows outbound TCP traffic on port 33001 (or the configured TCP port).

UDP connectivity errors: "Data transfer timeout"

If Connect appears to successfully connect to the server but:

- The transfer progress reads 0%.
- Files appear to be transferred to the destination but are 0 bytes.
- You eventually receive the error "Data transfer timeout."

UDP connectivity is blocked, likely by the firewall configuration (error codes 14, 15, and 18 in the log files). Ensure that the client-side firewall allows outbound traffic on the FASP UDP port (33001, by default) and the server firewall allows inbound traffic on UDP port 33001.

IBM Aspera Connect diagnostic tool

Aspera provides a web-based diagnostic tool that can be useful for identifying connection issues. You can access the tool here:

<https://test-connect.asperasoft.com/>

Other Connect troubleshooting

Address the most common issues with Aspera Connect using the articles in this section, including the Connect prompt reappearing, disabling Connect when Aspera HTTP Gateway is enabled, and more.

- [IBM Aspera Connect common issues](#)

Aspera on Cloud requires one of two transfer methods to power high-speed transfers between user desktops and Aspera transfer servers. Users can either download and install Aspera Connect, a free, lightweight, install-on-demand software program; or an admin can configure the IBM Aspera HTTP Gateway and attach it to your Aspera on Cloud organization.

- [Connect prompt continues to appear](#)

Once you download and install IBM Aspera Connect, the Connect installation prompt should no longer appear. However, there are two circumstances in which you may continue to see the installation dialog even though you've already installed Connect.

- [Disable IBM Aspera Connect](#)

If and only if your organization supports IBM Aspera HTTP Gateway, you can disable IBM Aspera Connect transfer client and the default prompt to install Aspera Connect.

IBM Aspera Connect common issues

Aspera on Cloud requires one of two transfer methods to power high-speed transfers between user desktops and Aspera transfer servers. Users can either download and install Aspera Connect, a free, lightweight, install-on-demand software program; or an admin can configure the IBM Aspera HTTP Gateway and attach it to your Aspera on Cloud organization.

Aspera Connect is the default transfer method for Aspera on Cloud and other Aspera web app. However, if your deployment of Aspera on Cloud does not allow users to download and install client software, an admin can configure an alternative transfer method: the [IBM Aspera HTTP Gateway](#). The Aspera HTTP Gateway is a standalone product that uses both HTTP/S and Aspera FASP to complete file transfers.

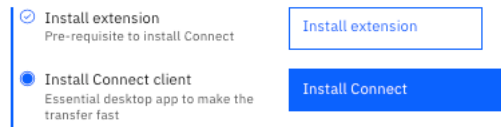
For troubleshooting the installation of IBM Aspera Connect, see [Installation troubleshooting](#).

IBM Aspera Connect powers high-speed transfers between desktops and Aspera servers. Once installed, Connect runs automatically runs in the background for each upload and download you initiate using Aspera on Cloud.

When you first log in to Aspera on Cloud, the app prompts you to download and install Aspera Connect. The installation is an easy, two-step process in most browsers; Aspera on Cloud guides you through the process. The first guidance dialog looks something like this:

Get started now — install the IBM Aspera Connect transfer client.

Install the [IBM Aspera Connect](#) client and the Aspera Connect browser plug-in to enable our signature high-speed file transfer technology.



If you skip installing, you will be able to use IBM Aspera HTTP Gateway for transfers; for faster transfers come back and install Connect.

[I'll skip for now](#)

Install the Connect app once; Install the Connect extension for each browser

There are two components of IBM Aspera Connect; you must install both components as follows:

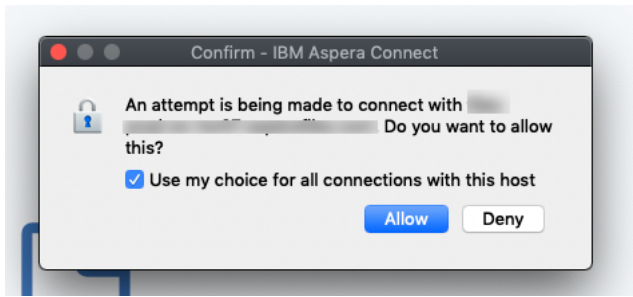
- The Connect application, which you *install once on any computer* you use to access Aspera on Cloud.
- The Connect browser extension, which you *install on each browser* you use to access Aspera on Cloud.

For detailed installation procedures, see [Installation](#).

Allow the connection for each transfer server

When you start a [transfer](#) that requires Connect, Connect displays a dialog requesting permission to connect with the relevant Aspera transfer server.

Connect displays this dialog for the transfer server relevant to each transfer you initiate. Depending on the location of your content, your recipients, and those who send to you, your transfers may involve multiple transfer servers. Connect requests your permission to connect with *each* server. *You must grant permission to allow the transfer to proceed.*



The exact wording of this dialog may vary depending on your browser. But in any case, IBM Aspera highly recommends that you check the option to allow *all connections* with the host, or *always allow*. Otherwise you must manually allow each transfer to initiate. If this dialog displays behind another application window, blocked from your immediate view, you may not realize that Connect is requesting your permission; without your permission the transfer cannot start.

Already installed Connect, but still being prompted?

There are two circumstances in which you may continue to see the installation dialog even though you've already installed Connect:

- There is a new version of Connect available, and the app prompts you to install the upgrade.
In this case, you must download and install the Connect app upgrade. You may or may not need to update your browser extension; the installation process will guide you.
- You have not installed the Connect extension in your current browser.
You may have installed the extension in a different browser, but the extension is required for each browser. In this case, there is no need to reinstall the Connect app, but you must install the browser extension.

To contact your local tech support administrator, click  in the banner and select "Technical support".

Connect prompt continues to appear

Once you download and install IBM Aspera Connect, the Connect installation prompt should no longer appear. However, there are two circumstances in which you may continue to see the installation dialog even though you've already installed Connect.

- There is a new version of Connect available, and the app prompts you to install the upgrade.
In this case, you must download and install the Connect app upgrade. You may or may not need to update your browser extension; the installation process will guide you.
- You have not installed the Connect extension in your current browser.
You may have installed the extension in a different browser, but the extension is required for each browser. In this case, there is no need to reinstall the Connect app, but you must install the browser extension. Find the appropriate installation procedure for your browser among these articles.

If you are not allowed to download and install software, the Aspera on Cloud administrator has configured the IBM Aspera HTTP Gateway for transfers. In this case, you can [disable Aspera Connect](#). Otherwise, you must download and [install the Aspera Connect transfer client](#), and install the Connect browser extension.

Disable IBM Aspera Connect

If and only if your organization supports IBM Aspera HTTP Gateway, you can disable IBM Aspera Connect transfer client and the default prompt to install Aspera Connect.

The Aspera on Cloud administrator may deploy the Aspera HTTP Gateway as an alternative transfer method when some users cannot download and install desktop software like Aspera Connect.

If your organization does not support Aspera HTTP Gateway, you must download and install Aspera Connect to upload from or download to your desktop.

You can transfer among remote sources without either transfer method. For example, go to the Files app, right-click a files or folder to select Move or Copy, then select the destination.

To disable the Aspera Connect transfer client and the default installation prompt, do the following:

1. Click your user image in the upper right to display the menu, then select Account settings.
2. Set the toggle labeled Disable IBM Aspera Connect to On. If you don't see this setting, your organization does not support Aspera HTTP Gateway; you must use Aspera Connect to transfer to and from your desktop.
3. Click Save.

Attach cloud and local storage

Understand how to give your AoC users access to content in your cloud and on-prem servers by connecting them as *nodes* to Aspera on Cloud. Review supported cloud providers and regions. Learn strategies to manage storage available to your users in the Files and Packages apps. Create network policies to manage node access for enhanced security. Create node policies to set encryption ciphers, default target rates, event logging, recursive counts, and more.

- [Node and storage basics](#)
This extensive section details the clouds and regions that Aspera on Cloud supports, along with default and maximum speeds for each. Learn how to manage storage usage; share storage content with your organization workspaces; and create network and node configuration policies. Understand and identify various node types.

- [Attach your own Aspera HSTS node](#)

These articles detail the entire process for attaching (tethering) your own Aspera High-Speed Transfer Server to Aspera on Cloud. Instructions include installing SSL certificates; firewall requirements; when and how to use an HTTPS proxy; configuring your HSTS, Nginx, and high-availability Redis backend. Complete important tasks like marking remote storage; configuring monitoring and metering; backups and restoring; and finally, installing the Preview Maker on your HSTS.

- [Attach your existing cloud storage](#)

Many organizations use Aspera on Cloud to access content in their existing cloud storage. These articles detail the procedures to attach all supported cloud storage types, including additional help in configuring AWS IAM roles and policies and KMS-encrypted AWS buckets.

- [Attaching storage troubleshooting](#)

Troubleshoot common issues with attaching your storage to your Aspera on Cloud organization.

Node and storage basics

This extensive section details the clouds and regions that Aspera on Cloud supports, along with default and maximum speeds for each. Learn how to manage storage usage; share storage content with your organization workspaces; and create network and node configuration policies. Understand and identify various node types.

- [Cloud platforms and regions supported](#)

AoC transfer service supports the following cloud platforms and regions. Expect performance at the default and maximum target rates shown for each.

- [Share a node folder with a workspace](#)

To allow the members of a workspace to use the content in a node attached to your org, an admin must give them access to the content. When you *administratively share* a folder with users, as described in this procedure, all admins in your org can manage the folder access. This shared management ability is typically preferable to having one admin user share a folder as an individual user; in such case, only that individual admin can revoke or change access permissions.

- [Managing storage usage](#)

There are several strategies you can use to manage storage. Some strategies are based on how you configure your Aspera on Cloud organization. Some are based on how to configure the storage you attach to your organization.

- [Creating network policies](#)

You can configure policies that govern how Aspera on Cloud transfer nodes interact. Once you configure such a policy, you can apply it to one or more nodes in your AoC organization.

- [Creating node configuration policies](#)

A configuration policy applied to a node or to an individual access key allows the AoC administrator to apply certain settings that were formerly configurable only through `aspera.conf` directly on the node.

- [Deleting a node](#)

Use caution when deleting a node attached to your Aspera on Cloud organization.

- [Node types in Aspera on Cloud](#)

An IBM Aspera *node* is a computing machine (physical, virtual, or container) on which IBM Aspera High-Speed Transfer Server (HSTS) software is installed. Your Aspera on Cloud subscription comes provisioned with one node, managed by IBM Aspera and connected to storage in IBM Cloud. You can connect additional storage to your AoC organization, either by attaching your own IBM Aspera HSTS node or cluster, or by using Aspera Transfer Service (ATS), the Aspera-managed auto-scaling transfer cluster.

- [Identifying a node type](#)

Use the URL associated with a node to determine the node type.

Cloud platforms and regions supported

AoC transfer service supports the following cloud platforms and regions. Expect performance at the default and maximum target rates shown for each.

IBM Cloud (12)

Target performance rates for Aspera-managed auto-scale transfer clusters (ATS)

- Default: 700 Mb
- Maximum:
 - 2000 Mb: Washington, Toronto, London, Dallas
 - 1250 Mb: All other regions

IBM Cloud Cross-Regional

- us-geo: Dallas, Washington
- eu-geo: Amsterdam, Frankfurt
- ap-geo: Tokyo, Seoul, Hong Kong

IBM Cloud Regional

- Dallas (us-south)
- Frankfurt (eu-de)
- London (eu-gb)
- Sydney (au-syd)
- Tokyo (jp-tok)
- Toronto (ca-tor)
- Washington, D.C. (us-east)

IBM Cloud Single Site

- Amsterdam (ams03)
- Toronto (tor01)

Amazon Web Services (8)

Target performance rates

- Default: 700 Mb
- Maximum: 3000 Mb

Regions

- Frankfurt (eu-central-1)
- Ireland (eu-west-1)
- London (eu-west-2)
- Virginia (us-east-1)
- Oregon (us-west-2)
- Sydney (ap-southeast-2)
- Tokyo (ap-northeast-1)
- Ohio (us-east-2)

Microsoft Azure (4)

Target performance rates

- Default: 700 Mb
- Maximum: 3000 Mb

Regions

- Central United States (ats-azure-centralus)
- West Europe (westeurope)
- West United States (ats-azure-westus)
- London (ats-azure-uksouth)

Google Cloud Services (2)

Target performance rates

- Default: 400 Mb
- Maximum: 2000 Mb

Regions

- Iowa (us-central1)
- Los Angeles (us-west2)

Retrieve public IP addresses

To retrieve the public IP addresses for the transfer service for allow listing in your firewall rules, use a curl request or point your browser to access the following endpoints:

- IBM Cloud: <https://ats.aspera.io/pub/v1/servers/softlayer>
- Amazon S3: <https://ats.aspera.io/pub/v1/servers/AWS>
- Microsoft Azure: <https://ats.aspera.io/pub/v1/servers/AZURE>
- Google Cloud Services: <https://ats.aspera.io/pub/v1/servers/Google>

Share a node folder with a workspace

To allow the members of a workspace to use the content in a node attached to your org, an admin must give them access to the content. When you *administratively share* a folder with users, as described in this procedure, all admins in your org can manage the folder access. This shared management ability is typically preferable to having one admin user share a folder as an individual user; in such case, only that individual admin can revoke or change access permissions.

Use this procedure to give users in the Files application:

- Shared access to content in your cloud or on-prem storage.
- A folder in which they can collaborate on content according the permissions you set.

Once you share the folder using this procedure, users see it on the top level of their Files app.

For each folder you share, you set permissions for each user and group you share with. These permissions determine the actions that users can take on the folder contents. For details, see [Content Permissions](#).

This procedure allows you to share one folder at a time with one or more members of a single workspace. To share multiple folders, or to share a folder with users in multiple workspaces, repeat the procedure

Procedure

Note: To complete this procedure, you need the secret of the node containing the folder you want to share.

1. Go to Workspaces > *workspaceName* > Applications > Files app > Shared folders > Create new.
2. Do one of the following:
 - Enter the node secret and click Log in.
 - If you have a different access key for this node, click **Use custom access key**, enter the key and associated secret, then click **Log in**.
3. (Optional) To create a new folder on the node, do the following:

- a. Click Create folder.
 - b. Enter a name for the new folder and click Create.
4. From the list of folders that displays, select the folder to share by clicking the option button on the folder row.
If required, you can click a folder name to drill into it. Go back up a level using the breadcrumb list at the top of the modal.
5. (Optional) To display a different name for the folder to the workspace users (perhaps a name that may be most meaningful to them), enter the desired name in the Display name text box.
6. Click Submit.
7. To give all members of the workspace access to this folder, click Add all workspace members.
 - a. Set the access permission level for these users.
 - b. If desired, add other members you want to access this folder at the permission level you set.
 - c. Click Add.
8. To give specific workspace members access to this folder, click Add member.
 - a. Set the access permission level for these users.
 - b. Enter the names of workspace members which whom to share this folder at this permission level.
 - c. Click Add.
9. To change a user's access to the shared folder, click the user row to open the record, adjust permissions as required, then click Save.
10. To remove a user's access to the shared folder, select the check box to the left of the user row and click Delete.

Note:

When new members join the workspace Files app, they can see and access shared folders as follows:

- Folders shared with the entire workspace.
- Folders shared with the new member as an individual or as a group member.

Add a member to an existing shared folder

1. Go to **Workspaces > workspaceName > Applications > Files app > Shared folders**.
2. Right-click the intended folder to see the current member list.
3. Do one of the following:
 - Enter the node secret and click Log in.
 - If you have a different access key for this node, click **Use custom access key**, enter the key and associated secret, then click **Log in**.
4. Click Add member.
5. Select the access permission for this new member.
6. Enter the member name.
7. Repeat steps 5 and 6 for additional new members.
8. Click Add.

Node access for workspace managers

1. Go to Workspaces > workspaceName > Profile > Node access for workspace managers.
2. Click Add.
3. In the Name drop down, select the node you want to give access to.
4. In the Access key field, enter the access key provided by your administrator.
5. In the Secret field, enter the secret associated with the access key.
Click the eye icon to show or hide the secret as you type.
6. From the Node owners drop down, select who can manage the node:
 - a. Only ATS admins: Only ATS administrators can manage the node.
 - b. All admins: All administrators can manage the node.
- Note: Node owners can browse and manage this node without the need of an access key.
7. Click Log in to save the configuration and establish node access.
8. Click Cancel if you do not want to save the configuration and exit.

Managing storage usage

There are several strategies you can use to manage storage. Some strategies are based on how you configure your Aspera on Cloud organization. Some are based on how to configure the storage you attach to your organization.

To understand storage in your subscription and billing, see [Manage storage in your subscription](#).

Bring your own storage

You can attach your own storage to your Aspera on Cloud organization.

If your existing storage is in [a supported region](#) in IBM Cloud, AWS S3, GCS, or Azure, you can access it through Aspera on Cloud.

Attach your storage using the procedures listed in this document: [Attaching Cloud Storage to Your AoC Organization](#). Then, when you [create a new workspace](#), select a location on your attached storage for the content in the workspace Files and Packages apps. These storage costs are then part of your normal cloud bill. In this scenario, you can also configure lifecycle policies from your cloud provider to remove files automatically. For more details and strategies, see the following section, "Configure Your Cloud Directory Structure".

Configure your cloud directory structure

You can configure your directory structure to take maximum advantage of cloud provider lifecycle policies to manage your storage.

As a bit of background, the Aspera on Cloud default directory structure allows users to proceed as quickly as possible to efficient usage and collaboration. The default directory structure is as follows:

```

'''
.
/
  <workspace_id>/
    home/
      <user_email_address + user_id>
        foo/
          bar
    packages/
      <package_id>/
        foo/
          bar
'''

```

However, in cloud object storage, file storage is a large, flat directory with file name prefixes that Aspera and other software use to assume the intended directory structure. Cloud object storage for an Aspera workspace is as follows:

```

'''
.
/<workspace_id>/
/<workspace_id>/home/
/<workspace_id>/home/<user_email_address + user_id>/
/<workspace_id>/home/<user_email_address + user_id>/foo/
/<workspace_id>/home/<user_email_address + user_id>/foo/bar
/<workspace_id>/packages/
/<workspace_id>/packages/<package_id>/
/<workspace_id>/packages/<package_id>/foo/
/<workspace_id>/packages/<package_id>/foo/bar
'''

```

In cloud object storage, directories are objects subject to deletion through lifecycle policies. It's vital to configure such policies so as not to delete folders that Aspera on Cloud requires for a workspace to function properly. For example, if you delete `/<workspace_id>/packages/`, package sending would be impossible. If you delete a user's home folder, `/<workspace_id>/home/`, that user would not have a working Files app.

A useful strategy is to centralize your files so that you can configure lifecycle policies with a prefix that will not disrupt the required folder structure.

Consider the following structure:

```

'''
.
/
  /Shared/
    foo/
      bar
  <workspace_id>/
    home/
      <user_email_address + user_id>/
        Shared.asp-link/
'''

```

Such a structure centralizes the content your users need in the `/Shared/` directory, outside the workspace folder.

To centralize your workspace content in the `/Shared/` directory, you can [share folders with workspace members using the Admin app](#) (rather than the Files app). This allows users to collaborate in folders that are not in the workspace structure. When you share from the Admin app, workspace members access shared content by means of *symlinks* that display in their Files app home folder. In your cloud storage, these symlinks appear as very small files with the suffix `.asp-link`.

When you set cloud lifecycle policies, apply deletion only to files with the prefix `/Shared/`; this configuration prevents deletion of directories that disrupt Aspera on Cloud workspace operations.

Prevent users from uploading content to any other workspace area by configuring the Files app home folder to be read-only; for details and a procedure, see the following section, "Centralize Storage in the Files App".

Configure file deletion policies

You can create policies to permanently delete files and folders when they reach a configured age. If the policy deletes all files in a given folder, the policy deletes the folder as well. Existing empty folders are not deleted. Shared folders and folders with public links are never deleted by a file deletion policy, though the content they contain may be deleted.

Attention:

- **For ATS nodes:** If there are additional nodes in the same bucket, the same file deletion policy applies to those nodes as well.
- **For tethered nodes:** The policy applies only to the specific node that you are creating the policy for. Beware that if there are other nodes that share the same storage and bucket path, this policy is going to affect those as well. This could lead to content being deleted from other nodes that the policy was not intended to.

Note: You can set file deletion policies on buckets in AWS, S3, CGCS and Microsoft Azure storage.

1. Go to Nodes and storage > Nodes. Click the row of the intended node.
2. Go to Profile > File deletion policy.
3. Click the toggle to On.
4. Set the deletion age in days. Valid values are 7 to 3650 days. The deletion job runs daily. A timer is set to start 24 hours after the last run. It does not have a set start time, as it runs depending on when it was last completed.

Note: The time the job takes to run depends on how large the bucket is.

For example, if you configure the deletion age to be 90 days, the policy will:

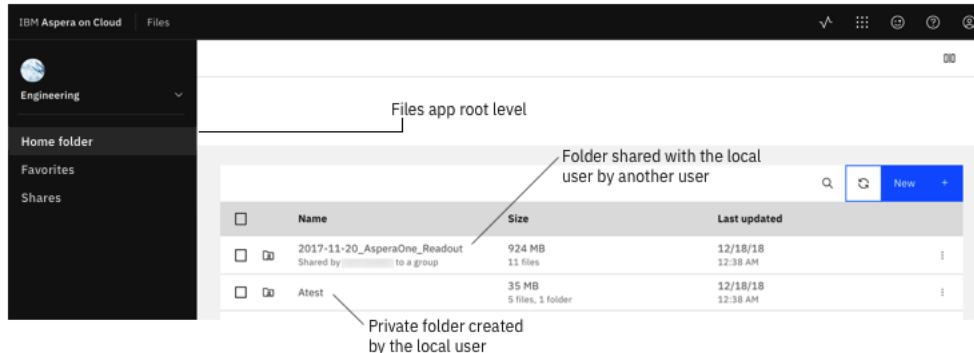
- Permanently delete files in that bucket 90 days after their creation. This deletion age applies to existing files that are older than the deletion age, as well as to new files when they reach the configured deletion age.
- Permanently delete folders that are emptied by the deletion job.
- Not delete empty folders that were not affected by the policy.
- Not delete shared folders or folders with public links, even if they are emptied by the deletion job.

5. Click Save to activate the file deletion policy.

Centralize storage in the Files app

By default, users can create folders and upload files in the root level of their Files app. Others cannot see that content until the user shares it with them.

This root level is also called the *home folder*. In the Aspera on Cloud interface, this area displays the label All files. The home folder includes folders created by the local user at the root level.



Note: Admins can view and manage content in Files home folders if they have the node secret. See the section "Managing User Storage in the Workspace" below in this article. Admins can also access the cloud storage directly if they have the proper credentials.

But in any given workspace, you can prevent members from uploading content to the root level of their Files app. This restriction ensures that:

- You can readily manage storage by applying cloud storage lifecycle policies to centralized storage in folders outside the workspace directory structure.
- The storage your organization pays for contains only the contents you intend.
- The transfer volume charged to your organization supports your corporate, team, or project mission, rather than being used for unrelated storage by individual members.

Whether or not you configure this restriction, you can [share folders with members using the Admin app](#) and grant them permission to view, upload to, or download from those folders. In this way, members can collaborate in centralized folders that you can readily monitor and manage, eliminating excess storage.

To restrict all users in a given workspace from uploading to and creating new folders in the root of their Files app, do the following:

1. Go to Workspaces > *workspace_name* > Profile > Node.
2. To restrict users of this workspace from creating new folders and from uploading content to the root level of their Files app, select the check box Workspace members cannot upload to workspace root level.
3. Click Save.

To exempt specific users from the workspace restriction, do the following:

1. Go to Workspaces > *workspace_name* > Member > *memberName* > Allow upload.
2. Select the check box labeled Allow this user to upload to root level of workspace.
3. Click Save.

Delete packages

You can manually delete package content when it is no longer required.

Note: You can also configure policies that automatically delete packages when certain time-based or event-based thresholds occur; see [Content Expiration Policies](#). Deleting package content does not delete the package listing or package details -- only the assets in the package. You can still access details, including metadata, by clicking the package row and selecting More detail or Metadata.

There are two ways to accomplish this task:

- Through Organization > Activity.
- Through Nodes > Workspaces > Packages.

Through Organization > Activity

Note: The Activity page in the Organization section or in the Workspaces section of the Admin app is different than the AoC Activity application that can be made available to users with an Advanced tier subscription to Aspera on Cloud.

1. Go to the Activity page:
 - Go to Organization > Activity.
 - Go to Workspaces > *workspaceName* > Activity.
2. The table labeled Recent transfer activity displays recent package transfer event. Click View all in the lower left of the table to display an expanded, filterable list.
3. To delete a package, do the following:
 - a. Search or filter for the intended package, then click the package row to view details.
 - b. Click the Actions (three dots) icon in the upper right of the package details panel, select Delete, then confirm Delete.

Through Nodes > Workspaces > Packages

1. Go to Nodes > *nodeName*.
2. In the Node access window, enter the node secret and click Log in.
3. Click Workspaces, then click the row of the intended workspace.
4. Click Packages.

5. Browse, filter, or search for the intended package.
6. To see package contents, click the package row to open the details panel.
7. To delete package contents, click the Actions (three dots) menu at the top right of the details panel; select Delete, then confirm.

Manage folders on a node

You can browse the node to create new folders and to inspect, rename, and delete content as required.

Note: You need the node secret or a valid custom access key/secret to complete this procedure.

Important: Use caution -- these actions can impact critical application files.

To monitor and manage general storage usage for a given node, do the following:

1. Go to Nodes > *nodeName* > Browse.
2. In the Node access window, enter the node secret and click Log in.
3. Click Storage.
4. Click a folder row to drill into it.
5. To delete a folder on the node, browse to the intended folder, right-click the folder row, and select Delete.
6. To rename a folder on the node, browse to the intended folder, right-click the folder row, and select Rename.
7. To create a new folder on the node, click Create folder, name the new folder, and click OK.

Manage user storage in the workspace

In a workspace with the Files app enabled, each standard user has their own root folder, containing the files and folders they upload and the folders shared with them by administrators or by other users.

In a workspace with the Packages app enabled, each standard user has their packages sent and received in this workspace.

As an administrator, you can do the following:

- Files app
 - Delete the entire Files root folder of a deleted user.
 - Browse, rename, or delete individual items within a user's Files app.
 - Restrict users from uploading to the root level of their Files app.
- Packages app
 - Delete all packages for a user in a workspace.
 - Delete specific packages.
 - Delete contents from within a package.
 - Configure package expiration policies. See [Content Expiration Policies](#) for details and [Configuring the Packages Application](#) for procedures.

Note: You need the node secret or a valid custom access key and secret to complete this procedure. In this view, workspaces are identified by workspace ID; packages are identified by package ID.

To manage user workspace storage, do the following:

1. Go to Nodes > *nodeName* > Browse.
2. In the Node access window, enter the node secret and click Log in.
3. Click Workspaces folder.
4. Browse or filter for the intended workspace (by workspace ID), then click the row to open the workspace record.
5. To manage content in a user's Files app:
 - a. Click home; the list of users in the workspace displays, listed by registered email address.
 - b. Browse or filter for the intended user; click the user row to display the content in that user's Files app.
Note: Folders shared with this user appear with the link icon; folders uploaded by this user appear with the folder icon.
 - c. If desired, sort the list by name or size by clicking the row heading.
 - d. To rename a folder, right-click the folder row and select Rename.
 - e. To unshare a shared folder, right-click the shared folder row and select Delete.
 - f. To delete an unshared folder or content within it, go to the content to delete, right-click Delete.
6. To manage content in a user's Packages app:
 - a. Click packages ; the list of packages in the workspace displays, listed by package ID.
 - b. To delete, select one or more packages, or click the package row to display its contents and select one or more items, then click Delete.

Creating network policies

You can configure policies that govern how Aspera on Cloud transfer nodes interact. Once you configure such a policy, you can apply it to one or more nodes in your AoC organization.

You can apply either or both of these policies to a given Aspera on Cloud node:

- Require transfer initiation
- Access control

Require transfer initiation

You can create and apply a policy that requires a node to initiate transfers. This is particularly useful when firewall settings block incoming connections but allow outbound connections.

Typically, a transfer starts on the node hosting the files or folders to be transferred. But you can apply a policy that requires a node to initiate the transfer, regardless of where the files reside. If the files reside on the initiating node, the initiating node issues a 'send' transfer to another node, pushing the files to the peer. If the files reside on the other node, the initiating node issues a 'receive' transfer to the peer node, pulling the files from the other.

If you do not apply a transfer initiation policy, a node can both receive and initiate transfers.

You can configure the following transfer initiation restrictions:

- **With all nodes:** A node with this policy applied always initiates transfers with *all* other nodes.
- **With the following nodes:** A node with this policy always initiates transfers with the other nodes *that you specify*. With nodes not specified, the node can initiate or receive the transfer, depending on where the files to transfer reside.

Access control

You can create and apply a policy that restricts a node from transferring with specified other nodes.

Nodes without access control can participate in transfers to or from any transfer node attached to the AoC organization.

- **Allow transfer with the following nodes** List specific nodes with which transfers are allowed. This setting is similar to a whitelist. For example, if you select Allow and list Node1 and Node5, the node with this policy supports transfers with *only* Node1 and Node5. User requests to transfer to or from nodes not listed are denied.
- **Disallow transfers with the following nodes** List specific nodes with which transfers are prohibited. This setting is similar to a blacklist. For example, if you select Disallow and list NodeA and NodeC, the node with this policy supports transfers with any node *except* NodeA and NodeC. User requests to transfer files and folders to or from NodeA and NodeC are denied; transfers with nodes not listed are allowed.

Create a network policy

To create a new network policy, do the following:

1. In the Admin Management console, click **Nodes and Storage > Node policies > Create new**.
2. Enter a name for this policy; the name must be unique across the Aspera on Cloud organization.
3. To create a policy that controls which node initiates a transfer, do the following:
 - a. Select the check box labeled **Require transfer initiation**.
 - b. To require this node to initiate transfers with *all* peer nodes, select **with all nodes**.
 - c. To require this node to initiate transfers with *specific* peer nodes, select **with the following nodes**; then enter the names of configured peer nodes with which this node must initiate transfers.
A node governed by this policy can still accept *or* initiate transfers with nodes you don't list.
4. To configure access restrictions, do the following:
 - a. Select the check box labeled **Access control**.
 - b. To allow a node to transfer with only specific nodes, select **allow transfer with the following nodes**; then list the allowed nodes. This is similar to creating a 'whitelist' of nodes.
 - c. To prevent a node from transferring with specific nodes, electing **disallow transfer with the following nodes**; then list the restricted nodes. This is similar to creating a 'blacklist' of nodes.
5. Click Save.

Apply this policy to a node attached to your organization.

Applying a policy to a node

To apply a network policy to a node, do the following:

Note: You need the [node secret](#) to complete this procedure.

1. Go to **Nodes and Storage**.
2. Search or browse for the intended node; click the node row and enter the node secret to open the node record.
3. Click Network policy field to display the configured policies, then select the intended policy.
4. Click Save.

Creating node configuration policies

A configuration policy applied to a node or to an individual access key allows the AoC administrator to apply certain settings that were formerly configurable only through `aspera.conf` directly on the node.

For details on `aspera.conf`, see the [IBM Aspera High-Speed Transfer Server Admin Guide](#).

If you configure only some of the available fields in a policy, the unconfigured fields in your policy are set to null on the nodes to which you apply your policy. When you delete a policy, all fields on the node are returned to the null setting. However, note that there are two exceptions to this rule: the "Activity event logging" field and the "Recursive count" field. If your policy does not configure these settings, they remain enabled on the node when you apply your policy; when you delete your policy, these same two fields remain enabled on nodes to which you had previously applied your now-deleted policy.

Procedures

Note: This procedure allows you to create a configuration policy; you must then apply the policy to the intended node in [a separate procedure](#).

To create a new configuration policy, do the following:

1. Go to **Nodes and Storage > Node policies > Configuration policies > Create new**.
2. Give the policy a name.
3. Choose the encryption cipher to be applied to transfers to and from this node.
This setting implies a negotiation between source and destination nodes and depends on settings at both; because of this, the parameter you choose here is not guaranteed. Note also that stronger encryption levels result in slower transfers.
4. Configure the default target transfer rate for transfers to and from this node.
5. Click Advanced to display additional settings (note that these settings apply only on nodes running IBM Aspera High-Speed Transfer Server software version 3.8.0 or higher):

a. In the "Transfer aggressiveness policy" field, configure the aggressiveness of transfers that are authorized by this node in claiming available bandwidth. Valid values are integers from 1 to 100.

On an Aspera High-Speed Transfer Server, this value is configured in `access_key_config.json`. In that file, the parameter name is *aggressiveness*, and valid values are 0.00 to 1.0. This parameter applies when the server is configured with a Vlink running concurrent transfers. The aggressiveness setting determines how much of the available bandwidth the transfer can use. For example, a setting of 0.5 means the transfer gets 50% of available bandwidth. If no parameter is set, all concurrent transfers get an even share of available bandwidth.

A setting of 50% in the UI translates to 0.5 for the transfer server. The transfer server node must be running software version 3.8.0 or higher to support this parameter.

b. Select Activity event logging to allow the Node API to query transfers that are associated with this node through the `/events` endpoint. The node configuration overrides the server configuration and must be enabled for event reporting to Aspera on Cloud.

You must select this check box when an AoC workspace or shared folder is located on this node. If you deselect this check box, the node does not report events to AoC; sent packages become stuck in 'pending' status.

c. Select Recursive count to enable recursive counts on this node.

You must select this check box when an AoC workspace or shared folder is located on this node. If you deselect this check box, the node does not report events to AoC, and sent packages become stuck in 'pending' status.

d. Select AEJ logging to enable AEJ (Aspera Event Journal) logging.

You must select this check box when an AoC workspace or shared folder is located on this node. If you deselect this check box, the node does not report events to AoC, and sent packages become stuck in 'pending' status.

6. To use the pagination setting on the transfer server when browsing content in storage, set the toggle labeled Paginated browsing to On.

The pagination facility, when enabled, returns an internally controlled number of items from the folder being browsed, whether the folder is in cloud storage or on your own tethered node. The paginated response help avoid the time-out issue that is common for large folders in cloud storage.

Note that any paginated return of folder contents does not support retrieval of sorted content. This means that lexicographical sorting of content occurs only within the returned batches.

Note: The transfer server must be running IBM Aspera HSTS v4.0 or higher. See the [IBM Aspera High-Speed Transfer Server Admin Guide](#) for details.

7. To delete skipped files from the source folder after a "move" transfer (as opposed to a "copy" transfer) completes, check the box labeled Remove skipped files.

After a transfer completes, Aspera on Cloud deletes transferred files from the source folder. However, files in the source folder that already exist in the destination folder are not transferred: they are skipped. Select this option to include these skipped files in the automatic deletion. Otherwise, skipped files remain in the source folder.

8. Click Save.

To apply an existing configuration policy to a node, do the following:

9. Go to Nodes and Storage.

10. Search or browse for the intended node; click the node row to open the node record.

11. In the "Configuration policy" field, click the downward caret to display the configured policies, click to select the intended policy.

12. Click Save.

Deleting a node

Use caution when deleting a node attached to your Aspera on Cloud organization.

CAUTION:

1) When you delete a *transfer service (ATS) node*, you automatically and permanently delete all the application data from the Aspera on Cloud organization, along with the associated access key (if used). This operation does not delete the data on the node.

2) When you delete an *Aspera-managed or subscriber-managed tethered node*, you permanently delete all the application data from the Aspera on Cloud organization; this operation does not delete the data on the node itself. You have the option to retain the access key (for example, when the key is being used by another application).

See [Node types in Aspera on Cloud](#) for details.

Delete a transfer service node

1. Go to Nodes and storage > Nodes.
2. Hover over the row of the node to delete to display the Actions (three dots) icon that appears on the right.
3. Click Delete to confirm.

Delete an Aspera-managed or subscriber-managed tethered node

1. Go to Nodes and storage > Nodes.
2. Right-click the row of the node to delete; select Delete.
3. To delete the access key associated with this node, do the following:
 - a. Select Delete access key.
 - b. Enter the Node API username and password associated with this node.
4. Click Delete to confirm.

Node types in Aspera on Cloud

An IBM Aspera *node* is a computing machine (physical, virtual, or container) on which IBM Aspera High-Speed Transfer Server (HSTS) software is installed. Your Aspera on Cloud subscription comes provisioned with one node, managed by IBM Aspera and connected to storage in IBM Cloud. You can connect additional storage to your AoC organization, either by attaching your own IBM Aspera HSTS node or cluster, or by using Aspera Transfer Service (ATS), the Aspera-managed auto-scaling transfer cluster.

The vast majority of Aspera on Cloud (AoC) features are supported on all node types. In the rare cases when node type is relevant, the related Help Center article makes node-type support clear.

Aspera Transfer Service (ATS)

Managed by IBM Aspera, ATS is an auto-scaling, multi-tenant cluster of IBM Aspera High-Speed Transfer Servers (HSTS).

Use ATS as a transfer engine to connect your own cloud object storage to your AoC organization. IBM Aspera runs ATS in all the major cloud platforms; your storage must be in a [region supported by ATS](#). While the cloud storage is associated with your cloud account, the ATS engine is associated with *IBM Aspera's* cloud account.

Each AoC organization has one built-in ATS transfer cluster provisioned in IBM Cloud during the subscription process. In addition to this built-in transfer cluster, you can attach as many ATS clusters to your AoC organization as necessary to make your cloud-based content available to AoC users.

- **Usage accrual**
All transfers using an attached ATS cluster accrue to your AoC subscription usage allotment. ATS automatically sends usage records to the [AoC Activity app](#) to give you monitoring and reporting capabilities. ATS also send usage records to the IBM Aspera billing app, to be reported on the AoC [Subscription management](#) page and billed to your account.
- **Transfer rate**
Each cloud platform has default and maximum target performance rates; see [Cloud Platforms and Regions Supported](#).
- **Attach your cloud storage to your AoC organization**
 - AWS: [Attach an AWS S3 bucket](#).
 - IBM Cloud: [Attach your IBM Cloud storage](#).
 - Microsoft Azure Blob: [Attach your Azure Blob storage](#).
 - Microsoft Azure Files: [Attach your Azure Files storage](#)
 - Google Cloud Storage: [Attach your Google storage](#)

To identify the type of a particular node attached to your AoC organization, see [Identifying a node type](#).

Subscriber-managed tethered node or cluster

A tethered node is a subscriber-managed instance of IBM Aspera HSTS installed on a physical machine on your customer premises or on a virtual machine in the cloud or on your customer premises, attached to Aspera on Cloud.

A tethered cluster, similarly, is a subscriber-managed auto-scale cluster of IBM Aspera HSTS. The tethered cluster can be an array of physical or virtual machines on your premises or in the cloud.

You can tether any number of your HSTS nodes to any AoC subscription that includes a pre-committed transfer volume. You can tether one HSTS node to a Pay-as-You-Go subscription.

Other Aspera products like Console, Faspex, and Shares can also access and use your tethered nodes and cluster, as can other computing resources like transcoders.

- **Usage accrual**
If your tethered node or cluster is enabled by:
 - An entitlement, transfer usage accrues to your AoC subscription.
 - A license, transfer usage does *not* accrue to your AoC subscription.
- **Transfer rate**
If your tethered node or cluster is enabled by:
 - An entitlement, transfer rates depend on your server settings and on available bandwidth in the network.
 - A license, the maximum bandwidth allowed by the license governs transfer rate.
- **Tether your Aspera HSTS node or cluster to your AoC organization**
You must first configure your node or cluster specifically for this purpose. Once configured, you can tether or attach the node or cluster. See [Tether Your Aspera Transfer Server to Aspera on Cloud](#).

To identify the type of a particular node attached to your AoC organization, see [Identifying a node type](#).

Identifying a node type

Use the URL associated with a node to determine the node type.

To identify [the type of a particular node](#) attached to your AoC organization, do the following:

1. Go to the Nodes listing at Admin > Nodes and storage > Nodes.
2. Examine the URL listed with each node in the Storage Provider column.
 - A URL that conforms to this format identifies an **Aspera-managed auto-scale cluster (ATS)**.
`ats-<xxx-yyy-n>.aspera.io`
 - When a URL that does not conform to an Aspera-managed auto-scale cluster format, it is identified as a **customer-managed tethered node or cluster**.

Attach your own Aspera HSTS node

These articles detail the entire process for attaching (tethering) your own Aspera High-Speed Transfer Server to Aspera on Cloud. Instructions include installing SSL certificates; firewall requirements; when and how to use an HTTPS proxy; configuring your HSTS, Nginx, and high-availability Redis backend. Complete important tasks like marking remote storage; configuring monitoring and metering; backups and restoring; and finally, installing the Preview Maker on your HSTS.

- [Tether Your Aspera Transfer Server to Aspera on Cloud](#)
To attach your own user-managed High-Speed Transfer Server (HSTS) to Aspera on Cloud, you must configure it as a *tethered node*. This article covers prerequisites and provides a map of the process. Linked articles describe the configuration steps in detail.
- [Installing SSL certificates for tethered nodes](#)
The first step in tethering your IBM Aspera High-Speed Transfer Server (HSTS) node to your Aspera on Cloud organization is to install SSL certificates on the node.
- [Firewall requirements for tethered nodes](#)
Administrators must configure the proper firewall settings to enable high-speed transfers using Aspera on Cloud.
- [Using an HTTPS proxy for outgoing ALEE and AEJD traffic from your tethered node](#)
This is an optional step in the process of tethering your IBM Aspera HSTS node to your AoC organization. To use an HTTPS proxy for outgoing ALEE (Aspera License and Entitlement Engine) traffic between your tethered node and Aspera on Cloud (optional), you must add options to the JVM_OPTIONS assignment.
- [Configure your transfer server as a tethered node](#)
The next step in tethering your IBM Aspera HSTS node to your Aspera on Cloud organization is to configure the required settings on your node.
- [Configure Nginx reverse proxy and server certificates](#)
You must protect your Aspera on Cloud tethered transfer nodes with an Nginx reverse proxy.
- [Create the transfer user for your tethered node](#)
To use an HSTS Server as a tethered node with Aspera on Cloud, your HSTS server requires a specially configured system user for SSH authentication when starting transfers. This system user must be named *xfer*. Use this procedure to configure the system user name, file restriction, public key, API credentials, and other required settings.
- [Configure the HA Redis backend for a tethered node cluster](#)
If you are preparing a high-availability cluster of HSTS nodes as your tethered node, you must configure the Redis database backend to support your tethered cluster.
- [Tether your HSTS node to Aspera on Cloud](#)
Once you have completed the preceding configuration steps, you can add your IBM Aspera HSTS node to your Aspera on Cloud organization.
- [Mark remote storage attached to your tethered node as mount points](#)
Mark the local directory of each mounted folder as a mount point. This marking ensures that you maintain access to mounted folders over a transient network disconnection.
- [Configure monitoring and metering for your tethered node](#)
You must configure the Aspera Event Journaling Daemon (AEJD) to enable event data transmission to the Aspera on Cloud Activity App. You must also configure the Aspera License Entitlement Engine (ALEE) to use token authentication for enhanced security of metering data transmissions (by default, ALEE uses entitlement credentials).
- [Backing up and restoring a tethered node database](#)
This article describes how to back up and restore the entire Redis database of a node, which includes Node API users, their access keys, and transfer history.

Tether Your Aspera Transfer Server to Aspera on Cloud

To attach your own user-managed High-Speed Transfer Server (HSTS) to Aspera on Cloud, you must configure it as a *tethered node*. This article covers prerequisites and provides a map of the process. Linked articles describe the configuration steps in detail.

To tether (attach) your HSTS node to Aspera on Cloud, you must configure the transfer server for communication with Web applications and set up a user account on the server so that it conforms with AoC requirements. Then you must protect your Aspera on Cloud transfer nodes with an Nginx reverse proxy.

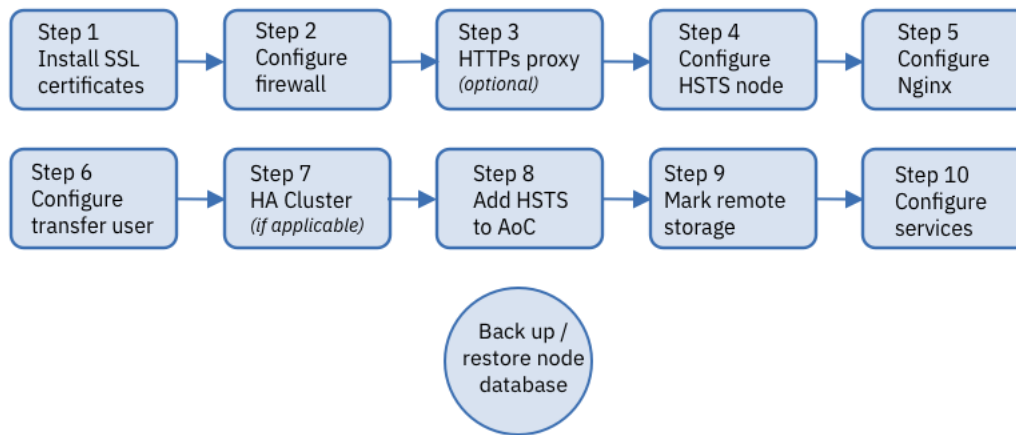
Prerequisites

Before you can configure the transfer server for use as a tethered node with AoC, you must have the following:

- The Aspera High-Speed Transfer Server (latest available version) installed on a supported platform, and configured for your entitlement or license. See the [IBM Aspera High-Speed Transfer Server Admin Guide](#) for your platform.
- To connect your HSTS node to storage in the public cloud, your HSTS must be in the same region as the cloud storage you want to access through the HSTS node.
- The public DNS name of the node accessible from all internal and external clients, as well as the node itself.
- The node clock synchronized with an NTP server. For information in this regard, see the platform OS product documentation.
- A signed certificate and key from an authorized, globally trusted Certificate Authority listed in the [Mozilla CA bundle](#) installed on the node. You'll install the certificate on your node as a part of this process; see [Installing SSL certificates for tethered nodes](#).
- Allow traffic on TCP/443 (refer to [Firewall requirements for tethered nodes](#)).

Process map

This illustration shows the required steps to tether your HSTS node to your Aspera on Cloud organization. Linked topics guide you through the process.



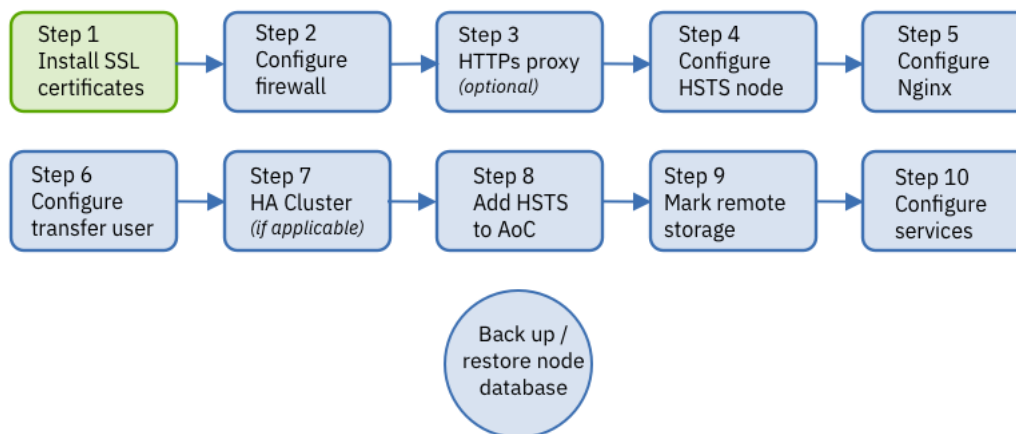
To start, go to [Installing SSL certificates for tethered nodes](#).

Installing SSL certificates for tethered nodes

The first step in tethering your IBM Aspera High-Speed Transfer Server (HSTS) node to your Aspera on Cloud organization is to install SSL certificates on the node.

This is step 1 in tethering a node

For an overview and prerequisites, see [Tether Your Aspera Transfer Server to Aspera on Cloud](#).



Prerequisites

To configure an Aspera High-Speed Transfer Server (HST Server) with an SSL certificate, you must have:

- the key
- the signed root certificate, or a certificate bundle (root certificate plus intermediate certificates)

The key and certificate files must be in `.pem` or `.crt` format.

Note: The key and certificate (or certificate bundle) must be provided by an authorized, globally trusted Certificate Authority (CA) included in the [Mozilla CA bundle](#). You cannot use a self-generated SSL certificate.

Task overview

To install and verify your SSL certificates you must:

1. Replace the contents of the default Aspera key and certificate files in your installation (`aspera_server_key.pem` and `aspera_server_cert.pem`) with the contents of the files that you got from the CA, in the required order.
2. Create a new file (`aspera_server_cert.chain`) in the same directory, and add the required certificate content to it.
3. Use the `openssl` command to determine whether or not your certificate installation is correct.

Install key and certificates

1. Back up the default private-key file and the self-signed certificate file in your HST Server installation. For example, make copies of the files with a `.bak` extension. The private key and certificate files are:

- `aspera_server_key.pem`
- `aspera_server_cert.pem`

For Linux and Mac, the files are in `/opt/aspera/etc`.

For Windows, the files are in `drive-name:\Program Files\Aspera\Enterprise Server\etc`.

2. Replace the existing content of `aspera_server_key.pem` with the new private key that you have received for the HST Server from the CA.
3. Replace the existing contents of `aspera_server_cert.pem` with the new private key and certificate information.

The new contents must be in the following order:

- a. The private key.
- b. The server certificate.
- c. Any intermediate certificates that were provided by the CA.

Note: These may be provided in the same file as the root certificate (as a *certificate bundle*), or in separate files. If they are provided in separate files, place them in order of ascending authority (that is, lowest first, next lowest below it, and so on).

- d. The root certificate of the CA.

4. In the same directory as `aspera_server_key.pem` and `aspera_server_cert.pem`, create a new file named `aspera_server_cert.chain`.
5. Copy the *certificate information* from `aspera_server_cert.pem` into your new `aspera_server_cert.chain` file. Do not include the *key* information. The contents of `aspera_server_cert.chain` and `aspera_server_cert.pem` are therefore the same, *except* that `aspera_server_cert.chain` does *not* include the key.

6. Restart the `asperacentral` and `asperanoded` services.

For Linux and Mac:

```
# service asperacentral restart
# service asperanoded restart
```

For Windows:

- a. Select Control Panel > Administrative Tools > Services.
- b. Select Aspera HTTPD, then click Restart.
- c. Select Control Panel > Administrative Tools > Services.
- d. Select Aspera Central, click Start, and run the following commands:

```
> sc stop asperanoded > sc start asperanoded
```

Check certificates

Verify that you've installed the key and certificate information correctly.

Use the `openssl s_client` command to connect to the HST Server and check whether or not the certificate files were correctly assembled and installed.

Use your system version of `openssl`. Do *not* use `/opt/aspera/bin/openssl`.

The syntax for the command is:

```
openssl s_client -connect server-ip-addr:port-number
```

For *port-number*, use the port number that you have configured the HST Server to use for HTTPS, which should be one of these:

- 443 (the standard HTTPS port number)
- 9092 (if you are using the Nginx reverse proxy—which is strongly recommended by Aspera)

Near the end of the command output, the **Verify return code:** statement indicates whether or not the installation was successful.

This message indicates that the installation was successful:

```
Verify return code: 0 (ok)
```

If the installation was not successful, an error message displays. For example:

```
Verify return code: 21 (unable to verify the first certificate)
```

Troubleshooting

If your output indicates an unsuccessful verification, inspect the certificate content with the `openssl x509` command. If your output indicates an unsuccessful verification, inspect the certificate content with the `openssl x509` command.

For example:

```
# openssl x509 -in aspera_server_cert.pem -text -noout
```

Next step in tethering a node

You've completed the installation of the SSL certificates for your HSTS node. For step 2 in tethering the HSTS node to your AoC organization, go to [Firewall requirements for tethered nodes](#).

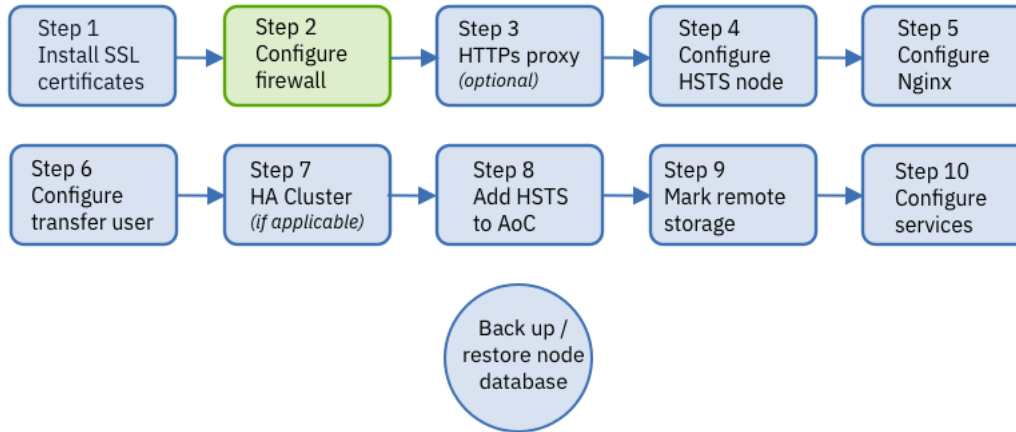
Firewall requirements for tethered nodes

Administrators must configure the proper firewall settings to enable high-speed transfers using Aspera on Cloud.

For Aspera IP addresses, only a few of those in the listed subnet ranges will be active at any given time. However, you should allow the entire set of ranges below to ensure continuous service in the event of a failover. (To determine the set of active IP addresses, check what `api.ibmaspera.com` resolves to using a tool such as `dig` or `nslookup`.)

This is step 2 in tethering a node

Before you begin step 2, be sure you have completed step 1: [Installing SSL certificates for tethered nodes](#).



Allowing traffic from your network to AoC

To use AoC APIs, web interfaces, or Aspera Connect clients on your network with Aspera on Cloud, and to connect to the Aspera metering system (ALEE), configure (allowlist/whitelist) your firewall as follows:

- Allow traffic on TCP/443.
- For Aspera Connect clients and nodes (ATS, user-managed, and so on), also allow traffic on UDP/33001 and TCP/33001.
- Provide *egress* access for the following AoC service IP addresses:

IP Address
169.46.4.68/31
169.46.4.70/31
169.48.106.192/26
169.48.226.120/31
169.48.236.50/31
169.48.249.64/26
169.60.129.66/31
169.60.151.232/31
169.60.197.0/26
169.61.233.80/29
169.61.54.112/29

Allowing traffic from AoC to tethered nodes (user-managed transfer servers)

To use your own transfer server as a tethered node with Aspera on Cloud, configure your firewall as follows:

- Allow traffic on TCP/443.
- For Aspera Connect clients and nodes (ATS, user-managed, and so on), also allow traffic on UDP/33001 and TCP/33001.
- Provide *ingress* access for the following AoC service IP addresses:

IP Address
169.46.4.68/31
169.46.4.70/31
169.48.106.192/26
169.48.226.120/31
169.48.236.50/31
169.48.249.64/26
169.60.129.66/31
169.60.151.232/31
169.60.197.0/26
169.61.233.80/29
169.61.54.112/29

Allowing traffic using IBMid authentication

If your AoC authentication methods include IBMid, you must allow (allowlist/whitelist) the following URLs:

From	To	
	Service name	Service FQDN + Port =TCP/443
Aspera on Cloud front-end web client	IBM Cloud	- iam.cloud.ibm.com - identity-?*.iam.cloud.ibm.com/identity/authorize Where: ? = one character * = one region name (no deeper subdomain allowed) For example: https://identity-2.us-south.iam.cloud.ibm.com/identity/authorize

Next step in tethering a node

You've completed the firewall configuration for your tethered node. For step 3 in tethering the HSTS node to your AoC organization, go to [Using an HTTPS proxy for outgoing ALEE and AEJD traffic from your tethered node](#).

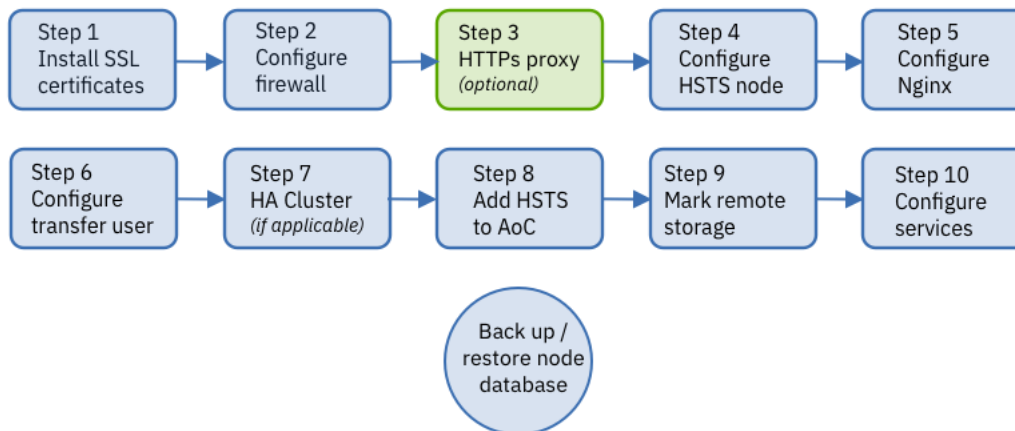
Using an HTTPS proxy for outgoing ALEE and AEJD traffic from your tethered node

This is an optional step in the process of tethering your IBM Aspera HSTS node to your AoC organization. To use an HTTPS proxy for outgoing ALEE (Aspera License and Entitlement Engine) traffic between your tethered node and Aspera on Cloud (optional), you must add options to the JVM_OPTIONS assignment.

Go to the [HSTS Admin Guide](#) for your platform and release, then search for the topic "Aspera Entitlement Service (ALEE) Configuration for Use with an HTTP Web Proxy". For a Linux server, see also the IBM Support article "[How to make ALEE on Linux connect via forward HTTPS proxy](#)"; this article includes troubleshooting and implementation details that may be useful for any server platform.

This is step 3 in tethering a node

Before you begin step 3, be sure you have completed step 2: [Firewall requirements for tethered nodes](#).



Note: Transfer volume through your own tethered, bandwidth-based, licensed Aspera HSTS node is not metered or charged in your AoC subscription.

Set environment variables

To use an HTTPS proxy for outgoing AEJD (Aspera Event Journaling Daemon) traffic between your tethered node and Aspera on Cloud (optional), you must set environment variables. On a Linux server, go to `/usr/lib/systemd/system/asperaejd.service` and set environment variables like in a regular systemd service, as follows:

```
[Unit]
Description=IBM Aspera Event Journal Daemon
ConditionPathExists=/opt/aspera/sbin/aejd

[Service]
Environment="AEJD_LOG_FILE=/opt/aspera/var/log/aejd/aejd.log"
Environment="HTTPS_PROXY=proxy_host:proxy_port"
Type=simple
User=asperadaemon
Group=aspadmins
PIDFile=/opt/aspera/var/run/aspera/aejd.pid
ExecStart=/opt/aspera/sbin/aejd
ExecReload=/bin/kill -HUP $MAINPID
TimeoutStopSec=20
KillMode=process
Restart=on-failure
```

Next step in tethering a node

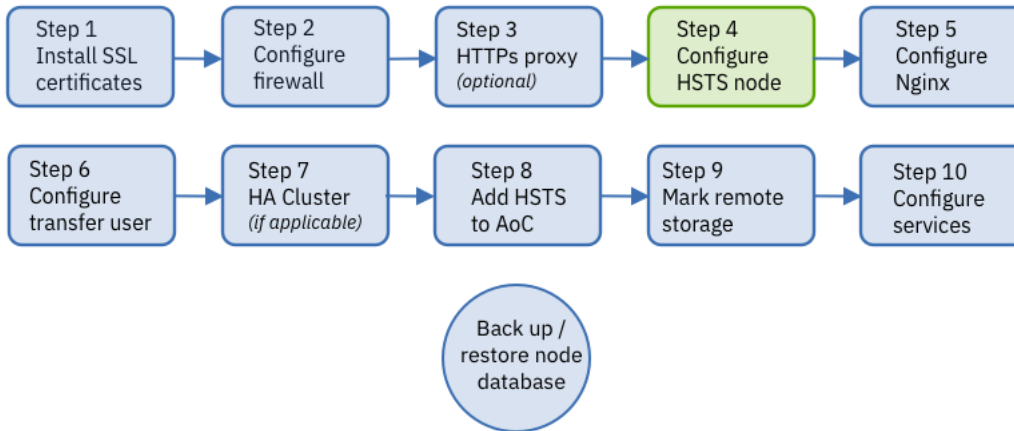
You've completed the HTTPS proxy configuration for your tethered node. For step 4 in tethering the HSTS node to your AoC organization, go to [Configure your transfer server as a tethered node](#).

Configure your transfer server as a tethered node

The next step in tethering your IBM Aspera HSTS node to your Aspera on Cloud organization is to configure the required settings on your node.

This is step 4 in tethering a node

Before you begin step 4, be sure you have completed step 3: [Using an HTTPS proxy for outgoing ALEE and AE3D traffic from your tethered node](#).



1. Create (or select) at least one system user account for managing the transfer server.

CAUTION:

The transfer-server manager account cannot be *root*. In the process of configuring the server and creating the *xfer* transfer user account, root login is disabled. In addition, the transfer-server manager account must not be named *xfer*, which must be reserved for the transfer user account (see [Create the transfer user for your tethered node](#)).

2. Make sure that `/etc/hosts` includes the entry `127.0.0.1 localhost`.

3. Ensure that your system is configured for SSH to use TCP port 33001.

Do not use Port 22. For information on configuring TCP ports, see [IBM Aspera High-Speed Transfer Server Admin Guide: Securing Your SSH Server](#).

4. Configure the transfer server to use a custom file extension to identify files that are partially transferred (during the transfer process).

If using object storage, this setting is on and defaults to `.partial`. No changes required. If you use local storage or want to change the partial file suffix, continue with sub-steps *a* and *b*.

The file extension appears only when a file is partially transferred. It is removed automatically once the transfer is complete.

- a. For local storage, run this command (example custom extension: `.inprogress`)

```
# /opt/aspera/bin/asconfigurator -x "set_node_data;partial_file_suffix,.inprogress"
```

- b. For transfers through TrapD to object storage (the most typical case for a tethered node), configure this option in `aspera.conf`:

Important: Be sure to use the same extension in this step that you used in the previous step (example custom extension: `inprogress`).

```
/opt/aspera/bin/asconfigurator -x "set_node_data;pvc1_browse_partial_extension,.inprogress"
```

and this option in the corresponding `/opt/aspera/etc/trapd/*.properties` file:

```
aspera.session.browse.partial.ext=.inprogress
```

5. Configure your HSTS node to enable activity logging and activity event reporting.

This will enable you to use the AoC logging and event reporting facilities.

```
# /opt/aspera/bin/asconfigurator -x "set_server_data;activity_logging,true;activity_event_logging,true"
```

6. Enable recursive counts.

Recursive counts must also be enabled for displaying file transfer numbers in AoC.

Use the following command syntax:

```
/opt/aspera/bin/asconfigurator -x "set_server_data;files_recursive_counts_workers,value"
```

For *value*, use a number from one to eight. Aspera recommends starting with a value of one and adjusting if needed. For example:

```
# /opt/aspera/bin/asconfigurator -x "set_server_data;files_recursive_counts_workers,1"
```

Lower count values (one or two) result in slower updates but reduced load on the Redis database. Higher values (four to eight) increase the load on Redis; to use higher values, the platform should have twice as many cores.

7. Restart the `asperacentral` and `asperanoded` services.


```
# systemctl restart asperacentral
# systemctl restart asperanoded
```

8. Before you add your node to AoC, you must set up full backups for the Redis database.

The node Redis database includes information about Node API users, their access keys, and transfer history. Scheduling full backups (in addition to Redis Persistence) is required for recovery from data loss that would otherwise be catastrophic for a tethered node.

In your `cron` script, use the following command to create the backup file:

```
/opt/aspera/bin/asredis -p 31415 BGREWRITEAOF
```

This creates the file `/opt/aspera/var/appendonly.aof`, which your script should copy to a backup location.

For information about Redis persistence, and Redis' recommendations for backups, see <https://redis.io>. For information about restoring the Redis database from a backup, see [Backing up and restoring a tethered node database](#).

Next step in tethering a node

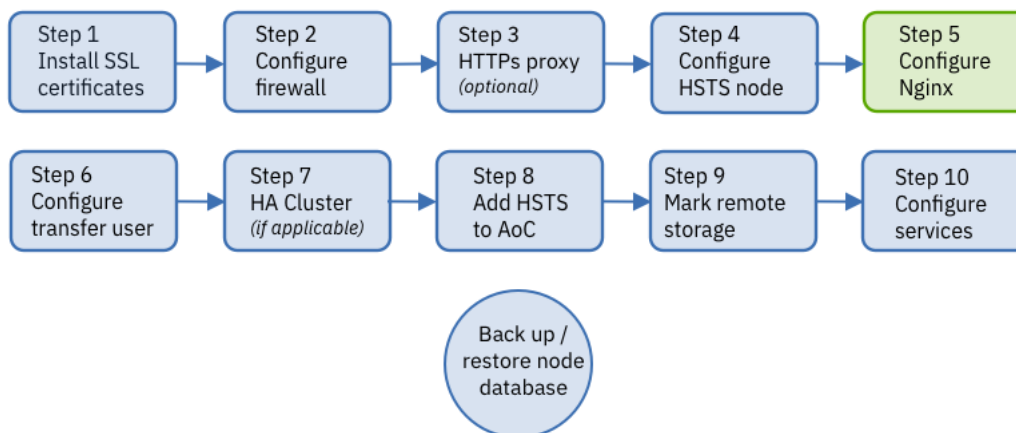
You've completed the HTTPS proxy configuration for your tethered node. For step 5 in tethering the HSTS node to your AoC organization, go to [Configure Nginx reverse proxy and server certificates](#).

Configure Nginx reverse proxy and server certificates

You must protect your Aspera on Cloud tethered transfer nodes with an Nginx reverse proxy.

This is step 5 in tethering a node

Before you begin step 5, be sure you have completed step 4: [Configure your transfer server as a tethered node](#).



1. Download and install Nginx.
2. Set the HTTPS port to 9092.

```
# /opt/aspera/bin/asconfigurator -x "set_server_data;https_port,9092"
```

3. Open the Nginx configuration file in a text editor.

Open `/etc/nginx/nginx.conf` and ensure the following `include` directive is present in the `http` section. If it is not present, add it to the file:

```
http {
...
include /etc/nginx/conf.d/*.conf;
}
```

4. Create a file named `aspera_node_proxy.conf` and save it in `/etc/nginx/conf.d/`.

5. Paste the following content into `aspera_node_proxy.conf`:

```
#
# Aspera configuration - reverse proxy for asperanoded
#
server {
    listen 443;
    server_name your.servername.com;
    ssl_certificate /opt/aspera/etc/aspera_server_cert.pem;
    ssl_certificate_key /opt/aspera/etc/aspera_server_key.pem;

    ssl on;
    ssl_session_cache builtin:1000 shared:SSL:10m;
    ssl_protocols TLSv1.2;
    ssl_ciphers EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH;
    ssl_prefer_server_ciphers on;

    access_log /var/log/nginx/node-api.access.log;
```

```
location / {
    proxy_pass https://127.0.0.1:9092;
    proxy_read_timeout 60;
    proxy_redirect https://127.0.0.1:9092 https://your.servername.com;
    proxy_set_header Host $host:$server_port;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_set_header X-Forwarded-Proto $scheme;
}
```

Note: Configure SSL ciphers as required. The preceding sample is not configured for backwards compatibility, and the recommended list of secure ciphers might change. Aspera recommends reviewing and staying current with the list provided in <https://ciphersli.st/>.

6. Restart the Aspera NodeD service (asperanoded).

```
# systemctl restart asperanoded
```

7. Restart Nginx.

```
# systemctl restart nginx
```

Next step in tethering a node

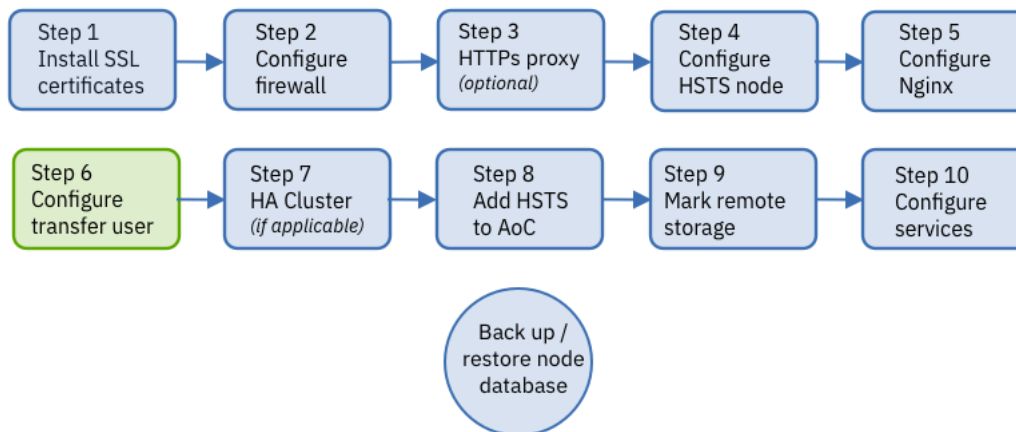
You've completed the HTTPS proxy configuration for your tethered node. For step 6 in tethering the HSTS node to your AoC organization, go to [Create the transfer user for your tethered node](#).

Create the transfer user for your tethered node

To use an HSTS Server as a tethered node with Aspera on Cloud, your HSTS server requires a specially configured system user for SSH authentication when starting transfers. This system user must be named *xfer*. Use this procedure to configure the system user name, file restriction, public key, API credentials, and other required settings.

This is step 6 in tethering a node

Before you begin step 6, be sure you have completed step 5: [Configure Nginx reverse proxy and server certificates](#).



Procedure

Note: You can connect your HSTS node to storage in the public cloud; to do so, your HSTS must be in the same region as the cloud storage you want to access through the HSTS node.

1. Create a system user account named *xfer*.
The user account name must be *xfer* for use with AoC. Do not use any other name; only *xfer* will work. Do not create a password for *xfer* unless the system requires it, in which case use a very large and complex one.
2. Restrict the *xfer* user's access to the file system or object storage. With the correct file restriction, your tethered node can connect with storage in the public cloud, in a private cloud, on premises, or on local disk.
Use the following syntax:

```
/opt/aspera/bin/asconfigurator -x "set_user_data;user_name,xfer;file_restriction,|path"
```

The pipe character is a delimiter.

The restriction path syntax depends on the storage:

- Local, Unix-like OS:
 - Specific folder: `file:///folder/*`
 - Drive root: `file:///*`

- Local: Windows OS:
 - Specific folder : `file:///c%3A/folder/*`
 - Drive root: `file:///c*`
- Alibaba Cloud: `oss://*`
- Amazon S3: `s3://*`
- Azure storage: `azu://*`
- Azure Data Lake: `adl://*`
- Azure Files storage: `azure-files://*`
- Google Cloud storage : `gs://*`
- HDFS: `hdfs://*`
- IBM Cloud Object Storage - S3: `s3://*`
- Multiple storage locations in the region, in the local disk, or in the UNC path: *

For example, to limit the `xfer` user's access to its home directory:

```
# /opt/aspera/bin/asconfigurator -x "set_user_data;user_name,xfer;file_restriction, |file:///home/xfer/*"
```

- As another example, this command sets a file restriction in S3 storage:

```
# /opt/aspera/bin/asconfigurator -x "set_user_data;user_name,xfer;file_restriction, |s3://*"
```

- As a third example, use the command that follows to set a file restriction allowing multiple storage locations in the region, in the local disk, or in the UNC path. With this configuration you can add multiple nodes to Aspera on Cloud based on this tethered HSTS node, with each node secured by a unique access key.

```
# /opt/aspera/bin/asconfigurator -x "set_user_data;user_name,xfer;file_restriction, |*"
```

Using this file restriction, you could, for example, point to multiple locations as follows (Linux example):

```
/mnt/nfs/mount/path
/home/xfer/transferfolder
```

3. Make sure that the `xfer` user has browse, read, write, and execute privileges to the local directories or mount points that must be accessed for transfers. For example, the `xfer` user's home directory.

If the storage is AWS S3, see [Create an AWS S3 IAM role and policy](#) for a procedure.

4. Make sure that the `xfer` user has read and write privileges to the local directories or mount points that must be accessed for transfers. For example, the `xfer` user's home directory.

5. Restrict the `xfer` user's operations on the server with `aspsell`. Aspera strongly recommends this restriction. By default, system users can establish a FASP connection and are only restricted by file permissions. The `aspsell` permits only the following operations:

- Running Aspera uploads and downloads to or from this computer.
- Establishing connections in the application.
- Browsing, listing, creating, renaming, or deleting contents.

In addition, the `aspsell` does not allow interactive login.

Do the following:

```
# usermod -s /bin/aspsell xfer
```

Then confirm that the `xfer` user's account has been updated for `aspsell`:

```
# grep xfer /etc/passwd
xfer:x:1002:1002:xfer user,,,:/home/xfer:/bin/aspsell
```

6. Add the Aspera public key to the `xfer` transfer user's SSH `authorized_keys` file. Set the Aspera public SSH key as an authorized key for the `xfer` transfer user, and ensure that the user owns the file.

```
# mkdir /home/xfer/.ssh
# cp /opt/aspera/var/aspera_tokenauth_id_rsa.pub /home/xfer/.ssh/authorized_keys
# chmod 700 /home/xfer/.ssh
# chmod 600 /home/xfer/.ssh/authorized_keys
# chown -R xfer:xfer /home/xfer/.ssh
```

7. Create Node API user credentials for the `xfer` transfer user. Node API credentials are required for accessing the AoC Web application.

Use the following syntax:

```
/opt/aspera/bin/asnodeadmin -a -u node_username -p node_password -x xfer
```

For example:

```
# /opt/aspera/bin/asnodeadmin -a -u nu-001 -p 2seKret4u -x xfer
```

8. Confirm that the Node API credentials were created successfully. Use the following command:

```
# /opt/aspera/bin/asnodeadmin -l
```

Based on the preceding credentials-creation example, the output looks like this:

```
List of node user(s):
=====
user          system/transfer user          acls
=====
nu-001        xfer                          []
```

9. Configure the `xfer` transfer user for token authorization.

Token-based authorization is used for transfers. It can be set independently for incoming transfers and outgoing transfers. There are two methods available.

- Aspera recommends best practices using `askmscli`, supported in IBM Aspera HSTS v3.9.6.2 and above. For details and procedures, see "Token Encryption Key" in this document: [Security Enhancements for HSTS 3.9.6.2](#).
- You can also configure token authorization in `aspera.conf`. See the following example.

This example shows the method using `aspera.conf` to require token authorization for both uploads and downloads, and to set the token encryption key (passphrase), which is used to encrypt the authorization token, to a random string. Aspera recommends that you set `token_encryption_key` to a value of least 20 random characters. Do not use the string shown in this example.

```
# asconfigurator -x
"set_user_data;user_name,xfer;authorization_transfer_in_value,token;authorization_transfer_out_value,token;token_encryption_key,gj5o930t78m34ejme9dx"
```

10. Restart asperanoded to activate your changes.

```
# systemctl restart asperanoded
```

Next step in tethering a node

You've completed the configuration of the `xfer` transfer user required for your tethered node. For step 7 in tethering the HSTS node to your AoC organization, go to [Configure the HA Redis backend for a tethered node cluster](#).

Configure the HA Redis backend for a tethered node cluster

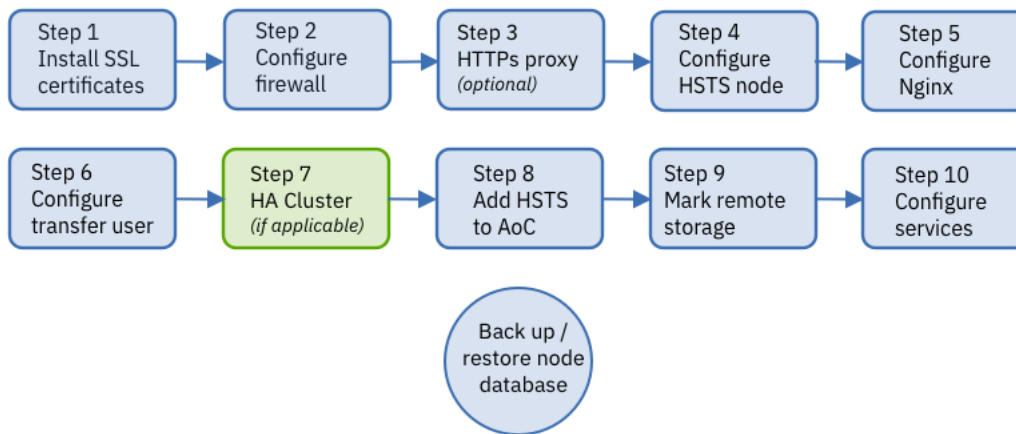
If you are preparing a high-availability cluster of HSTS nodes as your tethered node, you must configure the Redis database backend to support your tethered cluster.

If you are tethering a single HSTS node to your AoC organization, skip this procedure and go to [Tether your HSTS node to Aspera on Cloud](#).

This is step 7 in tethering a node

Before you begin step 7, be sure you have completed step 6: [Create the transfer user for your tethered node](#).

To configure a highly-available Redis backend for an HSTS cluster, go to [IBM Aspera HSTS Admin Guide](#). Select your HSTS software version and platform, then search for *Redis backend* or *Redis database*.



Next step in tethering a node

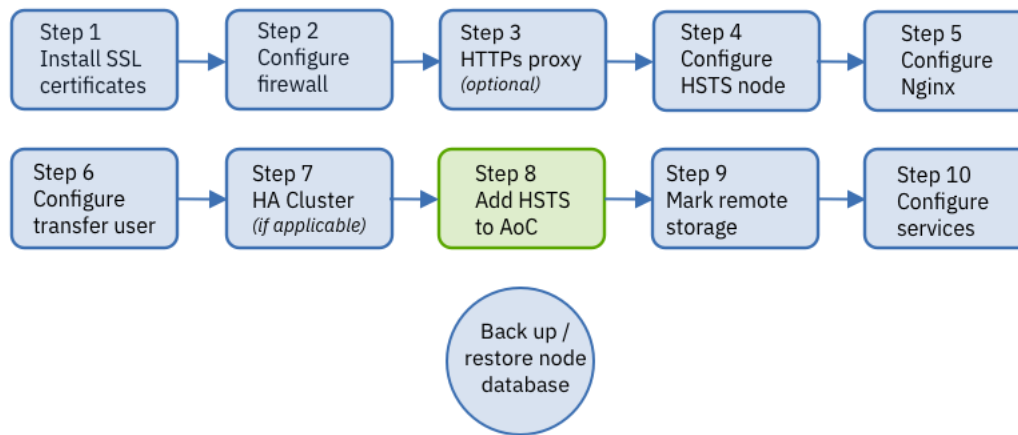
You've completed the configuration of the `xfer` transfer user required for your tethered node. For step 8 in tethering the HSTS node to your AoC organization, go to [Tether your HSTS node to Aspera on Cloud](#).

Tether your HSTS node to Aspera on Cloud

Once you have completed the preceding configuration steps, you can add your IBM Aspera HSTS node to your Aspera on Cloud organization.

This is step 8 in tethering a node

Before you begin step 8, be sure you have completed the previous steps.



Note: Adding a node to AoC requires an access key and secret. It is simplest to generate them when you add the node with the AoC Web UI. But you can also generate them on the node (server) itself from the command line in advance, and then enter them in the Web UI. For information about command-line usage, see [IBM Aspera High-Speed Transfer Server Admin Guide: Access Key Authentication](#).

Prerequisites

Important: Before you can add your transfer server to AoC, you must complete the previous configuration steps. Refer to the process map diagram above. To complete this procedure, you need the following information:

- Node URL.
- Node SSH fingerprint. Aspera recommends that you secure transfers with the SSH fingerprint from the transfer node (but it is not required). For information about retrieving the node fingerprint, see *Securing Your SSH Server* in the [IBM Aspera High-Speed Transfer Server Admin Guide](#).
- To use an existing access key for the node (that you created on the transfer server), you need the access key ID and secret.
- To create a new access key in the process of adding the transfer server (node) to your organization, you need the Node user name and password, and information about the storage you are using.
For local storage, this is simply the path on the node. For cloud storage you need to know the details of that storage (for IBM Cloud, Amazon S3, Microsoft Azure Blob, or Microsoft Azure Files). For example, for Amazon S3, you need the storage class, IAM Assume role credentials, endpoint, bucket, and path.

Add the node

This is the procedure that actually tethers the node you've configured to your Aspera on Cloud organization.

Important: If you have multiple Aspera on Cloud organizations that use the same storage, you must use separate access keys for each organization.

1. In the Admin application, go to **Nodes > Create new**.
2. Enter the name that you want to use for this node.
3. Enter the node's URL and asperanoded port.
For example: `https://www.example.com:443`.
- Note: Be sure to use the asperanoded port as configured for your tethered-node server. See [Configure monitoring and metering for your tethered node](#).
4. Optionally, enter the node SSH fingerprint.
5. To apply a configured network policy to this node, click the downward caret in the Network Policy field and select the intended policy; see [Creating Network Policies](#).
6. To apply a configured node configuration policy to this node, click the downward caret in the Configuration Policy field and select the intended policy; see [Creating Node Configuration Policies](#).
7. To apply a file deletion policy to help manage storage usage, click the field and select the intended policy; see "Configure file deletion policies" in [Managing storage usage](#).
8. Provide an access key/secret pair.
 - If you have already created a key/secret pair for this node on your transfer server, click **Use existing** and enter the node access key and secret. Then click **Save**, and you are done with this procedure.
 - Otherwise, click **Create new access key** and proceed with the following steps.
9. Enter the Node user name.
10. Enter the Node user password.
11. Select the storage type, and configure storage details with data relevant to this storage type.

- **Local**

Local Term	Local Definition
Path	The absolute path on the storage.

- **Amazon S3**

Amazon S3 Term	Amazon S3 Definition
Storage class	Select a storage class. Select from: Standard, Standard Infrequent Access, Intelligent Tiering, Glacier Instant Retrieval, Glacier Flexible Retrieval, Glacier Deep Archive, One Zone Infrequent Access. For important details on AoC functionality in specific storage classes, see Attach an AWS S3 bucket .
Server-side encryption	Select to configure encryption on the server in AWS: None, AES-256, AWS KMS.

Amazon S3 Term	Amazon S3 Definition
KMS key ID ARN or KMS key alias ARN	If using AWS KMS server-side encryption: The AWS Key Management Service key ID, in the format <code>arn:aws:kms:<region>:<account_number>:key/<encryption_key_id></code>. KMS key ID example: "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab". or The AWS Key Management Service key alias, in the format <code>arn:aws:kms:<region>:<account_number>:alias/<encryption_key_alias></code>. KMS key alias example: "arn:aws:kms:us-west-2:111122223333:alias/my_key_alias" Note: Be sure to include the AWS bucket region in the ARN.
IAM Role ARN	The Amazon Resource Name (ARN) of the IAM role to assume.
External ID	The unique identifier used by third parties when assuming roles in their customers' accounts. The storage account holder sets this ID. To find it, go to the AWS management console, then click Roles > yourRole > Trust Relationship . Find your trust relationship in the list, and see the External ID listed in the 'Conditions' column for that relationship. If your trust relationship does not include an external ID, you can edit the trust relationship to add one as required. For more information on External ID, see " How to use an external ID when granting access to your AWS resources to a third party. "
Session name	The role session name that uniquely identifies a session when the same role is assumed by different principals or for different reasons.
Bucket	The bucket name.
Endpoint	The URL that is the entry point to the storage for a web service. Example: <code>s3.amazonaws.com</code> .
Path	The relative path under the bucket.

• **IBM Cloud**

IBM Cloud Term	IBM Cloud Definition
Access key ID	The ID of the access key for the IBM Cloud.
Secret access key	The secret that matches the key.
Bucket	The bucket name.
Endpoint	The URL that is the entry point to the storage for a web service. Example: <code>s3.us.cloud-object-storage.appdomain.cloud</code> .
Path	The relative path under the bucket.

• **Microsoft Azure Blob**

MS Azure Blob Term	MS Azure Blob Definition
API type	Select as appropriate: (1) Block, or (2) Page.
Storage credentials	The access key for SAS URL for the storage.
Storage account	The storage account provides a unique namespace in Azure for your data. Every object that you store in Azure Storage has an address that includes your unique account name. The combination of the account name and the Azure Storage blob endpoint forms the base address for the objects in your storage account.
Access key	The key ID associated with the storage account.
Container	The name of the container that organizes a set of blobs. A container is similar to a directory in a file system.
Path	The relative path in the container.

• **Microsoft Azure Files**

MS Azure Files Term	MS Azure Files Definition
API type	Select as appropriate: (1) Block, or (2) Page.
Storage account	The storage account provides a unique namespace in Azure for your data. Every object that you store in Azure Storage has an address that includes your unique account name. The combination of the account name and the Azure Storage blob endpoint forms the base address for the objects in your storage account.
Password	The password to the storage account.
Path	The relative path on the storage.

12. Click **Save**.

13. Click **Download Access Key Pair**.

14. Download or copy and save the Aspera on Cloud access key and secret according to local site practice. These credentials allow you to access this node for content management and configuration activities. If you download, Aspera generates a text file with the default name `KeySecret.txt`. Aspera recommends that you rename this file to make it easier to track and manage. You must download or copy these credentials to proceed.

Important: Store the key and secret in a secure and accessible location according to local site security practices. Aspera on Cloud does not store the secret. Once you complete this step, you can no longer retrieve the secret.

15. Click **OK**.

16. To protect content on this node with Aspera encryption at rest, do one of the following:

- To use Aspera's native key management capabilities, see [Use Aspera-Managed Keys for Server-Side Encryption at Rest](#).
- To use your own key management service (KMS), see [Bring your own key for server-side encryption at rest](#).

17. Click **Save**.

Updating node status

Aspera on Cloud polls the transfer node for node settings every five minutes; configuration changes you make to the node (for example, changes to `aspera.conf`) are propagated to Aspera on Cloud at that polling interval. If necessary, you can initiate an immediate poll from Aspera on Cloud to the node so that node configuration changes are reflected immediately in Aspera on Cloud behaviors.

1. Go to **Nodes and storage > Nodes**.
2. Filter, search, or browse for the intended node in the node list.
3. Double-click the node row and select **Update Status**, then click **OK** to confirm.

Next step in tethering a node

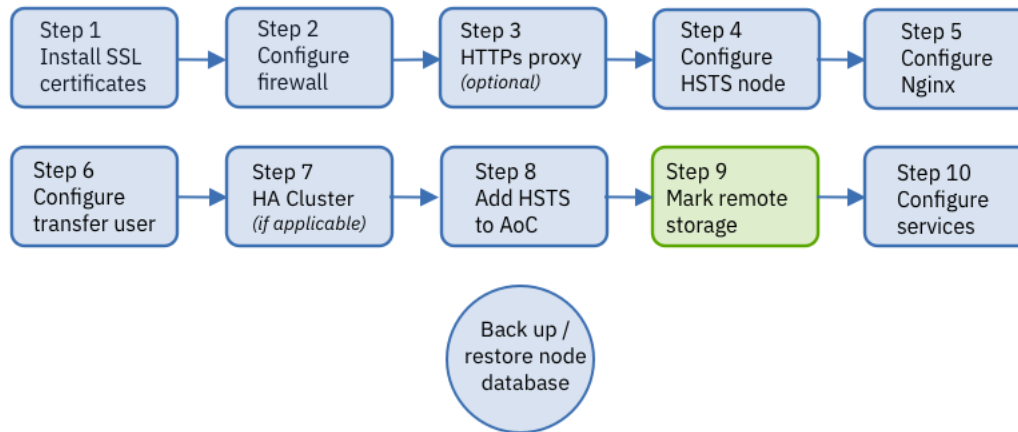
You've added your tethered node to your AoC organization. For step 9 in tethering the HSTS node to your AoC organization, go to [Mark remote storage attached to your tethered node as mount points](#).

Mark remote storage attached to your tethered node as mount points

Mark the local directory of each mounted folder as a mount point. This marking ensures that you maintain access to mounted folders over a transient network disconnection.

This is step 9 in tethering a node

Before you begin step 9, be sure you have completed step 8: [Tether your HSTS node to Aspera on Cloud](#).



Procedure

As a normal part of database maintenance, the transfer node deletes database records of deleted files and folders.

During a transient network disconnection, a mounted remote storage would appear empty to the node. The node would perform this database cleanup on your remote storage. The cleanup would result in access issues even when the remote storage reconnects.

To prevent this database cleanup for the contents of your remote storage, mark your remote storage, including your object storage, as a mount point. Be sure to mark the *local directory* on the tethered node to which the remote volume mounts.

Aspera also recommends that you create a file named `do_not_delete` in each mounted storage.

Note: The example commands shown here assume that your mounted folders are at the root level of your storage. Correct commands vary depending on location of your mounted folders.

1. Retrieve the ID of each folder that will contain an AoC workspace.

```
curl -ki -u [access_key]:[secret] https://[host]:[port]/files/1/files
```

2. Using the ID returned in step 1, mark each mounted folder as a mount point.

```
curl -ki -u [access_key]:[secret] https://[host]:[port]/files/[folder_id] -XPUT -d '{"mount_point":true}'
```

For example, if the folder ID returned in step 1 is 10:

```
curl -ki -u [access_key]:[secret] https://[host]:[port]/files/10 -XPUT -d '{"mount_point":true}'
```

3. Confirm the success of the operation.

Confirm that the folder ID and name are accurate. Confirm that `mount_point` is set to `true`.

```
{
  "id" : "10",
  "name" : "<remote_storage>",
  "path" : "/<remote_storage>",
  "type" : "folder",
  "modified_time" : "2020-07-17T17:50:30Z",
  "mount_point" : "true",
  ...
}
```

Next step in tethering a node

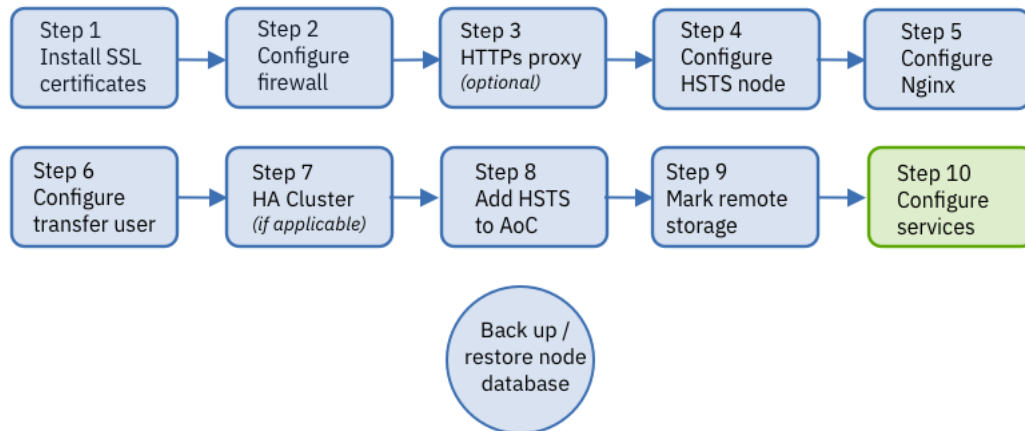
You've marked your attached remote folders as mount points. For step 10 in tethering the HSTS node to your AoC organization, go to [Configure monitoring and metering for your tethered node](#).

Configure monitoring and metering for your tethered node

You must configure the Aspera Event Journaling Daemon (AEJD) to enable event data transmission to the Aspera on Cloud Activity App. You must also configure the Aspera License Entitlement Engine (ALEE) to use token authentication for enhanced security of metering data transmissions (by default, ALEE uses entitlement credentials).

This is step 10 in tethering a node

Before you begin step 10, be sure you have completed step 9: [Mark remote storage attached to your tethered node as mount points](#).



Procedure

The **asp-cloud-config** CLI utility is used in the instructions below to perform service registration with Aspera on Cloud, but it has additional functionality. For detailed information, use the **asp-cloud-config -h** command.

1. Log on to Aspera on Cloud.
2. Select Admin > Integrations > Aspera node services.
3. Click Create new to open the Create a new node services integration dialog.
4. In the **Name** field, enter the name that you want to use for registering the service (or services).
5. Select the node services to integrate: select both AEJD and ALEE.
6. Click **Generate token** to generate and display the token.
7. Copy the registration token.
You will use the registration token to configure the services on your transfer server, so copy it to a place that will be convenient for this purpose.
8. Click **Done**.
 - The new entry is listed on Aspera node services, under Registration pending.
 - If you need to retrieve the token later, click the service name. If the token has expired, you see a prompt to generate a new one.
 - Once you complete the registration process on the server, you can click the service name to display the service client ID, the type of service, the creation date, and the creator's user name.

CAUTION:
Do not delete an ALEE registration. ALEE registration is required to transfer files to and from the server (files on the server will not be affected).

CAUTION:
Do not delete an AEJD registration. AEJD registration is required to report usage and events to the Activity app.
9. Log on to your transfer server.
10. For event reporting with the Aspera on Cloud Activity App, update **aspera.conf** to enable AEJD usage.
 - a.

```
$ sudo /opt/aspera/bin/asconfigurator -x "set_server_data;https_port,9092;activity_logging,true;activity_event_logging,true;aej_logging,true;aej_port,28000;aej_host,127.0.0.1"
```
 - b.

```
$ sudo /opt/aspera/bin/asconfigurator -x "set_node_data;pre_calculate_job_size,yes"
```
11. To use token authentication with ALEE, retrieve your customer ID and entitlement ID, and then disable ALEE.
 - a. If you not registered your entitlement, you will need to have the customer ID and the entitlement ID on hand for a later step.
If have already registered your entitlement, retrieve the information from the transfer server with the following command, and save it to a convenient location for later use. You will not be able to retrieve it from the server after you disable ALEE.

```
$ sudo /opt/aspera/bin/alee-admin entitlement
```
 - b. Disable ALEE.

```
$ sudo /opt/aspera/bin/asalee-config.sh disable
```
12. Using the registration token that you generated, register your services with Aspera on Cloud.
Use the following **asp-cloud-config** command syntax:


```
sudo /opt/aspera/bin/asp-cloud-config tether --aoc-registration-token reg_token_value --aoc-url https://api.ibmaspera.com
```

Note: You can use a registration token only once. If for some reason the registration command fails (for example, due to network connection problems), you must generate a new token on Aspera on Cloud.

13. If you have registered the ALEE service with Aspera on Cloud, enable the service and set up your entitlement.
- First, enable ALEE.

```
$ sudo /opt/aspera/bin/asp-cloud-config alee enable
```

- Then use the following syntax with your customer ID and entitlement ID to register your entitlement:

```
sudo /opt/aspera/bin/alee-admin register customer_ID entitlement_ID
```

14. If you have registered AEJD with Aspera on Cloud, first restart AEJD and then restart asperanoded.

- Restart AEJD, so that it picks up the Aspera on Cloud registration configuration.

```
$ sudo systemctl restart asperaejd
```

- Restart asperanoded, so that the server picks up the aspera.conf changes. Use one of the following commands. The second command below is for Linux systems that use `init.d`.

- ```
$ sudo systemctl restart asperanoded
```
- ```
$ sudo service asperanoded restart
```

15. To verify that your service configuration is correct, log on to Aspera on Cloud and select Admin > Organization > Integrations > Aspera node services. If your configuration is correct, and your service has been registered with Aspera on Cloud, it will be listed under Registered node services.

For the AEJD service, you can also initiate file transfers, and then go to the Aspera on Cloud Activity app to view transfer data. For details, see [Architecture and components of the activity app](#).

Next step in tethering a node

You've configured your tethered node for activity and usage monitoring and for metering.

To allow your Aspera on Cloud users use the content in this node, you must give them access. Note that when you *administratively share* a folder with users, as in this procedure, all admins in your org can manage the folder access. This shared management ability is typically preferable to having one admin user share a folder as an individual user; in such case, only that individual admin can manage access to that folder.

For important maintenance procedures, see [Backing up and restoring a tethered node database](#).

Backing up and restoring a tethered node database

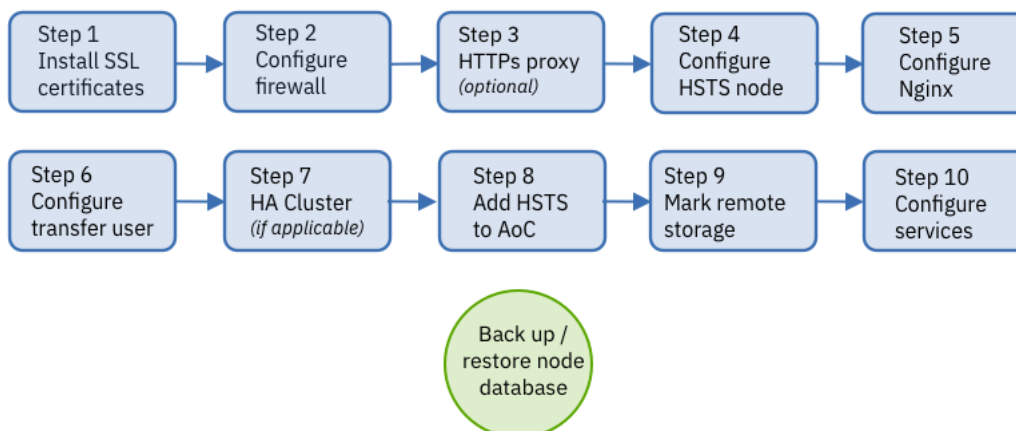
This article describes how to back up and restore the entire Redis database of a node, which includes Node API users, their access keys, and transfer history.

If your transfer server is an IBM Aspera on Cloud (AoC) node, you can migrate AoC data from one node to another by backing up the Redis database on the original node and restoring the database on a new node.

If you need to back up and restore only the Node API user names and passwords (the Node API user database), or if you want to back up and restore only the access keys, refer to the IBM Aspera [HSTS documentation](#).

These instructions assume that the node is using the default port for the Redis database, port 31415. If your deployment uses a different port for Redis, substitute it in the commands accordingly.

Process map



Procedure

1. Verify that the original node and new node are running the same version of Aspera software.
Run `ascp -A` on a command line to view the Aspera product and version
2. On the original node, stop asperanoded and back up the database:

```
# systemctl stop asperanoded
# /opt/aspera/bin/asredis -p 31415 BGREWRITEAOF
```

The backup file is
`/opt/aspera/var/appendonly.aof`.
3. If you are migrating the database, move the `appendonly.aof` file to the same location on the new node.
4. On the new node, stop asperanoded:

```
# systemctl stop asperanoded
```
5. Flush the existing data from the Redis database on the new node:

```
#/opt/aspera/bin/asredis -p 31415 FLUSHALL
```
6. Load the backup data into the new node database:

```
# cat appendonly.aof | /opt/aspera/bin/asredis --pipe -p 31415
```
7. On both nodes, restart asperanoded:

```
# systemctl start asperanoded
```
8. Confirm the database restoration succeeded.
Use the following syntax to run the command on both the original node and the new node. If the database restoration succeeded, the output from each is identical.

```
# curl -ki -u {node_username:node_password} http[s]://{hostname}:{http_port}access_keys
```

Note: Curl is included in many Unix-based distributions. To check if it is installed, enter `curl` on the command line. If it is not installed, download it from the Curl website: <https://curl.haxx.se/download.html>.
9. In AoC, confirm that the hostname matches the DNS entry for the new node.
To view the node hostname and URL, go to Admin > Nodes and storage.

Attach your existing cloud storage

Many organizations use Aspera on Cloud to access content in their existing cloud storage. These articles detail the procedures to attach all supported cloud storage types, including additional help in configuring AWS IAM roles and policies and KMS-encrypted AWS buckets.

- [Firewall requirements for ATS and cloud storage](#)
Administrators must configure the proper firewall settings to enable high-speed transfers using Aspera on Cloud.
- [Share a node folder with a workspace](#)
To allow the members of a workspace to use the content in a node attached to your org, an admin must give them access to the content. When you *administratively share* a folder with users, as described in this procedure, all admins in your org can manage the folder access. This shared management ability is typically preferable to having one admin user share a folder as an individual user; in such case, only that individual admin can revoke or change access permissions.
- [Attach your IBM Cloud storage](#)
You can attach existing IBM Cloud storage to your AoC organization using the Aspera transfer service available in Aspera on Cloud.
- [Attach your Google storage](#)
You can attach existing Google Cloud Storage (GCS) to your AoC organization using the Aspera transfer service available in Aspera on Cloud.
- [Attach your Azure Blob storage](#)
You can attach existing Azure Blob storage to your AoC organization using the Aspera transfer service available in Aspera on Cloud.
- [Attach your Azure Files storage](#)
You can attach existing Azure Files storage to your AoC organization using the Aspera transfer service available in Aspera on Cloud.
- [Attach an AWS S3 bucket](#)
You can attach an existing AWS S3 storage to your AoC organization. Once attached, you can make the bucket and its contents available to your AoC users.
- [Create an AWS S3 IAM role and policy](#)
To allow your AoC users to access the content in your AWS S3 storage, you must connect the storage to AoC through an Aspera transfer node. This connection requires a trusted relationship between AoC and the storage. This topic describes how to configure the IAM role and policy that is central to creating that trusted relationship.
- [Attach a KMS-encrypted AWS bucket](#)
This article shows how to configure an AWS bucket with KMS encryption, and to attach that bucket as storage to your Aspera on Cloud organization.
- [Sample IAM Policies for AWS S3](#)
This article contains sample AWS S3 IAM policies with typical permissions configurations.
- [Creating AWS IAM roles for transfer service nodes](#)
To add Amazon S3 storage to Aspera on Cloud (AoC) as a node, you must create an IAM role because AWS user credentials are not supported.
- [Installing File preview](#)
Generates a preview on the user files (videos, images, and PDFs) when they are uploaded to S3.
- [File preview supported file types](#)

Firewall requirements for ATS and cloud storage

Administrators must configure the proper firewall settings to enable high-speed transfers using Aspera on Cloud.

Note: For Aspera IP addresses, only a few of those in the listed subnet ranges will be active at any given time. However, you should allow the entire set of ranges below to ensure continuous service in the event of a failover. (To determine the set of active IP addresses, check what `api.ibmaspera.com` resolves to using a tool such as `dig` or

nslookup.)

Allowing traffic from your network to Aspera on Cloud

To use AoC APIs, AoC web interfaces, or Aspera Connect clients on your network with Aspera on Cloud, and to connect to the Aspera metering system (ALEE), configure (allowlist/whitelist) your firewall as follows:

- Allow traffic on TCP/443.
- For Aspera Connect clients and nodes (ATS, user-managed, and so on), also allow traffic on UDP/33001 and TCP/33001.
- Provide *egress* access for the following AoC service IP addresses:

IP Address
169.46.4.68/31
169.46.4.70/31
169.48.106.192/26
169.48.226.120/31
169.48.236.50/31
169.48.249.64/26
169.60.129.66/31
169.60.151.232/31
169.60.197.0/26
169.61.233.80/29
169.61.54.112/29

Allowing traffic to transfer service nodes connected to cloud storage

You must also allow access for any transfer service nodes that attach your cloud storage to your Aspera on Cloud organization. Transfer service nodes typically use the **aspera.io** domain.

To retrieve the public IP addresses and ports for the transfer service for allowing in your firewall rules, do the following:

1. Go to Nodes and Storage > Nodes.
2. In the list of nodes, scan for nodes NOT listed as Hosted by Aspera = Aspera.
3. Click the node row and enter the node secret to view details.
4. In the Node URL field, note the URL. The node URL contains the service provider region.
5. Use a curl request or your browser to access the following endpoints:
 - IBM Cloud: <https://ats.aspera.io/pub/v1/servers/softlayer>
 - Amazon S3: <https://ats.aspera.io/pub/v1/servers/AWS>
 - Microsoft Azure: <https://ats.aspera.io/pub/v1/servers/AZURE>
 - Google Cloud: <https://ats.aspera.io/pub/v1/servers/Google>
6. Search for the region you noted in step 4. Note all IP addresses associated with that region, along with the port found in the `transfer_setup_url` field.
7. Enter these IP addresses and ports in your firewall allowlist (whitelist) rules.

From	To		
	Service name	Service IP address	Service port
Aspera on Cloud API client or front-end web client	ATS transfer server	ATS IP address range	TCP/443
Aspera Connect clients	ATS transfer server	ATS IP address range	UDP/33001, TCP33001
Aspera Connect browser	ATS transfer server	ATS IP address range	UDP/33001, TCP33001

Allowing traffic using IBMid authentication

If your AoC authentication methods include IBMid, you must allow (allowlist/whitelist) the following URLs:

From	To	
	Service name	Service FQDN + Port =TCP/443
Aspera on Cloud front-end web client	IBM Cloud	• iam.cloud.ibm.com • identity-?.*.iam.cloud.ibm.com/identity/authorize Where: • ? = one character • * = one region name (no deeper subdomain allowed) For example: https://identity-2.us-south.iam.cloud.ibm.com/identity/authorize

Share a node folder with a workspace

To allow the members of a workspace to use the content in a node attached to your org, an admin must give them access to the content. When you *administratively share* a folder with users, as described in this procedure, all admins in your org can manage the folder access. This shared management ability is typically preferable to having one admin user share a folder as an individual user; in such case, only that individual admin can revoke or change access permissions.

Use this procedure to give users in the Files application:

- Shared access to content in your cloud or on-prem storage.
- A folder in which they can collaborate on content according to the permissions you set.

Once you share the folder using this procedure, users see it on the top level of their Files app.

For each folder you share, you set permissions for each user and group you share with. These permissions determine the actions that users can take on the folder contents. For details, see [Content Permissions](#).

This procedure allows you to share one folder at a time with one or more members of a single workspace. To share multiple folders, or to share a folder with users in multiple workspaces, repeat the procedure

Procedure

Note: To complete this procedure, you need the secret of the node containing the folder you want to share.

1. Go to Workspaces > *workspaceName* > Applications > Files app > Shared folders > Create new.
2. Do one of the following:
 - Enter the node secret and click Log in.
 - If you have a different access key for this node, click **Use custom access key**, enter the key and associated secret, then click **Log in**.
3. (Optional) To create a new folder on the node, do the following:
 - a. Click Create folder.
 - b. Enter a name for the new folder and click Create.
4. From the list of folders that displays, select the folder to share by clicking the option button on the folder row.
If required, you can click a folder name to drill into it. Go back up a level using the breadcrumb list at the top of the modal.
5. (Optional) To display a different name for the folder to the workspace users (perhaps a name that may be most meaningful to them), enter the desired name in the Display name text box.
6. Click Submit.
7. To give all members of the workspace access to this folder, click Add all workspace members.
 - a. Set the access permission level for these users.
 - b. If desired, add other members you want to access this folder at the permission level you set.
 - c. Click Add.
8. To give specific workspace members access to this folder, click Add member.
 - a. Set the access permission level for these users.
 - b. Enter the names of workspace members which whom to share this folder at this permission level.
 - c. Click Add.
9. To change a user's access to the shared folder, click the user row to open the record, adjust permissions as required, then click Save.
10. To remove a user's access to the shared folder, select the check box to the left of the user row and click Delete.

Note:

When new members join the workspace Files app, they can see and access shared folders as follows:

- Folders shared with the entire workspace.
- Folders shared with the new member as an individual or as a group member.

Add a member to an existing shared folder

1. Go to **Workspaces > *workspaceName* > Applications > Files app > Shared folders**.
2. Right-click the intended folder to see the current member list.
3. Do one of the following:
 - Enter the node secret and click Log in.
 - If you have a different access key for this node, click **Use custom access key**, enter the key and associated secret, then click **Log in**.
4. Click Add member.
5. Select the access permission for this new member.
6. Enter the member name.
7. Repeat steps 5 and 6 for additional new members.
8. Click Add.

Node access for workspace managers

1. Go to Workspaces > *workspaceName* > Profile > Node access for workspace managers.
2. Click Add.
3. In the Name drop down, select the node you want to give access to.
4. In the Access key field, enter the access key provided by your administrator.
5. In the Secret field, enter the secret associated with the access key.
Click the eye icon to show or hide the secret as you type.
6. From the Node owners drop down, select who can manage the node:
 - a. Only ATS admins: Only ATS administrators can manage the node.
 - b. All admins: All administrators can manage the node.

Note: Node owners can browse and manage this node without the need of an access key.
7. Click Log in to save the configuration and establish node access.
8. Click Cancel if you do not want to save the configuration and exit.

Attach your IBM Cloud storage

You can attach existing IBM Cloud storage to your AoC organization using the Aspera transfer service available in Aspera on Cloud.

Once you attach the storage, you can create access keys to enable Aspera transfers to and from the cloud storage. The storage is then available to support your organization workspace(s). You can make content in the storage available to your AoC users in the form of administratively shared folders (see [Share a node folder with a workspace](#)).

This procedure also creates access keys to the cloud storage that you can share with other users so that they can run Aspera transfers with the cloud storage from any Aspera client application. You can create multiple access keys to the same cloud storage to allow access to different areas of the storage. To do so, repeat the procedure in this topic, creating a transfer service node for each individual access key. The transfer service attaches the cloud storage to your organization and performs the transfers your users request.

Use this procedure when you have existing cloud storage but no Aspera transfer node associated with it, and want to use the transfer service to connect with it. If you already have an existing Aspera transfer node (which can be on-prem or in the cloud, and managed by you or by Aspera) with its Node URL and password, see [Tether Your Aspera Transfer Server to Aspera on Cloud](#).

Note: Once you create the new transfer service node, you can use the Aspera GUI to transfer to the cloud storage; see [Transfer to cloud with Desktop Client, HST Server, or HST Endpoint GUI](#).

Prerequisites

- You must be a transfer service administrator (ATS admin) in Aspera on Cloud.
- Your IBM Cloud storage must be in a region that is supported by the transfer service. To view the supported regions, to see IP addresses for whitelisting in your firewall configuration, and to retrieve your transfer service server URL, see <https://ats.aspera.io/pub/v1/servers/softlayer>.
- You must have HMAC credentials for the IBM Cloud bucket. Specifically, you need the IBM Cloud bucket Access Key ID and Secret Access Key to complete this procedure.

Procedure

1. In the Admin Management console, click Nodes and storage > Nodes > Create new.
2. Click Attach my cloud storage.
If you do not see this option at the top of the page, you do not have [transfer service admin](#) privileges and cannot perform this procedure.
3. Enter a Node name for the transfer service node.
If you are creating multiple access keys to the same storage for different users or groups of users, make the name descriptive enough to tell them apart.
4. To apply a pre-configured network policy to this node, click the Network policy field and select the intended policy. For details, see [Creating Network Policies](#).
5. To apply a pre-configured node configuration policy to this node, click the Configuration policy field and select the intended policy. For details, see [Creating Node Configuration Policies](#).
6. In the Storage field, select IBM COS. Then do the following:
 - a. Select the region where the storage to attach exists.
 - b. Enter the bucket Access key ID.
 - c. Enter the bucket Access key secret.
 - d. Enter the name assigned to this bucket.
 - e. Enter the path: / or the desired path.
7. Click Create.
If you see the error message, "Unable to create ATS access key and secret", see [Trouble creating a new access key](#) for a troubleshooting procedure.
8. Download or copy and save the Aspera on Cloud access key and secret according to local site practice. These credentials allow you to access this node for content management and configuration activities. If you download, Aspera generates a text file with the default name `KeySecret.txt`. Aspera recommends that you rename this file to make it easier to track and manage.
Important: Aspera on Cloud does not store the secret. Once you complete this step, you can no longer retrieve the secret. You must track these credentials according to your own local site security practices.
9. To protect content on this node with Aspera encryption at rest, do one of the following:
 - To use Aspera's native key management capabilities, see [Use Aspera-managed keys for server-side encryption at rest](#).
 - To use your own key management service (KMS), see [Bring your own key for server-side encryption at rest](#)
10. Click Save to complete creation of the new transfer service node.

This storage can now be used to support a workspace.

- To share a folder in the storage with members of an existing workspace, see [Share a node folder with a workspace](#).
- To create a new workspace hosted on this storage, see [Create a new workspace](#).

Attach your Google storage

You can attach existing Google Cloud Storage (GCS) to your AoC organization using the Aspera transfer service available in Aspera on Cloud.

Once you attach the storage, you can create access keys to enable Aspera transfers to and from your Google storage. The storage is then available to support your organization workspace(s). You can make content in the storage available to your AoC users in the form of administratively shared folders (see [Share a node folder with a workspace](#)).

This procedure also creates access keys to the cloud storage that you can share with other users so that they can run Aspera transfers with the cloud storage from any Aspera client application. You can create multiple access keys to the same cloud storage to allow access to different areas of the storage. To do so, repeat the procedure in this topic, creating a transfer service node for each individual access key. The transfer service attaches the cloud storage to your organization and performs the transfers your users request.

Use this procedure when you have existing cloud storage but no Aspera transfer node associated with it, and want to use the transfer service to connect with it. If you already have an existing Aspera transfer node (which can be on-prem or in the cloud, and managed by you or by Aspera) with its Node URL and password, see [Tether Your Aspera Transfer Server to Aspera on Cloud](#).

Note: Once you create the new transfer service node, you can use the Aspera GUI to transfer to the cloud storage; see [Transfer to cloud with Desktop Client, HST Server, or HST Endpoint GUI](#).

Prerequisites

- You must be a transfer service administrator (ATS admin) in Aspera on Cloud.
- Your cloud storage must be in a region that is supported by the transfer service. To view the supported regions, to see IP addresses for whitelisting in your firewall configuration, and to retrieve your transfer service server URL, see <https://ats.aspera.io/pub/v1/servers/Google>.
- Have the cloud storage credentials available.

Procedure

1. In the Admin Management console, click Nodes and storage > Nodes > Create new.
2. Click Attach my cloud storage.
If you do not see this option at the top of the page, you do not have [transfer service admin](#) privileges and cannot perform this procedure.
3. Enter a Node name for the transfer service node.
If you are creating multiple access keys to the same storage for different users or groups of users, make the name descriptive enough to tell them apart.
4. To apply a pre-configured network policy to this node, click the Network policy field and select the intended policy. For details, see [Creating Network Policies](#).
5. To apply a pre-configured node configuration policy to this node, click the Configuration policy field and select the intended policy. For details, see [Creating Node Configuration Policies](#).
6. Select the Google Cloud storage type.
7. Select the region where the storage to attach exists.
8. Provide a private key or OAuth token for authentication. Both require that you create a service account:
 - a. Log in to Google Cloud Platform (GCP).
 - b. Select the project that contains the storage that you want to add to AoC.
 - c. Go to IAM & admin > Service accounts and click Create service account.
 - d. Enter a Service account name, such as "ats-google-bucket_name-access". If desired, edit the Service account ID.
 - e. Select the Project role. The minimum role required for Aspera to access the storage is Storage Object Admin.
 - f. To use Private key authentication, select Furnish a new private key and leave JSON selected for the key type.
 - g. Click Save. If you created a private key, store it according to local site practice.
 - h. The private key ID is now listed in the table.

To use Private key authentication:

 - a. In the GCP console, copy the project ID (for example, "test-project-1234") and paste it into the Project ID field in the AoC UI.
 - b. In the GCP console, copy the private key ID that is listed in the Service account keys table (for example, "4g444gd311ff277d34722gcgc5fbd51795b56fg4") and paste it into the Private key ID field in the AoC UI.
 - c. Open the private key that you saved to your computer, copy the value for "private_key".
For example:

```
-----BEGIN PRIVATE KEY-----
MB91dowSoh\\nyUtv...Ttzt9u3s8cYyJE4bf4g=
-----END PRIVATE KEY-----
```

 Paste it into the Private key field in the AoC UI.
 Important: Replace the "\n" characters in the content you pasted with actual line breaks.
 - d. In the GCP console, copy the email address of the service account (for example, "ats-google-bucket_name-access@test-project-1234.iam.gserviceaccount.com") and paste it into the Client ID field in the AoC UI.
 - e. In the AoC UI, enter the Path that Aspera can access with the format "bucket_name/path". To allow access to the entire bucket, enter the bucket name.
9. Click Save.
If you see the error message, "Unable to create ATS access key and secret", see [Trouble creating a new access key](#) for a troubleshooting procedure.
10. Download or copy and save the Aspera on Cloud access key and secret according to local site practice. These credentials allow you to access this node for content management and configuration activities. If you download, Aspera generates a text file with the default name `KeySecret.txt`. Aspera recommends that you rename this file to make it easier to track and manage.
Important: Aspera on Cloud does not store the secret. Once you complete this step, you can no longer retrieve the secret. You must track these credentials according to your own local site security practices.
11. To protect content on this node with Aspera encryption at rest, do one of the following:
 - To use Aspera-managed keys, see [Use Aspera-managed keys for server-side encryption at rest](#).
 - To use your own key, see [Bring your own key for server-side encryption at rest](#).
12. Click Save to complete creation of the new transfer service node.

This storage can now be used to support a workspace.

- To share a folder in the storage with members of an existing workspace, see [Share a node folder with a workspace](#).
- To create a new workspace hosted on this storage, see [Create a new workspace](#).

Attach your Azure Blob storage

You can attach existing Azure Blob storage to your AoC organization using the Aspera transfer service available in Aspera on Cloud.

Note: Aspera on Cloud only supports Block blob and Page blob storage.

Once you attach the storage, you can create access keys to enable Aspera transfers to and from the cloud storage. The storage is then available to support your organization workspace(s). You can make content in the storage available to your AoC users in the form of administratively shared folders (see [Share a node folder with a workspace](#)).

This procedure also creates access keys to the cloud storage that you can share with other users so that they can run Aspera transfers with the cloud storage from any Aspera client application. You can create multiple access keys to the same cloud storage to allow access to different areas of the storage. To do so, repeat the procedure in this topic, creating a transfer service node for each individual access key. The transfer service attaches the cloud storage to your organization and performs the transfers your users request.

Use this procedure when you have existing cloud storage but no Aspera transfer node associated with it, and want to use the transfer service to connect with it. If you already have an existing Aspera transfer node (which can be on-prem or in the cloud, and managed by you or by Aspera) with its Node URL and password, see [Tether Your](#)

Note: Once you create the new transfer service node, you can use the Aspera GUI to transfer to the cloud storage; see [Transfer to cloud with Desktop Client, HST Server, or HST Endpoint GUI](#).

Prerequisites

- You must be a transfer service administrator (ATS admin) in Aspera on Cloud.
- Your Azure storage must be in a region that is supported by the transfer service. To view the supported regions, to see IP addresses for allow listing in your firewall configuration, and to retrieve your transfer service server URL, see <https://ats.aspera.io/pub/v1/servers/AZURE>.
- Have the cloud storage credentials available.
- Azure Blob buckets must have hierarchical namespace disabled before attaching.

Procedure

1. In the Admin Management console, click Nodes and storage > Nodes > Create new.
2. Click Attach my cloud storage.
If you do not see this option at the top of the page, you do not have [transfer service admin](#) privileges and cannot perform this procedure.
3. Enter a Node name for the transfer service node.
If you are creating multiple access keys to the same storage for different users or groups of users, make the name descriptive enough to tell them apart.
4. To apply a pre-configured network policy to this node, click the Network policy field and select the intended policy. For details, see [Creating Network Policies](#).
5. To apply a pre-configured node configuration policy to this node, click the Configuration policy field and select the intended policy. For details, see [Creating Node Configuration Policies](#).
6. Select the storage type Microsoft Azure Blob.
7. Select the region where the storage to attach exists.
8. For Premium Blob storage, select Page API in the API type field.
9. For Standard Blob storage, select either Page API or Block API.
10. Provide an access key or SAS URL for the storage credentials:
Access key:
 - In the Azure portal storage account **Access keys** page, copy the storage account name; paste that info into the AoC Storage account field.
 - In the Azure portal storage account **Access keys** page, copy the access key; paste that info into the AoC Key field.
 - In the Azure portal storage account Container page, copy the container; paste that info into the AoC Container field.
 - In the Path field, enter / to access the root level, or enter /<pathName> to access a specific folder.**SAS URL:**
 - Paste the complete URL, with queries, in the Shared access signature field. For example, `https://aspera.blob.core.windows.net/?sv=2018-05-22&ss=bfqt&sr=b&sp=rwdlacup&se=2019-07-23T04:56:28Z&st=2019-08-22T20:56:28Z&spr=https&sig-ivlRmKYM2lR1BgaBe1r97KY02RinVnQzKbBnDixgCFg%8J`.
 - The SAS URL must contain a query parameter (in the URL, everything after '?').
 - The SAS URL must have more than five parameter items (each parameter item follows '&').
 - The SAS URL must have the following parameters set:
 - sv (&sv=): Storage services version. For storage services version 2012-02-12 and later, this parameter indicates the version to use.
 - se (&se=): Expiry time. Specified in UTC time.
 - sp (&sp=): Permissions. The permission granted by the SAS include Read and Write.
 - sig (&sig=): Signature. Used to authorize access to the blob. The signature is an HMAC computed over a string-to-sign and key using the SHA256 algorithm, and then encoded using Base64 encoding.
 - sr (&sr=): Resource. b = blob. The resource is a blob.
 - st (&st=): Start time. Specified in UTC time.
11. In the Path field, enter / to access the root level, or enter /<pathName> to access a specific folder.
12. Click Save.
If you see the error message, "Unable to create ATS access key and secret", see [Access keys](#) for a troubleshooting procedure.
13. Download or copy and save the Aspera on Cloud access key and secret according to local site practice. These credentials allow you to access this node for content management and configuration activities. If you download, Aspera generates a text file with the default name `KeySecret.txt`. Aspera recommends that you rename this file to make it easier to track and manage.
Important: Aspera on Cloud does not store the secret. Once you complete this step, you can no longer retrieve the secret. You must track these credentials according to your own local site security practices.
14. To protect content on this node with Aspera encryption at rest, do one of the following:
Note: You can enable encryption only on nodes that are not configured for watermarking. See [this article](#) for details.
 - To use Aspera's native key management capabilities, see [Use Aspera-managed keys for server-side encryption at rest](#).
 - To use your own key management service (KMS), see [Bring your own key for server-side encryption at rest](#)
15. Click Save to complete creation of the new transfer service node.

This storage can now be used to support a workspace.

- To share a folder in the storage with members of an existing workspace, see [Share a node folder with a workspace](#).
- To create a new workspace hosted on this storage, see [Create a new workspace](#).

Attach your Azure Files storage

You can attach existing Azure Files storage to your AoC organization using the Aspera transfer service available in Aspera on Cloud.

Once you attach the storage, you can create access keys to enable Aspera transfers to and from the cloud storage. The storage is then available to support your organization workspace(s). You can make content in the storage available to your AoC users in the form of administratively shared folders (see [Share a node folder with a workspace](#)).

This procedure also creates access keys to the cloud storage that you can share with other users so that they can run Aspera transfers with the cloud storage from any Aspera client application. You can create multiple access keys to the same cloud storage to allow access to different areas of the storage. To do so, repeat the procedure in this topic, creating a transfer service node for each individual access key. The transfer service attaches the cloud storage to your organization and performs the transfers your users request.

Use this procedure when you have existing cloud storage but no Aspera transfer node associated with it, and want to use the transfer service to connect with it. If you already have an existing Aspera transfer node (which can be on-prem or in the cloud, and managed by you or by Aspera) with its Node URL and password, see [Tether Your Aspera Transfer Server to Aspera on Cloud](#).

Note: Once you create the new transfer service node, you can use the Aspera GUI to transfer to the cloud storage; see [Transfer to cloud with Desktop Client, HST Server, or HST Endpoint GUI](#).

Prerequisites

- You must be a transfer service administrator (ATS admin) in Aspera on Cloud.
- Your Azure storage must be in a region that is supported by the transfer service. To view the supported regions, to see IP addresses for whitelisting in your firewall configuration, and to retrieve your transfer service server URL, see <https://ats.aspera.io/pub/v1/servers/AZURE>.
- Have the cloud storage credentials available.

Procedure

1. In the Admin Management console, click Nodes and storage > Nodes > Create new.
2. Click Attach my cloud storage.
If you do not see this option at the top of the page, you do not have [transfer service admin](#) privileges and cannot perform this procedure.
3. Enter a Node name for the transfer service node.
If you are creating multiple access keys to the same storage for different users or groups of users, make the name descriptive enough to tell them apart.
4. To apply a pre-configured network policy to this node, click the Network policy field and select the intended policy. For details, see [Creating Network Policies](#).
5. To apply a pre-configured node configuration policy to this node, click the Configuration policy field and select the intended policy. For details, see [Creating Node Configuration Policies](#).
6. Select the storage type Microsoft Azure Files.
7. Select the region where the storage to attach exists.
8. Select the API type.
9. Enter the Storage account and Password.
10. In the Path field, enter / to access the root level, or enter /<pathName> to access a specific folder.
11. Click Save.
If you see the error message, "Unable to create ATS access key and secret", see [Trouble creating a new access key](#) for a troubleshooting procedure.
12. Download or copy and save the Aspera on Cloud access key and secret according to local site practice. These credentials allow you to access this node for content management and configuration activities. If you download, Aspera generates a text file with the default name `KeySecret.txt`. Aspera recommends that you rename this file to make it easier to track and manage.
Important: Aspera on Cloud does not store the secret. Once you complete this step, you can no longer retrieve the secret. You must track these credentials according to your own local site security practices.
13. To protect content on this node with Aspera encryption at rest, do one of the following:
Note: You can enable encryption only on nodes that are *not* configured for watermarking. See [this article](#) for details.
 - To use Aspera's native key management capabilities, see [Use Aspera-managed keys for server-side encryption at rest](#).
 - To use your own key management service (KMS), see [Bring your own key for server-side encryption at rest](#)
14. Click Save to complete creation of the new transfer service node.

This storage can now be used to support a workspace.

- To share a folder in the storage with members of an existing workspace, see [Share a node folder with a workspace](#).
- To create a new workspace hosted on this storage, see [Create a new workspace](#).

Attach an AWS S3 bucket

You can attach an existing AWS S3 storage to your AoC organization. Once attached, you can make the bucket and its contents available to your AoC users.

Use this procedure when you have an existing AWS S3 and want to make it (or content from it) accessible to users in your AoC workspaces. If you already have an existing Aspera transfer node (which can be on-prem or in the cloud, and managed by you or by Aspera) with its Node URL and password, see [Tether Your Aspera Transfer Server to Aspera on Cloud](#).

AWS storage classes

When you attach an AWS bucket to your Aspera on Cloud organization, you select an AWS storage class. You can attach AWS buckets with these storage classes to AoC:

- Standard
- Intelligent Tiering
- Standard Infrequent Access
- One-zone Infrequent Access
- Glacier Instant Retrieval
- Glacier Flexible Retrieval
- Glacier Deep Archive

In a workspace configured on nodes with storage class Glacier Flexible Retrieval and Glacier Deep Archive, note the following:

- The Packages app is not available due to extended AWS retrieval times.
- Files app users:

- Can view files and folders. Files are marked with the label "Glacier storage". Folders are not labeled.
- Can share folders.
- Can upload files and folders. These items appear in the Files view after some time, depending on the duration required by AWS processing.
- Cannot download, move, copy, or rename files. If a user downloads a folder from such a workspace, the folder appears in the expected download location but remains empty.

AoC access keys

Once you attach the AWS S3 bucket, you can give various users access to specifically designated parts of the storage using AoC access keys. *Distinct from the AWS S3 bucket access keys*, these native AoC access keys are an additional layer of security that allow you to securely access the bucket through AoC and other Aspera client applications. You can create multiple AoC access keys to the same AWS S3 bucket to partition access to specific areas of the storage. For details, see the articles in [Access keys](#).

Note: Once you attach the S3 bucket, you can use the Aspera GUI to transfer to your cloud storage; see [Transfer to cloud with Desktop Client, HST Server, or HST Endpoint GUI](#).

Prerequisites

- You must have transfer service administrator (ATS admin) access to Aspera on Cloud.
- You must have administrative access to the AWS S3 configuration portal.
- The AWS S3 bucket must be in a region that is supported by the Aspera transfer service. To view the supported regions, to see IP addresses for whitelisting in your firewall configuration, and to retrieve your transfer service server URL, follow this link: <https://ats.aspera.io/pub/v1/servers/AWS>.
- You must have an AWS S3 IAM Role to use for trust relationship policies. You need to add this role in the AWS portal Trust relationships tab. Note the role name so you can add it in the following procedure; for example, "Aspera-Role". To create an IAM role, see [Create an AWS S3 IAM role and policy](#).
- To provide extra security for your environment, see the procedure below called "Enhance Access Security for an AWS S3 Bucket".

Important: Consider configuring a lifecycle policy on your S3 bucket to automatically clean up incomplete multipart uploads older than 7 days.

Procedure: How to attach the bucket to AoC

This procedure requires you to use both the Aspera on Cloud Admin interface and the AWS portal interface.

1. In the Aspera on Cloud Admin app, do the following:
 - a. Go to Nodes and storage > Nodes > Create new.
 - b. Click Attach my cloud storage.

If this option does not appear at the top of the page, you do not have transfer service admin (ATS admin) privileges. You must ask a user who has ATS admin privileges to add this privilege to your user profile. The transfer service admin should go to Users, filter for your user name, then click the row to open your user record; then, in the Admin roles section, click the check box labeled ATS admin, then Save.
 - c. Enter a Node name for the transfer service node; this name refers to the AWS S3 storage.
 - d. If a pre-configured network policy is required for this node, click the Network policy field and select the intended policy.

For details, see [Creating Network Policies](#).
 - e. If a pre-configured node configuration policy is required for this node, click the Configuration policy field and select the intended policy.

For details, see [Creating Node Configuration Policies](#).
 - f. In the **Storage** field, select Amazon S3.
 - g. In the **Region** field, select the Amazon region that contains the S3 bucket.
 - h. In the **Storage class** field, select the desired setting.
 - i. In the **Amazon S3 Server-side encryption** field, select the desired encryption type, if any.

Note: You can enable encryption only on nodes that are not configured for watermarking. See [this article](#) for details.
 - j. If you selected **AWS KMS** in the previous field, enter the KMS key ID ARN or key alias ARN in the **KMS key ID or key alias ARN** field.

KMS key **ID** ARN:
 Syntax: `arn:aws:kms:<region>:<account_number>:key/<encryption_key_id>`
 Example: `"arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"`
 KMS key **alias** ARN:
 Syntax: `arn:aws:kms:<region>:<account_number>:alias/<encryption_key_alias>`
 Example: `"arn:aws:kms:us-west-2:111122223333:alias/my_key_alias"`
 Note: Be sure to include the AWS bucket region in the ARN.
 - k. Copy the contents of the Trust relationship policy field. If necessary, you can edit the policy before you copy it.

Important: The trust relationship JSON updates with each page load.

 - Before you copy the trust policy, be sure that you have correctly configured the region (step **1g** above).
 - After you copy the trust relationship, be sure to save the configuration or otherwise verify the page is not reloaded.

If the page reloads after you copy the trust relationship, there will be a mismatch between the trust relationship in AoC and the trust relationship in the AWS console.

Trust relationship policy

Please paste this policy in your AWS Trust relationship policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::120942126197:role/atp-aws-us-east-1-ts-atc-
node"
      },
      "Action": "s3:*"
    }
  ]
}
```

2. Log in to the AWS portal and do the following:
 - a. Go to Services > IAM > Roles. Find the IAM role you created for the trust relationship policy; for example, "Aspera-Role".
 - b. Click to select the role and go to the Trust relationships tab.
 - c. Click Edit trust relationship.
 - d. Paste the policy you copied from the Aspera on Cloud **Trust relationship policy** field in step **1h**. Be sure the paste operation replaces all existing text.

- e. Click Update Trust Relationship.
- f. Copy the role ARN (Amazon Resource Name) for this role.
3. Return to the Aspera on Cloud **Nodes > Create new > Attach my cloud storage** window and do the following:
 - a. Paste the role ARN that you copied from the AWS portal in the AoC IAM Role ARN field.
 - b. Complete the form with the S3 bucket and path.
 - To grant access to the entire bucket, enter / (that is, a slash character).

Path

/

- To grant access to a specific directory in the bucket, enter /<path_name> (that is, slash+path_name).

Path

/west-2-14

- c. Click Save.
- Note: If you see the error message, "Unable to create ATS access key and secret", see [Trouble creating a new access key](#) for a troubleshooting procedure.
- d. Download or copy and save the Aspera on Cloud access key and secret according to local site practice. These credentials allow you to access this node for content management and configuration activities. If you download, Aspera generates a text file with the default name `KeySecret.txt`. Aspera recommends that you rename this file to make it easier to track and manage.
- Important: Aspera on Cloud does not store the secret. Once you complete this step, you can no longer retrieve the secret. You must track these credentials according to your own local site security practices.
- e. To protect content in this bucket with Aspera encryption at rest, do one of the following:
 - To use Aspera's native key management capabilities, see [Use Aspera-managed keys for server-side encryption at rest](#).
 - To use your own key management service (KMS), see [Bring your own key for server-side encryption at rest](#)
- f. Click Save to complete creation of the new transfer service node. See this new node in the list of nodes by going to Nodes and storage > Nodes.

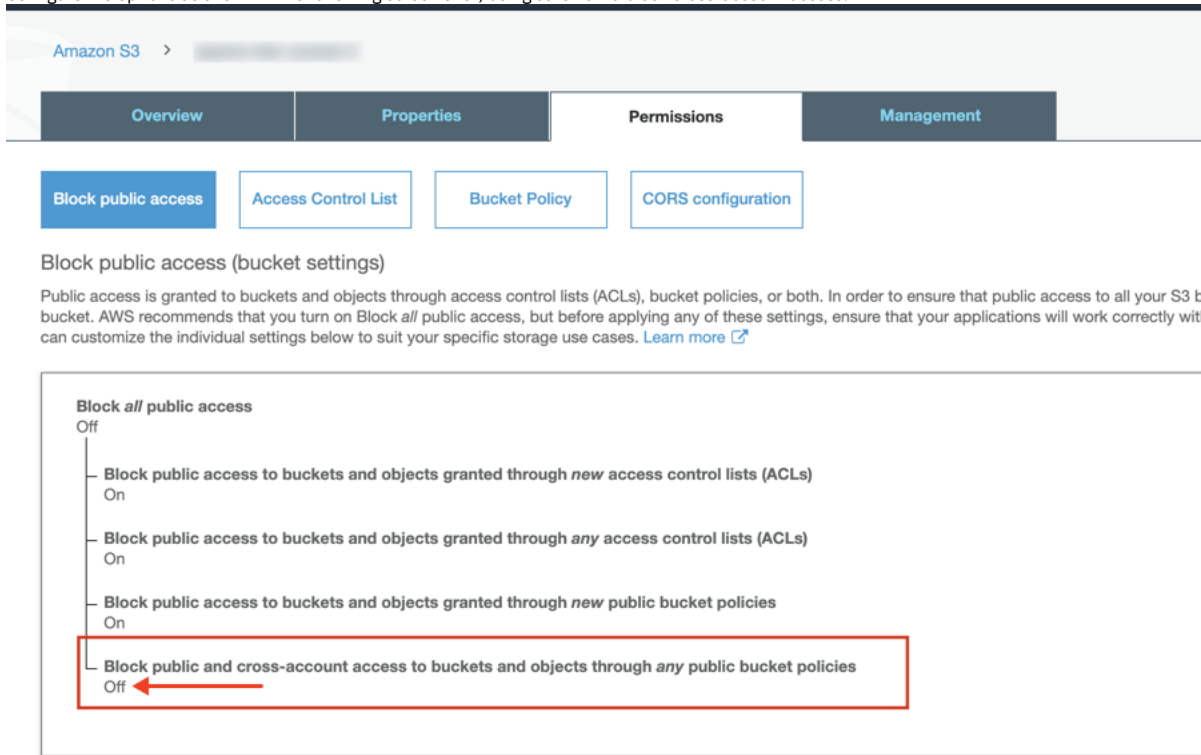
This storage can now be used to support a workspace.

- To share a folder in the bucket with members of an existing workspace, see [Share a node folder with a workspace](#).
- To create a new workspace hosted on this bucket, see [Create a new workspace](#).
- To create native AoC access keys to the bucket or a partition of the bucket, see [Create a sub-access key to a cloud storage folder](#).

Optional: Enhance access security for an AWS S3 bucket

You can apply an optional policy to enhance AWS S3 bucket access security. Use the procedure below to restrict access to the bucket from any IP address except those you specifically designate; this restriction is also known as *whitelisting*. This policy will still allow the Aspera transfer service to access the bucket for transfer operations.

1. In the Amazon console, go to the intended bucket, then click Permissions > Block public access.
2. Configure the options as shown in the following screen shot, being sure *not* to block cross-account access.



3. Go to **Permissions > Bucket Policy**.
4. Enter the same policy that you applied to the associated role.

5. Copy the "Principal" stanza from the trust relationship in the role to the bucket policy, as show in the screen shot below.



Bucket policy editor ARN: arn:aws:s3::: [redacted]

Type to add a new policy or edit an existing policy in the text area below.

Granting public access in this policy will be blocked because Block public access settings are turned on for this bucket. To determine which s

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Principal": {
8         "AWS": "arn:aws:iam::880559705280:role/[redacted]"
9       },
10      "Action": [
11        "s3:PutObject",
12        "s3:GetObject",
13        "s3:AbortMultipartUpload",
14        "s3:DeleteObject",
15        "s3:ListMultipartUploadParts"
16      ],
17      "Resource": "arn:aws:s3:::[redacted]/*"
18    },
19    {
20      "Sid": "VisualEditor1",
21      "Effect": "Allow",
22      "Principal": {
23        "AWS": "arn:aws:iam::880559705280:role/[redacted]"
24      },
25      "Action": [
26        "s3:ListBucketMultipartUploads",
27        "s3:ListBucket",
28        "s3:GetBucketLocation"
29      ],
30      "Resource": "arn:aws:s3:::[redacted]"
31    }
32  ]
33 }
```

[Documentation](#) [Policy generator](#)

6. If desired, use this JSON example, changing the following:

- Replace the sample "Principal" stanza shows below with the actual "Principal" stanza from the trust relationship in the associated role.
- For the variable <region>, substitute the region for your bucket.
- For the variable <bucket_name>, substitute the bucket name.
- For the variable <allowed_IP_address>, substitute the allowed IP address(es), formatted in a JSON array (for example: ["192.0.2.0/24", "203.0.113.0/24"])
- For the variable <ats_vpc>, substitute the AWS virtual private cloud ID or VPC endpoint ID (see list following this sample).

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::880559705280:role/atp-aws-us-<region>-ts-atc-node"
    },
    "Action": [
      "s3:AbortMultipartUpload",
      "s3:DeleteObject",
      "s3:ListMultipartUploadParts",
      "s3:PutObject"
    ],
    "Resource": [
      "arn:aws:s3:::<bucket_name>/*"
    ],
    "Condition": {
      "NotIpAddress": {
        "aws:SourceIp": "<allowed_IP_address>"
      },
      "StringNotEquals": {
        "aws:SourceVpc": "<ats_vpc>"
      }
    }
  ]
},
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::880559705280:role/atp-aws-<region>-ts-atc-node"
```

```

    },
    "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
    ],
    "Resource": [
        "arn:aws:s3:::<bucket_name>"
    ],
    "Condition": {
        "NotIpAddress": {
            "aws:SourceIp": "<allowed_IP_address>"
        },
        "StringNotEquals": {
            "aws:SourceVpc": "<ats_vpc>"
        }
    }
}
}
]
}

```

Find the required VPC ID and VPCE ID listed by AWS region below:

```

atp-aws-ap-northeast-1-vpc = -----
vpc name: atp-ap-northeast-1-ts-vpc
vpc id: vpc-ddce48b9
vpce id: vpce-86f431ef
atp-aws-ap-southeast-1-vpc = -----
vpc name: atp-ap-southeast-1-ts-vpc
vpc id: vpc-c9b884ad
vpce id: vpce-c25a8bab
atp-aws-ap-southeast-2-vpc = -----
vpc name: atp-ap-southeast-2-ts-vpc
vpc id: vpc-3cc0c758
vpce id: vpce-8c9c5ae5
atp-aws-eu-central-1-vpc = -----
vpc name: atp-eu-central-1-ts-vpc
vpc id: vpc-dac878b2
vpce id: vpce-bfae55d6
atp-aws-eu-west-1-vpc = -----
vpc name: atp-eu-west-1-ts-vpc
vpc id: vpc-00a8d564
vpce id: vpce-7495681d
atp-aws-sa-east-1-vpc = -----
vpc name: atp-sa-east-1-ts-vpc
vpc id: vpc-5c7aed3b
vpce id: vpce-31945458
atp-aws-us-east-1-vpc = -----
vpc name: atp-us-east-1-ts-vpc
vpc id: vpc-dc6a60bb
vpce id: vpce-4c278825
atp-aws-us-west-2-vpc = -----
vpc name: atp-us-west-2-ts-vpc
vpc id: vpc-b69e77d1
vpce id: vpce-62c1390b

```

For more information on bucket policies, refer to the AWS documentation.

Create an AWS S3 IAM role and policy

To allow your AoC users to access the content in your AWS S3 storage, you must connect the storage to AoC through an Aspera transfer node. This connection requires a trusted relationship between AoC and the storage. This topic describes how to configure the IAM role and policy that is central to creating that trusted relationship.

Once you have completed the procedure in this topic, you can use the IAM role and policy you create to attach your AWS S3 storage to AoC in a trusted relationship as described in this topic: [Attach an AWS S3 bucket](#).

Minimum IAM role permissions required

The IAM role requires certain minimum permissions to enable AoC to upload, download, browse, or delete content in your AWS S3 bucket. Find these minimum permissions in the following table.

Permission	Required for			
	Upload	Download	Browse	Delete
s3:AbortMultipartUpload	X	—	X	X
s3:DeleteObject	X	—	X	X
s3:GetBucketLocation (see note 1)	X	X	X	—
s3:GetObject	—	X	X	—
s3:ListBucket	X	X	X	—
s3:ListBucketMultipartUpload	X	X	X	X
s3:ListMultipartUploadParts	X	—	—	—
s3:PutObject	X	—	—	—
s3:ListAllMyBuckets (see note 2)	X	—	—	—

Note 1: Tuning exists if you want to remove the need for this permission.

Note 2: No longer required as of HSTS v3.5.2; however, it is required if a bucket name is not included on the policy (like *).

Configure the IAM role and policy

1. Configure the IAM role and policy according to the AWS S3 user documentation.
2. At the appropriate step, paste the following policy into the text box, replacing all existing text:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:ListMultipartUploadParts"
      ],
      "Resource": "arn:aws:s3:::bucket-name/*"
    },
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucketMultipartUploads",
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::bucket-name"
    }
  ]
}
```

3. Replace the two instances of `bucket-name` with the name of your S3 bucket.

This is the minimum required policy; to create a more flexible policy, see [Creating AWS IAM roles for transfer service nodes](#), and [Sample IAM Policies for AWS S3](#).

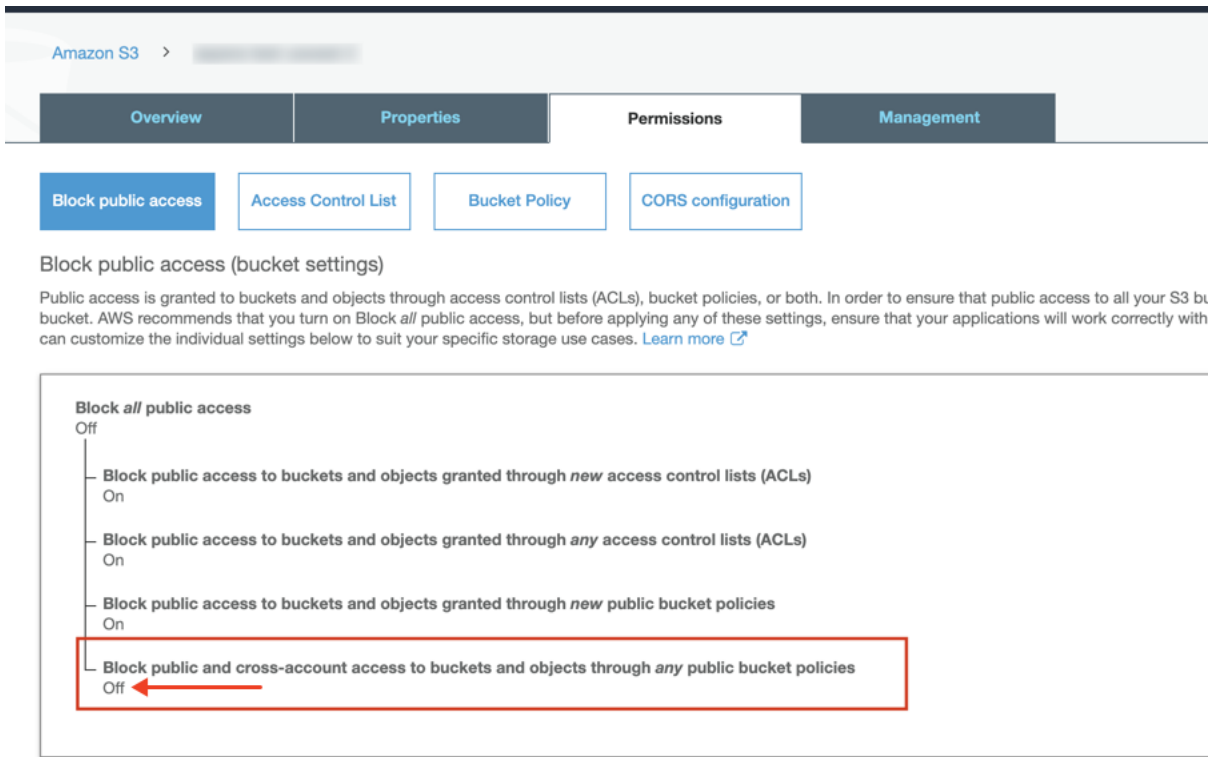
Use the role and policy you created to configure the trusted relationship between AoC and your S3 storage as described in [Attach an AWS S3 bucket](#).

Attach a KMS-encrypted AWS bucket

This article shows how to configure an AWS bucket with KMS encryption, and to attach that bucket as storage to your Aspera on Cloud organization.

Prerequisites

1. Create the AWS bucket.
 - Using AWS command line: <https://docs.aws.amazon.com/cli/latest/reference/s3api/create-bucket.html>
 - Syntax: # aws s3api create-bucket --bucket BUCKET_NAME --region AWS_REGION
2. Set S3 bucket public access to allow for cross-account access.
 - Using AWS console: <https://docs.aws.amazon.com/AmazonS3/latest/user-guide/block-public-access-bucket.html>
Do not block cross-account access. Cross-account access allows you to access content in your AWS bucket through Aspera on Cloud. Configure the options as shown in the following screenshot:



3. Create a KMS key.
 - Using AWS command line: <https://docs.aws.amazon.com/cli/latest/reference/kms/create-key.html>
 - Syntax: `# aws kms create-key --tags TagKey=Purpose,TagValue=YOUR_DESCRIPTION --description YOUR_KEY_DESCRIPTION`
4. Create a KMS alias.
 - Using AWS command line: <https://docs.aws.amazon.com/cli/latest/reference/kms/create-alias.html>
 - Syntax: `# aws kms create-alias --alias-name alias/YOUR_KEY_ALIAS_NAME --target-key-id TARGET_KEY_ID`
 - To obtain the key ID, use the following: `# aws kms list-keys`
5. Create IAM policy for S3 bucket access.
 - Using AWS command line: <https://docs.aws.amazon.com/cli/latest/reference/iam/create-policy.html>
 - Syntax: `# aws iam create-policy --policy-name YOUR_S3_POLICY_NAME --policy-document file://s3.policy.json`
 - To obtain the key ID, use the following: `# aws kms list-keys`
 - For an example of the `s3.policy.json` file, see "S3 Access Policy: Sample Configuration" below.
6. Create IAM policy for KMS alias access.
 - Using AWS command line: <https://docs.aws.amazon.com/cli/latest/reference/iam/create-policy.html>
 - Syntax: `# aws iam create-policy --policy-name YOUR_KMS_POLICY_NAME --policy-document file://kms-alias.policy.json`
 - To obtain the key ID, use the following: `# aws kms list-keys`
 - For an example of the `kms-alias.policy.json` file, see "KMS Alias Management: Sample Configuration" below.
7. Create the IAM role.

Note: You'll add the trust policy in a following step.

 - Using AWS command line: <https://docs.aws.amazon.com/cli/latest/reference/iam/create-role.html>
 - Syntax: `# aws iam create-role --role-name YOUR_ROLE_NAME`
8. Attach the policies you created in steps 5 and 6 to the role you create in step 7.
 - Using AWS command line: <https://docs.aws.amazon.com/cli/latest/reference/iam/attach-role-policy.html>
 - Syntax: `# aws iam attach-role-policy --role-name YOUR_ROLE_NAME --policy-arn YOUR_S3_POLICY_ARN --policy-arn YOUR_KMS_POLICY_ARN`

Attaching your bucket to Aspera on Cloud

1. Use the procedure in [Attach an AWS S3 bucket](#).
2. Specify the S3 region for your bucket.
3. Set Server-side encryption to KMS.
4. Enter the ARN for the KMS key ID or KMS key alias, using the following format:
 KMS key ID ARN format: `arn:aws:kms:<region>:<account_number>:key/<encryption_key_id>`
 KMS key alias ARN format: `arn:aws:kms:<region>:<account_number>:alias/<encryption_key_alias>`
 To obtain the key ID, use the following: `# aws kms list-keys`
5. Configure the trust policy by copying the policy that AoC generates into your AWS Trust relationship policy in the AWS console. Be sure you have set the region before copying the trust relationship policy.
 Important: The trust relationship JSON updates with each page load.
 - Before you copy the trust policy, be sure that you have correctly configured the region (step 2 above).
 - After you copy the trust relationship, be sure to save the configuration or otherwise verify the page is not reloaded.
 If the page reloads after you copy the trust relationship, there will be a mismatch between the trust relationship in AoC and the trust relationship in the AWS console.
6. Configure the IAM role ARN, the S3 bucket name, and the bucket path.

Note: If you see the error message, "Unable to create ATS access key and secret", see [Trouble creating a new access key](#) for a troubleshooting procedure.

Example bucket policy configuration

Adjust the bucket policy if required to support actions as shown in the following sample syntax and example.

Sample bucket policy syntax

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmnt1464034295000",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AOC_ACCOUNT_ID:role/AOC_IAM_ROLE"
      },
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource": "arn:aws:s3::BUCKET_NAME/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AOC_ACCOUNT_ID:role/AOC_IAM_ROLE"
      },
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource": "arn:aws:s3::BUCKET_NAME"
    }
  ]
}
```

Example bucket policy configuration

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmnt1464034295000",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::860559707280:role/atp-aws-us-east-1-ts-atc-node"
      },
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource": "arn:aws:s3::aspera-kms/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::860559707280:role/atp-aws-us-east-1-ts-atc-node"
      },
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource": "arn:aws:s3::aspera-kms"
    }
  ]
}
```

S3 access policy: Sample configuration

Sample S3 access policy syntax

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmnt1464034295000",
      "Effect": "Allow",
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3::BUCKET_NAME/*"
      ]
    }
  ]
}
```

```

    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource": [
        "arn:aws:s3:::BUCKET_NAME"
      ]
    }
  ]
}

```

Example S3 access policy configuration

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1464034295000",
      "Effect": "Allow",
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::aspera-kms/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource": [
        "arn:aws:s3:::aspera-kms"
      ]
    }
  ]
}

```

KMS alias management: Sample configuration

Configure a policy that permits AoC to access your key management service.

Sample KMS alias management syntax

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1464034295000",
      "Effect": "Allow",
      "Action": [
        "kms:EnableKey",
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource": [
        "arn:aws:kms:AWS_REGION:AWS_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    }
  ]
}

```

Sample KMS alias management configuration

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1464034295000",
      "Effect": "Allow",
      "Action": [
        "kms:EnableKey",
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:239600258224:key/65a140e1-8c8f-4dd5-b2d7-d6cf05e15b46"
      ]
    }
  ]
}

```



```
}  
]  
}
```

Sample IAM Policies for AWS S3

This article contains sample AWS S3 IAM policies with typical permissions configurations.

Configure these policies in the AWS console in Security & Identity > Identity & Access Management > Create Policy.

Policy for upload, download, and list content

The following sample IAM policy contains the minimum IAM permissions required to upload, download, or list content in an S3 bucket. Replace *my_bucket* with your actual S3 bucket name.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "Stmt1464034295000",  
      "Effect": "Allow",  
      "Action": [  
        "s3:AbortMultipartUpload",  
        "s3:DeleteObject",  
        "s3:ListMultipartUploadParts",  
        "s3:PutObject",  
        "s3:GetObject"  
      ],  
      "Resource": [  
        "arn:aws:s3::my_bucket/*"  
      ]  
    },  
    {  
      "Effect": "Allow",  
      "Action": [  
        "s3:GetBucketLocation",  
        "s3:ListBucket",  
        "s3:ListBucketMultipartUploads"  
      ],  
      "Resource": [  
        "arn:aws:s3::my_bucket"  
      ]  
    }  
  ]  
}
```

Policy to restrict users to a single folder

The following sample IAM policy restricts user access to a specific folder in the bucket. It grants minimum permissions upload, download or list content, restricted to the folder, as well as allows users to list the bucket and get its location. Replace *my_bucket* with your actual S3 bucket name and *my_folder* with the name of the folder in the bucket.

```
{  
  "Statement": [  
    {  
      "Sid": "AllowUserToReadWriteObjectInFolder",  
      "Action": [  
        "s3:GetObject",  
        "s3:PutObject",  
        "s3:DeleteObject",  
        "s3:ListMultipartUploadParts",  
        "s3:AbortMultipartUpload"  
      ],  
      "Effect": "Allow",  
      "Resource": [  
        "arn:aws:s3::my_bucket/my_folder/",  
        "arn:aws:s3::my_bucket/my_folder/*"  
      ]  
    },  
    {  
      "Sid": "AllowGetBucketLocation",  
      "Action": [  
        "s3:GetBucketLocation"  
      ],  
      "Effect": "Allow",  
      "Resource": [  
        "arn:aws:s3::my_bucket"  
      ]  
    },  
    {  
      "Sid": "AllowListBucketInFolder",  
      "Action": [  
        "s3:ListBucket"  
      ],  
      "Effect": "Allow",  
      "Resource": [  
        "arn:aws:s3::my_bucket"  
      ]  
    }  
  ],  
}
```

```

    "Condition": {
      "StringLike": {
        "s3:prefix": [
          "my_folder",
          "my_folder/*"
        ]
      }
    },
  },
  {
    "Sid": "AllowListBucketUploads",
    "Action": [
      "s3:ListBucketMultipartUploads"
    ],
    "Effect": "Allow",
    "Resource": [
      "arn:aws:s3:::my_bucket"
    ]
  }
]
}

```

Creating AWS IAM roles for transfer service nodes

To add Amazon S3 storage to Aspera on Cloud (AoC) as a node, you must create an IAM role because AWS user credentials are not supported.

You need access to the AWS console and the privileges to create IAM policies and roles for your storage.

Creating the custom S3 access IAM policy

AWS Identity & Access Management (IAM) manages credentials for the transfer service. Attaching policies to these roles grant the associated instances permissions such as starting, stopping, and terminating instances in EC2, or associating IAM roles with a new instance. IAM Roles are also used to provide the transfer service access to your S3 buckets.

The S3 Access IAM policy grants an IAM role the permission to access the specified S3 bucket. An IAM role requires a minimum level of permissions in its policy in order for Aspera to upload, download, or list contents in an S3 buckets. The following table lists the IAM policy rules required for each operation.

Permission	Required for Upload?	Required for Download?	Required for Browse or Delete?
s3:AbortMultipartUpload	Yes	No	Browse & Delete
s3:DeleteObject	Yes	No	Browse & Delete
s3:GetBucketLocation	Yes	Yes	No
s3:GetObject	No	Yes	No
s3:ListBucket	Yes	Yes	Browse
s3:ListBucketMultipartUploads	Yes	Yes	Browse
s3:ListMultipartUploadParts	Yes	No	Browse & Delete
s3:PutObject	Yes	No	No
s3:ListAllMyBuckets	Yes (Required only if the Role does not include a bucket name and the resource is set as "arn:aws:s3:::*")	No	No

If you want to allow access to all of your S3 buckets, you can use the built in policy, AmazonS3FullAccess, instead of creating a custom policy. Otherwise, create the S3 Access IAM policy:

1. In the AWS console, go to Security & Identity > Identity & Access Management and select Policies from the Details sidebar.
2. Click Create Policy. Select the Create Your Own Policy option.
3. Name the new policy ats-s3-policy.
4. Enter the following policy into the Policy Document field to grant access to your S3 bucket.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::your_s3_bucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource": [

```

```

    "arn:aws:s3:::your_s3_bucket"
  ]
}
]
}

```

For example, if your S3 Bucket is named ats-s3-policy, the `Resource` object in the `Statement` section is the following:

```
"Resource": "arn:aws:s3:::ats-s3-policy"
```

Note: For more information on specifying `Resource` in a policy, see "Specifying Resources in a Policy" at <http://docs.aws.amazon.com/AmazonS3/latest/dev/s3-arn-format.html> on the AWS website.

5. Click Validate Policy to check for formatting issues. The policy must be well-formed JSON text.
6. Click Create Policy.

Creating an IAM role for S3 access in the same AWS account

To create the ats-s3-role role, you use the ats-s3-policy policy to grant the transfer service access to the S3 bucket specified in the policy. You must have already created the policy to create the role.

1. From the AWS Console, go to Security & Identity > Identity & Access Management and select Roles from the Details sidebar.
2. Click Create role.
3. Click EC2 to select that role type.
4. Click Next: Permissions.
5. In the Permissions section, select the policy.
Attach the policy to this IAM role to provide access to your S3 bucket. You can either grant your IAM role access to all of your S3 buckets or grant access to selected S3 buckets configured by custom policies:
 - To grant your IAM role access to all of your S3 buckets, select the default AmazonS3FullAccess policy.
 - To grant your IAM role access to specific S3 buckets, select your custom policies such as the ats-s3-policy.
6. Click Next: tags. Tags are optional in this configuration.
7. Click Next, enter the name (for example, ats-s3-role) and description, then Create role

The AWS Console redirects you to the Roles page. The new ats-s3-role role appears in the list of roles.

Creating the trust relationship and adding it to the IAM role

The trust relationship can be created in the AoC GUI, as described in the following steps, or by using the ATS API. For more information about the ATS API, see <https://developer.ibm.com/aspera/docs/ats-api-reference/>.

1. In the Aspera on Cloud UI, go to Admin > Nodes > Create new > Attach my cloud storage.
2. Enter a name for this node.
3. If desired, apply existing node and network policies.
For details, see [Creating network policies](#) and [Creating node configuration policies](#).
4. By default, Amazon S3 storage is selected. Select your region from the drop-down menu and a trust relationship policy is automatically generated for the correct region.
Important: The trust relationship JSON updates with each page load.
 - Before you copy the trust policy, be sure that you have correctly configured the region (step **1g** above).
 - After you copy the trust relationship, be sure to save the configuration or otherwise verify the page is not reloaded.
 If the page reloads after you copy the trust relationship, there will be a mismatch between the trust relationship in AoC and the trust relationship in the AWS console.
5. Copy the trust policy. Open the ats-s3-role role in the AWS Console and paste the policy in the **Trust relationships** tab: Click Edit trust relationships and paste the trust policy.

Creating the transfer service access key

The access key can be created in the AoC GUI, as described in the following steps, or by using the ATS API. For more information about the ATS API, see <https://developer.ibm.com/aspera/docs/ats-api-reference/>.

1. In the Aspera on Cloud UI where you got the trust relationship, select your storage class and server-side encryption, then enter the ARN for IAM role (copy it from AWS Console), the bucket, and the path (enter "/" to allow access to the entire bucket).
2. Review your entries for accuracy and click Save.
3. Save the access key that is generated according to your company policy.
Important! This is your only chance to save the secret. Once you click Done, you can not retrieve the secret. Aspera does not save the secret. Save the key and secret according to your local site security practices.
4. Use the access key to transfer to and from your cloud storage.
 - [Desktop Client GUI](#)
 - [Node API](#)
 Or use the access key to support workspaces in your organization.
 - Share the content in the storage with workspace members. See [Share a node folder with a workspace](#).
 - Use this node as storage to host a workspace. See [Create a new workspace](#).

Installing File preview

Generates a preview on the user files (videos, images, and PDFs) when they are uploaded to S3.

Important: This feature is available for Aspera on Cloud Premium subscribers. To enable the use of the IBM Aspera File preview, you must build a container image with FFmpeg packaged inside. FFmpeg is a free open-source utility, that is not provided or managed by IBM and is subject to third party's terms and conditions. FFmpeg contains codecs for encoding and decoding various video coding formats. Certain codecs contained within FFmpeg may be covered by patents and require a license to use.

The Dockerfile provided by IBM will enable all codecs in FFMPEG by default; however, you must assess your licensing needs in connection with your use of FFmpeg and adjust which codecs to enable accordingly. IBM makes no warranties or conditions, express or implied, and IBM will have no liability to Client, regarding the FFmpeg utility when used with the Cloud Service.

For a list of file types that are available for preview, see [File preview supported file types](#).

Prerequisites

Before you begin, fulfill these requirements:

- Access file preview's public repository at <https://github.com/IBM/aspera-on-cloud-file-previews>
- Install Docker Engine following the official documentation <https://docs.docker.com/engine/install/>.
- You need an AWS account with permissions to create an ECR private repository and push docker images into it.
- AWS CLI installed and configured with [credentials](#).
- In the later steps, you will need to define `aws_access_key`, `aws_secret_key` and `security_token` in the `variables.tf` file under the directory `./terraform-aws/previews`, and which will be used in the `terraform` script.
- Install Terraform following the official documentation <https://developer.hashicorp.com/terraform/tutorials/aws-get-started/install-cli>

Configuring File preview

Update the `./terraform-aws/variables.tf` configuration file depending on your use case.

- **preview_duration**: adjusts the duration of a preview for video files.
 - Default value is set to 15 seconds
 - You can update this value in the AWS Lambda page, inside the Configuration > Environment variables section.
- **preview_audio**: Set this to `true` to enable the audio of preview videos.
- There will be 2 instances of File Preview in AWS Lambda:
 - One with high resources used for the **video** preview processing
 - One with low resources for the **image** thumbnail processing.
 - Depending on the file extension, it will invoke either one of them to reduce **costs** of the running AWS Lambda Instances.
 - You do not need to change the environment variables for `high_resource_lambda_name` nor `low_resource_lambda_name` unless the names for the lambda functions are manually changed outside of Terraform.

Installing File preview

Important: You must wait a few minutes before uploading or transferring new files after the installation is complete.

To install File preview, do the following:

1. Create an AWS ECR private repository (if one does not exist already).

```
aws ecr create-repository \
  --repository-name {repo_name} \
  --image-scanning-configuration scanOnPush=true \
  --region {region}
```

2. Provide Docker access to push docker images in AWS ECR private repositories.

```
aws ecr get-login-password --region {region} | docker login --username AWS --password-stdin {account_id}.dkr.ecr.
{region}.amazonaws.com
```

You can obtain the `{account_id}` value running:

```
aws sts get-caller-identity | grep Account
```

Build the docker images:

3. **Preview**: The main core function to generate the previews for the uploaded files.

Note: There are four different encoders to replace the `encoder` value with: `vp9`, `av1`, `x264`, or `openh264`.

The following code represents an example using `vp9`:

```
cd previews && docker build --build-arg encoder=vp9 -t {account_id}.dkr.ecr.{region}.amazonaws.com/{repo_name}:previews .
```

Note: The value `{repo_name}` has to match the name of the AWS ECR private repository you created in step one.

4. **Previews-checker**: Check existing items in the bucket on a particular path. `previews-checker` calls File Preview on each file that does not have a preview.

```
cd ../previews-checker && docker build -t {account_id}.dkr.ecr.{region}.amazonaws.com/{repo_name}:checker .
```

5. **Previews-filter**: Filters out S3 upload triggers by file extensions using a low resource lambda.

```
cd ../previews-filter && docker build -t {account_id}.dkr.ecr.{region}.amazonaws.com/{repo_name}:filter .
```

6. Push all docker images to your ECR repository.

```
docker push {account_id}.dkr.ecr.{region}.amazonaws.com/{repo_name}:previews
docker push {account_id}.dkr.ecr.{region}.amazonaws.com/{repo_name}:checker
docker push {account_id}.dkr.ecr.{region}.amazonaws.com/{repo_name}:filter
```

7. Update both `aws_secret_key` and `aws_access_key` in `./terraform-aws/previews/variables.tf`. Make sure to use a `security_token` when using short-term credentials. Your account must be able to install the following resources:

- Bucket
- IAM roles and policies
- Lambda functions

Note: You can modify the variables in the `variables.ft` file as needed.

8. Initialize a working directory containing Terraform configuration files.

```
cd terraform-aws/previews
terraform init
```

The Terraform script will create a new bucket. You can also import an existing bucket, to do this **make sure** the `bucket_names` value in `variables.tf` is properly updated and run `./import.sh`. Do the following to find the `bucket_names` for your existing AWS S3 bucket:

- Sign in to your AWS account, and search for the keyword **S3**.
- In the Buckets list, choose the names of the buckets that you want to select, and use those names as the list for the `bucket_names` variable.

9. Create an execution plan that lets you preview the changes that Terraform plans to make to your infrastructure.

```
terraform plan
```

10. Validate the configuration files.

```
transform validate
```

11. Execute the actions proposed in the Terraform plan.

```
terraform apply
```

Using Previews-checker

Previews-checker generates previews for existing files without previews (more specifically for files that were in the bucket before installing File Preview).

1. Define the following parameters to invoke the AWS Lambda function:

- **path**: Location in the bucket where you want to check for previews, and which can also be empty to invoke Lambda function from the bucket root level.
- **bucket**: Bucket name. The associated role should have access to it.

2. Invoke **previews-checker** lambda function with the previously defined parameters.

```
$ aws lambda invoke \
  --function-name {checker_function_name} \
  --invocation-type Event \
  --payload '{ "path": {my_path}, "bucket": {bucket_name} }' \
  --region {region} \
  response.json
```

3. **Optional**: You can delete **previews-checker** if you don't have files without previews.

```
$ terraform destroy --target aws_cloudwatch_log_group.terraform_log_checker --target
aws_lambda_function.terraform_lambda_checker
```

4. **Optional**: Delete the docker image from your ECR private repository.

```
$ aws ecr batch-delete-image \
  --repository-name {repo_name} \
  --region {region} \
  --image-ids imageTag=checker
```

File preview supported file types

Supported file types

Note: AoC does not support previews for audio-only files.

In addition to support for **.pdf** documents, file preview supports the following formats for videos and images.

Video

```
.m2v
.avi
.divx (preview will be displayed as image)
.m4v
.flv
.mp4
.mkv
.h261
.mpg
.wmv
.h263
.mpeg
.mov
.h264
.mxf (preview will be displayed as image)
```

Image

```
.aai
.fig
.pam
.rfg
.art
.fits
.clipboard
.rla
.arw
.fpx
.pbm
.rle
.avs
```

.gif
.pcd
.sct
.bpg
.gplt
.pcds
.sfw
.bmp
.gray
.pcl
.sgi
.bmp2
.hdr
.pcx
.sid
.bmp3
.hpgl
.pdb
.mrsid
.cals
.hrz
.pdf
.sparse-color
.cgm
.ico
.pef
.sun
.cin
.info
.pfa
.svg
.cmyk
.inline
.pfb
.tga
.cmyka
.jbig
.pfm
.tiff
.cr2
.jng
.pgm
.tim
.crw
.jp2
.picon
.ttf
.cur
.jpt
.pict
.uil
.cut
.j2c
.pix
.uyvy
.dcm
.j2k
.png
.vicar
.dcr
.jpeg
.png8
.viff
.dcx
.jpg
.png00
.wbmp
.dds
.jxr
.png24
.wdp
.dib
.man
.png32
.webp
.djvu
.mat
.png48
.wmf
.dng
.miff
.png64
.wpg
.dot
.mono
.pnm
.x
.dpx
.mng
.ppm
.xbm
.emf
.mpc
.ps
.xcf
.epdf

.mpr
.ps2
.xpm
.epi
.mrw
.ps3
.xwd
.eps
.msl
.psb
.x3f
.eps2
.mtv
.psd
.ycbcr
.eps3
.mvg
.ptif
.ycbra
.epsf
.nef
.pwp
.yuv
.epsi
.orf
.rad
.ept
.otb
.raf
.exr
.p7
.rgb
.fax
.palm
.rgba

Attaching storage troubleshooting

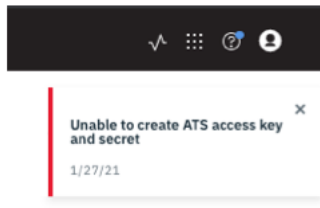
Troubleshoot common issues with attaching your storage to your Aspera on Cloud organization.

- [Trouble creating a new access key](#)
To create a new node and attach storage to your Aspera on Cloud organization, you must create a new access key. Review this procedure if you encounter errors.
- [Tracking your node access credentials](#)
Logging in to a transfer server node with access credentials gives the user full access to the content there. AoC never stores the credentials, so it is imperative that you track and store them according to your site's established security practices.

Trouble creating a new access key

To create a new node and attach storage to your Aspera on Cloud organization, you must create a new access key. Review this procedure if you encounter errors.

If Aspera on Cloud displays the error message "Unable to create ATS access key and secret", verify that the data you entered into each configuration field is accurate. Often this error indicates no more than a typo when entering your storage configuration settings.



This article highlights the fields to verify for each supported storage type.

For all node types, go to Nodes > Create new > Attach my cloud storage.

IBM Cloud

Verify content in the highlighted fields. Ensure there are no typos and that cloud configuration settings are copied accurately.

IBM Aspera on Cloud

Admin

Access key

Storage

IBM COS

Region

Choose an option

Access key ID

Access key secret

Bucket

Path

AWS (Amazon Web Services)

Verify content in the highlighted fields. Ensure there are no typos and that cloud configuration settings are copied accurately.

IBM Aspera on Cloud

Admin

Storage

Amazon S3

Region

us-east-1

Storage class

Standard

Amazon S3 Server-Side Encryption (optional)

None

Select the Amazon S3 encryption-at-rest method. Note: Nodes with server-side encryption enabled do not support watermarking.

Trust relationship policy

```
{
  "Version": "2012-10-17",
  "Statement": [
```

IAM role ARN

arn:aws:iam:123:role/mine

Session name (optional)

Bucket

Path

Microsoft Azure Blob

Verify content in the highlighted fields. Ensure there are no typos and that cloud configuration settings are copied accurately.

IBM Aspera on Cloud

Admin

Storage

Microsoft Azure Blob

Region

eastus

API type

Block

Storage credentials

Key

Storage account

Key

Container

Path

Microsoft Azure Files

Verify content in the highlighted fields. Ensure there are no typos and that cloud configuration settings are copied accurately.

IBM Aspera on Cloud

Admin

Storage

Microsoft Azure Files

Region

eastus

API type

Block

Storage account

Password

Path

GCS (Google Cloud Service)

Verify content in the highlighted fields. Ensure there are no typos and that cloud configuration settings are copied accurately.

IBM Aspera on Cloud | Admin

Storage

Google Cloud

Region

us-west1

Authentication

Private key

Project ID

Client email

client_id@gserviceaccount.com

Private key ID

Private key

Path

Tracking your node access credentials

Logging in to a transfer server node with access credentials gives the user full access to the content there. AoC never stores the credentials, so it is imperative that you track and store them according to your site's established security practices.

AoC access credentials take the form of access keys, each of which is composed of two parts:

- Key ID. For example, N26Y-pfC33hcsOw24keUlzSR
- Secret. For example, Yppsv_iXH5pyFBKe5cvA2nTlaxStd4NYpgjxWA0239_3

Built-in node access credentials

The credentials for the built-in node that is included with your initial AoC subscription are delivered in a digital package to the AoC admin who first created the AoC organization, as described in [Secure the access credentials for your built-in node](#).

Additional access credentials

Over the course of your AoC subscription, you may have reason to create several access keys. For example, you may want to:

- Give a workspace manager access only to specific content on the transfer server rather than all content.
- Give an API client access to specific folders on the transfer server.
- Attach your existing cloud storage to your AoC organization and allow AoC users to access content in it.
- Attach an Aspera server that you manage to your AoC organization and allow AoC users to access content in it.

For procedures, see [Access keys](#).

Recommended practices

Each time you create an access key, you have the option to name it and add descriptive notes. This step is optional but highly recommended to make key management and use easier. If you add a name and notes, they'll be included in the file you download in a following step.

You can add or edit a name and notes for your existing keys. To edit both name and notes, click the node row to open the key details. To edit notes only, right-click the key row and select Edit.

Each time you create an access key, AoC requires you to *download or copy* it to complete the creation process. When you download the key, AoC generates a text file that is always called `KeySecretPair.txt`.

IBM Aspera recommends that you rename this file with a meaningful label and save it to a secure and accessible location according to your local site security practices. Important: Once you close the window that displays your key and secret, you can no longer retrieve the secret. Be sure to save the key and secret in a secure and accessible location according to local site security practices. Aspera on Cloud does not store the secret.

Recovering a lost key

If however, you do not rename the file, you may have to search for the file by the default name. If you've created multiple access credentials without renaming them, you may need to rely on the timestamp to identify each file, doing your best to recall which credentials you created on which days and times. You can combine the timestamp information with the key ID that displays in the AoC interface when you right-click the row of the transfer server, shared folder, etc., and select View access key.

The screenshot shows the IBM Aspera on Cloud Admin interface. On the left is a sidebar with navigation links: Organization, Workspaces, Applications, Users, Groups, Nodes and storage (expanded), Nodes (selected), Network policies, Configuration policies, Settings, Authentication, Integrations, and Subscription. The main area is titled 'Nodes' and contains a table with the following columns: Name, Storage provider, and Hosted by. The table lists several nodes, including 'files-prod-es-tor03.a...', 'Files Internal Dallas ...', 'ATS AWS East', 'Japan ATS Demo', and 'https://ats-aws-us-e...'. A right-click context menu is open over the 'Files Internal Dallas ...' node, showing three options: 'View access key' (highlighted with a red rectangle), 'Update status', and 'Delete'.

Name	Storage provider	Hosted by
files-prod-es-tor03.a...	Amazon S3	IBM Aspera
Files Internal Dallas ...		IBM Aspera
ATS AWS East		Other
Japan ATS Demo	Amazon S3	Other
https://ats-aws-us-e...	Other storage	Other

Simply cannot find your credentials?

If you cannot locate your credentials after a thorough search as described in this article, try the following, based on the type of node.

- For a transfer server that you manage, use your node user name and password to change the secret; see [Tether Your Aspera Transfer Server to Aspera on Cloud](#).
- For cloud storage that you have attached to your AoC organization, use the storage credentials to create a new access key; see [Attach your existing cloud storage](#).

Workspaces

Workspaces are a key organizational unit in Aspera on Cloud. Depending on your AoC subscription, you can configure each workspace with specific security, access, and collaboration settings, add specific members, provide access to specific storage, and enable specific apps like Files and Packages. Delegate specific local admin tasks to a workspace manager. Share specific content from your storage to specific workspace members.

- **What is a workspace?**
The workspace is a collection of Aspera on Cloud users working together—on a project perhaps, or in a department or division. Users in a given workspace can freely collaborate with other members of the same workspace.
- **Create a new workspace**
Each Aspera on Cloud workspace inherits the settings you configure for your organization. However, you can override inherited settings for an individual workspace.
- **Create workspace distribution lists**
As an administrator, you can set up workspace-level distributions lists that you can make available to specific member user types. These workspace user types can select the list in the To field of the Send files form.
- **Delegate to a workspace manager**
If desired, you can grant workspace manager privileges to one or more members in a workspace. A workspace manager can take over certain management tasks in that workspace.
- **Share a node folder with a workspace**
To allow the members of a workspace to use the content in a node attached to your org, an admin must give them access to the content. When you *administratively share* a folder with users, as described in this procedure, all admins in your org can manage the folder access. This shared management ability is typically preferable to having one admin user share a folder as an individual user; in such case, only that individual admin can revoke or change access permissions.
- **Which folders are shared with a workspace?**
You can easily determine which folders in storage an admin has shared with workspace members.

- [Delete a workspace](#)
To avoid loss of data, use caution when deleting a workspace.

What is a workspace?

The workspace is a collection of Aspera on Cloud users working together—on a project perhaps, or in a department or division. Users in a given workspace can freely collaborate with other members of the same workspace.

You need specific permissions, configured by the organization administrator or workspace manager, to collaborate with users outside the workspace.

The users, packages, files, and folders in one workspace are completely separate from those in another workspace.

The workspace name displays in the upper left corner, immediately below the app name (Files or Packages apps).

Membership in multiple workspaces

You may be a member of more than one workspace. You may have different permissions and access in one workspace than you do in another.

If you are a member of multiple workspaces, you can display them by clicking the caret beside the workspace name, then selecting the intended workspace to switch to it. If you have membership in more than five workspaces, you can pin one or more to keep them at the top of your list for convenient access.

Note: Multiple workspaces are available depending on your subscription edition. To see your edition, click the User icon and see Account settings > Account > IBM Aspera on Cloud Edition.

Workspaces in the Packages app

As a workspace member in the Packages app, you send and receive [digital packages](#). You can access your personal inbox ("My Inbox"), which contains the packages sent to you as an individual. You can also access your sent, archived, and deleted or expired packages.

Optional Permissions

You may also have the following capabilities in your Packages workspace:

- Sending to people who are not members of your workspace.
- Sending a [file request](#) to someone outside your workspace, inviting them to send you a digital package.
- Membership in one or more [shared inboxes](#).

Note: Shared inboxes are available depending on your subscription edition.

Workspaces in the Files app

As a workspace member in the Files app, you have access to a collection of folders shared with you by your administrator and by other members of your workspace. When others share a folder, they may share it with you only, or they may share it with multiple people. Your collection of folders may be very different than the collection of another user in the same workspace, though you may share some of the same folders.

The person sharing also grants various [permission levels](#) to these folders and their contents (for example: view, download, delete, and several others); your permission to one folder may be different than your permission to another folder. Similarly, your permission to a folder may be different than the permission another user has to that folder.

Even when folders are shared with multiple members of your workspace, you can move and rename folders without affecting the location and naming of those same shared folders in other users' applications. However, for important conditions regarding deleting shared folders and files from your Files app, see [Delete files and folders](#).

You can share folders in your workspace with other members of your workspace; you may also be able to share folders with people outside your workspace.

Note: In rare circumstances, folders in your workspace may display in red, indicating that they are currently unavailable; contact your administrator or workspace manager for assistance.

Optional permissions

You may also have the following capabilities in your Files app:

- [Uploading](#) files and folders into your Files app workspace; the content you upload remains private to you until you share it with others.
- [Creating new folders](#) in your workspace.
- [Sharing](#) a folder with someone outside your workspace.

Create a new workspace

Each Aspera on Cloud workspace inherits the settings you configure for your organization. However, you can override inherited settings for an individual workspace.

Note: Your ability to create new workspaces depends on your Aspera on Cloud subscription [edition](#).

To create a new workspace, do the following:

- Define and brand it
 - The name label appears to members as the workspace name.
 - The description is available to admin users only, for the purposes of identifying, describing, or distinguishing it from other workspaces.
 - An optional graphic can help identify the workspace to its members.
- Designate the transfer node and folder to store the workspace home folders and packages
 - Accept the default inherited from the organization setting or select from the list of available nodes.
- Designate members

- You can select members from users, user groups, and external users.
 - Designate certain users as managers of this workspace.
- If desired, override the global settings governing the behavior of the applications in the organization. App settings configured globally are inherited by each workspace. You can configure the applications available to users of this workspace, and the settings of each application available to members of this workspace.
- Configure management settings for this workspace.
- Configure email notification templates and delivery settings for this workspace.

Create a workspace

Your ability to create new workspaces depends on your Aspera on Cloud subscription [edition](#).

1. Go to Workspaces > Create new.
2. Enter a name, up to 20 characters in length, that appears to end users as the workspace name; if desired, enter a description visible to administrators only.
3. To brand the workspace with a logo or other graphic, select or drag and drop the graphic to add.
4. To change the [default storage location](#) for this workspace, click the field labeled Node to store home folders and packages field and select the desired node.

Note: If you select a node in AWS storage with an archival storage class (Glacier, etc.), Aspera on Cloud disables the Packages app and limits certain user actions in the Files app in this workspace. For details, see [Attach an AWS S3 bucket](#).

On the node you select, the default storage paths are:

 - For content in the Packages app: `/workspace_id/packages`.
 - For content in the Files app: `/workspace_id/home`.

Note: Once you click Create at the end of this procedure, you cannot change the node that supports it.
5. To select a different storage path, do the following (if you do not select a specific folder, the workspace folder resides on the root level of the node):
 - a. Click to set the toggle labeled Use default storage path to No, then click Choose path.
 - b. Provide access credentials:
 - Enter the node secret and click Log in.
 - Click **Use custom access key**, enter the key and secret, then click Log in.
 - c. To navigate into an existing folder, click the folder row. To return to a previous level of the folder tree, click the breadcrumb and select the intended level.
 - d. To create a new folder on the node, click go to the intended location in the folder tree and click Create folder, name the folder, then click Create.
 - e. Select the folder: click to select the button to the left of the intended folder, then Click Submit.

In the location you select, the storage paths are:

 - For content in the Packages app: `/chosen_folder/packages`.
 - For content in the Files app: `/chosen_folder/home`.
6. Click Save.

Add members to a workspace

The Members tab appears after you create the workspace.

1. Click Members > Add members.
2. Enter the names of existing users or user groups to add as members to this workspace.

If you add user groups, the members of the group inherit membership in the workspace. For related details, see [Direct and inherited memberships](#).
3. To make a member a [manager](#) of this workspace, click Workspace manager on the user row.
4. Click Add.
5. To remove a member, select the user row, then click **Revoke** in the table header.

If a member has both direct and inherited membership, see [Direct and inherited memberships](#) for a procedure to remove them from the workspace.

AoC sends this user an email notification inviting them to join the workspace, including a direct link to the workspace.

Note that individual users can configure their email notifications settings, including this one, by clicking their user icon in the upper right of the app and selecting Account settings. If the email notification does not arrive, the user should check these settings. If the issue persists, see [Email notifications](#).

Configure applications for a workspace

By default, the Files and Packages apps are available for all users in each workspace when these apps are enabled for the organization. For details, see [Applications: Overview](#).

Apps in a workspace inherit the settings configured globally for the organization. You can override the inherited settings for a workspace if desired.

For details and procedures, see [Packages app: Send and receive files and folders](#) and [Files App: Using a shared file repository](#).

Note: The **Applications** tab appears after the workspace is created.

Configure manager settings for a workspace

You can designate one or more members of a given workspace to be a manager of the workspace. You can then delegate these specific management tasks to the workspace manager:

- Configure email delivery settings
- Configure the Files app for this workspace
- Configure the Packages app for this workspace

For details, see [Assign the workspace manager role](#).

Note: The **Settings** tab appears after you create the workspace.

Configure email templates and notification settings for a workspace

Email notification templates and delivery settings for a workspace are inherited from the global email settings configured for your organization. You can override global settings for a given workspace. See [Customize email notification templates](#) and [Control email notification delivery](#).

Note: The **Email settings** tab appears after the workspace is created.

Create workspace distribution lists

As an administrator, you can set up workspace-level distributions lists that you can make available to specific member user types. These workspace user types can select the list in the To field of the Send files form.

Users can create [personal](#) distributions lists as well. All distribution lists respect admin settings in the Package app. This means that no matter the members listed for any distribution list, Aspera on Cloud delivers the package only to valid recipients as configured in Workspaces > Applications > Packages > Collaboration.

1. Go to Workspaces and select the intended workspace. Then click Distribution lists.
2. Click Create new.
3. Give the distribution list a name that is unique across the organization; be sure the name is meaningful to your intended users.
4. Select which user type can use the list: All Workspace members or only Workspace managers.
5. Click Create.
6. Click Members, then click Add members.
7. Enter the user names, groups, and email addresses for this list.
8. Click Add.

This distribution list is now available in the workspace you selected in step 1 for the user type that you selected in step 4.

Delegate to a workspace manager

If desired, you can grant workspace manager privileges to one or more members in a workspace. A workspace manager can take over certain management tasks in that workspace.

For example:

- Adding and removing workspace members.
- Creating and managing groups.
- Granting and revoking workspace manager privileges to other users in the same workspace.
- Manage email notification templates and delivery options.
- Manage the settings of the Files app in the workspace.
- Manage the settings of the Packages app in the workspace, including shared inboxes.

The workspace manager role is optional, since organization administrators can manage every aspect of all workspaces. The workspace manager must be a member of the workspace.

Access keys

You can [generate an access key and secret](#) to a folder on a transfer node that you have shared to a workspace ("administratively shared folder"). You can give this key pair to a workspace manager to allow them to manage content in this shared folder without giving the manager access to other content on the node.

Privacy in a multi-tenant organization

In a multi-tenant organization, when strict privacy between workspaces is required, you can ensure that workspace managers cannot see organization members beyond those in the groups they are enabled to manage. Otherwise, workspace managers can see the users and groups across the entire organization during operations like adding a member to a shared inbox, to a group, or to a workspace. Control this privacy setting at Organization > Advanced settings > Workspace manager privileges. The setting you configure here applies to all workspace managers in the entire organization.

For more information, see [Assign the workspace manager role](#).

Delegate app and email configuration

To delegate configuration of the Packages and Files apps and of email notifications in a specific workspace, do the following.

1. Go to Workspaces > *workspaceName* > Settings.
2. Select checkboxes for these settings:
 - a. To allow workspace managers to configure the email templates and delivery options for the workspaces they manage, allowing them to override the email settings inherited from the global org settings, select the box labeled Workspace managers can edit email settings.
 - b. To allow workspace manager to configure the Files app in the workspaces they manage, allowing them to override the Files app settings inherited from the global org settings, select the box labeled Workspace managers can edit the settings of the Files application.
 - c. To allow workspace manager to configure the Packages app in the workspaces they manage, allowing them to override the Files app settings inherited from the global org settings, select the box labeled Workspace managers can edit the settings of the Packages application.
3. Click Save.

To reserve these configuration responsibilities for org admins, clear the checkboxes.

Share a node folder with a workspace

To allow the members of a workspace to use the content in a node attached to your org, an admin must give them access to the content. When you *administratively share* a folder with users, as described in this procedure, all admins in your org can manage the folder access. This shared management ability is typically preferable to having one admin user share a folder as an individual user; in such case, only that individual admin can revoke or change access permissions.

Use this procedure to give users in the Files application:

- Shared access to content in your cloud or on-prem storage.
- A folder in which they can collaborate on content according to the permissions you set.

Once you share the folder using this procedure, users see it on the top level of their Files app.

For each folder you share, you set permissions for each user and group you share with. These permissions determine the actions that users can take on the folder contents. For details, see [Content Permissions](#).

This procedure allows you to share one folder at a time with one or more members of a single workspace. To share multiple folders, or to share a folder with users in multiple workspaces, repeat the procedure

Procedure

Note: To complete this procedure, you need the secret of the node containing the folder you want to share.

1. Go to Workspaces > *workspaceName* > Applications > Files app > Shared folders > Create new.
2. Do one of the following:
 - Enter the node secret and click Log in.
 - If you have a different access key for this node, click **Use custom access key**, enter the key and associated secret, then click **Log in**.
3. (Optional) To create a new folder on the node, do the following:
 - a. Click Create folder.
 - b. Enter a name for the new folder and click Create.
4. From the list of folders that displays, select the folder to share by clicking the option button on the folder row.
If required, you can click a folder name to drill into it. Go back up a level using the breadcrumb list at the top of the modal.
5. (Optional) To display a different name for the folder to the workspace users (perhaps a name that may be most meaningful to them), enter the desired name in the Display name text box.
6. Click Submit.
7. To give all members of the workspace access to this folder, click Add all workspace members.
 - a. Set the access permission level for these users.
 - b. If desired, add other members you want to access this folder at the permission level you set.
 - c. Click Add.
8. To give specific workspace members access to this folder, click Add member.
 - a. Set the access permission level for these users.
 - b. Enter the names of workspace members which whom to share this folder at this permission level.
 - c. Click Add.
9. To change a user's access to the shared folder, click the user row to open the record, adjust permissions as required, then click Save.
10. To remove a user's access to the shared folder, select the check box to the left of the user row and click Delete.

Note:

When new members join the workspace Files app, they can see and access shared folders as follows:

- Folders shared with the entire workspace.
- Folders shared with the new member as an individual or as a group member.

Add a member to an existing shared folder

1. Go to **Workspaces > *workspaceName* > Applications > Files app > Shared folders**.
2. Right-click the intended folder to see the current member list.
3. Do one of the following:
 - Enter the node secret and click Log in.
 - If you have a different access key for this node, click **Use custom access key**, enter the key and associated secret, then click **Log in**.
4. Click Add member.
5. Select the access permission for this new member.
6. Enter the member name.
7. Repeat steps 5 and 6 for additional new members.
8. Click Add.

Node access for workspace managers

1. Go to Workspaces > *workspaceName* > Profile > Node access for workspace managers.
2. Click Add.
3. In the Name drop down, select the node you want to give access to.
4. In the Access key field, enter the access key provided by your administrator.
5. In the Secret field, enter the secret associated with the access key.
Click the eye icon to show or hide the secret as you type.
6. From the Node owners drop down, select who can manage the node:
 - a. Only ATS admins: Only ATS administrators can manage the node.
 - b. All admins: All administrators can manage the node.

Note: Node owners can browse and manage this node without the need of an access key.
7. Click Log in to save the configuration and establish node access.
8. Click Cancel if you do not want to save the configuration and exit.

Which folders are shared with a workspace?

You can easily determine which folders in storage an admin has shared with workspace members.

Go to Workspaces > *workspaceName* > Applications > Files > Shared folders.

The listing includes the following:

- Name: The name of the folder on the node
- Shared as: The folder name that appears to those the folder is shared with
- Node: The node hosting the shared folder
- Last updated: Date and time of last change to content in the shared folder

Delete a workspace

To avoid loss of data, use caution when deleting a workspace.

CAUTION:

When you delete a workspace, you permanently delete all workspace data (links, memberships, and so on); they cannot be retrieved. Content on the transfer server is not deleted.

1. Go to Workspaces to display the list of workspaces.
2. On the row of the workspace to delete, click the Delete icon.
3. Click Delete again to confirm.

Users and groups

Understand and assign user types and roles. Create and manage users and groups. Manage memberships in workspaces, shared folders, shared inboxes, and more. Troubleshoot membership issues.

- [Users, groups, and roles](#)
Learn how to create users and groups, and how to assign roles like workspace manager, admin, and ATS admin. Included is how to manage inactive users with greatest efficiency, especially useful for organizations with intermittent and project-based contributors.
- [Content access: User permissions and memberships](#)
Understand how to assign permissions and memberships so your content is secure and your teams are most effective. Learn about direct and inherited memberships in workspaces, shared folders, shared inboxes, and applications like Files, Packages, Automation, and Activity.
- [Membership Troubleshooting](#)
Address membership issues when undesired access persists.

Users, groups, and roles

Learn how to create users and groups, and how to assign roles like workspace manager, admin, and ATS admin. Included is how to manage inactive users with greatest efficiency, especially useful for organizations with intermittent and project-based contributors.

- [User roles and types](#)
Each Aspera on Cloud user has a role, type, and status; these attributes help define the activities permitted to each user.
- [Create and manage users](#)
Add users to your organization to give them access to Aspera on Cloud functions and content.
- [Create and manage groups](#)
Create user groups in Aspera on Cloud to make addressing and managing multiple users easier.
- [Assign the organization administrator role](#)
An org admin has full administrative rights in your Aspera on Cloud org, with these exceptions: creating a new ATS node and creating a new ATS admin.
- [Assign the ATS administrator role](#)
The ATS admin can attach cloud storage to Aspera on Cloud by creating a new Aspera transfer service (ATS) node, and then give Aspera on Cloud workspace members access to content in the cloud storage. There can be one or more ATS admins in the org. An ATS admin is an org admin and may or may not be a member of a workspace.
- [Assign the workspace manager role](#)
A workspace manager is a member of a workspace with certain management privileges in that given workspace. This is an optional role in a workspace, since administrators can manage workspaces as required. Any number of user accounts can be designated as manager for a given workspace.
- [Manage inactive users](#)
You can automatically deactivate users who have not logged in for a specified number of consecutive days. Automatic deactivation can be particularly useful when your work is project-based. While a project is active, your users need access to key digital assets and to the collaboration tools that AoC delivers. Between projects, you need to limit access to sensitive content.

User roles and types

Each Aspera on Cloud user has a role, type, and status; these attributes help define the activities permitted to each user.

The Aspera on Cloud user roles, types, and statuses are:

- Global roles
 - Organization administrator
 - ATS (Aspera transfer service) administrator
 - User
- Workspace roles
 - Workspace manager
 - Member

- User types
 - Standard
 - Limited
- User status:
 - Active
 - Pending
 - Deactivated

Administrators can filter the AoC user listing by role (org admin, ATS admin, user), by type (standard, limited), by authentication method (IBMid, SAML, Google), and status (active, deactivated, pending). Go to **Users** in the Admin app.

Organization administrator

There may be one or more administrators in an organization. An administrator is a member of the organization and may or may not be a member of a workspace.

Users assigned this role can do the following across the entire organization:

- Configure authorization (OAuth, SAML, etc.) settings for the organization.
- Configure branding for the organization and for workspaces.
- Configure and manage nodes and storage.
- Share content from configured nodes to Aspera on Cloud users.
- Delete content from configured transfer nodes.
- Monitor all activities.
- Monitor all transfers.
- Create, manage, and delete workspaces, including shared inboxes.
- Assign the administrator role for the organization.
- Assign the manager role for a workspace.
- Create, manage, and delete users, outside users, and groups.
- Assign the owner and manager roles for groups.
- Configure email notification templates (globally, per workspace, and per shared inbox).

ATS (Aspera transfer service) administrator

Note: A user must be an Aspera on Cloud administrator to be assigned this role.

There may be one or more ATS admins in the org. An ATS admin is an org admin and may or may not be a member of a workspace.

A user can be assigned the ATS admin role in either of two ways:

- Be the initial creator of an Aspera on Cloud organization.
- Be assigned the role by an existing ATS administrator.

An ATS admin has these additional administrative privileges:

- Create a transfer service node. For procedures, see [Attach your existing cloud storage](#).
- Assign ATS admin privileges to another org administrator.

Workspace manager

A workspace manager is a member of a workspace with certain management privileges in that given workspace. This is an optional role in a workspace, since administrators can manage workspaces as required. Any number of user accounts can be designated as manager for a given workspace.

Note: The organization administrator configures the initial manager for a given workspace. Users with workspace manager privileges can grant and revoke that role for other workspace members.

Users assigned this role can do the following for the managed workspace only:

- Edit the workspace profile, including branding, description, and naming.
- Add, manage, and remove workspace members, including granting and removing manager privileges.
- Create and manage groups.
- View workspace activity.
- In the Packages app, create, manage, and delete shared inboxes (including metadata and shared inbox members).
- In the Files app, share folders from storage to one or more workspace members (requires node secret).
- If specifically granted by the org admin:
 - Manage settings for the Files and Packages apps in that workspace.
 - Configure email notification templates and delivery options.

See also [Delegate to a workspace manager](#).

Standard user

Standard users have membership in at least one workspace in the organization and can do the following:

- If the standard user is a member of the Packages app in a workspace:
 - Send content to anyone in their workspace.
 - Get to know about other member of the workspace through the auto-complete function of the **Send files** window.
 - Download packages or package contents.
 - Invite others to send a package.
 - If Packages app collaboration settings (configured by administrator or workspace manager) permit:
 - Send packages to users outside the workspace and to colleagues without an Aspera on Cloud account.
 - Share files and folders with users outside the workspace and with colleagues without an Aspera on Cloud account.
 - Invite outside users to submit content.

- If Packages app shared inbox privileges permit, send and receive content using an AoC shared inbox; invite outside users to join a shared inbox .
- If the standard user is a member of the Files app in a workspace:
 - Share folders with anyone in their workspace.
 - Get to know about other member of the workspace through the auto-complete function of the **Share** window.
 - Assign access permissions for each folder for each person shared with.
 - Access folders shared with them according to the permission granted by the person who shared.
 - Download from their own Files app (if folder permissions permit).
 - If Files app collaboration settings permit:
 - Upload to their own Files app.
 - Create new folders in their Files app.
- In Account settings (click the user icon in upper right of the interface, select **Account settings**):
 - Upload a user image.
 - Manage certain email notification settings.
 - Set a default language for AoC.
 - Set a default application, which opens automatically upon log in.
 - Set a default workspace, which opens automatically upon log in.

Limited user

Limited user are members of an AoC organization who do not have membership in any workspace. They appear in the organization user listing with their type listed as "Limited".

For example, an org admin or ATS admin may have no need for workspace membership. They can complete management tasks from the Admin app and may have no need to access the user functions of the Files or Packages apps.

As another example, when a member of a shared inbox with **Add users** permission adds a user who does not have AoC membership to the inbox, that user becomes a limited user of AoC. They can send packages to the specific shared inbox, but they do not have membership in any workspaces in the organization.

User status

- **Active:** Active users have logged in to the organization at least once.
- **Pending:** Pending users have received an invitation to join the organization but have not yet done so. The account remains in the pending state in the user database. The admin can re-invite a pending user.
- **Deactivated:** Active or pending users can be deactivated by the administrator. The account remains in the user database, but the user cannot access their account or run API requests. The admin can reactivate a deactivated account.

Note: Deleted users don't appear in the user listing. Usage incurred by users who are later deleted remains recorded in the Activity app, although you cannot filter for the activity of a deleted user. Folders shared by a user remain available even after the user is deleted. But a submission link issued by a user of the Packages app becomes invalid when that user is deleted.

Create and manage users

Add users to your organization to give them access to Aspera on Cloud functions and content.

Note: For details on the various user roles and privileges, see [this article](#).

Important: If a workspace manager attempts to create a user who is already a member of the organization, they may receive the following message: `Encountered error trying to process the full operation. Please check the new users and verify all memberships and settings.` This error typically occurs when the user you are trying to add is already part of the organization. To resolve this, review the user's existing memberships and confirm their settings before attempting to add them again. For more information, refer to the [Manage workspace memberships and roles](#) section.

When you create a new user in Aspera on Cloud, you can configure the following for that user:

- Email address
- Identity provider for login
- Workspace membership
- Group membership and role
- Optional Aspera on Cloud administrator privileges
- Optional transfer service administrator privileges (requires Aspera on Cloud administrator privileges)

Note:

A user must be a member of a workspace to use the Files and Packages applications; see [Create a new workspace](#) for a procedure.

To create a new user in your Aspera on Cloud application, do the following:

1. Go to Users > Create new.
2. In the Email field, enter one or more user email addresses; these become the user login names.
3. Select the identity provider (IdP) that the new user should use to log in to Aspera on Cloud.
 - The menu contains the identity providers configured for this organization in **Admin > Authentication**. If you don't see the IdP you expect, configure it for your organization in that location.
 - If you select **IBMid**, Aspera on Cloud sends the new user an email invitation to join the organization. The email contains a link that allows them to create an account and log in.
 - To allow users to log in through one SAML provider only, select that specific SAML provider.
 - To allow your users to login through multiple SAML providers, set the Authentication type to **Any identity provider**.
 - Unless you select **Any identity provider**, the user must log in using the identity provider you select.
 - If you select **Any identity provider**, the user can log in using any configured authentication method for which they have valid credentials.
4. To make this user a member of a workspace (required to use the Files and Packages apps), click Add to workspaces.
 - a. Enter the workspace name.
 - b. To set the user's role in that workspace, select Member or Manager.
 - c. Click Add.

5. To make this user a member of a group, click Add to groups. This user will inherit the memberships and privileges assigned to this group.
 - a. Enter the name of one or more groups.
 - b. Click Add.
6. To give this user transfer service administrator privileges in the Aspera on Cloud organization, select the check box labeled Transfer service admin. This privilege includes organization admin privileges.

Note:
You must be a transfer service administrator to see this setting and to grant this privilege to another user.
7. To give this user administrator privileges in the Aspera on Cloud organization, select Organization admin.
8. Click Create user.

Update a user record

You can update a user's email address directly in AoC only if the user logs in to AoC directly, rather than through an external authentication system or identity provider like IBMid or a SAML system.

For a user who logs in through an external system, you must change the user's name and email address in the external system. However, even after the update in the external system, the user must continue to log in to AoC using their *original* email address. AoC sends email notifications to the *new* email address.

You can make the following changes to an existing user record:

- Upload a profile photo (click Upload to open your Finder or Explorer). Individual users can open their Account settings to upload their own photo.
- Enter the user's public key for use with an [API client](#). Individual users can open their Account settings to update their own public key.
- Update the identity provider this user can use to log in to Aspera on Cloud.
 - If this user was assigned an IdP that has since become unavailable, the authentication type for this user shows as "Deleted." You must assign an available IdP for this user.
- Assign or remove workspace or group memberships.
- Assign or remove administrator privileges.
- If the user has never logged in ('pending' status), click Re-invite to send a new email invitation.
- Click Deactivate to prevent a user from logging in without deleting their account. A deactivated user cannot log in or run API requests. Click Reactivate to reactivate a deactivated user account. For related information, see [Manage inactive users](#).
- Click Delete to remove the user account entirely from the user listing. Usage incurred by users who are later deleted remains recorded in the Activity app, although you cannot filter for activity by a deleted user. Folders shared by a user remain available even after the user is deleted. But a submission link issued by a user becomes invalid when that user is deleted.

Note: When you delete a user, you do not delete the user's packages, files, or folders. To browse, share, or delete a user's content, see [Managing storage usage](#).

Create and manage groups

Create user groups in Aspera on Cloud to make addressing and managing multiple users easier.

Create a new group

To create a new group in your Aspera on Cloud application, do the following:

1. In the Admin Management console, go to Groups.
2. Click Create new.
3. Enter a name, which appears to end users as the group name.
4. Enter an optional description, visible to administrators only.
5. To make this group a SAML group, select the check box and enter the SAML distinguished name (DN) as defined at the IdP.

Note: See [Configuring SAML Authentication: Overview](#) and [Configuring SAML Authentication: Procedures](#).
6. Click Save.

Once you create this group, you can return to the group record and click **Delete** to remove the group from Aspera on Cloud.

Add members to the group

Once the group exists, you can add members from the existing organization users.

1. Click Members > Add member.
2. Enter the name of the first user to add; Aspera on Cloud returns the list of users that conform to your search string. Press Enter on your keyboard to add the intended user to the list.
3. If required, enter additional user names.
4. To remove a user from this list, click X on the user row.
5. Click Add.

Remove a member from the group

1. Browse, filter, or search for the user to remove.
2. Hover over the user row, then click Actions (three dots) icon to the right.
3. Select Revoke, then confirm to remove the user from this group.

Designate a group manager or group owner

You can designate existing users and groups in the organization as managers or owners of a group; however, only users with organization admin or workspace manager privileges can actually administer these groups since such group administration requires access to the Admin app. Following are the privileges held by these roles.

Group managers and owners may or may not be group members. Assigning manager or owner roles does not assign the member role.

- Group manager
 - Can add and delete members to the group. During the 'Add member' operation, the member field auto-completes, as do many member fields in AoC. If the group manager is a workspace manager rather than an org admin, the auto-complete entries are limited to:
 - All users and groups from the workspaces in which they are members, including their own personal contacts.
 - All members of groups they manage or own.
 - Can assign manager role to another user.
- Group owner
 - All privileges of group manager role.
 - Can assign owner role to another user.
 - Can edit group profile.
 - Can delete the group.

Note: You automatically have owner privileges for a group if:

- You created the group.
- You are an organization administrator. If you lose the admin role, you lose the group owner role. A group owner can enable the same role for you if required, although you must have at least workspace manager privileges to be a group owner or manager.

Keep in mind that group manager and owner privileges can be passed along by existing owners and managers, and group membership can be changed by group owners and managers across the various workspaces they manage.

To designate a group manager or group owner, do the following:

1. Go to Groups > *groupName* > Managers > Add managers.
2. Select the role: Manager or Owner.
3. Enter one or more user names.
4. To remove a user from this list, click X on the user row.
5. Click Add.
6. To change the assigned role, click the user row to open the record and select the intended role, then click Save.

To remove owner or manager role from a user:

1. Click Edit on the user row.
2. Select the role and click Save.

Add or remove a group from a workspace

When you add a group to a workspace, each member of the group becomes a workspace member. When a user gains workspace membership through a group, that user has *inherited* membership in the workspace.

To add this group to one or more workspaces:

1. Go to Groups > *groupName* > Managers > Workspace memberships > Add workspaces.
2. Select Member or Workspace manager to determine the role members of this group have in the workspaces you select.
3. Enter one or more workspace names; then click Add.
4. To remove this group from a workspace, right-click the workspace row and select Revoke, then confirm.
For details about removing inherited membership, see [Direct and inherited memberships](#).

Assign the organization administrator role

An org admin has full administrative rights in your Aspera on Cloud org, with these exceptions: creating a new ATS node and creating a new ATS admin.

There can be one or more administrators in an organization. An administrator is a member of the organization and may or may not be a member of a workspace or an app.

To create a new user, see [Create and manage users](#).

To add org admin privileges to an existing user, do the following:

1. Go to Users > Management.
2. Browse or filter for the intended user, then click the row to open the user record.
3. Select the Organization admin checkbox.
4. Click Save.

Remove admin privileges by clearing the checkbox and saving.

Assign the ATS administrator role

The ATS admin can attach cloud storage to Aspera on Cloud by creating a new Aspera transfer service (ATS) node, and then give Aspera on Cloud workspace members access to content in the cloud storage. There can be one or more ATS admins in the org. An ATS admin is an org admin and may or may not be a member of a workspace.

A user can be assigned the ATS admin role in either of two ways:

- Be the initial creator of an Aspera on Cloud organization.
- Be assigned the role by an existing ATS administrator.

To create a new user, see [Create and manage users](#).

You must be an ATS admin to complete this procedure.

Do the following:

1. Go to Users > Management.
2. Browse or filter for the intended user, then click the row to open the user record.
3. Select the ATS admin checkbox.
If you are not yourself an ATS admin, you cannot see this setting.
4. Click Save.

Remove ATS admin privileges by clearing the checkbox and saving.

Assign the workspace manager role

A workspace manager is a member of a workspace with certain management privileges in that given workspace. This is an optional role in a workspace, since administrators can manage workspaces as required. Any number of user accounts can be designated as manager for a given workspace.

The organization administrator configures the initial manager for a given workspace. Users with workspace manager privileges can grant and revoke that role for other workspace members.

Users assigned this role can do the following for the managed workspace only:

- Edit the workspace profile, including branding, description, and naming.
- Add, manage, and remove workspace members, including granting and removing manager privileges.
- Create and manage groups.
- View workspace activity.
- In the Packages app, create, manage, and delete shared inboxes (including metadata and shared inbox members).
- In the Files app, share folders from storage to one or more workspace members (requires node secret).
- If specifically granted by the org admin:
 - Manage settings for the Files and Packages apps in that workspace.
 - Configure email notification templates and delivery options.

To create a new user, see [Create and manage users](#).

To add workspace manager privileges to an existing workspace member (an individual user or a group), do the following:

1. Go to Workspaces > *workspaceName* > Members.
2. Browse or filter for the intended user or group, then click the row to open the user record.
If the intended user is not a member of this workspace, click Add members, select Manager, and click Add.
3. Select the checkbox labeled This member can manage this workspace.
Remove workspace manager privileges by clearing the checkbox.
4. Click Save.

Remember that any given user or group may have both direct and indirect roles and memberships; to remove workspace manager privileges for a user, you may have to remove them from a group with workspace manager privileges as well. For details, see [Direct and inherited memberships](#).

Configure workspace manager auto-complete privacy

This setting determines which users and groups a workspace manager can see through the auto-complete function. Auto-complete acts when entering user or group names during the following operations:

- Adding members to a workspace, group, shared inbox, or shared folder.
- Sending package (recipients field).
- Sharing submission link (recipients field).

Such visibility is especially sensitive in a multi-tenant or reseller organization when strict separation between workspaces within the organization is required to ensure privacy for tenants.

- By default, workspace managers can see all users and groups in the entire organization, including in workspaces in which they are not members, along with the personal contacts of all users (including outside users).
- Alternatively, workspace managers can see only users and groups from the workspaces in which they are members, along with their own personal contacts in any workspace and with outside users.

Keep in mind that the alternative setting does not prevent workspace managers from adding users or recipients beyond their own contacts. But contacts beyond their own will not appear as selections through auto-complete. Instead, workspace managers must enter the entire username or email address manually.

Note: Workspace and application collaboration settings also affect the way workspace managers can interact with users outside the workspace and organization.

To configure this setting for your organization, do the following:

1. Go to **Organization > Advanced settings > Workspace manager privileges**.
2. Select the desired setting, then click **Save**.

Manage inactive users

You can automatically deactivate users who have not logged in for a specified number of consecutive days. Automatic deactivation can be particularly useful when your work is project-based. While a project is active, your users need access to key digital assets and to the collaboration tools that AoC delivers. Between projects, you need to limit access to sensitive content.

You can deactivate users who will need access to your org assets in the future. Delete users you won't work with again.

Deactivated users have no access to your assets. They cannot log in or run API requests. When required, you can reactivate these users to restore their previous access, permissions, and settings.

Automatically deactivate inactive users

Manually filtering for and deleting users based on their inactivity duration would be tedious and prone to error. Furthermore, the process would be an ongoing maintenance task. Avoid the tedium and potential for errors by automating the deactivation of inactive users.

Keep in mind that deactivation occurs immediately and retroactively when you configure and save this parameter. For example, enable the function and configure 15 days as the inactivity threshold. AoC deactivates all users who have not logged in for 15 or more consecutive days immediately preceding the day you click Save. From that point forward, AoC deactivates users as soon as they meet your configured criteria.

Notifications

Track automatic deactivation events with notifications that list deactivated user accounts in digest form. See [Control email notification delivery](#) for details and procedures. When these notifications are enabled, they are delivered to all org admins. An individual administrator can suppress them by deselecting that notification in their own account settings (User icon > Account settings > Notification settings).

Procedure

To configure automatic deactivation of inactive users, do the following:

1. Go to Users > Advanced.
2. Select the labeled Deactivate inactive users to On.
3. Enter the inactivity duration. This is the number of consecutive days without logging in.
4. Click **Save**.

Automatic user reactivation

To enable the automatic reactivation of users, do the following:

1. Go to User > Advanced > Auto reactivation.
2. For users who were deactivated due to inactivity, check the box next to the Automatically reactivate users when they receive a package option.
3. For SAML users who were deactivated due to inactivity, check the box next to the Automatically reactivate SAML users when they log in via their SAML provider option.

Note: Auto reactivation rules only apply for users who are deactivated due to inactivity. These rules do not apply if a user is deactivated by an admin

Manual user reactivation

To manually reactivate inactive users, do the following:

1. Go to Users > Management.
2. Set the **Status** filter to Deactivated.
3. Do one of the following to select the deactivated users to reactivate:
 - To select all currently deactivated users, select the check box at the top of the list.
 - To select specific deactivated users, select the check box by each intended user.
4. Click **Activate** at the top of the user listing.

These reactivated users can now log in. Previous settings, memberships, and permissions for each user remain unchanged.

Content access: User permissions and memberships

Understand how to assign permissions and memberships so your content is secure and your teams are most effective. Learn about direct and inherited memberships in workspaces, shared folders, shared inboxes, and applications like Files, Packages, Automation, and Activity.

- [Content permissions](#)
You have a specific permission or access level for each file or folder in your Files app. Check your permission to a given folder by right-clicking and selecting Info.
- [Direct and inherited memberships](#)
An user or user group in an organization can have direct or inherited membership – or both – in an org entity like a workspace, application, or group.
- [Manage workspace memberships and roles](#)
Users in your Aspera on Cloud organization are typically members in one or more workspaces. In fact, to use the Packages and Files apps to send or share files and folders, users must be members of a workspace. Use this article to add or remove workspace membership to or from a user or group, and to manage roles within a workspace.
- [Manage shared folder memberships](#)
A member or *collaborator* in a shared folder has access to folder contents according to the permissions given by the member who shared the folder with them.
- [Manage shared inbox memberships](#)
As an admin, you can manage membership in shared inboxes, including the permissions and membership expiration.
- [Manage application memberships](#)
When the Files or Packages apps are enabled for a workspace, all workspace members can use the app. To give users access to the Activity and Automation apps, you must specifically add them as app members.
- [Manage group memberships and roles](#)
Create user groups in Aspera on Cloud to make addressing and managing multiple users easier.

Content permissions

You have a specific permission or access level for each file or folder in your Files app. Check your permission to a given folder by right-clicking and selecting Info.

There are four preset or composite permissions and seven custom permissions for content in your Files app:

- Preset or Composite permissions:
 - **Edit** (also called *Can Edit*)

This is the highest level of permission and gives a user full control over the item; it contains all other permissions.
 - **View** (also called *Download Only*)

Includes *Browse*, *Download*, and *Preview* permissions.
 - **Upload**

Includes *Create/Upload folders* and *Upload files*
 - **Preview**

Includes *Browse* and *Preview*
- Custom permissions (content must reside on a transfer server with node software at version 3.7.4 or higher; see the "Package Information" section of the IBM Aspera High-Speed Transfer Service [Release Notes](#) for specific build numbers for your platform):
 - **Create/Upload folders**

Create or upload an empty folder; to upload folders containing files, enable this permission along with *Upload files*.
 - **Rename**

Rename files and folders.
 - **Upload files**

Upload files and folders; to upload folders containing files, enable this permission along with *Create/Upload folders* permission -- or use *Upload* composite permission. See *Delete* below for uploading a file with the same name as an existing file (overwrite or replace). You need *Upload* permission to a folder to move or copy content to it.
 - **Download**

Download the folder or file in the folder.
 - **Preview**

Preview movie files in the folder. Thumbnail previews of supported image tiles are always available.
 - **Browse**

Browse folder content; if this setting is not enabled, you can see the folder but cannot view folder contents.
 - **Delete**

Delete or overwrite files and folders in the folder.

The permission you have to a given file or folder depends upon how you gained access to it. Check your permission to a given folder by right-clicking and selecting Info.

- For items you upload to the root level of your Files app, and for items you move from a package in your Packages app to the root level of your Files app, you have full *Edit* permission (requires *Upload* permission to the root level; if your administrator has restricted upload capability to the root level of your Files app in this workspace, you can upload only to folders to which you have upload permission, not to the root level).
- For items you upload or move into a folder, you have the same permission that you have to the folder.
- For folders shared with you, you have the permission granted to you by the person who shared.

Note: The person who shared a folder with you is the only person who can change your permission to that folder.

The person sharing can grant you only the permissions they have to the given folder, or a lesser permission; for example, if I have **Browse**, **Preview**, and **Download** permission, I can grant you one or more of those three permissions, but I cannot grant you **Delete** permission, since I myself don't have **Delete** permission.)

In the same way, the permission you can grant to a folder you share depends on the permissions you have to that folder. You can grant any or all of the permissions that you yourself have to that folder, but you cannot grant a permission that you do not have.

Internal and other permissions

An administrator or workspace manager may see a shared item identified as having an "Internal" or "Other" permission. These permission may appear only when you set the advanced filter to Show all permissions.

This identification can indicate a number of different scenarios, as follows:

- Internal permission: workspace folder
This permission was created by the system to display and track shared folders in Aspera on Cloud.
- Internal permission: application
This permission was created by the system for internal purposes.
- Other permission: node or other app
This permission was created by an admin on an attached node, by an API user, or by a user of another app like Aspera Drive.
- Created by the Automation app
This permission was created in an automated workflow in the Automation app.

Direct and inherited memberships

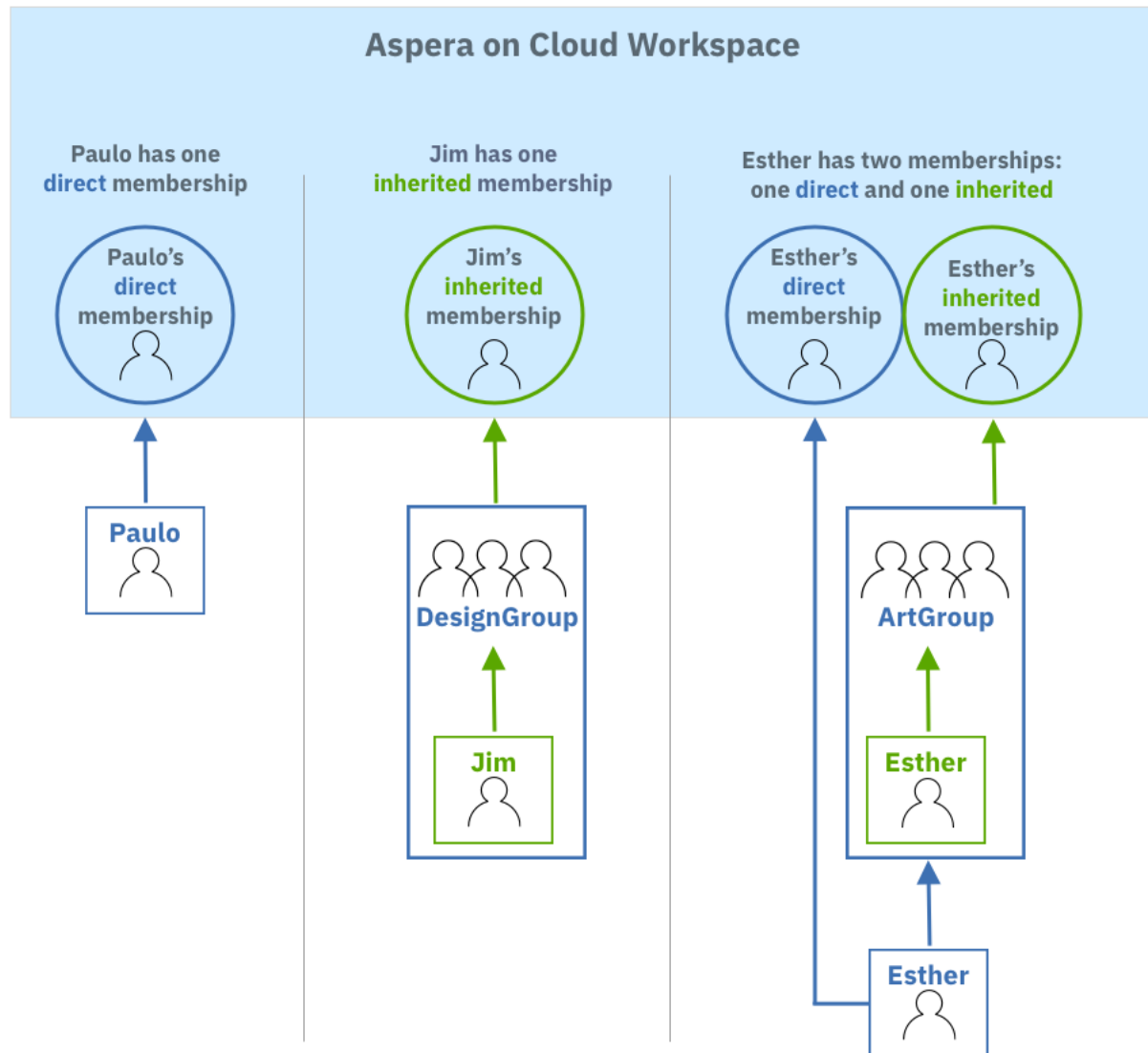
An user or user group in an organization can have direct or inherited membership – or both – in an org entity like a workspace, application, or group.

You can add a user to a workspace, an application, or group. When you do, you give the user *direct* membership in that entity.

You can also add a group to a workspace or app (or another group). When you do, the group becomes a *direct* member of the workspace or app. The members of the group *inherit* membership in the workspace or app through their membership in the group. When you see a user group as a member of any entity, you are dealing with inherited membership.

Note that a user or user group can have both direct and inherited membership in a workspace, app, or group.

Keep both direct and inherited memberships in mind, especially when revoking memberships; when any member has both direct and inherited membership, revoking membership in an entity requires more than one step.



Managing Workspace Memberships and Roles

To view membership in a workspace, do the following:

1. Click **Workspaces > workspaceName > Members**.
2. Browse, filter or search for the member to remove. You can filter the member listing using the following filter presets:
 - Membership type: Direct, Inherited
 - Member type: User, Group
 - Role: Member; Workspace manager
 - Status: Active, Deactivated, Pending
3. Click the row to display the member record.

Managing Workspace Roles

The member's role in the workspace may be either Member or Workspace manager. The role displayed is the *effective* role in the workspace. The effective role is the *highest* role the user has through any membership in this workspace. If the member has:

- Direct membership only, the Role field displays the role granted to them as a direct member. This field includes **Direct** as the source of the role.
- Inherited membership, or has both direct and inherited membership, their effective role may come from the direct or inherited membership, whichever is highest. If the effective role is inherited through group membership, the Role field includes the group or groups that are the source of the role.

For example, the user's direct membership may grant them the role of member. However, if the user also inherits membership in this workspace through a group that has the Manager role, this user's effective role in the workspace is Manager.

To change a user's role in the workspace *from Member to Manager*, assign the user the Manager role in *any* workspace membership. You can do either the following, whichever makes most sense from the user management perspective:

- Change the user's direct membership role to Manager.
- Change the workspace membership role for a group through which this user inherits workspace membership to Manager.

To change a user's role *from Workspace manager to Member*, you must change the user role to Member in *all* workspace memberships. Do the following as required:

1. Change the user's direct membership role to Member.
2. Change the workspace membership role for all groups through which this user inherits workspace membership to Member.

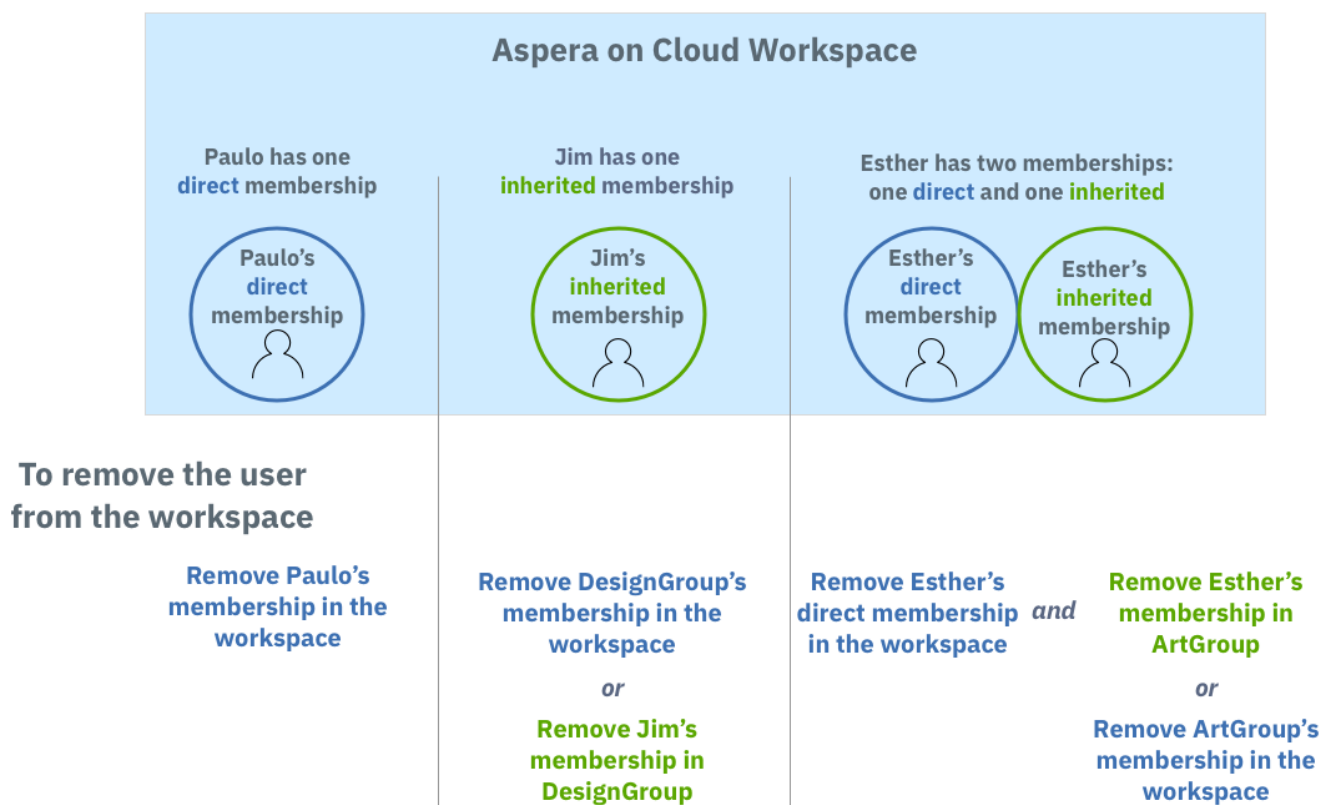
Managing Workspace Memberships

To make a user a member of a workspace, you can assign direct or inherited membership, or both.

- To assign direct membership in a workspace, see "Adding Members to a Workspace" in [Create a new workspace](#).
- To assign inherited membership, add the member to a group that has either direct or inherited membership; see "Adding Members to the Group" in [Create and manage groups](#).

To completely remove a user from a workspace, you must remove all memberships they have in the workspace – both direct and inherited. Do the following in the user profile page, Membership type panel:

1. If required, select Revoke direct membership.
2. If the user has inherited memberships, do the following:
 - a. Click the group name listed to jump to the group profile page.
 - b. Find the user in either the Members tab or the Managers tab.
 - c. Right-click the user row and select Revoke; then confirm.
 - d. Return to the workspace members page and repeat steps a through c for other inherited memberships.
3. Click Save.



Manage workspace memberships and roles

Users in your Aspera on Cloud organization are typically members in one or more workspaces. In fact, to use the Packages and Files apps to send or share files and folders, users must be members of a workspace. Use this article to add or remove workspace membership to or from a user or group, and to manage roles within a workspace.

Add a workspace member

This procedure describes how an admin or workspace manager can add an individual org member or group directly to a workspace. When you add a group as a workspace member, the group members [inherit membership](#) in the workspace through the group.

1. Click **Users > Management > *userName*** or Groups > *groupName*, then click the row to open the record.
2. Click **Workspace memberships > Add workspaces**.
3. In the **Search for workspaces** field, enter the name or partial string for one or more workspaces.
4. To make this user or group a manager in the workspaces you selected, select **Workspace manager**.
5. Click **Add**.
6. To give this user or group different roles in various workspaces, repeat this procedure, entering the workspaces for which you want the same role.

Note: AoC sends this user an email invitation that includes a direct link to the workspace. Individual users can configure their email notifications settings, including this one, by clicking their user icon in the upper right of the app and selecting **Account settings**.

Remove a workspace member

This procedure describes how to remove an individual user from a workspace.

Keep in mind that a workspace member, whether individual user or user group, can have direct membership, inherited membership, or both. Using this procedure, you can remove a user's direct workspace memberships. To completely remove a user from a workspace, you must also remove inherited memberships, if any. For details, see [Direct and Inherited Memberships](#).

- A member has *direct* workspace membership when they have been added directly to the given workspace.
- A member has *inherited* workspace membership when they are member of a group that is a workspace member, but not a direct member of the workspace.
- A member has *both* direct and inherited memberships when they are a direct member of the workspace and simultaneously a member of a group that is a workspace member.

To remove a member's direct workspace membership, do the following:

1. Click **Users > Management > *userName*** or Groups > *groupName*, then click the row to open the record.
2. Click **Workspace memberships**.
3. Right-click the row of the intended workspace and select **Revoke**; then confirm.

Change a user's role in a workspace

As an org admin or a [workspace manager](#), you can manage users roles (*member* or *manager*) in a workspace.

Keep in mind that when a group is a workspace member, the members of the group *inherit* membership and role in the workspace. To change the role for a user with inherited membership, remove them from the group; see [Direct and Inherited Memberships](#).

1. Click **Users > Management > *userName***. Click the row to open the user record.
2. Click **Workspace memberships**, then click the row of the intended workspace.
3. Check or clear the checkbox labeled **This member can manage this workspace**.
4. Click **Save**.

Manage shared folder memberships

A member or *collaborator* in a shared folder has access to folder contents according to the permissions given by the member who shared the folder with them.

As an administrator, you can open or restrict org-level and workspace-level collaboration settings for sharing folders. For example, you can determine who can send public links and share with external users, and who can be eligible external users. See the articles in [Configuration options](#) for details and procedures.

Share as user or as administrator?

As an administrator, you can share content in your cloud or local storage with a workspace or with specific workspace members. When you share as an administrator rather than as a user, all admins in your organization can manage the folder access. This shared management ability is typically preferable to having one admin user share a folder as an individual user; in such case, only that individual admin can revoke or change access permissions. For details, see [Share a node folder with a workspace](#).

View folder members

To see who has access to a given folder, do the following:

1. Go to your Files app and click the row of the folder.
2. Click the Collaborators icon to open the Collaborators panel.
3. Click See all collaborators.
4. To display both [direct and inherited memberships](#), click the Advanced filters icon; set the View inherited permissions toggle to On, then click Apply.
5. For any collaborator that you shared with, you can change the collaborator's access permission. Click the gear icon on a member row to open the Edit permissions window. Edit permissions as required, then click Save.

Add a folder member

To add a folder collaborator, do the following:

1. Go to your Files app and click the row of the folder.
2. Click the Collaborators icon to open the Collaborators panel.

3. Click Add collaborators.
4. Enter the email address of the member to add.
5. Assign access permissions for this member.
6. Click Add.

Remove a folder member

To remove a folder collaborator, do the following:

1. Go to your Files app and click the row of the folder.
2. Click the Collaborators icon to open the Collaborators panel.
3. Click See all collaborators.
4. Filter or browse for the member to remove.
5. On the member row, click the Revoke icon. Click Revoke to confirm.

Change member permissions

To change access permissions for a folder collaborator, do the following:

1. Go to your Files app and click the row of the folder.
2. Click the Collaborators icon to open the Collaborators panel.
3. Click See all collaborators.
4. Filter or browse for the member.
5. On the member row, click the Edit permissions icon.
6. Select the desired permission; click Save.

Manage shared inbox memberships

As an admin, you can manage membership in shared inboxes, including the permissions and membership expiration.

Add a member to a shared inbox

1. Go to Workspaces > *workspaceName* > Applications > Packages > Shared inboxes > *sharedInboxName* > Members > Add members.
2. Add one or more user names or email addresses who require the same access permissions to the shared inbox.
3. Select one or more permissions in the shared inbox for these users.
4. If desired, select an expiration for the members' Send permission. After the date you select, these members can no longer submit packages to the shared inbox. Other inbox permissions are not affected by this setting.
5. Click Add.

Change user permissions in a shared inbox

You can configure one or more discrete access permissions to the shared inbox for each shared inbox member:

- Send: The user with 'Send' permission can send packages to the shared inbox.
 - Receive: The user with 'Receive' permission can receive packages submitted to the shared inbox.
 - Add users: The user with 'Add users' permission can add new members to the shared inbox and grant them any of the three permissions. This user can also send a submission link to invite others to submit files and folders to the shared inbox.
1. Go to Workspaces > *workspaceName* > Applications > Packages > Shared inboxes > *sharedInboxName* Members.
 2. Double-click the member row and select Edit. Select or deselect permissions as required.

Allow self-registration for a shared inbox

To simplify and accelerate the task of adding external users to a shared inbox, you can deliver a self-registration link that enables a user to join or apply to join a shared inbox with *Send* permission only.

The self-registration link is a single, generic link that you can deliver to any number of external users. You can configure one self-registration link per shared inbox at any one time. You can customize self-registration link behavior to suit your specific collaboration requirements.

For details and a procedure to configure the self-registration link, see [Allow self-registration for a shared inbox](#).

Management of self-registered users is the same as for other members. However, keep in mind that once an outside user has a self-registration link, they can use it repeatedly to join or apply to join the shared inbox, and can also share it with others. If necessary, delete the existing self-registration link, then generate and distribute a new one.

Remove a member from a shared inbox

1. Go to Workspaces > *workspaceName* > Applications > Packages > Shared inboxes > *sharedInboxName* Members.
2. To remove a single member, double-click the member row and select Revoke.
3. To remove multiple members, select the check box to the left of the user names, then click Revoke at the top of the user list.

Manage application memberships

When the Files or Packages apps are enabled for a workspace, all workspace members can use the app. To give users access to the Activity and Automation apps, you must specifically add them as app members.

Files app and Packages app memberships are always in the context of a [workspace](#). This is not true of the Activity and Automation apps because actions performed in these apps are not confined to any single workspace.

Files and Packages apps

Both the Files and Packages apps are enabled by default in the org and for all workspaces. You can disable either app at the org level; if you do, that app is not available in any workspace. If enabled at the org level, you can disable either app in any workspace. When disabled in a workspace, the app is not available to any user in that workspace. When enabled in a workspace, all workspace members are automatically members of the app; all new users added to the workspace are automatically members of the app. See [Accelerate setup using inherited settings](#) for details.

Activity app

[Activity app](#) members can monitor events, file access, transfer activity, and volume usage in the Aspera on Cloud organization. You can add org admins and regular users and groups as members of the Activity app.

Content security in the Activity app

Keep in mind that all Activity app members can monitor events, activity, and usage across the entire org, including in workspaces where they are not members. For this reason, app members are typically org admins.

Manage memberships

Assuming the [app is enabled](#) for the org and that the [user is an org member](#), manage membership in the Activity app:

1. To add an org member to the Activity app, go to Applications > Activity > Members > Add members.
2. Enter one or more user names and click Add.

To remove a member of the Activity app, do the following:

1. Go to Applications > Activity > Members.
2. Filter or browse for the member to remove.
3. Right-click the row and select Revoke; or select multiple members and click Revoke at the top of the member list.
4. Click Revoke to confirm.

Automation app

The Automation app is available in Standard Plus and Premium editions of Aspera on Cloud.

[Automation app](#) members can build automated workflows to initiate file transfers, make calls to an API, and send event notifications. You add org admins and regular users as members of the Automation app. Within the Automation app, org admins have certain options and privileges and regular users don't have. For details, see [Automation app: Automate your transfer workflows](#).

Content security in the Automation app

Keep in mind that all Automation app members can monitor events, activity, and usage across the entire org, including in workspaces where they are not members. For this reason, app members are typically org admins.

Manage memberships

Assuming the app is enabled for the org and that the [user is an org member](#), add a member to the Automation app:

1. Go to Applications > Automation > Members > Add member.
2. Enter the user name and click Add.

To remove a member of the Automation app, do the following:

1. Go to Applications > Automation > Members.
2. Filter or browse for the member to remove.
3. Right-click the row and select Revoke; or select multiple members and click Revoke at the top of the member list.
4. Click Revoke to confirm.

Manage group memberships and roles

Create user groups in Aspera on Cloud to make addressing and managing multiple users easier.

For details and procedures, see [Create and manage groups](#).

Membership Troubleshooting

Address membership issues when undesired access persists.

- **Removed member still has access**
Use this procedure when you have removed a member from a workspace, group, shared folder, or other resource, but the user still has access.

Removed member still has access

Use this procedure when you have removed a member from a workspace, group, shared folder, or other resource, but the user still has access.

Any member may have both *direct* and *indirect* membership in an Aspera on Cloud asset. To remove that user's access, you may have to remove both types of membership.

- A user has *direct* membership when they have been added as an individual member of the asset, whether workspace, shared folder, or other.
- A user has *indirect* membership when they are a member of a group that is a member of the asset.

For details and a procedure, see [Direct and inherited memberships](#).

Packages app: Send and receive files and folders

The Aspera on Cloud Packages app lets users send and receive digital "packages", collections of files, folders, images, and video. Learn how to configure collaboration rules that govern content exchange within and beyond the workspace. Configure and manage shared inboxes that allow all inbox members to access content sent to the inbox, enhancing and accelerating team activities. Troubleshoot issues related to sending digital packages.

- **[Packages app basics](#)**
Understand the Packages app, its functionality, and its content security features. Find methods to accelerate Packages app configuration. Learn about submission links and package expiration policies to manage storage usage.
- **[Configuration options](#)**
Get step-by-step procedures to configure the many capabilities of the Packages app for sending and receiving files and folders. Configure collaboration options so workspace members can work securely with those outside your organization. Protect content and member privacy. Configure link styles for personalization and tracking. Enable JSON sidecar files to capture transfer details, package statistics, and user-configured metadata.
- **[Shared inboxes](#)**
Gain in-depth knowledge of shared inboxes, one of the most-used Packages app features. Learn to create and manage shared inboxes, including inbox metadata. Manage membership and permissions. If desired, configure links to allow external users to join the membership based on domain filtering or admin approval.
- **[Troubleshooting: Sending files and folders](#)**
Address issues with Packages app event notifications. Understand "draft" packages that result from transfer issues.

Packages app basics

Understand the Packages app, its functionality, and its content security features. Find methods to accelerate Packages app configuration. Learn about submission links and package expiration policies to manage storage usage.

- **[What is the Packages app?](#)**
The Aspera on Cloud Packages app allows users in a workspace to send, receive, and request files and folders. Workspace members can also send, receive, and request files and folders from people outside the workspace according to permissions configured by the org admin or workspace manager. Administrators can configure shared inboxes in a workspace to facilitate specific collaboration workflows.
- **[What is a submission link?](#)**
When you need to ask another person to send you files and folders, you can send a submission link (sometimes called a file request). A submission link allows the other person to send you a digital package using IBM Aspera high-speed transfer technology. A submission link is a feature of the Packages app.
- **[Accelerate Packages app setup through inheritable settings](#)**
Certain aspects of the Packages app are hierarchical, allowing administrators to speed deployment.
- **[Content security in the Packages app](#)**
In addition to secure access controls, protecting content directly ensures that digital assets retain their value even as Aspera on Cloud users collaborate to develop, exchange, and deliver content. This article collects and describes configuration options that administrators can set in the Packages app to protect content assets.
- **[Package expiration policies for storage management](#)**
Aspera on Cloud provides policies that can automatically delete digital packages in the Packages app when certain conditions are met. Automatic deletion can help you manage the storage volume your organization uses. Storage management can help you avoid overage charges to your subscription.

What is the Packages app?

The Aspera on Cloud Packages app allows users in a workspace to send, receive, and request files and folders. Workspace members can also send, receive, and request files and folders from people outside the workspace according to permissions configured by the org admin or workspace manager. Administrators can configure shared inboxes in a workspace to facilitate specific collaboration workflows.

Send, receive, and request files and folders

The Packages app allows users to exchange copies of files and folders using an email-like workflow. Users can select files and folders from any storage, mount, or desktop accessible through Aspera on Cloud. The Packages app collects these items into a [digital package](#). Users can address recipients allowed by administrative configuration, include a message to recipients, and enable various settings (for example, password protection, expiration policies, and notifications) per admin configuration, and send the content -- all from a single interface. Aspera on Cloud sends the package using IBM Aspera's high-speed transfer technology.

Packages app users can also send a [submission link](#), requesting another user to send a digital package. Packages app users can send such file requests to individuals or groups as allowed by administrative configuration.

Packages app users in a workspace have an inbox to store packages sent to them, and folders for Packages they've sent, for draft packages, for archived, deleted, and expired packages. See articles in the User Guide for procedures to send, download, recall, and manage packages.

Depending on workspace configuration, Packages app users may exchange files using one or more [shared inboxes](#).

See also [Should I send or share?](#) and [What is the Files app?](#)

Packages app in the organization and in the workspace

The Packages app is enabled for your organization by default. You can disable it for the entire org if no workspaces need to send digital packages.

If enabled for your organization, you can enable or disable the Packages app in each workspace. When you enable the Packages app for a given workspace, all members of that workspace can access and use Packages. When you add a new member to the workspace, that person automatically gains access to the Packages app in that workspace.

You configure the Packages app at the global level. Global settings are inherited by the Packages app in each workspace where it is enabled. An admin or a workspace manager can customize inherited settings at each workspace. For details, see [Accelerate Packages app setup through inheritable settings](#).

When you add a new member the workspace, that person automatically gains access to the Packages app in that workspace. They can begin using the Packages app according to the configurations set by the admin for that workspace.

Save from the Packages app to the Files app

Packages app users can save content they receive in a package directly to their Files app (assuming they are member of both apps in the same workspace).

Send packages directly from the Files app

Packages app users can send digital packages directly from the Files app (assuming they are member of both apps in the same workspace). This means users don't have to download content from Files, switch to the Packages app, then create a digital package and send. Rather, they can right-click an item in their Files app and select Send via Packages to open the Send files form.

What is a submission link?

When you need to ask another person to send you files and folders, you can send a submission link (sometimes called a file request). A submission link allows the other person to send you a digital package using IBM Aspera high-speed transfer technology. A submission link is a feature of the Packages app.

Use a submission link to ask others to send a [package](#) as follows:

- To you as an individual. The file you request appears in My inbox.
- To a shared inbox for which you have 'Add users' permission. The file you request appears in the shared inbox.

When you send a submission link, AoC sends an email notification to your recipients. The notification includes the submission link, which allows them to send you a digital package using Aspera's high-speed transfer technology, whether or not they have an AoC account.

When a recipient clicks the submission link in the email notification, AoC presents a sending portal that allows the user to collect the files and folders you asked for and send them to you in a digital package. The recipient of your invitation can send any number of packages until the link expires or until you revoke the link.

You can send an email message inviting your recipient to send you files or folders. This request is called a submission link, because the email includes a link that allows your recipient to use IBM Aspera technology to send, or submit, the files you request.

Note: Your administrator can limit the use of submission links to certain users, or can disable it for all users.

You can send a submission link to the following:

- A person without an Aspera on Cloud account.
- An Aspera on Cloud user who is not a member of your workspace.
- An Aspera on Cloud user who is a member of your workspace.

For a procedure to send a submission link, see [Request a package to My inbox](#) or [Request a package to a shared inbox](#)

Note: When someone submits a package for the first time, Aspera on Cloud prompts them to install Aspera Connect. For more information, refer to [What is IBM Aspera Connect?](#)

Accelerate Packages app setup through inheritable settings

Certain aspects of the Packages app are hierarchical, allowing administrators to speed deployment.

There are several settings for the Packages app that you can configure at the global app level. Global app settings are inherited by the Packages app in each workspace in the org. Shared inboxes in the workspace inherit the workspace-level app settings. These settings include:

- Collaboration
- Public and authenticated link styles
- Security
- Package expiration
- JSON "sidecar" metadata file

Hierarchical Level	Inheritance and Customization	Configuration Location
Organization: Packages app	Can customize defaults.	Applications > Packages > Settings

Hierarchical Level	Inheritance and Customization	Configuration Location
Workspace: Packages app	Default: Inherit from global app settings. Can override inheritance and customize.	Workspaces > workspaceName > Applications > Packages > Settings
Workspace: Packages app: Shared inboxes	Default: Use workspace setting. Can override inheritance and customize.	Workspaces > workspaceName > Applications > Packages > Shared inboxes > sharedInboxName > Settings

Configure inheritable Packages app settings

You can configure settings that determine how members of the Packages application can use Packages app features.

As an organization administrator, you can:

- Configure global, organization-wide Packages app settings that are inherited as defaults in all workspaces.
- In a given workspace, override inherited global settings. Workspace settings are inherited as defaults by all shared inboxes in that workspace.
- In a given shared inbox, override certain settings inherited from the workspace.
- Delegate workspace and shared-inbox settings to a workspace manager.

To configure global, organization-wide settings for the Packages app, do the following:

1. Go to **Applications > Packages**.
2. Select the checkbox labeled **Enable application**; the Packages app is enabled by default.
3. Configure the settings as described in related articles.

All workspaces in your organization inherit the settings you configure for the Packages app at the global level. If desired, you can customize these inherited settings for a given workspace.

To configure workspace-level settings for the Packages app, do the following:

1. Go to **Workspaces**, then select the workspace.
2. Go to **Applications > Packages > Settings**.
3. Select the check box labeled **Enable application**.
4. Select the check box labeled **Override global app settings**.
5. Configure the settings as described in related articles.

To configure shared-inbox settings for the Packages app, do the following:

1. Go to **Workspaces**, then select the workspace.
2. Go to **Applications > Packages > Shared inboxes**.
3. Select the shared inbox, then click **Settings**.
4. In the **Expiration** field, select **Custom** instead of **Use workspace settings**.
5. Configure the available settings as described in [Configure shared inbox settings](#).

Content security in the Packages app

In addition to secure access controls, protecting content directly ensures that digital assets retain their value even as Aspera on Cloud users collaborate to develop, exchange, and deliver content. This article collects and describes configuration options that administrators can set in the Packages app to protect content assets.

Admin controls

Global: Admin > Applications > Packages

Workspace: Admin > Workspaces > workspaceName > Applications > Packages

- Prevent app users from requesting packages from non-workspace members: Who can send submission links
- Prevent app users from sending packages to non-workspace members: Who can send packages to external users
- Require non-workspace recipients to create an account and log in to receive a package: Require external users to log in when receiving packages
- Prevent accidental sending to the entire workspace: Who can send packages to the entire workspace
- Require encryption at rest for all send packages: Automatically apply encryption at rest to all packages

Global: Integrations > Watermarking

- If you [integrate your Irdeto forensic watermarking service with Aspera on Cloud](#), you can *allow* or *require* workspace members of the Packages app to apply a watermark to all packages they send.

User controls

As an admin, you can establish workflows that guide your workspace members how to use these additional content security measures:

- Require package recipients to apply a password
- Apply watermarking when sending a package

Package expiration policies for storage management

Aspera on Cloud provides policies that can automatically delete digital packages in the Packages app when certain conditions are met. Automatic deletion can help you manage the storage volume your organization uses. Storage management can help you avoid overage charges to your subscription.

This article explains the package expiration policies and the available settings. For procedures to configure package expiration policies, see [Set package expiration policies](#) and [Configure shared inbox settings](#).

For information about storage in your subscription, see [Manage storage in your subscription](#). For additional storage management strategies, see [Managing storage usage](#).

Policy types

You can configure optional content expiration policies that apply to digital packages in your organization. As always, you can override the organization-level settings for a given workspace. In the case of package expiration settings, you can also customize settings for each shared inbox.

- **Time-based content expiration:** This setting determines how long Aspera on Cloud maintains contents of a package. For example, if you configure this setting for 10 days, Aspera on Cloud deletes package contents 10 days after the package becomes available to the intended recipients. You can apply a separate time-based expiration policy to Draft packages in the workspace.
Note: Content expiration policies also apply to packages in failed transfers.
- **Download-based content expiration:** This setting determines whether Aspera on Cloud deletes package contents either:
 - After all recipients have downloaded the package
 - After any one recipient downloads the package

In this context, *downloaded* means either downloaded the entire package (Download all) or downloaded all the individual contents of the package in one operation. Downloading only some of the package contents does not meet the expiration threshold.

If desired, you can configure a grace period that delays deletion for the number of days you configure, even after the expiration threshold is met.

Note: For a shared inbox, the download-based policy can either *delete* or *archive* the package. Archiving moves the package from the shared inbox to the recipients' Archived tab. Archiving does not delete package content. See [Shared inboxes](#).

How policies affect package contents

- Default policy settings do not delete package content at all; you must configure these setting to enable automatic deletion per policy.
- Configuring these policies results in permanent deletion of package contents from the transfer node per the policy. Once deleted, the contents cannot be retrieved.
- Even when packages contents are deleted, related transfer details are still available in the package details panel (click package row to view the details panel).
- If you configure multiple policies for a workspace or shared inbox, Aspera on Cloud deletes packages according to the policy that applies soonest.
- The package expiration policies apply only to packages sent after the policy is configured; previous packages are not affected.
- You can configure shared inboxes in the workspace to inherit workspace policies. You can also override the workspace policy by setting a shared inbox-level policy, which can be more restrictive or more relaxed than the workspace policy.

When a package expiration policy is in place for a given workspace or shared inbox, that expiration policy displays to users as follows:

- In the Send files form.
- In the email notification to package recipients.
- In the package details panel; click the package row to open the panel.

Sender-applied policies

If you configure this capability for a workspace, a sender can set time-based or download-based (or both) policies to an individual package by using a field in the Send files form. If a workspace-level policy is already applied, the sender can further restrict the existing policy, but cannot relax it. For example:

- If there is no workspace-level policy for time-based expiration, the sender can configure one, with a value from 1 to 30 days.
- If the workspace time-based policy calls for expiration after 10 days, a sender can further restrict the policy to, say, 5 days, but cannot relax the policy to, say, 15 days.
- If a download-based policy does not already exist, the sender can apply one; if a download-based policy exists, senders cannot remove that policy.

Note: Senders cannot modify the policy applied to Draft packages or to shared inboxes.

Configuration options

Get step-by-step procedures to configure the many capabilities of the Packages app for sending and receiving files and folders. Configure collaboration options so workspace members can work securely with those outside your organization. Protect content and member privacy. Configure link styles for personalization and tracking. Enable JSON sidecar files to capture transfer details, package statistics, and user-configured metadata.

- [Set package expiration policies](#)
You can configure optional content expiration policies that apply to digital packages in your organization. As always, you can override the organization-level settings for a given workspace. In the case of package expiration settings, you can also customize settings for each shared inbox.
- [Send files to external users](#)
Configure which workspace member types, if any, can send packages to users outside the workspace. When you allow members to send to external users, you can list specific eligible recipients.
- [Request files from external users](#)
Configure which workspace member types can use *submission links* to request another user to send a digital package. When you allow members or managers to send submission links, you can list specific eligible recipients.
- [Require external users to log in](#)
By default, external or outside recipients can receive and access packages without creating an Aspera on Cloud account and signing in. However, you can require external recipients to create an Aspera on Cloud account and sign in to access the packages sent. These external recipients thereby become *limited* members of the workspace.
- [Control content distribution in the workspace](#)
By default, all members of a workspace can send a package to the entire workspace by entering the workspace name as a recipient when sending files. To reduce the risk of a workspace member unintentionally sending sensitive content workspace-wide, you can restrict this capability to workspace managers only. You can also prevent all members and managers from sending to the entire workspace in this way.
- [Disable package sending](#)
Configuration settings to disable package sending.

- [Require encryption at rest](#)
You can configure an organization-level setting requiring that all packages sent in the organization automatically have encryption at rest (EAR) applied. Sending with EAR applied ensures that package contents remain encrypted at the receiving end, even after the recipient downloads the files and folders in the packages.
- [Configure link styles for requesting digital packages](#)
Members of the Aspera on Cloud Packages application send URL links, also called *submission links*, when requesting files and folders from others. The administrator can configure one of three link styles that Aspera on Cloud generates for file request operations.
- [Protect privacy in the workspace](#)
By default, package senders and recipients can see the download counters in the details panel of each package; when these users hover over the counters, AoC displays the names of recipients who have downloaded the package. You can prevent this visibility into workspace member identity by hiding the download counter.
- [Creating JSON sidecar files for digital packages](#)
You can configure a given workspace to generate a JSON *sidecar* file to be included in each package sent from the workspace. This JSON file appears in the package very shortly after the transfer completes; it contains transfer statistics like package size and average transfer rate, and package details like sender, recipients, contents, user-configured metadata, and more.
- [Give all workspace members access to all sent packages](#)
You can give all members of a workspace access to all packages sent by all workspace members. Among other benefits, this access allows teammates within a workspace to add recipients to a package already sent by another workspace member. This capability can accelerate collaboration with recipients because any available member can add recipients to a sent package; there is no need to wait for the original sender to add recipients.

Set package expiration policies

You can configure optional content expiration policies that apply to digital packages in your organization. As always, you can override the organization-level settings for a given workspace. In the case of package expiration settings, you can also customize settings for each shared inbox.

For details on package expiration policy types and functions, see [Package expiration policies for storage management](#)

Organization configuration

To configure this global Packages app settings, go to Applications > Packages > Package expiration.

1. To configure time-based expiration, check the box labeled **Delete this package after** and set the number of days after which package contents should expire.
2. To configure download-based expiration, check the box labeled **Delete after download**. Select either **All recipients have downloaded** or **Any recipient has downloaded**. If desired, set a grace period that delays package deletion for the number of days you select, even after the expiration threshold is met.
3. To configure a time-based expiration for recalled packages, check the box labeled **Delete recalled packages after** and set the number of days after which recalled packages in users' Sent folder should expire. For more information, see [Recall a package](#).
4. To enable package senders to add an expiration policy if the admin does not set one, or to further restrict the workspace-level expiration policy for a given package, check the box labeled **Allow senders to set expiration**.
5. For the following settings, see [Creating JSON sidecar files for digital packages](#) and [Give all workspace members access to all sent packages](#).
6. Click **Save**.

Workspace configuration

All workspaces in the organization inherit the global settings. You can set custom expiration policies in a given workspace that override the global policies.

To configure these Packages app settings for a given workspace, do the following:

1. Go to **Workspaces > workspaceName > Applications > Packages > Profile**.
2. Clear the box labeled **Use global app settings**.
3. In the **Package expiration** section, do the following:
 - a. To configure time-based expiration, check the box labeled **Delete this package after** and set the number of days after which package contents should expire.
 - b. To configure download-based expiration, check the box labeled **Delete after download**. Select either **All recipients have downloaded** or **Any recipient has downloaded**. If desired, set a grace period that delays package deletion for the number of days you select, even after the expiration threshold is met.
 - c. To configure a time-based expiration for recalled packages, check the box labeled **Delete recalled packages after** and set the number of days after which recalled packages in users' Sent folder should expire.
 - d. To enable package senders to add an expiration policy if the admin does not set one, or to further restrict the workspace-level expiration policy for a given package, check the box labeled **Allow senders to set expiration**.
4. Click **Save**.

Shared inbox configuration

Shared inboxes in a given workspace inherit workspace settings. You can set custom expiration policies that override the workspace policies.

1. Go to **Workspaces > workspaceName > Applications > Packages > Shared inboxes > sharedInboxName**.
2. In the Expiration field, select **Custom**.
3. In the **Package expiration** section, do the following:
 - a. To configure time-based expiration, select the check box for **Delete this package after** and set the number of days after which package contents should expire.
 - b. To configure download-based expiration, select the checkbox for **Delete after download**. Select either **All recipients have downloaded** or **Any recipient has downloaded**. If desired, set a grace period that delays package deletion for the number of days you select, even after the expiration threshold is met.
4. Click **Save**.

Send files to external users

Configure which workspace member types, if any, can send packages to users outside the workspace. When you allow members to send to external users, you can list specific eligible recipients.

If the Packages app is enabled both globally and for a given workspace, all members of that workspace can send packages to fellow workspace members. This is a fundamental function and cannot be changed. By default, all such workspace members can also send packages to members in other workspaces, and to people outside the organization. However, you can limit that capability.

1. To configure global Packages app settings, go to **Applications > Packages > Collaboration > Who can Send packages to external users**.
 - Select **All members** (default) to allow all members of workspaces in your organization to send packages to users outside the current workspace. They do this by entering the recipient's email address in the 'Send files' form.
 - Select **Only workspace managers** to allow only managers workspaces in your organization to send packages to users outside the current workspace.
 - Select **No one** to prevent all members of all workspaces, including workspace managers, from sending packages to anyone outside the current workspace.

2. Click **Save**.

The setting you choose here is inherited by all workspaces in the organization. To override these inherited settings for a given workspace, go to the next step.

Note that in a given workspace, you can list specific outside users as eligible recipients; this list prevents workspace members from sending packages to outside users you have not specifically listed.

3. To configure Packages app settings for a given workspace, do the following:
 - a. Go to **Workspaces > workspaceName > Applications > Packages > Profile**.
 - b. Clear the box labeled **Use global app settings**.
 - c. In the field labeled **Who can send packages to external users**, select the desired option.
 - d. If you chose **All members** or **Only workspace managers** in the previous step, select eligible recipients in the field labeled **Who are eligible external users**.
 - e. If you selected **Only the following emails and groups** or **Any email plus the following groups** in the previous step, enter the intended recipients in the following field.
4. Click **Save**.

Note: This setting is not available for an individual shared inbox. All shared inboxes in the workspace inherit the workspace configuration.

Request files from external users

Configure which workspace member types can use *submission links* to request another user to send a digital package. When you allow members or managers to send submission links, you can list specific eligible recipients.

If the Packages app is enabled both globally and for a given workspace, all members of that workspace can send submission links to other members in the workspace. This is a fundamental function and cannot be changed. By default, all such workspace members can also send submission links to members in other workspaces, and to people outside the organization. However, you can limit that capability.

1. To configure the global Packages app, go to **Applications > Packages > Collaboration > Who can request packages by sharing submission links**.
 - Select **All members** (default) to allow all members of workspaces in your organization to request others to send packages to the workspace member or to a workspace shared inbox.
 - Select **Only workspace managers** to allow only managers of workspaces to request packages.
 - Select **No one** to prevent all workspace members, including workspace managers, from requesting packages.
2. Click **Save**.

The setting you choose here is inherited by all workspaces in the organization. To override these inherited settings for a given workspace, go to the next step.
3. To configure Packages app settings for a given workspace, do the following:
 - a. Go to **Workspaces > workspaceName > Applications > Packages > Profile**.
 - b. Clear the box labeled **Use global app settings**.
 - c. In the field labeled **Who can request packages by sharing submission links**, select the intended workspace member type for this workspace: **All members**, **Managers only**, **No one**.
4. Click **Save**.

Note: This setting is not available for an individual shared inbox. All shared inboxes in the workspace inherit the workspace configuration.

Note: When you delete a user from your AoC organization, any submission links they sent become invalid.

For more information, see these topics:

- [What is a submission link?](#)
- [Request a package to My inbox](#)
- [Request a package to a shared inbox](#)

Require external users to log in

By default, external or outside recipients can receive and access packages without creating an Aspera on Cloud account and signing in. However, you can require external recipients to create an Aspera on Cloud account and sign in to access the packages sent. These external recipients thereby become *limited* members of the workspace.

For more information about limited users, see [User roles and types](#).

External recipients (also called outside recipients) are not members of your current workspace. They may or may not have membership in a different workspace, or they may not be a member of the AoC org at all. As an admin, can configure whether or not workspace members can send to outside users; see [Send files to external users](#).

Watermarking

Recipients of a watermarked package must log in to access the package.

- If you make watermarking *required* for packages sent in this workspace, you must check this box.
- If you make watermarking *optional* for packages sent from this workspace, workspace members cannot send watermarked packages to external users unless you check this box.

Procedure

1. To configure the global Packages app, go to **Applications > Packages > Collaboration**.
2. Check the box labeled **Require external users to log in when receiving packages**.
3. Click **Save**.
The setting you choose here is inherited by all workspaces in the organization. To override this inherited setting for a given workspace, go to the next step.
4. To configure the Packages app setting for a given workspace, do the following:
 - a. Go to **Workspaces > workspaceName > Applications > Packages > Profile**.
 - b. Clear the box labeled **Use global app settings**.
 - c. Check the box labeled **Require external users to log in when receiving packages**.
5. Click **Save**.

Existing limited users

To allow existing limited users in a workspace to receive packages without logging in, you must remove their accounts from the Aspera on Cloud user listing and disable the authentication requirement. Do the following:

1. Clear the box labeled **Require external users to log in when receiving packages**.
2. Click **Save**.
3. Go to **Users**, filter for Type = Limited, then delete them.

After this procedure, external users who previously established limited accounts and logged in to receive packages no longer need to log in to receive a package from an Aspera on Cloud user in this workspace. These individuals are no longer limited members in the Aspera on Cloud application.

Control content distribution in the workspace

By default, all members of a workspace can send a package to the entire workspace by entering the workspace name as a recipient when sending files. To reduce the risk of a workspace member unintentionally sending sensitive content workspace-wide, you can restrict this capability to workspace managers only. You can also prevent all members and managers from sending to the entire workspace in this way.

When you configure this restriction, the **To** field in the **Send files** form does not accept the workspace name as a valid entry. Note that users can, however, work around this restriction by entering every workspace member name in the **To** field.

To configure this restriction, do the following:

1. To configure the global packages app, go to **Applications > Packages > Content control**.
2. In the field labeled **Who can send packages to the entire workspace**, select the intended workspace member type for this workspace: **All members, Only workspace managers, No one**.
3. Click **Save**. The setting you choose here is inherited by all workspaces in the organization. To override these inherited settings for a given workspace, go to the next step.
4. To configure Packages app settings for a given workspace, do the following:
 - a. Go to **Workspaces > workspaceName > Applications > Packages > Profile**.
 - b. Clear the box labeled **Use global app settings**.
 - c. In the field labeled **Who can send packages to the entire workspace**, select the intended workspace member type for this workspace: **All members, Only workspace managers, No one**.
5. Click **Save**.

Note: This setting is not available for an individual shared inbox.

Disable package sending

Configuration settings to disable package sending.

Admins can enable this setting to disable package sending for their users. This can be turned on at the organization level as well as in the workspace.

To configure this restriction, do the following:

1. Go to **Applications > Packages > Content control**.
2. In the field labeled **Disable sending packages to other users**, turn the toggle On.
3. Click **Save**.
4. To disable package sending for a given workspace, do the following:
 - a. Go to **Workspaces > workspaceName > Applications > Packages > Content control**.
 - b. In the field labeled **Disable sending packages to other users**, turn the toggle On.
5. Click **Save**.

Require encryption at rest

You can configure an organization-level setting requiring that all packages sent in the organization automatically have encryption at rest (EAR) applied. Sending with EAR applied ensures that package contents remain encrypted at the receiving end, even after the recipient downloads the files and folders in the packages.

Senders must enter and confirm a passphrase for every package they send with EAR applied, then must deliver the passphrase to the recipient according to local site security practices. The recipient must apply that passphrase to decrypt the downloaded package.

Every workspace inherits the organization setting, but the administrator can override the inherited setting and either apply or remove EAR for packages sent in the workspace.

When you require EAR at the workspace, senders cannot send a package without EAR. However, even if you do not require EAR at the workspace, senders have the option to apply EAR to individual packages. In the Send files panel of the Packages user view, EAR is called 'Password protection'.

1. To configure the global Packages app, go to Applications > Packages > Security.
2. Check or clear the box labeled Automatically apply encryption at rest to all packages.
3. Click Save.

The setting you choose here is inherited by all workspaces in the organization. To override this inherited setting for a given workspace, go to the next step.

4. To configure the Packages app setting for a given workspace, do the following:
 - a. Go to Workspaces > *workspaceName* > Applications > Packages > Profile.
 - b. Clear the checkbox labeled Use global app settings.
 - c. Select or clear the checkbox labeled Automatically apply encryption at rest to all packages.
5. Click Save.

Note: This setting is not available for an individual shared inbox. All shared inboxes in the workspace inherit the workspace configuration.

Configure link styles for requesting digital packages

Members of the Aspera on Cloud Packages application send URL links, also called *submission links*, when requesting files and folders from others. The administrator can configure one of three link styles that Aspera on Cloud generates for file request operations.

When a Packages app users requests another user to send a digital package, Aspera on Cloud sends the recipient an email notification containing a link. The link opens an AoC portal interface that allows the recipient to compose and send a digital package.

There are three URL styles available:

- **Standard URLs**
 - Select Standard to generate full-length URLs.
 - Example of standard URL: https://aspera.ibmaspera.com/public/send?token=HBf-sfRFIHFMUXuYdocSi22X8pYRk_E8OxXOi4IOOWs
- **Short URLs**
 - Short URLs are enabled by default for a workspace.
 - Example of short URL: <https://aspera.pub/2dexfa>
- **Personalized URLs**
 - When you select Personalized, Aspera on Cloud uses a default that includes the sender's username, or, for a shared inbox, the shared inbox name.
 - Example of default personalized URL for a user: https://aspera.pub/2dexfa/Jane_Doe
 - Example of default personalized URL for a shared inbox named "Captions": <https://aspera.pub/2dexfa/Captions>
 - When you select Personalized, users can customize the default URL and compose a string of up to 240 characters. All characters beyond the conventional alphanumeric set (A through Z; a through z; 0 through 9) are replaced with underscore characters.
 - Example of customized personalized URL: https://aspera.pub/2dax/My_Own_Personal_Link

1. To configure the global Packages app, go to Applications > Packages > Settings > Public and authenticated links > URL styles.
2. Select one of the following:
 - Standard
 - Short
 - Personalized
3. Click Save.

The setting you choose here is inherited by all workspaces in the organization. To override these inherited settings for a given workspace, go to the next step.

4. To configure this Packages app settings for a given workspace, do the following:
 - a. Go to Workspaces > *workspaceName* > Applications > Packages > Profile.
 - b. Clear the box labeled Use global app settings.
 - c. Go to Public and authenticated links > URL styles; select the intended style.
 - d. Click Save.

Note: Shared inboxes inherit link styling from the workspace. You cannot override workspace settings for link styles.

Protect privacy in the workspace

By default, package senders and recipients can see the download counters in the details panel of each package; when these users hover over the counters, AoC displays the names of recipients who have downloaded the package. You can prevent this visibility into workspace member identity by hiding the download counter.

When you deselect the check box labeled Show download count within package details, neither senders nor recipients can see the download counters, and so have no visibility regarding package downloads.

1. To configure the global Packages app, go to **Applications > Packages > Security**.
2. Check or clear the box labeled **Show download count within package details**.
3. Click **Save**.

The setting you choose here is inherited by all workspaces in the organization. To override this inherited setting for a given workspace, go to the next step.

4. To configure the Packages app setting for a given workspace, do the following:
 - a. Go to **Workspaces > *workspaceName* > Applications > Packages > Profile**.
 - b. Clear the box labeled **Use global app settings**.

- c. Check or clear the box labeled **Show download count within package details**.
5. Click **Save**.

Note: This setting is not available for an individual shared inbox. All shared inboxes in the workspace inherit the workspace configuration.

Creating JSON sidecar files for digital packages

You can configure a given workspace to generate a JSON *sidecar* file to be included in each package sent from the workspace. This JSON file appears in the package very shortly after the transfer completes; it contains transfer statistics like package size and average transfer rate, and package details like sender, recipients, contents, user-configured metadata, and more.

To configure this feature, do the following:

1. Go to Applications > Packages > Advanced settings.
2. Select the check box labeled Automatically create a JSON files within all packages.
3. Click Save.
All workspaces in your organization inherit the setting you choose here. To override this inherited settings for a given workspace, go to the next step.
4. To configure this Packages app setting for a given workspace, do the following:
 - a. Go to Workspaces > *workspaceName* > Applications > Packages.
 - b. Clear the box labeled Use global app settings.
 - c. In Advanced Settings, select or deselect the check box labeled Automatically create a JSON files within all packages.
 - d. Click Save.

This setting is not available for an individual shared inbox. All shared inboxes in the workspace inherit the workspace configuration.

Give all workspace members access to all sent packages

You can give all members of a workspace access to all packages sent by all workspace members. Among other benefits, this access allows teammates within a workspace to add recipients to a package already sent by another workspace member. This capability can accelerate collaboration with recipients because any available member can add recipients to a sent package; there is no need to wait for the original sender to add recipients.

This feature is disabled by default; members of this workspace can see and access only the sent packages they themselves sent. With this feature enabled, workspace members can apply the following filters to their Sent mailbox:

- All senders
- Sent by me
- Sent by others

Forward the package or add recipients?

There are two ways make a sent package available to additional recipients: forwarding a package and adding recipients to a package.

- Forwarding a package
 - Users must be the sender or recipient of a package to be able to forward it.
 - Users can add or remove attachments from the original package.
 - Users can change the original message.
 - Forwarding creates and transfers a new package. This means expiration policies set in the workspace apply to the forwarded package as to a new package; time-based intervals and download-based policies are reset when a user forwards a package. Once a package expires, users cannot forward it.
- Adding recipients to a package
 - If the administrator has enabled this capability for a given workspace, users can add recipients to any package sent by any workspace member.
 - Users cannot add or remove attachments from the original package.
 - Users cannot change the original message.
 - Adding recipients does not create and transfer a new package. It simply makes the same sent package available to additional recipients. So adding recipients can save transfer and storage usage compared to forwarding a package. **Note:** Whether recipients receive the package by forwarding or by being added to the recipients list, each recipient initiates a transfer when they download package contents.
 - Since adding recipients does not create a new transfer, any expiration policy applied to the original package applies to the new recipients. For example, if the package is set to expire after all recipients have downloaded it, the package will not expire until the added recipients have download it. If the package is set to expire on a particular date, any added recipients must access and download the package before that date. Once the package expires, users cannot add recipients to it.

Note: You cannot add recipients to a package sent to a shared inbox.

To read the related user documentation, see [Add recipients to a sent package](#) and [Forward a package](#).

Procedure

To enable this feature, do the following:

1. To configure this global Packages app setting, go to **Applications > Packages > Advanced settings**.
2. Check the box labeled **Make all sent packages accessible to all workspace members**.
3. Click **Save**.
All workspaces in your organization inherit the setting you choose here. To override this inherited settings for a given workspace, go to the next step.
4. To configure this Packages app setting for a given workspace, do the following:
 - a. Go to **Workspaces > workspaceName > Applications > Packages > Profile**.
 - b. Clear the box labeled **Use global app settings**.

- c. In Advanced settings, check or clear the box labeled **Make all sent packages accessible to all workspace members**.
- d. Click **Save**.

Shared inboxes

Gain in-depth knowledge of shared inboxes, one of the most-used Packages app features. Learn to create and manage shared inboxes, including inbox metadata. Manage membership and permissions. If desired, configure links to allow external users to join the membership based on domain filtering or admin approval.

- [Shared inboxes overview](#)
As an org admin or workspace manager, you can configure shared inboxes. A shared inbox is an optional workspace feature similar to a distribution list: Depending on access privileges you assign, users can send content directly and simultaneously to all members of the shared inbox and can view all packages sent to the shared inbox.
- [Accelerate shared inbox setup through inheritance](#)
Certain aspects of the Aspera on Cloud structure are hierarchical, allowing administrators to speed configuration and deployment of shared inboxes in the Packages app. In most cases, you can customize inherited settings for each individual shared inbox.
- [Manage shared inbox memberships](#)
As an admin, you can manage membership in shared inboxes, including the permissions and membership expiration.
- [Create a new shared inbox](#)
A shared inbox is an optional workspace feature that is part of the Packages application. As an organization administrator, you can create a shared inbox in any workspace; as a workspace manager, you can create a shared inbox within any workspace in which you have manager privileges.
- [Configure shared inbox settings](#)
You can create and manage shared inboxes from the Packages app or from the Admin app.
- [Add metadata fields to a shared inbox](#)
Create optional or required metadata fields that display on the Package Submission form to users sending content to a shared inbox.
- [Allow self-registration for a shared inbox](#)
To simplify and accelerate the task of adding external users to a shared inbox, you can use a self-registration link that enables users to join or apply to join a shared inbox with **Send only** permission.
- [Use shared inboxes for external collaboration](#)
There are several ways you can support collaboration between your AoC shared inbox members and outside users (users who are not members of your AoC organization).

Shared inboxes overview

As an org admin or workspace manager, you can configure shared inboxes. A shared inbox is an optional workspace feature similar to a distribution list: Depending on access privileges you assign, users can send content directly and simultaneously to all members of the shared inbox and can view all packages sent to the shared inbox.

Introduction

Shared inbox members may be users or user groups. A workspace may have multiple shared inboxes, each with discrete or overlapping membership. A user may be a member of multiple shared inboxes within the workspace, or of none.

When a user sends content to a shared inbox, Aspera on Cloud collects the selected content into a digital package and delivers it to the shared inbox, where each shared inbox member can access it (again, depending on assigned permissions).

For related information, see and [Creating a New Shared Inbox](#).

For a user perspective, see [What is a shared inbox?](#)

Managing shared inboxes

Access shared inbox management through either the Admin app or the Packages app.

- Admin app: Workspaces > Applications > Packages > Shared Inboxes.
- Packages app: Workspace > Manage shared inboxes.

Shared inbox content expiration policies

You can configure shared inbox-level content expiration policies that override policies set for the workspace. Such policies apply to digital packages sent to the shared inbox. Content expiration policies are one form of storage usage management available in Aspera on Cloud. You can configure both time-based and download-based expiration of package contents. For details, see [Setting Content Expiration Policy](#).

Shared inbox metadata

You can configure a shared inbox so that members with Send permission apply metadata tags that you define to each digital package sent to the shared inbox. AoC maintains the association between these tags and the package content to allow for easier identification, sorting, and searching. You can make metadata tags required or optional, and specify them in several forms, including a time/date field, single-text field, a text box, a single-choice drop-down, or multiple-choice check boxes.

Shared inbox recipient members can view metadata tags applied by senders in the package details panel for each package in their shared inbox packages list.

For details, see [Add metadata fields to a shared inbox](#).

Shared inbox permissions

You can configure one or more discrete access permissions to the shared inbox for each shared inbox member:

- Send: The user with 'Send' permission can send packages to the shared inbox.
- Receive: The user with 'Receive' permission can receive packages submitted to the shared inbox.
- Add users: The user with 'Add users' permission can add new members to the shared inbox and grant them any of the three permissions. This user can also send a submission link to invite others to submit files and folders to the shared inbox.

Shared inbox submission links

Administrators, workspace managers, and shared inbox members with 'Add users' permission can send submission links. There are three types of [submission links](#) for a given shared inbox.

- Private link: Send a private submission link to an existing member of the shared inbox to invite them to send a package to the shared inbox.
- Self-registration link: Send this submission link to allow the recipient to self-register as a member of the shared inbox. You can configure approval requirements that must be met before the link user is admitted. You can also bypass the approval requirements so that anyone with the self-registration link can become a member of the shared inbox automatically.
- Public link: Send this link to someone who is not a member of the shared inbox.

To configure self-registration for a shared inbox, see [Allow self-registration for a shared inbox](#). For a user procedure, see [Request a package to a shared inbox](#).

Accelerate shared inbox setup through inheritance

Certain aspects of the Aspera on Cloud structure are hierarchical, allowing administrators to speed configuration and deployment of shared inboxes in the Packages app. In most cases, you can customize inherited settings for each individual shared inbox.

For example, you can take advantage of:

- Sensible defaults for ready-to-use ease.
- An inheritance scheme to accelerate implementation and simplify customization.
In this case, global/org-level Packages app settings --> Workspace Packages app settings --> shared inbox settings.
- Granular configuration options for highly-customizable control.

Packages App settings

There are several settings for the Packages app that you can configure at the global app level. Global app settings are inherited by the Packages app in each workspace in the org. In a given workspace, you can override the inherited global settings and customize workspace settings. Shared inboxes in the workspace inherit the workspace-level app settings. In any given shared inbox, you can override workspace settings and customize for the needs of the shared inbox users. These settings include:

- Collaboration
- Public and authenticated link styles
- Security
- Package expiration
- JSON "sidecar" metadata file

Hierarchical Level	Inheritance and Customization	Configuration Location
Organization: Packages app	Can customize defaults.	Applications > Packages
Workspace: Packages app	Default: Inherit from global app settings. Can override inheritance and customize.	Workspaces > <i>workspaceName</i> > Applications > Packages > Profile
Workspace: Packages app: Shared inboxes	Default: Inherit workspace setting. For some settings, can override inheritance and customize.	Workspaces > <i>workspaceName</i> > Applications > Packages > Shared inboxes > <i>sharedInboxName</i> > Metadata/Manage links/Settings/Notifications/Email templates

To customize the settings of any shared inbox, do the following:

1. Go to Workspaces > *workspaceName* > Applications > Packages > Shared inboxes > *sharedInboxName*.
2. To customize metadata settings, see [Add metadata fields to a shared inbox](#).
3. To customize the link style available when users request a package be sent to the shared inbox, see [Configure link styles for requesting digital packages](#).
4. To customize package expiration settings, submission link settings, and subject line and message settings, see [Configure shared inbox settings](#).
5. Configure settings as required and Save.

Manage shared inbox memberships

As an admin, you can manage membership in shared inboxes, including the permissions and membership expiration.

Add a member to a shared inbox

1. Go to Workspaces > *workspaceName* > Applications > Packages > Shared inboxes > *sharedInboxName* > Members > Add members.
2. Add one or more user names or email addresses who require the same access permissions to the shared inbox.
3. Select one or more permissions in the shared inbox for these users.
4. If desired, select an expiration for the members' Send permission. After the date you select, these members can no longer submit packages to the shared inbox. Other inbox permissions are not affected by this setting.
5. Click Add.

Change user permissions in a shared inbox

You can configure one or more discrete access permissions to the shared inbox for each shared inbox member:

- **Send:** The user with 'Send' permission can send packages to the shared inbox.
 - **Receive:** The user with 'Receive' permission can receive packages submitted to the shared inbox.
 - **Add users:** The user with 'Add users' permission can add new members to the shared inbox and grant them any of the three permissions. This user can also send a submission link to invite others to submit files and folders to the shared inbox.
1. Go to Workspaces > *workspaceName* > Applications > Packages > Shared inboxes > *sharedInboxName* Members.
 2. Double-click the member row and select Edit. Select or deselect permissions as required.

Allow self-registration for a shared inbox

To simplify and accelerate the task of adding external users to a shared inbox, you can deliver a self-registration link that enables a user to join or apply to join a shared inbox with *Send* permission only.

The self-registration link is a single, generic link that you can deliver to any number of external users. You can configure one self-registration link per shared inbox at any one time. You can customize self-registration link behavior to suit your specific collaboration requirements.

For details and a procedure to configure the self-registration link, see [Allow self-registration for a shared inbox](#).

Management of self-registered users is the same as for other members. However, keep in mind that once an outside user has a self-registration link, they can use it repeatedly to join or apply to join the shared inbox, and can also share it with others. If necessary, delete the existing self-registration link, then generate and distribute a new one.

Remove a member from a shared inbox

1. Go to Workspaces > *workspaceName* > Applications > Packages > Shared inboxes > *sharedInboxName* Members.
2. To remove a single member, double-click the member row and select Revoke.
3. To remove multiple members, select the check box to the left of the user names, then click Revoke at the top of the user list.

Create a new shared inbox

A shared inbox is an optional workspace feature that is part of the Packages application. As an organization administrator, you can create a shared inbox in any workspace; as a workspace manager, you can create a shared inbox within any workspace in which you have manager privileges.

Create a new shared inbox

1.
 - **From the user view:** In the Packages application, select the workspace from the workspace drop-down menu. Click Manage shared inboxes in the left navigation bar, then click Create new.
 - **From the admin view:** In the admin view, go to Workspaces and click the specific workspace for the shared inbox; click **Applications > Packages > Shared inboxes**. Click Create new.
2. Give the shared inbox a name. The name becomes the shared inbox label in the workspace.
3. If desired, add an image to brand this shared inbox. Click Add file to browse for the image file, or drag and drop the image.
4. If desired, add a description, visible only to workspace managers and administrators.
5. If desired, add instructions that display in the Send files form to users submitting content to this shared inbox.
6. If you don't want to be a member of this shared inbox yourself, clear the box labeled Add me to this shared inbox.
7. Click Save.

Add members to the shared inbox

8. Click Members.
9. Type the name of an existing user in your organization and press Enter; repeat to add more users.
10. In the members list, adjust access permissions as necessary for each member.
 - **Send:** Members with 'Send' permission can send packages to the shared inbox. These members can select the shared inbox name when they click the Recipient field in the Send Files form.
 - **Receive:** Members with 'Receive' permission can receive packages submitted to the shared inbox. The shared inbox appears by name in these members' lists of available inboxes in the left side panel. When these members click the inbox name, the packages sent to that inbox display.
 - **Add users:** Members with 'Add users' permission can invite outside users to send packages to the shared inbox. The invitation is called a [submission link](#). See [Inviting Others to Send Content](#) for details. The shared inbox appears by name in these members' lists of available inboxes in the left-side panel. When these members click the inbox name, an Add button appears in the right panel that allows them to add members to the shared inbox. Unless these users also have 'Receive' permission, they cannot see packages sent to that inbox.
11. Click Save.

You can delete a shared inbox from Aspera on Cloud by returning to the shared inbox and clicking Delete.

You can create optional metadata fields that display on the Send files form for users sending content to this shared inbox. For more information, see [Adding Metadata Fields to a Shared Inbox](#).

You can configure shared inbox settings. For more information, see [Configuring Shared Inbox Settings](#).

You can configure a self-registration link that allows outside users to join or apply to join the shared inbox with Send only permission. See [Allow self-registration for a shared inbox](#).

Configure shared inbox settings

You can create and manage shared inboxes from the Packages app or from the Admin app.

Note: You can configure email notification templates and notification delivery specifically for each given [shared inbox](#); see these topics for details:

- [Customizing Email Notification Templates](#)
- [Customizing Email Notification Delivery](#)

To create a new shared inbox, go to [Create a new shared inbox](#).

To manage an existing shared inbox, do the following:

1. Go to the shared inbox settings page.
 - From the Packages app, click Manage in the right panel, then click Shared inboxes > *sharedInboxName* > Settings.
 - From the Admin app, go to Workspaces > *workspace_name* > Applications > Packages > Shared inboxes > *sharedInboxName* > Settings.
2. Configure package expiration policies for packages in this shared inbox (for more information, see [Content Expiration Policies](#)). You can choose one of the following options:
 - To apply the same package expiration policies configured at the workspace to this shared inbox, set the toggle labeled Use workspace settings to On. When you select this option, the policies (if any) configured for the workspace display for your information only and are not editable.
 - To configure customized expiration settings for packages in this shared inbox, select Custom, then do the following:
 - To configure a time-based expiration policy for this shared inbox, check the box labeled **Time-based policy**, then enter the number of days after which package contents should be deleted.
 - To configure a download-based expiration policy, check the box labeled **Download-based policy**. Then select Delete or Archive.
 - If you select Delete, AoC moves packages from the shared inbox to recipients' Deleted/Expired tab and deletes the package content when the threshold is met.
 - If you select Archive, AoC moves packages from the shared inbox to recipients' Archived tab when the threshold is met.

Select **After all recipients have downloaded** to archive or delete the package after all recipients have downloaded it.

Select **After any recipient has downloaded** to archive or delete the package after any one recipient has downloaded it.

If desired, set a grace period that delays package expiration for the number of days you enter, even after the expiration threshold has been met.
3. Enable or disable personalized URL links for the shared inbox.

When enabled, users can customize the URL of a submission link. For more information about submission links, see [What is a submission link?](#) For more information about personalized URLs, see [Configure link styles for requesting digital packages](#).

Note: If personalized URLs are disabled at the workspace, you cannot enable them for the shared inbox. The shared inbox inherits the URL type set at the workspace level.
4. To configure illegal characters that users cannot enter into the Package title field of the Send files form, enter those characters in the **Subject illegal characters** field.

If a user attempts to enter an illegal character, the web page does not print anything in the field, and the user must choose a different character.
5. To configure a list of illegal characters that users cannot enter into the message field of the Send Package form, enter those characters in the **Message illegal characters** field.

If a user attempts to enter an illegal character, the web page does not print anything in the field, and the user must choose a different character.
6. To configure a maximum length that users can configure for the Package title of the Send files form, enter the numeric value in the **Subject max length** field.
7. To configure a maximum length that users can configure for the Package message field of the Send files form, enter the numeric value **Message max length** field.
8. Click Save.

Add metadata fields to a shared inbox

Create optional or required metadata fields that display on the Package Submission form to users sending content to a shared inbox.

1. When managing a shared inbox, click **Metadata**.
2. You can add metadata fields in two ways:
 - To import metadata fields from an existing shared inbox, click **Import**. Select the inbox to import from and click **Import**.
 - To create a new metadata field, click **Add field**. Add as many fields as you need.

Follow the steps below for each metadata field:

3. Enter a field title. Aspera on Cloud displays this label to users on the Send Files form.
4. Select a field type and configure a label.

For the **Dropdown menu** and **Checkboxes** field types, click **Add option** and name that option. Check Default to pre-select that option in the Send files form. Users can still select a different option.
5. Set the **Required** toggle to On to make this option required. Users cannot send their package until they respond to a required metadata field.
6. Click Save.
7. To reorder the fields, click the up or down arrows on the upper right of the field panel.
8. To delete a field, click the **Delete** icon.
9. To see a preview of all the configured metadata fields, click **Preview**.
10. Click **Save**.

Allow self-registration for a shared inbox

To simplify and accelerate the task of adding external users to a shared inbox, you can use a self-registration link that enables users to join or apply to join a shared inbox with **Send only** permission.

Configuration

The self-registration link is a single, generic link that you can deliver to any number of external users. You can configure one self-registration link per shared inbox at any one time. You can customize link behavior to suit your specific collaboration requirements.

Approvals

You can allow any user with the link to join the shared inbox directly. Or you can require those with the link to go through a simple approval process.

When configured, the approval process sends users of the self-registration link to a pending state. Approvers can approve or reject pending users individually; they can also accept all pending approvals with a single click.

Approvers can view a list of pending users in both the user view and the admin view of the shared inbox:

- In the user view of the Packages app, click the shared inbox name in the left panel to enter the shared inbox. The list of pending users appears in the collaborators panel.
- In the Admin view, enter the workspace, then go to Applications > Packages > Shared inboxes > *sharedInboxName* > Members. The list of pending users appears at the top of the current member list.

Org admins and workspace manager are always able to approve or reject a self-registration request. If desired, you can add existing shared inbox member who have Add users permission as approvers.

You can combine the approval options that you configure with a domain-based filter, as described below.

Member permissions

A self-registration link grants **Send** permission only. To grant additional permissions to a shared inbox member, go to the Members tab in the shared inbox, right-click the user row, then select Edit permissions.

Domain-based filtering

You can restrict registration (if you do not configure approval requirements), or entry into the approval process (if you do configure approval requirements, based on user email domain).

You can designate Include domains, then list domains from which users *can* self-register. For example, if you include **abc.com**, only users with email addresses from that domain are allowed to self-register. If you configured approval requirements, users from **abc.com** must still be approved.

Alternatively, you can designate Exclude domains, then list domains from which user *cannot* self-register. For example, if you exclude **xyz.com**, users with email addresses from **xyz.com** are not allowed to self-register. Users from all other domains are allowed to self-register (subject to the approval requirements you configure).

Notifications

AoC generates email notifications for the following self-registration events:

- Registration requests (from users with self-registration links)
- Approvals (by approvers)
- Rejections (by approvers)

AoC delivers these event notifications to org admins and managers of this workspace. If you designate existing inbox members with Add users permission as additional approvers, they also receive the event notifications. To narrow the list of those who receive notifications, you can configure a subset of the designated approvers to be the only ones who receive the notifications.

Procedures

To configure a self-registration link for a shared inbox, do the following:

1. Go to the Admin app or the Packages app.
 - Workspaces > Applications > Packages > Shared Inboxes > *sharedInboxName* > Manage links.
 - Packages > Manage shared inboxes > *sharedInboxName* > Manage links.
2. Click Self-registration link > New link.
Link format is inherited from workspace settings.
3. To send the link with default settings (approval required; approvers are org admins and workspace managers (if any in this workspace); default notification recipients are org admins and workspace managers; no domain-based restrictions), copy the link and send as required.
4. To edit the default link settings, click Edit.
5. To configure approval, do the following:
 - a. Set the toggle labeled Approval. Administrators and workspace managers (if any in this workspace) are required approvers.
If you set to No approval required, users who click the link automatically become shared inbox members with Send permission.
If you set to Approval required, users who click the link move to a pending state. The list of pending users appears near the current user listing. Approvers can approve or reject pending users individually, or can accept all pending approvals with a single click.
If desired, add to the required approvers by checking the box labeled **Members of this shared inbox with 'Add users' permission**.
6. To configure email notifications about self-registration activities, do the following:
 - a. Select Default recipients to notify all org admins that managers of this workspace. Note that if you added approvers with Add users permission to the approvers list in step 5, those users are included as default recipients.
 - b. To configure a smaller list designated approvers, select **Selected recipients**; then enter the emails of specific default recipients.
7. For additional security, you can limit who can self-register based on email domain. Do the following to apply registration restrictions:
 - a. To limit self-registration to users from specific domains, select Include domains; then list the domains to include.
 - b. To limit self-registration to users who are not from specific domains, select Exclude domains; then list the domains from which users cannot self-register.
8. Click Save.
9. Click Copy next to the link and deliver it to the intended external users according to your local site practice.
10. To disable an existing self-registration link, click the Delete icon. Those who have already used the self-registration link to gain shared inbox membership maintain their membership. Users who have applied for shared inbox membership using the link can still be approved. No new users who have not already applied can join or apply to join the shared inbox using the link you deleted.

To approve or reject pending users, do the following:

1. In the user view of the Packages app, click the shared inbox name in the left panel to enter the inbox.
 - a. In the collaborators panel on the right side, click the link labeled See all collaborators.
 - b. Review the list of pending users (if any) at the top of the existing members list.

- c. To approve all pending users, select them all for a bulk operation and click Approve.
 - d. To approve or reject an individual pending user, click the three dots icon and select either Approve or Deny.
2. In the Admin view, go to the workspace, then go to Applications > Packages > Shared inboxes > *sharedInboxName* > Members.
 - a. In the collaborators panel on the right side, click the link labeled See all collaborators.
 - b. Review the list of pending users (if any) at the top of the existing members list.
 - c. To approve all pending users, select them all for a bulk operation and click Approve or Deny.
 - d. To approve or reject an individual pending user, click the three dots icon and select either Approve or Deny.
3. Click Save.

Use shared inboxes for external collaboration

There are several ways you can support collaboration between your AoC shared inbox members and outside users (users who are not members of your AoC organization).

For few or occasional submissions to a shared inbox

To fill the need for occasional collaboration with a few outside users, shared inbox members with Add users permission can send submission links to outside users. Using the link, an outside user can send a digital package of files and folders to the shared inbox.

AoC delivers the submission link in an email notification. When the outside user clicks the link in the email, AoC presents a portal page. The portal allows them use Aspera high-speed transfer technology to submit packages to that shared inbox. The packages they send appear in the shared inbox packages listing, available to all members with Receive permission. The packages listing displays the sender of such a package as "Anonymous Sender" unless the sender enters their name and email in the fields on the portal page.

The outside user can continue to use the submission link until the link expires. For user procedure, including setting link expiration, see [Request a package to a shared inbox](#).

Note: When you delete a user from your AoC organization, any submission links they sent become invalid.

Note that outside users need to download and install IBM Aspera Connect, the same free software program that AoC members install to enable web-based transfers using Aspera technology. For more information, see [Aspera Connect transfer client](#).

In this scenario, the outside user does not become a member of your Aspera on Cloud organization, workspace, application, or shared inbox. You do not see these outside users listed in your org member or shared inbox member listing. You cannot filter for these users in the activity portal in the Admin app or in the Activity app itself.

Ongoing collaborations and enhanced security for shared inboxes

For increased security, visibility, and monitoring, you can allow your outside users to become *limited* members of your AoC organization and of the specific shared inbox.

A limited user is a member of a shared inbox only. A limited member is not a member of your organization, of any workspace, or of the Packages app (see [User roles and types](#)). Limited users appear in the AoC organization user listing; org admins can readily filter for them in these member listings, and filter for them by user type in the organization user listing.

AoC tracks packages submitted by limited users by sender name, so you can readily identify packages they send. You can also monitor the activity of limited users in the Activity console of the Admin app and in the AoC Activity app (if supported in your AoC subscription edition).

There are two ways to invite limited users into your organization:

- The first method is perhaps most appropriate for ongoing collaboration with a few individuals. Add a user to the shared inbox and give them Send only permission. If you wish, you can configure an expiration to their permission, after which they can no longer send to the shared inbox. When the permission expires, AoC removes them from the shared inbox member list, but not from the org user listing. There are three user types that can add members to a shared inbox: administrators, workspace managers, and shared inbox members with Add users permission.
- The second method is more useful when you have numerous external users with whom you need ongoing collaboration. Send the outside users a self-registration link to the shared inbox. This link allows the outside users to join the shared inbox as long as they meet the approval criteria that you configure. You can send the same generic self-registration link to as many outside users as required. Configuring self-registration accelerates and simplifies the task of enabling outside users to collaborate using a shared inbox. For an admin procedure to configure self-registration links, see [Allow self-registration for a shared inbox](#).

Troubleshooting: Sending files and folders

Address issues with Packages app event notifications. Understand "draft" packages that result from transfer issues.

- [Email notifications](#)
Use this procedure when AoC email notifications do not arrive as expected.
- [Resending "Draft" packages](#)
When the transfer for a package you send fails to start, AoC displays a transient error message with the heading "Verify contents and resend" and moves the package to the Drafts folder in your Packages app.

Email notifications

Use this procedure when AoC email notifications do not arrive as expected.

If you are the person who is missing the notification, do the following:

1. Check that the notification is not in your email spam folder.
2. Check that you haven't disabled the notification. See User icon > Account settings and .
3. Contact your local tech support administrator. Click the Help icon in the banner and select "Technical support". Provide the email address where you expect to receive the notification.

If you are the local tech support administrator, do the following:

1. Check that the AoC user record lists the user's expected email address. See [Users > Management](#).
Note: If the user logs in to Aspera on Cloud through an external authentication or identity provider like IBMid or a SAML system, you cannot edit the name and email address in the AoC user record. The user must change these settings in the external system; that change will propagate to AoC.
2. Check that the user is in fact a member of the group, workspace, shared inbox, or other entity that should receive the missing notification.
3. Check that you have not disabled the specific notification that is missing; see [Organization > Notifications](#) and [Control email notification delivery](#).
4. Check that the SMTP server administrator has added the AoC email (donot-reply@ibmaspera.com) for notifications to the "allowed" list on the server.

Resending "Draft" packages

When the transfer for a package you send fails to start, AoC displays a transient error message with the heading "Verify contents and resend" and moves the package to the Drafts folder in your Packages app.

If you see the error message "Verify contents and resend", do the following:

1. Click Edit saved draft in the error message to open the Drafts folder. You can also open the Drafts folder from the left panel of the Packages app.
2. In your Packages app Drafts folder, click the package row to view the package details. Any files and folders listed have been transferred successfully. Files and folders that you sent but are not listed did not transfer.
3. Add the missing content: click Upload to browse, or drag items to the sending panel.
4. Click Send.
The files that were transferred successfully in the first attempt will not be transferred again since they already exist at your intended destination; this means you do not incur more transfer and storage charges. Yet the final package contents are intact in your Sent folder after the transfer succeeds.

To contact your local tech support administrator, click  in the banner and select "Technical support".

Files App: Using a shared file repository

The AoC Files app allows users to share access to a file repo. Learn how to share content from your cloud or local storage with Files app members. Configure collaboration rules that govern how and with whom members can share content. Understand content permissions and security. Troubleshoot shared folder access issues.

- [Files app basics](#)
Learn about the many features of the Files app for sharing content within and beyond the workspace. Understand content permissions and content security features. Find tips to accelerate Files app configuration.
- [Configuration options](#)
Learn key sharing strategies. Get step-by-step procedures to configure the Files app to protect content while allowing users to collaborate effectively. Control and monitor usage in the Files app. Share content from your storage to your Files app users.
- [Troubleshooting: Sharing files and folders](#)
Solve problems with shared folder access. Investigate and fix improper access issues in the Files app.

Files app basics

Learn about the many features of the Files app for sharing content within and beyond the workspace. Understand content permissions and content security features. Find tips to accelerate Files app configuration.

- [What is the Files app?](#)
The Aspera on Cloud Files app allows users in a workspace to access a collection or repository of folders. Once accessible in the Files app, these folders can be shared freely with one or more members of the workspace, according to permissions set by the person sharing the folder. Workspace members can also share with people outside the workspace according to permissions configured by the org admin or workspace manager.
- [Content permissions](#)
You have a specific permission or access level for each file or folder in your Files app. Check your permission to a given folder by right-clicking and selecting Info.
- [Content security in the Files app](#)
In addition to securing access controls, protecting content directly ensures that digital assets retain their value even as Aspera on Cloud users collaborate to develop, exchange, and deliver content. This article collects and describes configuration options that administrators and users can set in the Files app to protect content assets.
- [File deletion policies for storage management](#)
You can create policies to permanently delete files and folders when they reach a configured age. If the policy deletes all files in a given folder, the policy deletes the folder as well. Existing empty folders are not deleted. Shared folders and folders with public links are never deleted by a file deletion policy, though the content they contain may be deleted. Users with an Essentials edition of Aspera on Cloud have access to this policy on one node, Standard Plus users can configure it on ten nodes, and Premium edition users can configure it on 250 nodes.
- [Accelerate Files app setup through inheritable settings](#)
Certain aspects of the Files app are hierarchical, allowing administrators to speed deployment.

What is the Files app?

The Aspera on Cloud Files app allows users in a workspace to access a collection or repository of folders. Once accessible in the Files app, these folders can be shared freely with one or more members of the workspace, according to permissions set by the person sharing the folder. Workspace members can also share with people outside the workspace according to permissions configured by the org admin or workspace manager.

See also [Should I send or share?](#) and [What is the Packages app?](#)

Files app in the organization and in the workspace

The Files app is enabled for your organization by default. You can disable it for the entire org if no workspaces need permission-based access to folders in a shared repo. When you enable the Files app for a given workspace, all members of that workspace can access and use Files.

If enabled for your organization, you can enable or disable the Files app in each workspace. When you add a new member to the workspace, that person automatically gains access to the Files app in that workspace, including to folders shared with that workspace, by an administrator or by another user.

You configure the Files app at the global level. Global settings are inherited by the Files app in each workspace where it is enabled. An admin or a workspace manager can customize inherited settings at each workspace. For details, see [Accelerate Files app setup through inheritable settings](#).

When you add a new member the workspace, that person automatically gains access to the Files app in that workspace.

Add files and folders to the Files app

The folder must be in the Files app before it can be shared. Folders in the Files app may be added by:

- The administrator, who can make folders from a transfer server available to Files app users in a given workspace.
- Files app users with permission to upload, who can then share their folders with others.
- Other Files app users who share folders.
- A Files app user can save content they receive in a package in the Packages app directly to their Files app (assuming they are member of both apps in the same workspace).

Share folders

The folder must be in the Files app before it can be shared. Note that you cannot share a file, only a folder. To share a file, place it in a folder, then share the folder.

A workspace member with access to the Files app can freely share folders within the app with other workspace members. With proper permissions, the member can share folders with AoC users outside the workspace, or with people who do not have an AoC account.

Users who receive shared access to a folder can in turn share it with others, according to their permission in the workspace and to their permissions to the specific folder. When re-sharing a shared folder, they can grant only the access they have to the folder, or less.

Upload and share

Files app members with proper [permission](#) can upload files and folders from any accessible source (user desktop, local or remote storage, attached node) to the app. Once the folder is uploaded, that user can share the folder with others. Until the folder is shared, it is visible and accessible *only* to the user who uploaded it (and to the administrator). For details, see [Managing storage usage](#).

Permissions

When users share folders with others, they grant each recipient specific permissions to act on the folder and its contents. Users can share a folder with one group of colleagues, granting them specific permissions, and share with a different group of colleagues with a different set of permissions.

Permissions *presets* bundle the atomic content permissions most often used together:

- Edit (This is the highest level of permission and gives a user full control over the item, it contains all other permissions.)
- Download (browse folder content, preview supported movie file types, download the folder or its contents)
- Preview (browse and preview)
- Upload (create and upload folders and upload files)

Atomic permissions are also available:

- Browse folder contents
- Upload files and folders to the folder
- Create or upload an empty folder in the shared folder
- Download the folder or its contents
- Rename the folder
- Preview the movie files in the folder (users can always view thumbnail previews of supported image types)
- Delete or overwrite files and folders in the folder

Save to the Files app from the Packages app

Files app users can save content they receive in a package in the Packages app directly to their Files app (assuming they are member of both apps in the same workspace).

Send packages directly from the Files app

Packages app users can send digital packages directly from the Files app (assuming they are member of both apps in the same workspace). This means users don't have to download content from Files, switch to the Packages app, then create a digital package and send. Rather, they can right-click an item in their Files app and select Send via Packages to open the Send files form.

Content permissions

You have a specific permission or access level for each file or folder in your Files app. Check your permission to a given folder by right-clicking and selecting Info.

There are four preset or composite permissions and seven custom permissions for content in your Files app:

- **Preset or Composite permissions:**
 - **Edit** (also called *Can Edit*)

This is the highest level of permission and gives a user full control over the item; it contains all other permissions.
 - **View** (also called *Download Only*)

Includes *Browse*, *Download*, and *Preview* permissions.
 - **Upload**

Includes *Create/Upload folders* and *Upload files*
 - **Preview**

Includes *Browse* and *Preview*
- **Custom permissions** (content must reside on a transfer server with node software at version 3.7.4 or higher; see the "Package Information" section of the IBM Aspera High-Speed Transfer Service [Release Notes](#) for specific build numbers for your platform):
 - **Create/Upload folders**

Create or upload an empty folder; to upload folders containing files, enable this permission along with *Upload files*.
 - **Rename**

Rename files and folders.
 - **Upload files**

Upload files and folders; to upload folders containing files, enable this permission along with *Create/Upload folders* permission -- or use *Upload* composite permission. See *Delete* below for uploading a file with the same name as an existing file (overwrite or replace). You need *Upload* permission to a folder to move or copy content to it.
 - **Download**

Download the folder or file in the folder.
 - **Preview**

Preview movie files in the folder. Thumbnail previews of supported image tiles are always available.
 - **Browse**

Browse folder content; if this setting is not enabled, you can see the folder but cannot view folder contents.
 - **Delete**

Delete or overwrite files and folders in the folder.

The permission you have to a given file or folder depends upon how you gained access to it. Check your permission to a given folder by right-clicking and selecting Info.

- For items you upload to the root level of your Files app, and for items you move from a package in your Packages app to the root level of your Files app, you have full *Edit* permission (requires *Upload* permission to the root level; if your administrator has restricted upload capability to the root level of your Files app in this workspace, you can upload only to folders to which you have upload permission, not to the root level).
- For items you upload or move into a folder, you have the same permission that you have to the folder.
- For folders shared with you, you have the permission granted to you by the person who shared.

Note: The person who shared a folder with you is the only person who can change your permission to that folder. The person sharing can grant you only the permissions they have to the given folder, or a lesser permission; for example, if I have **Browse**, **Preview**, and **Download** permission, I can grant you one or more of those three permissions, but I cannot grant you **Delete** permission, since I myself don't have **Delete** permission.)

In the same way, the permission you can grant to a folder you share depends on the permissions you have to that folder. You can grant any or all of the permissions that you yourself have to that folder, but you cannot grant a permission that you do not have.

Internal and other permissions

An administrator or workspace manager may see a shared item identified as having an "Internal" or "Other" permission. These permission may appear only when you set the advanced filter to Show all permissions.

This identification can indicate a number of different scenarios, as follows:

- **Internal permission: workspace folder**

This permission was created by the system to display and track shared folders in Aspera on Cloud.
- **Internal permission: application**

This permission was created by the system for internal purposes.
- **Other permission: node or other app**

This permission was created by an admin on an attached node, by an API user, or by a user of another app like Aspera Drive.
- **Created by the Automation app**

This permission was created in an automated workflow in the Automation app.

Content security in the Files app

In addition to securing access controls, protecting content directly ensures that digital assets retain their value even as Aspera on Cloud users collaborate to develop, exchange, and deliver content. This article collects and describes configuration options that administrators and users can set in the Files app to protect content assets.

Admin controls

By default, collaboration in the Files app is unrestricted. But as an admin, you can apply increasingly restrictive controls to sharing actions available to Files app members.

Global: Admin > Applications > Files

Workspace: Admin > Workspaces > *workspaceName* > Applications > Files

- Prevent app users from sharing with unauthenticated recipients; restrict the use of [public links](#): Who can share folders via public links
- [Prevent](#) app users from sharing with non-workspace members: Who can share folders with external users
- Allow sharing with [designated non-workspace members only](#); list specific external users as the only valid recipients: Who are eligible external users
- Prevent accidental sharing with the entire workspace: Who can share folders with the entire workspace
- [Require](#) external users to create an AoC account and log in to receive a package

User controls

As an admin, you can establish workflows that guide your workspace members how to use these additional content security measures:

- Apply [content permissions](#) to shared content
- Require a password to access content shared using a [public link](#)
- [Unshare](#) a folder

File deletion policies for storage management

You can create policies to permanently delete files and folders when they reach a configured age. If the policy deletes all files in a given folder, the policy deletes the folder as well. Existing empty folders are not deleted. Shared folders and folders with public links are never deleted by a file deletion policy, though the content they contain may be deleted. Users with an Essentials edition of Aspera on Cloud have access to this policy on one node, Standard Plus users can configure it on ten nodes, and Premium edition users can configure it on 250 nodes.

Attention:

- **For ATS nodes:** If there are additional nodes in the same bucket, the same file deletion policy applies to those nodes as well.
- **For tethered nodes:** The policy applies only to the specific node that you are creating the policy for. Beware that if there are other nodes that share the same storage and bucket path, this policy is going to affect those as well. This could lead to content being deleted from other nodes that the policy was not intended to.

Note: You can set file deletion policies on buckets in AWS, S3, CGCS and Microsoft Azure storage.

1. Go to Nodes and storage > Nodes. Click the row of the intended node.
2. Go to Profile > File deletion policy.
3. Click the toggle to On.
4. Set the deletion age in days. Valid values are 7 to 3650 days. The deletion job runs daily. A timer is set to start 24 hours after the last run. It does not have a set start time, as it runs depending on when it was last completed.

Note: The time the job takes to run depends on how large the bucket is.

For example, if you configure the deletion age to be 90 days, the policy will:

- Permanently delete files in that bucket 90 days after their creation. This deletion age applies to existing files that are older than the deletion age, as well as to new files when they reach the configured deletion age.
- Permanently delete folders that are emptied by the deletion job.
- Not delete empty folders that were not affected by the policy.
- Not delete shared folders or folders with public links, even if they are emptied by the deletion job.

5. Click Save to activate the file deletion policy.

Workspace folder protection

The workspace package and home directory file system structure are preserved when there is a file deletion policy in place.

Accelerate Files app setup through inheritable settings

Certain aspects of the Files app are hierarchical, allowing administrators to speed deployment.

There are several settings for the Files app that you can configure at the global app level. Global app settings are inherited by the Files app in each workspace in the org. In each workspace, you can override inheritance to customize settings as required.

Inherited settings include:

- Collaboration
- Public and authenticated link styles
- [Restrict usage](#) (workspace level only; can exempt users and groups from the restriction)

To override inherited settings, go to Workspaces > *workspaceName* > Applications > Files > Settings; then select the check box for Override global app settings.

Hierarchical Level	Inheritance and Customization	Configuration Location
Organization: Files app	Can customize defaults.	Applications > Files
Workspace: Files app	Default: Inherit from global app settings. Can override inheritance to customize for an individual workspace.	Workspaces > <i>workspaceName</i> > Applications > Files

Configuring inheritable Files app settings

As an organization administrator, you can:

- Configure global Files app settings that are inherited as defaults in all workspaces.
- In a given workspace, override inherited global settings.
- Delegate workspace settings to a [workspace manager](#).

To configure global, organization-wide settings for the Files app, do the following:

1. Go to **Applications > Files**.
2. Check the box labeled **Enable application**.
3. Configure the settings as described in the related articles.
4. Click Save.

To configure workspace-level settings for the Files app, do the following:

1. Go to **Workspaces**, then select the workspace.
2. Go to **Applications > Files**.
3. Select the check box labeled **Enable application**.
4. Clear the box labeled **Use global app settings**.
5. Configure the settings as described in the related articles.
6. Click Save.

Configuration options

Learn key sharing strategies. Get step-by-step procedures to configure the Files app to protect content while allowing users to collaborate effectively. Control and monitor usage in the Files app. Share content from your storage to your Files app users.

- [Share a node folder with a workspace](#)
To allow the members of a workspace to use the content in a node attached to your org, an admin must give them access to the content. When you *administratively share* a folder with users, as described in this procedure, all admins in your org can manage the folder access. This shared management ability is typically preferable to having one admin user share a folder as an individual user; in such case, only that individual admin can revoke or change access permissions.
- [Share folders using public links](#)
When an Aspera on Cloud Files app member uses a public link to share folders, Aspera on Cloud notifies the recipient by email. The recipient can use the link in the email to access the shared content in an Aspera on Cloud portal. The recipient of a public link does not log in to Aspera on Cloud.
- [Share folders with external users](#)
When an Aspera on Cloud user shares folders with an external user, Aspera on Cloud sends an email to the recipient notifying them of the shared content. When the recipient clicks the link in the email notification, Aspera on Cloud directs them to create a password and log in to Aspera on Cloud. The recipient then has an Aspera on Cloud account, and can access the shared content in an Aspera on Cloud portal. This user becomes a Limited user in the organization.
- [Control content sharing in the workspace](#)
By default, all members of a workspace can share a folder with the entire workspace by entering the workspace name in the **Share** form. To reduce the risk of a workspace member unintentionally sharing sensitive content workspace-wide, you can restrict this capability to workspace managers only. You can also prevent all members and managers from sharing with the entire workspace in this way.
- [Configure public and authenticated link styles for sharing folders](#)
Members of the Aspera on Cloud Files app send URL links when sharing folders with others. The administrator can configure one of three link styles that Aspera on Cloud generates for file sharing operations.
- [Sharing strategies](#)
When a user shares folders using the Files app, they give those they share with direct access to the same source material they have. If the recipient changes, deletes, or overwrites the content shared with them, that content is changed at the source. The Files app provides multiple ways to share files within and outside the workspace. Choose the strategy that best meets your collaboration and content security goals.
- [Control and monitor usage in the Files app](#)
By default, all Files app users can upload and create folders without restriction. But in any given workspace, you can prevent members from uploading content you cannot readily monitor.
- [Unshare a folder](#)
You may need to remove a colleague's access to a folder you shared with them. You can unshare a folder, whether your colleague has access as a folder collaborator or via a shared link.
- [Configuration scenario: Sharing with external colleagues](#)
If your team collaborates with vendors, contractors, or other colleagues in a different company by sharing access to a repository of files and folders, use this article to configure your organization. You'll use the Aspera on Cloud Files app to enable secure and permission-based sharing of folders among designated collaborators.
- [Configuration scenario: Workspace members sharing a file repository](#)
If your team shares access to files and folders in a common repository, use this article to configure your organization. You'll use the Aspera on Cloud Files app to enable secure and permission-based sharing of folders among collaborators.

Share a node folder with a workspace

To allow the members of a workspace to use the content in a node attached to your org, an admin must give them access to the content. When you *administratively share* a folder with users, as described in this procedure, all admins in your org can manage the folder access. This shared management ability is typically preferable to having one admin user share a folder as an individual user; in such case, only that individual admin can revoke or change access permissions.

Use this procedure to give users in the Files application:

- Shared access to content in your cloud or on-prem storage.
- A folder in which they can collaborate on content according to the permissions you set.

Once you share the folder using this procedure, users see it on the top level of their Files app.

For each folder you share, you set permissions for each user and group you share with. These permissions determine the actions that users can take on the folder contents. For details, see [Content Permissions](#).

This procedure allows you to share one folder at a time with one or more members of a single workspace. To share multiple folders, or to share a folder with users in multiple workspaces, repeat the procedure

Procedure

Note: To complete this procedure, you need the secret of the node containing the folder you want to share.

1. Go to Workspaces > *workspaceName* > Applications > Files app > Shared folders > Create new.
2. Do one of the following:
 - Enter the node secret and click Log in.
 - If you have a different access key for this node, click **Use custom access key**, enter the key and associated secret, then click **Log in**.
3. (Optional) To create a new folder on the node, do the following:
 - a. Click Create folder.
 - b. Enter a name for the new folder and click Create.
4. From the list of folders that displays, select the folder to share by clicking the option button on the folder row.
If required, you can click a folder name to drill into it. Go back up a level using the breadcrumb list at the top of the modal.
5. (Optional) To display a different name for the folder to the workspace users (perhaps a name that may be most meaningful to them), enter the desired name in the Display name text box.
6. Click Submit.
7. To give all members of the workspace access to this folder, click Add all workspace members.
 - a. Set the access permission level for these users.
 - b. If desired, add other members you want to access this folder at the permission level you set.
 - c. Click Add.
8. To give specific workspace members access to this folder, click Add member.
 - a. Set the access permission level for these users.
 - b. Enter the names of workspace members which whom to share this folder at this permission level.
 - c. Click Add.
9. To change a user's access to the shared folder, click the user row to open the record, adjust permissions as required, then click Save.
10. To remove a user's access to the shared folder, select the check box to the left of the user row and click Delete.

Note:

When new members join the workspace Files app, they can see and access shared folders as follows:

- Folders shared with the entire workspace.
- Folders shared with the new member as an individual or as a group member.

Add a member to an existing shared folder

1. Go to **Workspaces > *workspaceName* > Applications > Files app > Shared folders**.
2. Right-click the intended folder to see the current member list.
3. Do one of the following:
 - Enter the node secret and click Log in.
 - If you have a different access key for this node, click **Use custom access key**, enter the key and associated secret, then click **Log in**.
4. Click Add member.
5. Select the access permission for this new member.
6. Enter the member name.
7. Repeat steps 5 and 6 for additional new members.
8. Click Add.

Node access for workspace managers

1. Go to Workspaces > *workspaceName* > Profile > Node access for workspace managers.
2. Click Add.
3. In the Name drop down, select the node you want to give access to.
4. In the Access key field, enter the access key provided by your administrator.
5. In the Secret field, enter the secret associated with the access key.
Click the eye icon to show or hide the secret as you type.
6. From the Node owners drop down, select who can manage the node:
 - a. Only ATS admins: Only ATS administrators can manage the node.
 - b. All admins: All administrators can manage the node.

Note: Node owners can browse and manage this node without the need of an access key.
7. Click Log in to save the configuration and establish node access.
8. Click Cancel if you do not want to save the configuration and exit.

Share folders using public links

When an Aspera on Cloud Files app member uses a public link to share folders, Aspera on Cloud notifies the recipient by email. The recipient can use the link in the email to access the shared content in an Aspera on Cloud portal. The recipient of a public link does not log in to Aspera on Cloud.

The public link is truly public, in that the recipient can forward the link to another user, who can use the link to access the content that was shared. Use public links with trusted colleagues and non-vital content.

To send a public link, the Files app user right-clicks the folder to share and selects **Manage all links**; then creates or selects an existing public link and applies the intended access permissions for this user. For more information, see [What is a Public Link?](#) and [Share with unauthenticated recipients using public links](#).

As an admin, you can determine which member types, if any, can send public links.

1. To configure the global Files app, go to **Applications > Files > Profile > Collaboration > Who can share folders via public links**.
 - Select **All members** (default) to allow all members of workspaces in your organization to share folders with external users using public links.
 - Select **Managers only** to allow only managers of workspaces to share using public links.
 - Select **No one** to prevent all workspace members, including workspace managers, from sharing with public links.
2. Click **Save**. The setting you choose here is inherited by all workspaces in the organization. To override this inherited setting for a given workspace, go to the next step.
3. To configure this Files app setting for a given workspace, do the following:
 - a. Go to **Workspaces > workspaceName > Applications > Files > Profile**.
 - b. Clear the check box labeled **Use global app settings**.
 - c. In the field labeled **Who can share folders via public links**, select the intended workspace member type for this workspace: **All members**, **Managers only**, **No one**.

Share folders with external users

When an Aspera on Cloud user shares folders with an external user, Aspera on Cloud sends an email to the recipient notifying them of the shared content. When the recipient clicks the link in the email notification, Aspera on Cloud directs them to create a password and log in to Aspera on Cloud. The recipient then has an Aspera on Cloud account, and can access the shared content in an Aspera on Cloud portal. This user becomes a Limited user in the organization.

The Aspera on Cloud workspace member shares with external users by right-clicking a folder in the Files app and selecting **Share**. Then they enter the email address of the external user and apply the intended [access permissions](#) for this user.

1. To configure the global files app, go to **Applications > Files > Profile > Collaboration > Who can share folders with external users**.
 - Select **All members** (default) to allow all members of workspaces in your organization to share folders with external users.
 - Select **Managers only** to allow only managers of workspaces to share folders with external users.
 - Select **No one** to prevent all workspace members, including workspace managers, from sharing with external users.
2. Click **Save**.

The setting you choose here is inherited by all workspaces in the organization. To override this inherited setting for a given workspace, go to the next step. Note that for a given workspace, you can specify emails and groups that are eligible to receive access to a shared folder; this prevents workspace members from sharing with users whom you have not designated as eligible.
3. To configure this Files app setting for a given workspace, do the following:
 - a. Go to **Workspaces > workspaceName > Applications > Files > Settings**.
 - b. Deselect the check box labeled **Use global app settings**.
 - c. In the field labeled **Who can share folders with external users**, select the intended workspace member type for this workspace: **All members**, **Managers only**, **No one**.
 - d. If you chose **All members** or **Managers only** in the previous step, you can specify people with whom workspace members are permitted to share folders. Select the intended users in the field labeled **Who are eligible external users**.
 - e. If you select **Only the following emails and groups** or **Any email plus the following groups** in the previous step, enter the intended recipients in the following field.
4. Click **Save**.

Control content sharing in the workspace

By default, all members of a workspace can share a folder with the entire workspace by entering the workspace name in the **Share** form. To reduce the risk of a workspace member unintentionally sharing sensitive content workspace-wide, you can restrict this capability to workspace managers only. You can also prevent all members and managers from sharing with the entire workspace in this way.

When you configure this restriction, the **Share** form does not accept the workspace name as a valid entry. Note that users can, however, work around this restriction by entering every workspace member name in the form.

To configure this restriction, do the following:

1. To configure the global Files app, go to **Applications > Files > Profile > Content control**.
2. In the field labeled **Who can share folder with the entire workspace**, select the intended workspace member type for this workspace: **Members**, **Managers**, **No one**.
3. Click **Save**.

The setting you choose here is inherited by all workspaces in the organization. To override these inherited settings for a given workspace, go to the next step.
4. To configure Files app settings for a given workspace, do the following:
 - a. Go to **Workspaces > workspaceName > Applications > Files > Profile**.
 - b. Deselect the check box labeled **Use global app settings**.
 - c. In the field labeled **Who can share folders with the entire workspace**, select the intended workspace member type for this workspace: **Members**, **Managers**, **No one**.
5. Click **Save**.

Configure public and authenticated link styles for sharing folders

Members of the Aspera on Cloud Files app send URL links when sharing folders with others. The administrator can configure one of three link styles that Aspera on Cloud generates for file sharing operations.

When a Files app users shares a folder, Aspera on Cloud sends the recipient an email notification containing a link.

There are three URL styles available:

- **Standard URLs**
 - Select Standard to generate full-length URLs.
 - Example of standard URL: https://aspera.ibmaspera.com/public/send?token=HBf-sfRFIHFMUXuYdocSi22X8pYRk_E8OxXOi4IOOWs
 - **Short URLs**
 - Short URLs are enabled by default for a workspace.
 - Example of short URL: <https://aspera.pub/2dexfa>
 - **Personalized URLs**
 - When you select Personalized, Aspera on Cloud uses a default that includes the sharer's username; for example: https://aspera.pub/2dexfa/Jane_Doe.
 - When you select Personalized, users can customize the default URL and compose a string of up to 240 characters. All characters beyond the conventional alphanumeric set (A through Z; a through z; 0 through 9) are replaced with underscore characters.
 - Example of customized personalized URL: https://aspera.pub/2dax/My_Own_Personal_Link
1. To configure the global Files app, go to Applications > Files > Public and authenticated links > URL styles.
 2. Select one of the following:
 - Standard
 - Short
 - Personalized
 3. Click Save.

The setting you choose here is inherited by all workspaces in the organization. To override these inherited settings for a given workspace, go to the next step.
 4. To configure this Files app settings for a given workspace, do the following:
 - a. Go to Workspaces > *workspaceName* > Applications > Files > Profile.
 - b. Clear the box labeled Use global app settings.
 - c. Go to Public and authenticated links > URL styles; select the intended style.
 - d. Click Save.

Sharing strategies

When a user shares folders using the Files app, they give those they share with direct access to the same source material they have. If the recipient changes, deletes, or overwrites the content shared with them, that content is changed at the source. The Files app provides multiple ways to share files within and outside the workspace. Choose the strategy that best meets your collaboration and content security goals.

Aspera on Cloud gives you three way to share folders:

- Share a link with an existing folder collaborator; the recipient must log in to access the folder. A *folder collaborator* already has access to the folder, but you can send a link to direct them to new or specific content in the folder.
- Share a folder and add the recipient as a folder collaborator; the recipient must log in.
- Share a link with someone who is not a member of your workspace without requiring them to create an AoC account and log in.

Share a link with an existing folder collaborator; recipient must log in

Use this method to share a link to the folder with someone who is already a member (collaborator) of the folder. This is a convenient way to link a collaborator to a specific location within a folder.

1. Right-click a folder row and select **Get shared link**.
 2. If this is the first private link to this folder, click **New link**.
 3. Select **Private link**. Only folder collaborators can access this folder with this link.
 4. If a modal displays with an editable text field, you can customize the link. Enter a link name that will be useful and informative to you and to your recipients; click **OK**. If you don't see this editable field, your admin has not configured this customization capability; go to the next step.
 5. To resend an existing link, click **Manage links**; locate the link to resend, then click **Copy**; deliver the link by any method you choose. Skip step 6.
 6. Deliver this link to your collaborator by either of these methods:
 - Click **Copy**, then deliver the link by any method you choose.
 - Enter an email address or username, and an optional message; then click **Send**.
- Results:**
- Your collaborator can use the link to jump directly to the folder you shared, even a nested folder.
 - They can access the folder according to the permissions they currently have to it.

Share a folder and add a folder collaborator; recipient must log in

Use this method to:

- Share a folder with a member of your workspace and add them as a folder collaborator.
- Share a folder with someone who is not a member of your workspace and add them as a folder collaborator; this can include someone who is not a member of your AoC organization at all. Note that your administrator determines whether you can share outside your workspace and with whom.

1. Right-click a folder row and select **Share**.
2. Select or enter one or more recipients.
3. Assign access permissions.
4. Click **Share**.

Results:

- For a workspace member, the folder you share displays at the root level of their Files app in the sort order your fellow member has configured. They have the access permissions that you set for them. AoC sends them an email notification that the shared folder is available (note that individual users can disable notifications). The

link in this notification takes them directly to the folder once they log in to AoC. They become a collaborator in the folder.

- For someone who is not a member of your workspace, AoC sends an email notification that the folder is available. When the recipient clicks the link in the email, AoC prompts them to download and install IBM Aspera Connect, the same software you installed to enable transfers between your desktop and an Aspera server (see Aspera Connect for Outside Users). Once the Connect installation is complete, AoC presents a portal that allows them to access the folder you shared. They can act on the folder contents according to the access permissions you set. If this person was not already a member of the AoC organization, this person becomes a [limited user](#) in the organization, without workspace membership, with access to this folder and its subfolders only. They must log in to Aspera on Cloud to access the folder contents.

Share a link with someone who is not a member; recipient does not need to log in

Use this method to share with someone outside your workspace without inviting them to your workspace or to your AoC organization.

This sharing method allows you to apply a password to the link. When your recipient clicks the password-protected link, they must apply the same password to access the folder. Aspera on Cloud generates a password, or you can choose your own password for a given link. You must deliver the password to your recipient based on your own site security practices.

1. Right-click a folder row and select **Get shared link**.
2. Select **Public link**. Anyone can access this folder with this link.
Note: Be aware that the public link you send is not restricted to the person you send it to. The recipient of your public link can forward the link to someone else, who can then use the link to access the content you share. Share public links only with trusted colleagues when the security of the folder content is not vital.
3. If this is the first public link to this folder, click **Create one**.
4. If a modal displays with an editable text field, you can customize the link. Enter a link name that will be useful and informative to you and to recipients; click **OK**. If you don't see this field, your admin has not configured this customization capability; go to the next step.
5. Set the expiration for this link to determine the duration that your recipient should have access to this folder. After that duration, the link becomes invalid.
6. Set the permission you want your recipient to have to the contents of this folder. For details, see [Content permissions](#).
7. To require a password for this link, click the toggle labeled **Require password**.
Aspera on Cloud generates and displays a password.

- a. To generate a new password, click the circular icon.

When you regenerate a password, all previous passwords become invalid. If past recipients are using this link with a previous password, give your past recipients the new password.

- b. To create your own password, delete the generated password and enter your desired password into the field.

- c. To copy the password, click the copy icon.

The password remains on your clipboard until you copy something else. Be sure to save the password in secure file before you copy anything else.

Important: Aspera on Cloud does not save the password. Once you click Save in the following step, you cannot recover the password. You can regenerate the password for a link, but when you do, the former password becomes obsolete: other users (if any) of the link will be locked out unless you give them the new password.

Note: If you use multiple password-protected links, consider keeping a secure file of links and their passwords. You cannot recover a lost password.

- d. Click **Save**.
 - e. Deliver the password to your recipient according to your local site security practices.
8. Deliver this link to your collaborator using one of these methods:
 - Click the **Copy** icon in the link field, then deliver the link to your recipient according to your local site practice. **Important:** When you click **Copy**, the link overwrites anything existing on your clipboard. If you previously copied the password, be sure you stored the password in a secure location before copying the link itself.
 - Enter an email address or username, and an optional message; then click **Send**.
AoC sends an email notification to each recipient. When they click the link in the email, AoC presents a portal that allows them to access the folder.

Results:

- When your recipient tries to use the link, AoC prompts them to download and install IBM Aspera Connect, the same software you installed to enable high-speed transfers between your desktop and an Aspera server. It may be helpful to remind them that, after they install Connect, they may need to adjust their browser settings to allow Aspera Connect to run. Just like you, they must install the Connect app once on their computer, and they must add the browser extension once in each browser they'll use to access Aspera on Cloud. For details, see [Installation](#).
- Link recipients can act on the folder according to the permissions you set until the expiration you set for the link.

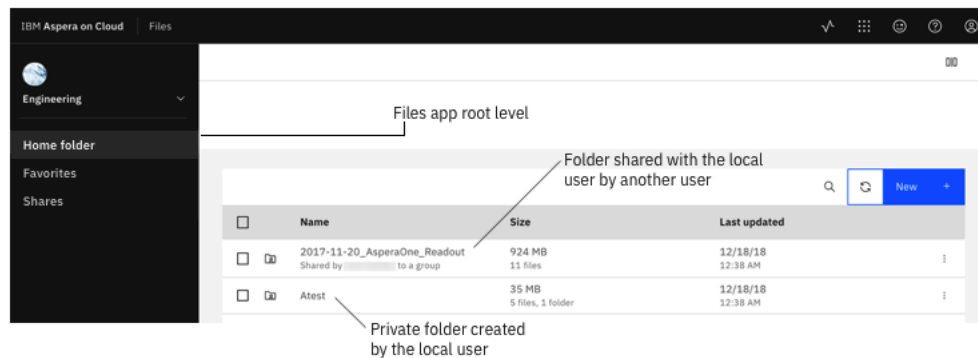
Control and monitor usage in the Files app

By default, all Files app users can upload and create folders without restriction. But in any given workspace, you can prevent members from uploading content you cannot readily monitor.

This restriction ensures that:

- The storage your organization pays for contains only the contents you intend.
- The transfer volume charged to your organization supports your corporate, team, or project mission, rather than being used for unrelated storage by individual members.

To prevent unrelated storage, you can disable members' ability to upload to the root level of the Files app. This root level, also called the home folder, is a storage area that you cannot readily monitor. The home folder includes folders created by the local user at the root level. This area displays the label **Home folder**.



Even if you configure this restriction, you can share folders with members and grant members permissions to view, upload to, or download from those specific folders. In this way, members can collaborate in folders that you can watch; they cannot upload to locations that you can't readily monitor.

Note: Admins can view and manage content in Files home folders if they have the node secret. See "Managing User Storage in the Workspace" in [Managing storage usage](#). Once you configure this restriction for a workspace, you can exempt specific users or groups from it. The members you exempt can upload to and create folders on the root level of their Files app.

- To restrict all users in your organization from uploading their Files app as described previously, do the following:
 - Go to **Applications > Files**.
 - In the **Restrict usage** area, set the toggle labeled **Members can upload to and create folders on their home folder** to Off.
 - Click **Save**.
The setting you choose is inherited by all workspaces in the organization. To override this inherited setting for a given workspace, go to the next step.
- To override the global app setting for a given workspace, do the following:
 - Go to **Workspaces > workspaceName > Applications > Files > Profile**.
 - Clear the box labeled Use global app settings.
 - Set the toggle labeled **Workspace members cannot upload to workspace root level** to On.
 - Click **Save**.
The setting you choose applies to all members of this workspace. When the restriction is in place for a given workspace, you can exempt specific users or groups from this restriction. Go to the next step.
- To exempt a specific member from this restriction, do the following:
 - Go to **Workspaces > workspaceName > Members > memberName**. Click the member row to open the record.
 - Check the box labeled **This member can upload to root of this workspace**.
 - Click **Save**.

Unshare a folder

You may need to remove a colleague's access to a folder you shared with them. You can unshare a folder, whether your colleague has access as a folder collaborator or via a shared link.

Remove a folder collaborator

To remove a folder collaborator's access to a shared folder, do the following:

- Click to open the folder to unshare.
- In the upper right, click the Collaborators icon; then click See all collaborators.
- Find the intended collaborator; click the **Revoke** icon, then confirm.

Delete a shared link

To remove folder access via a link, do the following:

- Right-click the intended folder and select **Manage all links**.
- For the intended link, click the trash can icon.
Note: When you delete a link, everyone using that link to access the folder loses access.

To troubleshoot unsharing issues, see [User still has access to unshared folder](#).

Configuration scenario: Sharing with external colleagues

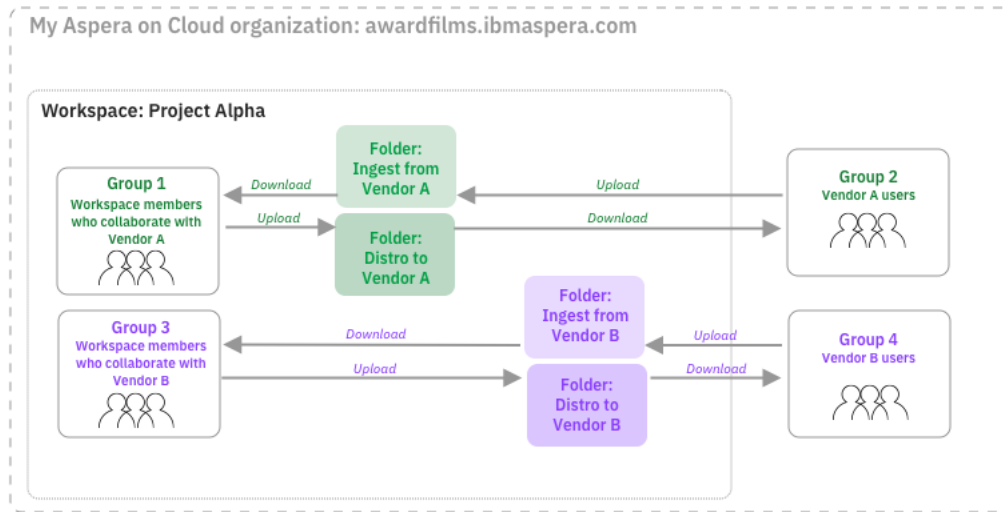
If your team collaborates with vendors, contractors, or other colleagues in a different company by sharing access to a repository of files and folders, use this article to configure your organization. You'll use the Aspera on Cloud Files app to enable secure and permission-based sharing of folders among designated collaborators.

For example, perhaps your team is:

- A news organization receiving files from dispersed reporters and content providers.
- A production company distributing files to theaters in diverse locations.
- A team of scientists collaborating with researchers at a distant university to study the feasibility of exploratory mining in a given site.

- Part of a production company sharing assets with vendors who provide coloration or other services.
- A medical research group sharing large sets of genomic data files with scientific collaborators at remote sites.

Aspera proposes a workspace like this. This setup is flexible of course, and you can adapt it for your specific needs.



Your AoC organization: Overview

Your Aspera on Cloud (AoC) organization is the primary container and administrative unit in your AoC subscription.

Customize your URL to brand your org

You can name your org and configure the subdomain of the URL that users will browse to access your org. For example, if your company name is Award Films, you can choose to use the URL `awardfilms.ibmaspera.com`. For details on this one-time-only configuration, see [Customize your organization URL, name, and logo](#).

Your users collaborate in a workspace

A workspace is a digital space where designated members can collaborate. Each workspace is a collection of specific users, files and folders, access permissions, and collaboration rules. The users, files, and folders in one workspace are completely separate from those in another workspace. You'll configure a workspace in Procedure 2 below.

Users in a given workspace can collaborate freely with other members of the same workspace. By default, workspace members can also collaborate with users outside the workspace. But the admin can restrict that privilege if necessary; see Procedure 3 below.

Your files and folders are in IBM Cloud storage

Each Aspera on Cloud subscription includes one built-in, [Aspera-managed auto-scale transfer cluster](#) attached to storage in IBM Cloud.

This Aspera transfer cluster (also called ATS, Aspera transfer service; sometimes called a *node*) is the engine that AoC uses to upload and download your files and folders to and from your built-in IBM Cloud storage. ATS is hosted and managed by IBM Aspera.

The built-in IBM Cloud storage hosts your organization workspace, including the content your users upload and share using the Files app. As an admin, you can also upload content directly to this storage and then make that content available to your users. (Storage capacity depends on your AoC subscription tier.) See procedure 4 below.

The access credentials (access key and secret) for this transfer cluster and storage are delivered to the administrator who first created the AoC organization. You should [retrieve and securely store the access credentials](#); they allow you to access and manage your IBM Cloud storage.

Note: You can attach your own local or cloud storage to Aspera on Cloud and then share storage contents with workspace users, but that process is not covered in this document; see articles in the Nodes section of this Help Center.

- To attach your existing cloud storage to AoC, see [Attach your existing cloud storage](#).
- To attach your own Aspera HSTS server, see [Tether Your Aspera Transfer Server to Aspera on Cloud](#).

Process overview

These are the high-level steps required to configure the scenario shown in the graphic in the opening section of this article; detailed procedures follow. Adapt as needed for your own requirements.

Use the AoC Admin app to:

1. Create groups of users, both internal and external, to simplify and accelerate user management.
2. Configure the workspace in which your groups will collaborate. Add your internal user groups as workspace members.
3. (Optional) Configure the Files app to allow your workspace members to collaborate with your designated external groups only. This configuration is by no means required, but provides content security for your proprietary assets.
4. Create the folders in which your internal and external groups will collaborate; share the folders with your groups, assigning specific permissions to allow them access while preserving content security.
5. (Optional) Configure notifications to alert internal users when new content appears in their folders.

Important: As an admin, you must provide a transfer method for your users. You can do either of the following:

- Notify your users that they will be prompted to download and install [IBM Aspera Connect](#), the free, lightweight client app that enables high-speed transfers between the AoC app and the user desktop. For most browsers, users must also install a browser extension on each browser they use to access Aspera on Cloud. See [Installation](#).
- Configure the [IBM Aspera HTTP Gateway](#), then attach it to Aspera on Cloud. This transfer method does not require users to download and install the Aspera Connect client.

1. Create groups to accelerate user management

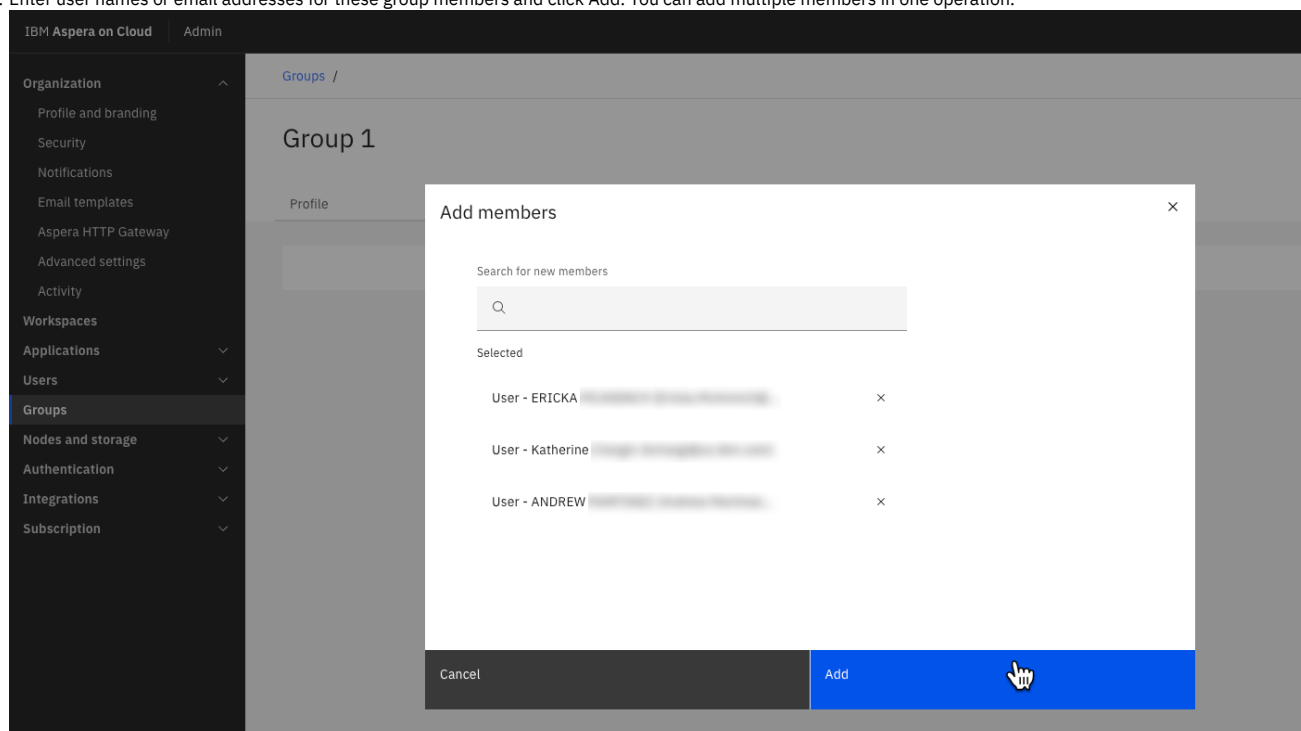
Use the AoC Admin app to create groups and add members to each group. You can add group members as follows:

- Add users who are already members of your AoC organization. You'll see their names or email addresses auto-filling in the *Add members* dialog.
- Add users who are not part of your AoC org. When you add new users to a group, you simultaneously add them as members of the organization.

1. Go to the Admin app by clicking the app switcher  and selecting Admin.
2. Go to Groups > Create new.
3. Give the group a name; for example, Group 1.
4. Click Save.

You have created the group; now add members to it.

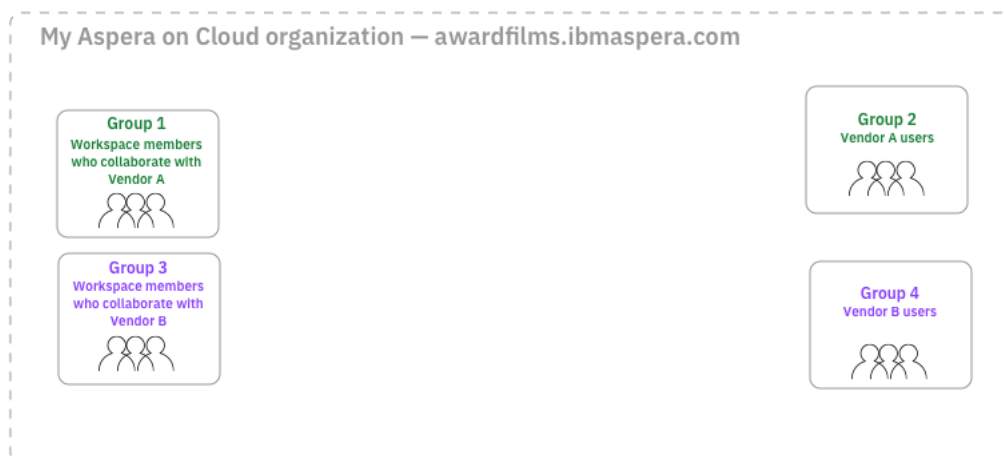
5. Click Members > Add members.
6. Enter user names or email addresses for these group members and click Add. You can add multiple members in one operation.



7. Repeat this procedure for the additional groups:

- Group 2 (external group: Vendor A users)
- Group 3 (internal users who collaborate with Vendor B)
- Group 4 (external group: Vendor B users)

After you create the four groups, your Aspera on Cloud org looks like this:



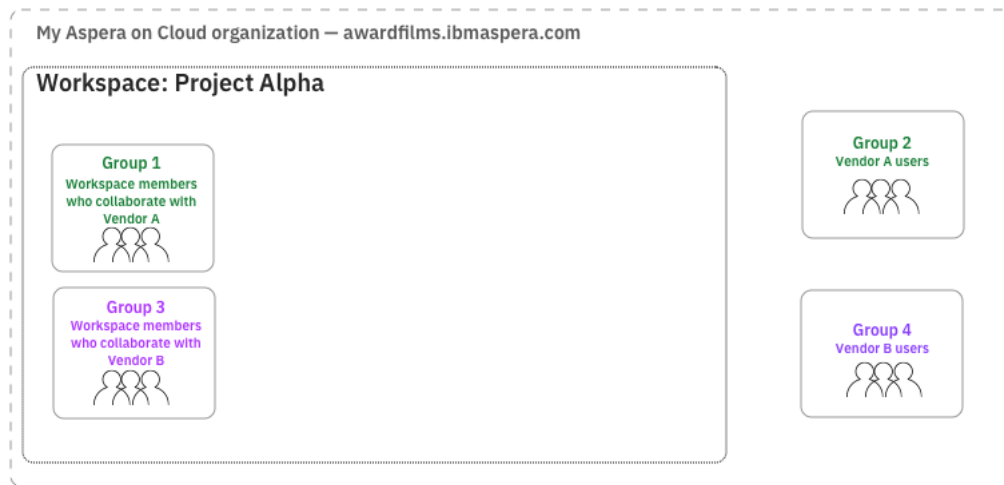
2. Configure the workspace for user collaboration

Now set up the workspace and make your internal groups workspace members.

Every AoC subscription is configured with one default [workspace](#). Aspera recommends that you rename and use your default workspace. Depending on your [subscription](#), you may be able to create a new workspace.

1. Go to **Workspaces > Default workspace**.
2. Give this workspace a name that clearly indicates its purpose; for example, Project Alpha.
3. Click Save.
4. Click Members > Add member.
5. In the Search for new members field, enter the names of your *internal* user groups; for example: Group 1, Group 3.
Note: Add yourself as a workspace member so you can verify correct workspace configuration. You can revoke your membership later if desired.
Important: Do *not* enter the names of the external groups.
These external users become [limited users](#) in your AoC org. Limited users have no access to workspace content beyond what you specifically share with them; this limited access enhances security for the content in the workspace.
6. Click Add.

You now have a workspace with your internal groups as members.



2a. Disable the Packages app in your workspace (optional)

Both the Files and Packages apps are enabled by default. This workspace uses only the Files app, so disable the Packages app. You can re-enable it at any time.

Important: Before you perform this procedure, be sure that you have [retrieved the access key for your built-in node and storage](#); the admin who created the AoC organization received the credentials in a digital package from Aspera Tech Support. You can re-enable the Packages app any time.

1. If necessary, open your new workspace: Workspaces > Project Alpha.
2. Click Applications > Packages.
3. Clear the checkbox labeled Use global app settings.
4. Clear the checkbox labeled Enable application.
5. Click Save.

3. Configure the workspace Files app for secure collaboration (optional)

In this optional procedure, you'll configure the following specific collaboration capabilities for your workspace members. If you don't need these additional controls and security, skip this procedure.

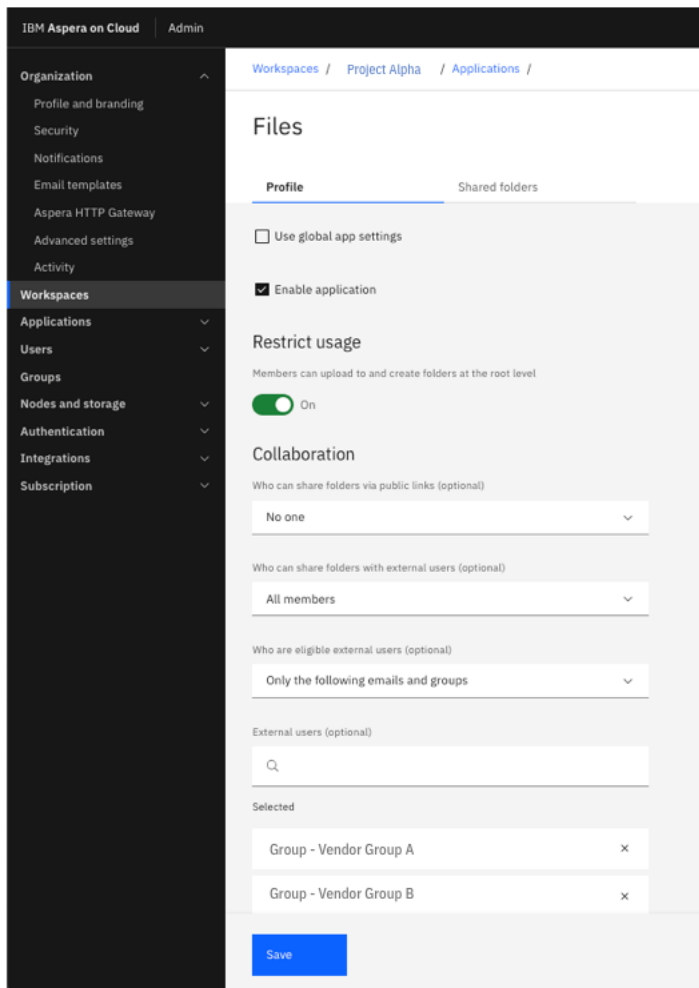
- Allow workspace members to upload content *only* into the folders you designate. This configuration makes it easy for you to monitor storage usage and transfer volume.
- Designate your external groups (Group 2 and Group 4) as the *only* external users your workspace members can share with. This configuration ensures content security.

Configure the Files app:

1. Go to Workspaces > Project Alpha > Applications > Files.
2. Clear the checkbox labeled Use global app settings.
3. In Restrict usage, click the toggle labeled Members can upload to and create folders on their home folder to On.
The home folder is the root level of the Files app. By preventing uploads to this root level, you ensure that users upload content only into the folders you create on the built-in IBM Cloud storage and share with the workspace (see Procedure 4); these are folders you can readily monitor. For details, see [Managing storage usage](#).
4. In Collaboration, do the following:
 - a. Set Who can share folders via public links to No one.
This setting prevents members from sharing folders with public users.
 - b. Set Who are eligible external users to Only the following emails and groups.
 - c. Click the Search field and enter the external vendor groups; for example, Group 2 and Group 4.

This configuration ensures that workspace members can share folders only with each other and with your two external vendor groups.

5. Click Save.

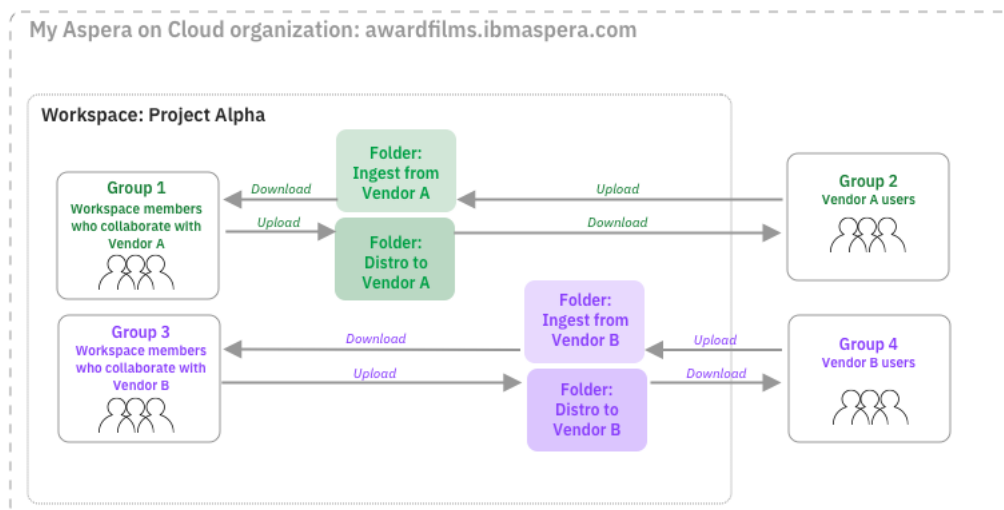


4. Create and share the collaboration folders with the groups

Now set up folders on your IBM Cloud storage and share them with your groups, giving them the spaces to collaborate in. You'll give access and the required permissions to each group. Then you can upload the desired content to the folders, or allow the users with "Upload" permission to populate the folder content.

You'll need the node secret for this procedure. To find the secret, see Important note in procedure 2a.

Recall that this is the configuration goal:



Folder permissions

As you share, you'll assign permissions to each folder based on the group and their access needs. Aspera recommends the following permissions matrix. Adjust for your own situation and goals.

Note: If you don't need to restrict user actions on content in your folders, you can leave the default permission of "Can edit" in place for all folders. In this case, you can skip this table and simplify the following procedure to omit assigning permissions. For details, see [Content permissions](#).

Folders	Permissions			
	Group 1	Group 2	Group 3	Group4
Ingest from Vendor A	• Browse • Download • Delete • Preview	• Browse • Upload files • Create directory	n/a	n/a
Distro to Vendor A	• Browse • Upload files • Create directory	• Browse • Download • Delete • Preview	n/a	n/a
Ingest from Vendor B	n/a	n/a	• Browse • Download • Delete • Preview	• Browse • Upload files • Create directory
Distro to Vendor B	n/a	n/a	• Browse • Upload files • Create directory	• Browse • Download • Delete • Preview

To create and share folders, do the following:

1. Go to Workspaces > *Project Alpha* > Applications > Files > Shared folders > Create new.
2. In the *Node access* dialog that opens, select the intended node, enter your node secret, and click Log in.
3. Create a folder for Group 1 to upload content for Group 2 to download:
 - a. In the *Choose folder to share* dialog that opens, click Create folder.
 - b. Name the folder "Distro to Vendor A", then click OK. The new folder appears in the list.
 - c. Click to select this new folder, then click Submit. This action makes the folder a shared folder.

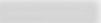
Choose folder to share

Display name (optional)

Enter the name that members see. Leave blank to use the current folder name.

Root

Create folder

	Name	↑	Size	Last updated
☐	 		—	—
☒	 Distro to Vendor A		—	—
☐	 		4 MB	1/31/19 3:45 PM

Cancel

Submit

- d.
- e.
4. Share the folder "Distro to Vendor A" with Group 1, giving your internal users permission to upload to this folder:
 - a. Click the folder row to open it, then click Add member.
 - b. Click the field that displays Can edit to display permission options.
 - c. Select permissions for Browse, Upload, Create folders. Then click off the permission list to close it. The field displays "Custom."

Permissions to "Distro to Vendor A" for Group 1 (workspace members who collaborate with Vendor A).

Add members

×

Select permissions

Custom

▼

☒ Browse
 ☐ Download
 ☒ Upload files
 ☐ Delete
 ☒ Create directory
 ☐ Rename
 ☐ Preview

Choose new members to add

🔍

Search for users or groups

Selected

Group - Group 1

×

Cancel

Add

- d.
 - e. In the field that displays Search for users or groups, enter Group 1.
 - f. Click Add.
 5. Share the folder "Distro to Vendor A" with Group 2, giving your users from Vendor A permission to download from this folder.
 - a. Click Add member.
 - b. Click the field that displays Can edit to open the permission options.
 - c. Select permissions for Browse, Download, Delete, and Preview. Then click off the permission list to close it. The field displays "Custom."
- Permissions to "Distro to Vendor A" for Group 2 (the users from Vendor A).**

Add members

×

Select permissions

Custom

▼

☒ Browse
 ☒ Download
 ☐ Upload files
 ☒ Delete
 ☐ Create directory
 ☐ Rename
 ☒ Preview

Choose new members to add

🔍

Search for users or groups

Selected

Group - Group 2

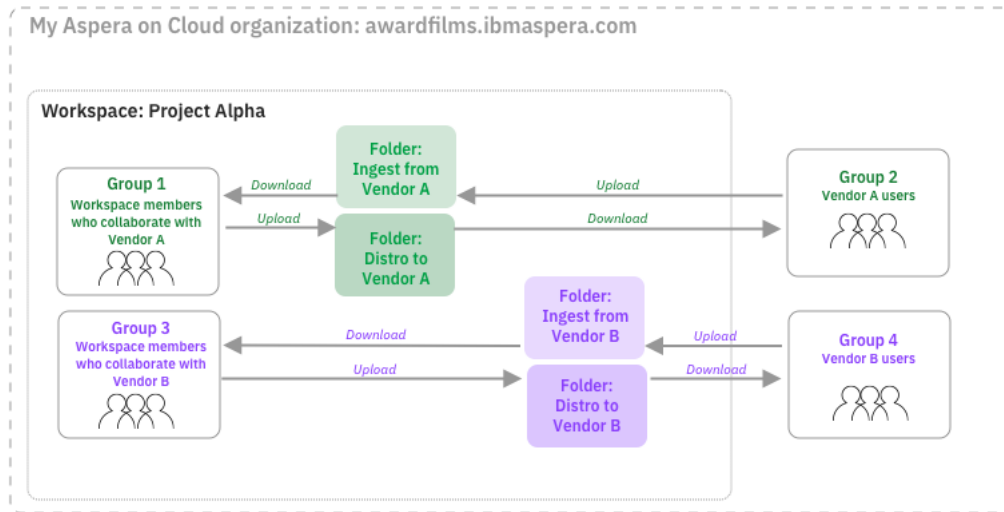
×

Cancel

Add

- d. In the field that displays Search for new members, enter Group 2.
6. Repeat the previous steps to create the folder "Ingest from Vendor A" with Group 1 and Group 2, reversing the permissions as shown in the permissions matrix.
7. Repeat these steps to create and share two more folders for collaboration with Vendor B, giving access and permissions to Group 3 and Group 4. Refer to the table in the section "Folder permissions".

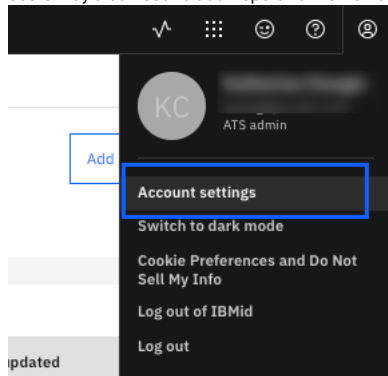
Result: Your internal and external groups can see the folders you created, and access folder content according to the permissions you assigned. Users must go to the workspace you set up in Procedure 2, and access the Files app in that workspace.



5. Configure notifications

By default, AoC sends email notifications to all users when they receive access to a shared folder. This means that the users in your internal and external groups receive an email with a link to access each folder you share.

Note: If internal users don't see the notifications, ask them to verify that they've enabled receipt of notifications in their Account Settings page. Both internal and external users may also need to add Aspera to their email contacts. See also ["Troubleshooting Email Notifications"](#).



You can also allow your internal users to configure a notification when content is added to a folder they need to monitor.

1. Go to Workspaces > Project Alpha > Notifications.
2. Click the toggle labeled Use organization settings to Off.
3. Click the toggle labeled Allow users to turn on notifications for new shared folder content to On.
4. Click Save.

Your internal users can now set notifications for themselves when new content is added to the folders they need to monitor. For a user procedure, see [Set notifications for new content in a shared folder](#).

Results

Your configuration work is done.

- Members of your internal groups are members of your org and the workspace Project Alpha. Each member of each internal group receives four email notifications.
 - The first contains a link allowing them to join the organization by logging in and creating an account.
 - The second email contains a link to join the workspace. These are *standard* users in your org.
 - The third and fourth emails contain links to the two folders you shared with them.
- In the workspace, your internal groups see two folders in their Files app. They can browse and upload content to the Distro folder, and browse, download, preview and delete content from the Ingest folder.
- Members of your external groups receive two email notifications, each with a link to one of the two folders you shared with them. When they click the link, an AoC portal opens to allow them access to the folder according to the permissions you set.
- The external group members do not see the workspace or any content beyond what has been shared with them. These are *limited* users in your org.

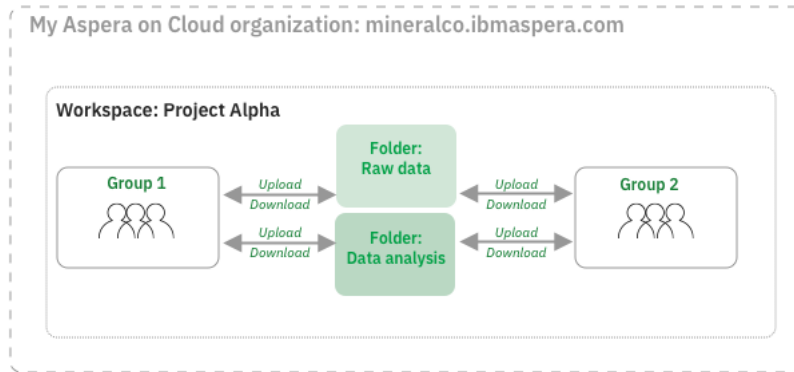
Configuration scenario: Workspace members sharing a file repository

If your team shares access to files and folders in a common repository, use this article to configure your organization. You'll use the Aspera on Cloud Files app to enable secure and permission-based sharing of folders among collaborators.

For example, perhaps your team is:

- A video production company developing a film through ideation, production, and editing.
- A team of geologists studying the feasibility of exploratory mining in a given site.
- Part of a production company sharing assets among internal teams who provide coloration, titles, or other services.

Aspera proposes a workspace like this. This setup is flexible of course, and you can adapt it for your specific needs.



Your AoC organization: Overview

Your Aspera on Cloud (AoC) organization is the primary container and administrative unit in your IBM Aspera subscription.

Customize your URL to brand your org

You can name your org and configure the subdomain of the URL that users will browse to access your org. For example, if your company name is American Mineral Company, you can choose to use the URL `mineralco.ibmaspera.com`. For details on this one-time-only configuration, see [Customize your organization URL, name, and logo](#).

Your users collaborate in a workspace

A workspace is a digital space where designated members can collaborate. Each workspace is a collection of specific users, files and folders, access permissions, and collaboration rules. The users, files, and folders in one workspace are completely separate from those in another workspace. You'll configure a workspace in Procedure 2 below.

Users in a given workspace can collaborate freely with other members of the same workspace. By default, workspace members can also collaborate with users outside the workspace. But the admin can restrict that privilege if necessary; see Procedure 3 below.

Your files and folders are in IBM Cloud storage

Each Aspera on Cloud subscription includes one built-in, [Aspera-managed auto-scale transfer cluster](#) attached to storage in IBM Cloud.

This Aspera transfer cluster (also called ATS, Aspera transfer service; sometimes called a *node*) is the engine that AoC uses to upload and download your files and folders to and from your built-in IBM Cloud storage. ATS is hosted and managed by IBM Aspera.

The built-in IBM Cloud storage hosts your organization workspace, including the content your users upload and share using the Files app. As an admin, you can also upload content directly to this storage and then make that content available to your users. (Storage capacity depends on your AoC subscription tier.) See procedure 4 below.

The access credentials (access key and secret) for this transfer cluster and storage are delivered to the administrator who first created the AoC organization. You should see [Secure the access credentials for your built-in node](#) retrieve and securely store the access credentials; they allow you to access and manage your IBM Cloud storage.

Note: If desired, you can attach your own local or cloud storage to Aspera on Cloud and then share storage contents with workspace users, but that process is not covered in this document; see articles in the Nodes section of this Help Center.

- To attach your existing cloud storage to AoC, see [Attach your existing cloud storage](#).
- To attach your own Aspera HSTS server, see [Tether Your Aspera Transfer Server to Aspera on Cloud](#).

Process overview

These are the high-level steps required to configure the scenario shown in the graphic in the opening section of this article; detailed procedures follow. Adapt as needed for your own requirements.

Use the AoC Admin app to:

1. Create groups of users to simplify and accelerate user management.
2. Configure the workspace in which your groups will collaborate. Add your user groups as workspace members.
3. (Optional) Configure the Files app to allow your workspace members to collaborate only within the workspace. This configuration is by no means required, but it allows you greater control over access to your proprietary assets.

4. In your built-in IBM Cloud storage, create the folders in which your groups will collaborate; share the folders with your groups, assigning specific permissions to allow access while preserving content security.
5. (Optional) Configure notifications to alert internal users when new content appears in their folders.

Important: As an admin, you must provide a transfer method for your users. You can do either of the following:

- Notify your users that they will be prompted to download and install [IBM Aspera Connect](#), the free, lightweight client app that enables high-speed transfers between the AoC app and the user desktop. For most browsers, users must also install a browser extension on each browser they use to access Aspera on Cloud. See [Installation](#).
- Configure the [IBM Aspera HTTP Gateway](#), then attach it to Aspera on Cloud. This transfer method does not require users to download and install the Aspera Connect client.

1. Create groups to accelerate user management

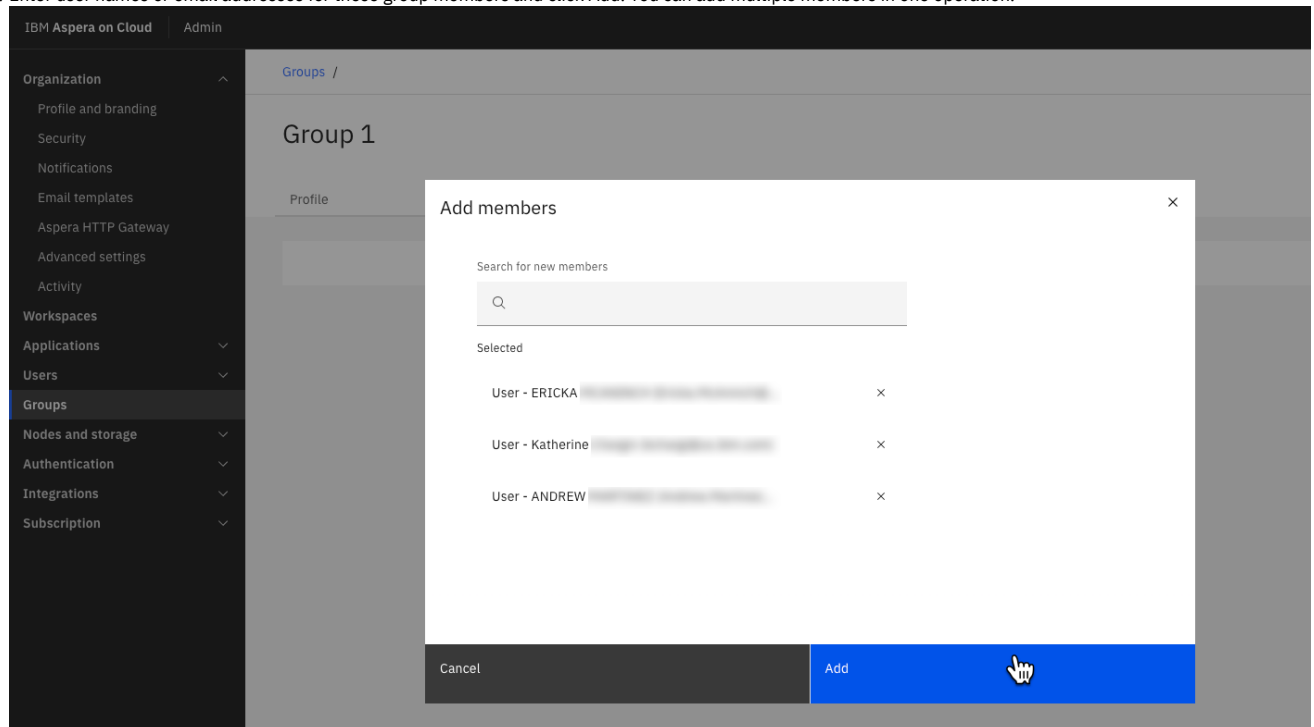
Use the AoC Admin app to create groups and add members to each group. You can add group members as follows:

- Add users who are already members of your AoC organization. You'll see their names or email addresses auto-filling in the *Add members* dialog.
- Add users who are not part of your AoC org. When you add new users to a group, you simultaneously add them as members of the organization.

1. Go to the Admin app by clicking the app switcher and selecting Admin.
2. Go to Groups > Create new.
3. Give the group a name; for example, Group 1.
4. Click Save.

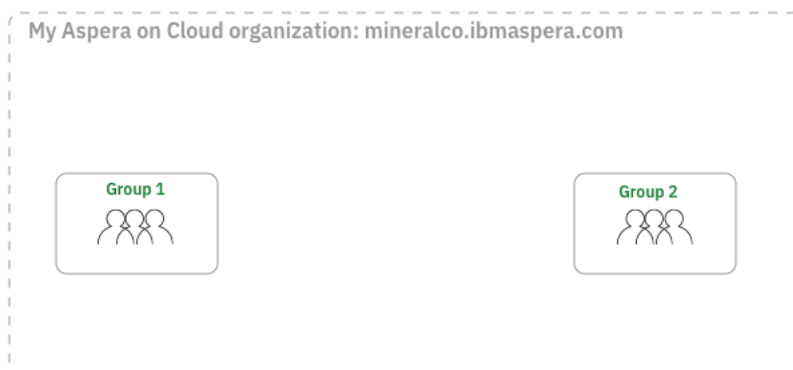
You have created the group; now add members to it.

5. Click Members > Add members.
6. Enter user names or email addresses for these group members and click Add. You can add multiple members in one operation.



7. Repeat this procedure for Group 2 (other internal users who collaborate with Group 1)

After you create the two groups, your Aspera on Cloud org looks like this:



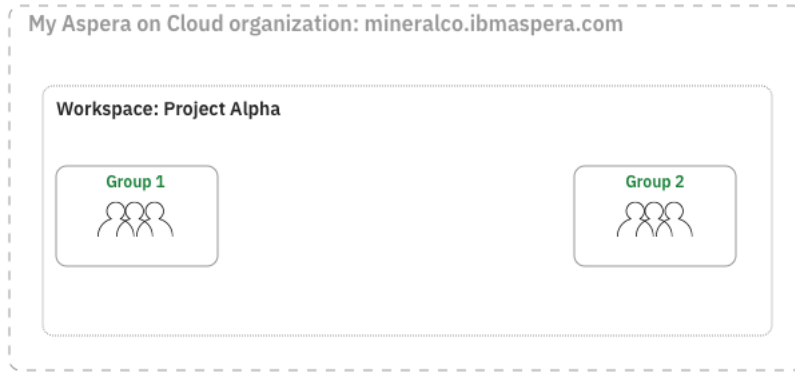
2. Configure the workspace for collaboration

Now set up the workspace and add your groups as members of the workspace.

Every AoC subscription is configured with one default [workspace](#). Aspera recommends that you rename and use your default workspace. (Depending on your [subscription](#), you may be able to create a new workspace).

1. Go to **Workspaces > Default workspace**.
2. Give this workspace a name that clearly indicates its purpose; for example, Project Alpha.
3. Click Save.
4. Click Members > Add member.
5. In the Search for new members field, enter the names of your user groups.
Note: Add yourself as a workspace member so you can verify correct workspace configuration. You can revoke your membership later if desired.
6. Click Add.

You now have a workspace with your groups as members.



2a. Disable the Packages app in your workspace (optional)

Both the Files and Packages apps are enabled by default. This workspace uses only the Files app, so disable the Packages app. You can re-enable it at any time.

Important: Before you perform this procedure, be sure that you have [retrieved the access key for your built-in node](#) and storage; the admin who created the AoC organization received the credentials in a digital package from Aspera Tech Support. You can re-enable the Packages app any time.

1. If necessary, open your new workspace: Workspaces > Project Alpha.
2. Click Applications > Packages.
3. Clear the checkbox labeled Use global app settings.
4. Clear the checkbox labeled Enable application.
5. Click Save.

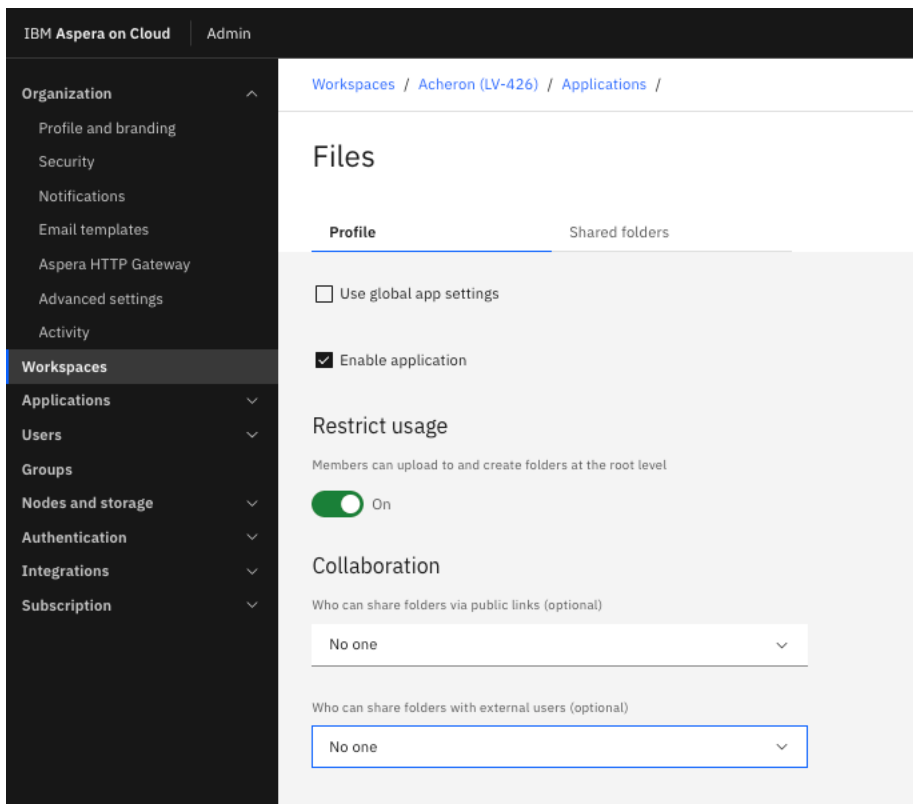
3. Configure the workspace Files app for secure collaboration (optional)

In this optional procedure, you'll configure the following specific collaboration capabilities for your workspace members. If you don't need these additional controls and security, skip this procedure.

- Allow workspace members to upload content *only* into the folders you designate. This configuration makes it easy for you to monitor storage usage and transfer volume.
- Restrict sharing to workspace members only. This means that workspace members can share with other members of the workspace only; they cannot share with anyone outside the workspace or outside the AoC organization.

Configure the Files app:

1. Go to Workspaces > Project Alpha > Applications > Files.
2. In Custom application settings, clear the checkbox labeled Use global app settings.
3. In Restrict usage, click the toggle labeled Members cannot upload to or create folders on their home folder to On.
The home folder is the root level of the Files app. By preventing uploads to this root level, you ensure that users upload content only into the folders you create on the built-in IBM Cloud storage and share with the workspace (see Procedure 4); these are folders you can readily monitor. For details, see [Managing storage usage](#).
4. In Collaboration, do the following:
 - a. Set Who can share folders via public links to No one.
This setting prevents members from sending a public link to share folders with people outside the workspace or organization.
 - b. Set Who can share folders with external users to No one.
This setting ensure that members can share only with each other.
5. Click Save.

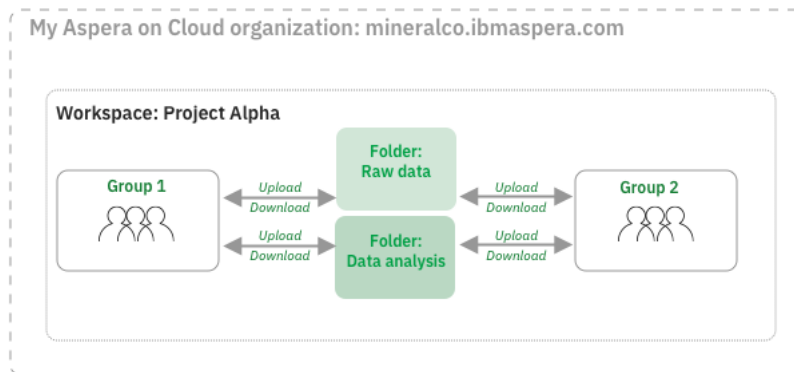


4. Create and share the collaboration folders with the groups

Now set up folders on your IBM Cloud storage and share them with your groups, giving them the spaces to collaborate in. You'll give access and the required permissions to each group. Then you can upload the desired content to the folders, or allow the users with "Upload" permission to populate the folder content.

You'll need the node secret for this procedure. To find the secret, see Important note in procedure 2a.

Recall that this is the configuration goal:



To create and share folders, do the following:

1. Go to Workspaces > *Project Alpha* > Applications > Files > Shared folders > Create new.
2. In the *Node access* dialog that opens, select the intended node, enter your node secret, and click Log in.
3. Create the first folder for your groups to collaborate in:
 - a. In the *Choose folder to share* dialog that opens, click Create folder.
 - b. Name the folder "Raw data", then click OK. The new folder appears in the list.
 - c. Click to select this new folder, then click Submit. This action makes the folder a shared folder.

Choose folder to share ×

Display name (optional)

Enter the name that members see. Leave blank to use the current folder name.

Root

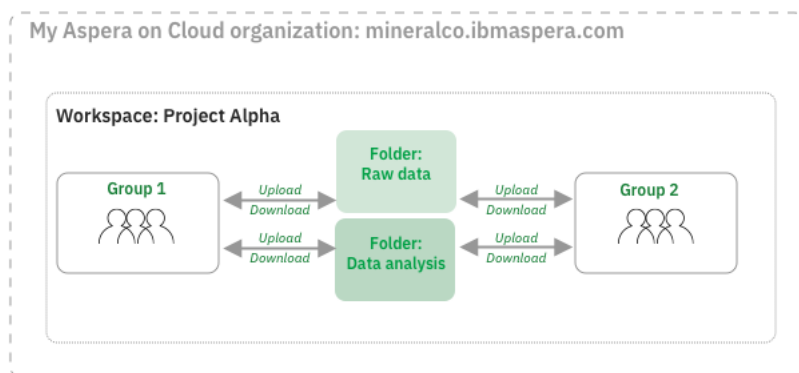
Create folder

	Name	Size	Last updated
☐		—	—
☒	Raw data	—	—
☐		4 MB	1/31/19 3:45 PM

Cancel
Submit

4. Share the folder "Raw data" with Group 1 and Group 2, giving both user groups Edit permission to this folder:
 - a. Click the folder row to open it, then click Add member.
 - b. In the field that displays Search for new members, enter Group 1 and Group 2.
The default permission setting is **Can edit**. This permission allows members full access to folder contents, including **Delete**. Click **Custom** to apply only specific permission.
 - c. Click Add.
5. Repeat the previous steps to create the folder "Data analysis", then add Group 1 and Group 2 as members with **Can edit** permission.

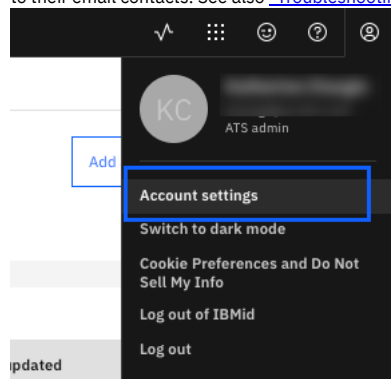
When you complete this procedure, your users can see the folders you created and can access folder content according to the permissions you assigned. Users must go to the workspace you set up in Procedure 2, and access the Files app in that workspace.



5. Configure notifications (optional)

By default, AoC sends email notifications to all users when they receive access to a shared folder. This means that the users in your groups receive an email with a link to access each folder you share.

Note: If users don't see the notifications, ask them to verify that they've enabled receipt of notifications in their Account settings page. They may also need to add Aspera to their email contacts. See also "[Troubleshooting Email Notifications](#)".



You can also allow your users to configure a notification when content is added to a folder they need to monitor.

1. Go to Workspaces > Project Alpha > Notifications.
2. Click the toggle labeled Use organization settings to Off.

3. Click the toggle labeled Allow users to turn on notifications for new shared folder content to On.
4. Click Save.

Your users can now set notifications for themselves when new content is added to the folders they need to monitor. For a user procedure, see .

Results

Your configuration work is done.

- Your groups are members of your org and the workspace Project Alpha. Each member receives four email notifications.
 - The first contains a link allowing them to join the organization by logging in and creating an account.
 - The second email contains a link to join the workspace. These are *standard* users in your org.
 - The third and fourth emails contain links to the two folders you shared with them.
- In the workspace, your groups see and can access the two folders you created in their Files app.

Troubleshooting: Sharing files and folders

Solve problems with shared folder access. Investigate and fix improper access issues in the Files app.

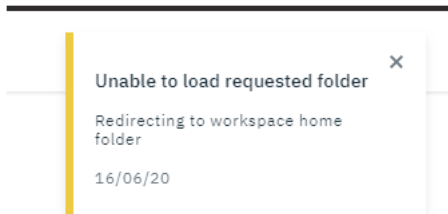
- [Can't access a shared folder](#)
Use this procedure when you can see a shared folder in your Files app but cannot access it.
- [User still has access to unshared folder](#)
If you've unshared a folder to remove access from a specific user, but that user can still access the folder, use this article.

Can't access a shared folder

Use this procedure when you can see a shared folder in your Files app but cannot access it.

If instead your shared folder issue is that you have 'unshared' a folder with a user but the user still has access, see [User still has access to unshared folder](#).

On rare occasions, you may see the error message "Unable to load requested folder" when you try to access a folder that has been shared with you:



When you try to access a folder but the folder is not available, AoC redirects you to the Files app home folder in that workspace. Your home folder is the top level of your Files application in that workspace. If you are a member of the Files app in multiple workspaces, you have a home folder in each workspace.

If you are the person who can't access a folder that you can see, do the following:

1. In your own Files app, check your permissions on the folder (right-click folder row, select Info); do you have the expected access permission?
2. Check with the folder owner that the shared folder still exists. The person who shared is listed in subtext on the row of the shared folder.

☐		Export		0 B
☐		ey		10 MB
		Shared by an admin to this workspace		1 file
☐		Files for Check Out		750 MB
		Shared by [redacted] to you		1,176 files, 363 folders

3. Ask the folder owner to verify that you are in the list of folder collaborators and that you have the proper access permissions.
The folder owner can click the folder row in their own Files app to display the folder details and collaborators panel. If your name is not there, ask the folder owner to share with you again, being sure to select the desired permissions for you.
4. Contact your local tech support administrator. Click  in the banner and select "Technical support". Provide the URL of the affected folder.

User still has access to unshared folder

If you've unshared a folder to remove access from a specific user, but that user can still access the folder, use this article.

You can share folders with individual users, with groups, and with entire workspaces. Any given user may have access to a shared folder directly, or may have access through a group or workspace that has shared access.

If you unshared a folder with an individual but that user still has access, you may have to remove the user from a group that has access. For details, see [Direct and inherited memberships](#). Contact your admin to change group membership.

Activity app: Monitor events, activity, and usage in your organization

The AoC Activity app gives detailed insight into activity and usage in your Aspera on Cloud organization. Learn how to monitor transfer activity, volume usage, and application events. Create detailed reports to export or download. Customers can ingest Activity API events like application and security events, volume usage and transfer details into their analytics tool of choice.

- [Overview](#)
A general overview of the Activity App available information.
- [Enabling the Activity app and adding members](#)
An administrator must enable the Activity app for your Aspera on Cloud organization. Once the app is enabled, the admin must grant access to specific users by making them members of the Activity app.
- [Aspera Activity App API](#)
The Activity App allows you to track transfer activity and volume. The Activity API returns data on Aspera objects related to performance, history, and usage of file transfers in Aspera on Cloud.
- [Architecture and components of the activity app](#)
The Activity app in Aspera on Cloud (AoC) shows app events and the performance, history, and usage for file transfers. Activity's responsive engine streams log data to the web application, generating interactive visualizations of real-time and historical data.
- [Reporting activity and usage](#)
You can download reports of your filtered results in CSV format. Depending on your Aspera on Cloud edition, you can export a report or you can generate an asynchronous report.
- [Data retention](#)
This article describes data retention and deletion strategies for the Activity app.
- [Monitoring](#)
Learn how to monitor transfer activity, bandwidth and volume usage, file access and application events.
- [Use cases](#)
Example use cases for the Aspera Activity app.

Overview

A general overview of the Activity App available information.

To enable the Activity app in your organization, see [Enabling the Activity app and adding members](#). Once enabled, you can add members to the app, who can then access Activity using the app switcher .

The Transfer activity page displays real-time and historical transfer data for your organization. It includes context for a given transfer, such as the time of the transfer and whether it completed or failed. You can also review performance data for the resources (workspaces, nodes, and users) associated with your workspace. This can help you identify issues in the system; for example, an inactive server may need to be evaluated for connectivity issues.

The Volume usage page displays historical usage and associated data for workspaces and nodes. This information can help you evaluate the effectiveness of resource usage.

The Application events page displays data for all app events, filterable by event type (such as user login or file creation), user, and time.

Enabling the Activity app and adding members

An administrator must enable the Activity app for your Aspera on Cloud organization. Once the app is enabled, the admin must grant access to specific users by making them members of the Activity app.

Prerequisites

To use the Activity app, fulfill the requirements listed here.

- Enable the Activity app for your organization. See [Enabling the Activity app and adding members](#).
- Add members to the Activity app.
- If you have a *tethered node* (a user-managed IBM Aspera High-Speed Transfer Server that is connected to Aspera on Cloud), review [Configure monitoring and metering for your tethered node](#) to ensure the tethered node is configured properly to send transfer data to Activity.

To enable the Activity app, do the following:

1. Go to Admin > Applications > Activity.
2. Select Enable application, then click Save.
3. Add members to the Activity app. Before a user (including yourself) can use the Activity app, you must make them a member of the app.
Note: Add only trusted users as members since all Activity app members, including non-admin members, can view all available data for your organization without restrictions.
 - a. Click Members > Add members.
 - b. Enter the user name or email, then click Add.
Note: If the full user name does not appear, that user is not yet a member in the organization. [Add the user](#) to the organization.The Activity app is now enabled for your organization and available through the app switcher  to the members you added.

Aspera Activity App API

The Activity App allows you to track transfer activity and volume. The Activity API returns data on Aspera objects related to performance, history, and usage of file transfers in Aspera on Cloud.

IBM Developer (API Hub)

You can find reference information and developer guides for the [Aspera Activity App API](#) inside the IBM API Hub.

Available endpoints

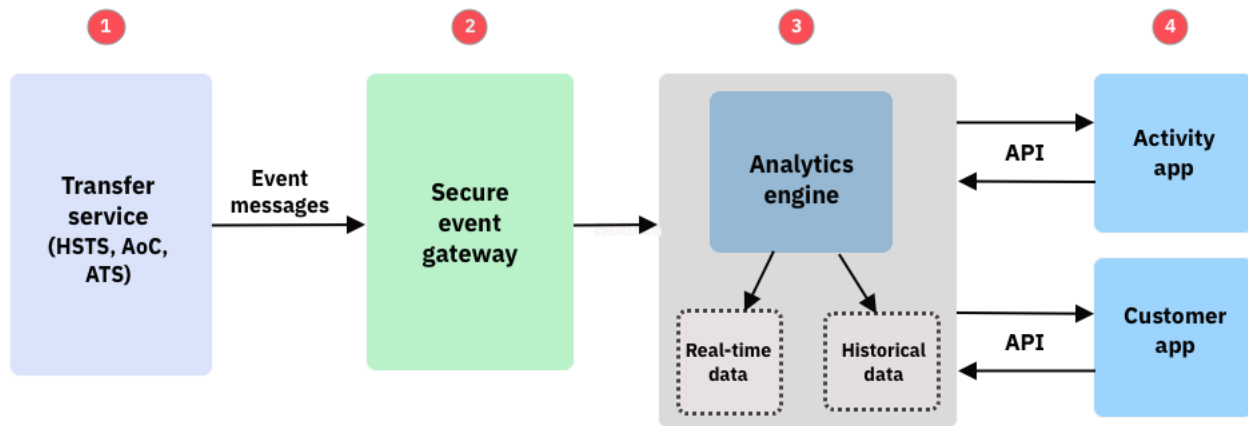
This section provides a list of available endpoints for the Aspera Activity API. Each one contains a description, parameters, request, responses, and the ability to try each one of them from the current page you are viewing.

- **Transfers**
 - [Get an array of all transfers](#)
 - [Get a CSV file with all transfers](#)
 - [Get data for a specific transfer](#)
 - [Get data for a specific multisession transfer](#)
- **Transfer rates and volume usage**
 - [Get the data transfer rate for downloads](#)
 - [Get the data transfer rate for uploads](#)
 - [Get the transfer usage of uploads and downloads](#)
 - [Get a CSV file with transfer usage of uploads and downloads](#)
- **Application events**
 - [Get data for events in Aspera on Cloud](#)
 - [Get a CSV file with data for events in Aspera on Cloud](#)

Architecture and components of the activity app

The Activity app in Aspera on Cloud (AoC) shows app events and the performance, history, and usage for file transfers. Activity's responsive engine streams log data to the web application, generating interactive visualizations of real-time and historical data.

Architecture and components



1. Each time a user performs an action on the transfer service*, such as logging in, sending a file, or creating a user, the service produces a corresponding event.
2. The secure event gateway authenticates each activity message, adds the message to a queue, and then routes the message to the analytics engine.
3. The analytics engine receives the event message in the database for real-time data, then sends the events to the database for historical data.
4. Using the Activity API, the Activity app requests both real-time and historical data to display in the Activity app UI. Alternatively, an external application uses the Activity API to request real-time and historical data.

Note: The version of an Aspera High-Speed Transfer Server must be v. 3.9.3 or later. IBM Aspera recommends that you always use the latest version server software.

Reporting activity and usage

You can download reports of your filtered results in CSV format. Depending on your Aspera on Cloud edition, you can export a report or you can generate an asynchronous report.

Export reports

If you subscribe to the Aspera on Cloud Essentials edition, you can export a report. Exported reports can have up to approximately 100,000 records. The oldest records beyond this limit may not be included. For larger data sets, use the custom Start date and End date filters to export multiple reports with shorter time frames.

Note that exporting a large report may take some time. Once the export process completes, the compressed archive (.zip) appears in the download location you select when you export.

1. In the top-right corner of the page, click Export.
2. Name your report (`report_name.zip`) and click Export.
3. Select the location for the report download. The downloaded ZIP file contains one or more CSV files, depending on your filtering.

Enable and generate asynchronous reports

If you subscribe to the Standard Plus or Premium edition, your organization administrator can enable you to generate reports that are stored in a shared space in the Activity app. Then you can generate reports of any size. Report generation is asynchronous, so you are free to attend to other tasks even during extended processing times. When the report is available, you can view it on the Stored reports page in the Activity app.

If you are an org admin, enable stored reports for your organization as follows:

1. Go to Admin > Applications > Activity.
2. Check the box labeled Enable stored reports.
3. In the field that displays, select the location to store these reports.
Select any attached node. The default path for Activity reports is `/Activity reports`. If desired, select a different path; Aspera on Cloud creates a folder called "Activity reports" in the location you select. The reports generated by all Activity app users are stored in this "Activity reports" folder.
4. Click Save.
If you change this location, reports in the original location may be inaccessible through the Stored reports page. To troubleshoot, see [Stored report not available in Activity app](#).

To generate a stored report, do the following:

1. On any page in the Activity app, click Export.
2. Name the report and click Export. When the report is available, Aspera on Cloud displays a toast notification.
3. To view the report, go to Stored reports. This page displays reports generated by all users.
4. To download or get information on any report, right-click the report row and select from the menu.
5. If desired, use the filter to display all reports or only the reports that you generated. You can also filter for report type.

Data retention

This article describes data retention and deletion strategies for the Activity app.

The Activity app retains all activity data for the lifetime of the app (currently 2+ years), and all historical activity data for an individual organization.

Aspera on Cloud retains these attributes for a file transfer:

- Organization
- User's workspace
- Data package name
- Sender user's ID
- Receiver user's ID
- File ID
- Filename
- File size
- File transfer timestamp
- File transfer source IP address
- Server IP address
- Transfer size
- Transfer rate

IBM Aspera on Cloud deletes all Personally Identifiable Information (PII) from the backend databases no more than 60 days after the end of the organization's subscription.

Users can query the data as far back in time as needed. Each query returns a maximum of 6 months of data.

Monitoring

Learn how to monitor transfer activity, bandwidth and volume usage, file access and application events.

- [Monitor bandwidth usage](#)
Use the Transfer activity page to monitor transfer activity for your entire organization or filtered by each component of the transfer system: nodes, access keys, workspaces, and users. You can zoom in to data based on configurable time spans (reported in UTC).
- [Monitor volume usage](#)
Use the Volume usage page to monitor transfer volume for your entire organization or filtered by each component of the transfer system: entitlements, nodes, access keys, workspaces, and users. You can zoom in to data based on configurable time spans (reported in UTC).
- [Monitor application events](#)
Get insights into events throughout your Aspera on Cloud application, including user creation or deletion; file activity, folder sharing events, and more. Also filter for admin-specific events like security setting changes.

Monitor bandwidth usage

Use the Transfer activity page to monitor transfer activity for your entire organization or filtered by each component of the transfer system: nodes, access keys, workspaces, and users. You can zoom in to data based on configurable time spans (reported in UTC).

To open this page in the Activity app, click Transfer activity in the left navigation menu.

Review your transfer bandwidth over time

The top-level panel displays aggregate bandwidth data for the selected time period, with the most recent transfers displaying at the far right portion of the graph. The data is separated into lines for transfer throughput by sender (blue line) and receiver (green line). Breaks in the line represent periods of inactivity, during which no transfers occur.

The graph is interactive. You can hover over a point in time on the graph to see:

- Overall transfer performance, in Mbps. Hover over the blue and green lines (download rate and upload rate, respectively).
- The reason for a failure or error. Hover over one of the red dots on the graph.

Near the graph, find upload and download data for the following:

- Average rate
- Peak (aggregate) rate
- Current rate

You will also see data for:

- Total transfers for the selected time period
- Number of current transfers
- Number of failed transfers

Filter to find specific transfer data

Depending on the entity you selected for the filtering options, data tables display the send and receive throughput for active workspaces, nodes, and users.

- The default, unfiltered view displays transfer activity tables for each node, workspace, and user.
- Filter by a specific node to display data tables for each associated workspace and user.
- Filter by a specific workspace to display tables for each associated node and user.
- Filter by a specific user to display tables for each associated node and workspace.

The term *Trusted source* in a table refers to a transfer client or some other source that is not a workspace or a human user.

The term *Public link* in a column means that the transfer occurred through a public link sent to user. Since the link is public, the user identity can't be determined.

Transfers table

At the bottom of the page, you can filter the Transfers table by transfer status: active, failed, and completed transfers.

Each transfer event is identified by its source application in Aspera on Cloud:

- **Package sent** - Package uploaded from the Packages app
- **Package download** - Package downloaded to the Packages app
- **File upload** - File uploaded from the Files app
- **File download** - File downloaded from the Files app
- **Node to node** - File moved or copied from one transfer server to another using the Files app

Click the table row for a transfer event to open the **Event** panel and get key transfer session details, such as the user who initiated the transfer, the file or package size, and the transfer rate.

Multisession transfers

If any transfer events have the multisession icon () next to it, the transfer was initiated from the command line with the multisession feature. The Event details panel for a multisession transfer includes the session ID and status for each part of the multisession transfer.

Note: If one part of a multisession transfer fails, the entire transfer fails.

To learn more about multisession transfers, see the [High Speed Transfer Server Admin Guide](#).

Monitor volume usage

Use the Volume usage page to monitor transfer volume for your entire organization or filtered by each component of the transfer system: entitlements, nodes, access keys, workspaces, and users. You can zoom in to data based on configurable time spans (reported in UTC).

To open this page in the Activity app, click Volume usage in the left navigation menu.

Review your volume usage over time

The graph displays aggregate volume data for the selected time period, with the most recent usage displaying at the far right portion of the graph. The data is separated into data uploaded and data downloaded.

The graph is interactive. You can hover over any bar on the graph to see upload and download values for that point in time.

Filter to find specific transfer data

Filter as required for volume usage by node, access key, workspace, user, entitlement, and time period. The interactive graph and data tables display the relevant data.

The term *Trusted source* in a table refers to a transfer client or some other source that is not a workspace or a human user.

The term *Public link* in a column means that the transfer occurred through a public link sent to user. Since the link is public, the user identity can't be determined.

Monitor application events

Get insights into events throughout your Aspera on Cloud application, including user creation or deletion; file activity, folder sharing events, and more. Also filter for admin-specific events like security setting changes.

Events available for monitoring

You can monitor these events:

- Admin events (see "Admin-specific events", for more details)
- Log in, log out
- Workspace created/deleted
- Workspace membership created/deleted
- User created/deleted
- Package sent/received/downloaded
- File uploaded/downloaded/moved/renamed/deleted
- Folder shared, folder shared via a public link, folder copied/ renamed/, folder deleted
- User left the shared folder
- Shared Inbox events:
 - - Created a Shared Inbox
 - Deleted a Shared Inbox
 - User has been added to a Shared Inbox
 - User has been removed from a Shared Inbox
 - Shared Inbox user permissions edited
- Shared folder events:
 - - Revoked user from a shared folder
 - Shared folder permissions modified

Admin-specific events

When you select **Admin events** for the event type, the Activity app returns a list of all events that occur in the Admin app of Aspera on Cloud, such as when an admin user:

- Gives another user admin privileges.
- Edits a security setting in a workspace or app.
- Enables or disables one of the available apps.

Field name	Description	Example
Event	Description of the event. For example, an admin added a user or updated a configuration in the UI.	Updated "inherit email notification settings"
Previous event value	Previous value of the field for the UI element.	true
Current event value	Current value of the field for the UI element.	false
Application	AoC application where the event occurred.	Admin
Event location	The menu navigation to the page where the event occurred ("click this, then click this").	Workspace > Shared inbox
Initiated by	Name of the user who initiated the event	Jill Lee <jlee@ln.ibm.com>
Workspace	Workspace where the event occurred	Marketing
Date	Date of the event	Jul 27, 2020, 1:51:05 AM

For any field which is not applicable to an event, Activity will return "--" for the field. For example, an event that creates a new organization ID will not have a value for Previous event value.

Filtering events data

In the first field, select the desired event type, whether All events, or a specific event, such as Log in.

In the second field, select a time range, either a preset option or a custom option (note that all times are in UTC):

- For a preset option, select the range of time past—from a minimum of 15 minutes to a maximum of one month.
- To select a custom time range, click Custom and enter the start date and stop date. The start date can be as far back as you wish. The stop date is a maximum of 6 months after the start date you enter.

To further refine your results, enter a username or workspace name in the Filter search box.

A table with your search results appears.

Category	Description
Events	Event, such as "Created User" or "Received Package"
User	Username of the user initiating the event
Workspace	Name of the workspace for the user
Date	Date the event occurred

The term *Trusted source* in a column refers to a transfer client or some other source that is not a workspace or a human user.

The term *Public link* in a column means that the file access occurred through a public link sent to user. Since the link is public, the user identify can't be determined.

Use cases

Example use cases for the Aspera Activity app.

- [Example use cases for monitoring transfer activity](#)
For billing and monitoring purposes, get insights into transfer activity that accrues to your subscription. Remember that some transfer activity may not occur through Aspera on Cloud, depending on your subscription.
- [Example use cases for monitoring volume usage](#)
For billing and monitoring purposes, get insights into volume usage that accrues to your subscription. Remember that some volume usage may not occur through Aspera on Cloud, depending on your subscription.
- [Example use cases for monitoring file access](#)
For security and monitoring purposes, get insights into file access in your subscription.
- [Example use cases for monitoring application events](#)
For security and monitoring purposes, get insights into application events in your subscription.

Example use cases for monitoring transfer activity

For billing and monitoring purposes, get insights into transfer activity that accrues to your subscription. Remember that some transfer activity may not occur through Aspera on Cloud, depending on your subscription.

How do I find the public link associated with a transfer?

You must be an organization admin to complete this procedure.

The Details panel for each public link transfer event includes the URL token for both standard-form and short/personalized-form links. Having both tokens means that you can find and manage the link even if the Admin has reset the URL style since the link was issued. Both tokens refer to the same link, and you can find one token or the other as you manage public links in the Files or Packages apps.

1. Go to **Activity > Transfer activity**.
2. In the Transfers table, click the row of the transfer that lists "Public link" in the Started by column to open the Event details panel.
3. Check the Event field:
 - a. A file or folder event (for example, "File upload" means the link was sent from the Files app.
 - b. A package event (for example, "Package sent") means the link was sent from the Packages app.
4. Note the links and tokens:
 - a. In the Started by or From field, note the public link. This is the link that the user sent.
 - b. In the Tokens fields, note the Standard and Short/personalized tokens. These tokens are different forms of the same public link in the Started by or From field.
 - c. If you configured the Files and Packages apps to use personalized URL formats with the link sender's name (best practice), you can readily see who sent the public link. You cannot tell who used the public link to transfer.
5. Note the workspace.
6. To search for the link in the Files app, do the following:
 - a. In the Files app, go to the workspace listed in the Activity transfer Event details panel. Click a shared folder to open the folder Details panel.
 - b. Below the list of collaborators, click Manage all links.
 - c. In the public links listing, look for one of the tokens you noted in the Activity app Details panel.
7. To find the link from the Packages app, do the following:
 - a. In the Details panel, note the recipient in the To field. If this is a shared inbox, go to the Packages app and enter the shared inbox.
 - b. In the right panel below the list of members, click Manage all links.
 - c. In the Public link section, locate any of the link tokens you noted in the Activity app.

Is someone using an excessive amount of bandwidth?

1. Go to **Activity > Transfer activity**.
2. Click the filter marked **All**, and select **User**.
3. In the search box, enter a user name and click the name when it appears in the list.
4. Click the time filter and select a time range.
5. In the graph, examine upload and downloads for that user. In the tables below, you can see a breakdown of the bandwidth for the resources (workspaces and nodes) used by that user.

How can I diagnose the problem with a failed transfer?

1. Go to **Activity > Transfer activity**.
2. Find the failed transfer: filter by date, workspace, user, or other data, depending on the initial information you have.
3. In the table, check the Event column to determine the [transfer type](#).
The table represents an *upload* or *download* on a single line. A *node-to-node* transfer occupies two lines in the table; Activity app reports both directions of a node-to-node transfer.
4. In the Status column, hover over the Status field to display the error message.

Example: Upload

- The transfer type listed in the Event column is confirmed by the Node, Direction, and Peer columns as follows: The node "tor04_node" received the transfer from a peer with the IP address listed. Presumably the peer is the local computer of the user listed in the Started by column.

- In the Status column, click the error.
- Search the user documentation for the error label "[Session data transfer timeout](#)".

Example: Node-to-Node Transfer

- The two rows show the two directions of the same node-to-node transfer.
- Check the Node and Peer columns. Since node and peer are the same ("aejd2"), the transfer was from one location on the node aejd2 to a different location on the same node aejd2.
- In the error message displayed in the screenshot, the text states that it was the client that reset the connection. Since this message displays at the IP address 127.0.1.1, we can see that the client is at IP 127.0.0.1. So the client is initiating a transfer from the server at 127.0.1.1.
- Search the web for the error "Connection reset by peer". In most cases, this error means that the remote end of the transfer dropped the TCP connection without the expected state transition. A first course of action would be to retry the transfer.

Which packages on a particular node have failed in the last day?

1. Next to **Bandwidth usage by**, select Node from the menu.
2. From the **Choose Node** menu, select the desired node, then from the **in** menu, select "Last 1 day".
3. Scroll down to the bottom panel and click Failed.
4. You can now examine the list of failed transfers of type, "Package". Click a transfer row to view event details.

Example use cases for monitoring volume usage

For billing and monitoring purposes, get insights into volume usage that accrues to your subscription. Remember that some volume usage may not occur through Aspera on Cloud, depending on your subscription.

How can I see usage for each of my subscription entitlements?

Your subscription may contain multiple entitlements. To see usage per entitlement, do the following:

1. Go to **Activity > Transfer activity**.
2. Filter for **Entitlement ID**.
3. Enter at least three consecutive characters of your entitlement ID.
4. Review the results, displayed by Node and by Access key in that entitlement.

How can I find usage data for a specific shared inbox?

1. Go to **Activity > Volume usage**.
2. Filter for the workspace that contains the shared inbox.
3. In the new filter box that appears, enter the name of the shared inbox. Enter at least three characters to begin filtering.
The results include usage by Node and by User for the time period and shared inbox.

Which departments (workspaces) are transferring the most data?

1. Go to **Activity > Volume usage**.
2. Click the filter marked **All** to select **Workspace**.
3. In the **Search** box, enter a workspace name and click the name when it appears in the list.
4. Click the time filter to select a time range.
5. In the graph, examine volume usage for that workspace. In the table, view the breakdown of total transfer usage by nodes associated with that workspace.

Example use cases for monitoring file access

For security and monitoring purposes, get insights into file access in your subscription.

I need to restrict permissions on a particular file, and I want to see who currently has access.

1. Go to Activity > File access.
2. In the search box, enter a file name and click the name when it appears in the list.
3. In the permissions filter, keep the default (**All permissions**) or select a permission such as **Read**.

Example use cases for monitoring application events

For security and monitoring purposes, get insights into application events in your subscription.

Is a given user logging in frequently enough to justify giving them an account?

1. Go to **Activity > Application events**.
2. Click the filter marked **All events** to select **Logged in**.
3. Click the time filter to select the desired time period.

4. (Optional) To refine your results, in the **Filter** box at the top right, enter a user name.

Automation app: Automate your transfer workflows

Review Automation app highlights, key concepts, and prerequisites. Enable the app and add users. Link to the Automation app API. Understand and configure workflows triggers, actions, and jobs.

- [Get started](#)
Review Automation app highlights, key concepts, and prerequisites. Enable the app and add users. Link to the Automation app API.
- [Create and manage automated workflows](#)
Review a sample workflow. Understand and configure workflows triggers, actions, and jobs.

Get started

Review Automation app highlights, key concepts, and prerequisites. Enable the app and add users. Link to the Automation app API.

- [Automation app: Overview](#)
The Automation app in Aspera on Cloud lets you create automated workflows that initiate file transfers, make calls to an API, and send notifications to users. This article describes the app, its components, key concepts for automated workflows and jobs, and provides an example use case.
- [Prerequisites](#)
Before a user in your organization can use the Automation app, an admin must enable the app and add members. The admin must also enable communication between the Activity app and the attached node and storage.
- [Enabling the Automation app and adding members](#)
The Automation app is not enabled by default. As an admin, you must enable it and add members, organization members who you want to use the Automation app. For content security purposes, note that a user of any role who is a member of the Automation app can use all the features of the app and see all content in the app, regardless of their workspace membership.
- [Resources for developers](#)
You can find reference information and developer guides for the Automation API on the IBM API Hub.

Automation app: Overview

The Automation app in Aspera on Cloud lets you create automated workflows that initiate file transfers, make calls to an API, and send notifications to users. This article describes the app, its components, key concepts for automated workflows and jobs, and provides an example use case.

Automation is available to users with a Standard Plus or Premium edition of Aspera on Cloud.

Highlights

- Automate your file transfer workflows with event-based triggers cued to IBM Aspera on Cloud endpoints.
- Seamlessly integrate with external web services via API calls.
- Communicate workflow status with event-driven email notifications.
- Easily build, execute, and manage workflows with an intuitive interface.

Automation monitors your file storage system for event triggers; for example, a specific date and time can initiate a transfer, and a file upload to a shared folder can trigger an email notification.

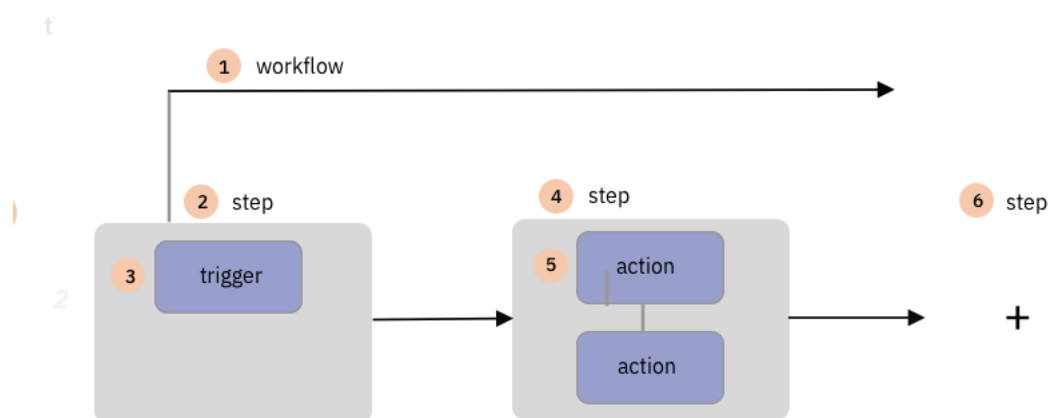
You can transfer files and folders to an Aspera on Cloud (AoC) workspace, an on-premises node, or a node in the cloud. The IBM Aspera FASP protocol embedded in AoC allows you to transfer files of any size, securely and reliably, at unrivaled speed.

The Job Queue page in the Automation app allows you to easily monitor all running and completed workflow jobs.

Key concepts

To build an automated workflow in the Automation app, create the new workflow, then add steps: first, a workflow trigger, then a number of various actions. When your workflow is complete, activate it to generate jobs (a job is a running instance of a workflow). For a sample build, see [Tutorial: Create a simple workflow that transfers a package](#).

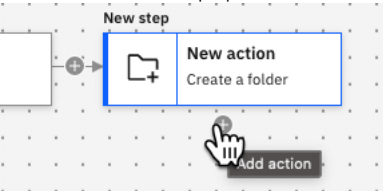
Building a workflow: components



- 1 Create the new workflow.
- 2 Create the first step in the workflow.
- 3 Create the workflow trigger in the first step.
- 4 Create the second step.
- 5 Create one or more (parallel) actions in the second step.
- 6 Continue to create steps, as needed, with one or more actions in each step.

Key concepts: Workflows

The elements below are available on the Workflows page. You interact with them when you build a new workflow or edit an existing workflow.

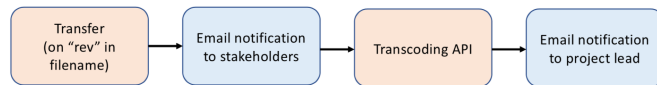
Element	Description
workflow	A workflow is the container for a trigger and for all the tasks you need to accomplish. A workflow can contain any number of steps. Each workflow starts with a trigger that you configure to run the workflow.
step	The first step in the workflow always contains the trigger that runs the workflow. All subsequent steps contain one or more actions, which perform the actual "work" in the workflow. The steps in a workflow organize and sequence these actions for maximum effectiveness.
trigger	The first step in a workflow is always a trigger step. It defines the conditions for launching the workflow. These are the available triggers types (for details, see Workflow triggers and their attributes): - Manual: Trigger the workflow with a manual action. - A user can run the workflow by clicking the workflow row to open it, then clicking Run now. - An API call can run the workflow. - A workflow with a Manual trigger must contain at least one Transfer or Send a Package action. - Time schedule: Use this trigger to launch a workflow at a scheduled time. You can make this a recurring scheduled launch, repeating as required by your situation. A workflow with a Time schedule trigger must contain at least one Transfer or Send a Package action. - File event: Trigger the workflow when Automation detects a new file added to a folder. You need the node secret to select the folder. - Shared inbox event: Trigger the workflow when a package arrives in a shared inbox. - File/folder delete event: Trigger the workflow when a file or folder is deleted.
action	An action step in Automation performs the tasks required in the workflow. It performs one of the following tasks (for details, see Workflow actions and their attributes): - Transfer: Transfer files or folders. - Send a package: Create and send a digital package to users, groups, or a shared inbox in Aspera on Cloud. See Packages app: Send and receive files and folders. - Call an API: Call an external API. - Notify: Send an email notification to stakeholders. - Custom variables: Create custom variables. - Create a folder: Create a new sub-folder inside an existing folder on a workspace or a node. Note: You can have multiple <i>parallel</i> actions in a step. To create a parallel action, click the plus icon below an existing action step. 

Key concepts: Jobs

The Job queue page displays your running jobs and any jobs still in the queue:

Components	Description
job	An instance of an active workflow that is launched each time that workflow is triggered. You can see the status of your jobs on the Job queue page. Depending on your Aspera on Cloud subscription edition, these are the concurrent job maximums: - Standard Plus edition: 5 concurrent jobs max - Premium edition: 10 concurrent jobs max
queue	The queue contains all jobs beyond the allowed maximum number of running jobs. As each running job completes, another job is released from the queue. Jobs move from the queue to running in the order that they were added to the queue. Depending on your Aspera on Cloud subscription edition, these are the queue size maximums: - Standard Plus edition: 5,000 jobs - Premium edition: 10,000 jobs

Example use case



For a team that submits video content to a shared inbox in the AoC Packages app, the project lead sets up a workflow that triggers each time a member submits a package with the metadata value, 'rev'. When the workflow is triggered, the following things happen:

1. AoC automatically transfers the video files in the package from shared storage to remote cloud storage.
2. Three stakeholders receive email notifications that the files have successfully transferred.
3. Once the transfer is successfully completed, an API triggers a step that runs a transcoder on the files.
4. The project lead receives an email that contains the success or error response code from the API.

Prerequisites

Before a user in your organization can use the Automation app, an admin must enable the app and add members. The admin must also enable communication between the Activity app and the attached node and storage.

- Your organization must have the Standard Plus or Premium edition of Aspera on Cloud. To confirm your subscription level, click the user menu icon at the top right of the page, then click **Account settings**.
- Both the Activity app and the Automation app must be enabled. See [Enabling the Automation app and adding members](#).
- Add your transfer node IP address to your firewall allowlist (whitelist). See the section about firewall requirements in [Prerequisites](#).
- You must configure the node attached to your Aspera on Cloud app to send data to the Activity app. See the following sections in this article.

Configure an Aspera on Cloud node to send data to the Activity app

To enable the Automation app, you must first configure the Aspera on Cloud node to send data to the AoC Activity app. This process ensures that Automation receives the data it needs to function properly.

1. In the left navigation menu, click **Nodes and storage > Node policies**.
2. Click **Configuration policies**, then click **Add policy**.
3. Enter a name for the configuration policy and update other fields, as needed.
4. Check the box labeled **AEJ logging**, then click **Save**.
5. In the left navigation, click **Nodes**.
6. Select your node and apply the new configuration policy.

Configure your tethered node to send data to the Activity app

A *tethered node* is a user-managed High-Speed Transfer Server that is attached, or tethered, to Aspera on Cloud. For the tethered node to work properly with Automation, you must first configure it to send data to the AoC Activity app. This process ensures that Automation receives the data it needs to function properly.

These are the requirements for using a tethered node with Automation:

- The HST server installed on the node must be v. 4.0 or higher.
- Nodes on the Windows platform are not currently supported.

To tether a node to your Aspera on Cloud organization, see [Tether Your Aspera Transfer Server to Aspera on Cloud](#). The specific procedure in the tethering process is [Configure Monitoring and Metering for your Tethered Node](#), but the entire tethering process is required.

Enabling the Automation app and adding members

The Automation app is not enabled by default. As an admin, you must enable it and add members, organization members who you want to use the Automation app. For content security purposes, note that a user of any role who is a member of the Automation app can use all the features of the app and see all content in the app, regardless of their workspace membership.

To enable the Automation app, you must first select the check box to enable the application, then add members.

1. In the left navigation menu, go to Admin > Applications > Automation.
2. Select the check box next to **Enable application**, then click **Save**.
3. Add members to the Automation app. Any user (including yourself) must be added as a member before they can use the Automation app.
 - a. Click Members > Add members.
 - b. Start typing the email for the user. Select the full user name when it appears in the menu. Click **Add**.

If the full user name does not appear, that user is not yet a member of the organization. Follow these additional steps:

1. In the left navigation menu, click **Users**, then click **Create new**.
2. Enter the user's email and any other relevant data, then click **Create user**. For details, see [Create and manage users](#).
3. In the left navigation menu, click **Applications > Automation** and add the user as a member of the Automation app.

Resources for developers

You can find reference information and developer guides for the Automation API on the IBM API Hub.

See <https://api.ibm.com/explorer/catalog/aspera/product/ibm-aspera/api/automation-api/spec/automation-api>.

Create and manage automated workflows

Review a sample workflow. Understand and configure workflows triggers, actions, and jobs.

- [Tutorial: Create a simple workflow that transfers a package](#)
In this tutorial, you create and configure an automated workflow that triggers each time a package is received by a shared inbox in Aspera on Cloud. While this example may not match your precise use case, it demonstrates the basic process for assembling the components of a workflow in the Automation app.
- [Workflow actions and their attributes](#)
This topic provides detailed information on workflow actions and their specific configurable attributes. Workflow actions include transfer, send a package, notify, call an API, and so on.
- [Workflow triggers and their attributes](#)
This topic provides detailed information on workflow triggers available and their specific configurable attributes. Workflow triggers include scheduled or time based; file, folder, and shared inbox events; and so on.
- [Managing workflows and jobs](#)
You can manage your workflows and jobs by changing their current activity.
- [Use substitution variables in workflow actions](#)
You can use global or customer substitution variables to configure the fields in workflow actions.
- [Configuring API callback](#)
When you enable API callback in Automation, after the API action makes a call to the defined API, the workflow pauses and waits for the external service to call back to Automation. If Automation receives a response with a `status` value of `success`, the workflow proceeds to the next step.

Tutorial: Create a simple workflow that transfers a package

In this tutorial, you create and configure an automated workflow that triggers each time a package is received by a shared inbox in Aspera on Cloud. While this example may not match your precise use case, it demonstrates the basic process for assembling the components of a workflow in the Automation app.

1. Create the workflow and add the trigger

In this procedure, you create a new workflow and then create the trigger. The triggering event for this workflow is a package arriving in a shared inbox in Aspera on Cloud. You also create custom conditions using metadata that is already configured on the shared inbox.

1. On the Workflows page, click Create new.
2. Enter a name for your workflow, then click Submit.
3. Select the trigger for the first step.
In the New trigger window, click Shared inbox event.
4. In the View as field, select User or Admin.
5. Select the workspace where this event must occur to trigger the workflow.
6. Select the shared inbox. Click Save.
7. Under Workspace, select the desired workspace.
Under Name, select a shared inbox. Click Select.
8. Return to the right pane, under Trigger location.
To create a metadata condition, select Custom in the right pane.
From the menu, select Any of the following conditions.
9. Under Condition 1, select a field, such as File type.
Select a matching condition, such as Contains.
In the text box, enter a string, such as jpg, png.

The transfer now triggers for a package with a metadata field called "File type" that contains the values "jpg" or "png".
10. Click Save.

2. Create actions in the workflow

In this procedure, you select an action for the second step in the workflow. Each step can contain one or more parallel actions. You will configure a transfer action, which transfers a file or folder from the shared inbox you selected in the first procedure to the node you select here. You then create a final step to notify stakeholders.

1. Select an action for the second step in the workflow. Each step can contain one or more parallel actions.
In the right pane, click Transfer.
2. Click Source location for your transfer, then click Same as trigger.
3. Click Destination location for your transfer; then click Nodes.
4. In the Node access dialog, select a node from the dropdown; then enter the secret.
Click Log in.
5. Select a folder from the Name list, then click Select.
6. To add a final step with a notification action, click the plus sign (+) to the right of the transfer action step.
7. In the right pane, click Notify.
8. Enter an email address in the To field, and add an optional message.
Click Save.
Now you're ready to activate your workflow.

3. Activate and launch your workflow

In this final procedure, you activate your workflow so that it begins automatically launching a new *job* (a running instance of the workflow) each time a package is received by the shared inbox.

1. At the top right of the page, click Activate.
2. In the Activate workflow dialog, click OK.
Each new job transfers the package from the shared inbox to the *node* (transfer server) location that you specified in your workflow configuration.
Note: The following is the number of jobs that Automation can run at the same time (in parallel), by subscription type:
 - Standard plus edition of Aspera on Cloud: 5 jobs
 - Premium edition of Aspera on Cloud: 10 jobsAs each running job completes, another job is released from the queue.
3. To view the status of your workflow, click Job queue in the left pane.

Workflow actions and their attributes

This topic provides detailed information on workflow actions and their specific configurable attributes. Workflow actions include transfer, send a package, notify, call an API, and so on.

Transfer

Use this action to transfer files or folders. The following are configurable settings.

- **Source of your transfer**

To use the location you set as the trigger location for the transfer source, select Same as trigger.

To select or create a folder on a transfer node, select On a node; you need the node secret.

To select a folder in a workspace, select the workspace and:

- Click My folders to select any folder you can access in the Files app in that workspace.
- Select Admin shared folders to select any folder shared by an admin in that workspace.

When you configure a *node folder* as your transfer source, you have additional options.

In After transfer, select the action you want.

You can configure the workflow to delete or archive the contents of the source folder after the transfer.

- Delete source content
Select this option to delete the source folder contents that were transferred.
 - Delete remaining files
Files that already exist at the destination are not transferred again; they are skipped by the transfer and remain in the source folder. Select this option to delete files that remain in the source folder after the transfer because they were skipped by the transfer.
 - Delete empty nested folders
After the transfer, delete empty nested folders in the source folder. If you don't select this option, empty folders remain in the source folder.
 - Delete empty source folder
If the source folder is empty after the transfer, delete it.
Note: When you configure your workflow to delete an empty source folder, and if your workflow contains multiple transfer actions, verify that each transfer action uses a different source folder.
- Archive source content
Select this option to archive the source folder contents that were transferred.

Keep in mind that when files already exist at the destination they are not transferred again; they are skipped by the transfer, remain in the source folder, and are not archived by this setting.

Select the archive folder location based on the location of the source folder, as shown in the following table.

If the Source folder is a ...	Select the Archive folder by browsing from this start point
Node folder	Node root folder. You can select any location on the node for the archive folder.

If the Source folder is a ...	Select the Archive folder by browsing from this start point
Workspace personal (unshared) folder	Workspace home folder. You can select any location in the workspace for the archive folder, with one exception: you cannot select a shared folder.
Workspace shared folder	Top level of the shared folder in the workspace. For example, if the source folder path is <code>workspace/abc/xyz/previews</code> , selection starts at <code>/abc</code> . You can select any location starting at <code>/abc</code> .
Workspace shared inbox	Workspace home folder. You can select any location in the workspace for the archive folder, with one exception: you cannot select a shared folder.

- **Destination of your transfer**

Select the destination folder for your transfer. You can select a folder on a transfer node or a folder in a workspace; you need the node secret.

- **Create folder when workflow runs**

If necessary, the workflow can automatically create a folder at the destination location. Use text and substitution variables (click View substitution variables) to name the created folder. The created folder acts as the transfer destination.

- **Transfer settings**

The settings available depend on the admin configuration. For details on these settings, see the [Aspera High-Speed Transfer Server Admin Guide](#) for your platform and software version and the [IBM Aspera Node API documentation](#).

- **Action timeout**

If the Automation app does not receive an update from the transfer server within the duration you configure here, the action step times out and fails, causing the workflow job to fail. When you set this value, consider the latency in your network; if latency is high, extending the timeout interval may allow more action steps to complete.

See also the section below, "Action Timeout Settings Details", for defaults and valid values for each action type.

- **Target rate**

Configure the target rate for the transfer. To set this rate, keep in mind the write speed of your transfer endpoints and set your target rate so that the destination buffer is not overrun. Note that this setting interacts with the target rate setting at the transfer node; the actual transfer behavior will obey the lower of the two settings.

- **Retry attempts**

If you want the workflow to retry the transfer in the event of a failure, set the number of times you want the workflow to retry the transfer. If you don't want the workflow to reattempt a failed transfer, leave this field blank.

- **Time between retries**

Set the time duration, in seconds, that the workflow should wait before the next retry attempt.

- **Rate policy**

The rate policy for the transfer in this step can be High, Fair, Low, Fixed. This setting interacts with the rate policy setting at the transfer node. The rate policy actually applied is always the more restrictive of the two settings.

For example, if the rate policy setting at the node is Fair and the setting in Automation is High, the actual transfer behavior will be Fair. Similarly, if the setting at the node is High and the setting in Automation is Low, the actual transfer behavior will be Low.

Be sure you understand the impact of this setting before changing it; it affects how Aspera transfers share available bandwidth with other traffic.

- **Transport encryption**

Set the encryption algorithm to be applied to your data in flight. The actual transfer behavior will depend on the interaction between Automation app settings and transfer server settings. In all cases, the higher key-length setting will take precedence.

For example, if the encryption algorithm at the node is set to AES-128 and at the Automation app is set to AES-192, the actual encryption used will be AES-192.

Similarly, if the setting at the node is AES-256 and the setting at the Automation app is AES-192, the actual encryption algorithm will be AES-256.

- **Content protection**

To encrypt this content at the destination, enter a password. The recipient needs the password to decrypt the content in the destination folder. Send that password to the recipient under separate cover. Leave this field blank to decrypt the content in the destination folder. For more details, see [Sending: Detailed procedure](#), [Content encryption: In flight and at rest](#), and [Require encryption at rest](#).

- **Resume partially transferred files**

If a transfer is interrupted or fails to finish, select this option to resume the transfer from where it previously stopped, without re-transferring already transferred content.

- **Overwrite policy**

If a complete version of a file in your source location already exists at your destination location, configure the policy to govern whether to overwrite the existing destination file with the source file.

You can set the policy to overwrite always (Yes) or never (No). Or you can set to overwrite based on a comparison between source and destination files. You can overwrite when the source file is different in any way from the destination file; when the source file is newer; or only when the source file is both newer and different.

For details on how the overwrite policy interacts with the resume policy, see the [IBM Aspera High-Speed Transfer Server Admin Guide](#) for your platform and software version.

- **Preserve file attributes**

To preserve all the timestamps from source files at the destination, select this option. You may need to preserve the timestamp on the source file when, for example, another process must act on the file based on the original timestamp.

Send a Package

Use this action to send a [digital package](#). The following are configurable options.

- **Source**

See Source of your transfer under "Transfer". Note that source archiving is not available for this action.

- **Send a package**
See [Send files and folders in a digital package](#).
- **Transfer settings**
See Transfer settings under "Transfer".

Call an API

Use this action to call an external API. The following are configurable options.

- **Request type**
Select the request type: GET, POST, PUT, DELETE.
- **API URL**
Enter the URL for the specific API you want to call.
- **Authorization**
Select the authorization type for this API call, bearer token or basic auth, and enter the required credentials.
- **Verify SSL certificate**
Verify that the SSL certificate is valid.
- **Headers**
To include a custom header, click Add header, then enter the key and value.
- **Action timeout**
If the Automation app does not receive an update from the transfer server within the duration you configure here, the action step times out and fails, causing the workflow job to fail. When you set this value, consider the latency in your network; if latency is high, extending the timeout interval may allow more action steps to complete.

See also the section below, "Action Timeout Settings Details", for defaults and valid values for each action type.
- **Add an API callback.**
See [Configuring API callback](#).

Notify

Use this action to configure notifications to interested parties about the workflows.

- **Sender**
Select the default sender or yourself as the sender of the automated email notification. The default sender is configured in the base template for the organization. For details, see [Customize email notification templates](#).
- **Subject, To, Message**
Configure the subject line of the email notification, the recipient(s), and the message or body of the email to send.
- **Action timeout**
If the Automation app does not receive an update from the transfer server within the duration you configure here, the action step times out and fails, causing the workflow job to fail. When you set this value, consider the latency in your network; if latency is high, extending the timeout interval may allow more action steps to complete.

See also the section below, "Action Timeout Settings Details", for defaults and valid values for each action type.

Custom Variables

Use this action to create custom substitution variables to use in your workflow. Once the custom variable step completes, a following step in the workflow can use the custom variable.

- **Name and Value**
For details, see "Custom Variables Created with the Custom Variable Action" in [Use substitution variables in workflow actions](#).

Create a Folder

Use this action to create a folder to use in the workflow.

You need the node secret to select the location to create the folder.

Once you log in to the node or workspace, navigate to the location where you want the folder created. Select that location.

To name the folder, enter text or select variables as required. To select variables, click View substitution variables.

Action Timeout Settings Details

If the Automation app does not receive an update from the node within the interval you configure, the step that contains the action will fail, and then the job will fail:

Action	Timeout Default	Minimum Allowed	Maximum Allowed
Transfer	24 hours	1 hour	48 hours
Send a Package	24 hours	1 hour	48 hours
Call an API	5 minutes	1 minute	24 hours

Action	Timeout Default	Minimum Allowed	Maximum Allowed
Call an API (with API callback enabled)	24 hours	1 hour	48 hours
Notify	5 minutes	1 minute	60 minutes
Custom variables	5 minutes	1 minute	60 minutes
Create a folder	5	1 minute	60 minutes

Workflow triggers and their attributes

This topic provides detailed information on workflow triggers available and their specific configurable attributes. Workflow triggers include scheduled or time based; file, folder, and shared inbox events; and so on.

Manual

Launch (trigger) the workflow with one of these manual triggers.

A workflow with a manual trigger must contain at least one Transfer action or Send package action.

- **Run now**
For any workflow you own or manage, simply right-click the workflow and select Run now.
- **API call**
Use an API call to launch the workflow. Send a POST call to this endpoint: `/workflows/:id/launch`.

Time schedule

Launch the workflow at a recurring scheduled time.

A workflow with a time-based trigger must contain at least one Transfer action or Send package action.

- Select a date and time to launch the workflow.
- Set the time interval for the recurring launch.
- If desired, set a date to end the workflow. After this date, passage of the configured interval no longer launches the workflow. Set the toggle to Yes, then set the date and time to end the recurrence.

For example, you create an automated workflow that takes about two hours to complete.

- In the The flow starts field, set the initial start time to January 1 at 1:00 AM.
- In the Repeats every fields, set the recurrence interval to 6 hours.
- The workflow first runs on January 1 at 1:00 AM.
- The workflow completes in two hours, around 3:00 AM. Then the 6-hour recurrence interval begins (at around 3:00 AM).
- The workflow runs during the next 6-hour interval, before 9:00 AM (3:00 AM + 6 hour interval).

File addition event

Launch the workflow when Automation detects a new file in the folder you select. You can select a folder on an attached node or in a workspace.

Select the folder to monitor and set file conditions if required.

1. Click Choose an option.
2. To select a folder on a node, do the following:
 - a. Select On a node, select the node, enter the node secret, then click Log in.
 - b. Select the folder to be the trigger for this workflow, then click Select.
You can navigate into a folder. You can create a new folder.
3. To select a folder in a workspace, do the following:
 - a. Select the workspace.
Select from the list of workspaces where you are a member. To select a workspace where you are not a member, go back to step 2 and navigate to the desired folder on the node.
 - b. Click Browse folders to see your own home folder in the workspace. Select the folder, or create and select a new folder.
 - c. If you are an org admin, click Browse shared folders to see all shared folders in the workspace.
 - d. Click Select.
4. In Trigger when, do the following:
 - To trigger the workflow when any new file is detected, select Any file is added.
 - To trigger only when a new file of a certain name, size, or type is detected, select Custom, then configure the conditions.
You can configure multiple conditions; click Add condition.
5. Click Save.

When Automation detects a new matching file in that folder, the workflow launches.

Shared inbox event

Launch the workflow when Automation detects a new package in the shared inbox you select.

Select the workspace, then the shared inbox.

- Any file is added
Launch the workflow when Automation detects any new package in the shared inbox.
- Custom
Select one or more of the configured metadata fields on the shared inbox, an operator, and a value. When a package arrives that matches the condition(s) you set, the workflow launches.

File or folder deletion event

Launch the workflow when Automation detects that a file or folder was deleted (Files app). You can select a folder on an attached node or in a workspace.

Select the folder to monitor and set file conditions if required.

- Click Choose an option, or click Change if already selected.
- To select a folder on a node, do the following:
 - Select On a node, select the node, enter the node secret, then click Log in.
 - Select the folder to be the trigger for this workflow, then click Select.
You can navigate into a folder. You can create a new folder.
- To select a folder in a workspace, do the following:
 - Select the workspace.
Select from the list of workspaces where you are a member. To select a workspace where you are not a member, go back to step 2 and navigate to the desired folder on the node.
 - Click Browse folders to see your own home folder in the workspace. Select the folder, or create and select a new folder.
 - If you are an org admin, click Browse shared folders to see all shared folders in the workspace.
 - Click Select.
- In Trigger when, do any of the following:
 - To trigger the workflow only when the trigger folder is deleted, select This folder is deleted.
 - Select the boxes so that the workflow launches when either the trigger folder OR the top-level item in the trigger folder is deleted.
 - To trigger the workflow when either the trigger folder OR when a file of a certain name, size, or type is deleted, select Custom, then configure the conditions.
You can configure multiple conditions; click Add condition.
- Click Save.

Managing workflows and jobs

You can manage your workflows and jobs by changing their current activity.

See [Automation app: Overview](#) for more information about workflows and jobs.

Managing workflows

On the Workflows page, you can change the current activity of a workflow to achieve your goals; for example, you might need to edit a workflow that is active and is currently launching new jobs.

To manage your workflow, click the overflow menu to the right of the workflow name and click the item described in the "User Action" column below.

Note: The actions that are available for a given workflow vary depending on your ownership and the current workflow status.

User Clicks . . .	Resulting Change to Workflow Behavior	New Status (in Status Column)
Activate	The workflow begins launching jobs. Note: If you have a workflow with a manual trigger, you must next select Run now from the overflow menu to start launching jobs.	Active
Deactivate	Pauses an active workflow. Currently running jobs can complete, although you have the option to cancel them. All future jobs are canceled. Organization admins can deactivate workflows created by other users. Previously, organization admins were only able to activate other users' workflows.	Inactive
Delete	Cancels all currently running jobs and all future jobs.	Removed from page
Duplicate	Duplicates the selected workflow. Organization admins can duplicate workflows created by other users. Note: You can duplicate workflows regardless of their trigger type (for example, manual, scheduled, or event-based). However, successful execution of the duplicated workflow depends on your permissions. If you do not have the required access to the associated resources (such as a shared inbox or a shared folder), the workflow may fail at runtime.	Draft
Edit	Cancels all currently running jobs and all future jobs.	Draft
Email notifications	Configure notifications for specific individuals or groups that need to know when a workflow has started, completed, or failed.	No change
Job queue	Jump to the job queue for the workflow.	No change
Rename	No change to current or future activity.	No change
Run now	Start a job for this workflow.	Running
Share	Share a workflow you own with another individual user, granting Manage jobs permission, which allows your recipient to view your workflow and to start, cancel, and delete job in it.	No change

Managing jobs

Manage your jobs on the Job Queue page. Check the box to the left of the job and click the action described in the first column below:

User Clicks . . .	Resulting Change to Job Behavior	New Status (In Status Column)
Cancel running jobs	You can cancel jobs in Running now Or Queued status. For an in-progress (blue dot on step indicates in-progress) transfer step, Automation sends an asynchronous cancel request to the node, then reports the job as cancelled. Automation does not track the node response; if the node fails to cancel the transfer, the transfer continues even though you cancelled the job. All queued jobs are automatically cancelled.	Cancelled
Delete jobs	Deletes the job from the list of jobs on the page.	Removed from page

To see the status for each step of an existing job, click a job in the list. Steps are marked green for success, blue for in progress, and red for failed.

Use substitution variables in workflow actions

You can use global or customer substitution variables to configure the fields in workflow actions.

Variables allow you to customize the results of an action. For example, you can configure the message in an email notification to contain the response body from an previous action that calls an API.

Substitution variables can be global or custom. Custom variables capture output values from previous actions in the workflow.

The available substitution variables are constrained by the type of trigger or other actions in the preceding steps. Some examples are:

- File event trigger: filename and timestamp
- API action: response code and response body
- Transfer action: status and transfer UUID
- Metadata: shared inbox metadata

You can also use a substitution variable to name a subfolder in a transfer action.

To use a substitution variable when configuring an action, click in any field that allows you to enter text, then click View custom variables. You can combine text and multiple variables as required.

Use global substitution variables

Global variables are standardized variables that appear in every workflow action. They can be used in any configuration field that supports output variables.

These variables include the ID for a job, and the time when the workflow is triggered and launches the job:

- uuid: The ID of the job that launches when the workflow is triggered
- DD: Two-digit day of the month (for example, 28)
- MM: Two-digit month (for example, 03)
- MMM: Three-letter month name (for example, Oct)
- YYYY: Four-digit year (for example, 2020)
- hh: Two-digit hour (for example, 10 for 10:00am, or 15 for 3:00pm)
- mm: Two-digit minutes (for example, 52)
- date_time: Date and time in GMT (for example, 2020-02-03 08:11:22TZD)

Create custom substitution variables

The Custom variable action let you create one or more custom variables, which can then be used in actions in subsequent steps.

For each custom variable, you create a name and a corresponding value. The value can be a combination of a unique text variables, substitution variables, and global variables. For example, you can create a value that combines:

- a user's email that you enter (custom variable).
- a session ID (global variable).
- metadata (substitution variable from a previous step).

Note: Custom variable names can't contain spaces.

Configuring API callback

When you enable API callback in Automation, after the API action makes a call to the defined API, the workflow pauses and waits for the external service to call back to Automation. If Automation receives a response with a status value of success, the workflow proceeds to the next step.

Prerequisites

You must configure your API server to support API callback. Otherwise, the action will fail and your workflow will fail. The server must include these elements when it responds to Automation:

- Automation's static URL (the callback endpoint): https://api.ibmaspera.com/automation/v1/external/api_callback
- The token from Automation (which it can parse from the payload sent in step 1, below).

Enabling API callback in the UI

To use API callback, go the Automation Workflows page:

1. Create or open a workflow and select the Call an API action.
2. Select a Request type of POST or PUT.
3. Check the box labeled Add an API callback.
4. Configure the rest of the fields as needed, then click Save.
5. Activate the workflow.

Sequence of events

If you enable callback for an API action, the following things happen automatically when the action is triggered:

1. Your workflow sends the JSON payload to the API you defined for the action. Automation inserts a required token (a unique identifier) in the payload, by default. At this point, the workflow pauses to wait for a response.
Note: When you enable the callback feature, the default timeout value—the maximum time the action can take before it is marked as `failed`—changes from 5 minutes to 24 hours.
2. (Optional) The external service may send status notifications to the callback endpoint. These responses contain a `status` field with a value of `in progress` and a `progress` field with a value between 0–100. The data is displayed in the Automation UI, on the Workflows page.
3. When the service completes its process, it returns a JSON response to the callback endpoint. The payload must include the unique identifier token from Automation and a status of `success` or `failed`.
4. If the status is `success`, the workflow proceeds to the next step.

Troubleshooting

Address issues with transfers, access, notifications, and more. Subscribe to app status information, maintenance schedules, and new features announcements. Get access to IBM Support.

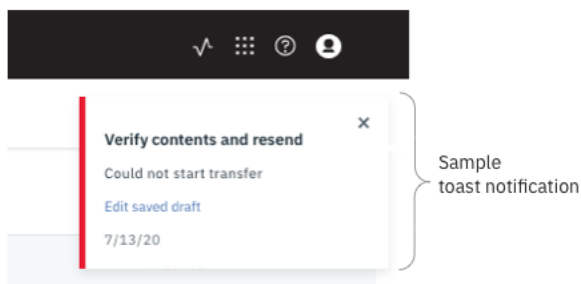
- [Failure notification types and locations](#)
This topic describes the various notifications that AoC provides when a transfer fails.
- [Get current status information for Aspera on Cloud](#)
IBM Aspera provides an up-to-date status page with current system status and performance, along with planned maintenance windows and known issues. You can subscribe to status notification updates if you wish.
- [Transfer issues](#)
Get troubleshooting procedures to investigate, characterize, and address slow transfer speeds, transfer failures, node-to-node transfer issues, and more.
- [Access, notifications, and other issues](#)
Investigate, isolate, and address issues like missing credentials and email notifications, shared folder access, stored report availability, deleting and renaming large folders, and more.
- [Aspera Connect installation issues](#)
Find troubleshooting procedures addressing Aspera Connect installation-specific issues.
- [Specific error messages](#)
This article describes troubleshooting options for some specific error messages.
- [Get IBM technical assistance](#)
Find answers to questions about eligibility for technical support, registering with IBM Support, opening cases, subscribing to Support notifications, and other IBM Support resources.
- [Error code reference](#)
A link to reference tables with information about IBM Aspera error codes.

Failure notification types and locations

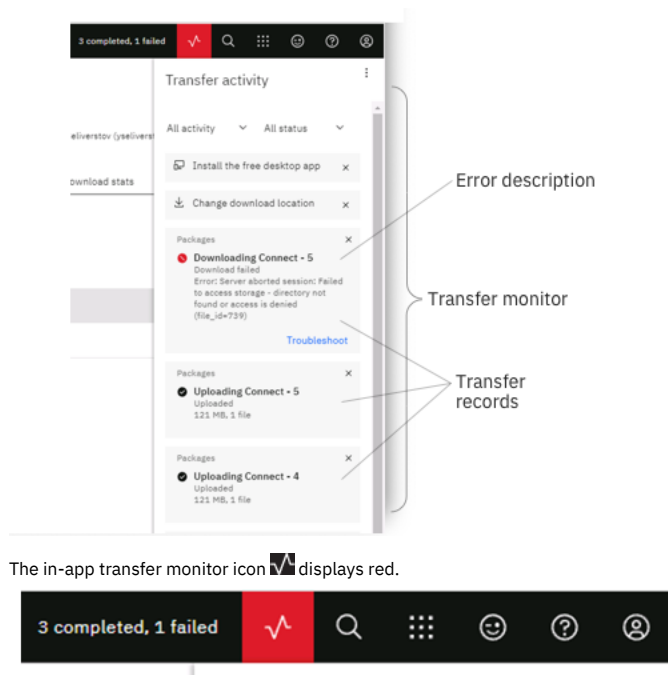
This topic describes the various notifications that AoC provides when a transfer fails.

When a transfer fails, AoC may present feedback in three ways:

- A transient ("toast") message that appears for several seconds in the upper right corner of the AoC app.



- An error description (that may include a recommended action) in a transfer record in the in-app transfer monitor. Display the transfer monitor by clicking this icon in the top banner of the app: .



- The in-app transfer monitor icon  displays red.

To contact your local tech support administrator, click  in the banner and select "Technical support".

Get current status information for Aspera on Cloud

IBM Aspera provides an up-to-date status page with current system status and performance, along with planned maintenance windows and known issues. You can subscribe to status notification updates if you wish.

You can view this information here: <https://status.aspera.io>.

IBM Support My Notifications Service

You can also subscribe to the IBM Support notifications service for Aspera on Cloud. This service sends emails alerting you to scheduled maintenance windows, certain API changes, product updates, and support incidents.

For subscription instructions, go to <https://www.ibm.com/support/pages/node/6123669>. Be sure to subscribe specifically to IBM Aspera on Cloud notifications. You can subscribe to other IBM product notifications as well.

Transfer issues

Get troubleshooting procedures to investigate, characterize, and address slow transfer speeds, transfer failures, node-to-node transfer issues, and more.

- [Select a transfer method](#)
Aspera on Cloud requires one of two transfer methods to power high-speed transfers between user desktops and Aspera transfer servers. Users can either download and install Aspera Connect, a free, lightweight, install-on-demand software program; or an admin can configure the IBM Aspera HTTP Gateway and attach it to your Aspera on Cloud organization.
- [Retry the transfer](#)
You may be able to address a failed transfer by fixing a simple issue and then retrying the transfer.
- [Resending "Draft" packages](#)
When the transfer for a package you send fails to start, AoC displays a transient error message with the heading "Verify contents and resend" and moves the package to the Drafts folder in your Packages app.
- [Node-to-node transfer issues](#)
A node-to-node transfer (also called a *share-to-share* transfer) moves files from one transfer node or cloud storage location to another, as opposed to a transfer between a user desktop and a transfer node.
- [Slow transfer speeds](#)
Many factors affect IBM Aspera on Cloud transfer speed. Some can be addressed by IBM Aspera on Cloud users and administrators. Some must be addressed by administrators of tethered IBM Aspera High-Speed Transfer Servers. Some may be due to cloud service or network conditions that may or may not be under your control.
- [Specific transfer failures](#)
This article describes troubleshooting options for some specific transfer failures.
- [More transfer troubleshooting resources](#)
The IBM Support Knowledge Base contains articles to help identify potential performance bottlenecks, firewall considerations, collect network traces, and find IBM Aspera logs.
- [IBM Aspera Connect common issues](#)
Aspera on Cloud requires one of two transfer methods to power high-speed transfers between user desktops and Aspera transfer servers. Users can either download and install Aspera Connect, a free, lightweight, install-on-demand software program; or an admin can configure the IBM Aspera HTTP Gateway and attach it to your Aspera on Cloud organization.

- [Connect prompt continues to appear](#)

Once you download and install IBM Aspera Connect, the Connect installation prompt should no longer appear. However, there are two circumstances in which you may continue to see the installation dialog even though you've already installed Connect.

Select a transfer method

Aspera on Cloud requires one of two transfer methods to power high-speed transfers between user desktops and Aspera transfer servers. Users can either download and install Aspera Connect, a free, lightweight, install-on-demand software program; or an admin can configure the IBM Aspera HTTP Gateway and attach it to your Aspera on Cloud organization.

Aspera Connect is the default transfer method for Aspera on Cloud and other Aspera web apps. However, if your deployment of Aspera on Cloud does not allow users to download and install client software, you can configure an alternative transfer method: the [IBM Aspera HTTP Gateway](#). The Aspera HTTP Gateway is a standalone product that uses both HTTP/S and Aspera FASP to complete file transfers.

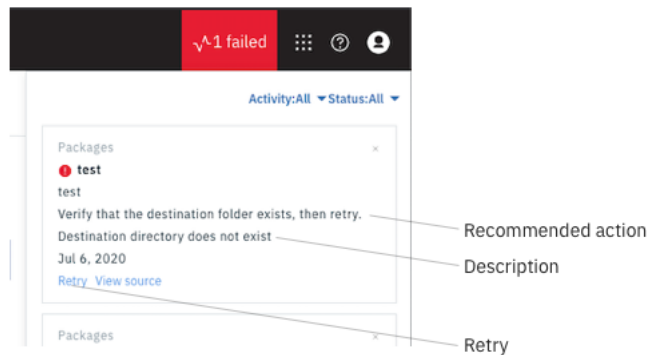
For details about Aspera Connect, see [Aspera Connect transfer client](#).

Retry the transfer

You may be able to address a failed transfer by fixing a simple issue and then retrying the transfer.

When you see the blue Retry link in the transfer record, address the issue described.

For example, consider the following transfer record. Verify that the directory you are trying to transfer to (the "destination" directory) exists; if it does not, create it at the expected path. Then click Retry in the transfer record to attempt the transfer again. This same strategy applies for some session and network anomalies. Perform the recommended action, then click Retry.



To contact your local tech support administrator, click  in the banner and select "Technical support".

If you are the local tech support administrator and need help after using this information, contact IBM support. Include the file available from Help > Download support data.

Resending "Draft" packages

When the transfer for a package you send fails to start, AoC displays a transient error message with the heading "Verify contents and resend" and moves the package to the Drafts folder in your Packages app.

If you see the error message "Verify contents and resend", do the following:

1. Click Edit saved draft in the error message to open the Drafts folder. You can also open the Drafts folder from the left panel of the Packages app.
2. In your Packages app Drafts folder, click the package row to view the package details. Any files and folders listed have been transferred successfully. Files and folders that you sent but are not listed did not transfer.
3. Add the missing content: click Upload to browse, or drag items to the sending panel.
4. Click Send.

The files that were transferred successfully in the first attempt will not be transferred again since they already exist at your intended destination; this means you do not incur more transfer and storage charges. Yet the final package contents are intact in your Sent folder after the transfer succeeds.

To contact your local tech support administrator, click  in the banner and select "Technical support".

Node-to-node transfer issues

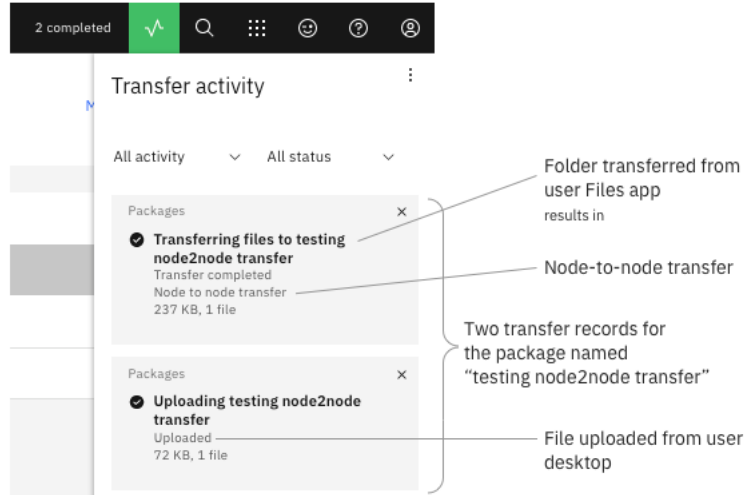
A node-to-node transfer (also called a *share-to-share* transfer) moves files from one transfer node or cloud storage location to another, as opposed to a transfer between a user desktop and a transfer node.

This is as opposed to uploading files from a user desktop or remote storage to a transfer node or cloud storage (or downloading files from the cloud to a user desktop or remote storage).

Folders in a user's Files app may be in any number of storage locations, including in different buckets or different cloud providers. When a user moves files from one folder in the Files app to another, a node-to-node transfer occurs.

Likewise, in the Packages app, sending a digital package that includes files or folders from the Files app ("Upload from Files" in the Send files panel) also results in a node-to-node transfer. And if a digital package includes files or folders already in cloud storage along with files and folders from the user desktop or remote storage, the AoC transfer monitor displays the package transfer on two separate transfer records: one transfer for the upload and a separate transfer for the node-to-node transfer.

For example, the screenshot below shows two transfer reports for a single transfer. The package contains one file ("byok_architecture copy.png") on the user's desktop and one folder ("AoC Self-Packed Onboarding") in the user's Files app.



There may be times when the error message "Unable to start node-to-node transfer" displays.

If you are the user attempting the transfer, try the transfer again because the issue may be ephemeral.

To contact your local tech support administrator, click  in the banner and select "Technical support".

If you are the local tech support administrator, do the following:

1. The security token may have expired. Check configurations in Organization > Security. See [Configuring Organization Security Settings](#).
2. If the transfer is to or from a [tethered node](#), check the transfer logs on the node; see [Where are the IBM Aspera client and server logs?](#)
3. Work with the user to collect web browser network traces; see [How to collect network traces for troubleshooting](#).

Slow transfer speeds

Many factors affect IBM Aspera on Cloud transfer speed. Some can be addressed by IBM Aspera on Cloud users and administrators. Some must be addressed by administrators of tethered IBM Aspera High-Speed Transfer Servers. Some may be due to cloud service or network conditions that may or may not be under your control.

Isolating potential causes

An important step in any troubleshooting process is isolating the cause of the issue. See [this article](#) on the IBM Support site to begin narrowing down the potential source.

Home network limitations

You may experience slow transfer speeds when using Aspera on Cloud at home. Most home internet connections are slower than expected; this is particularly true for upload speeds.

There are several free apps to verify your actual internet speed. Search the web for "internet speed test" to find one. Transfer speeds can never surpass the limits of the local internet connection.

Configuration of IBM Aspera Connect

IBM Aspera recommends that users consult with their administrators before adjusting default settings in Aspera Connect. Misconfiguration can lead to local network overload, degraded transfer speeds, and overloaded storage, among other issues.

If you are the administrator, refer to the [IBM Aspera Connect Admin and User Guides](#).

Connectivity issues test

Use this web-based [diagnostic tool](#) to help identify connection issues. This page also provides additional troubleshooting options and easy access to both the latest version of Aspera Connect should you not already have the latest version and to the Aspera Connect documentation set.

Transfer protocol in use

By default, Aspera on Cloud uses the IBM Aspera Connect app to transfer files and folders between user desktops and remote storage. Connect enables Aspera FASP, the IBM-proprietary high-speed transfer protocol.

An administrator can also configure an alternative transfer method using HTTPS/HTTP protocol for users who cannot install Aspera Connect. This method requires the standalone product called IBM Aspera HTTP Gateway. Once the Gateway is configured, the admin can enable an Aspera on Cloud organization to use it for transfers. See [Transfer with Aspera HTTP Gateway instead of Aspera Connect](#).

Typically, Aspera Connect is the faster transfer method; however, the Aspera HTTP Gateway is available for use cases that demand it. IBM recommends the use of Aspera Connect whenever possible.

When both Connect and HTTP Gateway are available, users can choose to disable Aspera Connect and the FASP protocol it supports. But typically, transfers using Aspera Connect are faster.

Users can regain access to Aspera Connect as follows:

1. Click the user icon and select Account settings. Set Disable Connect to Off, then click Submit to save the setting.
2. Launch the Connect installation:
 - a. Click  to open the transfer monitor.
 - b. At the bottom of the transfer monitor, click Install Connect.

Once users download and install Aspera Connect, transfer speeds typically increase.

For additional information, see [Installation](#). See also the troubleshooting procedures in [Installation troubleshooting](#) and the [IBM Aspera Connect Admin Guide](#).

For admins, see also the [IBM Aspera HTTP Gateway Admin Guide](#).

Additional troubleshooting resources

These IBM Support articles provide additional troubleshooting tips.

- [Identifying and understanding performance bottlenecks with Aspera Transfers](#)
- [How to identify the root cause of a slow transfer](#)
- [Testing performance to isolate issues](#)
- [Find logs for IBM Aspera Connect](#)
- [Find logs for IBM Aspera Desktop Client and IBM Aspera Server](#)

Specific transfer failures

This article describes troubleshooting options for some specific transfer failures.

To contact your local tech support administrator, click  in the banner and select "Technical support".

Aspera Connect is unavailable

- Recommended action: Download and install IBM Aspera Connect. See [Installing Aspera Connect](#).
- More information: See [Select a transfer method](#).

Session data transfer timeout

- Recommended action: Verify network connectivity, then retry the transfer.
- More information: This error typically indicates a UDP timeout. The most likely cause is a network interruption for more than 60 seconds.

Session shutdown failed

- Recommended action: Verify network connectivity, then retry the transfer.
- More information: The session did not shut down properly, and the channel data could not be sent. The most likely cause is a network timeout.

Destination path directory does not exist

- Recommended action: Verify that the destination folder exists, then retry the transfer.
- More information: The target folder cannot be found. Verify that the folder name is accurate and that the folder exists at the expected path. If it does not, create the destination folder at the expected path, then try the transfer again.

Network down

- Recommended action: Verify network connectivity, then retry the transfer.
- More information: The network layer of the operating system may return this error when the Aspera tries to send to a destination that can't be reached because of a disabled or disconnected network interface or router.

Server aborted session: Could not validate bearer token

- Recommended action: Create a new transfer and try again. A simple retry of the same transfer usually does not succeed.
- More information: The security token may have expired. The AoC admin should check configurations in Organization > Security. See [Configuring Organization Security Settings](#).

Server aborted session: Failed to extract JSON data from bearer token

- Recommended action: Log out of Aspera on Cloud, then log in again. Retry the transfer. If the issue persists, create a new transfer and try again after logging out and back in to AoC.

- More information: The security token may have expired. The AoC admin should check configurations in Organization > Security. See [Configuring Organization Security Settings](#).

More transfer troubleshooting resources

The IBM Support Knowledge Base contains articles to help identify potential performance bottlenecks, firewall considerations, collect network traces, and find IBM Aspera logs.

Find these valuable resources at:

- [Identifying and understanding performance bottlenecks with Aspera transfers](#)
- [Firewall considerations](#)
- [How to collect network traces in a web browser for troubleshooting](#)
- [Finding IBM Aspera logs](#)

To contact your local tech support administrator, click  in the Aspera on Cloud banner and select "Technical support".

Access, notifications, and other issues

Investigate, isolate, and address issues like missing credentials and email notifications, shared folder access, stored report availability, deleting and renaming large folders, and more.

- **[Can't find the access credentials to your built-in node](#)**
Each Aspera on Cloud subscription includes one built-in, Aspera-managed transfer server node with storage in IBM Cloud Object Storage. The access credentials (or access key) for this transfer server are delivered to the administrator who first created the AoC organization in a digital package from Tech Support in the Packages app. It's very important to track and store these credentials securely.
- **[Email notifications](#)**
Use this procedure when AoC email notifications do not arrive as expected.
- **[Trouble creating a new access key](#)**
To create a new node and attach storage to your Aspera on Cloud organization, you must create a new access key. Review this procedure if you encounter errors.
- **[Can't access a shared folder](#)**
Use this procedure when you can see a shared folder in your Files app but cannot access it.
- **[User still has access to unshared folder](#)**
If you've unshared a folder to remove access from a specific user, but that user can still access the folder, use this article.
- **[Stored report not available in Activity app](#)**
Use this article to troubleshoot the error message "Unable to download stored report", which may display when you try to access a report listed on the Stored reports page in the Activity app.
- **[Delete large files and folders](#)**
Use this topic to troubleshoot issues that arise when you delete large files and folders in your Aspera on Cloud Files app workspace.
- **[Rename large folders](#)**
This article describes how to troubleshoot an attempt to rename a large folder in your Files app that didn't seem to succeed.
- **[Irdeto watermarking integration](#)**
This topic lists codes and descriptions for errors that may display related to watermarking. It also includes a link to the Irdeto documentation that provides troubleshooting procedures for each error.

Can't find the access credentials to your built-in node

Each Aspera on Cloud subscription includes one built-in, Aspera-managed transfer server node with storage in IBM Cloud Object Storage. The access credentials (or access key) for this transfer server are delivered to the administrator who first created the AoC organization in a digital package from Tech Support in the Packages app. It's very important to track and store these credentials securely.

To retrieve the credentials for your built-in, Aspera-managed node, do the following:

Attention: You must be the administrator who first configured the Aspera on Cloud organization.

1. Go to the Packages app. If necessary, click the app switcher  and select Packages.
2. In the left-side gray panel, click My inbox.
3. In the packages list, click the row of the package from IBM Aspera Tech Support called "Access key information". This package contains a text file listing the key and secret.
4. Review the message included with the package.
5. Right-click the text file and select Download to...
6. In the Finder or Explorer window that opens, select the location for this download.
7. Click Open or Done.
8. Aspera highly recommends you rename the file to make it easier to track. Track and protect the text file with the key and secret according to your local site security practices. Note that IBM Aspera does not keep a copy of the access key secret.

Note: Selecting Download to... affects *only this download*. To change your *default* download location, open Aspera Connect from your system tray or launcher; go to Preferences > Transfers. In the Downloads location field, enter the default location for your downloads.

Email notifications

Use this procedure when AoC email notifications do not arrive as expected.

If you are the person who is missing the notification, do the following:

1. Check that the notification is not in your email spam folder.
2. Check that you haven't disabled the notification. See User icon > Account settings and .
3. Contact your local tech support administrator. Click the Help icon in the banner and select "Technical support". Provide the email address where you expect to receive the notification.

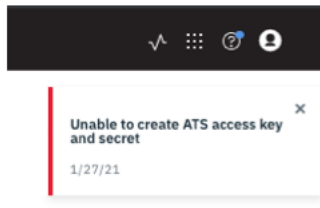
If you are the local tech support administrator, do the following:

1. Check that the AoC user record lists the user's expected email address. See Users > Management.
Note: If the user logs in to Aspera on Cloud through an external authentication or identity provider like IBMid or a SAML system, you cannot edit the name and email address in the AoC user record. The user must change these settings in the external system; that change will propagate to AoC.
2. Check that the user is in fact a member of the group, workspace, shared inbox, or other entity that should receive the missing notification.
3. Check that you have not disabled the specific notification that is missing; see Organization > Notifications and [Control email notification delivery](#).
4. Check that the SMTP server administrator has added the AoC email (donot-reply@ibmaspera.com) for notifications to the "allowed" list on the server.

Trouble creating a new access key

To create a new node and attach storage to your Aspera on Cloud organization, you must create a new access key. Review this procedure if you encounter errors.

If Aspera on Cloud displays the error message "Unable to create ATS access key and secret", verify that the data you entered into each configuration field is accurate. Often this error indicates no more than a typo when entering your storage configuration settings.



This article highlights the fields to verify for each supported storage type.

For all node types, go to Nodes > Create new > Attach my cloud storage.

IBM Cloud

Verify content in the highlighted fields. Ensure there are no typos and that cloud configuration settings are copied accurately.

IBM Aspera on Cloud | Admin

Access key

Storage

IBM COS

Region

Choose an option

Access key ID

Access key secret

Bucket

Path

AWS (Amazon Web Services)

Verify content in the highlighted fields. Ensure there are no typos and that cloud configuration settings are copied accurately.

IBM Aspera on CloudAdmin

Storage

Amazon S3

Region

us-east-1

Storage class

Standard

Amazon S3 Server-Side Encryption (optional)

None

Select the Amazon S3 encryption-at-rest method. Note: Nodes with server-side encryption enabled do not support watermarking.

Trust relationship policy

```
{
  "Version": "2012-10-17",
  "Statement": [

```

IAM role ARN

arn:aws:iam:123:role/mine

Session name (optional)

Bucket

Path

Microsoft Azure Blob

Verify content in the highlighted fields. Ensure there are no typos and that cloud configuration settings are copied accurately.

IBM Aspera on Cloud

Admin

Storage

Microsoft Azure Blob

Region

eastus

API type

Block

Storage credentials

Key

Storage account

Key

Container

Path

Microsoft Azure Files

Verify content in the highlighted fields. Ensure there are no typos and that cloud configuration settings are copied accurately.

IBM Aspera on Cloud

Admin

Storage

Microsoft Azure Files

Region

eastus

API type

Block

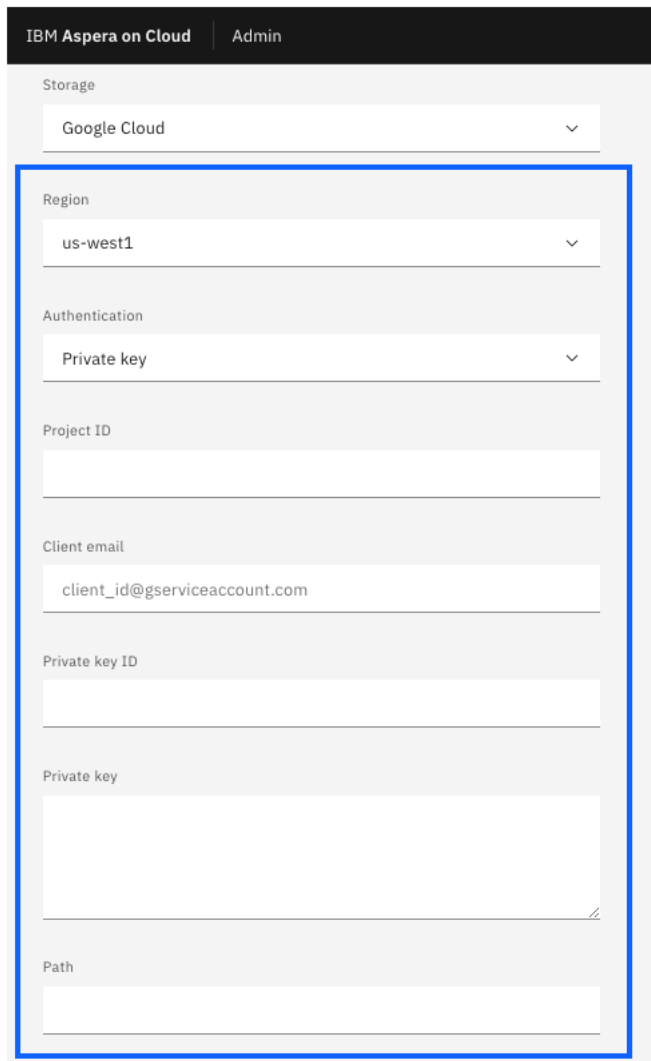
Storage account

Password

Path

GCS (Google Cloud Service)

Verify content in the highlighted fields. Ensure there are no typos and that cloud configuration settings are copied accurately.



IBM Aspera on Cloud | Admin

Storage

Google Cloud

Region

us-west1

Authentication

Private key

Project ID

Client email

client_id@gserviceaccount.com

Private key ID

Private key

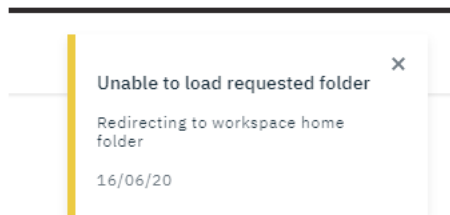
Path

Can't access a shared folder

Use this procedure when you can see a shared folder in your Files app but cannot access it.

If instead your shared folder issue is that you have 'unshared' a folder with a user but the user still has access, see [User still has access to unshared folder](#).

On rare occasions, you may see the error message "Unable to load requested folder" when you try to access a folder that has been shared with you:



When you try to access a folder but the folder is not available, AoC redirects you to the Files app home folder in that workspace. Your home folder is the top level of your Files application in that workspace. If you are a member of the Files app in multiple workspaces, you have a home folder in each workspace.

If you are the person who can't access a folder that you can see, do the following:

1. In your own Files app, check your permissions on the folder (right-click folder row, select Info); do you have the expected access permission?
2. Check with the folder owner that the shared folder still exists. The person who shared is listed in subtext on the row of the shared folder.

☐		Export		0 B
☐		ey	Shared by an admin to this workspace	10 MB 1 file
☐		Files for Check Out	Shared by _____ to you	750 MB 1,176 files, 363 folders

'Shared by'

3. Ask the folder owner to verify that you are in the list of folder collaborators and that you have the proper access permissions.
The folder owner can click the folder row in their own Files app to display the folder details and collaborators panel. If your name is not there, ask the folder owner to share with you again, being sure to select the desired permissions for you.
4. Contact your local tech support administrator. Click in the banner and select "Technical support". Provide the URL of the affected folder.

User still has access to unshared folder

If you've unshared a folder to remove access from a specific user, but that user can still access the folder, use this article.

You can share folders with individual users, with groups, and with entire workspaces. Any given user may have access to a shared folder directly, or may have access through a group or workspace that has shared access.

If you unshared a folder with an individual but that user still has access, you may have to remove the user from a group that has access. For details, see [Direct and inherited memberships](#). Contact your admin to change group membership.

To unshare a folder, see [Unshare a folder](#).

Stored report not available in Activity app

Use this article to troubleshoot the error message "Unable to download stored report", which may display when you try to access a report listed on the Stored reports page in the Activity app.

Note: To enable, configure, and access stored reports, see [Reporting activity and usage](#).

This error displays in several cases. If the secondary line of the error notification advises you that "Storage or report was deleted. Recreate the report", the report you are trying to access is not recoverable; either the storage or the folder in the storage was deleted. You must recreate the report. Use the filters as required to generate the report again.

If, however, the secondary line of the error notification suggests that troubleshooting may be able to recover the report, consider the following information.

Recoverable scenarios

There are three possible scenarios, two of which may be recoverable:

- The node where reports are stored is inaccessible at the moment, but may be accessible after a status update.
- The report has actually been deleted and must be recreated.
- The directory where reports are stored has been changed. The desired report may be recoverable from the previous storage location.

Prerequisites

- You must be an Aspera on Cloud administrator to complete this procedure.
- You may need to access the Activity report storage location directly to search for the report; if so, you need access to your storage management portal and appropriate credentials to the storage.

Procedure

1. Go to Nodes and filter for the node where reports are stored.
To determine which node is currently used for storing Activity reports, go to Applications > Activity > Stored reports. The node and path are listed there.
2. If the node status displays as "Unavailable", right-click the node row and select Update status.
3. Return to Activity > Stored reports and try again to access the report.
If the same error message appears, go to the next step.
4. Access the storage location directly, using the appropriate interface and credentials. Search for the desired report.
 - a. If you find the report, you can download it directly from the node.
 - b. If you cannot find the report, go to the next step.
5. If the location for stored reports has been changed from its initial setting, you can search the previous location for the desired report.
 - a. Access the previous storage location directly, using the appropriate interface and credentials. Search for the desired report.
 - b. If you find the report, you can download it directly from storage.
 - c. If you cannot find the report, you must recreate it.

Delete large files and folders

Use this topic to troubleshoot issues that arise when you delete large files and folders in your Aspera on Cloud Files app workspace.

In the vast majority of cases, deleting a file or folder is an operation performed by your cloud storage. Deleting very large items may require some time to complete; the larger the file or folder, the longer the operation takes. For the largest files and folders, it may take several hours or even an entire day or more. AoC treats deletion as a background operation so you can continue working in Files while the operation completes. See "Managing files in the Aspera on Cloud user guide for related information.

After you initiate the delete operation, AoC recommends that you not perform other actions on the item.

Refresh the browser to verify that the operation is complete and the file or folder no longer displays.

If after some time you refresh your browser and still see the item you want to delete, to the following:

1. Perform the delete operation again.
2. If the item is a folder, try deleting sub-folders or files within the folder first; then perform the delete operation on the folder again.
3. If the issue persists, contact your local tech support administrator: click  in the banner and select "Technical Support".

Rename large folders

This article describes how to troubleshoot an attempt to rename a large folder in your Files app that didn't seem to succeed.

Note: To rename a very large folder (one with more than about 20 items), select the Rename and move option from the right-click menu. This feature improves performance for such large file operations. The renamed folder appears in the same location in the Files app. Note that when this operation completes, you must recreate all existing shared links to contents in the renamed folder.

In the vast majority of cases, renaming a file or folder is an operation performed by your cloud storage. The various cloud platforms use different schemes to rename.

For example, to rename a folder "OldFolder" to "NewFolder":

- Some cloud platforms change a prefix in the file path. For example, the original file path may be OldFolder/MyFile. After renaming, that same file will use the path NewFolder/MyFile.
- Some cloud platforms first create NewFolder. Then they move or copy the contents of OldFolder to New Folder. When all the contents of OldFolder are present in NewFolder, the cloud storage deletes OldFolder.

In any case, the larger the item, the longer the rename requires. For the largest files and folders, it may take several hours or even several days. AoC treats renaming as a background operation so you can continue working in Files while the operation completes.

During the renaming operation, AoC disables the folder to prevent further actions on OldFolder until renaming completes. Note that the folder is not disabled to other users who may have shared access to it. Aspera recommends that no one perform any operations on the folder and its contents until the renaming operation completes.

Once complete, AoC deletes OldFolder and displays NewFolder.

Note: You must refresh your Files listing to see NewFolder.

Identify the issue

If an anomaly occurs in the network or in cloud storage, the renaming may not complete. You know that renaming did not complete if you see either of these situations:

- After seven days, OldFolder still displays after you refresh the page.
- At any time, both OldFolder and NewFolder display. (Remember that, depending on folder names and the sort order you set for your Files listing, the two folders may be on different pages in the Files app.) In this case, folder content may be split between OldFolder and NewFolder. There may some content that exists in both folders.

Cloud storage will not lose any of your content in either case.

Troubleshoot

If after seven days Old Folder still displays after you refresh the page, perform the rename operation again.

If both OldFolder and New Folder display, do the following:

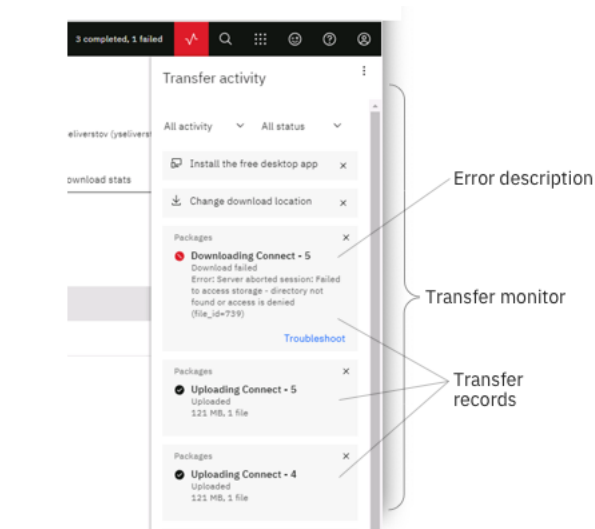
1. Determine which of the two folders contains the majority of the content. Consider item sizes as well as item count.
2. Move the content manually to the folder with the most content.
Note: For the items you move manually, you must restore the intended access permissions manually.
3. If in step 2 you moved content to OldFolder, try the rename operation again.

Irdeto watermarking integration

This topic lists codes and descriptions for errors that may display related to watermarking. It also includes a link to the Irdeto documentation that provides troubleshooting procedures for each error.

To configure your Irdeto integration, see [Watermarking: Integrate your Irdeto service](#). To apply watermarking to a package after the integration is complete, see [Sending: Detailed procedure](#).

Errors that may occur for the transfer of watermarked packages appear in the AoC transfer monitor, on the individual transfer record.



The table below lists watermarking-related errors that may occur. For troubleshooting procedures, see the [Irdeto documentation](#).

Error code	Error message
106	Service: Could not embed enough watermarks for proper detection
130	Service: Failed bits per sample validity check
131	Service: Failed Resolution validity check
132	Service: Failed Framerate validity check
133	Service: Failed Bitrate validity check
134	Service: Unsupported input file codec
165	Service: Task processing retries attempted but still failed
1001	Watermark: Invalid parameter value received
1002	Watermark: Embedder was forcefully interrupted
1003	Watermark: Not implemented
1007	Watermark: Input file not found
1008	Watermark: General IO error
1009	Watermark: Unsupported input format
1011	Watermark: No permissions to read input file
1013	Watermark: Corrupted stream
1014	Watermark: Cannot write variant file
3000	Unknown system error

Aspera Connect installation issues

Find troubleshooting procedures addressing Aspera Connect installation-specific issues.

- **[Overview: Aspera Connect installation troubleshooting](#)**
Use this topic to start troubleshooting issues with installing or running IBM Aspera Connect.
- **[Select a transfer method](#)**
Aspera on Cloud requires one of two transfer methods to power high-speed transfers between user desktops and Aspera transfer servers. Users can either download and install Aspera Connect, a free, lightweight, install-on-demand software program; or an admin can configure the IBM Aspera HTTP Gateway and attach it to your Aspera on Cloud organization.
- **[Connect prompt continues to appear](#)**
Once you download and install IBM Aspera Connect, the Connect installation prompt should no longer appear. However, there are two circumstances in which you may continue to see the installation dialog even though you've already installed Connect.
- **[Windows OS: Error when installing with a non-admin account](#)**
Use this procedure to troubleshoot an Aspera Connect installation on a Windows machine when you have a non-admin account.
- **[Windows OS: Connectivity issues](#)**
Use this procedure to troubleshoot an Aspera Connect installation on a Windows machine when you have connectivity issues.
- **[MacOS X: Connectivity issues](#)**
Use this procedure to troubleshoot an IBM Aspera Connect installation on MacOS.
- **[Linux: AppArmor prevents access to Connect](#)**
AppArmor is a Linux security module that uses mandatory access control (MAC) to restrict some applications' system access. It may prevent Connect from running correctly on some Linux systems.
- **[Linux: Connectivity issues](#)**
Use this topic to troubleshoot connectivity issues for Connect on Linux.

Overview: Aspera Connect installation troubleshooting

Use this topic to start troubleshooting issues with installing or running IBM Aspera Connect.

For your reference, the Connect installation process performs the following tasks:

- Installs the Connect browser extension.
- Downloads the Connect app.
- Installs the Connect app.

Before troubleshooting, make sure your Connect installation meets the requirements specified in the IBM Aspera Connect [user documentation and release notes](#), particularly with regard to the supported versions of operating systems, browsers, and (if Linux) OpenSSL.

In all cases, the first troubleshooting step is to run Aspera's web-based [Connect diagnostic tool](#) to get a preliminary assessment of your Connect installation. This diagnostic tool does the following:

- Reports the version number of your current Connect installation, if installed.
- Indicates whether your installed version is up to date.
- Checks whether Connect is running.
- Verifies whether your current version of Connect is compatible with your current browser.
- Tests your ports.
- Attempts to perform a test transfer.
- Generates a summary report that you can download and send to IBM Aspera support, if necessary.

Use the other topics in this section to further troubleshoot your Connect installation, according to the OS of your local machine. See also [IBM Aspera Connect common issues](#).

Select a transfer method

Aspera on Cloud requires one of two transfer methods to power high-speed transfers between user desktops and Aspera transfer servers. Users can either download and install Aspera Connect, a free, lightweight, install-on-demand software program; or an admin can configure the IBM Aspera HTTP Gateway and attach it to your Aspera on Cloud organization.

Aspera Connect is the default transfer method for Aspera on Cloud and other Aspera web apps. However, if your deployment of Aspera on Cloud does not allow users to download and install client software, you can configure an alternative transfer method: the [IBM Aspera HTTP Gateway](#). The Aspera HTTP Gateway is a standalone product that uses both HTTP/S and Aspera FASP to complete file transfers.

For details about Aspera Connect, see [Aspera Connect transfer client](#).

Connect prompt continues to appear

Once you download and install IBM Aspera Connect, the Connect installation prompt should no longer appear. However, there are two circumstances in which you may continue to see the installation dialog even though you've already installed Connect.

- There is a new version of Connect available, and the app prompts you to install the upgrade.
In this case, you must download and install the Connect app upgrade. You may or may not need to update your browser extension; the installation process will guide you.
- You have not installed the Connect extension in your current browser.
You may have installed the extension in a different browser, but the extension is required for each browser. In this case, there is no need to reinstall the Connect app, but you must install the browser extension. Find the appropriate installation procedure for your browser among these articles.

If you are not allowed to download and install software, the Aspera on Cloud administrator has configured the IBM Aspera HTTP Gateway for transfers. In this case, you can [disable Aspera Connect](#). Otherwise, you must download and [install the Aspera Connect transfer client](#), and install the Connect browser extension.

Windows OS: Error when installing with a non-admin account

Use this procedure to troubleshoot an Aspera Connect installation on a Windows machine when you have a non-admin account.

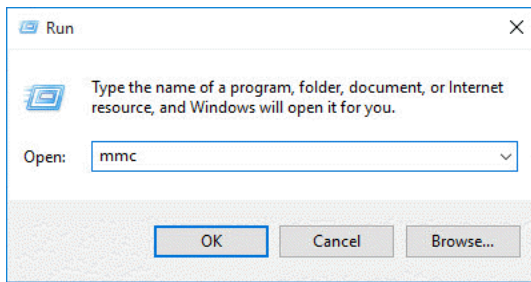
You may encounter an error such as the following (or with similar wording) if you are not an Administrator when executing the MSI installer file.

The system administrator has set policies to prevent this installation.

These error messages are due to not having permissions to install an MSI package as a non-admin account. Other than logging in as an administrator to install Connect, you may also ask that your Administrator grant the group policy access for non-admin users to install applications.

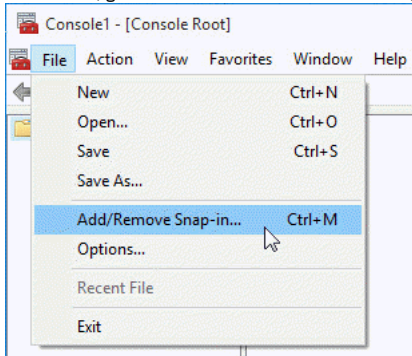
The following example shows you how to grant group policy access for non-admins to install software on Windows 2016:

1. Launch the Microsoft Management Console (MMC).
Go to **Start menu > Run**. Enter `mmc` and click **OK** to launch it.

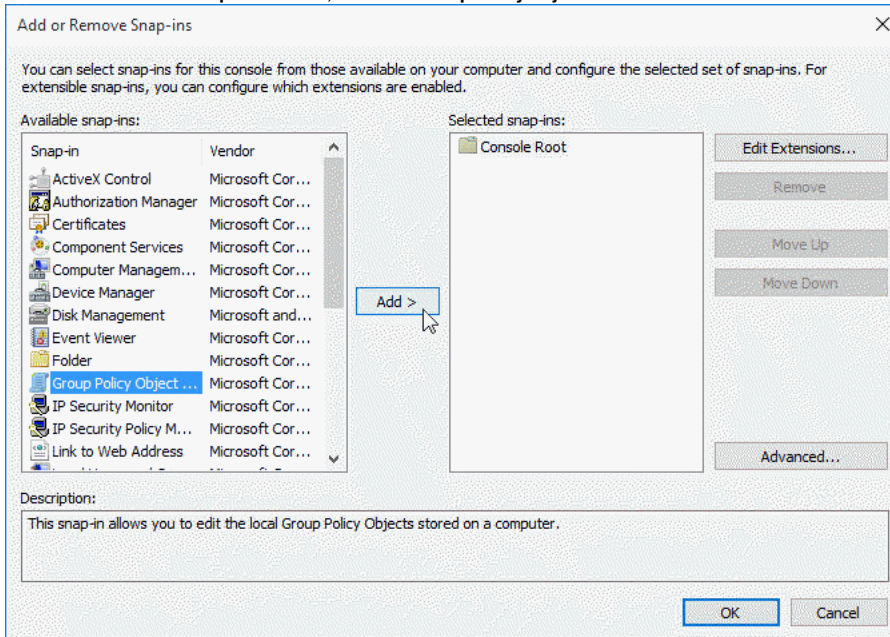


2. Add the Group Policy Object Editor Snap-in.

a. In the MMC, go to the toolbar and select **File > Add/Remove Snap-in:**



b. In the **Add or Remove Snap-ins** window, select the **Group Policy Object Editor** and click **Add:**

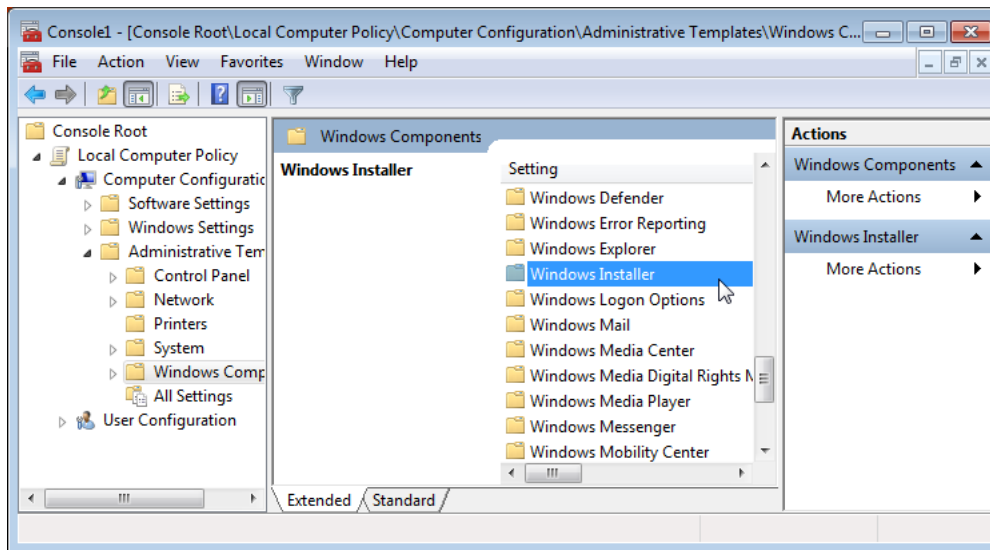


c. In the Select Group Policy Object window (wizard), under Group Policy Object, click **Browse** and select either **This Computer** or specify another computer. When done, click **OK** to return to the wizard window.

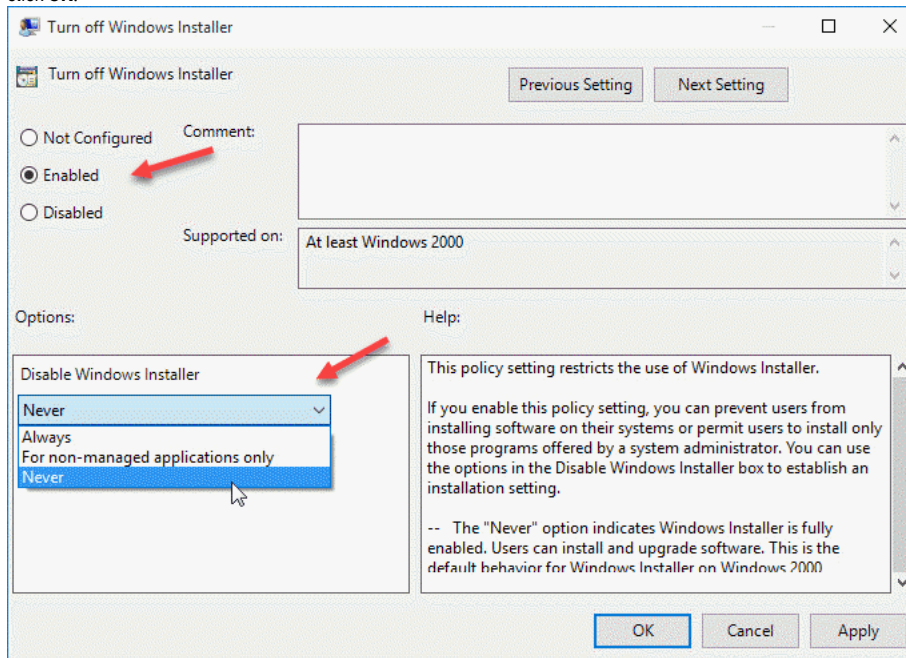
d. In the wizard window, click **Finish**. When you are returned to the **Add/Remove Snap-ins** window, click **OK** to save the changes.

3. Grant the Windows installation group policy.

a. In the MMC, navigate into **Console Root > Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components** and locate **Windows Installer:**



- b. Double-click **Windows Installer**.
- c. In the list that appears, locate **Turn off Windows Installer** and double-click it. The Turn Off Windows Installer window opens.
- d. Under the Turn off Windows Installer heading, select **Enabled**. In the Disable Windows Installer box, open the pull-down and select **Never**. When finished, click **OK**:



- e. To close the MMC, click **File > Exit**.
- f. When prompted to save console settings, click **Yes** to save the settings to a file. When prompted for a .msc filename, click **Save**.
- g. Reboot the computer to apply the changes, or execute the following command at a command prompt:

```
> gpupdate /force
```

Windows OS: Connectivity issues

Use this procedure to troubleshoot an Aspera Connect installation on a Windows machine when you have connectivity issues.

SSH connectivity errors: "Timeout establishing connection"

If you receive the error "Timeout establishing connection," the TCP connection between Connect and the server is blocked (error codes 13, 15, or 40 in the log files). To determine the cause, open a Terminal or a Command prompt on the client machine (where Connect is installed). Use **telnet** to test the connection to the server:

```
> telnet server-ip-address 33001
```

where *server-ip-address* is the IP address of the Aspera server (for example, 10.0.1.1) on TCP port 33001 (or the configured TCP port, if other than 33001).

You will receive one of the following errors and can take the appropriate action:

- **"Connection refused"**: The Aspera server is not running the SSHD service. Have your server administrator review the server's SSH service status.

- **"Timeout"**: The client-side firewall is disallowing outbound TCP traffic. Ensure that the client-side firewall allows outbound TCP traffic on port 33001 (or the configured TCP port).

UDP connectivity errors: "Data transfer timeout"

If Connect appears to successfully connect to the server but:

- The transfer progress reads 0%.
- Files appear to be transferred to the destination but are 0 bytes.
- You eventually receive the error "Data transfer timeout."

UDP connectivity is blocked, likely by the firewall configuration (error codes 14, 15, and 18 in the log files). Ensure that the client-side firewall allows outbound traffic on the FASP UDP port (33001, by default) and the server firewall allows inbound traffic on UDP port 33001.

IBM Aspera Connect diagnostic tool

Aspera provides a web-based diagnostic tool that can be useful for identifying connection issues. You can access the tool here:

<https://test-connect.asperasoft.com/>

MacOS X: Connectivity issues

Use this procedure to troubleshoot an IBM Aspera Connect installation on MacOS.

SSH connectivity errors: "Timeout establishing connection"

If you receive the error "Timeout establishing connection," the TCP connection between Connect and the server is blocked (error codes 13, 15, or 40 in the log files). To determine the cause, open a Terminal or a Command prompt on the client machine (where Connect is installed). Use `telnet` to test the connection to the server:

```
$ telnet server-ip-address 33001
```

where *server-ip-address* is the IP address of the Aspera server (for example, 10.0.1.1) on TCP port 33001 (or the configured TCP port, if other than 33001).

You will receive one of the following errors and can take the appropriate action:

- **"Connection refused"**: The Aspera server is not running the SSHD service. Have your server administrator review the server's SSH service status.
- **"Timeout"**: The client-side firewall is disallowing outbound TCP traffic. Ensure that the client-side firewall allows outbound TCP traffic on port 33001 (or the configured TCP port).

UDP connectivity errors: "Data transfer timeout"

If Connect appears to connect successfully to the server but:

- The transfer progress reads 0%.
- Files appear to be transferred to the destination but are 0 bytes.
- You eventually receive the error "Data transfer timeout."

UDP connectivity is blocked, likely by the firewall configuration (error codes 14, 15, and 18 in the log files). Ensure that the client-side firewall allows outbound traffic on the FASP UDP port (33001, by default) and the server firewall allows inbound traffic on UDP port 33001.

IBM Aspera Connect diagnostic tool

Aspera provides a web-based diagnostic tool that can be useful for identifying connection issues. You can access the tool here:

<https://test-connect.asperasoft.com/>

Linux: AppArmor prevents access to Connect

AppArmor is a Linux security module that uses mandatory access control (MAC) to restrict some applications' system access. It may prevent Connect from running correctly on some Linux systems.

To disable AppArmor, enter the following commands on the affected computer:

```
# /etc/init.d/apparmor stop
# update-rc.d -f apparmor remove
```

Linux: Connectivity issues

Use this topic to troubleshoot connectivity issues for Connect on Linux.

SSH connectivity errors: "Timeout establishing connection"

If you receive the error "Timeout establishing connection," the TCP connection between Connect and the server is blocked (error codes 13, 15, or 40 in the log files). To determine the cause, open a Terminal or a Command prompt on the client machine (where Connect is installed). Use `telnet` to test the connection to the server:

```
# telnet server-ip-address 33001
```

where *server-ip-address* is the IP address of the Aspera server (for example, 10.0.1.1) on TCP port 33001 (or the configured TCP port, if other than 33001).

You will receive one of the following errors and can take the appropriate action:

- **"Connection refused"**: The Aspera server is not running the SSHD service. Have your server administrator review the server's SSH service status.
- **"Timeout"**: The client-side firewall is disallowing outbound TCP traffic. Ensure that the client-side firewall allows outbound TCP traffic on port 33001 (or the configured TCP port).

UDP connectivity errors: "Data transfer timeout"

If Connect appears to successfully connect to the server but:

- The transfer progress reads 0%.
- Files appear to be transferred to the destination but are 0 bytes.
- You eventually receive the error "Data transfer timeout."

UDP connectivity is blocked, likely by the firewall configuration (error codes 14, 15, and 18 in the log files). Ensure that the client-side firewall allows outbound traffic on the FASP UDP port (33001, by default) and the server firewall allows inbound traffic on UDP port 33001.

IBM Aspera Connect diagnostic tool

Aspera provides a web-based diagnostic tool that can be useful for identifying connection issues. You can access the tool here:

<https://test-connect.asperasoft.com/>

Specific error messages

This article describes troubleshooting options for some specific error messages.

Aspera Connect is unavailable

- Recommended action: Download and install IBM Aspera Connect. See [Installing Aspera Connect](#).
- More information: See [IBM Aspera Connect common issues](#).

Unable to load files

- Recommended action: Check with the person who sent you the link. The link may be expired or deleted; or the person who sent you the link may have changed your access permission.
- More information: If you used a browser bookmark to access the files, the location of the files may have changed.

Unable to load requested folder

- Recommended action: Check with the person who shared the folder with you. The person who shared it may have changed your access permission.
- If AoC redirects you to your Files home folder, check with your local technical support staff. Click the Help icon and select "Technical support".

Unable to get package or Unable to show package details

- Recommended action: If you used a link to access the package, the link may have expired or been deleted; or the person who sent you the link may have changed your access permission. Check with the person who sent you the link.
- More information: The package may have been deleted. Check with the person who sent you the package.

Unable to get files information

- Recommended action: Check with the person who gave you permission to access the files.
- More information: You are not authorized to access the item. Your link to the item may be expired or deleted, or your permission to it may have been changed by sender or sharer.

Failed to open TCP connection for SSH

- Recommended action: Use the [Aspera Connect diagnostic tool](#) to run a test transfer and return diagnostic information.
- More information: The most common cause of this error is that firewall settings do not allow traffic on port 33001, which is required for Aspera FASP transfers. See also [Firewall considerations](#) on the IBM Support site.

Client unable to connect to server

- Recommended action: Use the [Aspera Connect diagnostic tool](#) to run a test transfer and return diagnostic information.
- More information: The most common cause of this error is that firewall settings do not allow traffic on port 33001, which is required for Aspera FASP transfers. See also [Firewall considerations](#) on the IBM Support site.

Verify contents and resend

- For the recommended action and more information, see [Resending "Draft" packages](#).

To contact your local tech support administrator, click the Help icon in the banner and select "Technical support".

Get IBM technical assistance

Find answers to questions about eligibility for technical support, registering with IBM Support, opening cases, subscribing to Support notifications, and other IBM Support resources.

- [Who is eligible for technical assistance?](#)
If you are eligible for and registered with IBM Support, you can contact IBM Support to open a technical support case. If you are not eligible for IBM Support, click the Help icon in the upper black banner and select Technical support to contact your local support staff.

- [Register for technical assistance](#)
For those who are eligible, this page describes how to register with IBM Support and how to file a support request.
- [Open a case](#)
If you are registered as a *contact* with IBM Support, you can open a support case.
- [Subscribe to notifications](#)
You can subscribe to Aspera on Cloud announcements and status information.
- [Resources](#)
The IBM Support web site offers numerous videos, FAQs, and guides to help you succeed with Aspera on Cloud.

Who is eligible for technical assistance?

If you are eligible for and registered with IBM Support, you can contact IBM Support to open a technical support case. If you are not eligible for IBM Support, click the Help icon in the upper black banner and select Technical support to contact your local support staff.

Eligibility for IBM Support

Employees of the company that purchased Aspera on Cloud (AoC) are eligible to be *contacts* on the IBM Support Community portal. Contacts can open and manage cases with the IBM Support team.

One of the contacts listed for the company must act as the Support Administrator. This Support Administrator must [approve or deny employee requests](#) to register as a contact.

AoC users who are not employees of the company that purchased AoC are not eligible to be contacts. They cannot open and manage cases with IBM Support.

The company that purchased AoC must provide technical support to users who are not contacts. See [Configure technical support for your users](#).

If that technical support cannot resolve a technical issue, a contact should open a case with IBM Support.

Using a trial version of Aspera on Cloud?

If you are using a trial version of Aspera on Cloud and need technical support, send an email to aspera-sales@ibm.com. A representative will help you.

Register for technical assistance

For those who are eligible, this page describes how to register with IBM Support and how to file a support request.

First-time users of IBM Support must set up their access to support resources:

Go to <https://www.ibm.com/mysupport/s/article/User-Administration>.

If you have any problems configuring your support access, contact the IBM Help Desk. Use either of the following methods to contact the Help Desk:

- Click "Report a problem submitting a case or registering for support." You'll find this link at the bottom of all pages in the IBM Support Community.
- Send an email requesting assistance to mysphelp@us.ibm.com.

Open a case

If you are registered as a *contact* with IBM Support, you can open a support case.

To determine whether you are eligible to be a contact, see [Who is eligible for technical assistance?](#)

Collect relevant data such as URL, IDs (for workspace, user, shared inbox, and so on), and screenshots. From the Help menu , select Download support data. Attach these items to the Support case.

1. Go to <https://www.ibm.com/mysupport>.
2. Log in with your IBMid to access your own support account.
If you do not have an IBMid, you can sign up for one at <https://www.ibm.com/account/us-en/signup/register.html>.
See also the video tutorial [How to Create an IBMid](#).
3. Click **Open a case**.
Attach the supporting data you collected to the case. Include the file available from Help > Download support data.

Note: If you don't see Open a case, contact your Support Administrator to request that your IBMid be enabled to open support tickets.

Subscribe to notifications

You can subscribe to Aspera on Cloud announcements and status information.

Receive AoC announcements from IBM Support *My Notifications*

You can subscribe to the IBM Support notifications service for Aspera on Cloud. The *My Notifications* service sends emails alerting you to scheduled maintenance windows, API changes, support incidents, product and documentation updates, and more. You can customize the notification types you receive and the frequency at which you receive them.

For subscription instructions, go to <https://www.ibm.com/support/pages/node/6123669>. Be sure to subscribe specifically to IBM Aspera on Cloud notifications. You can subscribe to other IBM product notifications as well.

Subscribe to AoC status information

IBM Aspera provides an up-to-date status page with current system status and performance, along with planned maintenance windows and known issues. You can subscribe to status notification updates if you wish. Go to <https://status.aspera.io>.

Resources

The IBM Support web site offers numerous videos, FAQs, and guides to help you succeed with Aspera on Cloud.

Support portal videos

The following short videos will help you use the Support Portal effectively:

- Video: [Introducing the Customer Support Portal](#)
- Video: [Open and Manage Cases](#)
- Video: [Search the IBM Support Community](#)

Additional resources

- [Aspera support resources and FAQs](#)
- [IBM Support Guide](#)
- [Set up IBM Support](#)
- [Manage your Support account access](#)
- [Manage Support access requests](#)
- [Developer support](#)
- [Download IBM Aspera software](#)

Error code reference

A link to reference tables with information about IBM Aspera error codes.

When using Aspera on Cloud, you may encounter different error codes. The Error code reference tables summarize each error and provide a description to better understand what each of them mean. To access this information refer to the [Error code reference tables](#) from the IBM support page.

Integration and APIs

Integrate your AoC organization with other Aspera products like transfer clients and servers. Integrate your IBM Key Protect KMS or your Irdeto watermarking service. Register an API client to build your own integration.

- [Registering an API client](#)
For developers building clients, this topic contains the procedure to register your client for use of the Aspera on Cloud API.
- [Watermarking: Integrate your Irdeto service](#)
Forensic watermarking is an anti-piracy solution to prevent and trace illegal content redistribution and security breaches. This article describes how to integrate your Irdeto watermarking service with Aspera on Cloud. After integration, Packages app users can apply watermarking when sending digital packages.
- [Bring your own key for server-side encryption at rest](#)
You can bring your own key to protect your data in storage attached to your AoC organization. This article describes how to bring your own key by integrating your key-management service (KMS) with AoC.
- [Transfer Clients](#)
Learn how to integrate the other IBM Aspera transfer clients beyond Aspera Connect: IBM Aspera mobile app, Aspera CLI, or Aspera desktop client. Or get desktop access to Aspera on Cloud content without using the browser.
- [Transfer Servers](#)
Transfer to the Cloud with the Aspera HST server or HST endpoint GUI.
- [Aspera APIs](#)
Using Aspera on Cloud APIs means using endpoints from several API collections. This article links to all related APIs, SDKs, and Developer Guides in the IBM API Hub.

Registering an API client

For developers building clients, this topic contains the procedure to register your client for use of the Aspera on Cloud API.

See also [IBM Aspera Developer Center](#).

Note: IBM Aspera provides a full suite of APIs to support customer integrations. Always use the Aspera APIs to build integrations. Do not build integrations using application URLs or other methods.

Registering a client that uses browser-based authentication

If your client uses browser-based (authorization code grant flow) authentication, you can configure whether or not the browser prompts users of your client explicitly to grant your client access Aspera on Cloud. If not, your users are not prompted and permission is assumed.

To register your API client for browser-based authentication, do the following:

1. In the Admin application, select Integrations > API clients.
2. Click Create new.
3. Enter the name of the client; this name is for your reference only and does not need to match the actual name of your app.
4. Select the check box labeled Users must explicitly allow the client to access IBM Aspera on Cloud if you want Aspera on Cloud to present a dialog box to your application users asking them to allow your client application to access Aspera on Cloud for contacts and other resources.
5. In the Redirect URIs field, enter the redirect URIs for your application, separating multiple URIs with commas.
A redirect URI (protocol-host-port) is an absolute URI invoked after the authorization flow to return the user to the client app. For more information, refer to the Aspera on Cloud API documentation on the [IBM API Hub](#).
6. In the Origins field, enter the origins for your app, separating multiple origins with commas.
An origin is the URI or protocol-host-port of the client app initial login page, from which the user must arrive to the authentication flow.
7. Click Save.

Result: Aspera on Cloud completes registration of your client app, then generates and displays the client ID and secret you need to access the API.

Registering a client that uses JWT authentication

Aspera on Cloud supports the JSON Web Token-based OAuth 2.0 grant type (a grant type specifies how a client interacts with an identity server to authorize access to protected resources) to enable client applications to use the API without a user having to log in from a web browser.

A JSON web token includes, among other things, a user ID (the email of the user to authenticate), and is signed with a valid private key. In response to a valid JWT request submitted to the API, AoC returns an access token for the user identified in the JWT token request. Further requests to the API must include this access token to be valid. Requests as a specific user are permitted according to that user's permissions and access in the Aspera on Cloud application.

Note: JWT authentication for a given Aspera on Cloud user requires either a user-specific public/private key pair, or a client-level 'global' (not user-specific) public/private key pair, depending on your configuration. Creating a public/private key pair is a simple, standardized process; search the web for a procedure appropriate to your platform.

Retrieving admin tokens

You can enable users of this client who are organization administrators to retrieve admin-scoped node access tokens from the API. Such a token provides the user with admin privileges on the node itself. See the procedure below.

Users and keys

You must configure which users can access the API using your client, and which key – either a user-specific key or a global key – each user can submit to retrieve an access token.

There are two configuration parameters for users and keys.

- Users:
 - All users: All users in the Aspera on Cloud organization are eligible to retrieve an access token.
 - Only listed users: Only users you list are eligible to receive an access token.
- Keys:
 - User-specific keys: The JWT must be signed with the specified user's own private key.
 - User-specific keys and global key: The JWT can be signed with the specified user's own private key or with the global private key. (The global key is tied to the client just as the user-specific key is, but the global key can be applied to all users.)

Note: Any user accessing the Files API using the JWT method must have their public key listed in their Aspera on Cloud user record. The user can enter their own public key using the Account settings option of the User menu, or the organization administrator can enter the user's public key in the individual user's record.

Important: API clients with a global key can retrieve access tokens for and act as any listed user. Use global keys according to local site security practice.

The Users and Keys parameters interact with each other to enable various valid combinations, as the table below indicates:

	User-Specific Key	User-Specific Key and Global Key
All Users	API clients can request access as any Aspera on Cloud user. A valid request for access token must: • Contain the user ID of any Aspera on Cloud user. • Be signed by that user's private key.	API client can request access as any Aspera on Cloud user. A valid request for access token must: • Contain the user ID of any Aspera on Cloud user. • Be signed by that user's private key or by the global private key.
Only Listed Users	API client can request access as any eligible (listed) Aspera on Cloud user. A valid request for access token must: • Contain the user ID of a listed Aspera on Cloud user. • Be signed by that listed user's private key.	API client can request access as any eligible (listed) Aspera on Cloud user. A valid request for access token must: • Contain the user ID of a listed Aspera on Cloud user. • Be signed by that listed user's private key or the global private key.

Procedure

To configure JWT authentication for your registered client application, do the following:

Note: This procedure assumes that you have already entered the public keys required in the appropriate user record. To add a key to your own user record, see [Add your public key](#). If you are an admin, see [Create and manage users](#) to update your record or another user's record with a public key.

1. When viewing your integration, click JSON Web Token Auth.
2. Select Enable JWT grant type.
3. To enable administrative users of this client to retrieve an administrator-scoped client, select the check box labeled Enable AoC administrators to retrieve a transfer node token that grants node administrator permissions.
4. Select which keys your API client can use to retrieve tokens for the users you specify in the next step:
 - a. To allow your API client to use only the user-specific keys for the users listed below, select User-specific keys.
 - b. To allow your API client to use either user-specific keys or a global key to retrieve access tokens, select User-specific keys and global key. In the text box that appears, enter the global public key.
5. Select the users for which your API client can retrieve access tokens:
 - a. To allow your API client to retrieve tokens for all users in the Aspera on Cloud organization, select All users.
 - b. To restrict your API client to retrieving tokens for a specific list of users or groups, select Only selected users and enter the user names or group names in the text box.
6. Click Save.

Managing registered clients

You can retrieve your client ID and secret, display and update details for any registered client, and delete a client.

1. In the Admin application, select Integrations > API clients.
2. To delete a client, right-click the row and select Delete; then confirm deletion.
3. To open any client record and display the client ID and secret, click the row.
4. Edit other fields as required, then click Save.
5. To delete this client, click Delete, then confirm deletion.

Watermarking: Integrate your Irdeto service

Forensic watermarking is an anti-piracy solution to prevent and trace illegal content redistribution and security breaches. This article describes how to integrate your Irdeto watermarking service with Aspera on Cloud. After integration, Packages app users can apply watermarking when sending digital packages.

It's important that you work with your Irdeto representative to set up proper access between your Irdeto service and your AoC nodes. Aspera cannot validate that you have configured your Irdeto service correctly.

Once that access is properly configured, use the Aspera on Cloud Admin app to configure watermarking for your organization and for the specific workspaces in which you want watermarked packages. The Admin app UI flow accomplishes these actions:

1. Create a watermarking profile.
Name the profile that maps your Irdeto service to AoC.
2. Associate the watermarking profile with a [node](#) attached to your organization.
You can attach any watermarking profile to one or more nodes. (A node is your cloud storage bucket that you've attached to your AoC org.)
3. Enable watermarking for the AoC Packages application in each workspace where you want watermarking available.
Once enabled, you can make watermarking required for every package sent from that workspace, or you can allow workspace members to choose whether to apply watermarking to individual packages they send.
For the Packages app user procedure showing how senders can apply watermarking, see [Sending: Detailed procedure](#). For a more in-depth treatment, see the relevant section in [Sending: Become an expert](#).

For step-by-step instructions, see "Configure watermarking in Aspera on Cloud" later in this article.

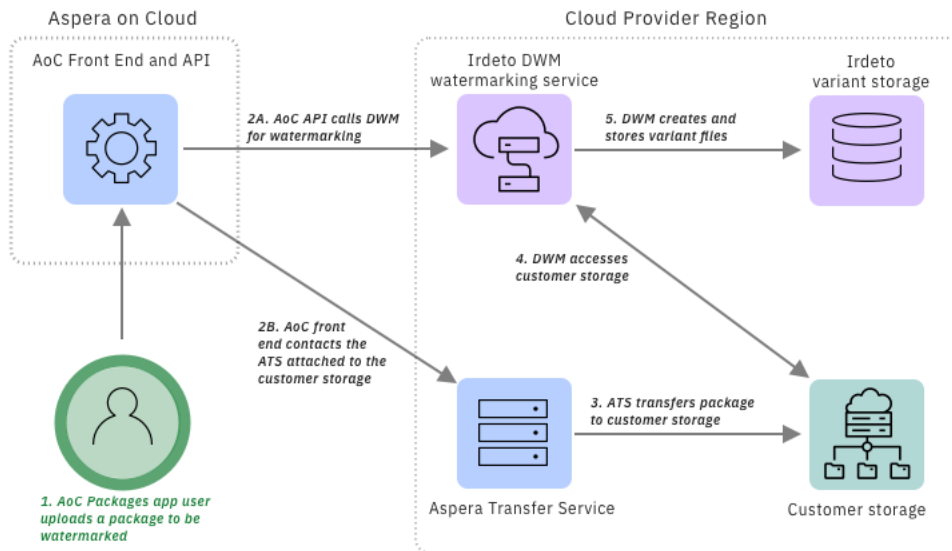
Watermarking with Irdeto in Aspera on Cloud

Watermarking combats piracy by applying an invisible yet traceable 'signature' on digital files. The watermark allows you to track that asset through the development and distribution process.

Each time an AoC user downloads a watermarked file, Irdeto updates the watermark to indicate the specific user who downloaded it. If a user who downloads a watermarked file then forwards the file using some mechanism other than AoC, the file retains the watermark identifying the user who downloaded it.

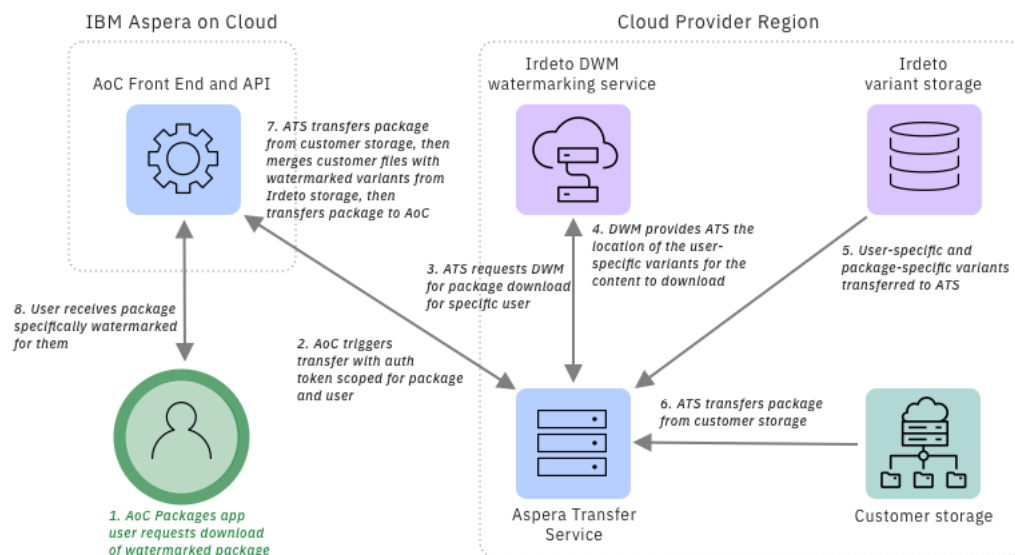
The following drawing is a schematic representation of the package upload workflow for your integration of Irdeto with AoC.

Upload a package for watermarking



The following drawing is a schematic representation of the package download workflow for your integration of Irdeto with AoC.

Download a watermarked package



Prerequisites

Work with your Irdeto representative to establish the following:

- The DWM (distributed watermarking) service API endpoint address(es) that are local to your cloud storage location(s).
- The tenant ID for your organization.
- Read-only access permissions from Irdeto to your storage.

Important: AoC cannot validate that your Irdeto service is configured correctly. You must work with Irdeto to validate your Irdeto implementation.

Cloud and node support

This section details support and constraints for Irdeto watermarking in Aspera on Cloud.

- Supported cloud platforms
 - AWS S3
 - N. Virginia (us-east-1); Oregon (us-west-2); N. California (us-west-1)
 - Sao Paulo (sa-east-1)
 - Ireland (eu-west-1); London (eu-west-2); Frankfurt (eu-central-1)
 - Tokyo (ap-northeast-1); Singapore (ap-southeast-1); Sydney (ap-southeast-2)
 - GCS
 - us-central1

Note: Your Irdeto account and your associated cloud storage must be in same provider region. See [Irdeto documentation](#) for more information.

- Supported [Aspera node type](#): Aspera-managed auto-scale clusters (ATS).
- You can enable watermarking only on nodes that do *not* have encryption at rest (EAR) applied.
 - This EAR constraint includes both cloud-provider server-side encryption and Aspera-provided encryption-at-rest (whether Aspera or your own KMS manages the root key).
 - If you are unsure whether a node is enabled for encryption at rest, Aspera recommends creating one or more new nodes to support your organization's watermarking needs.
 - For supporting documentation, see [Use Aspera-managed keys for server-side encryption at rest](#); [Bring your own key for server-side encryption at rest](#).

Using watermarking in Aspera on Cloud

This section describes how Packages app users can work with the watermarking capabilities you configure.

Watermarking applies to content in the AoC Packages app only.

Receiving a watermarked package

Recipients of watermarked packages must log in to retrieve the package. Traceability using forensic watermarking requires that users in the content workflow be authenticated. Therefore, recipients cannot download a watermarked package from a public link.

Recipients must download watermarked packages using the Aspera on Cloud Packages app with [IBM Aspera Connect](#).

File types and profiles supported

In a watermarked package, watermarking applies only to files that conform to supported profiles. Profiles comprise not only the supported file types (.ts; .ps; .mpg; .mpeg; .mov; .mxf; .mp4), but codecs, dimensions, and more; see the [Irdeto watermarking service documentation](#) for requirements.

GCS caveat

Ensure that watermarked packages do not contain files from Google Cloud Storage (GCS) that have special characters in file names.

Package actions

- [Recalled packages](#): You cannot recall a watermarked package.
- [Forward packages](#): You cannot forward a watermarked package.
- [Save to Files app](#): You cannot use the Actions menu to save a watermarked package to the Files app.
- [Add recipients to a package](#): When you add recipients to a watermarked package, the new recipients receive packages with their watermark. Adding recipients generates an immediate notification to the new recipients.
- [Draft packages](#): If a transfer fails to start, AoC moves the package to the Drafts folder. You cannot change the watermarking setting for a package in the Drafts folder.

Configure watermarking in Aspera on Cloud

To complete this procedure, you need the following:

- The name of the workspace in which you want members to send watermarked packages.
 - The node secret for the node that contains the workspace in which you want members to send watermarked packages.
 - These parameters from your Irdeto account:
 - Storage provider
 - Storage provider region
 - DWM API endpoint
 - Tenant ID
1. Create a watermarking profile.
 - a. In the Admin app, go to Integrations > Watermarking > Create new.
 - b. Give this profile a name and add a description if you wish.
 - c. In the following fields, select your cloud provider and region, then enter your Irdeto DWM API endpoint and Tenant ID.
 - d. Click Create.

AoC displays a list of nodes available to use with the Irdeto account you specified in the profile.
 2. Associate the profile with a node.
 - a. From the list of nodes, select the node hosting the workspace in which you want members to send watermarked packages.
 - b. Enter the [node secret](#), then click OK.

The list of available workspaces on that node appears.
 3. Enable watermarking for Packages in a workspace.
 - a. In the list of workspaces that appears, click the intended workspace to display a configuration window.
 - b. Set the toggle labeled Watermarking enabled to On.
 - c. Set the toggle labeled Watermarking required.

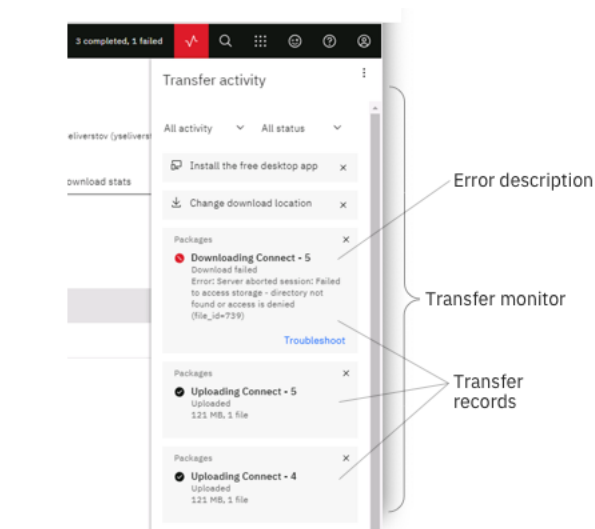
Select Yes to make watermarking automatic for every package sent from this workspace.

Select No if you want workspaces members to choose whether to apply watermarking to a given package as they send it.

Note: As noted previously in this article, recipients of a watermarked package *must* log in to AoC to download the package. Does this workspace allow members to send to external users? If yes, and you select Required, you must also check the Packages app setting Require external users to log in when receiving packages. An external user who does not log in cannot download watermarked package contents. See [Require external users to log in](#).
 4. Click Save.

Troubleshooting

Errors that may occur for the transfer of watermarked packages appear in the AoC transfer monitor, on the individual transfer record.



The table below lists watermarking-related errors that may occur. For troubleshooting procedures, see the [Irdeto documentation](#).

Error code	Error message
106	Service: Could not embed enough watermarks for proper detection
130	Service: Failed bits per sample validity check
131	Service: Failed Resolution validity check
132	Service: Failed Framerate validity check
133	Service: Failed Bitrate validity check
134	Service: Unsupported input file codec
165	Service: Task processing retries attempted but still failed
1001	Watermark: Invalid parameter value received
1002	Watermark: Embedder was forcefully interrupted
1003	Watermark: Not implemented
1007	Watermark: Input file not found
1008	Watermark: General IO error
1009	Watermark: Unsupported input format
1011	Watermark: No permissions to read input file
1013	Watermark: Corrupted stream
1014	Watermark: Cannot write variant file
3000	Unknown system error

Bring your own key for server-side encryption at rest

You can bring your own key to protect your data in storage attached to your AoC organization. This article describes how to bring your own key by integrating your key-management service (KMS) with AoC.

When you apply Aspera's server-side encryption at rest (SSEAR), you can choose either of two key-management strategies. You can use [Aspera's native key-management](#) function, or you can manage your own key by integrating a key-management service with AoC. In both cases, Aspera protects your data using a two-tier, AES-based encryption hierarchy.

When you bring your own key, it remains under your independent management the entire time. You use your KMS to protect and control your key, perform key rotation, key deletion, all other key-management functions. Your own key is never accessible to Aspera.

To bring your own key, you integrate your KMS with AoC by creating a KMS profile in AoC. Then you associate the profile with a node attached to your AoC organization.

Envelope encryption

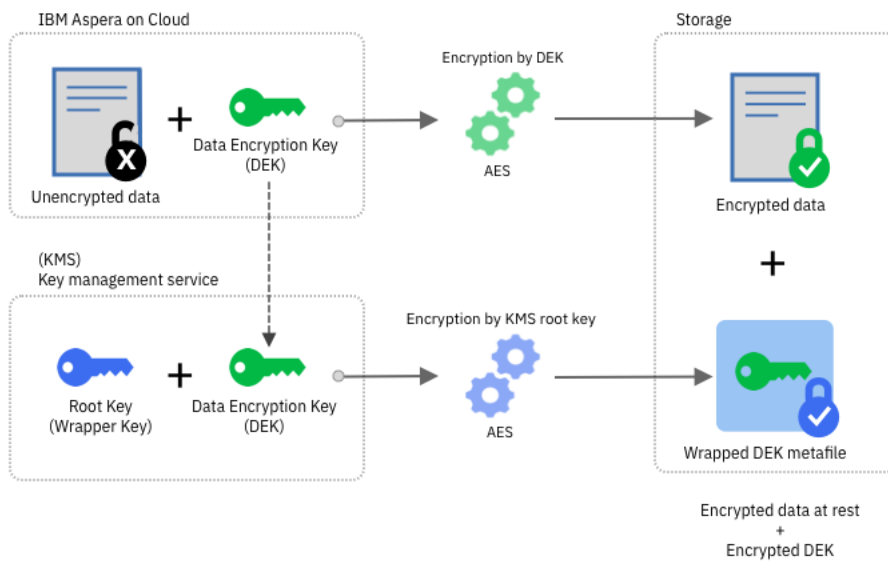
Aspera SSEAR uses *envelope encryption* to protect your content. Envelope encryption is the practice of encrypting data with a *data encryption key*, and then encrypting the data encryption key with a highly secure *key-wrapping key*.

The key you bring is key-wrapping key, also called the root key. The root key is independently managed by you using your KMS. The root key is never available to or under the control of Aspera.

When you apply envelope encryption using your own key, Aspera stores your encrypted data and the encrypted DEK in your cloud storage. Aspera never stores unencrypted DEKs and never has access to your root key in your KMS.

This double-encryption model combines the strengths of the AES algorithm with the inherent separation of key-management roles required for high-quality security.

Envelope encryption

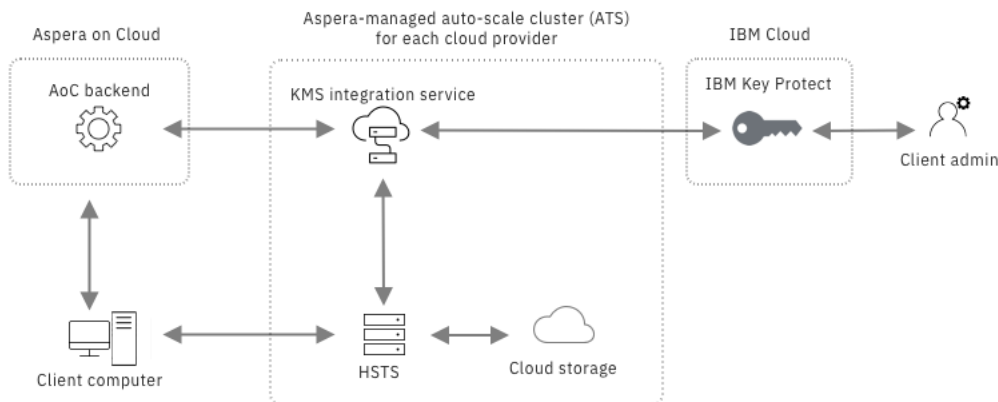


Using Your KMS with Aspera on Cloud

You can integrate your IBM Key Protect key-management service with Aspera on Cloud so that you can "bring your own key" for envelope encryption.

The following drawing is a schematic representation of the AoC/KMS integration architecture integration with IBM Key Protect.

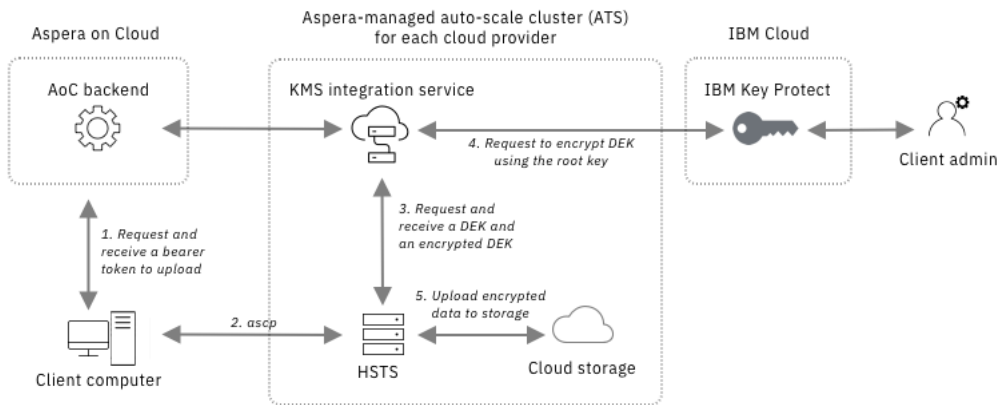
Architecture



The new Aspera KMS integration service interacts with both the AoC backend and the HST server in the Aspera-managed auto-scale cluster (ATS). It also interacts with your IBM Key Protect account using your IBM IAM with a service ID API key in the IBM Cloud. The following drawings show the upload and download workflows, illustrating the specific interactions among all these elements.

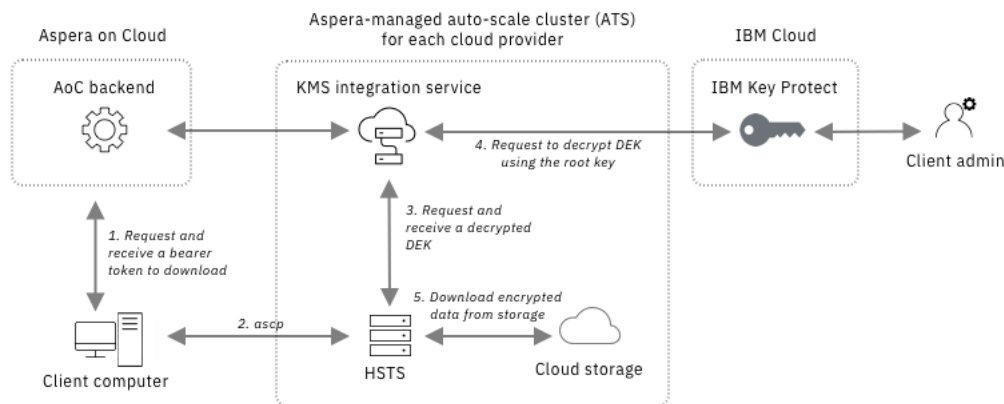
This drawing shows the end-to-end upload workflow.

Upload workflow



The download workflow reverses the process, as shown in the next diagram.

Download workflow



Implementation notes

- Supported KMS: [IBM Key Protect](#).
- Support for KMS key rotation.
- Supported storage types:
 - [IBM Cloud](#)
 - [AWS S3](#)
 - [Microsoft Azure](#)
 - [Google Cloud Storage](#)
- Supported Aspera node type: Aspera-managed auto-scale clusters (ATS).
- You can apply Aspera SSEAR in addition to or instead of encryption options offered by your cloud provider.
- You can enable encryption only on nodes that are not configured for watermarking. This applies to both Aspera SSEAR and cloud-provider encryption. See [this article](#) for details.

Prerequisites

- IBM Key Protect instance. Set the "Allowed network policy" to `public-and-private` (this is the default setting).
- IBM IAM authentication using Service ID API Key.

KMS provider specifications

To complete this task, you need the following information from your IBM Key Protect account.

Value	Definition	Example
KMS endpoint	The Key Protect service endpoint. The API endpoint to use when you connect to the Key Protect API.	<code>https://us-east.kms.cloud.ibm.com</code>
Key Protect Instance ID	The unique identifier assigned to your Key Protect service instance.	<code>ra385699-3d6f-47d4-8239-56b7890e5f73</code>
Root key ID	The unique identifier for the root key to use for encrypting and decrypting (wrapping and unwrapping) the DEK.	<code>41aed334-923f-4b6d-8d67-13e1f6c019b3</code>
API key	The key that AoC submits to Key Protect to be authenticated and be granted access. Aspera recommends that you use <i>Service ID API keys</i> . Aspera also supports <i>User API keys</i> .	<code>8uEy9TUDVtUHUGXpsMlpTb4rp8B_ZEfjU28ujik_nyw</code>

Procedures

To encrypt content using the root key in your KMS you must create at least one AoC KMS profile. Then you must associate the profile with a node attached to your organization. You can associate a profile with an existing attached node as long as you have not previously applied Aspera encryption-at-rest to it. You can also associate a profile with a new node during node creation.

KMS profile configuration notes

- Give each profile a unique name.
- You can associate any given profile with multiple nodes. Any given node can have only one KMS profile associated with it.
- You can update an existing profile by changing the profile name and API key, but you cannot update other profile settings.
- To protect your access to existing encrypted data, you cannot delete a KMS profile if you have associated it with any nodes. You must first [delete the associated nodes](#). Then you can delete the profile. Right-click a profile row and select Delete.

To complete this procedure on an existing attached node, you need the access key secret. You can also create a new access key. See

1. Create a KMS profile.
 - a. Go to Admin > Integrations > Third-party > Key-management services.
 - b. Click Create new to open the Key-management service profile page.
 - c. Give this profile a unique name.
 - d. Select your KMS provider.
 - e. Enter the required data into the form, according to the specifications of your KMS provider.
 - f. Click Save.
2. Apply the KMS profile to the node to encrypt.
 - a. Go to Admin > Nodes and storage > Nodes.
 - b. Select the intended node by clicking the node row.
 - c. Enter the access key secret and click Log in.
 - d. In the Details tab, go to Aspera encryption at rest.
 - e. In the Key-management method field, select Use my Key-management service.
 - f. In the following field, select the KMS profile to apply.
 - g. Click Save.

Once you complete these procedures successfully, all data you upload to this node will be protected using envelope encryption.

Note: Once you apply encryption at rest, you cannot remove or change it.

Note: Encryption applies only to new data that you upload after you apply encryption. Data that exists on the node before you encrypt remains unencrypted.

Transfer Clients

Learn how to integrate the other IBM Aspera transfer clients beyond Aspera Connect: IBM Aspera mobile app, Aspera CLI, or Aspera desktop client. Or get desktop access to Aspera on Cloud content without using the browser.

- [Desktop access to AoC using IBM Aspera for desktop](#)
IBM Aspera for desktop allows users to access their Aspera on Cloud content directly from the desktop without using a browser.
- [IBM Aspera mobile app](#)
You can link your existing Aspera on Cloud account to the IBM Aspera mobile app. Then you can use the mobile app for uploads, downloads, and other transfers. Available for both iOS and Android, the mobile app supports all features of the Aspera on Cloud web application.
- [Command Line Interface \(CLI\)](#)
To interact with Aspera on Cloud from the command line, download IBM Aspera Command-Line Interface (CLI) version 4.0 or newer, which is freely available.
- [Transfer to cloud with Desktop Client, HST Server, or HST Endpoint GUI](#)
You can use the IBM Aspera Desktop Client (freely available), IBM Aspera High-Speed Transfer Server, or IBM Aspera High-Speed Transfer Endpoint GUI to transfer to and from your object storage.

Desktop access to AoC using IBM Aspera for desktop

IBM Aspera for desktop allows users to access their Aspera on Cloud content directly from the desktop without using a browser.

When Aspera for desktop is connected to IBM Aspera on Cloud you can perform the following tasks from the Connect Remote View:

- Browse the contents of your Aspera on Cloud workspace.
- In your Aspera on Cloud Files app:
 - Upload and download files and folders.
 - Synchronize local folders with folders on the remote transfer server. You can sync in three directions: remote to local (pull); local to remote (push), and bi-directionally.
- In your Aspera on Cloud Packages app:
 - Send files and folder in a digital package, to another user or to shared inbox.
 - Download package that you receive in your personal inbox or in shared inboxes.
 - Schedule automated package downloads.

IBM Aspera mobile app

You can link your existing Aspera on Cloud account to the IBM Aspera mobile app. Then you can use the mobile app for uploads, downloads, and other transfers. Available for both iOS and Android, the mobile app supports all features of the Aspera on Cloud web application.

Important: Depending on the version of Aspera client you are using, the client may only support DSA keys for SSH authentication, or include a DSA key in addition to the RSA key. DSA keys are deprecated and the transfer servers won't be supporting this type of keys in the future.
Find IBM Aspera for [iOS](#) in the Apple App Store and for [Android](#) in the Google Play Store.

You must have an existing account with credentials in your Aspera on Cloud organization.

To add your Aspera on Cloud account to IBM Aspera, do the following:

1. Download and install IBM Aspera from Google Play or Apple App Store.
2. Open the app and accept the IBM privacy policy.
3. Tap Link account and select Aspera on Cloud.
4. Enter your organization subdomain.
For example, if your Aspera on Cloud URL is `https://bestapp.ibmaspera.com`, you should enter `bestapp`.
5. Click Connect.

Command Line Interface (CLI)

To interact with Aspera on Cloud from the command line, download IBM Aspera Command-Line Interface (CLI) version 4.0 or newer, which is freely available.

You use the `ascli` command line tool in a shell to perform the following actions using a command line:

- perform administrative tasks
- run high-speed transfers
- browse, rename or delete files and directories
- send or receive packages

Access is authorized using a private key.

Prerequisites

- Install the `ascli` command line tool following installation instructions in the [IBM Aspera CLI manual](#), including `ascp`.
Note: There are several options available for installation.
- Use the wizard to configure the CLI for use with Aspera on Cloud, following the instructions in the [IBM Aspera CLI manual](#).

Packages app

Follow the instructions as described in the [IBM Aspera CLI manual, packages section](#).

Files app

Follow the instructions as described in the [IBM Aspera CLI manual, files section](#).

Admin app

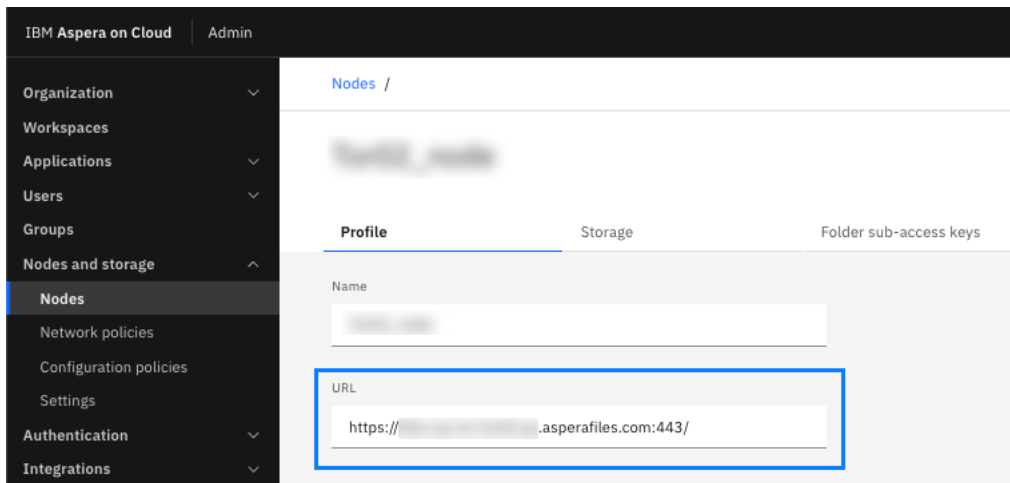
Follow the instructions as described in the [IBM Aspera CLI manual, admin section](#).

Transfer to cloud with Desktop Client, HST Server, or HST Endpoint GUI

You can use the IBM Aspera Desktop Client (freely available), IBM Aspera High-Speed Transfer Server, or IBM Aspera High-Speed Transfer Endpoint GUI to transfer to and from your object storage.

Prerequisites

1. Obtain a transfer service access key ID and secret from your transfer service admin. These are required to authenticate the connection and transfer to and from your object storage.
2. Obtain the transfer service URL for your storage type and region from your transfer service Admin.
Note: An AoC admin with the node secret can find the transfer service URL in the Admin app. In the Node > Details page, see the entry in the field labeled Node URL.



3. Install Desktop Client, HST Server, or HST Endpoint on your computer.

Desktop Client is freely available from the IBM Fix Central website (search for Aspera Desktop Client): <https://www.ibm.com/support/fixcentral>.

For installation instructions, see the [IBM Aspera Desktop Client Admin Guide](#). If needed, configure your Desktop Client computer's firewall to allow it to connect to the transfer service.

Create a connection to the transfer service

1. Open the Desktop Client, HST Server, or HST endpoint GUI.
2. Click Connections to open the Connection Manager window.
3. Click +.
4. Select Create a standard connection.
5. Click New Connection and rename the connection.
6. For Host, enter the transfer service URL that you got from your admin (see prerequisite 3 in the previous section).
7. For Username and Password, enter your transfer service access key ID and secret that you got from your admin.
8. Leave the Storage set to Default.
9. Click OK.
10. Confirm that the name of your new connection appears in the list under Connection Name.

Connecting to the transfer service and transferring content

1. In the Desktop Client, HST Server, or HST Endpoint GUI, the left window shows the local file system and the right window shows a list of connections. Double-click your transfer service connection name, or click the name and click Connect. If the connection is successful, the file system of your object storage is shown in the right window.
2. To upload content to your object storage from the local file system, go to the target path in the right window, select the content in the left window, and then either click the arrow that points to the right or drag and drop the items into the right window.
3. To download content to the local file system, go to the target path in the left window, select the content in the right window, and then either click the arrow that points to the left or drag and drop the items into the left window.

Transfer Servers

Transfer to the Cloud with the Aspera HST server or HST endpoint GUI.

- **[Transfer to cloud with Desktop Client, HST Server, or HST Endpoint GUI](#)**

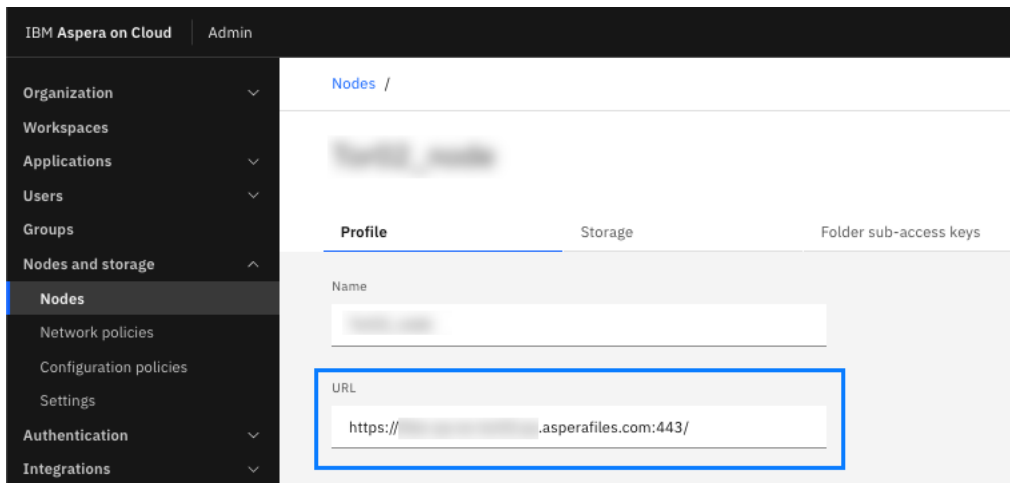
You can use the IBM Aspera Desktop Client (freely available), IBM Aspera High-Speed Transfer Server, or IBM Aspera High-Speed Transfer Endpoint GUI to transfer to and from your object storage.

Transfer to cloud with Desktop Client, HST Server, or HST Endpoint GUI

You can use the IBM Aspera Desktop Client (freely available), IBM Aspera High-Speed Transfer Server, or IBM Aspera High-Speed Transfer Endpoint GUI to transfer to and from your object storage.

Prerequisites

1. Obtain a transfer service access key ID and secret from your transfer service admin. These are required to authenticate the connection and transfer to and from your object storage.
2. Obtain the transfer service URL for your storage type and region from your transfer service Admin.
Note: An AoC admin with the node secret can find the transfer service URL in the Admin app. In the Node > Details page, see the entry in the field labeled Node URL.



3. Install Desktop Client, HST Server, or HST Endpoint on your computer.

Desktop Client is freely available from the IBM Fix Central website (search for Aspera Desktop Client): <https://www.ibm.com/support/fixcentral>.

For installation instructions, see the [IBM Aspera Desktop Client Admin Guide](#). If needed, configure your Desktop Client computer's firewall to allow it to connect to the transfer service.

Create a connection to the transfer service

1. Open the Desktop Client, HST Server, or HST endpoint GUI.
2. Click Connections to open the Connection Manager window.
3. Click +.
4. Select Create a standard connection.
5. Click New Connection and rename the connection.
6. For Host, enter the transfer service URL that you got from your admin (see prerequisite 3 in the previous section).
7. For Username and Password, enter your transfer service access key ID and secret that you got from your admin.
8. Leave the Storage set to Default.
9. Click OK.
10. Confirm that the name of your new connection appears in the list under Connection Name.

Connecting to the transfer service and transferring content

1. In the Desktop Client, HST Server, or HST Endpoint GUI, the left window shows the local file system and the right window shows a list of connections. Double-click your transfer service connection name, or click the name and click Connect. If the connection is successful, the file system of your object storage is shown in the right window.
2. To upload content to your object storage from the local file system, go to the target path in the right window, select the content in the left window, and then either click the arrow that points to the right or drag and drop the items into the right window.
3. To download content to the local file system, go to the target path in the left window, select the content in the right window, and then either click the arrow that points to the left or drag and drop the items into the left window.

Aspera APIs

Using Aspera on Cloud APIs means using endpoints from several API collections. This article links to all related APIs, SDKs, and Developer Guides in the IBM API Hub.

Note: IBM Aspera provides a full suite of APIs to support customer integrations. Always use the Aspera APIs to build integrations. Do not build integrations using application URLs or other methods.

- [Aspera on Cloud API](#)
- [AoC Automation API](#)
- [AoC Activity API](#)
- [Aspera Node API](#)
- [Aspera ATS API](#)
- [Aspera HTTP Gateway Javascript SDK](#)
- [Aspera Connect SDK](#)

Notifications and announcements

Important notifications and announcements for IBM Aspera on Cloud.

- [Deprecation notices](#)
- [Important updates](#)

Deprecation notices

For more information related to Aspera on Cloud status and communications, visit the [status page](#).

DSA public key for IBM Aspera ascp transfers

Effective **January 31, 2025**, the `aspera_tokenauth_id_dsa` public key will not be available for ascp transfers and will stop working with IBM Aspera managed transfer servers. After the deprecation date, any ascp transfers that rely on the `aspera_tokenauth_id_dsa` key will fail to authenticate. To avoid interruptions in your data transfer processes, you should migrate to RSA-based authentication for enhanced security and wider compatibility with current security practices. All versions of transfer clients currently supported will continue to work without any required changes. You may need to upgrade older clients as well as review and update custom integrations. For further assistance with this transition, contact our support team at <https://www.ibm.com/mysupport/>.

Sync feature in AWS environments with IBM Aspera Connect versions older than 4.1.3

On **December 7, 2024**, Aspera on Cloud will no longer support the Sync feature in AWS environments with IBM Aspera Connect versions older than 4.1.3. To continue using this feature, update Connect to at least version 4.1.3 or later. Alternatively, you can switch to the latest version of IBM Aspera for desktop to replace Connect. It is important to highlight that this will **only affect the Sync feature in Aspera on Cloud in AWS**, other features and cloud environments will not be impacted.

Aspera on Cloud Activity App: Deprecation notice of file access page

On **November 15, 2024**, the File Access Page in the Activity App will be deprecated. The page will no longer be available, and any APIs associated with that specific feature will be disabled. This means that permission events from transfer nodes will not be collected for processing in the Activity app anymore. This will not affect file sharing nor setting permissions. Permissions settings for files or folders will continue to be retained.

Important updates

IBM Cloud Object Storage network updates

December 17, 2025

IBM Aspera is updating a subset of its infrastructure to maintain service quality and optimize performance for IBM Cloud Object Storage locations. Ensure that traffic to the following IP addresses is allowed in your firewall configuration to maintain uninterrupted access to IBM Aspera services.

To verify the most up-to-date IP address ranges for IBM Cloud, see <https://ats.aspera.io/pub/v1/servers/softlayer>.

For additional information about firewall requirements for Aspera on Cloud, refer to the [Firewall requirements for ATS and cloud storage](#) section.

Dallas (us-south)	Frankfurt (eu-de)	London (eu-gb)	Osaka (jp-osa)	Sao Paulo (br-sao)	Sydney (au-syd)	Tokyo (jp-tok)	Toronto (ca-tor)	Washington, DC (us-east)
52.116.142.13	158.176.10.212	161.156.201.182	163.73.84.11	13.116.90.99	135.90.128.116	162.133.130.93	163.75.95.120	150.239.82.61
52.118.206.160	149.81.33.204	158.175.188.162	163.69.87.115	163.107.86.129	159.23.100.173	128.168.141.70	163.75.91.120	52.117.122.245
52.116.197.18	149.81.36.190	141.125.156.80	163.73.84.10	163.109.87.184	130.198.15.77	165.192.140.45	163.74.91.27	169.63.99.45
67.18.96.81	149.81.1.16	158.176.194.109	163.68.87.146	13.116.81.218	130.198.18.184	165.192.128.168	163.66.90.109	169.63.186.3
67.18.5.255	149.81.218.166	158.176.188.0	163.68.93.118	163.107.92.250	135.90.135.91	165.192.140.44	163.66.92.254	52.117.125.223
150.240.71.59	158.177.7.117	158.176.173.236	163.69.87.114	13.116.94.205	159.23.100.170	162.133.139.219	163.66.81.89	150.239.113.111
67.18.92.224	161.156.171.89	158.175.188.161	163.68.87.145	163.107.92.249	159.23.91.186	165.192.128.169	163.75.81.221	52.117.120.179
52.118.253.123	161.156.80.151	141.125.105.113	163.73.95.187	163.109.93.223	135.90.140.10	128.168.138.58	163.74.94.59	169.63.186.2
52.118.210.60	149.81.163.140	141.125.107.240	163.69.94.102	163.109.83.99	135.90.128.114	162.133.139.217	163.66.92.253	150.239.211.164
150.240.71.52	158.177.7.115	158.176.173.235	163.68.90.239		159.23.93.246	162.133.135.110	163.75.95.119	150.239.113.110
52.116.192.139	149.81.236.11	141.125.159.95	163.69.91.179		130.198.22.210	128.168.138.59	163.74.87.28	150.239.211.162
150.239.164.50	161.156.160.221	158.176.191.181	163.73.91.10		130.198.15.75	128.168.134.105	163.74.94.58	169.59.188.170
150.240.165.143	158.176.5.80	161.156.196.153						150.239.113.109
52.118.210.43	149.81.216.220	161.156.196.156						169.59.191.109
52.118.184.10	149.81.167.75	141.125.105.109						52.117.122.244
150.240.68.230	149.81.218.165	158.175.179.30						169.62.17.227
169.48.155.101	158.177.7.116	158.176.171.234						150.239.109.68
150.240.67.98	158.176.6.244	141.125.163.37						169.63.102.7

Dallas (us-south)	Frankfurt (eu-de)	London (eu-gb)	Osaka (jp-osa)	Sao Paulo (br-sao)	Sydney (au-syd)	Tokyo (jp-tok)	Toronto (ca-tor)	Washington, DC (us-east)
67.18.104.105								150.239.209.6
67.18.120.51								52.117.125.222
67.18.92.222								150.239.82.58
67.18.92.223								169.59.163.34
150.239.164.101								169.63.191.195
67.18.110.81								150.240.1.62
52.118.208.236								169.63.191.192
52.118.184.9								169.63.179.247
67.18.120.49								150.239.110.98

IBMid update

We have updated the IBMid settings for all organizations that log in using the IBMid to now require multifactor authentication (MFA) for every login. End users can configure their preferred MFA methods at <https://login.ibm.com>, accessing Profile & Settings > Security > Verification methods.

New and Coming Soon

As a SaaS solution, IBM Aspera on Cloud receives frequent updates to deliver new features, functionality, and bug fixes. Get previews into upcoming new features and get insights into enhancements and features as they are released, including links to details user documentation.

- [What's new in Aspera on Cloud](#)
As a SaaS solution, IBM Aspera on Cloud receives frequent updates to deliver new features, functionality, and bug fixes. This topic is a reverse chronological listing of new features and enhancements as they became available for Aspera on Cloud users and administrators.
- [Coming soon to Aspera on Cloud](#)
This topic is a preview of features that IBM Aspera will soon release on Aspera on Cloud.

What's new in Aspera on Cloud

As a SaaS solution, IBM Aspera on Cloud receives frequent updates to deliver new features, functionality, and bug fixes. This topic is a reverse chronological listing of new features and enhancements as they became available for Aspera on Cloud users and administrators.

See [Coming soon to Aspera on Cloud](#) for a preview of features that IBM Aspera will release soon.

For important announcements and notifications, see the [Notifications and announcements](#) section.

Enhanced shared inbox custom metadata controls

June 10, 2026

This new feature enhances shared inbox custom metadata by providing administrators with greater control over field visibility and validation. You can now add a new text block metadata field to shared inboxes metadata configurations. These new text block fields allow administrators to define information that is included with packages and delivered to recipients. Administrators can also control whether the field is required and if package senders can view these fields during package creation. To configure these fields, go to Workspaces > *Select a workspace* > *Select a shared inbox* > Metadata > Add field.

Shared folders visibility for workspace users

May 11, 2026

Admins can now view the shared folders that a workspace member has access to by going to Admin > Users > Management, selecting a user, and accessing the new Shared Folders tab. The Shared Folders tab displays the following information for each shared folder:

- Folder name
- Node name
- Permissions
- Membership type

This enhancement helps admins more easily review and manage user access to shared folders.

Duplicate and deactivate Automation workflows

March 26, 2026

Organization admins can now duplicate and deactivate automation workflows across the organization. From the Workflows page, switch to the **All workflows** view to access workflows created by any user and take action as needed. This enhancement improves administrative control, making it easier to manage workflows even when the original owner is unavailable.

Activity app: Track Shared Inbox and Shared folder events

March 26, 2026

You can now filter Shared inbox and Shared folder events directly from the Activity app. To do this, navigate to Activity app > Application events and filter by the relevant event types that you want to monitor. For more information on the new filters, visit the [Monitor application events](#) section.

Multi-session transfers

December 10, 2025

With multi-session transfers you can simultaneously transfer large files dividing them into smaller segments through multiple sessions. Instead of relying on a single transfer session, you can distribute the workload across several parallel sessions. This accelerates the transfer process, taking advantage of the combined bandwidth from multiple connections. To learn more about this feature, refer to the [Multi-session transfers](#) section.

Password complexity configuration

November 25, 2025

Aspera on Cloud now supports configurable password complexity requirements for client-side encryption. You can define custom complexity rules, so passwords setup for packages must match the rule provided, enabling stronger security controls that match your organization's standards.

To configure this feature, go to Admin > Nodes and Storage > *Select a Node* > Node Configuration > Node Profile > Aspera Encryption at Rest, and enable the option to customize password complexity.

Transfer Diagnostics Aspera for desktop support

November 24, 2025

The [Diagnostics](#) page now includes support for the new IBM Aspera for Desktop application. Under Client Options, you can verify that your device with the new IBM Aspera for desktop client can successfully establish a connection with our transfer servers.

Antivirus scanning

October 2, 2025

With the introduction of this feature, you can now enable antivirus scanning to use with your Trend Micro instance. Packages are automatically scanned for viruses and malware, ensuring safer transfers whether you are collaborating internally or with external parties. For detailed instructions about the setup and configuration process, refer to the [Antivirus scanning](#)

Node access for workspace managers

July 18, 2025

You can now provide workspace managers access to a node by configuring specific paths they can use. This new feature, available under Workspaces > *workspaceName* > Profile > Node access for workspace managers, lets you define and assign one or more paths for managers to access. With this change, workspace managers can also create shared folders for their workspace, enabling a seamless sharing experience. For more information about this feature, see the [Node access for workspace managers](#) section.

Redesigned shared folder experience in the Files app

June 26, 2025

With the implementation of this new feature, the Files application has received the following updates to make access and navigation more intuitive:

- Home folder (formerly *All files*): contains all the files and folders available in your workspace.
- Favorites: displays all the folders that you marked as favorites for quick access.
- Shares: a new section where you can see all the shared folders you have access to in the workspace. You can also click View all under Shares, to browse, rename, or remove any shared folders.

Important: The left navigation only displays the first 20 shared folders. If you have access to more, you can find them in the **Shares > View all** section. To access shared folders with the legacy layout, you can go to the Move/Copy panel.

These updates are designed to make it easier to manage shared content within your workspace.

Simplified folder sharing

June 18, 2025

With this new feature, admins only need to enter the node access key and secret once when creating or managing their nodes. After the initial authentication, you can set the node's ownership to either ATS admins only or all organization admins. Once ownership is set, users can browse, share, and manage node folders without the need to re-enter their credentials, making the shared folder creation process a lot easier. Nodes that were previously added are automatically set to ATS admins only. It is important to note that you still need to provide the secret when creating sub-access keys.

Support for additional IBM Cloud regions

April 21, 2025

The Aspera on Cloud transfer service now supports these additional IBM Cloud regional data centers: Ohio (us-east-2), and Oregon (us-west1). For a complete listing of supported regions, see [Cloud platforms and regions supported](#).

Share folders directly from the Files app

March 31, 2025

Creating and sharing folders in the Files app is now easier! Admins and users with shared folder creation permissions can share folders directly from the Files view—no need to navigate to the Admin section. This update simplifies collaboration and saves valuable time.

Shared folders and shared inboxes access

March 4, 2025

You can now access and manage shared folders and shared inboxes directly from your workspace (Admin > Workspaces > *your workspace* > Shared folders/Shared inboxes). This enhancement makes accessing and creating these shared folders and inboxes much easier and faster, resulting in less clicks and an improved user experience.

Enhanced folder sharing security

February 20, 2025

Admins can now enhance security and access control over folder sharing within a specific workspace. This new feature allows admins to define who (all members, managers, or none) can re-share folders with other workspace members, making sure that only authorized members can extend access to shared content.

Easier group management

February 20, 2025

Managing groups just got a lot simpler. Admins and workspace managers can now search for existing groups when assigning group managers or owners. This eliminates the need to add members individually, making group management faster and more efficient.

Improved group member management

February 11, 2025

It is now easier for admins to add multiple users to groups. Instead of manually adding users one by one, admins can now copy and paste a list of email addresses directly into the search bar, just like when adding members to a workspace. This new feature not only saves time, but it also provides a streamlined workflow and a consistent experience throughout Aspera on Cloud.

Custom profiles for file permissions

February 11, 2025

We are introducing a new feature that allows users to save custom profiles for files permissions. This feature allows users to create, save, and reuse custom permissions, eliminating the need to manually configure permissions each time. Additionally, admins can mirror an existing user's permissions to streamline onboarding. This enhancement simplifies permission management and improves efficiency for growing teams. Custom profiles are applied at the user level, not globally across the organization.

Send form enhancement

February 11, 2025

You can now use markdown to format the text in the instructions text box when sending a package to a shared inbox.

IBM Aspera for desktop

January 23, 2025

Users on Essentials and Standard Plus subscriptions can now switch to IBM Aspera for desktop. This new application is a modern and reliable transfer client that removes the need for Connect's web browser extension, allows for automatic updates, and much more. This new application will be replacing Connect, becoming the primary transfer client for FASP transfers. For more information about what IBM Aspera for desktop can do, refer to the [official documentation](#).

In-app alert notifications

December 20, 2024

We have introduced a new notification system to help organization admins stay informed about usage levels and avoid overages. This feature displays an alert when an organization approaches 80% and 100% of its entitled volume, storage, or egress usage. This enhancement ensures better visibility before limits are exceeded. Notifications for upcoming maintenance windows are also available.

Disable package sending

October 15, 2024

You can now disable package sending within an organization or workspace. This provides added control and flexibility when migrating workflows or restructuring your organization. Both organization admins and workspace managers can disable/enable this setting. When this setting is turned on, users are still able to send packages to shared inboxes. For more information, see the [Disable package sending](#) section.

Scheduled packages

September 12, 2024

With this feature you can create and schedule packages to send them at a specific time, providing greater flexibility, reliability, and improving the way you manage and send your packages. This ensures everything is ready for release without the pressure of immediate sending. IBM Aspera on Cloud will send you a reminder at least 24 hours before your scheduled package is ready to be sent. For more information see the [Schedule packages to send later](#) section.

File deletion policies: Tethered nodes support

June 10, 2024

You can now apply file deletion policies to tethered nodes. When an administrator creates a file deletion policy on an tethered node, the policy applies only to that specific node. If there are other nodes on the same storage and location, this policy is going to affect those as well. For more information see the [File deletion policies for storage management](#) section.

Standard subscription name update

May 7, 2024

IBM Aspera on Cloud Standard subscription has been renamed to Essentials. This is only a new name for that subscription tier, all features and cost remain the same. If you are subscribed to the Standard edition, there's no action needed and you can continue to enjoy the same benefits you already had.

Save packages as drafts

March 13, 2024

No more lost work and time constraints! With this new feature, you can save packages as drafts, preventing you from losing all your progress and incorporating the ability to stage deliveries for future release. For more information about this feature refer to the [Save packages as drafts](#) section.

Automatic user reactivation

February 21, 2024

Deactivated Aspera on Cloud users (due to inactivity) can now login again as soon as they receive a package. Also, SAML users who were previously deactivated due to inactivity, will be reactivated when they login through their SAML provider. You can automatically do this without admins having to manually activate them, optimizing both time and manual effort. Admins can configure the settings for this new feature in User > Advanced > Auto reactivation. For more information see the [Automatic user reactivation](#) section.

Workspace customization

December 22, 2023

You can currently customize your organization and now you can do the same for individual workspaces. These new customization features allow admins to set custom backgrounds (such as in headers, buttons, left menu) and fonts (including font color) at the workspace level. To configure these settings, open the workspace you want to customize and adjust the settings under the Login page and Theme editor tabs accordingly.

Move/copy files between workspaces

December 6, 2023

We are introducing a significant enhancement to the move/copy panel in Aspera On Cloud. Users can seamlessly transfer files between different workspaces, eliminating the need to create shared links. This improvement makes node-to-node transfers more accessible and efficient than ever before.

Key feature updates:

- **Independent workspace browsing:** Users can independently browse through different workspaces and explore their folder structures directly within the move/copy panel. This flexibility provides seamless navigation between workspaces.
- **Streamlined move/copy functionality:** We retain the core move/copy functionality, ensuring a familiar experience for users. The process remains straightforward and efficient.

Transfer activity modal

November 6, 2023

With the new Transfer Activity Modal, keeping an eye on your file transfers has never been easier. When you initiate a file transfer, you can now access an activity modal by simply clicking the information icon. The modal gives you the ability to adjust the target rate of desktop transfers that were started using the Aspera clients, and provides you with real-time insights including transfer rate, percent completion, and much more.

Note: You cannot exceed the server maximum target rate. For more information see the [Cloud platforms and regions supported](#) section.

Customization

October 3, 2023

To help you incorporate your own branding and style we have released new customization features. These features allow admins to set custom backgrounds (headers, buttons, left menu) and fonts (including font color) at the Organization level. To configure these settings at the Organization level, navigate to the Admin application, open the Organization drop-down, and select Profile and Branding.

Branding

October 3, 2023

The user experience starts as soon as a user lands on the login screen, that's why we want customization capabilities to extend beyond the in-app experience. As an admin you can customize the login screens and their respective URLs at the Workspace level. You can also add a logo and full HD splash screen background to the workspace login screen, replacing the default IBM Aspera on Cloud theme. To configure these settings go to the Admin app, open the Organization drop-down, and select Profile and Branding.

File deletion policy new cloud support

October 3, 2023

Previously limited to AWS storage, IBM Aspera on Cloud's file deletion policy is now supported in Google Cloud Platform and Azure. The file deletion policy allows admins to set a length of time before files are automatically deleted from a node (and the associated storage bucket). Automating the deletion of outdated files helps save storage space, reduces storage costs, and streamlines workflows.

Logout notification

September 21, 2023

With the new logout notification feature, users are notified five minutes before their session is about to expire due to inactivity. They can extend their session before it expires due to inactivity, or they have to reauthenticate if their session expires. This minimizes the number of times a user must log in, saving time and increasing productivity. This option is disabled by default for new organizations, meaning users are never logged out due to inactivity. Admins can enable and configure the maximum duration for inactive sessions, as well as login token expiration by navigating to the Admin application, selecting the Organization drop-down, and then the Security tab. The recommended duration for inactive session logout is one hour, but valid durations range from 15 minutes to seven days. For more information see [Session and token duration](#).

File preview

June 7, 2023

Introducing our new File preview feature. With this new capability, you can generate video or image thumbnails from your files to preview their content while browsing through them. File preview adds triggers in a cloud storage (AWS S3) to invoke a function every time you upload a supported file type. With that trigger, the function has enough information to pull data from that file to generate a preview using FFmpeg (in the case of video files) and upload it back to cloud storage.

File preview also checks S3 files to see if they already have a preview. If not, it calls File preview with the necessary info to process it. In some cases, this feature temporarily downloads the file to work with it. Don't worry, we make sure that it is deleted (not from your cloud storage) after it's done processing it.

To enable File preview, you have to build a container image with FFmpeg packaged inside. FFmpeg is a free open-source utility that is not provided or managed by IBM and is subject to third-party terms and conditions. FFmpeg contains codecs for encoding and decoding various video coding formats. Certain codecs contained within FFmpeg may be covered by patents and require a license to use. The Dockerfile provided by IBM will enable all codecs in FFMPEG by default. However, you must assess your own licensing needs in connection with the use of FFmpeg and adjust which codecs to enable accordingly.

File preview on AWS requires self-hosted preview generation on your own AWS Lambda instance. We're currently developing an IBM managed solution for all cloud platforms. This feature is available for Aspera on Cloud Premium subscribers

File deletion policies

March 9, 2023

Admin and Files apps.

Admins have an additional tool to manage storage in their Aspera on Cloud organization by creating policies to permanently delete files and folders when they reach a configured age. File deletion policies automate a formerly manual administrative process. When an administrator creates a file deletion policy on an attached node, the policy applies to all nodes on the same storage. Once the policy is active, it will also apply to new nodes that you create in the same storage.

ATS enhancements

December 15, 2022

IBM Aspera enhanced Aspera Transfer Service (ATS) to improve platform stability.

Support for additional AWS storage classes

November 18, 2022

Admin app.

Aspera on Cloud now supports several additional AWS storage classes, including the increasingly popular Glacier archival classes. Files app users can write directly to Glacier storage and see the "Glacier storage" label for files in Glacier storage.

- Standard
- Intelligent Tiering
- Standard Infrequent Access
- One-zone Infrequent Access
- Glacier Instant Retrieval
- Glacier Flexible Retrieval
- Glacier Deep Archive

In a workspace configured on a node with storage class Glacier Flexible Retrieval or Glacier Deep Archive, the Packages app is disabled due to extended AWS retrieval times. In the Files app, users can view and upload to the storage, but cannot download, move, copy, or rename files. For details, see [Attach an AWS S3 bucket](#).

Renaming large folders

October 12, 2022

Files app.

To rename very large folders, the Files app provides a new option: Rename and move. This feature improves performance for such large file operations. The renamed folder appears in the same location in the Files app. Note that when this operation completes, you must recreate all existing shared links to contents in the renamed folder. For details, see [Rename folders in your Files app](#).

Automation: New options for transfer actions

October 12, 2022

Automation app.

Transfer is a commonly configured action in automated workflows. This change makes new options available for the disposition of transfer source folder contents when the transfer completes. For details, see [Workflow actions and their attributes](#).

Distribution lists for sending packages

September 21, 2022

Admin and Packages apps.

Aspera on Cloud now supports both personal and global distribution lists for sending packages.

Users can create lists for their own personal use and then select them as recipients in the To field of the Send packages form. Administrators can create workspace-level distribution lists and make them available to either all members in the workspace or to workspace managers only.

For details, see [Create a personal distribution list](#) and [Create workspace distribution lists](#).

New IBM Aspera mobile app

July 10, 2022

The new mobile app, IBM Aspera, offers streamlined functionality for fast file transfers to and from your Aspera servers.

Using the new Carbon X interface, this consolidated mobile experience matches what you see on your web browser for Aspera on Cloud. Use your Aspera server account credentials to log into Aspera on Cloud to transfer files to and from your mobile device.

The new mobile app is FASP-native, so you can transfer files to and from your mobile device with the amazing speeds of IBM Aspera's proprietary FASP protocol. The app is available on both the [Apple App Store](#) and the [Google Play Store](#).

IBM Aspera replaces the functionality of the following legacy mobile applications:

- Aspera on Cloud
- Aspera Uploader
- Aspera Drive
- Aspera Faspex

To connect your IBM Aspera to your Aspera on Cloud account, see [IBM Aspera mobile app](#). For more information, see the [IBM Aspera mobile support page](#).

Public link enhancements for increased admin control

May 4, 2022

Admin, Files, and Packages apps.

Aspera on Cloud provides two enhancements to improve admin control of public link usage. These enhancements apply to public links in the Files app and in the Packages app, including shared inboxes. The admin can apply either or both enhancements across the entire organization, for one or more given workspaces, or to specific shared inboxes in a workspace.

Workspace members have always had the option to apply a password to a public link. Unless the link recipient can enter the password, the link target remains inaccessible. This new enhancement allows the administrator to *enforce the password requirement* for all public links.

Similarly, workspace members have always been able to set an expiration for a public link, after which the link target becomes inaccessible. This new enhancement allows the admin to *set a default expiration* for all public links. An individual user can reduce the expiration set by the admin, but cannot extend it.

Disallow encryption-at-rest during package send operations

May 4, 2022

Packages app.

Users of the Packages app can enable encryption-at-rest (EAR) for packages they send, allowing them to apply a password to a given package. Until the recipient applies the password, Aspera on Cloud retains package encryption at the recipient's end, even when the recipient downloads the package to their own local or remote storage.

This enhancement enables admins to *disallow* the application of EAR to packages in all workspaces or in specific workspaces, including in shared inboxes. With this feature applied, senders will not be able to apply EAR on individual packages, which is essential for organizations with downstream automation workflows that leverage server-side encryption-at-rest options instead.

File synchronization support on ATS

May 4, 2022

Note: This feature works with Connect 4.1.3 only; you must upgrade if you're still using an older version of Connect.
Admin, Files, and Packages apps.

Aspera on Cloud has supported integration with IBM Aspera Drive, enabling users to access content in Aspera on Cloud workspaces directly from their desktops without using a browser. Aspera Drive was recently consolidated into Aspera Connect. So your organization members now use Aspera Connect for desktop access to Aspera on Cloud workspace content. Such desktop access allows browsing, uploads, downloads, and sync functions from the desktop.

This enhancement to ATS servers supports synchronization of local folders with remote folders on all ATS transfer regions. Previously, this sync capability was available only on [user-managed tethered nodes](#), AoC-managed nodes, and in a few ATS regions. With this enhancement, all node types support sync using Aspera Connect. See [Desktop access to AoC using IBM Aspera for desktop](#).

New IBM Aspera mobile app

April 30, 2022

The new mobile app, IBM Aspera, offers streamlined functionality for fast file transfers to and from your Aspera servers.

Using the new Carbon X interface, this consolidated mobile experience matches what you see on your web browser for Aspera on Cloud. Use your Aspera server account credentials to log in to Aspera on Cloud to transfer files to and from your mobile device.

The new mobile app is FASP-native, so you can transfer files to and from your mobile device with the amazing speeds of IBM Aspera's proprietary FASP protocol. The app is available for both [iOS](#) and [Android](#).

IBM Aspera replaces the functionality of the following legacy mobile applications:

- Aspera on Cloud
- Aspera Faspex
- Aspera Drive
- Aspera Uploader

To link IBM Aspera to your existing Aspera on Cloud account, see [IBM Aspera mobile app](#). See also the [IBM Support page for IBM Aspera](#).

Enhanced watermarking support

April 14, 2022

Admin and Packages apps

While the Aspera on Cloud integration with Irdeto's watermarking service has been in place for well over a year, these new enhancements extend the usability and functionality of the integration for users of the Packages app. The first enhancement supports watermarking even for short video clips, which previously was not possible. The second enhancement ensures the success of a package transfer even when not all files in the package can be watermarked. See [Watermarking: Integrate your Irdeto service](#) and [Sending: Become an expert](#).

Browser support now adheres to Carbon Design System requirements

March 22, 2022

The Carbon Design System underlies the Aspera on Cloud user interface. Aspera on Cloud browser support now adheres to the Carbon Design System requirements, available [here](#).

New support for additional GCS region

March 17, 2022

Admin app

The Aspera on Cloud transfer service now supports the Google Cloud Service London data center (europe-west2). For a complete listing of supported regions, see [Cloud platforms and regions supported](#).

A new experience for Aspera on Cloud

March 9, 2022

IBM Aspera has launched the next generation of Aspera on Cloud.

Improved responsiveness and a modernized user interface are two highlights of a thorough remake of Aspera on Cloud. Existing features and functionality persist in the new experience, along with numerous enhancements to app behavior and appearance. A few key changes:

Global

- Full support for smartphone and tablet access
- Global search relocated to the upper banner near the transfer monitor
- User interface dark and light modes: the default follows your computer setting; custom control available from the User menu

Tables

- Faster loading throughout; improved browsing responsiveness
- Set personal default page size in Account settings
- Right-click context menus support multi-select operations
- Functional icons now consolidated to the upper-right of the view
- Advanced filters now grouped in one location at top right of each table

More troubleshooting resources

- Admin access to error and session data through Help menu
- Additional articles and procedures

Help center

- Reorganized content and addressed information gaps according to user research findings
- Discrete admin and user articles
- Bookmark favorite articles and list recently viewed articles for easy reuse

End of support for certain IBM Cloud regions

As part of our modernization strategy, we have closed the following ATS regions:

- Paris (par01)
- Chennai (che01)
- Mexico (mex01)
- Montreal (mon01)
- Singapore (sng01)

For supported regions, see [Cloud platforms and regions supported](#).

A new experience for Aspera on Cloud

February 4, 2022

IBM Aspera will launch the next generation of Aspera on Cloud on *March 9, 2022*.

Improved responsiveness and a modernized user interface are two highlights of a thorough remake of Aspera on Cloud. Existing features and functionality persist in the new experience, along with numerous enhancements to app behavior and appearance. A few key changes:

Global

- Full support for smartphone and tablet access
- Global search relocated to the upper banner near the transfer monitor
- User interface dark and light modes: the default follows your computer setting; custom control available from the User menu

Tables

- Faster loading throughout; improved browsing responsiveness
- Right-click context menus support multi-select operations
- Functional icons now consolidated to the upper-right of the view
- Advanced filters now grouped in one location at top right of each table

More troubleshooting resources

- Admin access to error and session data through Help menu
- Additional articles and procedures

Help center

- Reorganized content and addressed information gaps according to user research findings
- Discrete admin and user articles
- Bookmark favorite articles and list recently viewed articles for easy reuse

End of support for node search service

January 21, 2022

Because of the `log4j` vulnerability, the IBM Aspera team strongly recommends uninstalling the `files-node-search` application. This feature is deprecated and is no longer used by our software. Instead, configure the AEJD service on your user-managed server (tethered node) to transmit data to Aspera on Cloud. See [Configure monitoring and metering for your tethered node](#).

If you have installed the `files-node-search` application, remove it now.

1. Stop the service:

```
# /opt/aspera/files-node-search/etc/init.d/files-node-search stop
```

2. Remove the folder:

```
# rm -rf /opt/aspera/files-node-search
```

Decommissioning certain IBM Cloud regions

As part of our modernization strategy, we will close the following ATS regions on January 31, 2022:

- Paris (par01)
- Chennai (che01)
- Mexico (mex01)
- Montreal (mon01)
- Singapore (sgn01)

For supported regions, see [Cloud platforms and regions supported](#). Please contact IBM Sales if you have any concerns about the closure of these ATS regions.

Required firewall changes

On January 22, 2022, Aspera on Cloud will begin using the Akamai Technologies network in front of the AoC API and Front end. You must update your firewall rules before that date.

If your firewall allows the IP ranges shown in "[System requirements and browser support](#)" for your users to access AoC, you must update your settings to also allow the hostnames `api.ibmaspera.com` and `<your_org_subdomain>.ibmaspera.com`, both on port 443. After January 22, 2022, you can disallow the IP ranges you now list.

Customers using the legacy `api.asperafiles.com` endpoint for API clients must update their allowlist in the same way.

Customers who tether their own entitlement-based (usage-based) HSTS installation must also update their allowlists to continue to communicate to `api.ibmaspera.com`.

The currently published IP range for communication from AoC to tethered nodes, to ATS nodes, and to Aspera-manages nodes remain unchanged.

A new experience for Aspera on Cloud

Beta release: December 16, 2021

Improved responsiveness and a modernized user interface are two highlights of a thorough remake of Aspera on Cloud. Existing features and functionality persist in the new experience, along with numerous enhancements to app behavior and appearance. A few key changes:

Global

- Full support for smartphone and tablet access
- Global search relocated to upper banner near transfer monitor
- Dark and light modes; default matches computer setting, controllable from the User menu

Tables

- Faster loading throughout; improved browsing responsiveness
- Right-click context menus support multi-select
- Functional icons consolidated to upper right of the view
- Advanced filters grouped in one location at the top-right of the table

More troubleshooting resources

- Additional articles and procedures
- Admin access to error and session data through the Help menu

Help center enhancements

- Reorganized content and addressed information gaps according to user research findings
- Discrete admin and user articles
- Bookmark favorite articles and list recent articles for easy reuse

New reporting capability: Generate and store asynchronous reports

December 16, 2021

Activity app

Activity app users are already able to export, save, and download reports for transfer activity, volume usage, file access, and app events. An extensive collection of filters allows you to fine-tune the report to address specific data needs. Each report can contain up to approximately 100,000 records relevant to the filters you set.

This new feature enhances the performance and behavior of these Activity app reports in several ways. First, the reports can be generated asynchronously. You can start the report, attend to other tasks, and be notified by the app when the report is available. Second, there is no limit to the number of records the report can contain. And third, the reports are stored in a shared space that makes them available to all Activity app users.

The Activity interface allows an admin to set up this shared space in the desired location in attached storage. Users then see this shared space and its contents as a new page, called Stored reports, in the Activity app.

This new Stored reports page allows you to filter for your own reports and for specific report types (for example, for transfer activity reports). Activity app users can download, get info on, and delete these reports. For details, see [Reporting activity and usage](#).

Revised browser support, including end of support for MS Internet Explorer

November 15, 2021

IBM Aspera has revised the list of browser versions supported. This update includes the end of support for Microsoft Internet Explorer on December 31, 2021. See [System requirements and browser support](#).

Support for additional IBM Cloud regions

October 18, 2021

The Aspera on Cloud transfer service now supports these additional IBM Cloud regional data centers: Osaka (jp-osa), Toronto (ca-tor), Sao Paulo (br-sao); and this additional single-site data center: Singapore (sng01). For a complete listing of supported regions, see [Cloud platforms and regions supported](#).

Support for additional MS Azure region

September 24, 2021

The Aspera on Cloud transfer service now supports the Microsoft Azure London data center (uksouth). For a complete listing of supported regions, see [Cloud platforms and regions supported](#).

Support for additional AWS region

September 14, 2021

The Aspera on Cloud transfer service now support the AWS Northern California data center (us-west-1). For a complete listing of supported regions, see [System requirements and browser support](#).

Support for files and folders in AWS Glacier storage

July 19, 2021

Files and Packages apps.

IBM Aspera is phasing in support for access to content in AWS S3 Glacier storage.

Before this Phase 1 enhancement, the Aspera on Cloud web UI did not mark items in AWS S3 Glacier storage. When users tried to access such an item, they received an error message.

In Phase 1 support, items in Glacier storage are labeled as such. The only action allowed on an item in Glacier in Phase 1 is a request for more information; a dialog appears that informs users that Glacier files are not accessible through Aspera on Cloud, and suggests they contact their administrator for access.

New transfer setting in Node Configuration policies

July 19, 2021

Admin app.

This new feature provides an advanced setting that you can apply in a node configuration policy to any node connected to your organization.

After a "move" transfer (as opposed to a "copy" transfer) completes, Aspera on Cloud deletes transferred files from the source folder. However, files in the source folder that already exist in the destination folder are not transferred: they are skipped. Select this option to include these skipped files in the automatic deletion. Otherwise, skipped files remain in the source folder. For details, see [Creating node configuration policies](#).

Key rotation for Azure storage

June 30, 2021

Admin app.

ATS admins can now use the Aspera on Cloud web UI to update Azure storage credentials to support key rotation. For details, see [Rotate keys for your Azure storage](#).

This new functionality adds to existing support for key rotation for Azure storage using the Aspera Node API. ATS administrators can send a PUT call to the endpoint `/access_key` with the updated storage credentials.

Multifactor authentication with IBMid

June 30, 2021

Admin app.

Your Aspera on Cloud organization will soon support multifactor authentication. An administrator can require this feature for users who authenticate with IBMid.

When a user presents their IBMid credentials, Aspera on Cloud presents two options. The user can elect to receive either an email with a verification code or a time-based, one-time passphrase (TOTP) using an authenticator app like IBM Verify. When the user enters the code or passphrase, they'll be logged into their AoC account. For details, see [Require multifactor authentication for IBMid users](#).

Management support for multi-entitlement subscriptions

June 9, 2021

Admin app.

Administrators of IBM Aspera subscriptions with multiple entitlements now have access to the Subscription management page. These admins can now take advantage of the usage dashboard and of the detailed graphs and tables that visualize transfer usage, egress, and storage. They can also filter the transfer and egress tables by entitlement as well as by month. See [Understanding your subscription usage and billing](#).

Automated archive support for workspace folders

June 9, 2021

Automation app.

This enhancement adds another advanced setting for transfer action steps in your automated workflows.

The Automation app previously included support for automated archiving of transfer source content when the source folder is on a node. This enhancement adds support for archiving of transfer source content when the source folder is in a workspace. See [Workflow actions and their attributes](#).

Enhancement to transfer source treatment: Include skipped files

May 21, 2021

Automation app.

This enhancement adds another advanced setting for transfer action steps in your automated workflows.

When your transfer source folder is a node folder (as opposed to a workspace folder), you can already configure automatic deletion of files from the source folder after the transfer step. This enhancement will allow you to include *skipped* files in the delete option.

Files that already exist at the destination are *skipped* by the transfer since they already exist at your configured destination. When you select this option, the workflow deletes files in the source folder that were skipped, along with those that were transferred (not skipped). The result after the transfer is an empty source folder, which is also automatically deleted. For details, see [Workflow actions and their attributes](#).

New filter for job queue

May 6, 2021

Automation app.

This enhancement gives org administrators better insight into ongoing activity in the Automation app.

The Job queue page has always shown in-progress jobs for workflows that you own or manage. This new filter allows you to switch views between your jobs only and all jobs in progress. This expanded view of current activity helps admins understand whether to expect a specific job to be running or to be queued behind other in-progress jobs.

Monitor and report transfer volume by entitlement

May 5, 2021

Activity app.

To make internal cost accounting easier and faster for organizations with multiple entitlements, you can report transfer volume usage by specific subscription entitlement. For details, see [Example use cases for monitoring transfer activity](#).

Watermarking support in additional AWS regions

April 19, 2021

You can now apply forensic watermarking to more of your sensitive content. Aspera on Cloud supports watermarking in all these AWS regions:

- N. Virginia (us-east-1); Oregon (us-west-2);
- Sao Paulo (sa-east-1)
- Ireland (eu-west-1); London (eu-west-2); Frankfurt (eu-central-1)
- Tokyo (ap-northeast-1); Singapore (ap-southeast-1); Sydney (ap-southeast-2)

For details, see [Watermarking: Integrate your Irdeto service](#).

Volume usage for deleted workspaces

April 8, 2021

Activity app.

You can now filter and report on volume usage in workspaces that have been deleted. This enhancement includes clear labeling for deleted workspaces in the workspace choices filter.

Field deprecations in Activity app API

April 7, 2021

Activity app.

If you use either of the two deprecated fields below, this is a breaking change.

In the Transfer Activity API endpoint `/transfers`, these two fields are deprecated and will be removed from the Activity app API on July 7, 2021:

- **Deprecated fields**
 - `client_ip_address`

- `server_ip_address`

The data contained in these deprecated fields are better represented by these new fields, available for your use now in the Activity app API:

- **Replacement fields available now**
 - `local_ip_address`
 - `peer_ip_address`

The values in these new fields are relative to the transfer direction, represented by the `direction` field. See the [Aspera Activity API on IBM API Hub](#).

Monitor and report transfer volume by shared inbox

April 7, 2021

Activity app.

To make internal cost accounting easier and faster, you can now filter and report transfer volume usage by shared inbox. On the Transfer usage page, first filter for the workspace, then for the intended shared inbox within that workspace.

Support for IBM Aspera HTTP Gateway

April 6, 2021

Admin, Files, and Packages apps.

When some users cannot install the IBM Aspera Connect transfer client, your organization needs an alternative transfer method. To address this need, Aspera on Cloud supports the [IBM Aspera HTTP Gateway](#).

Once you configure your Aspera HTTP Gateway, you can point your Aspera on Cloud organization to it. Enabling the Gateway ensures that all Aspera on Cloud users can transfer.

Even when the Aspera HTTP Gateway is enabled, users who install Aspera Connect can continue to use it. Keep in mind that Aspera Connect transfers are typically faster than Aspera HTTP Gateway transfers. For details, see [Transferring with HTTP Gateway instead of Aspera Connect](#).

Automation: New archive option for source content in node Folder

March 30, 2021

Automation app.

Take advantage of a new option for source content disposition when you build a transfer step in an automated workflow.

Existing options allow you to delete the content in your designated source folder after the transfer. The new option allows you to archive content rather than deleting it when the source folder is on a transfer node. You can designate an existing folder as the archive destination or create a new folder.

This new option supports clarity in the source folder and avoids duplicate transfers without losing the transferred content. It also allows you to track which items you've transferred by reviewing the contents of the Archive folder.

For details, see [Workflow actions and their attributes](#).

New transfer settings in automated workflows

February 25, 2021

Automation app.

You can already configure multiple transfer settings in your automated workflow transfer action steps. This enhancement adds a new transfer setting and two additional options for an existing setting.

You can now apply a rate policy setting that governs how Aspera transfers behave when other outgoing traffic is present. You can select one of four policy options (Fair, Low, High, Fixed). Note that the actual transfer behavior depends on the interaction between Automation app settings and transfer server settings. The actual transfer behavior conforms to the more restrictive setting.

This enhancement also adds two new transport encryption options (AES-192 and AES-256) to the existing option to apply AES-128. Again, the settings at the transfer server and the Automation app interact. The higher key-length setting takes precedence.

For details and examples, see [Workflow actions and their attributes](#).

Support for pagination on attached transfer servers

February 9, 2021

Admin app.

A new enhancement in IBM Aspera transfer server software allows you to change the browsing experience for your Aspera on Cloud users.

This enhancement is a new pagination capability released in IBM Aspera HSTS v4.0. You can choose whether to enable this pagination setting for each transfer server attached to your Aspera on Cloud org. For details and a procedure, see [Creating node configuration policies](#)

The pagination facility, when enabled, returns an internally controlled number of items from the folder being browsed, whether the folder is in cloud storage or on your own tethered node. The paginated response help avoid the time-out issue that is common for large folders in cloud storage.

Note that any paginated return of folder contents does not support retrieval of sorted content. This means that lexicographical sorting of content occurs only within the returned batches.

All Aspera-managed auto-scale clusters (ATS) are upgraded automatically to HSTS v4.0. Customers who tether their own transfer servers to Aspera on Cloud and want to enable this behavior must upgrade to IBM Aspera HSTS v4.0.

Enhanced transfer activity data

January 13, 2021

Activity app.

The Transfers table in the Transfer activity page now provides additional data to help you track and analyze individual transfers and overall usage. The new data also helps you troubleshoot transfer issues if they occur. And all this new information is included when you export a report.

This table has always provided, for each transfer, the event type and start date, along with the associated user, workspace, node.

The existing Node column now provides the IP address along with the name of the node for each transfer. Two new columns indicate the direction and peer for each transfer. Together, the Node, Direction, and Peer columns provide key data for analyzing individual transfers. You have names and IP addresses of both endpoints for each transfer and know which direction (from the perspective of the node) the transfer flowed.

An additional new column reports event status.

Share your automated workflows

January 13, 2021

Automation app.

You can now share your workflows with others, giving them permission to manage workflow jobs. The users you share with can view the workflow and can start, cancel and delete jobs. A new notification, when enabled by the admin, notifies each user you share with of their access to your workflow.

Notification enhancements for automated workflows

January 13, 2021

Automation app.

Automation app builders have always been able to incorporate email notifications to interested individuals as actions in a workflow. Similarly, you've been able to configure notifications to individuals about job status (start/fail/complete) for a given workflow.

This enhancement adds the ability to address groups in these notifications. Org admins can send notifications to any group in the organization. Automation app users who are not org admins can send notifications to groups of which they are members.

Workflow revision tags

January 13, 2021

Automation app.

Each time you revise and activate a workflow, the workflow version increments. This UI enhancement presents users with a visual, numeric, version tag on both the Workflows page and the Job queue page.

The Workflows page always shows the latest version of the workflow. The Job queue page always shows the workflow as it existed at the time the job was run. This means that the workflow as you see it on the Job queue page may be an earlier version than the workflow you see on the Workflows page.

The new version tags make it easy to distinguish which version of the workflow you are viewing.

On the Workflows page, version tags display on all workflows listed. On the Job queue page, the version tag displays on all jobs launched after the enhancement is released.

Coming soon to Aspera on Cloud

This topic is a preview of features that IBM Aspera will soon release on Aspera on Cloud.

For new features available now, see [What's new in Aspera on Cloud](#).

Legal Notice

© 2018-2026 Aspera, Inc., an IBM Company. All rights reserved.

Licensed Materials - Property of IBM

© Copyright IBM Corp., 2026. Used under license.

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Aspera, the Aspera logo, and FASP transfer technology are trademarks of Aspera, Inc., registered in the United States. Aspera Connect, IBM Aspera High-Speed Transfer Server (a merger of IBM products formerly named Aspera Connect Server and Aspera Enterprise Server, 2008 and 2007), IBM Aspera High-Speed Endpoint (formerly Aspera Point-to-Point, 2006), IBM Aspera Desktop Client (formerly Aspera Client, 2005), Aspera Connect, Aspera Cargo, Aspera Console, Aspera Orchestrator, Aspera Shares, the Aspera Add-in for Microsoft Outlook, Aspera FASPstream, and Aspera Faspex are trademarks of Aspera, Inc. All other trademarks mentioned in this document are the property of their respective owners. Mention of third-party products in this document is for informational purposes only. All understandings, agreements, or warranties, if any, take place directly between the vendors and the prospective users.

User

- [Get started](#)
Welcome to Aspera on Cloud (AoC). Build foundational knowledge by understanding key aspects of AoC like transfers, workspaces, and more. Find streamlined procedures to send, share, upload, and download files and folders. Set your personal defaults for language, download location, notifications, and more.
- [Packages app: Send and receive files and folders](#)
The Aspera on Cloud Packages app lets you assemble copies of any number of files and folders into a digital "package" and send the package to others. You can also send colleagues a link that allows them to send you a digital package. And learn how to use a shared inbox for enhanced collaboration with your teams. Get detailed procedures in this section.
- [Files app: Sharing folders](#)
The Aspera on Cloud Files app lets you share folders in your workspace with others, granting specific permissions to each recipient for the content you share. Learn how to upload and download content to and from your Files app; how to move, copy, rename, and delete content; how to set notifications that alert you when new content appears in a shared folder you need to monitor; and more.
- [Aspera Connect transfer client](#)
Learn how to install the IBM Aspera Connect transfer client, how to help outside users install Connect, and how to troubleshoot installation problems.
- [Aspera for desktop transfer client](#)
IBM Aspera for desktop provides secure, fast, and reliable file transfer solutions for IBM Aspera servers.
- [Troubleshooting](#)
Understand failure notifications. Find troubleshooting procedures to address transfer issues like slow transfer speeds, when to retry a transfer, and node-to-node transfer issues. Also troubleshoot issues regarding email notifications, shared folder access, and more. Also find information on specific error messages.
- [New and Coming Soon](#)
As a SaaS solution, IBM Aspera on Cloud receives frequent updates to deliver new features, functionality, and bug fixes. Get previews into upcoming new features and get insights into enhancements and features as they are released, including links to details user documentation.
- [Legal Notice](#)

Get started

Welcome to Aspera on Cloud (AoC). Build foundational knowledge by understanding key aspects of AoC like transfers, workspaces, and more. Find streamlined procedures to send, share, upload, and download files and folders. Set your personal defaults for language, download location, notifications, and more.

- [Get to know Aspera on Cloud](#)
This section answers some fundamental questions about Aspera on Cloud. What is this app? What is a transfer? What is a workspace? And what is Aspera Connect, the transfer client that drives desktop-based uploads and downloads? Aspera on Cloud allows you to send files and to share them; understand the difference and when to use which in these brief introductory articles.
- [Quick start](#)
Take a look at the quick and simple requirements you need to fulfill, then get started sending, sharing, uploading, and downloading your files and folders. Learn to use the built-in transfer monitor to view transfer progress, rate, and status; to pause and restart active transfers; and more.
- [Set your account preferences](#)
Customize your Aspera on Cloud by setting your personal defaults for language, table size, download locations and more. Subscribe to email notifications, add your public key (optional), and disable IBM Aspera Connect if your organization uses Aspera HTTP Gateway for transfers.

Get to know Aspera on Cloud

This section answers some fundamental questions about Aspera on Cloud. What is this app? What is a transfer? What is a workspace? And what is Aspera Connect, the transfer client that drives desktop-based uploads and downloads? Aspera on Cloud allows you to send files and to share them; understand the difference and when to use which in these brief introductory articles.

- [What is IBM Aspera on Cloud?](#)
Aspera on Cloud is IBM's on-demand SaaS offering for global content transfer and exchange. The service enables organizations to move large files and data sets – securely and reliably – across on-premises and multi-cloud environments at unrivaled speed.
- [What is a transfer?](#)
A transfer moves files and folders from one storage location to another (examples of storage locations include your own local machine, a remote server, public or private cloud storage).
- [What is a package?](#)
In the Packages app, a package (also called a digital package) is a collection of digital assets (files, folders, video, images, etc.) that you gather to send to one or more individuals or user groups, or to an Aspera on Cloud shared inbox. When you send a package, Aspera on Cloud creates copies of the content you attach for each recipient; the source content remains unchanged.
- [Applications: Overview](#)
An Aspera on Cloud application is a self-contained service with its own memberships and configuration settings.
- [What is a workspace?](#)
The workspace is a collection of Aspera on Cloud users working together—on a project perhaps, or in a department or division. Users in a given workspace can freely collaborate with other members of the same workspace.
- [What is a shared inbox?](#)
An Aspera on Cloud Packages app shared inbox is an optional workspace feature similar to a drop box: you can send content directly and simultaneously to all members of the shared inbox without having to address it to particular users or user groups.

- [What is IBM Aspera Connect?](#)
Aspera on Cloud requires one of two transfer methods to power high-speed transfers between user desktops and Aspera transfer servers. Users can either download and install Aspera Connect, a free, lightweight, install-on-demand software program; or you can configure the IBM Aspera HTTP Gateway and attach it to your Aspera on Cloud organization.
- [Should I send or share?](#)
Sending files and folders using the Packages app and sharing folders in your Files app both initiate a FASP (fast, adaptable, secure, predictable) transfer. However, there are important distinctions between sending content and sharing content using Aspera on Cloud.
- [Key elements and roles in Aspera on Cloud](#)
This article describes the elements of your Aspera on Cloud organization, including workspaces and applications, along with key roles like organization admin, ATS admin, standard and limited users, and so on.
- [Multi-session transfers](#)
Multi-session transfers simultaneously transfer large files dividing them into smaller segments through multiple sessions. Instead of relying on a single transfer session, you can distribute the workload across several parallel sessions. This process takes advantage of the combined bandwidth from multiple connections.
- [What is a transfer?](#)
A transfer moves files and folders from one storage location to another (examples of storage locations include your own local machine, a remote server, public or private cloud storage).

What is IBM Aspera on Cloud?

Aspera on Cloud is IBM's on-demand SaaS offering for global content transfer and exchange. The service enables organizations to move large files and data sets – securely and reliably – across on-premises and multi-cloud environments at unrivaled speed.

Using Aspera on Cloud, organizations can store and readily access files and folders in multiple cloud-based and on-premises storage systems. Sharing among users is as easy as browsing or dragging-and-dropping – regardless of where the files are located – freeing collaboration from traditional boundaries among colleagues in both local and remote locations.

Aspera on Cloud uses IBM Aspera's FASP protocol, which overcomes the limitations of other file-transfer technologies. By moving large data sets at maximum speed, reliably and securely – regardless of network conditions, physical distance between sites, and file size, type, or number – Aspera technology enables a new world of collaboration, sharing, and content delivery.

Aspera on Cloud highlights include the following:

- Domain security within the application
- Intuitive file management tools
- Multiple permission or access levels for individual files and folders, configurable per user or group
- Ability to send content to multiple recipients using an intuitive, email-like interface
- Simple sharing of files and folders
- Configurable permissions to share with and send to outside users who do not have an Aspera on Cloud account
- Comprehensive administrative console
- Support for IBM Aspera transfer service, enabling automated self-scaling of transfer capacity to maximize performance while minimizing cost
- RESTful Platform API (including users, permissions, transfers, and reporting)

For AoC API documentation, see [IBM API Hub](#). For more information about integrations and related APIs, see [Integration and APIs](#).

What is a transfer?

A transfer moves files and folders from one storage location to another (examples of storage locations include your own local machine, a remote server, public or private cloud storage).

Aspera's FASP® transfer technology allows Aspera on Cloud users to share and send files and folders quickly, easily, securely – overcoming the traditional problems and bottlenecks of other transfer technologies.

For example, these are some of the operations you may perform that initiate a FASP transfer:

- Send or receive a [digital package](#) in your Packages app
- Download content you receive in a package
- Move files and folders from a package to your Files app
- Move files and folders from one directory to another directory within the Files app

The transfer may be a copy-and-paste action to the new location, leaving the source content intact in the original location. Or it may be a copy-and-delete operation, pasting the content to the new location while deleting the original content in the source location.

You can monitor active transfers and review completed transfers in the [transfer monitor](#).

There are four transfer types in Aspera on Cloud:

- **Upload:** Uploading content from your local machine or from a local or remote storage location into an Aspera on Cloud workspace. This is typically a copy/paste operation, leaving the source content intact in the original location. Most Send operations (Packages app) are also uploads, copying the content to an interim location on a transfer server accessible to the recipient for download.
- **Download:** Downloading content from the Aspera on Cloud workspace to your local machine, or to a local or remote storage location. This is also typically a copy/paste operation, leaving the source content in Aspera on Cloud intact while duplicating it in the target location.
- **Node-to-node:** Also called **share-to-share**. Moving content from one Aspera transfer server to another. This may be the case when moving files and folders from one location to another in your Aspera on Cloud workspace; for example, when you move files or folders from a package you received in your Packages app to a location in your Files app. Moving content from one location to another within your Files app may also be a transfer, depending on the source and destination locations. Such a move can be a copy or a move operation; hold the Alt key while you drag to change the default action (the default action varies based on the source or destination location; see also [Move or copy content in your Files app](#)).
- **Intra-node:** Moving content from one location on an Aspera transfer server to another location on the same server. This may be the case when moving files and folders from one location to another in your Aspera on Cloud workspace. For example, when you move files or folders from a package you received in your Packages

app to a location in your Files app; or when you move items from one directory to another within the Files app.

What is a workspace?

The workspace is a collection of Aspera on Cloud users working together—on a project perhaps, or in a department or division. Users in a given workspace can freely collaborate with other members of the same workspace.

You need specific permissions, configured by the organization administrator or workspace manager, to collaborate with users outside the workspace.

The users, packages, files, and folders in one workspace are completely separate from those in another workspace.

The workspace name displays in the upper left corner, immediately below the app name (Files or Packages apps).

Membership in multiple workspaces

You may be a member of more than one workspace. You may have different permissions and access in one workspace than you do in another.

If you are a member of multiple workspaces, you can display them by clicking the caret beside the workspace name, then selecting the intended workspace to switch to it. If you have membership in more than five workspaces, you can pin one or more to keep them at the top of your list for convenient access.

Note: Multiple workspaces are available depending on your subscription edition. To see your edition, click the User icon and see Account settings > Account > IBM Aspera on Cloud Edition.

Workspaces in the Packages app

As a workspace member in the Packages app, you send and receive [digital packages](#). You can access your personal inbox ("My Inbox"), which contains the packages sent to you as an individual. You can also access your sent, archived, and deleted or expired packages.

Optional Permissions

You may also have the following capabilities in your Packages workspace:

- Sending to people who are not members of your workspace.
- Sending a [file request](#) to someone outside your workspace, inviting them to send you a digital package.
- Membership in one or more [shared inboxes](#).

Note: Shared inboxes are available depending on your subscription edition.

Workspaces in the Files app

As a workspace member in the Files app, you have access to a collection of folders shared with you by your administrator and by other members of your workspace. When others share a folder, they may share it with you only, or they may share it with multiple people. Your collection of folders may be very different than the collection of another user in the same workspace, though you may share some of the same folders.

The person sharing also grants various [permission levels](#) to these folders and their contents (for example: view, download, delete, and several others); your permission to one folder may be different than your permission to another folder. Similarly, your permission to a folder may be different than the permission another user has to that folder.

Even when folders are shared with multiple members of your workspace, you can move and rename folders without affecting the location and naming of those same shared folders in other users' applications. However, for important conditions regarding deleting shared folders and files from your Files app, see [Delete files and folders](#).

You can share folders in your workspace with other members of your workspace; you may also be able to share folders with people outside your workspace.

Note: In rare circumstances, folders in your workspace may display in red, indicating that they are currently unavailable; contact your administrator or workspace manager for assistance.

Optional permissions

You may also have the following capabilities in your Files app:

- [Uploading](#) files and folders into your Files app workspace; the content you upload remains private to you until you share it with others.
- [Creating new folders](#) in your workspace.
- [Sharing](#) a folder with someone outside your workspace.

What is IBM Aspera Connect?

Aspera on Cloud requires one of two transfer methods to power high-speed transfers between user desktops and Aspera transfer servers. Users can either download and install Aspera Connect, a free, lightweight, install-on-demand software program; or you can configure the IBM Aspera HTTP Gateway and attach it to your Aspera on Cloud organization.

Aspera Connect is the default transfer method for Aspera on Cloud and other Aspera web app. However, if your deployment of Aspera on Cloud does not permit the download and installation of client software, the admin can [configure](#) an alternative transfer method: the [IBM Aspera HTTP Gateway](#). Otherwise, all users must install the Aspera Connect transfer client and the Connect browser extension to complete high-speed transfers.

Once installed, Connect runs automatically when you transfer content using one of the Aspera web apps. In Aspera on Cloud, Connect typically runs in the background rather than on screen as in many of the other Aspera web applications.

Important: Connect comprises an app and a browser extension; you must install both as follows:

- You must install the Connect app once on your computer.

See [Installing Aspera Connect](#).

- You must install the Connect extension for each browser (except Internet Explorer) you'll use to access Aspera on Cloud.

See the appropriate article:

- [Adding the Chrome browser extension for Connect](#).
- [Adding the Firefox Connect Browser Extension](#).
- [Adding the Safari browser extension for Connect](#).
- [Adding the Microsoft Edge browser extension for Connect](#).

If required, you can configure Connect to change default settings for download location, transfer bandwidth, and various network and security settings. Configure Connect settings with the guidance of your Aspera administrator. Note that the Connect Transfers window displays all your recent transfers, whether through Aspera on Cloud or another Aspera product.

After each successful login, Aspera on Cloud checks to see whether the most recent version of Connect is running on your machine. If a Connect upgrade is available, Aspera on Cloud prompts you through the upgrade process.

If you have any issues with Aspera Connect performance, run the [IBM Aspera Connect Diagnostic Tool](#). See also [Installation troubleshooting](#) and [IBM Aspera Connect common issues](#). For more details, see the [IBM Aspera Connect product documentation](#).

Should I send or share?

Sending files and folders using the Packages app and sharing folders in your Files app both initiate a FASP (fast, adaptable, secure, predictable) transfer. However, there are important distinctions between sending content and sharing content using Aspera on Cloud.

If you are an admin, remember that in any organization or workspace, you can allow users to send, or share, or both. You can configure transfer options based on what your team is used to or on how you want your team to perform transfer tasks.

Introduction

Send: Like sending an email with attachments

Sending files and folders using the Aspera on Cloud *Packages app* is very much like sending an email with attachments. Senders use a simple form to address recipients and attach content. Recipients receive a copy of the content and can download it to use however they want.

Share: Like collaborating in a shared file repo

Sharing folders using the Aspera on Cloud *Files app* is like collaborating using a shared file repository. Each user has access to certain folders in the repo, with specific permissions to each folder and its contents. Files app users can share their folders with others, assigning content permissions to each recipient. Keep in mind that when you upload to your Files app, no one sees your folder until you share it with them.

Send: Send a copy of files and folders using the Packages app

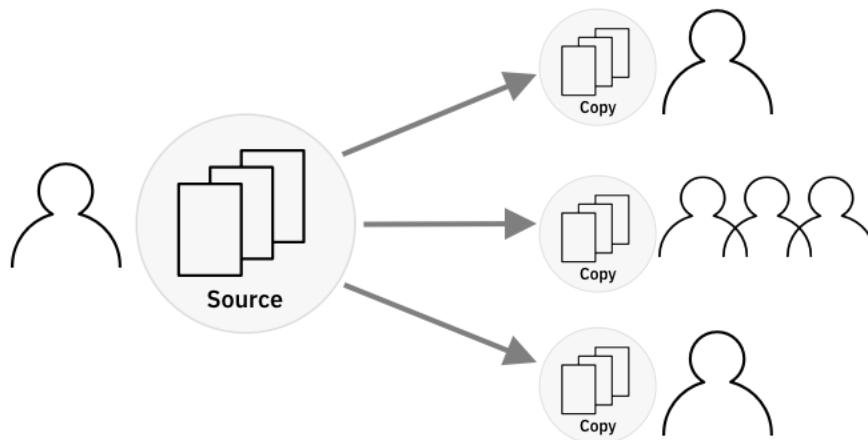
Use the AoC Packages app to send, receive, and request files and folders.

When you send files and folders, you send a *copy* of the source content to your recipients.

- You cannot modify the copy once you send it. Changes you make to the source content do not affect the copy you sent.
- Changes the recipient makes to the copy do not affect your source.
- Your recipient can act in any way on their copy of the content you send. Unlike sharing, you do not assign permissions to content you send.

You can send files and folders from any connected source: your own computer, an attached drive, share, or cloud storage, your Files app, and so on.

To request files, send a [submission link](#), also called a *file request*. Such a link enables another user to send files and folders to you.



Who can send to whom?

By default, any workspace member with access to the Packages app can send files to and request files from anyone else. Workspace members may also be able to send to users and groups outside the workspace.

As an admin, you can protect content security by using any of several options to restrict valid recipients outside the workspace. If necessary, you can keep all Packages app exchanges within the realm of the workspace. For details, see [Collaboration: Open or closed?](#) and [Content security in the Packages app](#).

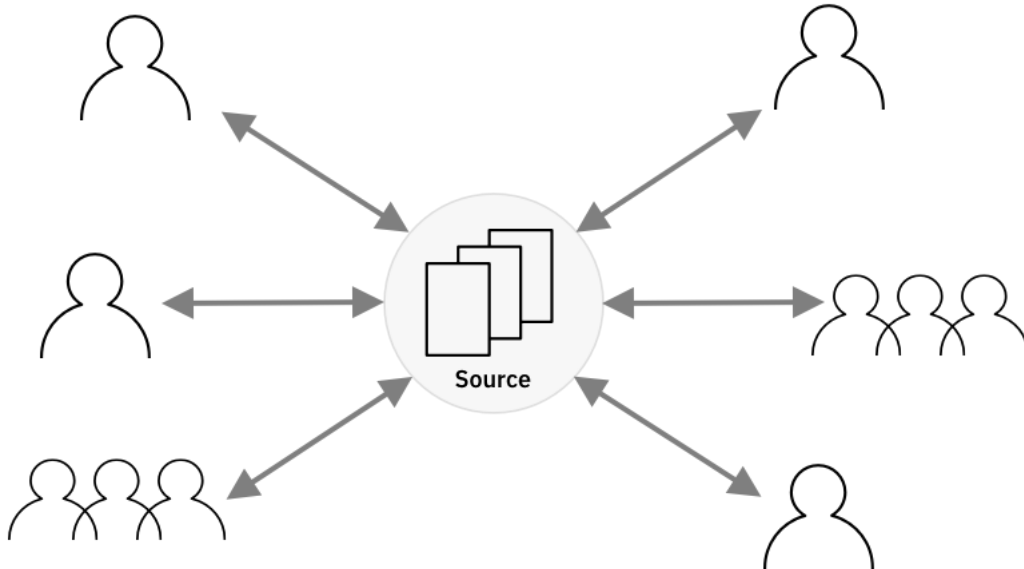
Share: Give others access to your *source* content using the Files app

Use the AoC Files app to share folders.

When you share a folder, you give others access to your *source* content. The folder content is *live*: all users with shared access can update folder contents and see the updates others make. You assign access permissions to the folder for each person you share with. These permissions determine what that person can do with the folder you share.

The folder to share must be in your AoC environment. There are three ways to get content into your Files app:

- You can upload a folder to your Files app and share it. Other members of your workspace won't be able to see the folder you upload until you share it. You can also upload a file, but you can only share a folder. To share a file, place it in a folder and share the folder.
- When someone shares a folder with you, it appears in your Files app. You can share a folder that has been shared with you.
- You can move files and folders from your Packages app to your Files app. Once in the Files app, you can share it.



Who can share with whom?

By default, any workspace member with access to the Files app can share folders with anyone else. As an admin, you can protect content security by using any of several options to restrict valid recipients outside the workspace. If necessary, you can keep all Files app exchanges within the realm of the workspace. For details, see [Collaboration: Open or closed?](#) and [Content security in the Files app](#). For configuration procedures, see [Files App: Using a shared file repository](#).

Shared content permissions

When you upload a folder to your Files app, you have all permissions to it. When someone shares a folder with you, you have the permissions they assign to you.

Permissions may include:

- Browse (View)
- Preview
- Rename
- Upload to
- Download
- Delete
- Create a new folder in

When you share a folder, you assign permissions to each user you share with. You can assign, at most, only the permissions that you yourself have to the folder; you can also share a folder and grant fewer permissions than you have to it.

For example, if a colleague shared a folder with you, giving you Browse, Preview, and Delete permissions, you can share that folder with another person, giving them the same Browse, Preview, and Delete permissions that you have. You can also share the that folder with only Browse permission. But you cannot share the folder with Download permission, since you don't have that permission to the folder. For a full discussion, refer to [Content permissions](#).

Quick start

Take a look at the quick and simple requirements you need to fulfill, then get started sending, sharing, uploading, and downloading your files and folders. Learn to use the built-in transfer monitor to view transfer progress, rate, and status; to pause and restart active transfers; and more.

- **Before you begin**
Just a few prerequisites before you begin: you most likely need to download the IBM Aspera for desktop, an easy-to-install app that powers Aspera high-speed transfers between your desktop and Aspera on Cloud. And be sure to use a supported web browser.

- [Quick start: Send files and folders](#)
Sending even the largest files or data sets is quick and simple, much like sending an email with attachments. Your recipients receive a copy of the files and folders you attach.
- [Quick start: Share a folder from your Files app repo](#)
You can share folders in your Files app. When you share folders, you give your recipients direct access to your source material. You also give each recipient a specific permission to access the folder contents.
- [Uploads and downloads](#)
In the Files app, upload files and folders so that you can share that content with others. Download from the Files app to access file and folder contents. In the Packages app, send a package to upload package contents to a transfer server. Download packages to access package contents.
- [Monitor transfers](#)
You can review your attempted and completed transfers and monitor your active, in-progress transfers using the transfer monitor. This in-app monitor reflects the transfer activity that you perform using the Aspera on Cloud app, including transfers that use the IBM Aspera Connect transfer client; the IBM Aspera HTTP Gateway; and direct node-to-node FASP transfers. To view transfer activity and usage for the entire organization, use the Aspera on Cloud Activity app.
- [File preview supported file types](#)

Before you begin

Just a few prerequisites before you begin: you most likely need to download the IBM Aspera for desktop, an easy-to-install app that powers Aspera high-speed transfers between your desktop and Aspera on Cloud. And be sure to use a supported web browser.

Transfer protocol

Aspera for desktop is the default transfer method for Aspera on Cloud. But if your network environment does not permit software downloads, your administrator has configured an alternative transfer method, the IBM Aspera HTTP Gateway.

If your organization uses Aspera for desktop for transfers, your Aspera on Cloud app displays a prompt that guides you through a very simple download and installation process.

If your organization uses the Aspera HTTP Gateway, you won't be prompted to take any action to download and install. In either case, you'll enjoy the speed and predictability of Aspera high-speed transfers.

For more information, visit the official [IBM Aspera for desktop](#) transfer client documentation.

Browser support

Aspera on Cloud is compatible with the following browsers:

Browsers	Minimum version supported
Mozilla Firefox	Latest version -1
Mozilla Firefox ESR	Latest version -1
Google Chrome (Desktop and mobile)	Latest version -1
Apple Safari (Desktop and mobile)	Latest version -2
Microsoft Internet Explorer	Latest version -1 Support ends on December 31, 2021.
Microsoft Edge	Latest version -2

Quick start: Send files and folders

Sending even the largest files or data sets is quick and simple, much like sending an email with attachments. Your recipients receive a copy of the files and folders you attach.

1. Open the sending form in the Packages app or in the Files app:
To change apps, use the app switcher 
 - In the Packages app, click **Send files**.
 - In the Files app, right-click the file or folder to send, then select **Send**.
2. Add recipients in the To field.
3. Enter a subject in the Package title field.
4. Attach content to send: drag and drop files and folders to the form, or click **Add files** to browse for content.
5. Click **Send**.

See also [Sending: Detailed procedure](#).

Quick start: Share a folder from your Files app repo

You can share folders in your Files app. When you share folders, you give your recipients direct access to your source material. You also give each recipient a specific permission to access the folder contents.

Note: You can share only folders; you cannot share a file. To share a file, place it in a folder, then share the folder.

Make sure that you are in the Files app. If necessary, use the app switcher .

1. Right-click the folder row and select **Share**.

2. Enter the name or email address of one or more collaborators.
3. Set the access permission that you want these collaborators to have for this folder.
4. Click **Add**.

For much more on collaborating using the Files app, see [Files app: Sharing folders](#)

Uploads and downloads

In the Files app, upload files and folders so that you can share that content with others. Download from the Files app to access file and folder contents. In the Packages app, send a package to upload package contents to a transfer server. Download packages to access package contents.

In the Files app

To open the Files app, click the app switcher  and select Files.

Upload

Remember that files and folders you upload to your Files app are not visible to other workspace members until you [share](#) them. Note also that you have full Edit permission to content you upload.

Add files and folders to your Files app in any of several ways:

- Drag content from your local machine or from a remote source and drop it into your Files app.
- Click the Upload icon, select Upload file or Upload folder, then browse to select content from your Finder or Explorer.
The AoC administrator controls whether or not you can upload to your Files app. If you don't see the Upload icon, check with your admin.
- Save to your Files app from your Packages app; in your Packages app, do the following:
 1. To save an entire package, right-click the package row and select **Save in Files**.
 2. To save specific content within a package, click the package row to open the details panel; then right-click the item row and select Save in Files.
The root level of your Files app in the same workspace displays.
 3. Select the location in your Files app where you want this content to reside.
 4. Click Save.

Note that you can save between apps in the same workspace only. You cannot save from the Packages app in Workspace A to the Files app in Workspace B.

Download

To download items to your default download location (configure your default location in IBM Aspera for desktop: Settings > Transfers), select the checkbox on one or more rows, then click **Download** at the top of your Files list.

To override the default download location, select the checkbox on one or more rows, then click Download to...; select the intended location from your Finder or Explorer, then click OK.

Note: Selecting Download to... affects *only this download*. To change your *default* download location, open Aspera for desktop, go to Settings > Transfers. Click Choose location, and select the default location for your downloads.

If you are not using Aspera Connect, check the Downloads location of your browser.

You must have the required permission to an item to download it. If you don't have download permission, ask the person who shared the item with you to grant you Download permission. Check the secondary text on the row of the file or folder to see who shared it with you.

☐		2017-11-20_AspiraOne_Readout	924 MB
		Shared by  to a group	11 files

In the Packages app

To open the Packages app, click the app switcher  and select Packages.

Upload

When you send a package, you upload the package contents to the transfer server. There is no upload action separate from sending a package. Click Send files, and follow the procedure in [Quick start: Send files and folders](#).

You can move files and folders from the Files app directly to your Packages app in the same workspace. In the Files app, check the box to select one or more items, then select Send via Packages.

Download

To download packages or items within packages, do the following:

1. To download an entire package to your default download location, right-click the package row and select **Download**.
To change your *default* download location, open Aspera for desktop, go to Settings > Transfers. Click Choose location, and select the default location for your downloads.
2. To download multiple packages, select the check box to the left of each package to download and click **Download** at the top of the Packages list.
3. To download one or more items from within a package, do the following:
 - a. Click the package row to display the details panel.
 - b. To download a single item to your default download location, click the Download icon on the item row.
 - c. To download multiple items to your default download location, select the check box to the left of each item and click **Download** at the top of the content list.

Monitor transfers

You can review your attempted and completed transfers and monitor your active, in-progress transfers using the transfer monitor. This in-app monitor reflects the transfer activity that you perform using the Aspera on Cloud app, including transfers that use the IBM Aspera Connect transfer client; the IBM Aspera HTTP Gateway; and direct node-to-node FASP transfers. To view transfer activity and usage for the entire organization, use the Aspera on Cloud Activity app.

Transfer monitor

To open the transfer monitor, click the Transfers icon . You can filter the list of transfers by activity type (all, upload, download) or by transfer status (all, failed, stopped, running).

Note these aspects of the transfer monitor:

- For each transfer:
 - Label indicates whether the transfer occurred in the Packages app or in the Files app
 - Main label indicates package name (for transfers in the Packages app) or file/folder path/name (for transfers in the Files app)
 - Check mark indicates successful completion
 - Progress bar indicates active, in-progress transfer
 - "x" icon indicates failed transfer
 - Statistics labels indicate transfer size and date, transfer status (Downloaded, Uploaded, Error, Stopped, InProgress)
 - Access the activity modal by clicking the information icon. You can adjust the target rate of desktop transfers that were started using the Aspera clients. This modal displays real-time insights including transfer rate, percent completion, and more.
 - Click View local folder to jump to the finder/explorer location of the content on the local machine or remote storage
 - Location path displays near transfer statistics
- For active transfers:
 - Click the Pause or Play icon to the right to pause or resume the transfer
 - Text labels indicate transfer progress, rate, and items remaining
 - Animated progress bar indicates transfer progress

Entries in the transfer monitor

Note that a single user transfer operation may generate multiple transfer entries in the transfer monitor.

For example, suppose a single package contains content from multiple sources. Content from a local or remote source is a separate transfer from content that already resides on an Aspera transfer server. In this case, it is possible for one transfer to succeed and another to fail, even though both transfers are initiated from sending a single package.

What starts a transfer?

Aspera on Cloud initiates a transfer when you perform any of the following actions:

- Upload content into your Files app
- Download content from your Files app
- Move content from one location in your Files app to another
- Save content from a package to a location in your Files app
- Send a digital package in the Packages app
- Send a package to a shared inbox
- Download content from a package (including a shared inbox submission)

In addition, Aspera on Cloud also initiates a transfer during these operations:

- When an outside user sends you content
- When an outside user submits content to a shared inbox
- When an outside user you've shared content with downloads it
- When an outside user you've sent content to downloads it

File preview supported file types

Supported file types

Note: AoC does not support previews for audio-only files.

In addition to support for **.pdf** documents, file preview supports the following formats for videos and images.

Video

```
.m2v
.avi
.divx (preview will be displayed as image)
.m4v
.flv
.mp4
.mkv
.h261
.mpg
.wmv
.h263
.mpeg
```

.mov
.h264
.mxf (preview will be displayed as image)

Image

.aai
.fig
.pam
.rfg
.art
.fits
.clipboard
.rla
.arw
.fpx
.pbm
.rle
.avs
.gif
.pcd
.sct
.bpg
.gplt
.pcds
.sfw
.bmp
.gray
.pcl
.sgi
.bmp2
.hdr
.pcx
.sid
.bmp3
.hpgl
.pdb
.mrsid
.cals
.hrz
.pdf
.sparse-color
.cgm
.ico
.pef
.sun
.cin
.info
.pfa
.svg
.cmyk
.inline
.pfb
.tga
.cmyka
.jbig
.pfm
.tiff
.cr2
.jng
.pgm
.tim
.crw
.jp2
.picon
.ttf
.cur
.jpt
.pict
.uil
.cut
.j2c
.pix
.uyvy
.dcm
.j2k
.png
.vicar
.dcr
.jpeg
.png8
.viff
.dcx
.jpg
.png00
.wbmp
.dds
.jxr
.png24
.wdp
.dib
.man
.png32
.webp
.djvu

```
.mat
.png48
.wmf
.dng
.miff
.png64
.wpg
.dot
.mono
.pnm
.x
.dpx
.mng
.ppm
.xbm
.emf
.mpc
.ps
.xcf
.epdf
.mpr
.ps2
.xpm
.epi
.mrw
.ps3
.xwd
.eps
.msl
.psb
.x3f
.eps2
.mtv
.psd
.ycbr
.eps3
.mvg
.ptif
.ycbr
.epsf
.nef
.pwp
.yuv
.epsi
.orf
.rad
.ept
.otb
.raf
.exr
.p7
.rgb
.fax
.palm
.rgba
```

Set your account preferences

Customize your Aspera on Cloud by setting your personal defaults for language, table size, download locations and more. Subscribe to email notifications, add your public key (optional), and disable IBM Aspera Connect if your organization uses Aspera HTTP Gateway for transfers.

- [Set your default language](#)
Aspera on Cloud is available in several languages. You can select a language as your default; each time you log in the app displays in the language you select.
- [Set your default items per page](#)
You can set a default page size that determines how many items per page display in each Aspera on Cloud table. You can override the default you set at each individual table. If you don't set this value, the system default is 25 items per page.
- [Set your default app](#)
If you have membership in multiple applications, you can designate one of them as your default app, so that each time you log in to Aspera on Cloud, and each time you enter a workspace, your default app displays. Your choice of default app applies to every workspace you access.
- [Set your default workspace](#)
If you have membership in multiple workspaces, you can designate one of them as your default workspace. Each time you log in to Aspera on Cloud, your default workspace displays. Your choice of default workspace applies to both the Packages app and to the Files app.
- [Set your default download location](#)
You can set or change the location for the folders, files, or packages you download using the IBM Aspera Connect transfer client in Aspera on Cloud. Once set, you can override this location for a specific transfer by selecting Download to.... instead of Download.
- [Add your public key](#)
You can add a public key to your Aspera on Cloud account, to be used in conjunction with your private key when accessing the Aspera on Cloud API using an API client.
- [Subscribe to email notifications](#)
You can subscribe or unsubscribe to specific Aspera on Cloud email notifications. The settings you select apply to notifications in every workspace you are part of, and override notification settings configured by the administrator.
- [Disable IBM Aspera Connect](#)
If and only if your organization supports IBM Aspera HTTP Gateway, you can disable IBM Aspera Connect transfer client and the default prompt to install Aspera Connect.

Set your default language

Aspera on Cloud is available in several languages. You can select a language as your default; each time you log in the app displays in the language you select.

To set your default language, do the following:

1. Click your user image in the upper right to display the menu, then select **Account settings**.
2. Go to **Defaults > Default language**. Click the field to select your default language.
3. Click **Save**.

If you do not set a default language, at each new login AoC displays in the last language you selected before your previous logout.

Set your default items per page

You can set a default page size that determines how many items per page display in each Aspera on Cloud table. You can override the default you set at each individual table. If you don't set this value, the system default is 25 items per page.

1. Click your user image in the upper right to display the menu, then select **Account settings**.
2. Go to **Defaults > Default items per page**. Click the field to select your default size.
3. Click **Save**.

Set your default app

If you have membership in multiple applications, you can designate one of them as your default app, so that each time you log in to Aspera on Cloud, and each time you enter a workspace, your default app displays. Your choice of default app applies to every workspace you access.

To set your default app, do the following:

1. Click your user image in the upper right to display the menu, then select **Account settings**.
2. Go to **Defaults > Default application**. Click the field to select your default app.
3. Click **Save**.

If you do not set a default app, at each new login AoC displays the last app you had open before your previous logout.

Set your default workspace

If you have membership in multiple workspaces, you can designate one of them as your default workspace. Each time you log in to Aspera on Cloud, your default workspace displays. Your choice of default workspace applies to both the Packages app and to the Files app.

To set your default workspace, do the following:

1. Click your user image in the upper right to display the menu, then select **Account settings**.
2. Go to **Defaults > Default workspace**. Click the field to display your list of workspaces, then select one as default.
3. Click **Save**.

If you do not set a default workspace, the app displays the first workspace you pinned. If you do not select a default workspace or a pinned workspace, Aspera on Cloud displays the first workspace returned in the `/workspaces` call.

Set your default download location

You can set or change the location for the folders, files, or packages you download using the IBM Aspera Connect transfer client in Aspera on Cloud. Once set, you can override this location for a specific transfer by selecting Download to.... instead of Download.

If you don't set this location, either through your Account preferences or by directly configuring Aspera Connect, the items you download end up in your Downloads folder or to the location set for your browser.

1. Click your user image in the upper right to display the menu, then select **Account settings**.
2. Go to **Download location for Aspera Connect transfers > Change download location**.
3. When Aspera Connect opens, click **Transfers** in the Preferences dialog.
4. In the Downloads location field, enter or browse to your intended location.
5. If you want to set an intended location for each download, click "Always ask me where to save downloaded files."
6. Click **Save**.

To close Account settings, click < at the top of the page.

Add your public key

You can add a public key to your Aspera on Cloud account, to be used in conjunction with your private key when accessing the Aspera on Cloud API using an API client.

This procedure assumes you have already generated your key pair and have your public key available in PEM format.

To add your public key, do the following:

1. Click your user image in the upper right to display the menu, then select **Account settings > Profile**.
2. Paste your public key in to the text box labeled **Public key**.
3. Click **Save**.

Subscribe to email notifications

You can subscribe or unsubscribe to specific Aspera on Cloud email notifications. The settings you select apply to notifications in every workspace you are part of, and override notification settings configured by the administrator.

To subscribe or unsubscribe, do the following:

1. Click your user image in the upper right to display the menu, then select **Account settings > Notifications**.
2. Select or deselect to subscribe to the notifications you wish to receive.
3. Click **Save**.

Disable IBM Aspera Connect

If and only if your organization supports IBM Aspera HTTP Gateway, you can disable IBM Aspera Connect transfer client and the default prompt to install Aspera Connect.

The Aspera on Cloud administrator may deploy the Aspera HTTP Gateway as an alternative transfer method when some users cannot download and install desktop software like Aspera Connect.

If your organization does not support Aspera HTTP Gateway, you must download and install Aspera Connect to upload from or download to your desktop.

You can transfer among remote sources without either transfer method. For example, go to the Files app, right-click a files or folder to select Move or Copy, then select the destination.

To disable the Aspera Connect transfer client and the default installation prompt, do the following:

1. Click your user image in the upper right to display the menu, then select Account settings.
2. Set the toggle labeled Disable IBM Aspera Connect to On. If you don't see this setting, your organization does not support Aspera HTTP Gateway; you must use Aspera Connect to transfer to and from your desktop.
3. Click Save.

Packages app: Send and receive files and folders

The Aspera on Cloud Packages app lets you assemble copies of any number of files and folders into a digital "package" and send the package to others. You can also send colleagues a link that allows them to send you a digital package. And learn how to use a shared inbox for enhanced collaboration with your teams. Get detailed procedures in this section.

- [Get started sending files and folders](#)
Dive in to sending and receiving files and folders the Aspera way! Get answers to these common questions: What is a package anyway? And why should I send instead of share my files and folders? And how?
- [Send files and folders in a digital package](#)
Learn more — or even become an expert — using these detailed procedures for sending and requesting files and folders. Create a personal distribution list to accelerate your common tasks. Also learn about forwarding packages you receive, downloading, recalling, and resending packages, and even adding recipients to an existing package. For packages you send, you can verify which of your recipients have downloaded it. And, of course, you can delete packages whenever you need to do so.
- [Request files and folders](#)
Learn to use, customize, revoke, and manage AoC *submission links*, the links you send to a colleague to allow them to send a digital package to you or to a shared inbox, even if they are not members of your AoC workspace.
- [Shared inboxes](#)
An Aspera on Cloud shared inbox is an optional workspace feature in the Packages app. You can send content directly and simultaneously to all members of the shared inbox without having to address it to particular users or user groups.

Get started sending files and folders

Dive in to sending and receiving files and folders the Aspera way! Get answers to these common questions: What is a package anyway? And why should I send instead of share my files and folders? And how?

- [What is a package?](#)
In the Packages app, a package (also called a digital package) is a collection of digital assets (files, folders, video, images, etc.) that you gather to send to one or more individuals or user groups, or to an Aspera on Cloud shared inbox. When you send a package, Aspera on Cloud creates copies of the content you attach for each recipient; the source content remains unchanged.
- [Should I send or share?](#)
Sending files and folders using the Packages app and sharing folders in your Files app both initiate a FASP (fast, adaptable, secure, predictable) transfer. However,

there are important distinctions between sending content and sharing content using Aspera on Cloud.

- [Save packages as drafts](#)

If you are not ready to send your packages right away, you can save them as drafts.

- [Schedule packages to send later](#)

Schedule packages to stage deliveries for future release.

- [Quick start: Send files and folders](#)

Sending even the largest files or data sets is quick and simple, much like sending an email with attachments. Your recipients receive a copy of the files and folders you attach.

- [Quick start: Request a file](#)

To ask another person to send you files and folders, send a submission link. The submission link allows them to send you a digital package using IBM Aspera high-speed transfer technology.

What is a package?

In the Packages app, a package (also called a digital package) is a collection of digital assets (files, folders, video, images, etc.) that you gather to send to one or more individuals or user groups, or to an Aspera on Cloud shared inbox. When you send a package, Aspera on Cloud creates copies of the content you attach for each recipient; the source content remains unchanged.

Introduction

For a procedure, see [Quick start: Send files and folders](#).

Aspera on Cloud allows you to use your Finder or Explorer to browse your local desktop, hard drive, or a remote source to select content to add to the package. You can also drag and drop content from any of these sources to the package as you construct it.

You can also attach files and folders in your Files app as you create a digital package in the Packages app; simply right-click the items in your Files app to include in the package and select the option to send. You can add content to a package you initiate from the Files app.

Once you are satisfied with the contents of the package, you can send it to the recipients you designate. Recipients can be:

- One or more of the following:
 - Aspera on Cloud users or groups in your workspace
 - All members of your Aspera on Cloud workspace (depending on settings configured by your admin)
 - Aspera on Cloud users outside your workspace, or users who do not have an Aspera on Cloud account (depending on settings configured by your admin)
- An Aspera on Cloud shared inbox (depending on settings configured by your admin)

Once you have sent the package, you must [recall](#) it to add, change, or remove the content in it. Your recipients can view, move, download, change or delete the copies of the content you send them without affecting the source content. For more information, see [Should I send or share?](#)

Monitor package transfer

Sending a package initiates a [FASP transfer](#); if desired, you can monitor the transfer in the [transfer panel](#) . You can also view statistics for recent, completed transfers.

Your Inbox and Sent folders

When the transfer completes, Aspera on Cloud displays the package in your recipient's Inbox and in your Sent folders. From that location, you and your recipient can do the following:

- Open the package to view its contents, along with summary details about the transfer, including status, size, average rate, duration, whether the package has been downloaded by recipients, and other information.
- Download all or part of the content to your local machine or to a remote storage location.
- Move package contents directly into your Files app.

Drafts folder

When a package transfer fails to start, AoC displays a toast message and moves the package to the Drafts folder in your Packages app. You must resend the Draft package with the intended content. See [Resending "Draft" packages](#).

Package details panel

You can click any package row to display the package contents and the package details panel. Click More detail to see package info like size, date, and contents (except archived and deleted packages), average transfer speed, package metadata if applicable, package recipients, and which recipients have downloaded all or part of the package.

Should I send or share?

Sending files and folders using the Packages app and sharing folders in your Files app both initiate a FASP (fast, adaptable, secure, predictable) transfer. However, there are important distinctions between sending content and sharing content using Aspera on Cloud.

If you are an admin, remember that in any organization or workspace, you can allow users to send, or share, or both. You can configure transfer options based on what your team is used to or on how you want your team to perform transfer tasks.

Introduction

Send: Like sending an email with attachments

Sending files and folders using the Aspera on Cloud *Packages app* is very much like sending an email with attachments. Senders use a simple form to address recipients and attach content. Recipients receive a copy of the content and can download it to use however they want.

Share: Like collaborating in a shared file repo

Sharing folders using the Aspera on Cloud *Files app* is like collaborating using a shared file repository. Each user has access to certain folders in the repo, with specific permissions to each folder and its contents. Files app users can share their folders with others, assigning content permissions to each recipient. Keep in mind that when you upload to your Files app, no one sees your folder until you share it with them.

Send: Send a copy of files and folders using the Packages app

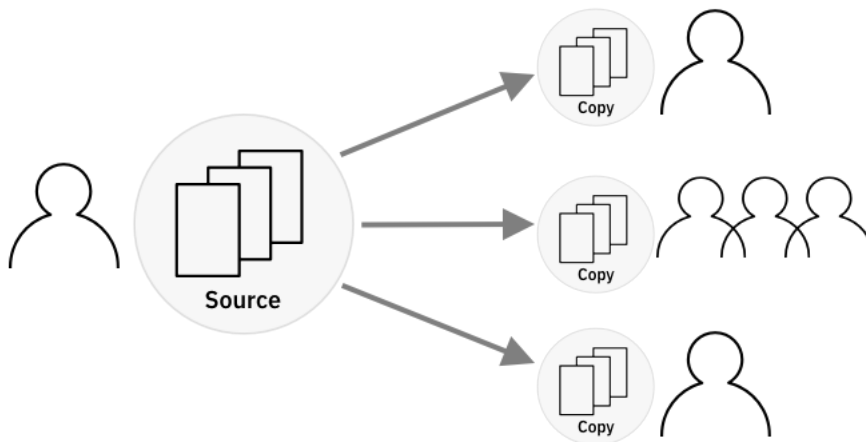
Use the AoC Packages app to send, receive, and request files and folders.

When you send files and folders, you send a *copy* of the source content to your recipients.

- You cannot modify the copy once you send it. Changes you make to the source content do not affect the copy you sent.
- Changes the recipient makes to the copy do not affect your source.
- Your recipient can act in any way on their copy of the content you send. Unlike sharing, you do not assign permissions to content you send.

You can send files and folders from any connected source: your own computer, an attached drive, share, or cloud storage, your Files app, and so on.

To request files, send a [submission link](#), also called a *file request*. Such a link enables another user to send files and folders to you.



Who can send to whom?

By default, any workspace member with access to the Packages app can send files to and request files from anyone else. Workspace members may also be able to send to users and groups outside the workspace.

As an admin, you can protect content security by using any of several options to restrict valid recipients outside the workspace. If necessary, you can keep all Packages app exchanges within the realm of the workspace. For details, see [Collaboration: Open or closed?](#) and [Content security in the Packages app](#).

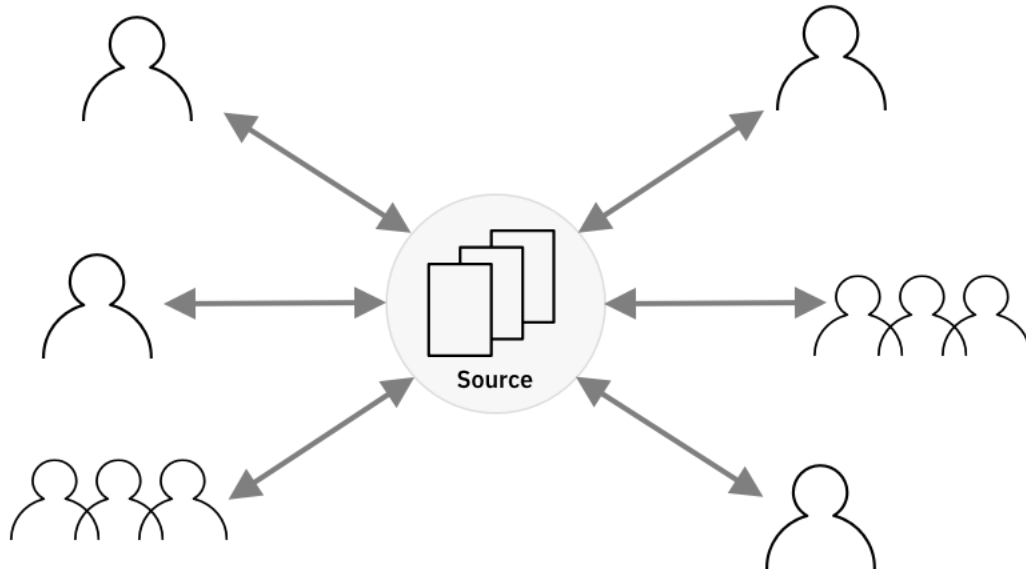
Share: Give others access to your *source* content using the Files app

Use the AoC Files app to share folders.

When you share a folder, you give others access to your *source* content. The folder content is *live*: all users with shared access can update folder contents and see the updates others make. You assign access permissions to the folder for each person you share with. These permissions determine what that person can do with the folder you share.

The folder to share must be in your AoC environment. There are three ways to get content into your Files app:

- You can upload a folder to your Files app and share it. Other members of your workspace won't be able to see the folder you upload until you share it. You can also upload a file, but you can only share a folder. To share a file, place it in a folder and share the folder.
- When someone shares a folder with you, it appears in your Files app. You can share a folder that has been shared with you.
- You can move files and folders from your Packages app to your Files app. Once in the Files app, you can share it.



Who can share with whom?

By default, any workspace member with access to the Files app can share folders with anyone else. As an admin, you can protect content security by using any of several options to restrict valid recipients outside the workspace. If necessary, you can keep all Files app exchanges within the realm of the workspace. For details, see [Collaboration: Open or closed?](#) and [Content security in the Files app](#). For configuration procedures, see [Files App: Using a shared file repository](#).

Shared content permissions

When you upload a folder to your Files app, you have all permissions to it. When someone shares a folder with you, you have the permissions they assign to you.

Permissions may include:

- Browse (View)
- Preview
- Rename
- Upload to
- Download
- Delete
- Create a new folder in

When you share a folder, you assign permissions to each user you share with. You can assign, at most, only the permissions that you yourself have to the folder; you can also share a folder and grant fewer permissions than you have to it.

For example, if a colleague shared a folder with you, giving you Browse, Preview, and Delete permissions, you can share that folder with another person, giving them the same Browse, Preview, and Delete permissions that you have. You can also share the that folder with only Browse permission. But you cannot share the folder with Download permission, since you don't have that permission to the folder. For a full discussion, refer to [Content permissions](#).

Save packages as drafts

If you are not ready to send your packages right away, you can save them as drafts.

1. In the Packages app, click Send files, in the Files app, right-click the file or folder to send, then select Send.
2. If you want to prepare the files you want to send, follow the instructions in the [Quick start: Send files and folders](#) section.
Note: You don't need to fill out the required fields to be able to save a draft.
3. Click Cancel.
4. You will be prompted to select between two options:
 - Save as draft and send later (transfer begins now but package won't be sent): Saves the package draft with its contents and triggers a transfer. The package is not sent to the recipient.
 - Discard attached files and save package details only: Saves the package draft metadata only. Contents of the package are discarded.
5. Click Save.

To access your saved drafts, go to the Drafts/Scheduled page from the left menu.

Important: You can encrypt your transfers when saving a draft for the first time, but not for transfers added to a draft package later.

Schedule packages to send later

Schedule packages to stage deliveries for future release.

1. In the Packages app, click Send files.
2. Prepare the files you want to send, follow the instructions in the [Quick start: Send files and folders](#) section.

3. Click Schedule for later and set the toggle to On.
4. Set the Release date and Choose a time for your package to be released in the future.
5. Optional – To protect your package with a password, click Password protection and enter one in the Password (optional) field.
Note: Package recipients will need to enter this password to decrypt its contents. This password is not sent through IBM Aspera.
6. Click Expiration policy to set a specific condition for your package files to expire after certain criteria is met.
 - Delete files by time (optional): Select a time from the drop down. If you choose Custom you can enter a specific date.
 - Delete files by download records: Choose between Delete after any recipient download all files, or Delete after all recipients download all files.
7. Click Send.

Your package is saved and will be sent at the specified date and time you selected.

Quick start: Send files and folders

Sending even the largest files or data sets is quick and simple, much like sending an email with attachments. Your recipients receive a copy of the files and folders you attach.

1. Open the sending form in the Packages app or in the Files app:
To change apps, use the app switcher 
 - In the Packages app, click **Send files**.
 - In the Files app, right-click the file or folder to send, then select **Send**.
2. Add recipients in the To field.
3. Enter a subject in the Package title field.
4. Attach content to send: drag and drop files and folders to the form, or click **Add files** to browse for content.
5. Click **Send**.

See also [Sending: Detailed procedure](#).

Quick start: Request a file

To ask another person to send you files and folders, send a submission link. The submission link allows them to send you a digital package using IBM Aspera high-speed transfer technology.

When your recipient clicks the link, Aspera on Cloud opens a web portal that allows your recipient to select content to send to you. The files and folders they send arrive to your inbox in a digital package.

To request files and folders using a submission link, do the following:

1. In your Packages app, click My inbox.
2. Click Manage submission link.
You can create a New link or send an existing link.
3. Click the Copy icon and send the link to your recipients according to your local site practice.

For details on managing submission links, including setting expiration dates, see the articles in [Request files and folders](#).

Send files and folders in a digital package

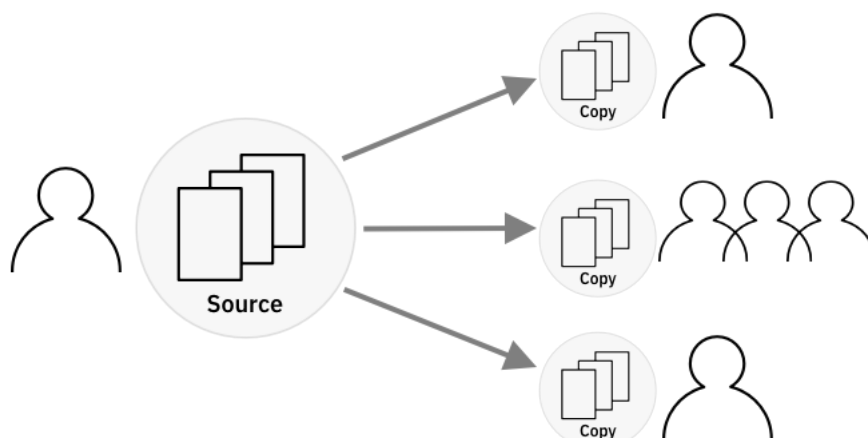
Learn more — or even become an expert — using these detailed procedures for sending and requesting files and folders. Create a personal distribution list to accelerate your common tasks. Also learn about forwarding packages you receive, downloading, recalling, and resending packages, and even adding recipients to an existing package. For packages you send, you can verify which of your recipients have downloaded it. And, of course, you can delete packages whenever you need to do so.

- [Sending: Detailed procedure](#)
Send others a copy of your source material using the Packages app. Once you send the copy, changes you make to the source material do not affect the copy you send. Changes your recipients make to the copies you send do not affect your source material.
- [Save packages directly to your Files app repo](#)
You can move an entire digital package or specific package components from your Packages app directly into your Files app. Note that you must have Upload permission to the destination folder in your Files app. From that location in your Files app you can share the content as needed.
- [Download from the Packages app](#)
You can download an entire digital package or specific items in the package. You can download packages in your Sent, Received, and Drafts lists. Once a package expires or is deleted, you can see details about the contents, but the contents are no longer available to download.
- [Sending: Become an expert](#)
Use this article to understand the nuances of the basic sending procedure, as well as the many optional features you can use when you send a digital package.
- [Create a personal distribution list](#)
Create a personal distribution list to send packages to a list of contacts. Contacts can be Aspera on Cloud user names and groups, along with external email addresses.
- [Forward a package](#)
You can forward a package from your personal inbox, from a shared inbox, from your Sent list, or from your Archived list. When you forward a package, the entire package is sent to those you list in the Recipients field. The forwarded package contains the original attachments and message; before you send it, you can remove any of the original attachments or attach additional files and folders; and you can add to the message.
- [Add recipients to a sent package](#)
You can add new recipients to a package you sent or received. Add recipients to an existing package when you simply want to make the package available, as is, to additional users. If you need to add or remove content, or change any package settings (such as password protection, content expiration, and so on), forward the package instead.

- [Recall a package](#)
When you recall a package you sent, the package in your Sent list shows the "Recalled" flag. Click the package row to open it; you can add or remove recipients and contents, and change other package settings. Your recipients see the "Recalled by sender" flag on the package in their inbox; they cannot browse or download package contents until you resend it. However, if a recipient downloads the package before you recall it, you cannot retrieve that downloaded content.
- [Resend packages in the Drafts folder](#)
This topic describes why packages you send may end up in the "Drafts" folder rather than being delivered to your recipients as expected. It also describes how to troubleshoot the issue and send the package as intended.
- [Delete a package you sent](#)
You can delete the contents from a digital package you sent. Aspera on Cloud retains package summary statistics even when you delete package contents.
- [Verify whether a package has been downloaded](#)
You can view details for each package you send, including recipients, package size and number of files and folders, package metadata (if applicable), the average transfer rate, and more. You can also determine who has downloaded your package, either in whole or in part.

Sending: Detailed procedure

Send others a copy of your source material using the Packages app. Once you send the copy, changes you make to the source material do not affect the copy you send. Changes your recipients make to the copies you send do not affect your source material.



For a simplified procedure, see [Quick start: Send files and folders](#).

1. Open the sending form in the Packages app or in the Files app:
 - In the Packages app, click **Send files** to open the sending form.
 - In the Files app, you can:
 - Send one item by right-clicking the item and selecting **Send via Packages**.
 - Send multiple files or folders by selecting each item to send, then clicking **Send via Packages** at the top of the files list.

Note: You cannot attach an entire folder that has been shared with you; instead, open the folder and attach the contents as individual items.
2. In the To field, enter recipients (see the *Recipients* section in [Sending: Become an expert](#)).
3. To send a blind copy, click **BCC** in the Recipients field to display the BCC field; enter the blind recipients (see the *BCC* section in [Sending: Become an expert](#)).
4. Send notifications about this package if desired (for details, see the *Notifications* section in [Sending: Become an expert](#)):
 - a. Click Notifications.
 - b. To notify a user that this package was uploaded to the relevant transfer server and is now accessible by the recipients, enter the username or email in the **When the package is available** field.
 - c. To notify a user that this package was downloaded, either in whole or in part, and by whom, enter the username or email in the **When the package is downloaded** field.
5. In the Package title field, give this package a label. This label identifies this package in your Sent list and in your recipients' Inbox lists.
6. If required, add more files or folders to send using one of these methods:
 - To send content contained in one of your existing packages, click the package row to display the content, then drag the intended files and folders to the file attachment area of the form.
 - Drag content from your computer or a remote source and drop it into the file attachment area of the form.
 - Click **Add files**, select **File** or **Folder** to open your Finder or Explorer and browse for items to attach.
 - Click **Upload**, select **Upload from Files** to view files in your Files application. You can select files and folders from any location in your Files app to add to this package.
7. If you see the **Apply watermark** toggle, you can switch it to **On** to apply a digital watermark to enable security and traceability for files in this package.

Note:
Watermarking is applied only to the files in the package that conform to supported profiles. Profiles comprise not only file types, but codecs, dimensions, and more; see the [Irdeto watermarking service documentation](#) for requirements. See the *Watermarking* section in [Sending: Become an expert](#).

You may be unable to send a watermarked package to recipients who are not members of your workspace. Your admin controls this setting.
8. To include an optional message with this package, enter it in the Package message field.
9. If you need this content to remain encrypted at the destination, do the following:

Note: Important: Do not apply password protection to a watermarked package.

Your administrator may have required encryption at rest for all packages in your workspace; in that case, skip to step c below.

 - a. Click **Password protection**.
 - b. Enter and confirm a password for this package. Your recipients must apply this password to decrypt the content.

- c. Deliver the password to your recipients according to your local site security practices
10. Set an expiration for this package if desired. When the package expires, the content is no longer available to recipients. Your administrator may have given you the ability to set an expiration policy for this package, or to change the expiration policy set globally by the administrator. If you have this capability, you can do the following (for details, see the *Package expiration policy* section in [Sending: Become an expert](#)):
 - a. Click **Expiration policy**.
 - b. Configure package expiration based on a number of days after the user receives it. The smaller the number, the sooner the package is deleted.
In the field labeled **Delete files by time**, select a pre-configured time period or set a specific date.
 - c. Configure package to expire after all recipients have downloaded it.
In the field labeled **Delete files by download records**, select the required option.
- Note: If you set both policies for this package, AoC deletes the package according to the policy that applies first.
11. Do one of the following:
 - a. Click **Send**.
 - b. Click **More**. On the next panel, enter the relevant information into the fields displayed; click **Send**. See the *Sending to a Shared Inbox* section in [Sending: Become an expert](#).

Results

When you send to someone in your workspace, Aspera on Cloud generates an email notification to your recipients, alerting them that the package you sent is available in their AoC Packages app inbox, in the same workspace you sent from. The email contains a link that allows them easy access to the package.

When you send to someone outside your workspace, or to someone who does not have an Aspera on Cloud account, Aspera on Cloud also generates an email notification to your recipients. The email contains a link that opens a web page that allows them to download the package.

Save packages directly to your Files app repo

You can move an entire digital package or specific package components from your Packages app directly into your Files app. Note that you must have Upload permission to the destination folder in your Files app. From that location in your Files app you can share the content as needed.

To save content from a digital package to your Files app, do the following:

1. To move the entire package to your Files app, right-click the package row and select **Save in Files**. A new window opens to display the contents of your Files app.
2. To move one or more items in the package, click the package row to open it, right-click the item and select **Save in Files**. A new window opens to display the contents of your Files app.
3. Save package contents to an existing folder or to a new folder:
 - To save to an existing folder, double-click the folder row to open it, then click **Save**.
 - To save to a new folder, do the following:
 - Go to the location to create the new folder.
 - Click **Create folder**.
 - Name the new folder and click **OK**.
 - Click the new folder to open it, then click **Save**.

Download from the Packages app

You can download an entire digital package or specific items in the package. You can download packages in your Sent, Received, and Drafts lists. Once a package expires or is deleted, you can see details about the contents, but the contents are no longer available to download.

To download packages or items within packages, do the following:

1. To download an entire package to your default download location, right-click the package row and select **Download**.
To change your *default* download location, open Aspera for desktop, go to Settings > Transfers. Click Choose location, and select the default location for your downloads.
2. To download multiple packages, select the check box to the left of each package to download and click **Download** at the top of the Packages list.
3. To download one or more items from within a package, do the following:
 - a. Click the package row to display the details panel.
 - b. To download a single item to your default download location, click the Download icon on the item row.
 - c. To download multiple items to your default download location, select the check box to the left of each item and click **Download** at the top of the content list.

Sending: Become an expert

Use this article to understand the nuances of the basic sending procedure, as well as the many optional features you can use when you send a digital package.

Overview

Sending content using Aspera on Cloud is similar to sending an email with attachments.

You can select content to attach (files, folders, video, images, and so on) from your local machine, from a remote source, or from your Files app.

When attaching folders that are in your Files app (rather than on your desktop or a remote source), note the following:

- You can attach a folder that you uploaded to the Files app yourself.
- You can attach a folder that you moved to your Files app from a package you received.

- You **cannot** attach an entire folder in your Files app that has been shared with you; instead, open the folder and attach the contents as individual items.

Aspera on Cloud collects the content you select into a [digital package](#), and transfers the package to your recipients when you click Send.

Recipients

You can send a package to either:

- One shared inbox (enter the shared inbox name)
- One or more of the following:
 - Aspera on Cloud users in your workspace (enter Aspera on Cloud user names)
 - Aspera on Cloud groups (enter Aspera on Cloud group names)
 - A [personal](#) or [workspace-level](#) distribution list
 - All members of your workspace (enter the workspace name; your administrator can disable this capability).
 - Aspera on Cloud users outside your workspace (enter Aspera on Cloud user names; requires specific permission: see "Sending to Outside Users" below)
 - People who are not Aspera on Cloud users (enter email addresses; requires specific permission: see "Sending to Outside Users" below)

Add new recipients to a sent package

You can add new recipients to a package you already sent.

Add recipients to an existing sent package when you simply want to make an existing package available, as is, to additional users.

If you need to add or remove content, or change any package settings (such as password protection, content expiration, and so on), forward the package instead. Note that you must be the sender or recipient of a package to forward it. See [Forwarding a Package](#).

Watermarking

You can add recipients to a watermarked package; AoC notifies the new recipients immediately as expected. The new recipients receive packages watermarked for them.

Procedure

1. In your Packages app, click **Sent** in the left panel.
2. Right-click the row of the intended package and select **Add recipients**.
3. Enter the name of additional recipients for this package, then click **Save**.

BCC

Blind-copy recipients see all standard recipients and the entire message, and receive all attachments. Standard recipients cannot see that the blind-copy recipients are included.

When blind-copy recipients download the attachments, Aspera on Cloud increments the download count in the package summary panel only for the sender and for the blind-copy recipients; standard recipients do not see the download counter increment for blind-copy downloads.

You can send to BCC recipients only, without recipients in the To field.

Sending to outside or external users

There may be limits on the outside users to whom you can send. In Aspera on Cloud, *outside* or *external* users are either of the following:

- Aspera on Cloud users who are not members of your current workspace.
- People without an Aspera on Cloud account.

When you send a package to an outside user, Aspera on Cloud delivers an email notification to your recipients; the email contains a link that allows them to access the package. Your recipients may be required to create an Aspera on Cloud account and log in to access the package. Aspera on Cloud presents a portal that provides access to the package you sent. The recipients do not become workspace members.

Notes:

- 1) Due to security reasons you are not allowed to send packages to external users on an Aspera on Cloud trial account.
- 2) You can also give an outside user access to Aspera on Cloud content by using the Files app to share a public link. A public link shares content rather than sending it in a digital package. For details and a procedure, see [Share with external users](#).
- 3) You may be unable to send a watermarked package to outside users. Your admin controls this setting.

Sending to a shared inbox

See also [What is a shared inbox??](#)

To send to a shared inbox, you must either be a member of the shared inbox with **Send** permission, or you must have a submission link that allows you to send. See [Request a package to a shared inbox](#).

If you address a shared inbox by name in the **To** field, all members of the shared inbox can browse and download the package contents, can forward the package, or save package contents to their own Files app. The administrator may have configured metadata fields to collect information about package contents; if so, the Send files form presents those to you as a sender when you click **Next**.

If desired, you can configure an application setting that accelerates your sending to a shared inbox. To configure this setting, do the following:

1. Click your user icon on the right side of the upper black banner; select **Account settings**.
2. In the Applications settings panel, select the check box labeled **Autofill the shared inbox name in the 'To' field when I send files from within a shared inbox**.

To take advantage of this setting when you are sending files and folders to a shared inbox, do the following:

1. In the Packages app, enter a shared inbox by clicking the inbox name in the left panel.
2. Click **Send files**.

The shared inbox name is automatically entered into the **To** field, saving you the time of entering it manually.

Watermarking

Forensic watermarking is an anti-piracy solution to prevent and trace illegal content redistribution and security breaches.

The AoC administrator can enable watermarking for packages sent in a given workspace. Once watermarking is enabled in a workspace, the admin can make watermarking required or optional.

- When required, Aspera on Cloud automatically applies a watermark to all packages sent from the workspace. Watermarking is transparent to the sender.
- When optional, you can choose whether to apply watermarking to a given package. You can click a toggle on the **Send files** form to apply watermarking.

In either case, every supported file type in the package receives the watermark. The watermark allows an integrated watermarking service to identify files outside the expected workflow and determine which individual users are most likely responsible for the piracy.

Supported File Types and Profiles

Watermarking is applied only to the files in the package that conform to supported profiles. Profiles comprise not only file types (supported file types are: .ts; .ps; .mpg; .mpeg; .mov; .mxf; .mp4), but codecs, dimensions, and more; see the [Irdeto watermarking service documentation](#) for requirements.

Special Characters Not Supported in File Names

Do not include files that have special characters in their names in a watermarked package.

Working with Watermarked Packages

A watermarked package in a package list displays the subtext "Watermarked".

Keep these points in mind as you work with watermarked packages:

- Recipients of watermarked packages must log in to retrieve the package. Traceability using forensic watermarking requires that users in the content workflow be authenticated. Therefore, package downloads from public links are not supported.
- Recalled packages: You cannot recall a watermarked package.
- Draft packages: If a transfer fails to start, AoC moves the package to the Drafts folder. You cannot change the watermarking setting for a package in the Drafts folder.
- Forwarded packages: You cannot forward a watermarked package.
- Adding recipients to a package: When you add recipients to a watermarked package, the new recipients receive packages watermarked for them. Adding recipients generates an immediate notification to the new recipients.
- Save to Files: You cannot use the Actions menu to save a watermarked package to the Files app.

Package expiration policy

Depending on the settings configured for your workspace, you can apply an expiration policy for this package or edit a policy already applied by the administrator. You can apply or edit one or both expiration policy types:

- Time-based expiration: Setting this policy type causes Aspera on Cloud to delete package contents at a configured number of days after the package transfer completes. For example, if you configure this setting for 10 days, Aspera on Cloud deletes package contents 10 days after the package becomes available to the intended recipients.
- Download-based expiration: Setting this policy type causes Aspera on Cloud to delete package contents after all recipients have downloaded the package (either the entire package or all the individual contents of the package in one operation), or after any one recipient has downloaded the package. For a shared inbox, the download-based policy can either delete or archive the package. Archiving moves the package from the shared inbox to the recipients' Archived tab. Archiving does not delete package content. The admin configures this setting.

If a policy already exists, you can further restrict the policy, but you cannot relax it. For example, if the admin-configured policy calls for expiration after 10 days, you can change the policy for this package to 5 days, but not to 12 days. Similarly, you can apply a download-based policy if one does not already exist, but you cannot remove it if it does exist.

When more than one policy is applied, the package expires or is archived based on the policy that applies sooner.

When a package expires according to the policy, the content is deleted from the transfer server and cannot be retrieved. You can view summary statistics for deleted packages by clicking the package row in your Deleted/Expired list.

When a package is archived according to the policy, the package is moved from the shared inbox to the recipients' Archived list.

Note: Your administrator may also have configured a separate policy that applies expiration parameters to packages you have sent and recalled and that now exist in Draft status.

Notifications

You can notify specific people or groups regarding package events by configuring notifications directly on the Send Package form.

- When the package is available: When your package is uploaded successfully to the relevant transfer server, Aspera on Cloud sends a notification to the individuals or groups you list in this field.
- When the package is downloaded: When a recipient downloads all or part of your package, Aspera on Cloud sends a notification to the individuals or groups that you list in this field. The notification includes the name of the recipient who downloaded.

Individuals and groups you list for notifications do not receive package contents or any message you include; Aspera on Cloud simply sends an email notification that the upload or download has occurred.

Create a personal distribution list

Create a personal distribution list to send packages to a list of contacts. Contacts can be Aspera on Cloud user names and groups, along with external email addresses.

You are the only person who can use and edit the distribution lists you create. You may also have access to distribution lists created by an administrator. Available distribution lists display in the auto-complete fields in the To field of the Send files form.

1. From the user menu () , select Account settings, then click the Distributions lists tab.
2. Click Create new.
3. Name your list. Use a name that is unique across the entire Aspera on Cloud organization; it's often useful to include your own name in the list and the word "list"; for example: Jin_list_projectA. Use your local conventions.
4. Click Create.
5. Enter the user names, groups, and email addresses for this list.
6. Click Add.

This distribution list is now available for you to enter or select in the To field of the Send files form.

Note: Aspera on Cloud validates the list when you click Send in the Send files form. If the list you select in the To field contains invalid recipients, the app displays a message that lists the invalid entries. You can send the package anyway, and only the valid recipients receive the package contents (valid external recipients are configured by your administrator).

Forward a package

You can forward a package from your personal inbox, from a shared inbox, from your Sent list, or from your Archived list. When you forward a package, the entire package is sent to those you list in the Recipients field. The forwarded package contains the original attachments and message; before you send it, you can remove any of the original attachments or attach additional files and folders; and you can add to the message.

Note: As an alternative to forwarding a package, you can add recipients to a package already sent. When you add recipients, you cannot change any of the contents or settings of the original package; you must send it as is. However, adding recipients to a sent package does not initiate another transfer, which conserves storage and bandwidth usage. For details, see [Add recipients to a sent package](#).

Note: You cannot forward a watermarked package.

Procedure

To forward a package, do the following:

1. Right-click the package row and select Forward to open the Send files form.
2. Complete the package forwarding procedure according to the steps in [Sending: Detailed procedure](#).

Add recipients to a sent package

You can add new recipients to a package you sent or received. Add recipients to an existing package when you simply want to make the package available, as is, to additional users. If you need to add or remove content, or change any package settings (such as password protection, content expiration, and so on), forward the package instead.

Note that you must be the sender or recipient of a package to forward it. See [Forward a package](#).

Watermarking

You can add recipients to a watermarked package; AoC notifies the new recipients immediately as expected. The new recipients receive packages watermarked for them.

Accessing Packages Sent by Other Workspace Members

You may be able to access all the packages sent by members of your workspace. Among other collaboration benefits, this access allow you to add recipients to a package sent by anyone in your workspace.

Note: Your administrator must enable this feature. If you do not see the filters described in step 2 below, contact your administrator to request this capability.

Procedure

1. In your Packages app, click Sent in the navigation panel.
2. If your admin has allowed all users in your workspace to access all packages sent in the workspace, you can filter the Sent packages listing by user.
 - a. The default filter setting is **All senders**. The setting displays all packages sent by all members of this workspace.
 - b. To display only packages you sent, click Sent by me.
 - c. To display only the packages sent by your fellow workspace members, click Sent by others.
3. Click the row of the intended package to open the details panel.
4. At the top of the details panel, click Add recipients.
5. Enter the name of additional recipients for this package, then click Add.

Recall a package

When you recall a package you sent, the package in your Sent list shows the "Recalled" flag. Click the package row to open it; you can add or remove recipients and contents, and change other package settings. Your recipients see the "Recalled by sender" flag on the package in their inbox; they cannot browse or download package

contents until you resend it. However, if a recipient downloads the package before you recall it, you cannot retrieve that downloaded content.

Note: You cannot recall a watermarked package.

Recalled package expiration

Your admin may have configured a package expiration policy that applies specifically to recalled packages. When you recall a package, the package becomes subject to that policy, if configured. When configured, the expiration timer resets each time you re-save the recalled package. For more information on package expiration policies, see the *Package expiration policy* section in [Sending: Become an expert](#).

Procedure

To recall a package, do the following.

1. In your Sent list, right-click the package row and select Recall; confirm Recall.
2. To edit and send a recalled package, do the following:
 - a. In your Sent list, click the row of the recalled package to open the Send files form.
 - b. To edit recipients, package name, message, or shared inbox metadata, edit directly in the relevant fields of the form.
 - c. To attach additional files and folders from a local or remote source, either click the Upload icon in the attachments section of the form and select the content to attach to the package, or drag the intended content from the source into the attachments section of the form.
 - d. To delete content currently included in the package, click X on the item row.
 - e. When your edits are complete, click Send.

Resend packages in the Drafts folder

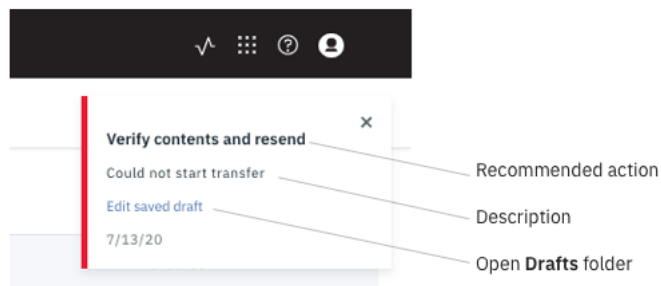
This topic describes why packages you send may end up in the "Drafts" folder rather than being delivered to your recipients as expected. It also describes how to troubleshoot the issue and send the package as intended.

Note: You must download and install IBM Aspera Connect to upload and download files and folders using the Packages app. Aspera Connect comprises both a free, lightweight app and a browser extension; you must install both. Further, you must allow Connect to connect your AoC app with the transfer server relevant to the files and folders in your package.

Failure to install the Connect app and browser extension, and failure to allow the connection to the transfer server are two of the primary reasons that Packages you send may end up in the Drafts folder.

For details, see [Installing Aspera Connect](#).

When AoC fails to start a transfer for a package you send, you'll see an error message, "Verify contents and resend". AoC moves the package to the Drafts folder in your Packages app. Click Edit saved draft in the error message to open the Drafts folder. You can also open the Drafts folder from the left panel of the Packages app.



In your Packages app Drafts folder, click the package row to view the package details. Any files and folders listed have been transferred successfully. Files and folders that you sent but are not listed did not transfer.

To add the missing content, click Upload or drag to add the missing items to the package. Then click Send. The files that were transferred successfully in the first attempt will not be transferred again since they already exist at your intended destination; this means you do not incur more transfer and storage charges. Yet the final package contents are intact in your Sent folder after the transfer succeeds.

Delete a package you sent

You can delete the contents from a digital package you sent. Aspera on Cloud retains package summary statistics even when you delete package contents.

When you delete package content, Aspera on Cloud removes the content permanently from the transfer server; it cannot be recovered.

You can delete packages you sent to an individual, a group, or a shared inbox. When you delete the contents of a package you sent, AoC removes the package from your Sent list and moves to your Deleted/Expired folder. It moves the deleted folder from your recipient's inbox to the recipient's Deleted/Expired folder. You and the package recipients can click the package row to view the package details.

Depending on notification configuration, Aspera on Cloud sends an email notification to package recipients that package contents have been deleted.

To delete the contents of package, do the following:

1. Right-click the package row and select Delete.
2. To delete multiple packages in one operation, select the intended packages. At the top of the package list, click Delete.

Verify whether a package has been downloaded

You can view details for each package you send, including recipients, package size and number of files and folders, package metadata (if applicable), the average transfer rate, and more. You can also determine who has downloaded your package, either in whole or in part.

This applies to users in the Packages app.

To display details for a package, do the following:

1. Click the package row to display the package details panel.
2. To display the download counters, click Download stats; user names and number of downloads displays.
3. To display package metadata, click Metadata.
4. To return to package contents, click Assets.

Aspera on Cloud provides many details about each digital package:

- If the package was sent to a shared inbox, the metadata (if any) attached by the sender
- Transfer/package status (Complete, Active, Paused, Failed, Expired, Deleted)
- Package size; number of files and folders
- Average transfer rate
- Transfer start and complete dates and times
- Number of full downloads of package contents, and by whom (this setting can be hidden by the administrator)
- Number of partial downloads, and by whom (this setting can be hidden by the administrator)
- Number of active/in-progress downloads, and by whom
- Package expiration details, if applicable

Request files and folders

Learn to use, customize, revoke, and manage AoC *submission links*, the links you send to a colleague to allow them to send a digital package to you or to a shared inbox, even if they are not members of your AoC workspace.

- [What is a submission link?](#)
When you need to ask another person to send you files and folders, you can send a submission link (sometimes called a file request). A submission link allows the other person to send you a digital package using IBM Aspera high-speed transfer technology. A submission link is a feature of the Packages app.
- [Request a package to My inbox](#)
To ask another person to send you files and folders, send a submission link. The submission link allows them to send you a digital package using IBM Aspera high-speed transfer technology.
- [Request a package to a shared inbox](#)
You must be a member of the shared inbox with 'Add users' permission to invite someone to send a package to the shared inbox.
- [Customize submission links](#)
You can customize the submission link URL if your Aspera on Cloud administrator has configured this capability for your workspace.
- [Manage submission links](#)
For each submission link you create, you can edit it, send it again, copy it to your clipboard, or delete it.

What is a submission link?

When you need to ask another person to send you files and folders, you can send a submission link (sometimes called a file request). A submission link allows the other person to send you a digital package using IBM Aspera high-speed transfer technology. A submission link is a feature of the Packages app.

Use a submission link to ask others to send a [package](#) as follows:

- To you as an individual. The file you request appears in My inbox.
- To a shared inbox for which you have 'Add users' permission. The file you request appears in the shared inbox.

When you send a submission link, AoC sends an email notification to your recipients. The notification includes the submission link, which allows them to send you a digital package using Aspera's high-speed transfer technology, whether or not they have an AoC account.

When a recipient clicks the submission link in the email notification, AoC presents a sending portal that allows the user to collect the files and folders you asked for and send them to you in a digital package. The recipient of your invitation can send any number of packages until the link expires or until you revoke the link.

You can send an email message inviting your recipient to send you files or folders. This request is called a submission link, because the email includes a link that allows your recipient to use IBM Aspera technology to send, or submit, the files you request.

Note: Your administrator can limit the use of submission links to certain users, or can disable it for all users.

You can send a submission link to the following:

- A person without an Aspera on Cloud account.
- An Aspera on Cloud user who is not a member of your workspace.
- An Aspera on Cloud user who is a member of your workspace.

For a procedure to send a submission link, see [Request a package to My inbox](#) or [Request a package to a shared inbox](#)

Note: When someone submits a package for the first time, Aspera on Cloud prompts them to install Aspera Connect. For more information, refer to [What is IBM Aspera Connect?](#)

Request a package to My inbox

To ask another person to send you files and folders, send a submission link. The submission link allows them to send you a digital package using IBM Aspera high-speed transfer technology.

When you send a [submission link](#), AoC sends an email notification to your recipients. The notification includes the submission link, which allows them to send you a digital package using Aspera's transfer technology even if they do not have an AoC account.

When a recipient clicks the submission link in the email notification, AoC presents a portal that allows the user to collect the files and folders you asked for and send them to you in a digital package.

Note: When you send a submission link to someone who is not an AoC user, Aspera on Cloud prompts them to install Aspera Connect when they submit the package. For more information, refer to [Aspera Connect for Outside Users](#).

When you send a public submission link, you can set an expiration for the link, after which the link is invalid. You can also set a password for the link. Anyone who has the public link (and password, if required) can use it to send digital packages to you, whether or not they are a member of your organization, as long as the link is valid. The packages they send arrive in *My inbox*.

Create a new link

1. In your Packages app, click **My inbox** in the left-side panel.
2. Click **Manage submission link** in the upper right side of your inbox listing.
3. If this is your first link, click **Create one**. Skip to step 5.
4. To create an additional new link, click **Manage links**, then click **New link**.
5. To send the link as is, click the Copy icon and deliver to your recipient by email or another method.
To set an expiration date or require a password, select Edit from the overflow menu.
6. If a window displays allowing you to customize the link, enter the text you want for the link, then click **OK**. See "Customize the Submission Link" below.
7. To set an expiration date for this link, select an existing preset or select **Custom** and set the intended date.
8. To require a password for this link, do the following:
 - a. Set the toggle labeled **Password protection** to On. AoC displays a password field with an auto-generated password.
 - b. To automatically generate a different password, click the **Generate** icon.
 - c. To compose a custom password, enter it in the password field.
 - d. To copy the password to your clipboard, click the **Copy** icon.
 - e. Record the password in a secure location, then click **Save**.**Note:** Once you click **Save**, you cannot recover the password. Click the Generate icon for a new password that you can save and share with your recipients.
9. To generate an AoC email notification to your recipient that contains the link, do one of the following:
 - a. Select **Send** from the overflow menu.
 - b. Enter the recipient user names or email addresses.
 - c. Include a message to your recipients if desired.
 - d. Click **Send**.
 - e. If you set a password for this link, send the password to your recipients according to your local site security practice.
10. To send the link to your intended recipients using email or another method, do the following:
 - a. Click the **Copy** icon in the link field to copy the link to your clipboard.
Note: When you click **Copy**, you overwrite anything previously stored on your clipboard. If you previously copied the password for this link, be sure you have stored the password in a secure location before copying the link to your clipboard.
 - b. Deliver the link to your recipients as desired.
 - c. If you set a password for this link, send it to your recipient according to your local site security practice.

Send an existing link

When you send an existing submission link, various settings for the link already exist.

- **Expiration date**
The expiration date already exists, though it may be set to "Will not expire". You can change the expiration for an existing link and send it to a new recipient, but keep in mind that the new expiration setting affects everyone who uses that submission link. For example, suppose you sent Link1 to Recipient A with the link expiration set to 'Will not expire'. If you reuse Link1 to send to Recipient B and change the link expiration to 7 days, that new expiration applies to both recipients A and B.
 - **Password**
If you reset an existing password, the previous password becomes invalid. You must give the new password to previous recipients of the link.
1. In your Packages app, click **My inbox** in the left-side panel.
 2. In the upper right side of the window, click **Manage submission link**.
 3. Do one of the following:
 - a. Click **Copy**, then send the link to your intended recipient using email or another method.
 - b. Select Send from the overflow menu. Enter the email address for your recipient; enter comments if desired, then click **Send**.
 - c. In either case, send the password, if required, according to your local site security practice.

Delete a submission link

Anyone with your submission link (and password, if set) can send you packages until the expiration date you set (if any) or until you deleted the link.

To delete a submission link, do the following:

1. From My inbox, click Manage submission link.
2. On the link to delete, select Delete from the overflow menu.
The link immediately becomes invalid.

Request a package to a shared inbox

You must be a member of the shared inbox with 'Add users' permission to invite someone to send a package to the shared inbox.

Do you have 'Add users' permission? In your Packages application, click the shared inbox name in the left-side panel. If you have 'Add users' permission, you'll see an 'Add' button at the top of the right-side panel and a 'Share submission link' link below the list of collaborators.

When you send a [submission link](#) to invite someone to send to a shared inbox:

- They receive an email notification containing the submission link.
- When they click the link, a sending portal displays, pre-addressed to the shared inbox. If you send a private link and your recipient has 'Send' permission to more than one shared inbox, they can click the **To** field to access those other shared inboxes.
- You can send a link you've already created, or you can create a new link.
 - If you create a new link, you may be able to customize it, depending on what your administrator has allowed; see "Customize the Submission Link" below.
- You can send a **Private link** to a current member of the shared inbox.
 - The submission link invites a current member with Send permission to submit a package to the shared inbox.
 - This is an authenticated link: the user must log in to Aspera on Cloud to access the sending portal; all packages sent by that user are tracked by the user's name.
- You can send a **Public link** to someone who is NOT a member of the shared inbox.
 - This recipient may or may not have an Aspera on Cloud account.
 - You can configure an expiration date for each submission link; the recipient of your invitation can send any number of packages to the shared inbox until the link expires.
 - You can require the recipient to use a password when submitting a package.
 - Unless the submitter includes their name and email address in the sending form, Aspera on Cloud identifies the sender of such a package as "Anonymous Sender." (The administrator can configure a setting that requires the submitter's name and email.)
 - Note that if the person you invite forwards the submission link (and the password, if set) to another person, that second person can send as many packages as they want to the shared inbox as long as the link is valid.
- If the shared inbox requests metadata, the recipient of the submission link will see the metadata fields when they send a package; they must enter data in any required fields.

Procedure

1. Enter the shared inbox by clicking the inbox name in the left panel.
2. In the right panel, click **Manage submission links**.
3. To create a new link, do the following:
 - a. Select the desired heading, 'Private link' or 'Public link', then click **New link**.
 - b. If a window displays allowing you to customize the link, enter the text you want for the link or accept the existing text, then click **OK**. See [Customize submission links](#).
 - c. To set an expiration date or password for a public link, click Edit. In the Expiration date field, select a preset date or click **Custom** to configure the desired expiration.
 - d. To set a password for a public link, click Edit. Set the **Password protection** toggle to **On**.
 - e. To copy the link, click the **Copy** icon. Save the password to a secure location; once you click Save, you cannot recover the password. Click Save.
 - f. To send an email notification with the link, click Send. Enter the recipient user names or email addresses, then click **Send**. If this link requires a password, send the password to your recipients according to your local site security practices.
 - g. To copy this link to send using email or another method, click the **Copy** icon and deliver the link to your recipients as desired.

When you click Copy, you overwrite anything previously stored on your clipboard. If you previously copied the password for this link, be sure you have stored the password in a secure location before copying the link to your clipboard.
4. To reuse the most recent link, select the link and click **Copy**; send the link to your recipient using email or another method.

If a password is required for this link, send the password to your recipients according to your local site security practice. You can regenerate the auto-generated password or create a custom password. Keep in mind that changing the password affects all users of the link, including those you previously gave the link to.

Customize submission links

You can customize the submission link URL if your Aspera on Cloud administrator has configured this capability for your workspace.

When link customization is enabled, the default submission link:

- To 'My inbox' includes your user name (for example, https://aspera.pub/Karen_Lane).
- To a shared inbox includes the inbox name (for example, <https://aspera.pub/SharedInbox1>).

The final portion of the a link appears in an editable field. You can send the link as is or you can customize that final portion. For example, if you enter **New Link** into this editable field, Aspera on Cloud generates the following link: https://aspera.pub/New_Link.

Note that Aspera on Cloud generates a unique ID for each link and inserts it before the final component of the link. This unique link ID comprises four to eight alphanumeric characters, for example: https://aspera.pub/pFTD1K4/New_Link.

Manage submission links

For each submission link you create, you can edit it, send it again, copy it to your clipboard, or delete it.

To manage your submission links, do the following:

1. Click **Manage submission links**.
2. In the link listing, identify the intended link.

3. To edit the link, click **Edit**. In the panel that opens, make any changes required, then click **Save**.
 - If you change the expiration date, that new expiration applies immediately to everyone using that link.
 - If you change the password, you must send the new password to both new and existing users of the link.
4. To send a link, click **Send**. Enter recipient user names or email addresses, include a message to your recipients if desired, then click **Send**.
5. To copy the link to your clipboard, click the **Copy** icon.
6. To delete a link, click **Delete**. When you delete a link, it becomes invalid immediately, and recipients of that link can no longer use it to send you content.

Shared inboxes

An Aspera on Cloud shared inbox is an optional workspace feature in the Packages app. You can send content directly and simultaneously to all members of the shared inbox without having to address it to particular users or user groups.

- [What is a shared inbox?](#)
An Aspera on Cloud Packages app shared inbox is an optional workspace feature similar to a drop box: you can send content directly and simultaneously to all members of the shared inbox without having to address it to particular users or user groups.
- [Send to a shared inbox](#)
You can send a digital package to a shared inbox to make package content available to all members of the shared inbox. You must have proper permission to send to a shared inbox.
- [Request a package to a shared inbox](#)
You must be a member of the shared inbox with 'Add users' permission to invite someone to send a package to the shared inbox.

What is a shared inbox?

An Aspera on Cloud Packages app shared inbox is an optional workspace feature similar to a drop box: you can send content directly and simultaneously to all members of the shared inbox without having to address it to particular users or user groups.

An Aspera on Cloud administrator or workspace manager creates the shared inbox, then designates members of the shared inbox from among the workspace members; each member has specific permissions to the inbox.

You as an individual user in the workspace may have membership in one or more shared inboxes, or in none. You may have different permissions in each shared inbox. Your permissions may be different than the permissions of other shared inbox members.

Am I a member of a shared inbox?

Find your shared inboxes, if any, as follows:

- For inboxes to which you have Receive or Add users permission:
 - Click Inboxes in the left panel. Any inboxes in the list that are not labeled My Inbox are your shared inboxes. Click the shared inbox name to display the content in that shared inbox only.
 - Click Send files, then click in the To field of the form to display all shared inboxes to which you can send packages.
- For inboxes to which you have only Send permission, click Send Files, then click the Recipient field of the form to display the list of shared inboxes to which you can send packages.

When you send a [digital package](#) to a shared inbox, you send to all members of that shared inbox simultaneously; each shared inbox member receives their own copy of the content you included in the package. As with all package sending in Aspera on Cloud, sending content to a shared inbox initiates a [transfer](#), which you can monitor in the [Transfer monitor](#) if you wish.

Metadata

The Aspera on Cloud administrator or workspace manager can configure metadata fields for each shared inbox, and can make these fields either optional or required. When present, these fields allow senders to apply metadata tags to packages they send to a shared inbox; these tags provide information about package contents without requiring the recipient to open the package, and allow shared inbox members to search and sort packages easily. If any metadata data fields are required, you cannot send the package without addressing the required field.

Permissions

Shared inbox members may have one or more access permissions (configured by the Aspera on Cloud administrator or the workspace manager) to a given shared inbox; users see the shared inboxes they have at least one permission to in the list of all inboxes on the left side panel.

- **Send:** Members with Send permission can send packages to the shared inbox.
 - Click Send files; in the form that displays, click the To field to display a list of shared inboxes to which you have Send permission.
 - See [Sending: Detailed procedure](#).
 - Members with only Send permission cannot see contents or receive packages from this shared inbox.
- **Receive:** These members can access packages sent to the shared inbox.
 - In the list of all inboxes on the left side panel, click the shared inbox name; packages in the shared inbox display.
 - Members with only Receive permission cannot send a package (upload files or folders) to the shared inbox.
- **Add users:** These members can invite others to send packages to the shared inbox.
 - In the list of all inboxes on the left side panel, click the shared inbox name.
 - In the Collaboration panel on the right, look for the Add button; if present, this member has Add permission to this shared inbox.
 - See [Request a package to a shared inbox](#) for details.

Send to a shared inbox

You can send a digital package to a shared inbox to make package content available to all members of the shared inbox. You must have proper permission to send to a shared inbox.

1. Open the sending form in the Packages app or in the Files app:

To change apps, use the app switcher .

- In the Packages app, click **Send files**.
 - In the Files app, right-click the file or folder to send, then select **Send**.
2. Click the Recipients field to display the inboxes you can send to. Select the intended shared inbox.
Note: When you send to a shared inbox, you cannot add any other recipients, including BCC recipients and other shared inboxes.
 3. Enter a subject.
 4. Attach content to send: drag and drop files and folders to the form, or click **Upload** to browse for content.
 5. Click **Send** or **Next**.
If you see the Next button, this shared inbox allows or requires you to apply additional information (metadata) that helps recipients and admins sort and process the package you send.
 6. Select or enter appropriate data in all required fields, then click **Send**.

Request a package to a shared inbox

You must be a member of the shared inbox with 'Add users' permission to invite someone to send a package to the shared inbox.

Do you have 'Add users' permission? In your Packages application, click the shared inbox name in the left-side panel. If you have 'Add users' permission, you'll see an 'Add' button at the top of the right-side panel and a 'Share submission link' link below the list of collaborators.

When you send a [submission link](#) to invite someone to send to a shared inbox:

- They receive an email notification containing the submission link.
- When they click the link, a sending portal displays, pre-addressed to the shared inbox. If you send a private link and your recipient has 'Send' permission to more than one shared inbox, they can click the **To** field to access those other shared inboxes.
- You can send a link you've already created, or you can create a new link.
 - If you create a new link, you may be able to customize it, depending on what your administrator has allowed; see "Customize the Submission Link" below.
- You can send a **Private link** to a current member of the shared inbox.
 - The submission link invites a current member with Send permission to submit a package to the shared inbox.
 - This is an authenticated link: the user must log in to Aspera on Cloud to access the sending portal; all packages sent by that user are tracked by the user's name.
- You can send a **Public link** to someone who is NOT a member of the shared inbox.
 - This recipient may or may not have an Aspera on Cloud account.
 - You can configure an expiration date for each submission link; the recipient of your invitation can send any number of packages to the shared inbox until the link expires.
 - You can require the recipient to use a password when submitting a package.
 - Unless the submitter includes their name and email address in the sending form, Aspera on Cloud identifies the sender of such a package as "Anonymous Sender." (The administrator can configure a setting that requires the submitter's name and email.)
 - Note that if the person you invite forwards the submission link (and the password, if set) to another person, that second person can send as many packages as they want to the shared inbox as long as the link is valid.
- If the shared inbox requests metadata, the recipient of the submission link will see the metadata fields when they send a package; they must enter data in any required fields.

Procedure

1. Enter the shared inbox by clicking the inbox name in the left panel.
2. In the right panel, click **Manage submission links**.
3. To create a new link, do the following:
 - a. Select the desired heading, 'Private link' or 'Public link', then click **New link**.
 - b. If a window displays allowing you to customize the link, enter the text you want for the link or accept the existing text, then click **OK**. See [Customize submission links](#).
 - c. To set an expiration date or password for a public link, click Edit. In the Expiration date field, select a preset date or click **Custom** to configure the desired expiration.
 - d. To set a password for a public link, click Edit. Set the **Password protection** toggle to **On**.
 - e. To copy the link, click the **Copy** icon. Save the password to a secure location; once you click Save, you cannot recover the password. Click Save.
 - f. To send an email notification with the link, click Send. Enter the recipient user names or email addresses, then click **Send**. If this link requires a password, send the password to your recipients according to your local site security practices.
 - g. To copy this link to send using email or another method, click the **Copy** icon and deliver the link to your recipients as desired.
When you click Copy, you overwrite anything previously stored on your clipboard. If you previously copied the password for this link, be sure you have stored the password in a secure location before copying the link to your clipboard.
4. To reuse the most recent link, select the link and click **Copy**; send the link to your recipient using email or another method.
If a password is required for this link, send the password to your recipients according to your local site security practice. You can regenerate the auto-generated password or create a custom password. Keep in mind that changing the password affects all users of the link, including those you previously gave the link to.

Files app: Sharing folders

The Aspera on Cloud Files app lets you share folders in your workspace with others, granting specific permissions to each recipient for the content you share. Learn how to upload and download content to and from your Files app; how to move, copy, rename, and delete content; how to set notifications that alert you when new content appears in a shared folder you need to monitor; and more.

- [Get started sharing folders](#)

- [Sharing folders](#)
- [Share with outside users](#)
Learn how to use a *public link* to share folders with colleagues outside your workspace.
- [Sharing problems](#)
The section provides troubleshooting procedures for deleting or renaming large folders and for addressing problems with access to shared folders.

Get started sharing folders

- [Should I send or share?](#)
Sending files and folders using the Packages app and sharing folders in your Files app both initiate a FASP (fast, adaptable, secure, predictable) transfer. However, there are important distinctions between sending content and sharing content using Aspera on Cloud.
- [Quick start: Share a folder from your Files app repo](#)
You can share folders in your Files app. When you share folders, you give your recipients direct access to your source material. You also give each recipient a specific permission to access the folder contents.
- [Unshare a folder](#)
You may need to remove a colleague's access to a folder you shared with them. You can unshare a folder, whether your colleague has access as a folder collaborator or via a shared link.
- [Upload files and folders to the Files app](#)
You can upload files and folders to the Files app. Once you upload a folder, or upload a file to a folder in your Files app, you can share the folder with other users, giving them access to your source material.
- [Download from the Files app](#)
You can download files and folders from your Files app.
- [Sharing permissions](#)
When you share a folder, you assign specific access permission to each recipient. Similarly, when someone shares a folder with you, they grant you specific access permission. You can act on the shared content based on the permission assigned.
- [Which permissions do I have?](#)
The permission you have to a given file or folder depends upon how you gained access to it.

Should I send or share?

Sending files and folders using the Packages app and sharing folders in your Files app both initiate a FASP (fast, adaptable, secure, predictable) transfer. However, there are important distinctions between sending content and sharing content using Aspera on Cloud.

If you are an admin, remember that in any organization or workspace, you can allow users to send, or share, or both. You can configure transfer options based on what your team is used to or on how you want your team to perform transfer tasks.

Introduction

Send: Like sending an email with attachments

Sending files and folders using the Aspera on Cloud *Packages app* is very much like sending an email with attachments. Senders use a simple form to address recipients and attach content. Recipients receive a copy of the content and can download it to use however they want.

Share: Like collaborating in a shared file repo

Sharing folders using the Aspera on Cloud *Files app* is like collaborating using a shared file repository. Each user has access to certain folders in the repo, with specific permissions to each folder and its contents. Files app users can share their folders with others, assigning content permissions to each recipient. Keep in mind that when you upload to your Files app, no one sees your folder until you share it with them.

Send: Send a copy of files and folders using the Packages app

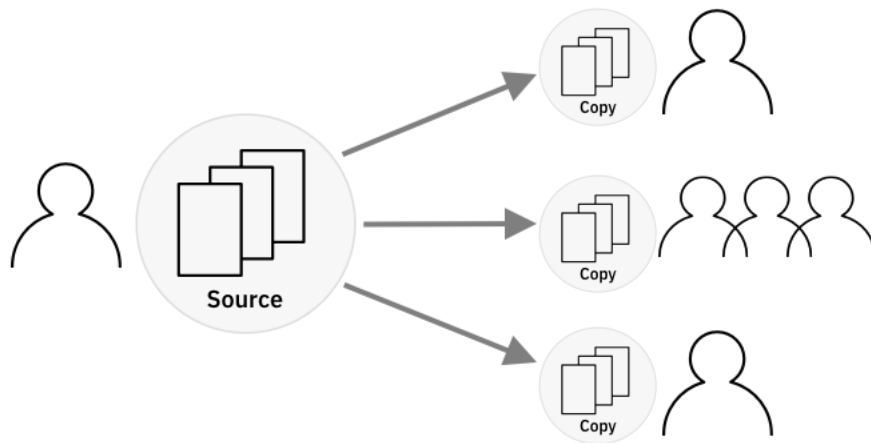
Use the AoC Packages app to send, receive, and request files and folders.

When you send files and folders, you send a *copy* of the source content to your recipients.

- You cannot modify the copy once you send it. Changes you make to the source content do not affect the copy you sent.
- Changes the recipient makes to the copy do not affect your source.
- Your recipient can act in any way on their copy of the content you send. Unlike sharing, you do not assign permissions to content you send.

You can send files and folders from any connected source: your own computer, an attached drive, share, or cloud storage, your Files app, and so on.

To request files, send a [submission link](#), also called a *file request*. Such a link enables another user to send files and folders to you.



Who can send to whom?

By default, any workspace member with access to the Packages app can send files to and request files from anyone else. Workspace members may also be able to send to users and groups outside the workspace.

As an admin, you can protect content security by using any of several options to restrict valid recipients outside the workspace. If necessary, you can keep all Packages app exchanges within the realm of the workspace. For details, see [Collaboration: Open or closed?](#) and [Content security in the Packages app](#).

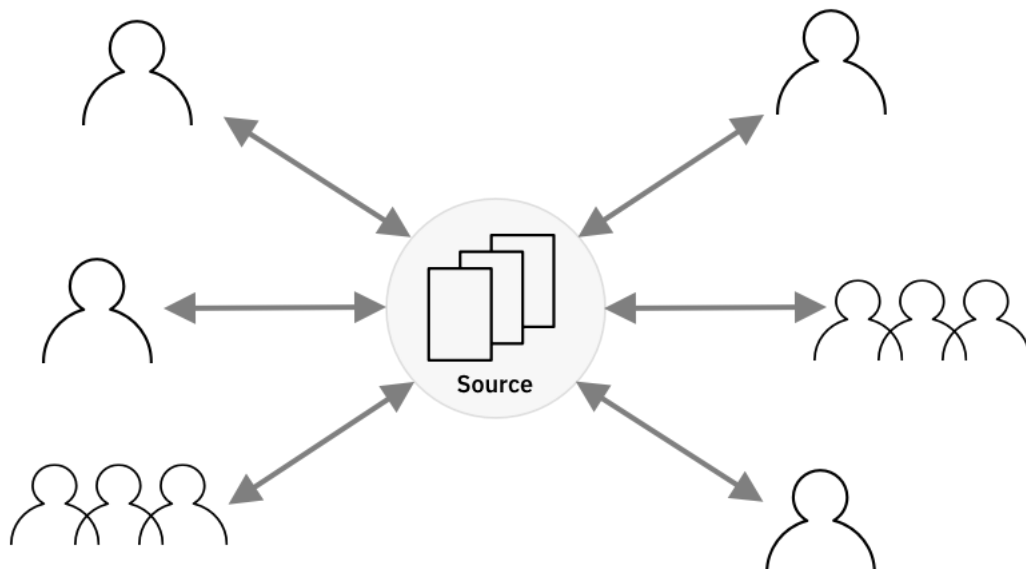
Share: Give others access to your *source* content using the Files app

Use the AoC Files app to share folders.

When you share a folder, you give others access to your *source* content. The folder content is *live*: all users with shared access can update folder contents and see the updates others make. You assign access permissions to the folder for each person you share with. These permissions determine what that person can do with the folder you share.

The folder to share must be in your AoC environment. There are three ways to get content into your Files app:

- You can upload a folder to your Files app and share it. Other members of your workspace won't be able to see the folder you upload until you share it. You can also upload a file, but you can only share a folder. To share a file, place it in a folder and share the folder.
- When someone shares a folder with you, it appears in your Files app. You can share a folder that has been shared with you.
- You can move files and folders from your Packages app to your Files app. Once in the Files app, you can share it.



Who can share with whom?

By default, any workspace member with access to the Files app can share folders with anyone else. As an admin, you can protect content security by using any of several options to restrict valid recipients outside the workspace. If necessary, you can keep all Files app exchanges within the realm of the workspace. For details, see [Collaboration: Open or closed?](#) and [Content security in the Files app](#). For configuration procedures, see [Files App: Using a shared file repository](#).

Shared content permissions

When you upload a folder to your Files app, you have all permissions to it. When someone shares a folder with you, you have the permissions they assign to you.

Permissions may include:

- Browse (View)
- Preview
- Rename
- Upload to
- Download
- Delete
- Create a new folder in

When you share a folder, you assign permissions to each user you share with. You can assign, at most, only the permissions that you yourself have to the folder; you can also share a folder and grant fewer permissions than you have to it.

For example, if a colleague shared a folder with you, giving you Browse, Preview, and Delete permissions, you can share that folder with another person, giving them the same Browse, Preview, and Delete permissions that you have. You can also share the that folder with only Browse permission. But you cannot share the folder with Download permission, since you don't have that permission to the folder. For a full discussion, refer to [Content permissions](#).

Quick start: Share a folder from your Files app repo

You can share folders in your Files app. When you share folders, you give your recipients direct access to your source material. You also give each recipient a specific permission to access the folder contents.

Note: You can share only folders; you cannot share a file. To share a file, place it in a folder, then share the folder.

Make sure that you are in the Files app. If necessary, use the app switcher .

1. Right-click the folder row and select **Share**.
2. Enter the name or email address of one or more collaborators.
3. Set the access permission that you want these collaborators to have for this folder.
4. Click **Add**.

For much more on collaborating using the Files app, see [Files app: Sharing folders](#)

Unshare a folder

You may need to remove a colleague's access to a folder you shared with them. You can unshare a folder, whether your colleague has access as a folder collaborator or via a shared link.

Remove a folder collaborator

To remove a folder collaborator's access to a shared folder, do the following:

1. Click to open the folder to unshare.
2. In the upper right, click the Collaborators icon; then click See all collaborators.
3. Find the intended collaborator; click the **Revoke** icon, then confirm.

Delete a shared link

To remove folder access via a link, do the following:

1. Right-click the intended folder and select **Manage all links**.
 2. For the intended link, click the trash can icon.
- Note:** When you delete a link, everyone using that link to access the folder loses access.

To troubleshoot unsharing issues, see [User still has access to unshared folder](#).

Upload files and folders to the Files app

You can upload files and folders to the Files app. Once you upload a folder, or upload a file to a folder in your Files app, you can share the folder with other users, giving them access to your source material.

Remember that files and folders you upload to your Files app are not visible to other workspace members until you [share](#) them. Note also that you have full Edit permission to content you upload.

Add files and folders to your Files app in any of several ways:

- Drag content from your local machine or from a remote source and drop it into your Files app.
- Click the Upload icon, select Upload file or Upload folder, then browse to select content from your Finder or Explorer.
The AoC administrator controls whether or not you can upload to your Files app. If you don't see the Upload icon, check with your admin.
- Save to your Files app from your Packages app; in your Packages app, do the following:
 1. To save an entire package, right-click the package row and select **Save in Files**.
 2. To save specific content within a package, click the package row to open the details panel; then right-click the item row and select Save in Files.
The root level of your Files app in the same workspace displays.
 3. Select the location in your Files app where you want this content to reside.

4. Click Save.

Note that you can save between apps in the same workspace only. You cannot save from the Packages app in Workspace A to the Files app in Workspace B.

Download from the Files app

You can download files and folders from your Files app.

To download items to your default download location (configure your default location in IBM Aspera for desktop: Settings > Transfers), select the checkbox on one or more rows, then click **Download** at the top of your Files list.

To override the default download location, select the checkbox on one or more rows, then click Download to...; select the intended location from your Finder or Explorer, then click OK.

Note: Selecting Download to... affects *only this download*. To change your *default* download location, open Aspera for desktop, go to Settings > Transfers. Click Choose location, and select the default location for your downloads.

If you are not using Aspera Connect, check the Downloads location of your browser.

You must have the required permission to an item to download it. If you don't have download permission, ask the person who shared the item with you to grant you Download permission. Check the secondary text on the row of the file or folder to see who shared it with you.

☐		2017-11-20_AspiraOne_Readout Shared by [redacted] to a group	924 MB 11 files

Sharing permissions

When you share a folder, you assign specific access permission to each recipient. Similarly, when someone shares a folder with you, they grant you specific access permission. You can act on the shared content based on the permission assigned.

There are four preset or composite permissions and seven custom permissions for content in your Files app:

- Preset or Composite permissions:
 - **Edit** (also called *Can Edit*)

This is the highest level of permission and gives a user full control over the item; it contains all other permissions.
 - **View** (also called *Download Only*)

Includes *Browse*, *Download*, and *Preview* permissions.
 - **Upload**

Includes *Create/Upload folders* and *Upload files*
 - **Preview**

Includes *Browse* and *Preview*
- Custom permissions (content must reside on a transfer server with node software at version 3.7.4 or higher; see the "Package Information" section of the IBM Aspera High-Speed Transfer Service [Release Notes](#) for specific build numbers for your platform):
 - **Create/Upload folders**

Create or upload an empty folder; to upload folders containing files, enable this permission along with *Upload files*.
 - **Rename**

Rename files and folders.
 - **Upload files**

Upload files and folders; to upload folders containing files, enable this permission along with *Create/Upload folders* permission -- or use *Upload* composite permission. See *Delete* below for uploading a file with the same name as an existing file (overwrite or replace). You need *Upload* permission to a folder to move or copy content to it.
 - **Download**

Download the folder or file in the folder.
 - **Preview**

Preview movie files in the folder. Thumbnail previews of supported image tiles are always available.
 - **Browse**

Browse folder content; if this setting is not enabled, you can see the folder but cannot view folder contents.
 - **Delete**

Delete or overwrite folder contents.

Which permissions do I have?

The permission you have to a given file or folder depends upon how you gained access to it.

To check your permission to a given file or folder, right-click the item and select **Info**.

- For items you upload (and for items you move from your Packages app) to the *root level* of your Files app (labeled **Home folder**), you have full *Edit* permission. If you don't see the **Upload** button in your **Home folder** level, your admin has restricted your permission. You may still have *Upload* permission to shared folders in your Files app.
- For items you upload or move into a given folder, you have the same permission that you have to the folder.
- For folders shared with you, you have the permission granted to you by the person who shared.

Note:

The person who shared a folder with you is the only person who can change your permission to that folder.

The person sharing can grant you only the permissions they have to the given folder, or a lesser permission. For example, if I have **Browse**, **Preview**, and **Download** permission, I can grant one or more of those three permissions to you for that folder, but I cannot grant you **Delete** permission, since I myself don't have **Delete** permission.

In the same way, the permission you can grant to a folder you share depends on the permissions you have to that folder. You can grant any or all of the permissions that you yourself have to that folder, but you cannot grant a permission that you do not have. And you are the only person who can change the permission you gave to a folder you shared.

Sharing folders

- [Determine who has shared access](#)
To determine who has access to a shared folder, use the information in this article.
- [Change permissions to a folder you shared](#)
For each folder you share, you grant specific access permission to each recipient you share with. You can change the permission you granted or revoke it entirely. No one else can change the permissions for a folder you shared.
- [Understand "Size" and "Last Updated" data](#)
This article describes how to interpret data in the *Size* and *Last updated* columns in the Files application. Understanding these data gives insight into how and when AoC refreshes the values displayed.
- [Set notifications for new content in a shared folder](#)
You can configure Aspera on Cloud to deliver email notifications to you when new content appears in a shared folder you need to monitor.
- [Move or copy content in your Files app](#)
- [Manage your shared links](#)
You can send shared links to give others access to folder contents. Each link gives the recipient specific access permissions. Use private links to share with current folder collaborators. Use public links to share with anyone. To view and manage your shared links, including resending, editing, and deleting links, use the procedures in this article.
- [Mark favorites in the Files app](#)
You can mark up to 50 files and folders as favorites. Once you mark an item as a Favorite, you can see it in a filtered view by clicking **Favorites** in the left navigation panel. The item you marked also continues to display in your **Home folder** and **Shared with me** views as appropriate.
- [Create a new folder](#)
With proper permissions, you can create a new folder in your Files app and use it to store and organize other files and folders.
- [Delete files and folders](#)
Use caution when deleting files and folders; the content may be permanently deleted and unrecoverable.
- [Rename folders in your Files app](#)
Since your Files list is private to you, you can rename shared folders without affecting how those items display to other users who share access to that folder.

Determine who has shared access

To determine who has access to a shared folder, use the information in this article.

Using Aspera on Cloud, you can share folders with the following:

- Other users or groups in your [workspace](#).
- Depending on permissions set by your admin:
 - Your entire Aspera on Cloud workspace; simply enter the workspace name in the Recipients field. New members automatically gain access to folders you share with your entire workspace.
 - AoC users outside your workspace.
 - People who do not have an AoC account.

Users you share with can in turn share with others. In this way, sharing becomes "chained."

How Many People Have Access to a Folder?

To determine how many users have shared access to a given folder, right-click the folder row and select **Info** from the context menu; the **Info** modal displays the number of collaborators who have shared access to this folder.

Who Has Access to a Folder?

To determine which users have shared access to a given folder, click the folder row; click the **Collaborators** icon, then click **See all collaborators**.

Note:

- 1) Keep in mind that entities listed may be users, groups, or an entire workspace, so a single listing may indicate more than a single user.
- 2) The user who initially uploaded this content into the Files app and shared it is not listed in this dialog.

Change permissions to a folder you shared

For each folder you share, you grant specific access permission to each recipient you share with. You can change the permission you granted or revoke it entirely. No one else can change the permissions for a folder you shared.

Important: Only administrators and workspace managers can manage collaborators (using a Node Access Key and Secret) in the Files app for admin-shared folders. If you uploaded the folder or saved it from your Packages app, you have full *Edit* permission. If someone shared this folder with you, you can grant the permissions you yourself have; you cannot grant permission that you don't have.

To change permission for a folder collaborator, do the following:

1. Click to open the intended folder; click the Collaborators icon , then click See all collaborators.
2. In the right-side panel, locate the intended collaborator; do the following:
 - a. Click the **Edit permissions** icon.
 - b. Click the **Permissions** field to select a pre-set permission group, or select **Custom**, then select the check box for each available custom permission to assign.
 - c. Click **Save**.

To change permission for someone using a public link, do the following.

1. Right-click the intended folder and select **Manage all links**.
 2. For the intended link, click Edit.
 3. Select the desired permissions, then click Save.
- Note: (1) When you reset the permission for this link, that new permission applies to every person who uses this link.
(2) You can grant only the permissions you yourself have to the folder.

Understand "Size" and "Last Updated" data

This article describes how to interpret data in the *Size* and *Last updated* columns in the Files application. Understanding these data gives insight into how and when AoC refreshes the values displayed.

Size column

For files, AoC displays the size reported by the storage. The file size displayed is accurate as of the time shown in the "Last updated" column.

For folders, AoC reports the calculated folder size and file count. To see when AoC last refreshed these values, right-click the folder and select Info. The value reported in the Size field does not reflect changes since the value in the Folder size and file count last checked field.

Last Updated column

Data in the *Last updated* column show the most recent time that the file or folder changed.

- **For files**, this is the time that the file was either:
 - First uploaded.
 - Most recently replaced with a new version.
- **For folders**, this is the time that the folder, including its files and sub-folders, was either:
 - First uploaded.
 - Most recently added, deleted, or updated.

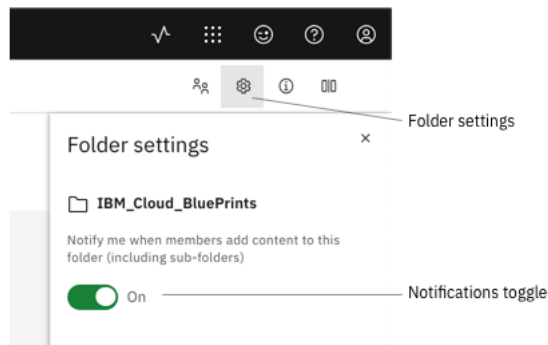
The data in this column come from the storage for the specific file or folder. The storage type determines how these data are reported to AoC.

- Local storage reports *Last updated* time for both files and folders.
- Cloud storage reports *Last updated* time for files only, not for folders.
 - AoC displays these data for files in cloud storage in the *Last updated* column.
 - AoC cannot display data for folders in cloud storage since the data do not exist. In this case, AoC displays "-" in the *Last updated* column.

Set notifications for new content in a shared folder

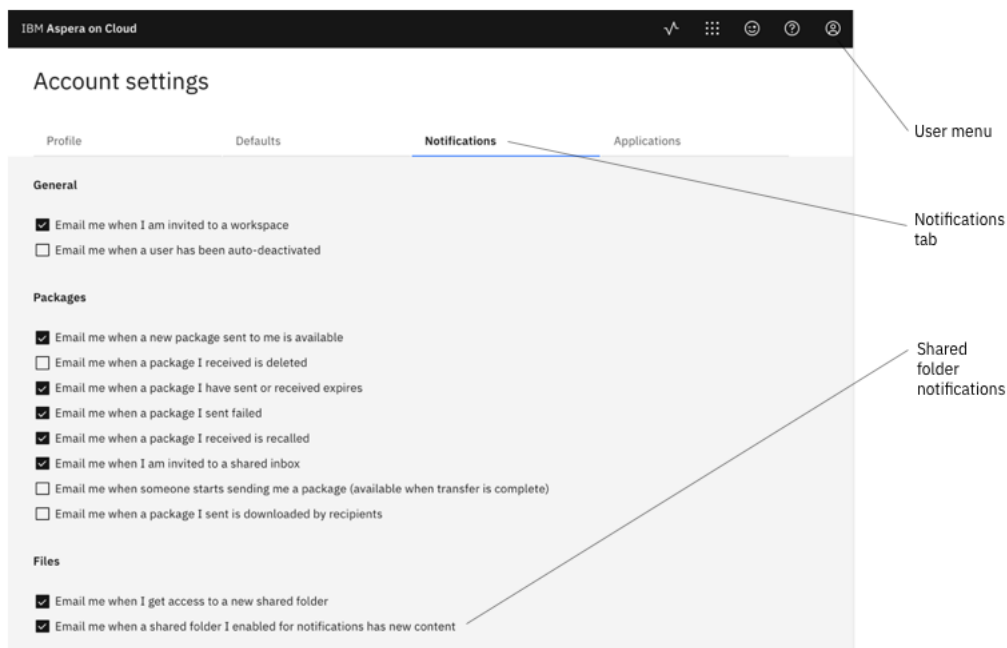
You can configure Aspera on Cloud to deliver email notifications to you when new content appears in a shared folder you need to monitor.

The administrator must enable this notification option (Admin > Organization > Notifications > Allow users to turn on notifications for new shared folder content. For a procedure, see [Control email notification delivery](#)). Unless the admin enables this notification, users do not see the notification toggle and cannot configure these notifications.



To enable notifications that new content has been uploaded to a shared folder in your workspace, do the following:

1. Verify that this notification is enabled for your account:
 - a. Click the User menu icon .
 - b. Select Account settings > Notifications.
 - c. Scroll to Notification settings > Files.
 - d. Click to enable Email me when a shared folder I enabled for notifications has new content.



- e. Click Save to save the change.
2. Go to the shared folder and click to select and open it.
3. In the upper right, click Folder settings .
4. Click the toggle to turn On notifications for this folder and its sub-folders.

When anyone uploads content to this folder, including its sub-folders, AoC delivers an email notification to you.

Move or copy content in your Files app

There are two ways to move and copy files and folders in your Files app:

- Right-click the item, select **Move** or **Copy**, and then, in the window that opens, select the new location for the item.
- Drag-and-drop the item to the new location. Use the move/copy panel if necessary.

These operations do not change the file structure in another user's home folder, even for shared content.

Keep these behaviors in mind as you move or copy items in your Files app:

- You cannot move an entire folder that has been shared with you; instead, open the folder and move or copy the specific items in it.
- You must have proper permissions in both the source and destination folders to complete a move or copy action.

Move and copy large files and folders

Move and copy actions on very large files or folders may require several minutes to complete. When you initiate a move or copy operation, the source item is disabled to prevent other actions on the item until the move or copy operation completes.

Depending on file size, there may be an interim period when AoC displays the item in both the source and destination locations. Once a move operation completes, the item disappears from the source location.

Right-click to move or copy

To move or copy an item in your Files app, do the following:

1. Right-click the item row and select **Move** or **Copy** as required. A window opens to display the contents of your Files app.
2. Go to the new location for the item.
3. To create a new folder, do the following:
 - a. Go to the new location for the item. If necessary, navigate into a folder to find the final destination location.
 - b. Click **Create folder**.
 - c. Name the folder, then click **Create**.
4. Click **Move** or **Copy**.

Drag and drop to move or copy

Move by default; Override to copy

When the source and destination locations are on the same storage, the drag-and-drop action, by default, initiates a move operation: Aspera on Cloud copies the content to the destination folder and deletes the copy in the source folder.

If you need to copy the content rather than move it, simply hold down the **Alt** key as you drag.

Copy by default; Override to move

In the following cases, the drag-and-drop action, by default, creates a copy operation:

- When the source and destination locations are on different storage locations.
- When dragging multiple content items in one operation, with source content items on different storage locations.

If you need to move the content rather than copy it, simply hold down the **Alt** key as you drag.

Procedure

To move or copy content from one location to another, do the following:

1. Go to the content to move.
2. Do one of the following:
 - If the destination folder is on the same level of your content directory as the source folder, drag and drop the content item to the destination folder. If required, hold down the **Alt** key or **Option** key to override the default action.
 - If the destination folder is on a different level of your content directory than the source folder, go to step 3.
3. Click the **Move/copy panel** icon  in the upper banner.
The left view is the source; the move/copy panel on the right is the destination.
4. In the move/copy panel, navigate to the desired destination.
5. From the left view, drag the content to the destination. If required, press and hold the **Alt** key while you drag to override the default action.
When you are done, close the panel.

Move or copy content between workspaces

You can move or copy files between different workspaces. By default, you will perform these actions in your current workspace. To move or copy files to another workspace, you have to select one from the Select workspace menu.

Manage your shared links

You can send shared links to give others access to folder contents. Each link gives the recipient specific access permissions. Use private links to share with current folder collaborators. Use public links to share with anyone. To view and manage your shared links, including resending, editing, and deleting links, use the procedures in this article.

To manage your existing links for a given folder, do the following:

1. Right-click the folder and select **Get shared link**; the Share link window displays.
2. In the Share link window, click **Manage links**.
3. For *private* links that you can share with current folder collaborators, you can do the following:
 - a. To send this link to one or more folder collaborators, click the **Send** icon.
 - b. To copy the link to your clipboard, click the **Copy** icon.
 - c. To delete this link, click the **Trash** icon. The link becomes invalid immediately. Anyone who has this link can no longer use it to access the folder.
4. For *public* links that you can share with anyone, you can do the following:
 - a. To change the expiration or permission for this link, or to apply a password to this link, or to reset an existing password, click the **Edit** icon. Such changes become effective immediately, and anyone who uses this link will be affected.
 - b. To send this link to more recipients, click the **Send** icon.
 - c. To copy the link to your clipboard, click the **Copy** icon.
 - d. To delete this link, click the **Trash** icon. The link becomes invalid immediately. Anyone who has this link can no longer use it to access the folder.

Mark favorites in the Files app

You can mark up to 50 files and folders as favorites. Once you mark an item as a Favorite, you can see it in a filtered view by clicking **Favorites** in the left navigation panel. The item you marked also continues to display in your **Home folder** and **Shared with me** views as appropriate.

To mark or unmark an item as a favorite, do the following:

1. In your **Home folder** and **Shared with me** views, right-click the row of the item to mark; select **Favorite** from the list.
2. To view your favorites, click **Favorites** in the left navigation panel.
3. To remove an item from your list of favorites, right-click the item in the Favorites view and select **Remove favorite**.

If you try to add an item to your Favorites list, but see a message that you've reached your limit, remove some items from your Favorites list to make room for new favorites.

Create a new folder

With proper permissions, you can create a new folder in your Files app and use it to store and organize other files and folders.

If you do not see the **Create folder** button, located at the top of your Files listing, your administrator has disabled your ability to create folders in this top level of your Files app. However, you may have this permission inside a folder someone shared with you. Click a folder row to open it and observe whether the **Create folder** button displays.

To create a new folder, do the following:

1. Go to the location in your Files app where you want to create the new folder.
2. Click **Create folder**.
3. Name the new folder.
4. Click **Create**.

Delete files and folders

Use caution when deleting files and folders; the content may be permanently deleted and unrecoverable.

If you delete a file within a folder that has been shared with you, you delete that file from the source and others lose access as well.

If you delete an entire folder that has been shared with you, the folder is removed from your view but not from the views of others who may share the same content.

1. To delete a single item, right-click and select **Delete**.
2. To delete multiple items, select the check boxes for the items to delete, then click **Delete** at the top of the list.

Rename folders in your Files app

Since your Files list is private to you, you can rename shared folders without affecting how those items display to other users who share access to that folder.

Note the following:

- When another user shares a folder with you, it appears on the top level of your Files app, according to the sort order you set in your Files list (for example, by name; by size). The shared folder displays the name it bears in the sharer's home folder.
- Once in your Files app, you can rename the folder as desired (assuming they gave you Edit or Rename permission). Your renaming does not affect the name of the folder in the original sharer's Files app.
- Even if the person who originally shared the item with you renames it in their home folder, the name of the item in your home folder is not affected.
- Note that these points apply only to the shared top-level folder; if you rename a folder that is nested within that shared folder, you rename it for all users who have access to it.
- To rename a very large folder (one with more than about 20 items), select the Rename and move option from the right-click menu. This feature improves performance for such large file operations. The renamed folder appears in the same location in the Files app. Note that when this operation completes, you must recreate all existing shared links to contents in the renamed folder.

These points imply the following example:

- Mary shares the folder "New Media" with Ravi.
 - Ravi sees "New Media" in his home folder.
 - Both Mary and Ravi have the item "New Media" in their home folders.
- Ravi renames the item to "Brochure Media".
 - Mary's item remains named "New Media".
- Mary renames her item: she changes "New Media" to "Client Media".
 - Ravi's item remains named "Brochure Media".

Therefore, a folder containing the same content may reside in the home folders of multiple users, and may display a different name in each.

Share with outside users

Learn how to use a *public link* to share folders with colleagues outside your workspace.

- [What is a public link?](#)

When you want to share a folder with someone not in the Files app in your workspace, without requiring your recipient to log in to Aspera on Cloud, send a *public link*. A public link enables unauthenticated sharing.

- [Share with external users](#)

Aspera on Cloud provides various methods to share folders with users outside your workspace. Choose a method based on your goals, your relationship with your recipients, and the required content security.

- [Share with unauthenticated recipients using public links](#)

You can use *public links* to share folders in your Files app without requiring your recipient to log in. Be aware that the public link you send is not restricted to the person you send it to. For additional security, you can set and require a password to use the public link.

What is a public link?

When you want to share a folder with someone not in the Files app in your workspace, without requiring your recipient to log in to Aspera on Cloud, send a *public link*. A public link enables unauthenticated sharing.

When you share using a public link, AoC sends your recipient an email containing a link. When your recipient clicks the link, an AoC portal opens, allowing your recipient to access the folder you shared. AoC does not require your recipient to log in. Your recipient can act on folder contents based on the permission you set for them.

When you create a public link, you can configure the following:

- The duration that the link is active. Once the link expires, your recipient can no longer access the folder you shared.
- The recipient's permission level to the folder. You can grant any permission that you yourself have to the folder you share; you cannot grant a permission that you do not have.
- Optionally, a password that your recipient must apply to access the folder using the link.

Note: Folder collaborators with **Edit** permission can manage all links to the folder, including those created by other users. For details, see [Sharing permissions](#).

You can generate an email to the outside user; the email includes the link, the expiration, and a message if you want. You can also simply copy the link and deliver it to the recipient by another means.

Note:

1) When your recipient clicks the link, Aspera on Cloud prompts them to install IBM Aspera Connect. For more information, refer to [Installing Aspera Connect](#).

2) This link is truly public, in that the user you give the link to can in turn give the link to another person, who can then access the content you shared. Use the public shared link with trusted colleagues.

For a procedure describing how to use the public shared link, refer to [Share with external users](#).

Share with external users

Aspera on Cloud provides various methods to share folders with users outside your workspace. Choose a method based on your goals, your relationship with your recipients, and the required content security.

Aspera on Cloud gives you various ways to share folders with users outside your workspace; this can include someone who is not a member of your AoC organization at all. Note that your administrator determines whether you can share outside your workspace and with whom:

- Share a folder; recipient must log in.
- Share a folder with a password to access it; your recipient does not need to log in to Aspera on Cloud.
- Share a link with someone who is not a member of your workspace; recipient does not need to log in.

Share, with limited org membership and login requirement

When you share using this procedure, Aspera on Cloud sends an email notification to your recipient. When the recipient clicks the link in the email, AoC prompts them to download and install IBM Aspera Connect, the same software you installed to enable transfers between your desktop and an Aspera server (see Aspera Connect for Outside Users).

Once the Connect installation is complete, AoC presents the app login page. By logging in, your recipient creates an account and becomes a limited member of your AoC organization. This means that they can access *only* the content that is specifically shared with or sent to them. They do not become a member of a workspace.

1. Right-click a folder row and select **Share**.
2. Select or enter one or more recipients.
3. Assign [access permissions](#).
4. Click **Share**.

Share, without login requirement; password optional

Use this method to share with someone outside your workspace without inviting them to your workspace.

This sharing method allows (but does not require) you to apply a password to the link. When your recipient clicks the password-protected link, they must apply the same password to access the folder. Aspera on Cloud generates a password, or you can choose your own password for a given link. You must deliver the password to your recipient according to your own site security practices.

1. Right-click a folder row and select **Get shared link**.
2. Select **Public link**. Anyone can access this folder with this link.

Note: Be aware that the public link you send is not restricted to the person you send it to. The recipient of your public link can forward the link to someone else, who can then use the link to access the content you share. Share public links only with trusted colleagues when the security of the folder content is not vital.

3. If this is the first public link to this folder, click **New link**.
4. If a modal displays with an editable text field, you can customize the link. Enter a link name that will be useful and informative to you and to recipients; click **OK**. If you don't see this field, your admin has not configured this customization capability; go to the next step.
5. Set the expiration for this link to determine the duration that your recipient should have access to this folder. After that duration, the link becomes invalid.

6. Set the permission you want your recipient to have to the contents of this folder. For details, see "Content Permissions" below.
7. To require a password for this link, click the toggle labeled **Require password**.
Aspera on Cloud generates and displays a password.
 - a. To generate a new password, click the circular icon.
When you regenerate a password, all previous passwords become invalid. If past recipients are using this link with a previous password, give your past recipients the new password.
 - b. To create your own password, delete the generated password and enter your desired password into the field.
 - c. To copy the password, click the copy icon.
The password remains on your clipboard until you copy something else. Be sure to save the password in secure file before you copy anything else.

Important: Aspera on Cloud does not save the password. Once you click Save in the following step, you cannot recover the password. You can regenerate the password for a link, but when you do, the former password becomes obsolete: other users (if any) of the link will be locked out unless you give them the new password.
Note: If you use multiple password-protected links, consider keeping a secure file of links and their passwords. You cannot recover a lost password.
 - d. Click **Save**.
 - e. Deliver the password to your recipient according to your local site security practices.

8. Deliver this link to your collaborator using one of these methods:

- In the Send this link field, enter an email address or username. If desired, include an optional message; then click **Send**.
- Click the **Copy** icon in the link field, then deliver the link to your recipient according to your local site practice.

Important: When you click **Copy**, the link overwrites anything existing on your clipboard. If you previously copied the password, be sure you stored the password in a secure location before copying the link itself.

Results:

- AoC sends an email notification to each recipient.
- When your recipient clicks the link in the email, AoC prompts them to download and install IBM Aspera Connect, the same software you installed to enable high-speed transfers between your desktop and an Aspera server. It may be helpful to remind them that, after they install Connect, they may need to adjust their browser settings to allow Aspera Connect to run. Just like you, they must install the Connect app once on their computer, and they must add the browser extension once in each browser they'll use to access Aspera on Cloud. For details, see [Installing Aspera Connect](#).
- Once the Connect installation completes, AoC presents a portal that allows them to access the folder.
- Link recipients can act on the folder according to the permissions you set, until the expiration you set for the link.

Share with unauthenticated recipients using public links

You can use *public links* to share folders in your Files app without requiring your recipient to log in. Be aware that the public link you send is not restricted to the person you send it to. For additional security, you can set and require a password to use the public link.

Note: The Aspera on Cloud administrator can disable this feature.

You can use a [public link](#) to share with:

- AoC users in your workspace.
- AoC users who are not members of your workspace.
- Colleagues who do not have an AoC account.

Note: Be aware that the public link you send is not restricted to the person you send it to. The recipient of your public link can forward the link to someone else, who can then use the link to access the content you shared. Share these links only with trusted colleagues when the security of the folder content is not vital.

Aspera on Cloud prompts the recipient of your link to download and install IBM Aspera Connect. It may be helpful to remind them that, after they install Connect, they may need to adjust their browser settings to allow Aspera Connect to run.

Share a public link

To share with an outside user, do the following:

1. Right-click a folder row and select **Get shared link**.
2. Select **Public link**. Anyone can access this folder with this link.
Note: Be aware that the public link you send is not restricted to the person you send it to. The recipient of your public link can forward the link to someone else, who can then use the link to access the content you share. Share public links only with trusted colleagues when the security of the folder content is not vital.
3. If this is the first public link to this folder, click **Create one**.
4. If a modal displays with a an editable text field, you can customize the link you are about to create. Enter a link name that will be useful and informative to you and to potential recipients; click **OK**. If you don't see this field, your admin has not configured this customization capability; go to the next step.
5. Set the expiration for this link to determine the duration that your recipient should have access to this folder. After that duration, the link becomes invalid.
6. Set the permission you want your recipient to have to the contents of this folder. For details, see "Content Permissions" below.
7. To require a password for this link, select the check box labeled Require password.
Aspera on Cloud generates and displays a password.
 - a. To generate a new password, click the circular icon.
When you regenerate a password, all previous passwords become invalid. If past recipients are using this link with a previous password, give your past recipients the new password.
 - b. To create your own password, delete the generated password and enter your desired password into the field.
 - c. To copy the password, click the copy icon.
The password remains on your clipboard until you copy something else. Be sure to save the password in secure file before you copy anything else.
Important: Aspera on Cloud does not save the password. Once you click **Save** in the following step, you cannot recover the password. You can regenerate the password for a link, but when you do, the former password becomes obsolete: other users (if any) of the link will be locked out unless you give them the new password.
Note: If you use multiple password-protected links, consider keeping a secure file of links and their passwords. You cannot recover a lost password.
 - d. Click **Save**.
 - e. Deliver the password to your recipient according to your local site security practices.
8. Deliver the public link to your collaborator using one of these methods:
 - Click the **Copy** icon in the link field, then deliver the link to your recipient according to your local site practice.

Important: When you click Copy, the link overwrites anything existing on your clipboard. If you previously copied the password, be sure you stored the password in a secure location before copying the link itself.

- Enter an email address or username, and an optional message; then click **Send**.

AoC sends an email notification to each recipient. When they click the link in the email, AoC presents a portal that displays the folder.

Results:

- When your recipient tries to use the link, AoC prompts them to download and install IBM Aspera Connect, the same software you installed to enable high-speed transfers between your desktop and an Aspera server. It may be helpful to remind them that, after they install Connect, they may need to adjust their browser settings to allow Aspera Connect to run. Just like you, they must install the Connect app once on their computer, and they must add the browser extension once in each browser they'll use to access Aspera on Cloud. For details, see [Aspera Connect transfer client](#).
- Link recipients can act on the folder according to the permissions you set, until the expiration you set for the link.

Send an existing link

To share a folder using an existing link, do the following:

1. Right-click the row of the folder to share, then select Get shared link.
2. Select Public link.
3. Select the intended link, then click the **Send** icon.
4. Either click the **Copy** icon in the link field and send the link to your recipient, or enter the recipient name, along with a message if desired, and click **Send**.

Note: Changes you make to existing links affect all the users you previously shared that link with.

Managing Existing Links

You can change or delete links you've made. If you are a folder collaborator with Edit permission to the folder, you can manage all links to the folder – both links that you've created and links that other users have created.

To change an existing link, do the following:

1. Right-click the folder and select Get shared link; the Share link window displays.
2. In the Share link window, click Manage links.
3. For *private* links that you can share with current folder collaborators, you can do the following:
 - a. Click the Send icon to send this link to one or more folder collaborators.
 - b. Click the Copy icon to copy the link to your clipboard.
 - c. Click the Trash icon to delete this link. The link becomes invalid immediately. Anyone who has this link can no longer use it to access the folder.
4. For public links that you can share with anyone, you can do the following:
 - a. Click the Edit icon to change the expiration or permission set on this link, or to apply a password to this link, or to reset an existing password. Such changes become effective immediately, and anyone who already has this link will be affected.
 - b. Click the Send icon to send this link to more recipients.
 - c. Click the Copy icon to copy the link to your clipboard.
 - d. Click the Trash icon to delete this link. The link becomes invalid immediately. Anyone who has this link can no longer use it to access the folder.

To delete a link, do the following:

1. Right-click the row of the folder to share, then select Get shared link.
2. Click Manage links.
3. Find the intended link in the list of public links and click the delete icon to the right.

Sharing problems

The section provides troubleshooting procedures for deleting or renaming large folders and for addressing problems with access to shared folders.

- [Delete large files and folders](#)
Use this topic to troubleshoot issues that arise when you delete large files and folders in your Aspera on Cloud Files app workspace.
- [Rename large folders](#)
This article describes how to troubleshoot an attempt to rename a large folder in your Files app that didn't seem to succeed.
- [Can't access a shared folder](#)
Use this procedure when you can see a shared folder in your Files app but cannot access it.
- [User still has access to unshared folder](#)
If you've unshared a folder to remove access from a specific user, but that user can still access the folder, use this article.

Delete large files and folders

Use this topic to troubleshoot issues that arise when you delete large files and folders in your Aspera on Cloud Files app workspace.

In the vast majority of cases, deleting a file or folder is an operation performed by your cloud storage. Deleting very large items may require some time to complete; the larger the file or folder, the longer the operation takes. For the largest files and folders, it may take several hours or even an entire day or more. AoC treats deletion as a background operation so you can continue working in Files while the operation completes. See "Managing files in the Aspera on Cloud user guide for related information.

After you initiate the delete operation, AoC recommends that you not perform other actions on the item.

Refresh the browser to verify that the operation is complete and the file or folder no longer displays.

If after some time you refresh your browser and still see the item you want to delete, to the following:

1. Perform the delete operation again.

2. If the item is a folder, try deleting sub-folders or files within the folder first; then perform the delete operation on the folder again.
3. If the issue persists, contact your local tech support administrator: click  in the banner and select "Technical Support".

Rename large folders

This article describes how to troubleshoot an attempt to rename a large folder in your Files app that didn't seem to succeed.

Note: To rename a very large folder (one with more than about 20 items), select the Rename and move option from the right-click menu. This feature improves performance for such large file operations. The renamed folder appears in the same location in the Files app. Note that when this operation completes, you must recreate all existing shared links to contents in the renamed folder.

In the vast majority of cases, renaming a file or folder is an operation performed by your cloud storage. The various cloud platforms use different schemes to rename.

For example, to rename a folder "OldFolder" to "NewFolder":

- Some cloud platforms change a prefix in the file path. For example, the original file path may be OldFolder/MyFile. After renaming, that same file will use the path NewFolder/MyFile.
- Some cloud platforms first create NewFolder. Then they move or copy the contents of OldFolder to New Folder. When all the contents of OldFolder are present in NewFolder, the cloud storage deletes OldFolder.

In any case, the larger the item, the longer the rename requires. For the largest files and folders, it may take several hours or even several days. AoC treats renaming as a background operation so you can continue working in Files while the operation completes.

During the renaming operation, AoC disables the folder to prevent further actions on OldFolder until renaming completes. Note that the folder is not disabled to other users who may have shared access to it. Aspera recommends that no one perform any operations on the folder and its contents until the renaming operation completes.

Once complete, AoC deletes OldFolder and displays NewFolder.

Note: You must refresh your Files listing to see NewFolder.

Identify the issue

If an anomaly occurs in the network or in cloud storage, the renaming may not complete. You know that renaming did not complete if you see either of these situations:

- After seven days, OldFolder still displays after you refresh the page.
- At any time, both OldFolder and NewFolder display. (Remember that, depending on folder names and the sort order you set for your Files listing, the two folders may be on different pages in the Files app.) In this case, folder content may be split between OldFolder and NewFolder. There may some content that exists in both folders.

Cloud storage will not lose any of your content in either case.

Troubleshoot

If after seven days Old Folder still displays after you refresh the page, perform the rename operation again.

If both OldFolder and New Folder display, do the following:

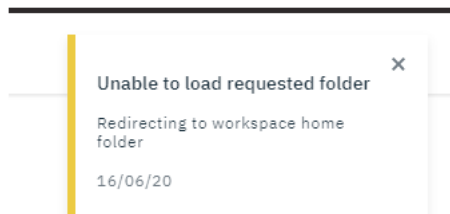
1. Determine which of the two folders contains the majority of the content. Consider item sizes as well as item count.
2. Move the content manually to the folder with the most content.
Note: For the items you move manually, you must restore the intended access permissions manually.
3. If in step 2 you moved content to OldFolder, try the rename operation again.

Can't access a shared folder

Use this procedure when you can see a shared folder in your Files app but cannot access it.

If instead your shared folder issue is that you have 'unshared' a folder with a user but the user still has access, see [User still has access to unshared folder](#).

On rare occasions, you may see the error message "Unable to load requested folder" when you try to access a folder that has been shared with you:



When you try to access a folder but the folder is not available, AoC redirects you to the Files app home folder in that workspace. Your home folder is the top level of your Files application in that workspace. If you are a member of the Files app in multiple workspaces, you have a home folder in each workspace.

If you are the person who can't access a folder that you can see, do the following:

1. In your own Files app, check your permissions on the folder (right-click folder row, select Info); do you have the expected access permission?
2. Check with the folder owner that the shared folder still exists. The person who shared is listed in subtext on the row of the shared folder.

☐		Export		0 B
☐		ey Shared by an admin to this workspace		10 MB 1 file
☐		Files for Check Out Shared by _____ to you		750 MB 1,176 files, 363 folders

'Shared by'

3. Ask the folder owner to verify that you are in the list of folder collaborators and that you have the proper access permissions.
The folder owner can click the folder row in their own Files app to display the folder details and collaborators panel. If your name is not there, ask the folder owner to share with you again, being sure to select the desired permissions for you.
4. Contact your local tech support administrator. Click in the banner and select "Technical support". Provide the URL of the affected folder.

User still has access to unshared folder

If you've unshared a folder to remove access from a specific user, but that user can still access the folder, use this article.

You can share folders with individual users, with groups, and with entire workspaces. Any given user may have access to a shared folder directly, or may have access through a group or workspace that has shared access.

If you unshared a folder with an individual but that user still has access, you may have to remove the user from a group that has access. For details, see [Direct and inherited memberships](#). Contact your admin to change group membership.

To unshare a folder, see [Unshare a folder](#).

Aspera Connect transfer client

Learn how to install the IBM Aspera Connect transfer client, how to help outside users install Connect, and how to troubleshoot installation problems.

- [What is IBM Aspera Connect?](#)
Aspera on Cloud requires one of two transfer methods to power high-speed transfers between user desktops and Aspera transfer servers. Users can either download and install Aspera Connect, a free, lightweight, install-on-demand software program; or you can configure the IBM Aspera HTTP Gateway and attach it to your Aspera on Cloud organization.
- [Aspera Connect for Outside Users](#)
Aspera Connect is a free, lightweight, install-on-demand software program that powers high-speed transfers between desktops and Aspera servers.
- [Monitor transfers](#)
You can review your attempted and completed transfers and monitor your active, in-progress transfers using the transfer monitor. This in-app monitor reflects the transfer activity that you perform using the Aspera on Cloud app, including transfers that use the IBM Aspera Connect transfer client; the IBM Aspera HTTP Gateway; and direct node-to-node FASP transfers. To view transfer activity and usage for the entire organization, use the Aspera on Cloud Activity app.
- [Installation](#)
This section gives step-by-step instructions for installing the IBM Aspera Connect transfer client. Also included are instructions for installing the Connect browser extension in each supported browser.
- [Installation troubleshooting](#)
Find troubleshooting procedures addressing Aspera Connect installation-specific issues.
- [Other Connect troubleshooting](#)
Address the most common issues with Aspera Connect using the articles in this section, including the Connect prompt reappearing, disabling Connect when Aspera HTTP Gateway is enabled, and more.

What is IBM Aspera Connect?

Aspera on Cloud requires one of two transfer methods to power high-speed transfers between user desktops and Aspera transfer servers. Users can either download and install Aspera Connect, a free, lightweight, install-on-demand software program; or you can configure the IBM Aspera HTTP Gateway and attach it to your Aspera on Cloud organization.

Aspera Connect is the default transfer method for Aspera on Cloud and other Aspera web app. However, if your deployment of Aspera on Cloud does not permit the download and installation of client software, the admin can [configure](#) an alternative transfer method: the [IBM Aspera HTTP Gateway](#). Otherwise, all users must install the Aspera Connect transfer client and the Connect browser extension to complete high-speed transfers.

Once installed, Connect runs automatically when you transfer content using one of the Aspera web apps. In Aspera on Cloud, Connect typically runs in the background rather than on screen as in many of the other Aspera web applications.

Important: Connect comprises an app and a browser extension; you must install both as follows:

- You must install the Connect app once on your computer.
See [Installing Aspera Connect](#).
- You must install the Connect extension for each browser (except Internet Explorer) you'll use to access Aspera on Cloud.
See the appropriate article:
 - [Adding the Chrome browser extension for Connect.](#)
 - [Adding the Firefox Connect Browser Extension.](#)
 - [Adding the Safari browser extension for Connect.](#)
 - [Adding the Microsoft Edge browser extension for Connect.](#)

If required, you can configure Connect to change default settings for download location, transfer bandwidth, and various network and security settings. Configure Connect settings with the guidance of your Aspera administrator. Note that the Connect Transfers window displays all your recent transfers, whether through Aspera on Cloud or another Aspera product.

After each successful login, Aspera on Cloud checks to see whether the most recent version of Connect is running on your machine. If a Connect upgrade is available, Aspera on Cloud prompts you through the upgrade process.

If you have any issues with Aspera Connect performance, run the [IBM Aspera Connect Diagnostic Tool](#). See also [Installation troubleshooting](#) and [IBM Aspera Connect common issues](#). For more details, see the [IBM Aspera Connect product documentation](#).

Aspera Connect for Outside Users

Aspera Connect is a free, lightweight, install-on-demand software program that powers high-speed transfers between desktops and Aspera servers.

Aspera on Cloud provides several ways for you to collaborate with outside users; an *outside user* is an Aspera on Cloud user outside your workspace, or a user without a Aspera on Cloud account. Depending on the permissions configured, you can:

- Send files and folders to an outside user.
- Share folders with an outside user.
- Invite an outside user to send files and folders to you or to an Aspera on Cloud shared inbox.

When the outside user attempts to access content you've sent or shared, or to send content to you, Aspera on Cloud prompts them to download and install Aspera Connect—the same software your computer uses to transfer content between your local machine and another location. Aspera on Cloud supports Connect on both Windows and Mac OS, and in the most common browsers for each platform.

The download and installation are quick and simple, and Aspera on Cloud guides users through the process. See the procedures in [Installation](#).

Important: You may need to remind your colleague that they must install the Connect app once on their computer, but they must install the Connect extension for each browser (except Safari and Internet Explorer) they'll use to access Aspera on Cloud.

If they still have problems, direct them to [Overview: Aspera Connect installation troubleshooting](#) and the related browser-specific topics. If problems persist, contact your Technical Support provider.

Installation

This section gives step-by-step instructions for installing the IBM Aspera Connect transfer client. Also included are instructions for installing the Connect browser extension in each supported browser.

- [Installing Aspera Connect](#)
IBM Aspera Connect is the free, lightweight app that powers Aspera high-speed transfers. Aspera Connect is one of the two transfer methods that enable high-speed transfers to and from user desktops. Once installed, Connect runs automatically in the background. Installing Connect is fast and easy, with a built-in installation wizard that provides step-by-step guidance.
- [Adding the Chrome browser extension for Connect](#)
This topic explains how to obtain and add the required IBM Aspera Connect extension to your Chrome browser. The extension is required in each browser you use to interact with Aspera on Cloud.
- [Adding the Firefox browser extension for Connect](#)
This topic explains how to obtain and add the required IBM Aspera Connect extension to your Firefox browser. The extension is required in each browser you use to interact with Aspera on Cloud.
- [Adding the Safari browser extension for Connect](#)
This topic explains how to obtain and add the required IBM Aspera Connect extension to your Safari browser. The extension is required in each browser you use to interact with Aspera on Cloud.
- [Adding the Microsoft Edge browser extension for Connect](#)
This topic explains how to obtain and add the required IBM Aspera Connect extension to your Edge browser. The extension is required in each browser you use to interact with Aspera on Cloud.
- [Adding the Firefox Connect Browser Extension](#)
This topic explains how to obtain and add the required IBM Aspera Connect extension to your Firefox browser. The extension is required in each browser you use to interact with Aspera on Cloud.

Installing Aspera Connect

IBM Aspera Connect is the free, lightweight app that powers Aspera high-speed transfers. Aspera Connect is one of the two transfer methods that enable high-speed transfers to and from user desktops. Once installed, Connect runs automatically in the background. Installing Connect is fast and easy, with a built-in installation wizard that provides step-by-step guidance.

Note: If you are unable to download software to your computer, see [Select a transfer method](#) and talk to your administrator.

Shortly after you log into Aspera on Cloud for the first time, you'll see an on-screen message prompting you to download and install Aspera Connect. A similar message displays when AoC detects that your local machine is not running the current version of Connect.

IBM Aspera recommends that you always use the latest version of Connect.

The procedure for installing IBM Aspera Connect requires enabling a browser extension for Connect in addition to installing the Connect application itself.

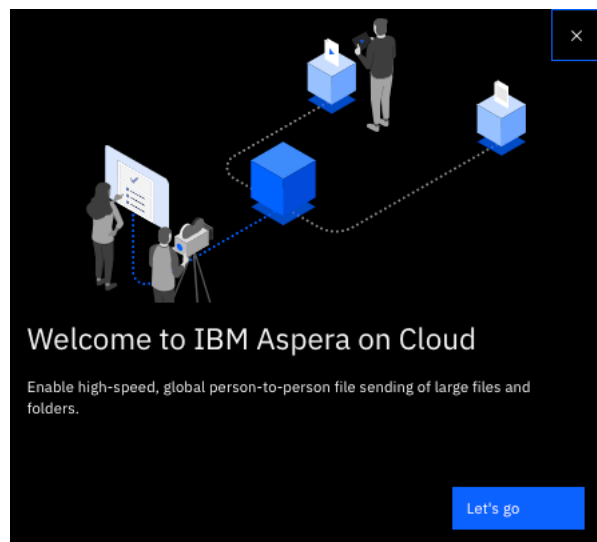
Important

- You must install the Connect app once on your computer. You must install the Connect extension for each browser (except Safari and Internet Explorer) you'll use to access Aspera on Cloud.

- Before performing a system-wide installation (all users of the machine), uninstall any per user installations. For details on uninstalling, see the [Connect user documentation](#).
- Remove all previous Connect installers before downloading the new installer.
- Connect works better when your browser's local storage is enabled; however, this is not a requirement.

Guided installation

When you log in to Aspera on Cloud for the first time, click Let's go on the Welcome screen.



Depending on your browser/platform combination, the screens shown in these instructions may vary.

1. In the Get started now screen, click Install extension and confirm to add the extension. Your browser's page for the Connect extension opens. See the instructions for your browser in [Installation](#). If successful, you'll see the message confirming the extension has been added.
2. The Get started now screen next prompts you to install Connect; click Install Connect:

Get started now — install the IBM Aspera Connect transfer client.

Install the [IBM Aspera Connect](#) client and the Aspera Connect browser plug-in to enable our signature high-speed file transfer technology.

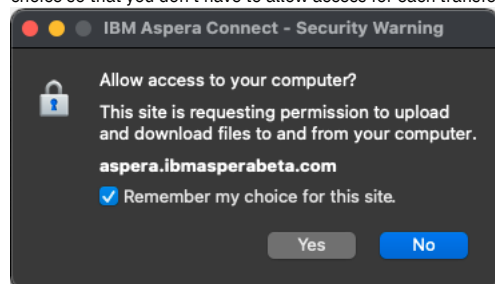
☒ Install extension Pre-requisite to install Connect	Install extension
☐ Install Connect client Essential desktop app to make the transfer fast	Install Connect

If you skip installing, you will be able to use IBM Aspera HTTP Gateway for transfers; for faster transfers come back and install Connect.

[I'll skip for now](#)

3. Once the Connect installation completes, refresh your browser.

Note: When you upload from or download to your computer, Connect requests access to your computer. IBM Aspera recommends you click the box to remember your choice so that you don't have to allow access for each transfer. Click Yes.



For more details, see the [Connect user documentation](#).

Adding the Firefox Connect Browser Extension

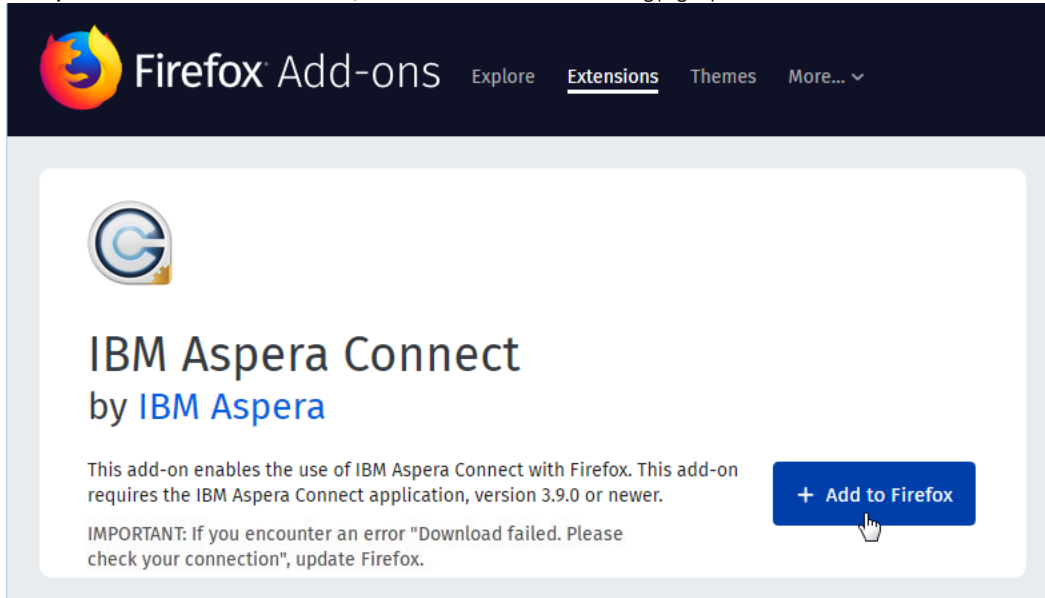
This topic explains how to obtain and add the required IBM Aspera Connect extension to your Firefox browser. The extension is required in each browser you use to interact with Aspera on Cloud.

The Connect extensions are specific to the browser; the procedure for adding an extension to a browser is the same regardless of which OS platform that browser is running on. With a guided install, clicking **Install Extension** opens the extension link for the browser you are using. With a manual install, be sure to download the extension for the browser you intend to use with Connect.

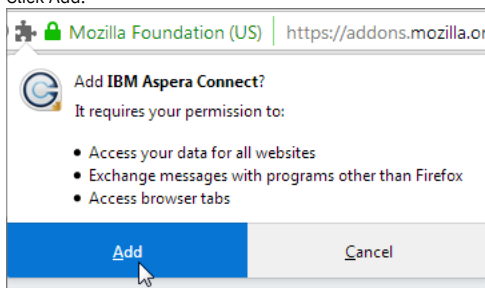
Important: You must install the Connect app once on your computer. You must install the Connect extension for each browser (except Safari and Internet Explorer) you use to access Aspera on Cloud.

To obtain and install the Connect extension for Firefox, follow the procedure below:

1. When you see the Connect Welcome screen, click Install Extension. The following page opens:



2. Click +Add to Firefox. The Add "IBM Aspera Connect"? dialog appears.
3. Click Add.



If successful, you'll see the message "IBM Aspera Connect has been added to Firefox."

Adding the Chrome browser extension for Connect

This topic explains how to obtain and add the required IBM Aspera Connect extension to your Chrome browser. The extension is required in each browser you use to interact with Aspera on Cloud.

The Connect extensions are specific to the browser; the procedure for adding an extension to a browser is the same regardless of which OS platform that browser is running on. With a guided install, clicking **Install Extension** opens the extension link for the browser you are using. With a manual install, be sure to download the extension for the browser you intend to use with Connect.

Important: You must install the Connect app once on your computer. You must install the Connect extension for each browser (except Internet Explorer) you use to access Aspera on Cloud.

To obtain and install the Connect extension for Chrome, follow the procedure below:

1. When you see the Get started now screen, click Install Extension.

Get started now — install the IBM Aspera Connect transfer client.

Install the [IBM Aspera Connect](#) client and the Aspera Connect browser plug-in to enable our signature high-speed file transfer technology.

☒ Install extension
Pre-requisite to install Connect

Install extension

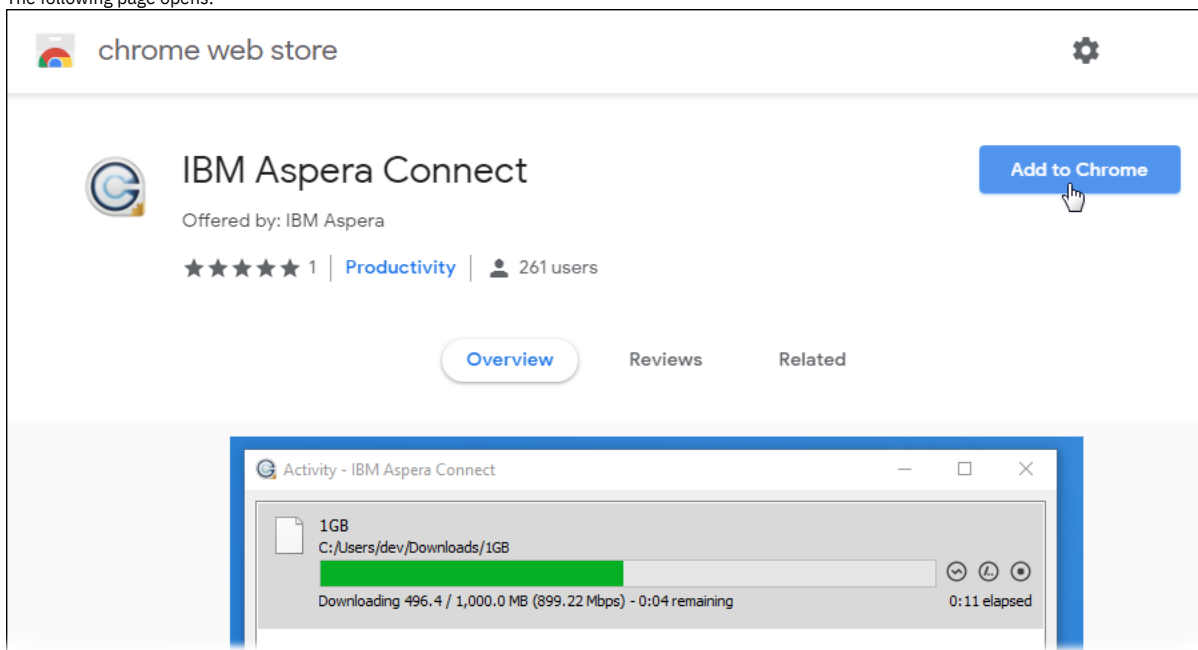
☐ Install Connect client
Essential desktop app to make the transfer fast

Install Connect

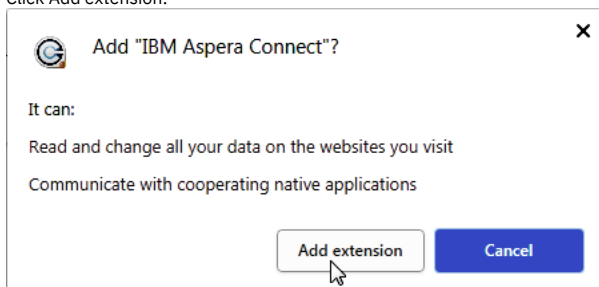
If you skip installing, you will be able to use IBM Aspera HTTP Gateway for transfers; for faster transfers come back and install Connect.

[I'll skip for now](#)

The following page opens:

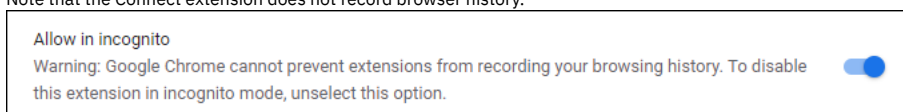


- Click Add to Chrome. The Add "IBM Aspera Connect"? dialog appears.
- Click Add extension.



If successful, you'll see the message "IBM Aspera Connect has been added to Chrome."

Note: By default, the Connect extension is disabled in Chrome's incognito mode. To enable the Connect extension, right-click the small Connect icon in the upper-right corner of your browser page. Then open Manage extensions and scroll down to the heading **Allow in incognito**. Then set the switch to ON as shown below. Note that the Connect extension does not record browser history.



Adding the Safari browser extension for Connect

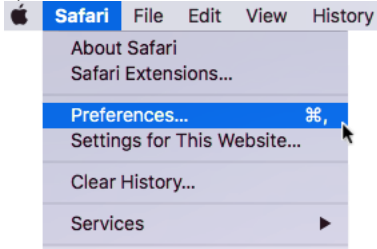
This topic explains how to obtain and add the required IBM Aspera Connect extension to your Safari browser. The extension is required in each browser you use to interact with Aspera on Cloud.

The Connect extensions are specific to the browser; the procedure for adding an extension to a browser is the same regardless of which OS platform that browser is running on. With a guided install, clicking **Install Extension** opens the extension link for the browser you are using. With a manual install, be sure to download the extension for the browser you intend to use with Connect.

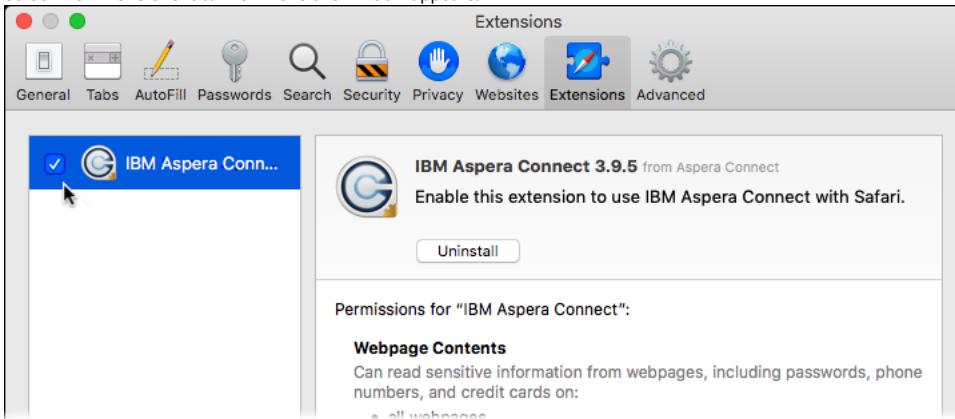
Important: You must install the Connect app once on your computer. You must install the Connect extension for each browser (except Safari and Internet Explorer) you use to access Aspera on Cloud.

The Connect browser extension for Safari is provided with the macOS installer for Connect. For this reason, the extension cannot be added to Safari until after the installer has been run. Once Connect is installed, add the Connect extension to Safari as follows:

1. Open **Safari > Preferences** (not Safari Extensions):



2. Select the **Extensions** tab. The Extensions window appears.



3. Look for the IBM Aspera Connect extension listed in the left panel, and click the check box to select it.
4. Close the dialog. The Connect extension has been added to your browser.

Adding the Microsoft Edge browser extension for Connect

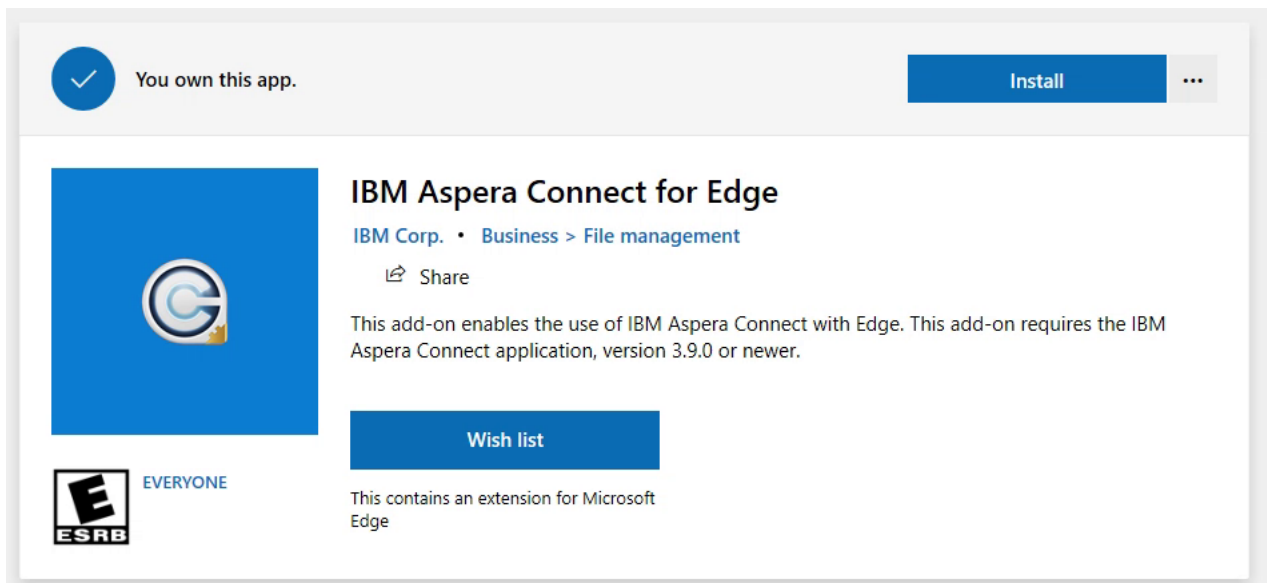
This topic explains how to obtain and add the required IBM Aspera Connect extension to your Edge browser. The extension is required in each browser you use to interact with Aspera on Cloud.

The Connect extensions are specific to the browser; the procedure for adding an extension to a browser is the same regardless of which OS platform that browser is running on. With a guided install, clicking **Install Extension** opens the extension link for the browser you are using. With a manual install, be sure to download the extension for the browser you intend to use with Connect.

Important: You must install the Connect app once on your computer. You must install the Connect extension for each browser (except Internet Explorer) you use to access Aspera on Cloud.

To obtain and install the Connect extension for Edge, follow the procedure below:

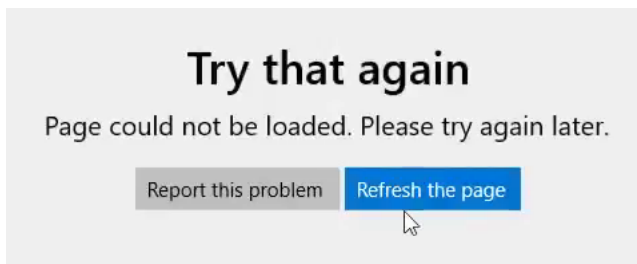
1. Click **Install Extension**. The following page opens:



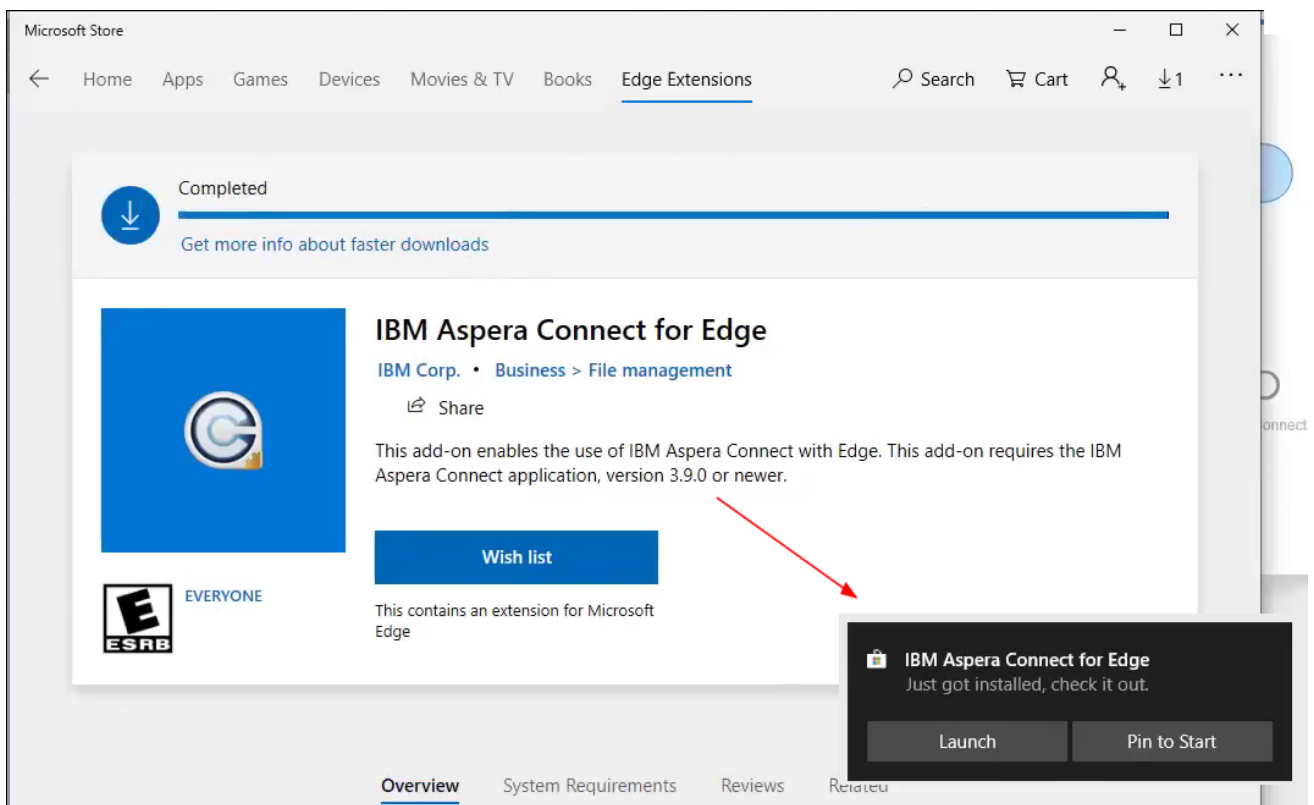
If you are prompted to sign in, you can dismiss the dialog; you are not required to sign in.

2. Click Install.

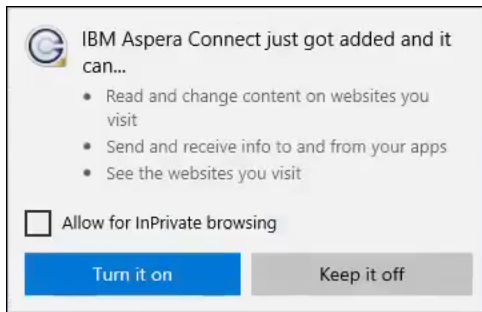
If the message below appears, click **Refresh the page**.



A dialog appears indicating the extension is installed.



3. Click Launch. This returns you to the browser, and the following dialog appears:



4. Click Turn it on.

Note: If the Connect extension for Edge is disabled, and you try to use a web app, the launch bar asks you to install the extension. Clicking Install Extension opens the Microsoft app store and shows a Launch button—however, the Launch button will *not* enable the extension. Enable the extension in the settings for Edge.

Installation troubleshooting

Find troubleshooting procedures addressing Aspera Connect installation-specific issues.

- [Overview: Aspera Connect installation troubleshooting](#)
Use this topic to start troubleshooting issues with installing or running IBM Aspera Connect.
- [Windows OS: Error when installing with a non-admin account](#)
Use this procedure to troubleshoot an Aspera Connect installation on a Windows machine when you have a non-admin account.
- [Windows OS: Connectivity issues](#)
Use this procedure to troubleshoot an Aspera Connect installation on a Windows machine when you have connectivity issues.
- [MacOS X: Connectivity issues](#)
Use this procedure to troubleshoot an IBM Aspera Connect installation on MacOS.
- [Linux: AppArmor prevents access to Connect](#)
AppArmor is a Linux security module that uses mandatory access control (MAC) to restrict some applications' system access. It may prevent Connect from running correctly on some Linux systems.
- [Linux: Connectivity issues](#)
Use this topic to troubleshoot connectivity issues for Connect on Linux.
- [Connect prompt continues to appear](#)
Once you download and install IBM Aspera Connect, the Connect installation prompt should no longer appear. However, there are two circumstances in which you may continue to see the installation dialog even though you've already installed Connect.

Overview: Aspera Connect installation troubleshooting

Use this topic to start troubleshooting issues with installing or running IBM Aspera Connect.

For your reference, the Connect installation process performs the following tasks:

- Installs the Connect browser extension.
- Downloads the Connect app.
- Installs the Connect app.

Before troubleshooting, make sure your Connect installation meets the requirements specified in the IBM Aspera Connect [user documentation and release notes](#), particularly with regard to the supported versions of operating systems, browsers, and (if Linux) OpenSSL.

In all cases, the first troubleshooting step is to run Aspera's web-based [Connect diagnostic tool](#) to get a preliminary assessment of your Connect installation. This diagnostic tool does the following:

- Reports the version number of your current Connect installation, if installed.
- Indicates whether your installed version is up to date.
- Checks whether Connect is running.
- Verifies whether your current version of Connect is compatible with your current browser.
- Tests your ports.
- Attempts to perform a test transfer.
- Generates a summary report that you can download and send to IBM Aspera support, if necessary.

Use the other topics in this section to further troubleshoot your Connect installation, according to the OS of your local machine. See also [IBM Aspera Connect common issues](#).

Connect prompt continues to appear

Once you download and install IBM Aspera Connect, the Connect installation prompt should no longer appear. However, there are two circumstances in which you may continue to see the installation dialog even though you've already installed Connect.

- There is a new version of Connect available, and the app prompts you to install the upgrade.

In this case, you must download and install the Connect app upgrade. You may or may not need to update your browser extension; the installation process will guide you.

- You have not installed the Connect extension in your current browser.
You may have installed the extension in a different browser, but the extension is required for each browser. In this case, there is no need to reinstall the Connect app, but you must install the browser extension. Find the appropriate installation procedure for your browser among these articles.

If you are not allowed to download and install software, the Aspera on Cloud administrator has configured the IBM Aspera HTTP Gateway for transfers. In this case, you can [disable Aspera Connect](#). Otherwise, you must download and [install the Aspera Connect transfer client](#), and install the Connect browser extension.

Windows OS: Error when installing with a non-admin account

Use this procedure to troubleshoot an Aspera Connect installation on a Windows machine when you have a non-admin account.

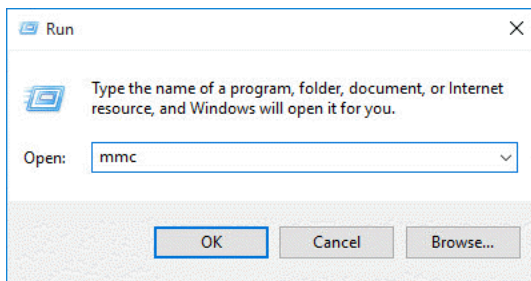
You may encounter an error such as the following (or with similar wording) if you are not an Administrator when executing the MSI installer file.

The system administrator has set policies to prevent this installation.

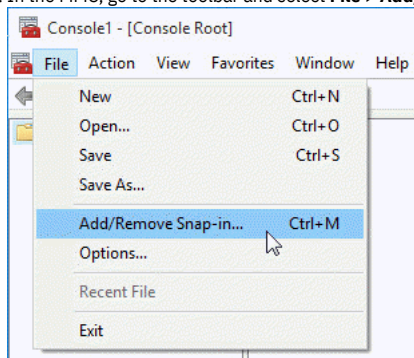
These error messages are due to not having permissions to install an MSI package as a non-admin account. Other than logging in as an administrator to install Connect, you may also ask that your Administrator grant the group policy access for non-admin users to install applications.

The following example shows you how to grant group policy access for non-admins to install software on Windows 2016:

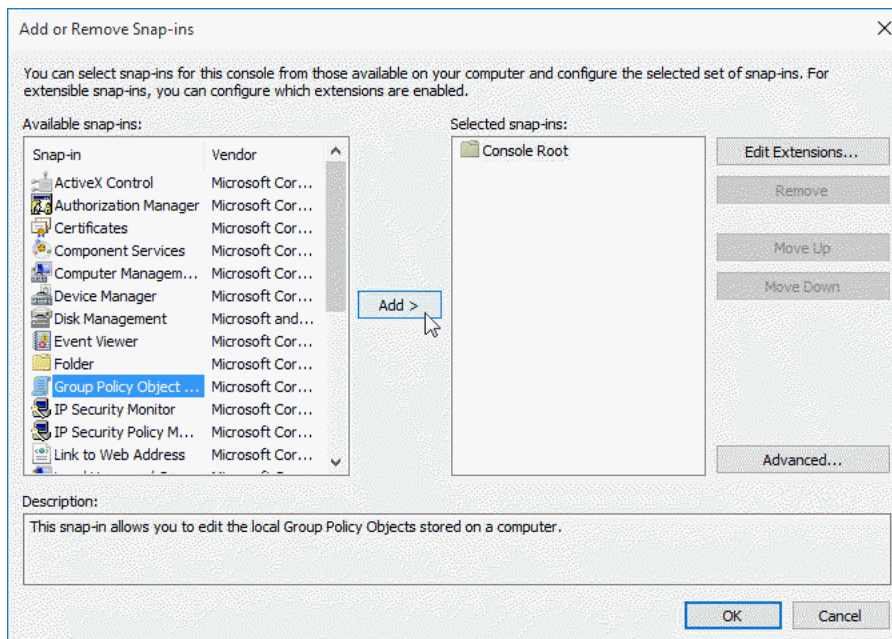
1. Launch the Microsoft Management Console (MMC).
Go to **Start menu > Run**. Enter `mmc` and click **OK** to launch it.



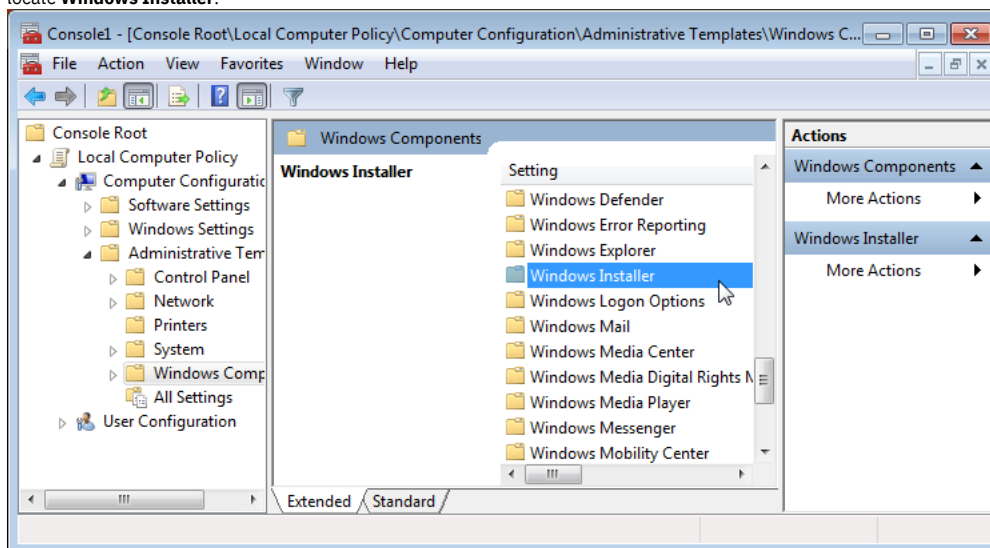
2. Add the Group Policy Object Editor Snap-in.
 - a. In the MMC, go to the toolbar and select **File > Add/Remove Snap-in**:



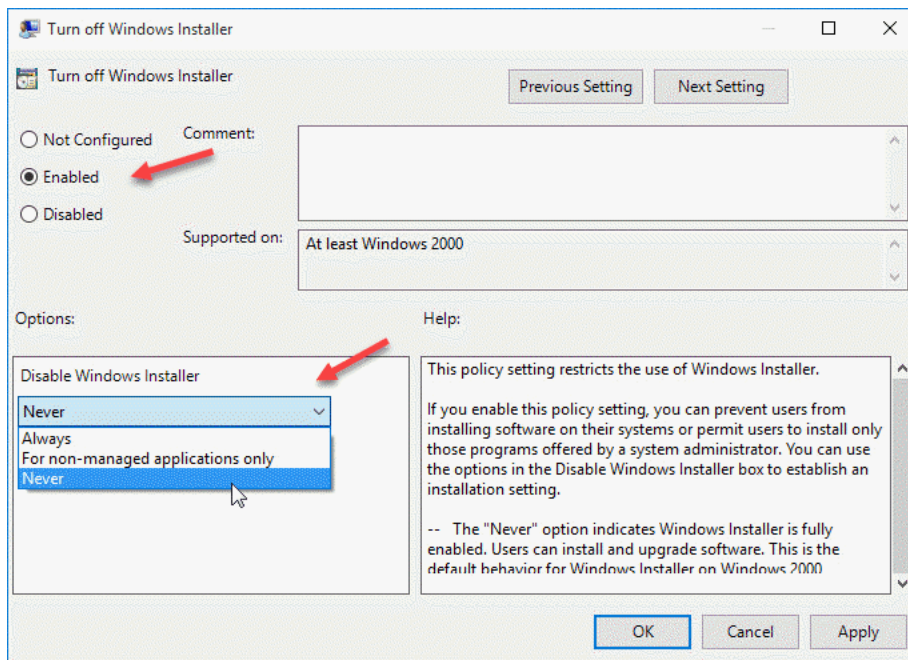
- b. In the **Add or Remove Snap-ins** window, select the **Group Policy Object Editor** and click **Add**:



- c. In the Select Group Policy Object window (wizard), under Group Policy Object, click **Browse** and select either **This Computer** or specify another computer. When done, click **OK** to return to the wizard window.
 - d. In the wizard window, click **Finish**. When you are returned to the **Add/Remove Snap-ins** window, click **OK** to save the changes.
3. Grant the Windows installation group policy.
- a. In the MMC, navigate into **Console Root > Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components** and locate **Windows Installer**:



- b. Double-click **Windows Installer**.
- c. In the list that appears, locate **Turn off Windows Installer** and double-click it. The Turn Off Windows Installer window opens.
- d. Under the Turn off Windows Installer heading, select **Enabled**. In the Disable Windows Installer box, open the pull-down and select **Never**. When finished, click **OK**:



- e. To close the MMC, click **File > Exit**.
- f. When prompted to save console settings, click **Yes** to save the settings to a file. When prompted for a .msc filename, click **Save**.
- g. Reboot the computer to apply the changes, or execute the following command at a command prompt:

```
> gpupdate /force
```

Windows OS: Connectivity issues

Use this procedure to troubleshoot an Aspera Connect installation on a Windows machine when you have connectivity issues.

SSH connectivity errors: "Timeout establishing connection"

If you receive the error "Timeout establishing connection," the TCP connection between Connect and the server is blocked (error codes 13, 15, or 40 in the log files). To determine the cause, open a Terminal or a Command prompt on the client machine (where Connect is installed). Use **telnet** to test the connection to the server:

```
> telnet server-ip-address 33001
```

where *server-ip-address* is the IP address of the Aspera server (for example, 10.0.1.1) on TCP port 33001 (or the configured TCP port, if other than 33001).

You will receive one of the following errors and can take the appropriate action:

- **"Connection refused"**: The Aspera server is not running the SSHD service. Have your server administrator review the server's SSH service status.
- **"Timeout"**: The client-side firewall is disallowing outbound TCP traffic. Ensure that the client-side firewall allows outbound TCP traffic on port 33001 (or the configured TCP port).

UDP connectivity errors: "Data transfer timeout"

If Connect appears to successfully connect to the server but:

- The transfer progress reads 0%.
- Files appear to be transferred to the destination but are 0 bytes.
- You eventually receive the error "Data transfer timeout."

UDP connectivity is blocked, likely by the firewall configuration (error codes 14, 15, and 18 in the log files). Ensure that the client-side firewall allows outbound traffic on the FASP UDP port (33001, by default) and the server firewall allows inbound traffic on UDP port 33001.

IBM Aspera Connect diagnostic tool

Aspera provides a web-based diagnostic tool that can be useful for identifying connection issues. You can access the tool here:

<https://test-connect.asperasoft.com/>

MacOS X: Connectivity issues

Use this procedure to troubleshoot an IBM Aspera Connect installation on MacOS.

SSH connectivity errors: "Timeout establishing connection"

If you receive the error "Timeout establishing connection," the TCP connection between Connect and the server is blocked (error codes 13, 15, or 40 in the log files). To determine the cause, open a Terminal or a Command prompt on the client machine (where Connect is installed). Use **telnet** to test the connection to the server:

```
$ telnet server-ip-address 33001
```

where *server-ip-address* is the IP address of the Aspera server (for example, 10.0.1.1) on TCP port 33001 (or the configured TCP port, if other than 33001).

You will receive one of the following errors and can take the appropriate action:

- **"Connection refused":** The Aspera server is not running the SSHD service. Have your server administrator review the server's SSH service status.
- **"Timeout":** The client-side firewall is disallowing outbound TCP traffic. Ensure that the client-side firewall allows outbound TCP traffic on port 33001 (or the configured TCP port).

UDP connectivity errors: "Data transfer timeout"

If Connect appears to connect successfully to the server but:

- The transfer progress reads 0%.
- Files appear to be transferred to the destination but are 0 bytes.
- You eventually receive the error "Data transfer timeout."

UDP connectivity is blocked, likely by the firewall configuration (error codes 14, 15, and 18 in the log files). Ensure that the client-side firewall allows outbound traffic on the FASP UDP port (33001, by default) and the server firewall allows inbound traffic on UDP port 33001.

IBM Aspera Connect diagnostic tool

Aspera provides a web-based diagnostic tool that can be useful for identifying connection issues. You can access the tool here:

<https://test-connect.asperasoft.com/>

Linux: AppArmor prevents access to Connect

AppArmor is a Linux security module that uses mandatory access control (MAC) to restrict some applications' system access. It may prevent Connect from running correctly on some Linux systems.

To disable AppArmor, enter the following commands on the affected computer:

```
# /etc/init.d/apparmor stop
# update-rc.d -f apparmor remove
```

Linux: Connectivity issues

Use this topic to troubleshoot connectivity issues for Connect on Linux.

SSH connectivity errors: "Timeout establishing connection"

If you receive the error "Timeout establishing connection," the TCP connection between Connect and the server is blocked (error codes 13, 15, or 40 in the log files). To determine the cause, open a Terminal or a Command prompt on the client machine (where Connect is installed). Use **telnet** to test the connection to the server:

```
# telnet server-ip-address 33001
```

where *server-ip-address* is the IP address of the Aspera server (for example, 10.0.1.1) on TCP port 33001 (or the configured TCP port, if other than 33001).

You will receive one of the following errors and can take the appropriate action:

- **"Connection refused":** The Aspera server is not running the SSHD service. Have your server administrator review the server's SSH service status.
- **"Timeout":** The client-side firewall is disallowing outbound TCP traffic. Ensure that the client-side firewall allows outbound TCP traffic on port 33001 (or the configured TCP port).

UDP connectivity errors: "Data transfer timeout"

If Connect appears to successfully connect to the server but:

- The transfer progress reads 0%.
- Files appear to be transferred to the destination but are 0 bytes.
- You eventually receive the error "Data transfer timeout."

UDP connectivity is blocked, likely by the firewall configuration (error codes 14, 15, and 18 in the log files). Ensure that the client-side firewall allows outbound traffic on the FASP UDP port (33001, by default) and the server firewall allows inbound traffic on UDP port 33001.

IBM Aspera Connect diagnostic tool

Aspera provides a web-based diagnostic tool that can be useful for identifying connection issues. You can access the tool here:

<https://test-connect.asperasoft.com/>

Aspera for desktop transfer client

IBM Aspera for desktop provides secure, fast, and reliable file transfer solutions for IBM Aspera servers.

- [What is IBM Aspera for desktop?](#)

Aspera for desktop is a transfer client that powers high-speed file transfers between your computer and Aspera transfer servers. When used with a website that is

integrated with Aspera, Aspera for desktop allows you to start uploads and downloads directly from the browser.

What is IBM Aspera for desktop?

Aspera for desktop is a transfer client that powers high-speed file transfers between your computer and Aspera transfer servers. When used with a website that is integrated with Aspera, Aspera for desktop allows you to start uploads and downloads directly from the browser.

Aspera for desktop integration

Once you download and install Aspera for desktop, you are ready to get started. Open a web browser of your choice and navigate to your company's website that integrates with Aspera. The desktop app seamlessly integrates with websites, and allows you to perform high-speed file transfer directly through your browser. Follow the instructions provided on the website to start transferring files.

Features and benefits of using Aspera for desktop

Since web browsers have limited file transfer functionality and often result in slow transfers, integrating with Aspera for desktop allows websites to offer users faster file transfers regardless of file size or physical distance. While Aspera also offer install-free solutions, the Aspera desktop app provides the best end-to-end high speed file transfer experience. Additionally, the desktop app provides these features:

- **High-speed file transfer**
Transfer large files or directories at maximum speed regardless of network conditions or physical distance.
- **Transfer management**
View your transfer history as well as your current transfer progress (you can pause and resume transfers). When used with Shares, the desktop app lets users transfer shared files faster and more reliably.
- **Remotely view and manage content**
Sign in to your IBM Aspera on Cloud (AoC), IBM Aspera Faspex 5, or IBM Aspera High-Speed Transfer Server (HSTS) accounts directly from the desktop app to browse and manage your account content.

Important: Going forward, if you are an AoC trial user, IBM Aspera for desktop will be the only option to use as your primary transfer client. For more information, visit the official [IBM Aspera for desktop](#) transfer client documentation.

Troubleshooting

Understand failure notifications. Find troubleshooting procedures to address transfer issues like slow transfer speeds, when to retry a transfer, and node-to-node transfer issues. Also troubleshoot issues regarding email notifications, shared folder access, and more. Also find information on specific error messages.

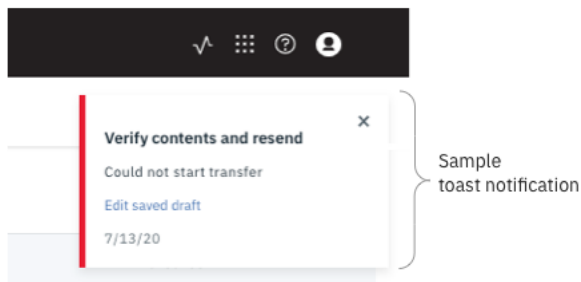
- [Failure notification types and locations](#)
This topic describes the various notifications that AoC provides when a transfer fails.
- [Transfer issues](#)
Get troubleshooting procedures to investigate, characterize, and address slow transfer speeds, transfer failures, node-to-node transfer issues, and more.
- [Other Issues](#)
Address issues regarding email notifications, shared folder access, problems managing very large folders, and more.

Failure notification types and locations

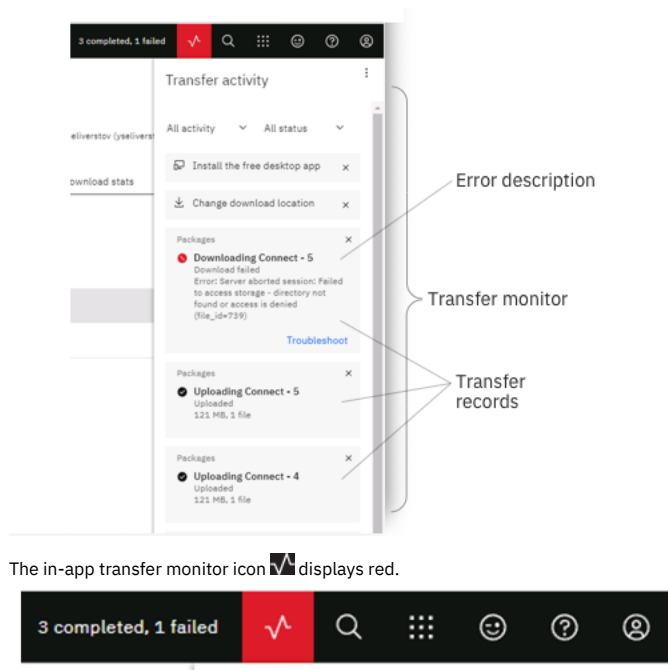
This topic describes the various notifications that AoC provides when a transfer fails.

When a transfer fails, AoC may present feedback in three ways:

- A transient ("toast") message that appears for several seconds in the upper right corner of the AoC app.



- An error description (that may include a recommended action) in a transfer record in the in-app transfer monitor. Display the transfer monitor by clicking this icon in the top banner of the app: 



- The in-app transfer monitor icon  displays red.

To contact your local tech support administrator, click  in the banner and select "Technical support".

Transfer issues

Get troubleshooting procedures to investigate, characterize, and address slow transfer speeds, transfer failures, node-to-node transfer issues, and more.

- [Select a transfer method](#)
Aspera on Cloud requires one of two transfer methods to power high-speed transfers between user desktops and Aspera transfer servers. Users can either download and install Aspera Connect, a free, lightweight, install-on-demand software program; or an admin can configure the IBM Aspera HTTP Gateway and attach it to your Aspera on Cloud organization.
- [Retry the transfer](#)
You may be able to address a failed transfer by fixing a simple issue and then retrying the transfer.
- [Resending "Draft" packages](#)
When the transfer for a package you send fails to start, AoC displays a transient error message with the heading "Verify contents and resend" and moves the package to the Drafts folder in your Packages app.
- [Node-to-node transfer issues](#)
A node-to-node transfer (also called a *share-to-share* transfer) moves files from one transfer node or cloud storage location to another, as opposed to a transfer between a user desktop and a transfer node.
- [Slow transfer speeds](#)
Many factors affect IBM Aspera on Cloud transfer speed. Some can be addressed by IBM Aspera on Cloud users and administrators. Some must be addressed by administrators of tethered IBM Aspera High-Speed Transfer Servers. Some may be due to cloud service or network conditions that may or may not be under your control.
- [Specific transfer failures](#)
This article describes troubleshooting options for some specific transfer failures.
- [More transfer troubleshooting resources](#)
The IBM Support Knowledge Base contains articles to help identify potential performance bottlenecks, firewall considerations, collect network traces, and find IBM Aspera logs.
- [IBM Aspera Connect common issues](#)
Aspera on Cloud requires one of two transfer methods to power high-speed transfers between user desktops and Aspera transfer servers. Users can either download and install Aspera Connect, a free, lightweight, install-on-demand software program; or an admin can configure the IBM Aspera HTTP Gateway and attach it to your Aspera on Cloud organization.
- [Connect prompt continues to appear](#)
Once you download and install IBM Aspera Connect, the Connect installation prompt should no longer appear. However, there are two circumstances in which you may continue to see the installation dialog even though you've already installed Connect.

IBM Aspera Connect common issues

Aspera on Cloud requires one of two transfer methods to power high-speed transfers between user desktops and Aspera transfer servers. Users can either download and install Aspera Connect, a free, lightweight, install-on-demand software program; or an admin can configure the IBM Aspera HTTP Gateway and attach it to your Aspera on Cloud organization.

Aspera Connect is the default transfer method for Aspera on Cloud and other Aspera web app. However, if your deployment of Aspera on Cloud does not allow users to download and install client software, an admin can configure an alternative transfer method: the [IBM Aspera HTTP Gateway](#). The Aspera HTTP Gateway is a standalone product that uses both HTTP/S and Aspera FASP to complete file transfers.

For troubleshooting the installation of IBM Aspera Connect, see [Installation troubleshooting](#).

IBM Aspera Connect powers high-speed transfers between desktops and Aspera servers. Once installed, Connect runs automatically in the background for each upload and download you initiate using Aspera on Cloud.

When you first log in to Aspera on Cloud, the app prompts you to download and install Aspera Connect. The installation is an easy, two-step process in most browsers; Aspera on Cloud guides you through the process. The first guidance dialog looks something like this:

Get started now — install the IBM Aspera Connect transfer client.

Install the [IBM Aspera Connect](#) client and the Aspera Connect browser plug-in to enable our signature high-speed file transfer technology.

☒ Install extension
Pre-requisite to install Connect

Install extension

☐ Install Connect client
Essential desktop app to make the transfer fast

Install Connect

If you skip installing, you will be able to use IBM Aspera HTTP Gateway for transfers; for faster transfers come back and install Connect.

[I'll skip for now](#)

Install the Connect app once; Install the Connect extension for each browser

There are two components of IBM Aspera Connect; you must install both components as follows:

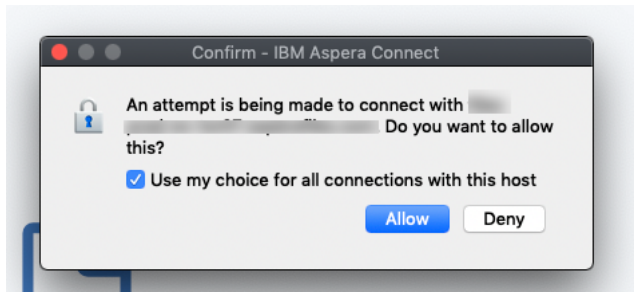
- The Connect application, which you *install once on any computer* you use to access Aspera on Cloud.
- The Connect browser extension, which you *install on each browser* you use to access Aspera on Cloud.

For detailed installation procedures, see [Installation](#).

Allow the connection for each transfer server

When you start a [transfer](#) that requires Connect, Connect displays a dialog requesting permission to connect with the relevant Aspera transfer server.

Connect displays this dialog for the transfer server relevant to each transfer you initiate. Depending on the location of your content, your recipients, and those who send to you, your transfers may involve multiple transfer servers. Connect requests your permission to connect with *each* server. *You must grant permission to allow the transfer to proceed.*



The exact wording of this dialog may vary depending on your browser. But in any case, IBM Aspera highly recommends that you check the option to allow *all connections* with the host, or *always allow*. Otherwise you must manually allow each transfer to initiate. If this dialog displays behind another application window, blocked from your immediate view, you may not realize that Connect is requesting your permission; without your permission the transfer cannot start.

Already installed Connect, but still being prompted?

There are two circumstances in which you may continue to see the installation dialog even though you've already installed Connect:

- There is a new version of Connect available, and the app prompts you to install the upgrade.
In this case, you must download and install the Connect app upgrade. You may or may not need to update your browser extension; the installation process will guide you.
- You have not installed the Connect extension in your current browser.
You may have installed the extension in a different browser, but the extension is required for each browser. In this case, there is no need to reinstall the Connect app, but you must install the browser extension.

To contact your local tech support administrator, click  in the banner and select "Technical support".

Connect prompt continues to appear

Once you download and install IBM Aspera Connect, the Connect installation prompt should no longer appear. However, there are two circumstances in which you may continue to see the installation dialog even though you've already installed Connect.

- There is a new version of Connect available, and the app prompts you to install the upgrade.
In this case, you must download and install the Connect app upgrade. You may or may not need to update your browser extension; the installation process will guide you.
- You have not installed the Connect extension in your current browser.
You may have installed the extension in a different browser, but the extension is required for each browser. In this case, there is no need to reinstall the Connect app, but you must install the browser extension. Find the appropriate installation procedure for your browser among these articles.

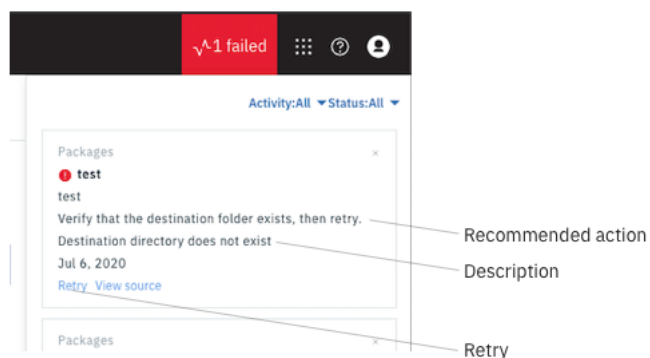
If you are not allowed to download and install software, the Aspera on Cloud administrator has configured the IBM Aspera HTTP Gateway for transfers. In this case, you can [disable Aspera Connect](#). Otherwise, you must download and [install the Aspera Connect transfer client](#), and install the Connect browser extension.

Retry the transfer

You may be able to address a failed transfer by fixing a simple issue and then retrying the transfer.

When you see the blue Retry link in the transfer record, address the issue described.

For example, consider the following transfer record. Verify that the directory you are trying to transfer to (the "destination" directory) exists; if it does not, create it at the expected path. Then click Retry in the transfer record to attempt the transfer again. This same strategy applies for some session and network anomalies. Perform the recommended action, then click Retry.



To contact your local tech support administrator, click  in the banner and select "Technical support".

If you are the local tech support administrator and need help after using this information, contact IBM support. Include the file available from Help > Download support data.

Resending "Draft" packages

When the transfer for a package you send fails to start, AoC displays a transient error message with the heading "Verify contents and resend" and moves the package to the Drafts folder in your Packages app.

If you see the error message "Verify contents and resend", do the following:

1. Click Edit saved draft in the error message to open the Drafts folder. You can also open the Drafts folder from the left panel of the Packages app.
2. In your Packages app Drafts folder, click the package row to view the package details. Any files and folders listed have been transferred successfully. Files and folders that you sent but are not listed did not transfer.
3. Add the missing content: click Upload to browse, or drag items to the sending panel.
4. Click Send.

The files that were transferred successfully in the first attempt will not be transferred again since they already exist at your intended destination; this means you do not incur more transfer and storage charges. Yet the final package contents are intact in your Sent folder after the transfer succeeds.

To contact your local tech support administrator, click  in the banner and select "Technical support".

Node-to-node transfer issues

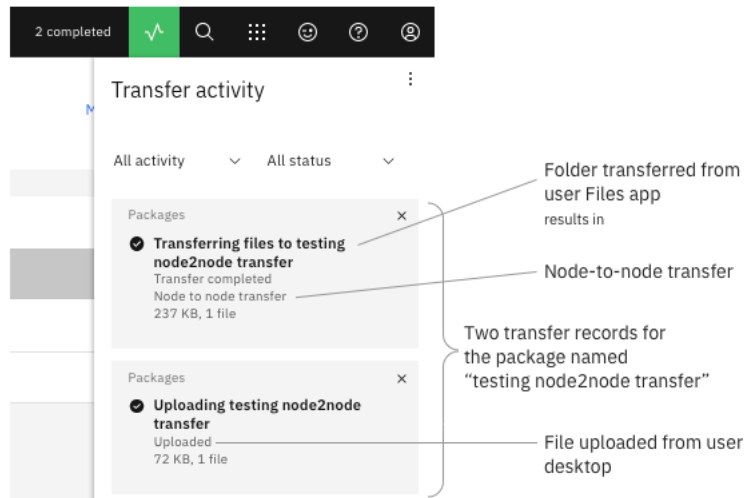
A node-to-node transfer (also called a *share-to-share* transfer) moves files from one transfer node or cloud storage location to another, as opposed to a transfer between a user desktop and a transfer node.

This is as opposed to uploading files from a user desktop or remote storage to a transfer node or cloud storage (or downloading files from the cloud to a user desktop or remote storage).

Folders in a user's Files app may be in any number of storage locations, including in different buckets or different cloud providers. When a user moves files from one folder in the Files app to another, a node-to-node transfer occurs.

Likewise, in the Packages app, sending a digital package that includes files or folders from the Files app ("Upload from Files" in the Send files panel) also results in a node-to-node transfer. And if a digital package includes files or folders already in cloud storage along with files and folders from the user desktop or remote storage, the AoC transfer monitor displays the package transfer on two separate transfer records: one transfer for the upload and a separate transfer for the node-to-node transfer.

For example, the screenshot below shows two transfer reports for a single transfer. The package contains one file ("byok_architecture copy.png") on the user's desktop and one folder ("AoC Self-Packed Onboarding") in the user's Files app.



There may be times when the error message "Unable to start node-to-node transfer" displays.

If you are the user attempting the transfer, try the transfer again because the issue may be ephemeral.

To contact your local tech support administrator, click  in the banner and select "Technical support".

If you are the local tech support administrator, do the following:

1. The security token may have expired. Check configurations in Organization > Security. See [Configuring Organization Security Settings](#).
2. If the transfer is to or from a [tethered node](#), check the transfer logs on the node; see [Where are the IBM Aspera client and server logs?](#)
3. Work with the user to collect web browser network traces; see [How to collect network traces for troubleshooting](#).

Slow transfer speeds

Many factors affect IBM Aspera on Cloud transfer speed. Some can be addressed by IBM Aspera on Cloud users and administrators. Some must be addressed by administrators of tethered IBM Aspera High-Speed Transfer Servers. Some may be due to cloud service or network conditions that may or may not be under your control.

Isolating potential causes

An important step in any troubleshooting process is isolating the cause of the issue. See [this article](#) on the IBM Support site to begin narrowing down the potential source.

Home network limitations

You may experience slow transfer speeds when using Aspera on Cloud at home. Most home internet connections are slower than expected; this is particularly true for upload speeds.

There are several free apps to verify your actual internet speed. Search the web for "internet speed test" to find one. Transfer speeds can never surpass the limits of the local internet connection.

Configuration of IBM Aspera Connect

IBM Aspera recommends that users consult with their administrators before adjusting default settings in Aspera Connect. Misconfiguration can lead to local network overload, degraded transfer speeds, and overloaded storage, among other issues.

If you are the administrator, refer to the [IBM Aspera Connect Admin and User Guides](#).

Connectivity issues test

Use this web-based [diagnostic tool](#) to help identify connection issues. This page also provides additional troubleshooting options and easy access to both the latest version of Aspera Connect should you not already have the latest version and to the Aspera Connect documentation set.

Transfer protocol in use

By default, Aspera on Cloud uses the IBM Aspera Connect app to transfer files and folders between user desktops and remote storage. Connect enables Aspera FASP, the IBM-proprietary high-speed transfer protocol.

An administrator can also configure an alternative transfer method using HTTPS/HTTP protocol for users who cannot install Aspera Connect. This method requires the standalone product called IBM Aspera HTTP Gateway. Once the Gateway is configured, the admin can enable an Aspera on Cloud organization to use it for transfers. See [Transfer with Aspera HTTP Gateway instead of Aspera Connect](#).

Typically, Aspera Connect is the faster transfer method; however, the Aspera HTTP Gateway is available for use cases that demand it. IBM recommends the use of Aspera Connect whenever possible.

When both Connect and HTTP Gateway are available, users can choose to disable Aspera Connect and the FASP protocol it supports. But typically, transfers using Aspera Connect are faster.

Users can regain access to Aspera Connect as follows:

1. Click the user icon and select Account settings. Set Disable Connect to Off, then click Submit to save the setting.
2. Launch the Connect installation:
 - a. Click  to open the transfer monitor.
 - b. At the bottom of the transfer monitor, click Install Connect.

Once users download and install Aspera Connect, transfer speeds typically increase.

For additional information, see [Installation](#). See also the troubleshooting procedures in [Installation troubleshooting](#) and the [IBM Aspera Connect Admin Guide](#).

For admins, see also the [IBM Aspera HTTP Gateway Admin Guide](#).

Additional troubleshooting resources

These IBM Support articles provide additional troubleshooting tips.

- [Identifying and understanding performance bottlenecks with Aspera Transfers](#)
- [How to identify the root cause of a slow transfer](#)
- [Testing performance to isolate issues](#)
- [Find logs for IBM Aspera Connect](#)
- [Find logs for IBM Aspera Desktop Client and IBM Aspera Server](#)

Specific transfer failures

This article describes troubleshooting options for some specific transfer failures.

To contact your local tech support administrator, click  in the banner and select "Technical support".

Aspera Connect is unavailable

- Recommended action: Download and install IBM Aspera Connect. See [Installing Aspera Connect](#).
- More information: See [Select a transfer method](#).

Session data transfer timeout

- Recommended action: Verify network connectivity, then retry the transfer.
- More information: This error typically indicates a UDP timeout. The most likely cause is a network interruption for more than 60 seconds.

Session shutdown failed

- Recommended action: Verify network connectivity, then retry the transfer.
- More information: The session did not shut down properly, and the channel data could not be sent. The most likely cause is a network timeout.

Destination path directory does not exist

- Recommended action: Verify that the destination folder exists, then retry the transfer.
- More information: The target folder cannot be found. Verify that the folder name is accurate and that the folder exists at the expected path. If it does not, create the destination folder at the expected path, then try the transfer again.

Network down

- Recommended action: Verify network connectivity, then retry the transfer.
- More information: The network layer of the operating system may return this error when the Aspera tries to send to a destination that can't be reached because of a disabled or disconnected network interface or router.

Server aborted session: Could not validate bearer token

- Recommended action: Create a new transfer and try again. A simple retry of the same transfer usually does not succeed.
- More information: The security token may have expired. The AoC admin should check configurations in Organization > Security. See [Configuring Organization Security Settings](#).

Server aborted session: Failed to extract JSON data from bearer token

- Recommended action: Log out of Aspera on Cloud, then log in again. Retry the transfer. If the issue persists, create a new transfer and try again after logging out and back in to AoC.
- More information: The security token may have expired. The AoC admin should check configurations in Organization > Security. See [Configuring Organization Security Settings](#).

More transfer troubleshooting resources

The IBM Support Knowledge Base contains articles to help identify potential performance bottlenecks, firewall considerations, collect network traces, and find IBM Aspera logs.

Find these valuable resources at:

- [Identifying and understanding performance bottlenecks with Aspera transfers](#)
- [Firewall considerations](#)
- [How to collect network traces in a web browser for troubleshooting](#)
- [Finding IBM Aspera logs](#)

To contact your local tech support administrator, click  in the Aspera on Cloud banner and select "Technical support".

Other Issues

Address issues regarding email notifications, shared folder access, problems managing very large folders, and more.

- [Email notifications](#)
Use this procedure when AoC email notifications do not arrive as expected.
- [Connect prompt continues to appear](#)
Once you download and install IBM Aspera Connect, the Connect installation prompt should no longer appear. However, there are two circumstances in which you may continue to see the installation dialog even though you've already installed Connect.
- [Can't access a shared folder](#)
Use this procedure when you can see a shared folder in your Files app but cannot access it.
- [Delete large files and folders](#)
Use this topic to troubleshoot issues that arise when you delete large files and folders in your Aspera on Cloud Files app workspace.
- [Rename large folders](#)
This article describes how to troubleshoot an attempt to rename a large folder in your Files app that didn't seem to succeed.
- [Specific error messages](#)
This article describes troubleshooting options for some specific error messages.

Email notifications

Use this procedure when AoC email notifications do not arrive as expected.

If you are the person who is missing the notification, do the following:

1. Check that the notification is not in your email spam folder.
2. Check that you haven't disabled the notification. See User icon > Account settings and .
3. Contact your local tech support administrator. Click the Help icon in the banner and select "Technical support". Provide the email address where you expect to receive the notification.

If you are the local tech support administrator, do the following:

1. Check that the AoC user record lists the user's expected email address. See Users > Management.
Note: If the user logs in to Aspera on Cloud through an external authentication or identity provider like IBMid or a SAML system, you cannot edit the name and email address in the AoC user record. The user must change these settings in the external system; that change will propagate to AoC.
2. Check that the user is in fact a member of the group, workspace, shared inbox, or other entity that should receive the missing notification.
3. Check that you have not disabled the specific notification that is missing; see Organization > Notifications and [Control email notification delivery](#).
4. Check that the SMTP server administrator has added the AoC email (donot-reply@ibmaspera.com) for notifications to the "allowed" list on the server.

Connect prompt continues to appear

Once you download and install IBM Aspera Connect, the Connect installation prompt should no longer appear. However, there are two circumstances in which you may continue to see the installation dialog even though you've already installed Connect.

- There is a new version of Connect available, and the app prompts you to install the upgrade.
In this case, you must download and install the Connect app upgrade. You may or may not need to update your browser extension; the installation process will guide you.
- You have not installed the Connect extension in your current browser.
You may have installed the extension in a different browser, but the extension is required for each browser. In this case, there is no need to reinstall the Connect app, but you must install the browser extension. Find the appropriate installation procedure for your browser among these articles.

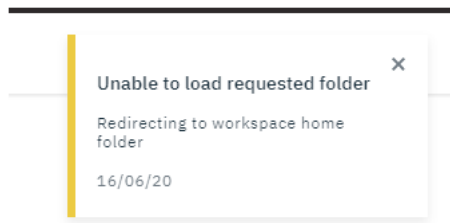
If you are not allowed to download and install software, the Aspera on Cloud administrator has configured the IBM Aspera HTTP Gateway for transfers. In this case, you can [disable Aspera Connect](#). Otherwise, you must download and [install the Aspera Connect transfer client](#), and install the Connect browser extension.

Can't access a shared folder

Use this procedure when you can see a shared folder in your Files app but cannot access it.

If instead your shared folder issue is that you have 'unshared' a folder with a user but the user still has access, see [User still has access to unshared folder](#).

On rare occasions, you may see the error message "Unable to load requested folder" when you try to access a folder that has been shared with you:



When you try to access a folder but the folder is not available, AoC redirects you to the Files app home folder in that workspace. Your home folder is the top level of your Files application in that workspace. If you are a member of the Files app in multiple workspaces, you have a home folder in each workspace.

If you are the person who can't access a folder that you can see, do the following:

1. In your own Files app, check your permissions on the folder (right-click folder row, select Info); do you have the expected access permission?
2. Check with the folder owner that the shared folder still exists. The person who shared is listed in subtext on the row of the shared folder.

☐		Export		0 B
☐		ey		10 MB
		Shared by an admin to this workspace		1 file
☐		Files for Check Out		750 MB
		Shared by [redacted] to you		1,176 files, 363 folders

3. Ask the folder owner to verify that you are in the list of folder collaborators and that you have the proper access permissions. The folder owner can click the folder row in their own Files app to display the folder details and collaborators panel. If your name is not there, ask the folder owner to share with you again, being sure to select the desired permissions for you.
4. Contact your local tech support administrator. Click in the banner and select "Technical support". Provide the URL of the affected folder.

Delete large files and folders

Use this topic to troubleshoot issues that arise when you delete large files and folders in your Aspera on Cloud Files app workspace.

In the vast majority of cases, deleting a file or folder is an operation performed by your cloud storage. Deleting very large items may require some time to complete; the larger the file or folder, the longer the operation takes. For the largest files and folders, it may take several hours or even an entire day or more. AoC treats deletion as a background operation so you can continue working in Files while the operation completes. See "Managing files in the Aspera on Cloud user guide for related information.

After you initiate the delete operation, AoC recommends that you not perform other actions on the item.

Refresh the browser to verify that the operation is complete and the file or folder no longer displays.

If after some time you refresh your browser and still see the item you want to delete, to the following:

1. Perform the delete operation again.
2. If the item is a folder, try deleting sub-folders or files within the folder first; then perform the delete operation on the folder again.
3. If the issue persists, contact your local tech support administrator: click in the banner and select "Technical Support".

Rename large folders

This article describes how to troubleshoot an attempt to rename a large folder in your Files app that didn't seem to succeed.

Note: To rename a very large folder (one with more than about 20 items), select the Rename and move option from the right-click menu. This feature improves performance for such large file operations. The renamed folder appears in the same location in the Files app. Note that when this operation completes, you must recreate all existing shared links to contents in the renamed folder.

In the vast majority of cases, renaming a file or folder is an operation performed by your cloud storage. The various cloud platforms use different schemes to rename.

For example, to rename a folder "OldFolder" to "NewFolder":

- Some cloud platforms change a prefix in the file path. For example, the original file path may be OldFolder/MyFile. After renaming, that same file will use the path NewFolder/MyFile.
- Some cloud platforms first create NewFolder. Then they move or copy the contents of OldFolder to New Folder. When all the contents of OldFolder are present in NewFolder, the cloud storage deletes OldFolder.

In any case, the larger the item, the longer the rename requires. For the largest files and folders, it may take several hours or even several days. AoC treats renaming as a background operation so you can continue working in Files while the operation completes.

During the renaming operation, AoC disables the folder to prevent further actions on OldFolder until renaming completes. Note that the folder is not disabled to other users who may have shared access to it. Aspera recommends that no one perform any operations on the folder and its contents until the renaming operation completes.

Once complete, AoC deletes OldFolder and displays NewFolder.

Note: You must refresh your Files listing to see NewFolder.

Identify the issue

If an anomaly occurs in the network or in cloud storage, the renaming may not complete. You know that renaming did not complete if you see either of these situations:

- After seven days, OldFolder still displays after you refresh the page.
- At any time, both OldFolder and NewFolder display. (Remember that, depending on folder names and the sort order you set for your Files listing, the two folders may be on different pages in the Files app.) In this case, folder content may be split between OldFolder and NewFolder. There may some content that exists in both folders.

Cloud storage will not lose any of your content in either case.

Troubleshoot

If after seven days Old Folder still displays after you refresh the page, perform the rename operation again.

If both OldFolder and New Folder display, do the following:

1. Determine which of the two folders contains the majority of the content. Consider item sizes as well as item count.
2. Move the content manually to the folder with the most content.
Note: For the items you move manually, you must restore the intended access permissions manually.
3. If in step 2 you moved content to OldFolder, try the rename operation again.

Specific error messages

This article describes troubleshooting options for some specific error messages.

Aspera Connect is unavailable

- Recommended action: Download and install IBM Aspera Connect. See [Installing Aspera Connect](#).
- More information: See [Select a transfer method](#).

Unable to load files

- Recommended action: Check with the person who sent you the link. The link may be expired or deleted; or the person who sent you the link may have changed your access permission.
- More information: If you used a browser bookmark to access the files, the location of the files may have changed.

Unable to load requested folder

- Recommended action: Check with the person who shared the folder with you. The person who shared it may have changed your access permission.
- If AoC redirects you to your Files home folder, check with your local technical support staff. Click  and select "Technical support".

Unable to get package or Unable to show package details

- Recommended action: If you used a link to access the package, the link may have expired or been deleted; or the person who sent you the link may have changed your access permission. Check with the person who sent you the link.
- More information: The package may have been deleted. Check with the person who sent you the package.

Unable to get files information

- Recommended action: Check with the person who gave you permission to access the files.
- More information: You are not authorized to access the item. Your link to the item may be expired or deleted, or your permission to it may have been changed by sender or sharer.

Failed to open TCP connection for SSH

- Recommended action: Use the [Aspera Connect diagnostic tool](#) to run a test transfer and return diagnostic information.
- More information: The most common cause of this error is that firewall settings do not allow traffic on port 33001, which is required for Aspera FASP transfers. See also [Firewall considerations](#) on the IBM Support site.

Client unable to connect to server

- Recommended action: Use the [Aspera Connect diagnostic tool](#) to run a test transfer and return diagnostic information.
- More information: The most common cause of this error is that firewall settings do not allow traffic on port 33001, which is required for Aspera FASP transfers. See also [Firewall considerations](#) on the IBM Support site.

Verify contents and resend

- See [Resending "Draft" packages](#).

To contact your local tech support administrator, click  in the banner and select "Technical support".

If you are the local tech support administrator and need help after using this information, contact IBM support.

New and Coming Soon

As a SaaS solution, IBM Aspera on Cloud receives frequent updates to deliver new features, functionality, and bug fixes. Get previews into upcoming new features and get insights into enhancements and features as they are released, including links to details user documentation.

- [What's new in Aspera on Cloud](#)

As a SaaS solution, IBM Aspera on Cloud receives frequent updates to deliver new features, functionality, and bug fixes. This topic is a reverse chronological listing

- of new features and enhancements as they became available for Aspera on Cloud users and administrators.
- [Coming soon to Aspera on Cloud](#)
This topic is a preview of features that IBM Aspera will soon release on Aspera on Cloud.

Coming soon to Aspera on Cloud

This topic is a preview of features that IBM Aspera will soon release on Aspera on Cloud.

For new features available now, see [What's new in Aspera on Cloud](#).

What's new in Aspera on Cloud

As a SaaS solution, IBM Aspera on Cloud receives frequent updates to deliver new features, functionality, and bug fixes. This topic is a reverse chronological listing of new features and enhancements as they became available for Aspera on Cloud users and administrators.

See [Coming soon to Aspera on Cloud](#) for a preview of features that IBM Aspera will release soon.

For important announcements and notifications, see the [Notifications and announcements](#) section.

Enhanced shared inbox custom metadata controls

June 10, 2026

This new feature enhances shared inbox custom metadata by providing administrators with greater control over field visibility and validation. You can now add a new text block metadata field to shared inboxes metadata configurations. These new text block fields allow administrators to define information that is included with packages and delivered to recipients. Administrators can also control whether the field is required and if package senders can view these fields during package creation. To configure these fields, go to Workspaces > *Select a workspace* > *Select a shared inbox* > Metadata > Add field.

Shared folders visibility for workspace users

May 11, 2026

Admins can now view the shared folders that a workspace member has access to by going to Admin > Users > Management, selecting a user, and accessing the new Shared Folders tab. The Shared Folders tab displays the following information for each shared folder:

- Folder name
- Node name
- Permissions
- Membership type

This enhancement helps admins more easily review and manage user access to shared folders.

Duplicate and deactivate Automation workflows

March 26, 2026

Organization admins can now duplicate and deactivate automation workflows across the organization. From the Workflows page, switch to the **All workflows** view to access workflows created by any user and take action as needed. This enhancement improves administrative control, making it easier to manage workflows even when the original owner is unavailable.

Activity app: Track Shared Inbox and Shared folder events

March 26, 2026

You can now filter Shared inbox and Shared folder events directly from the Activity app. To do this, navigate to Activity app > Application events and filter by the relevant event types that you want to monitor. For more information on the new filters, visit the [Monitor application events](#) section.

Multi-session transfers

December 10, 2025

With multi-session transfers you can simultaneously transfer large files dividing them into smaller segments through multiple sessions. Instead of relying on a single transfer session, you can distribute the workload across several parallel sessions. This accelerates the transfer process, taking advantage of the combined bandwidth from multiple connections. To learn more about this feature, refer to the [Multi-session transfers](#) section.

Password complexity configuration

November 25, 2025

Aspera on Cloud now supports configurable password complexity requirements for client-side encryption. You can define custom complexity rules, so passwords setup for packages must match the rule provided, enabling stronger security controls that match your organization's standards.

To configure this feature, go to Admin > Nodes and Storage > *Select a Node* > Node Configuration > Node Profile > Aspera Encryption at Rest, and enable the option to customize password complexity.

Transfer Diagnostics Aspera for desktop support

November 24, 2025

The [Diagnostics](#) page now includes support for the new IBM Aspera for Desktop application. Under Client Options, you can verify that your device with the new IBM Aspera for desktop client can successfully establish a connection with our transfer servers.

Antivirus scanning

October 2, 2025

With the introduction of this feature, you can now enable antivirus scanning to use with your Trend Micro instance. Packages are automatically scanned for viruses and malware, ensuring safer transfers whether you are collaborating internally or with external parties. For detailed instructions about the setup and configuration process, refer to the [Antivirus scanning](#)

Node access for workspace managers

July 18, 2025

You can now provide workspace managers access to a node by configuring specific paths they can use. This new feature, available under Workspaces > *workspaceName* > Profile > Node access for workspace managers, lets you define and assign one or more paths for managers to access. With this change, workspace managers can also create shared folders for their workspace, enabling a seamless sharing experience. For more information about this feature, see the [Node access for workspace managers](#) section.

Redesigned shared folder experience in the Files app

June 26, 2025

With the implementation of this new feature, the Files application has received the following updates to make access and navigation more intuitive:

- Home folder (formerly *All files*): contains all the files and folders available in your workspace.
- Favorites: displays all the folders that you marked as favorites for quick access.
- Shares: a new section where you can see all the shared folders you have access to in the workspace. You can also click View all under Shares, to browse, rename, or remove any shared folders.

Important: The left navigation only displays the first 20 shared folders. If you have access to more, you can find them in the **Shares > View all** section. To access shared folders with the legacy layout, you can go to the Move/Copy panel.

These updates are designed to make it easier to manage shared content within your workspace.

Simplified folder sharing

June 18, 2025

With this new feature, admins only need to enter the node access key and secret once when creating or managing their nodes. After the initial authentication, you can set the node's ownership to either ATS admins only or all organization admins. Once ownership is set, users can browse, share, and manage node folders without the need to re-enter their credentials, making the shared folder creation process a lot easier. Nodes that were previously added are automatically set to ATS admins only. It is important to note that you still need to provide the secret when creating sub-access keys.

Support for additional IBM Cloud regions

April 21, 2025

The Aspera on Cloud transfer service now supports these additional IBM Cloud regional data centers: Ohio (us-east-2), and Oregon (us-west1). For a complete listing of supported regions, see [Cloud platforms and regions supported](#).

Share folders directly from the Files app

March 31, 2025

Creating and sharing folders in the Files app is now easier! Admins and users with shared folder creation permissions can share folders directly from the Files view—no need to navigate to the Admin section. This update simplifies collaboration and saves valuable time.

Shared folders and shared inboxes access

March 4, 2025

You can now access and manage shared folders and shared inboxes directly from your workspace (Admin > Workspaces > *your workspace* > Shared folders/Shared inboxes). This enhancement makes accessing and creating these shared folders and inboxes much easier and faster, resulting in less clicks and an improved user experience.

Enhanced folder sharing security

February 20, 2025

Admins can now enhance security and access control over folder sharing within a specific workspace. This new feature allows admins to define who (all members, managers, or none) can re-share folders with other workspace members, making sure that only authorized members can extend access to shared content.

Easier group management

February 20, 2025

Managing groups just got a lot simpler. Admins and workspace managers can now search for existing groups when assigning group managers or owners. This eliminates the need to add members individually, making group management faster and more efficient.

Improved group member management

February 11, 2025

It is now easier for admins to add multiple users to groups. Instead of manually adding users one by one, admins can now copy and paste a list of email addresses directly into the search bar, just like when adding members to a workspace. This new feature not only saves time, but it also provides a streamlined workflow and a consistent experience throughout Aspera on Cloud.

Custom profiles for file permissions

February 11, 2025

We are introducing a new feature that allows users to save custom profiles for files permissions. This feature allows users to create, save, and reuse custom permissions, eliminating the need to manually configure permissions each time. Additionally, admins can mirror an existing user's permissions to streamline onboarding. This enhancement simplifies permission management and improves efficiency for growing teams. Custom profiles are applied at the user level, not globally across the organization.

Send form enhancement

February 11, 2025

You can now use markdown to format the text in the instructions text box when sending a package to a shared inbox.

IBM Aspera for desktop

January 23, 2025

Users on Essentials and Standard Plus subscriptions can now switch to IBM Aspera for desktop. This new application is a modern and reliable transfer client that removes the need for Connect's web browser extension, allows for automatic updates, and much more. This new application will be replacing Connect, becoming the primary transfer client for FASP transfers. For more information about what IBM Aspera for desktop can do, refer to the [official documentation](#).

In-app alert notifications

December 20, 2024

We have introduced a new notification system to help organization admins stay informed about usage levels and avoid overages. This feature displays an alert when an organization approaches 80% and 100% of its entitled volume, storage, or egress usage. This enhancement ensures better visibility before limits are exceeded. Notifications for upcoming maintenance windows are also available.

Disable package sending

October 15, 2024

You can now disable package sending within an organization or workspace. This provides added control and flexibility when migrating workflows or restructuring your organization. Both organization admins and workspace managers can disable/enable this setting. When this setting is turned on, users are still able to send packages to shared inboxes. For more information, see the [Disable package sending](#) section.

Scheduled packages

September 12, 2024

With this feature you can create and schedule packages to send them at a specific time, providing greater flexibility, reliability, and improving the way you manage and send your packages. This ensures everything is ready for release without the pressure of immediate sending. IBM Aspera on Cloud will send you a reminder at least 24 hours before your scheduled package is ready to be sent. For more information see the [Schedule packages to send later](#) section.

File deletion policies: Tethered nodes support

June 10, 2024

You can now apply file deletion policies to tethered nodes. When an administrator creates a file deletion policy on an tethered node, the policy applies only to that specific node. If there are other nodes on the same storage and location, this policy is going to affect those as well. For more information see the [File deletion policies for storage management](#) section.

Standard subscription name update

May 7, 2024

IBM Aspera on Cloud Standard subscription has been renamed to Essentials. This is only a new name for that subscription tier, all features and cost remain the same. If you are subscribed to the Standard edition, there's no action needed and you can continue to enjoy the same benefits you already had.

Save packages as drafts

March 13, 2024

No more lost work and time constraints! With this new feature, you can save packages as drafts, preventing you from losing all your progress and incorporating the ability to stage deliveries for future release. For more information about this feature refer to the [Save packages as drafts](#) section.

Automatic user reactivation

February 21, 2024

Deactivated Aspera on Cloud users (due to inactivity) can now login again as soon as they receive a package. Also, SAML users who were previously deactivated due to inactivity, will be reactivated when they login through their SAML provider. You can automatically do this without admins having to manually activate them, optimizing both time and manual effort. Admins can configure the settings for this new feature in User > Advanced > Auto reactivation. For more information see the [Automatic user reactivation](#) section.

Workspace customization

December 22, 2023

You can currently customize your organization and now you can do the same for individual workspaces. These new customization features allow admins to set custom backgrounds (such as in headers, buttons, left menu) and fonts (including font color) at the workspace level. To configure these settings, open the workspace you want to customize and adjust the settings under the Login page and Theme editor tabs accordingly.

Move/copy files between workspaces

December 6, 2023

We are introducing a significant enhancement to the move/copy panel in Aspera On Cloud. Users can seamlessly transfer files between different workspaces, eliminating the need to create shared links. This improvement makes node-to-node transfers more accessible and efficient than ever before.

Key feature updates:

- **Independent workspace browsing:** Users can independently browse through different workspaces and explore their folder structures directly within the move/copy panel. This flexibility provides seamless navigation between workspaces.
- **Streamlined move/copy functionality:** We retain the core move/copy functionality, ensuring a familiar experience for users. The process remains straightforward and efficient.

Transfer activity modal

November 6, 2023

With the new Transfer Activity Modal, keeping an eye on your file transfers has never been easier. When you initiate a file transfer, you can now access an activity modal by simply clicking the information icon. The modal gives you the ability to adjust the target rate of desktop transfers that were started using the Aspera clients, and provides you with real-time insights including transfer rate, percent completion, and much more.

Note: You cannot exceed the server maximum target rate. For more information see the [Cloud platforms and regions supported](#) section.

Customization

October 3, 2023

To help you incorporate your own branding and style we have released new customization features. These features allow admins to set custom backgrounds (headers, buttons, left menu) and fonts (including font color) at the Organization level. To configure these settings at the Organization level, navigate to the Admin application, open the Organization drop-down, and select Profile and Branding.

Branding

October 3, 2023

The user experience starts as soon as a user lands on the login screen, that's why we want customization capabilities to extend beyond the in-app experience. As an admin you can customize the login screens and their respective URLs at the Workspace level. You can also add a logo and full HD splash screen background to the workspace login screen, replacing the default IBM Aspera on Cloud theme. To configure these settings go to the Admin app, open the Organization drop-down, and select Profile and Branding.

File deletion policy new cloud support

October 3, 2023

Previously limited to AWS storage, IBM Aspera on Cloud's file deletion policy is now supported in Google Cloud Platform and Azure. The file deletion policy allows admins to set a length of time before files are automatically deleted from a node (and the associated storage bucket). Automating the deletion of outdated files helps save storage space, reduces storage costs, and streamlines workflows.

Logout notification

September 21, 2023

With the new logout notification feature, users are notified five minutes before their session is about to expire due to inactivity. They can extend their session before it expires due to inactivity, or they have to reauthenticate if their session expires. This minimizes the number of times a user must log in, saving time and increasing productivity. This option is disabled by default for new organizations, meaning users are never logged out due to inactivity. Admins can enable and configure the maximum duration for inactive sessions, as well as login token expiration by navigating to the Admin application, selecting the Organization drop-down, and then the Security tab. The recommended duration for inactive session logout is one hour, but valid durations range from 15 minutes to seven days. For more information see [Session and token duration](#).

File preview

June 7, 2023

Introducing our new File preview feature. With this new capability, you can generate video or image thumbnails from your files to preview their content while browsing through them. File preview adds triggers in a cloud storage (AWS S3) to invoke a function every time you upload a supported file type. With that trigger, the function has enough information to pull data from that file to generate a preview using FFmpeg (in the case of video files) and upload it back to cloud storage.

File preview also checks S3 files to see if they already have a preview. If not, it calls File preview with the necessary info to process it. In some cases, this feature temporarily downloads the file to work with it. Don't worry, we make sure that it is deleted (not from your cloud storage) after it's done processing it.

To enable File preview, you have to build a container image with FFmpeg packaged inside. FFmpeg is a free open-source utility that is not provided or managed by IBM and is subject to third-party terms and conditions. FFmpeg contains codecs for encoding and decoding various video coding formats. Certain codecs contained within FFmpeg may be covered by patents and require a license to use. The Dockerfile provided by IBM will enable all codecs in FFMPEG by default. However, you must assess your own licensing needs in connection with the use of FFmpeg and adjust which codecs to enable accordingly.

File preview on AWS requires self-hosted preview generation on your own AWS Lambda instance. We're currently developing an IBM managed solution for all cloud platforms. This feature is available for Aspera on Cloud Premium subscribers

File deletion policies

March 9, 2023

Admin and Files apps.

Admins have an additional tool to manage storage in their Aspera on Cloud organization by creating policies to permanently delete files and folders when they reach a configured age. File deletion policies automate a formerly manual administrative process. When an administrator creates a file deletion policy on an attached node, the policy applies to all nodes on the same storage. Once the policy is active, it will also apply to new nodes that you create in the same storage.

ATS enhancements

December 15, 2022

IBM Aspera enhanced Aspera Transfer Service (ATS) to improve platform stability.

Support for additional AWS storage classes

November 18, 2022

Admin app.

Aspera on Cloud now supports several additional AWS storage classes, including the increasingly popular Glacier archival classes. Files app users can write directly to Glacier storage and see the "Glacier storage" label for files in Glacier storage.

- Standard
- Intelligent Tiering
- Standard Infrequent Access
- One-zone Infrequent Access
- Glacier Instant Retrieval
- Glacier Flexible Retrieval
- Glacier Deep Archive

In a workspace configured on a node with storage class Glacier Flexible Retrieval or Glacier Deep Archive, the Packages app is disabled due to extended AWS retrieval times. In the Files app, users can view and upload to the storage, but cannot download, move, copy, or rename files. For details, see [Attach an AWS S3 bucket](#).

Renaming large folders

October 12, 2022

Files app.

To rename very large folders, the Files app provides a new option: Rename and move. This feature improves performance for such large file operations. The renamed folder appears in the same location in the Files app. Note that when this operation completes, you must recreate all existing shared links to contents in the renamed folder. For details, see [Rename folders in your Files app](#).

Automation: New options for transfer actions

October 12, 2022

Automation app.

Transfer is a commonly configured action in automated workflows. This change makes new options available for the disposition of transfer source folder contents when the transfer completes. For details, see [Workflow actions and their attributes](#).

Distribution lists for sending packages

September 21, 2022

Admin and Packages apps.

Aspera on Cloud now supports both personal and global distribution lists for sending packages.

Users can create lists for their own personal use and then select them as recipients in the To field of the Send packages form. Administrators can create workspace-level distribution lists and make them available to either all members in the workspace or to workspace managers only.

For details, see [Create a personal distribution list](#) and [Create workspace distribution lists](#).

New IBM Aspera mobile app

July 10, 2022

The new mobile app, IBM Aspera, offers streamlined functionality for fast file transfers to and from your Aspera servers.

Using the new Carbon X interface, this consolidated mobile experience matches what you see on your web browser for Aspera on Cloud. Use your Aspera server account credentials to log into Aspera on Cloud to transfer files to and from your mobile device.

The new mobile app is FASP-native, so you can transfer files to and from your mobile device with the amazing speeds of IBM Aspera's proprietary FASP protocol. The app is available on both the [Apple App Store](#) and the [Google Play Store](#).

IBM Aspera replaces the functionality of the following legacy mobile applications:

- Aspera on Cloud
- Aspera Uploader
- Aspera Drive
- Aspera Faspex

To connect your IBM Aspera to your Aspera on Cloud account, see [IBM Aspera mobile app](#). For more information, see the [IBM Aspera mobile support page](#).

Public link enhancements for increased admin control

May 4, 2022

Admin, Files, and Packages apps.

Aspera on Cloud provides two enhancements to improve admin control of public link usage. These enhancements apply to public links in the Files app and in the Packages app, including shared inboxes. The admin can apply either or both enhancements across the entire organization, for one or more given workspaces, or to specific shared inboxes in a workspace.

Workspace members have always had the option to apply a password to a public link. Unless the link recipient can enter the password, the link target remain inaccessible. This new enhancement allows the administrator to *enforce the password requirement* for all public links.

Similarly, workspace members have always been able to set an expiration for a public link, after which the link target becomes inaccessible. This new enhancement allows the admin to *set a default expiration* for all public links. An individual user can reduce the expiration set by the admin, but cannot extend it.

Disallow encryption-at-rest during package send operations

May 4, 2022

Packages app.

Users of the Packages app can enable encryption-at-rest (EAR) for packages they send, allowing them to apply a password to a given package. Until the recipient applies the password, Aspera on Cloud retains package encryption at the recipient's end, even when the recipient downloads the package to their own local or remote storage.

This enhancement enables admins to *disallow* the application of EAR to packages in all workspaces or in specific workspaces, including in shared inboxes. With this feature applied, senders will not be able to apply EAR on individual packages, which is essential for organizations with downstream automation workflows that leverage server-side encryption-at-rest options instead.

File synchronization support on ATS

May 4, 2022

Note: This feature works with Connect 4.1.3 only; you must upgrade if you're still using an older version of Connect.

Admin, Files, and Packages apps.

Aspera on Cloud has supported integration with IBM Aspera Drive, enabling users to access content in Aspera on Cloud workspaces directly from their desktops without using a browser. Aspera Drive was recently consolidated into Aspera Connect. So your organization members now use Aspera Connect for desktop access to Aspera on Cloud workspace content. Such desktop access allows browsing, uploads, downloads, and sync functions from the desktop.

This enhancement to ATS servers supports synchronization of local folders with remote folders on all ATS transfer regions. Previously, this sync capability was available only on [user-managed tethered nodes](#), AoC-managed nodes, and in a few ATS regions. With this enhancement, all node types support sync using Aspera Connect. See [Desktop access to AoC using IBM Aspera for desktop](#).

New IBM Aspera mobile app

April 30, 2022

The new mobile app, IBM Aspera, offers streamlined functionality for fast file transfers to and from your Aspera servers.

Using the new Carbon X interface, this consolidated mobile experience matches what you see on your web browser for Aspera on Cloud. Use your Aspera server account credentials to log in to Aspera on Cloud to transfer files to and from your mobile device.

The new mobile app is FASP-native, so you can transfer files to and from your mobile device with the amazing speeds of IBM Aspera's proprietary FASP protocol. The app is available for both [iOS](#) and [Android](#).

IBM Aspera replaces the functionality of the following legacy mobile applications:

- Aspera on Cloud
- Aspera Faspex
- Aspera Drive
- Aspera Uploader

To link IBM Aspera to your existing Aspera on Cloud account, see [IBM Aspera mobile app](#). See also the [IBM Support page for IBM Aspera](#).

Enhanced watermarking support

April 14, 2022

Admin and Packages apps

While the Aspera on Cloud integration with Irdeto's watermarking service has been in place for well over a year, these new enhancements extend the usability and functionality of the integration for users of the Packages app. The first enhancement supports watermarking even for short video clips, which previously was not possible. The second enhancement ensures the success of a package transfer even when not all files in the package can be watermarked. See [Watermarking: Integrate your Irdeto service](#) and [Sending: Become an expert](#).

Browser support now adheres to Carbon Design System requirements

March 22, 2022

The Carbon Design System underlies the Aspera on Cloud user interface. Aspera on Cloud browser support now adheres to the Carbon Design System requirements, available [here](#).

New support for additional GCS region

March 17, 2022

Admin app

The Aspera on Cloud transfer service now supports the Google Cloud Service London data center (europe-west2). For a complete listing of supported regions, see [Cloud platforms and regions supported](#).

A new experience for Aspera on Cloud

March 9, 2022

IBM Aspera has launched the next generation of Aspera on Cloud.

Improved responsiveness and a modernized user interface are two highlights of a thorough remake of Aspera on Cloud. Existing features and functionality persist in the new experience, along with numerous enhancements to app behavior and appearance. A few key changes:

Global

- Full support for smartphone and tablet access
- Global search relocated to the upper banner near the transfer monitor
- User interface dark and light modes: the default follows your computer setting; custom control available from the User menu

Tables

- Faster loading throughout; improved browsing responsiveness
- Set personal default page size in Account settings
- Right-click context menus support multi-select operations
- Functional icons now consolidated to the upper-right of the view
- Advanced filters now grouped in one location at top right of each table

More troubleshooting resources

- Admin access to error and session data through Help menu
- Additional articles and procedures

Help center

- Reorganized content and addressed information gaps according to user research findings
- Discrete admin and user articles
- Bookmark favorite articles and list recently viewed articles for easy reuse

End of support for certain IBM Cloud regions

As part of our modernization strategy, we have closed the following ATS regions:

- Paris (par01)
- Chennai (che01)
- Mexico (mex01)
- Montreal (mon01)
- Singapore (sng01)

For supported regions, see [Cloud platforms and regions supported](#).

A new experience for Aspera on Cloud

February 4, 2022

IBM Aspera will launch the next generation of Aspera on Cloud on *March 9, 2022*.

Improved responsiveness and a modernized user interface are two highlights of a thorough remake of Aspera on Cloud. Existing features and functionality persist in the new experience, along with numerous enhancements to app behavior and appearance. A few key changes:

Global

- Full support for smartphone and tablet access
- Global search relocated to the upper banner near the transfer monitor
- User interface dark and light modes: the default follows your computer setting; custom control available from the User menu

Tables

- Faster loading throughout; improved browsing responsiveness
- Right-click context menus support multi-select operations
- Functional icons now consolidated to the upper-right of the view
- Advanced filters now grouped in one location at top right of each table

More troubleshooting resources

- Admin access to error and session data through Help menu
- Additional articles and procedures

Help center

- Reorganized content and addressed information gaps according to user research findings
- Discrete admin and user articles
- Bookmark favorite articles and list recently viewed articles for easy reuse

End of support for node search service

January 21, 2022

Because of the `log4j` vulnerability, the IBM Aspera team strongly recommends uninstalling the `files-node-search` application. This feature is deprecated and is no longer used by our software. Instead, configure the AEJD service on your user-managed server (tethered node) to transmit data to Aspera on Cloud. See [Configure monitoring and metering for your tethered node](#).

If you have installed the `files-node-search` application, remove it now.

1. Stop the service:

```
# /opt/aspera/files-node-search/etc/init.d/files-node-search stop
```

2. Remove the folder:

```
# rm -rf /opt/aspera/files-node-search
```

Decommissioning certain IBM Cloud regions

As part of our modernization strategy, we will close the following ATS regions on January 31, 2022:

- Paris (par01)
- Chennai (che01)
- Mexico (mex01)
- Montreal (mon01)
- Singapore (sng01)

For supported regions, see [Cloud platforms and regions supported](#). Please contact IBM Sales if you have any concerns about the closure of these ATS regions.

Required firewall changes

On January 22, 2022, Aspera on Cloud will begin using the Akamai Technologies network in front of the AoC API and Front end. You must update your firewall rules before that date.

If your firewall allows the IP ranges shown in "[System requirements and browser support](#)" for your users to access AoC, you must update your settings to also allow the hostnames `api.ibmaspera.com` and `<your_org_subdomain>.ibmaspera.com`, both on port 443. After January 22, 2022, you can disallow the IP ranges you now list.

Customers using the legacy `api.asperafiles.com` endpoint for API clients must update their allowlist in the same way.

Customers who tether their own entitlement-based (usage-based) HSTS installation must also update their allowlists to continue to communicate to `api.ibmaspera.com`.

The currently published IP range for communication from AoC to tethered nodes, to ATS nodes, and to Aspera-manages nodes remain unchanged.

A new experience for Aspera on Cloud

Beta release: December 16, 2021

Improved responsiveness and a modernized user interface are two highlights of a thorough remake of Aspera on Cloud. Existing features and functionality persist in the new experience, along with numerous enhancements to app behavior and appearance. A few key changes:

Global

- Full support for smartphone and tablet access
- Global search relocated to upper banner near transfer monitor
- Dark and light modes; default matches computer setting, controllable from the User menu

Tables

- Faster loading throughout; improved browsing responsiveness
- Right-click context menus support multi-select
- Functional icons consolidated to upper right of the view
- Advanced filters grouped in one location at the top-right of the table

More troubleshooting resources

- Additional articles and procedures
- Admin access to error and session data through the Help menu

Help center enhancements

- Reorganized content and addressed information gaps according to user research findings
- Discrete admin and user articles
- Bookmark favorite articles and list recent articles for easy reuse

New reporting capability: Generate and store asynchronous reports

December 16, 2021

Activity app

Activity app users are already able to export, save, and download reports for transfer activity, volume usage, file access, and app events. An extensive collection of filters allows you to fine-tune the report to address specific data needs. Each report can contain up to approximately 100,000 records relevant to the filters you set.

This new feature enhances the performance and behavior of these Activity app reports in several ways. First, the reports can be generated asynchronously. You can start the report, attend to other tasks, and be notified by the app when the report is available. Second, there is no limit to the number of records the report can contain. And third, the reports are stored in a shared space that makes them available to all Activity app users.

The Activity interface allows an admin to set up this shared space in the desired location in attached storage. Users then see this shared space and its contents as a new page, called Stored reports, in the Activity app.

This new Stored reports page allows you to filter for your own reports and for specific report types (for example, for transfer activity reports). Activity app users can download, get info on, and delete these reports. For details, see [Reporting activity and usage](#).

Revised browser support, including end of support for MS Internet Explorer

November 15, 2021

IBM Aspera has revised the list of browser versions supported. This update includes the end of support for Microsoft Internet Explorer on December 31, 2021. See [System requirements and browser support](#).

Support for additional IBM Cloud regions

October 18, 2021

The Aspera on Cloud transfer service now supports these additional IBM Cloud regional data centers: Osaka (jp-osa), Toronto (ca-tor), Sao Paulo (br-sao); and this additional single-site data center: Singapore (sng01). For a complete listing of supported regions, see [Cloud platforms and regions supported](#).

Support for additional MS Azure region

September 24, 2021

The Aspera on Cloud transfer service now supports the Microsoft Azure London data center (uksouth). For a complete listing of supported regions, see [Cloud platforms and regions supported](#).

Support for additional AWS region

September 14, 2021

The Aspera on Cloud transfer service now support the AWS Northern California data center (us-west-1). For a complete listing of supported regions, see [System requirements and browser support](#).

Support for files and folders in AWS Glacier storage

July 19, 2021

Files and Packages apps.

IBM Aspera is phasing in support for access to content in AWS S3 Glacier storage.

Before this Phase 1 enhancement, the Aspera on Cloud web UI did not mark items in AWS S3 Glacier storage. When users tried to access such an item, they received an error message.

In Phase 1 support, items in Glacier storage are labeled as such. The only action allowed on an item in Glacier in Phase 1 is a request for more information; a dialog appears that informs users that Glacier files are not accessible through Aspera on Cloud, and suggests they contact their administrator for access.

New transfer setting in Node Configuration policies

July 19, 2021

Admin app.

This new feature provides an advanced setting that you can apply in a node configuration policy to any node connected to your organization.

After a "move" transfer (as opposed to a "copy" transfer) completes, Aspera on Cloud deletes transferred files from the source folder. However, files in the source folder that already exist in the destination folder are not transferred: they are skipped. Select this option to include these skipped files in the automatic deletion. Otherwise, skipped files remain in the source folder. For details, see [Creating node configuration policies](#).

Key rotation for Azure storage

June 30, 2021

Admin app.

ATS admins can now use the Aspera on Cloud web UI to update Azure storage credentials to support key rotation. For details, see [Rotate keys for your Azure storage](#).

This new functionality adds to existing support for key rotation for Azure storage using the Aspera Node API. ATS administrators can send a PUT call to the endpoint `/access_key` with the updated storage credentials.

Multifactor authentication with IBMid

June 30, 2021

Admin app.

Your Aspera on Cloud organization will soon support multifactor authentication. An administrator can require this feature for users who authenticate with IBMid.

When a user presents their IBMid credentials, Aspera on Cloud presents two options. The user can elect to receive either an email with a verification code or a time-based, one-time passphrase (TOTP) using an authenticator app like IBM Verify. When the user enters the code or passphrase, they'll be logged into their AoC account. For details, see [Require multifactor authentication for IBMid users](#).

Management support for multi-entitlement subscriptions

June 9, 2021

Admin app.

Administrators of IBM Aspera subscriptions with multiple entitlements now have access to the Subscription management page. These admins can now take advantage of the usage dashboard and of the detailed graphs and tables that visualize transfer usage, egress, and storage. They can also filter the transfer and egress tables by entitlement as well as by month. See [Understanding your subscription usage and billing](#).

Automated archive support for workspace folders

June 9, 2021

Automation app.

This enhancement adds another advanced setting for transfer action steps in your automated workflows.

The Automation app previously included support for automated archiving of transfer source content when the source folder is on a node. This enhancement adds support for archiving of transfer source content when the source folder is in a workspace. See [Workflow actions and their attributes](#).

Enhancement to transfer source treatment: Include skipped files

May 21, 2021

Automation app.

This enhancement adds another advanced setting for transfer action steps in your automated workflows.

When your transfer source folder is a node folder (as opposed to a workspace folder), you can already configure automatic deletion of files from the source folder after the transfer step. This enhancement will allow you to include *skipped* files in the delete option.

Files that already exist at the destination are *skipped* by the transfer since they already exist at your configured destination. When you select this option, the workflow deletes files in the source folder that were skipped, along with those that were transferred (not skipped). The result after the transfer is an empty source folder, which is also automatically deleted. For details, see [Workflow actions and their attributes](#).

New filter for job queue

May 6, 2021

Automation app.

This enhancement gives org administrators better insight into ongoing activity in the Automation app.

The Job queue page has always shown in-progress jobs for workflows that you own or manage. This new filter allows you to switch views between your jobs only and all jobs in progress. This expanded view of current activity helps admins understand whether to expect a specific job to be running or to be queued behind other in-progress jobs.

Monitor and report transfer volume by entitlement

May 5, 2021

Activity app.

To make internal cost accounting easier and faster for organizations with multiple entitlements, you can report transfer volume usage by specific subscription entitlement. For details, see [Example use cases for monitoring transfer activity](#).

Watermarking support in additional AWS regions

April 19, 2021

You can now apply forensic watermarking to more of your sensitive content. Aspera on Cloud supports watermarking in all these AWS regions:

- N. Virginia (us-east-1); Oregon (us-west-2);
- Sao Paulo (sa-east-1)
- Ireland (eu-west-1); London (eu-west-2); Frankfurt (eu-central-1)
- Tokyo (ap-northeast-1); Singapore (ap-southeast-1); Sydney (ap-southeast-2)

For details, see [Watermarking: Integrate your Irdeto service](#).

Volume usage for deleted workspaces

April 8, 2021

Activity app.

You can now filter and report on volume usage in workspaces that have been deleted. This enhancement includes clear labeling for deleted workspaces in the workspace choices filter.

Field deprecations in Activity app API

April 7, 2021

Activity app.

If you use either of the two deprecated fields below, this is a breaking change.

In the Transfer Activity API endpoint `/transfers`, these two fields are deprecated and will be removed from the Activity app API on July 7, 2021:

- **Deprecated fields**
 - `client_ip_address`
 - `server_ip_address`

The data contained in these deprecated fields are better represented by these new fields, available for your use now in the Activity app API:

- **Replacement fields available now**
 - `local_ip_address`
 - `peer_ip_address`

The values in these new fields are relative to the transfer direction, represented by the `direction` field. See the [Aspera Activity API on IBM API Hub](#).

Monitor and report transfer volume by shared inbox

April 7, 2021

Activity app.

To make internal cost accounting easier and faster, you can now filter and report transfer volume usage by shared inbox. On the Transfer usage page, first filter for the workspace, then for the intended shared inbox within that workspace.

Support for IBM Aspera HTTP Gateway

April 6, 2021

Admin, Files, and Packages apps.

When some users cannot install the IBM Aspera Connect transfer client, your organization needs an alternative transfer method. To address this need, Aspera on Cloud supports the [IBM Aspera HTTP Gateway](#).

Once you configure your Aspera HTTP Gateway, you can point your Aspera on Cloud organization to it. Enabling the Gateway ensures that all Aspera on Cloud users can transfer.

Even when the Aspera HTTP Gateway is enabled, users who install Aspera Connect can continue to use it. Keep in mind that Aspera Connect transfers are typically faster than Aspera HTTP Gateway transfers. For details, see [Transferring with HTTP Gateway instead of Aspera Connect](#).

Automation: New archive option for source content in node Folder

March 30, 2021

Automation app.

Take advantage of a new option for source content disposition when you build a transfer step in an automated workflow.

Existing options allow you to delete the content in your designated source folder after the transfer. The new option allows you to archive content rather than deleting it when the source folder is on a transfer node. You can designate an existing folder as the archive destination or create a new folder.

This new option supports clarity in the source folder and avoids duplicate transfers without losing the transferred content. It also allows you to track which items you've transferred by reviewing the contents of the Archive folder.

For details, see [Workflow actions and their attributes](#).

New transfer settings in automated workflows

February 25, 2021

Automation app.

You can already configure multiple transfer settings in your automated workflow transfer action steps. This enhancement adds a new transfer setting and two additional options for an existing setting.

You can now apply a rate policy setting that governs how Aspera transfers behave when other outgoing traffic is present. You can select one of four policy options (Fair, Low, High, Fixed). Note that the actual transfer behavior depends on the interaction between Automation app settings and transfer server settings. The actual transfer behavior conforms to the more restrictive setting.

This enhancement also adds two new transport encryption options (AES-192 and AES-256) to the existing option to apply AES-128. Again, the settings at the transfer server and the Automation app interact. The higher key-length setting takes precedence.

For details and examples, see [Workflow actions and their attributes](#).

Support for pagination on attached transfer servers

February 9, 2021

Admin app.

A new enhancement in IBM Aspera transfer server software allows you to change the browsing experience for your Aspera on Cloud users.

This enhancement is a new pagination capability released in IBM Aspera HSTS v4.0. You can choose whether to enable this pagination setting for each transfer server attached to your Aspera on Cloud org. For details and a procedure, see [Creating node configuration policies](#)

The pagination facility, when enabled, returns an internally controlled number of items from the folder being browsed, whether the folder is in cloud storage or on your own tethered node. The paginated response help avoid the time-out issue that is common for large folders in cloud storage.

Note that any paginated return of folder contents does not support retrieval of sorted content. This means that lexicographical sorting of content occurs only within the returned batches.

All Aspera-managed auto-scale clusters (ATS) are upgraded automatically to HSTS v4.0. Customers who tether their own transfer servers to Aspera on Cloud and want to enable this behavior must upgrade to IBM Aspera HSTS v4.0.

Enhanced transfer activity data

January 13, 2021

Activity app.

The Transfers table in the Transfer activity page now provides additional data to help you track and analyze individual transfers and overall usage. The new data also helps you troubleshoot transfer issues if they occur. And all this new information is included when you export a report.

This table has always provided, for each transfer, the event type and start date, along with the associated user, workspace, node.

The existing Node column now provides the IP address along with the name of the node for each transfer. Two new columns indicate the direction and peer for each transfer. Together, the Node, Direction, and Peer columns provide key data for analyzing individual transfers. You have names and IP addresses of both endpoints for each transfer and know which direction (from the perspective of the node) the transfer flowed.

An additional new column reports event status.

Share your automated workflows

January 13, 2021

Automation app.

You can now share your workflows with others, giving them permission to manage workflow jobs. The users you share with can view the workflow and can start, cancel and delete jobs. A new notification, when enabled by the admin, notifies each user you share with of their access to your workflow.

Notification enhancements for automated workflows

January 13, 2021

Automation app.

Automation app builders have always been able to incorporate email notifications to interested individuals as actions in a workflow. Similarly, you've been able to configure notifications to individuals about job status (start/fail/complete) for a given workflow.

This enhancement adds the ability to address groups in these notifications. Org admins can send notifications to any group in the organization. Automation app users who are not org admins can send notifications to groups of which they are members.

Workflow revision tags

January 13, 2021

Automation app.

Each time you revise and activate a workflow, the workflow version increments. This UI enhancement presents users with a visual, numeric, version tag on both the Workflows page and the Job queue page.

The Workflows page always shows the latest version of the workflow. The Job queue page always shows the workflow as it existed at the time the job was run. This means that the workflow as you see it on the Job queue page may be an earlier version than the workflow you see on the Workflows page.

The new version tags make it easy to distinguish which version of the workflow you are viewing.

On the Workflows page, version tags display on all workflows listed. On the Job queue page, the version tag displays on all jobs launched after the enhancement is released.

Legal Notice

© 2018-2026 Aspera, Inc., an IBM Company. All rights reserved.

Licensed Materials - Property of IBM

© Copyright IBM Corp., 2026. Used under license.

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Aspera, the Aspera logo, and FASP transfer technology are trademarks of Aspera, Inc., registered in the United States. Aspera Connect, IBM Aspera High-Speed Transfer Server (a merger of IBM products formerly named Aspera Connect Server and Aspera Enterprise Server, 2008 and 2007), IBM Aspera High-Speed Endpoint (formerly Aspera Point-to-Point, 2006), IBM Aspera Desktop Client (formerly Aspera Client, 2005), Aspera Connect, Aspera Cargo, Aspera Console, Aspera Orchestrator, Aspera Shares, the Aspera Add-in for Microsoft Outlook, Aspera FASPStream, and Aspera Faspex are trademarks of Aspera, Inc. All other trademarks mentioned in this document are the property of their respective owners. Mention of third-party products in this document is for informational purposes only. All understandings, agreements, or warranties, if any, take place directly between the vendors and the prospective users.