IBM Security Access Manager
Version 9.0.6
November 2018

Product overview

IBM Security Access Manager
Version 9.0.6
November 2018

Product overview

Contents

Accessibility features for Security Access Manager

Accessibility features assist users who have a disability, such as restricted mobility or limited vision, to use information technology content successfully.

Accessibility features

Security Access Manager includes the following major accessibility features:

Accessibility features
Supports interfaces commonly used by screen readers. This feature applies to applications on Windows operating systems only.
Can be operated by using only the keyboard.
Allows the user to request more time to complete timed responses.
Supports customization of display attributes such as color, contrast, and font size.
Communicates all information independently of color.
Supports interfaces commonly used by screen magnifiers. This feature applies to applications on Windows operating systems only.
Allows the user to access the interfaces without inducing seizures due to photosensitivity.

Security Access Manager uses the latest W3C Standard, WAI-ARIA 1.0 (http://www.w3.org/TR/wai-aria/), to ensure compliance to US Section 508 (http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards), and Web Content Accessibility Guidelines (WCAG) 2.0 (http://www.w3.org/TR/WCAG20/). To take advantage of accessibility features, use the latest release of your screen reader in combination with the latest web browser that is supported by this product.

The Security Access Manager online product documentation in IBM® Knowledge Center is enabled for accessibility. The accessibility features of IBM Knowledge Center are described at https://www.ibm.com/support/knowledgecenter/help?view=kc#accessibility.

Keyboard navigation

This product uses standard navigation keys.

Interface information

The Security Access Manager user interfaces do not have content that flashes 2 - 55 times per second.

The Security Access Manager web user interfaces and the IBM Knowledge Center rely on cascading style sheets to render content properly and to provide a usable experience. The application provides an equivalent way for low-vision users to use a user's system display settings, including high-contrast mode. You can control font size by using the device or web browser settings.

The Security Access Manager web user interface includes WAI-ARIA navigational landmarks that you can use to quickly navigate to functional areas in the application.

Related accessibility information

In addition to standard IBM help desk and support websites, IBM has established a TTY telephone service for use by deaf or hard of hearing customers to access sales and support services:

TTY service 800-IBM-3383 (800-426-3383) (within North America)

IBM and accessibility

For more information about the commitment that IBM has to accessibility, see IBM Accessibility (www.ibm.com/able).

Chapter 1. Documentation for getting started

The IBM Knowledge Center provides documentation that can help you get started with the IBM Security Access Manager product.

IBM Security Access Manager is available from Passport Advantage. You can use this distribution to either configure a new deployment or upgrade a previous version of the product.

1. If you are upgrading from a previous version of IBM Security Access Manager for Web 8.*, IBM Security Access Manager for Mobile 8.*, or IBM Security Access Manager 9.0 be sure to review Chapter 6, "Upgrading to the current version," on page 13. If applicable, you must complete these steps before you configure the product.
2. See Product activations overview to review the features you can use when you activate the Security Access Manager Platform, the Advanced Access Control Module, or the Federation Module.
3. Configure the appliance by using the instructions in Getting Started.
4. Complete the initial setup of your Security Access Manager appliance deployment by following the instructions in Initial configuration.
5. (Advanced Access Control Module only) Complete the initial setup of this module by following the instructions in Getting Started with Advanced Access Control.

Security Access Manager Platform includes an optional Java ADK, available for download. To install the Java ADK, see Installing IBM Security Access Manager Runtime for Java.

See Administering Web Reverse Proxy for instructions on how to use the local management interface on the appliance to configure and administer Security Access Manager Platform.

Chapter 2. What's new in this release

IBM Security Access Manager provides new features and extended functions for Version 9.0.6.

Access Manager Platform

- Rate limiting

  Reverse proxies can now perform rate limiting on web requests. For more information, see Rate Limiting.

- content-aware WebSEAL responses

  When you are generating a response, WebSEAL allows different response template files and response codes to be configured for different MIME sub-types. For more information, see default-response-type.

- Forwarding requests to an 'unavailable' WebSEAL junction

  The Web Reverse Proxy can now be configured to return an error when HTTP requests are received for junctioned servers which are currently failing the 'ping' operation. See disable-on-ping-failure.

- Packet Tracing

  Packet tracing can now be configured such that:

  – Packet capture does not stop once the log file is full.
  – The log file can be rotated to a defined number of rollover log files once it is full.
  – A snap length can be defined by specifying the maximum amount of data to be collected for each frame.

  For more information, see Manage Packet Tracing

- Junction specific options

  Response headers can now be configured on a per junction basis. For more information, see [rsp-header-names] stanza.

- Configuration file updates for HTTP transformation

  HTTP transformations can now be configured to match on a case insensitive basis. For more information see, Configuration file updates.

- Runtime Server Threads

  The minimum and maximum threads associated with the runtime server can be configured as part of the runtime tuning parameters. For more information, see Tuning runtime application parameters and tracing specifications.

- Adding microseconds to WebSEAL request logs

  The time, in micro-seconds, at which a request was processed by WebSEAL can now be added to the request log. For more information, see Customizing the HTTP request log.

- Reverse Proxy Management

  When you are starting, stopping, or restarting reverse proxy instances, it is now possible to perform the task on:

  – A single instance
  – A multiple selection of instances simultaneously
  – All instances simultaneously

  For more information, see Stopping, starting, or restarting an instance.

- Log File Management

  It is now possible to select multiple files and delete or clear all of them in a simultaneous operation. This includes:

  – Application log files. See Viewing application log files.
  – Reverse proxy log files. See Managing Reverse Proxy Log Files
  – Reverse proxy troubleshooting:
    - Tracing component files. See Managing the trace files for a component
    - Statistics component files. See Managing statistics log files
    - Transaction logging data files. See Managing transaction logging components and data files
    - Reverse proxy logging files. See Clearing a log file

Advanced Access Control

- New Advanced Configuration parameters

  A new AAC Advanced Configuration parameter **`mmfa.devicePrompt.skipIfOneDevice`** is added. When the parameter is set to `true` and the user has only one authenticator registered, the device selection page in a Mobile Multi-Factor Authentication flow is skipped. For more information, see Advanced Configuration Properties.

  A new AAC Advanced Configuration parameter **`authsvc.stateMgmt.cookieless`** is added. When the parameter is set to `true`, the Authentication-based and Content-based access modules no longer require client side cookies to be set to perform authentication flows. For more information, see Advanced Configuration Properties.

  Read-only and Sensitive API Protection token attributes are now handled differently. For more information on the new advanced configuration parameter **`oauth.useLegacyAttributes`**, see Advanced Configuration Properties.

- JavaScript Audit Logging

  JavaScript Mapping Rules can now audit events with **`IDMappingExtUtils.logAuditEvent`** (String username, String message, boolean result). For more information, see Auditing from Mapping Rules.

- QR Code Authentication Mechanism

  You can configure the QR code authentication mechanism to scan a generated QR code to successfully authenticate as an alternative-to-password authentication technology. There are two new pre-defined policies that can be used to configure the QR code authentication mechanism- **initiate** and **response**. For more information, see Configuring a QR Code authentication mechanism

- Mobile Multi-Factor (MMFA) Authenticator Mechanism

  The MMFA authenticator can now be figured to:

  – Provide a push notification message that is separate from the pending transaction description. For more information, see Configuring a Mobile Multi-Factor Authentication (MMFA) Authenticator Mechansim
  – Provide a list of attributes that is used for server side signature validation. For more information, see Authentication policy parameters and credentials

- Updating and Deleting OIDC Dynamic Clients

  Dynamic clients can now be updated and deleted. This provides additional capability, such as resetting the `client_secret`. For more information, see:

  – Updating a dynamic client
  – Deleting a dynamic client

- Cloud Identity Verify (CIV) API Integration

The following updates are made to the CIV StrongAuthenticaion/API Integration:

- IBM Verify enrollment through CIV
- Just-in-time enrollment
- Updated the Cloud Identity Server Connection type to allow administrators to override the Cloud Identity endpoint paths
- Redesign authentication flow pages
- Added functions to mapping rules to enable administrators to easily modify usernames

For more information, see Cloud Identity API Integration.

- Mobile Multi-Factor Authentication Infomap Usability

  Additional context keys are made available in the Infomap. For more information, see Context attributes

- **`isamcfg`** REST API

  The ISAM command line utility for configuring Advanced Access Control with a reverse proxy "isam aac config" is now deprecated. Use the Local Management Interface or REST API documented on the box to configure an instance for use with the authentication service and context based access. For more information, see Configuring advanced access control authentication on a reverse proxy.

- Support for MaxMind Geolocation database v2

  The GeoLocation policy information point is updated to allow the use of both GeoIP and GeoIP2. The latest release of the GeoIP Database can now be used to enforce access control policies by using the predefined geoCity, geoCountryCode, geoLocation, and geoRegion attributes. For more information, see Updating location attributes

- `apiauthsvc` headers

  The Accept header requirements for `apiauthsvc` have been relaxed. The request now succeed with no Accept header, `application/json` or `*/*`.

- Macro HTML encoding

  New sps.page configuration options for HTML encoding of macros have been added. For more information, see Advanced Configuration Properties.

- SCIM support for LDAP failover

  SCIM calls, when using the ISAM Runtime type server connection, now automatically fail over between configured LDAP replicas. This is controlled by the 'replica' configuration entry within the `[ldap] stanza` in the `ldap.conf file`.

- SCIM performance improvements

  SCIM calls to retrieve or update resources have significantly improved response times for direct LDAP and ISAM Runtime type server connections.

- SCIM support for multi-valued and operational attributes

  SCIM User Profile Attribute Mappings now correctly handle multi-valued and operational attributes from the underlying user registry.

- SCIM support for working with suffixes

  SCIM calls using the ISAM Runtime type server connection now honor the 'ignore-suffix' configuration entry within the `[ldap] stanza` in the `ldap.conf file`. This entry controls the defined suffixes to omit from searches which helps improve the user and group information searches.

  SCIM calls for both the direct LDAP and ISAM Runtime type server connections now allow the suffix under which resources are created to be specified using the 'registrySuffix' data in the request body. For example, `"registrySuffix":"cn=user,o=ibm,c=us"`.

Federation

- Improvements to the Distributed Session Cache Configuration.

  By default, the local cache of the Distributed Session Cache sessions within the Advanced Access Control or Federation runtime is now disabled. You can enable it by using the new advanced configuration parameter, **distributedSessionCache.localCacheEnabled**. For more information, see Advanced Configuration Properties.

- Capability to add samlp:Extensions to SAML messages

  SAML Message extensions can now be included in SAML messages. For more information see the following topics:

  – SAML 2.0 Service Provider Worksheet
  – SAML 2.0 Identity Provider Worksheet
  – SAML 2.0 Service Provider Partner Worksheet
  – SAML 2.0 Identity Provider Partner Worksheet

- Scalability improvements on the number of federations and partners

  Configuration and runtime operations of the federation module are improved to handle larger numbers of federations and partners.

- New Advanced Configuration Parameter

  A new advanced configuration parameter, `sps.illegalUrlSubstrings` is added. Single sign-on service stops processing an incoming HTTP request if the request query parameters contain any of the strings defined in this parameter. For more information, see Advanced Configuration Properties.

- Support for LDAP alias service database

  SAML 2.0 persistent nameid flows have the option to store alias information in high-volume runtime database by default or in an LDAP alias database. For more information, see Alias Service.

Chapter 3. Product requirements

You can view Software Product Compatibility Reports that list the system requirements and appliance specifications for the product.

The reports provide current information about hardware and software support and requirements for IBM Security Access Manager.

- System requirements for hardware appliance:
  - Prerequisite software, including supported databases, user registries, and browsers
  - Appliance specifications such as disk size, memory, network ports, physical characteristics, and electrical and environmental parameters
- System requirements for the virtual appliance:
  - Supported hypervisors, databases, user registries, and browsers
  - Disk space and memory requirements for virtual images

Note: IBM Security Access Manager versions 8.0 and 9.0 are not available as a software distribution. They are available only as a virtual or hardware-based appliance.

To view the reports, see Software Product Compatibility Reports.

You can also view the specifications of the hardware and virtual appliance in the following Technotes:

- Hardware appliance specifications: http://www-01.ibm.com/support/docview.wss?uid=swg22011035
- Virtual appliance specifications: http://www-01.ibm.com/support/docview.wss?uid=swg22011036

WebSEAL client support

When acting as a reverse proxy, WebSEAL generally supports clients that conform to the HTTP 1.1 standard as defined by RFC 2616 and the HTTP/2 standard as defined by RFC 7540. The preceding statement is not a comprehensive statement of support. WebSEAL relies on a number of client characteristics that are either not defined or are loosely defined by RFC 2616 and RFC 7540. Examples of such characteristics include, but are not limited to:

- Cookie management
- SSL support
- Concurrency of multiple connections

Widely used browsers such as Firefox, Chrome, Safari, and Internet Explorer support such characteristics during typical use.

The extension of browser capabilities that modify these characteristics can, however, introduce compatibility problems with WebSEAL. The same is true of other client types, such as mobile applications or rich clients. Compatibility complications that cannot be resolved through modification of the environment or configuration of the WebSEAL product are not supported.

Chapter 4. Documentation for an activation level

IBM Security Access Manager uses the listed activation levels, depending on the modules you purchase. Use the information in the tables to determine which topics to start with in the documentation.

Access Manager Supporting Components

No activation key is required for these functions.

Table 1. Access Manager Supporting Components functions and topic links

Function	Topic
Appliance Management: Local management interface	Appliance Management
Appliance Management: REST APIs	REST API documentation
Policy Server	Policy server administration tasks
Embedded LDAP server	Embedded LDAP server management
Authorization Server	Authorization servers

Access Manager Platform

An activation key is required for these functions.

Table 2. Access Manager Platform functions and topic links

Function	Topic
Web Reverse Proxy	Web Reverse Proxy configuration and Web Reverse Proxy administration
Layer 4/7 load balancer	Load balancing layer
X-Force threat protection	Configuring web application firewall
Distributed session cache	Distribued session cache

Advanced Access Control Module

This module is an add-on feature that requires an activation key.

Table 3. Advanced Access Control functions and topic links

Function	Topic
Authentication	Authentication
OAuth 2.0 API protection	Configuring API protection
Context-based access	Overview of context-based access
Device fingerprinting	Device fingerprints
Device registration	Consent-based device registration
HOTP and TOTP Key Manager	Managing OTP secret keys
Fine-grained authorization/XACML 2.0	Access control policies

Table 3. Advanced Access Control functions and topic links (continued)

Function	Topic
Runtime security services	Runtime security services external authorization service
Policy distribution (Policy administration point)	Risk management overview

Federation Module

This module is an add-on feature that requires an activation key.

Table 4. Federation functions and topic links

Function	Topic
SAML 2.0 Federations	SAML 2.0 federations
Open ID Connect Federations	OpenID Connect federations
Module chains	Manage module chains and Configuring STS modules

Related information

Product activations overview

Chapter 5. Secure deployment considerations

When you deploy the IBM Security Access Manager appliance, consider the following points.

- The Security Access Manager embedded user registry should only be used in the following scenarios:
  - Proof of Technology deployments
  - Deployments with a low number of Security Access Manager users (< 5000)
  - When using federated directories with the Security Access Manager basic user feature
- Choose the suitable Security Access Manager user authentication mode for your environment.
  - Use basic user for all scenarios unless GSO lock-box, user based ACLs, or account-valid/password-valid features are required.
  - Only use the full user model if basic user is not suitable. Basic user only supports minimal mode.
- The appliance has management and application interfaces. Network separation between the management and application interfaces must be maintained.
- Any Security Access Manager web reverse proxies that are hosted in the corporate DMZ network zone should be configured as restricted nodes.
- The Security Access Manager appliance that hosts the Policy Server component should be hosted in a secure network zone and not exposed to the internet.
- If the embedded user registry is used, it should be hosted on the same appliance as the Security Access Manager Policy Server in a secure network zone. The embedded user registry port (636) should not be routable from the internet.
- Security Access Manager clustering is recommended to provide a highly available solution. Two Security Access Manager appliances performing the primary and secondary roles respectively should be used. These should be hosted in the secure network zone with Security Access Manager runtime replication enabled.
- If advanced authentication/authorization is required, the Security Access Manager authentication service in the Advanced Access Control (AAC) component should be used. This should be hosted on the Security Access Manager primary and secondary appliances in the secure network zone. This service should not be routable from the internet.
- Second factor or multi-factor authentication should be considered to increase assurance of user identity.
- Enable Network Time Protocol (NTP) on all appliances to synchronize the time correctly. This is to ensure that the appliance works correctly with distributed components.
- Do not use self-signed certificates for any public facing services. Always obtain certificates issued by an appropriate certificate authority.
- All non-TLS communication should be disabled:
  - Only use port 636 for LDAP communication.
  - Only use HTTPS 443 application interfaces.
  - Only use TLS for junction communication.
- Enable the Security Access Manager Web Application Firewall (WAF) feature on all appliances hosting the Security Access Manager reverse proxy.

- Session affinity should be enabled between all Security Access Manager components for performance and scalability reasons.
- The Security Access Manager Distributed Session Cache (DSC) or failover cookie should be used to provide a highly available solution across multiple reverse proxy instances.
- If the DSC is deployed, it should be hosted in the secure network zone.
- Configure the reverse proxy cookie jar feature to prevent application cookies from being returned to clients unnecessarily.
- Connection pooling for junctions should be enabled to optimize performance of the solution. This capability is disabled by default.
- FIPS should be enabled if appropriate.
- Enable these security headers in the reverse proxy configuration:
  - **strict-transport-security**
  - **content-security-policy**
- Minimize access to unauthenticated resources using standard Security Access Manager ACL policy.
- Host the Security Access Manager runtime database on an external Database. This database is used for federation and/or AAC features. The runtime database should be hosted in a secure network zone and should not be routable from the internet.
- Use a highly available solution for the external Security Access Manager runtime database. This service is critical to Security Access Manager operation.
- Best practice is to use the Security Access Manager REST APIs for automated deployment to allow:
  - Rapid recovery
  - Consistent and repeatable deployment configuration
- Don't use Basic Authentication (BA) for authentication to Security Access Manager REST APIs when automating deployment and management of the Security Access Manager appliance. Certificate authentication should be used.
- Standard network security guidelines should be applied. Network access and administrative credentials to the appliance should only be available to authorized administrators on appropriate networks.
- Minimize on-board storage of logs by configuring remote syslog to store log and audit archives in a protected network zone. A separate logging server/service should be used to store logs.
- An appropriate patch process should be implemented to:
  - Subscribe to, and monitor IBM support site for Security Access Manager appliance patches
  - Apply all patches promptly when released

Chapter 6. Upgrading to the current version

Complete this task if you are upgrading an existing Access Manager for Web, Access Manager for Mobile, or Access Manager installation to the current version.

Before you begin

Important:

When you upgrade a cluster, upgrade the primary master first and do not upgrade the remaining cluster nodes until the primary master finishes upgrading and is operational.

In the case where one of the non-primary nodes is upgraded when the primary master is not available, upon upgrade completion the node will be in a non-operational state. To rectify this problem, remove the non-operational node from the cluster and then re-add it. This approach will ensure that the configuration and database replication returns to a working state.

If you are installing the virtual appliance for the first time, download the `.iso` image and follow the installation instructions in the IBM Security Access Manager Virtual Appliance Quick Start Guide.

Review the following tasks and complete the tasks that are appropriate to your environment:

Clear the browser cache
: As part of the upgrade process, clear your browser cache to reduce the likelihood of encountering issues with cached items.

USB drive for an update
: If you use a USB drive for an update, it must be formatted with a FAT file system.

Risk engine reports
: Any risk engine reports that you generated before you begin the upgrade task are not preserved. Export copies of the risk reports and save them locally by completing the following steps:

  1. Log in to the local management interface.
  2. Click **Monitor Analysis and Diagnostics** > **Application Log Files**.
  3. Expand **access_control** and select the risk reports to export.
  4. Click **Export** and save the files.

Database failover in a cluster
: For information about how the upgrade affects database failover in a cluster, see the Database failover capabilities vary during a cluster upgrade section in Advanced Access Control known issues and solutions.

Procedure

Choose one of the following upgrade methods and complete the steps:

Use the online update server.

1. Meet the following conditions:

- A valid license is installed on the appliance.
- The appliance has network connectivity to the online update server.

2. Log in to the local management interface. If you are upgrading a cluster, log in to the local management interface of the primary master first.
3. Select **Manage System Settings** > **Updates and Licensing** > **Available Updates**.
4. Click **Refresh**.
5. Select the firmware update.
6. Click **Install**. The firmware update might take a long time to complete, depending on the bandwidth that is available to the appliance. After the update is successfully applied, the appliance automatically restarts.
7. If you use any external databases, download the **dbupdate9.zip** file from **File Downloads** area of the appliance and upgrade the external databases.
8. If you are upgrading a cluster, complete the following steps:
   a. Repeat steps 2 through 6 on each node in the cluster starting with the secondary master.

      Note: If you use internal databases, do not subsequently reboot the primary master until the secondary master has been upgraded.
   b. Wait for the cluster to synchronize. The firmware for each appliance in the cluster is now upgraded and the cluster is operational.

   Note: Although the secondary master remains present and the embedded runtime database fails over to the secondary master when the primary master is down during the migration, you cannot avoid down time by leveraging this failover mechanism. This is due to the fact that the database changes made to the secondary master while the primary master is being migrated will likely be discarded and replaced by the upgraded databases from the primary master after it begins operating again after the migration.

Use the local management interface for a single appliance *not* in a cluster.

1. Download the `.pkg` file.
2. Log in to the local management interface.
3. Select **Manage System Settings** > **Updates and Licensing** > **Available Updates**.
4. Click **Upload**. The New Update window opens.
5. Click **Select Update**.
6. Browse to the `.pkg` file.
7. Click **Open**.
8. Click **Save Configuration**. The upload process might take several minutes.
9. Select the new firmware and click **Install**. The installation of the new firmware takes a few minutes. After the update is successfully applied, the appliance restarts automatically.

Use the local management interface for a cluster of appliances.

1. Download the `.pkg` file.
2. Log in to the local management interface of the primary master.

3. Upload and install the firmware `.pkg` file on the primary master. This step includes the automatic restart of the appliance. If you use internal databases, do not subsequently reboot the primary master until the secondary master has been upgraded.
4. If you use any external databases, download the `dbupdate9.zip` file from **File Downloads** area of the primary master and upgrade the external databases.
5. Upload and install the firmware `.pkg` file on each node in the cluster starting with the secondary master if present.
6. Wait for the cluster to synchronize. The firmware for each node in the cluster is now upgraded and the cluster is operational.

Note: Although the secondary master remains present and the embedded runtime database fails over to the secondary master when the primary master is down during the migration, you cannot avoid down time by leveraging this failover mechanism. This is due to the fact that the database changes made to the secondary master while the primary master is being migrated will likely be discarded and replaced by the upgraded databases from the primary master after it begins operating again after the migration.

Use a USB drive. (Only for upgrading a hardware appliance.)

1. Download the `.pkg` file.
2. Copy the firmware update from the `.pkg` file to a USB flash drive.
3. Insert the USB flash drive into the hardware appliance.
4. Log in to the appliance console as `admin` or use Secure Shell.
5. Type `updates` and press Enter.
6. Type `install` and press Enter.
7. Select the following options:
   a. Type 1 for a firmware update.
   b. Type 1 to install the update from a USB drive.
   c. Type `YES` to confirm that the USB drive is plugged into the appliance.
   d. Type the index number to select the appliance firmware from the list.
   e. Type `YES` to confirm the update and start the update process.

   Note: The firmware update takes a few minutes to complete and the appliance automatically restarts.

What to do next

- If you are using an external database to store the runtime or configuration data, you also need to update the database schema. This can be achieved by downloading the database update utility from the appliance and running this utility against the external database. For more details, see Upgrading external databases with the **dbupdate** tool (for appliance at version 9.0.0.0 and later).
- If you are upgrading an existing appliance, your Access Manager Platform is ready to use.
- If you are upgrading an existing Access Manager for Mobile appliance or Advanced Access Control module to the current version, continue with the Upgrading configuration instructions.

- If you are upgrading an existing Federation module to the current version, continue with the Upgrading configuration instructions.

Chapter 7. APARs fixed in this version

Several APARs were fixed with this version of the product.

For the latest list, see APARs fixed by IBM Security Access Manager version 9.0.6.

Chapter 8. Compatibility with earlier versions of the product

IBM Security Access Manager V9.0.* is compatible with previous versions of Security Access Manager for Web, Tivoli Access Manager for e-business, and Security Access Manager for Mobile.

The Version 9.0.* policy server can communicate with some previous versions of Security Access Manager for Web, Tivoli Access Manager for e-business, and Security Access Manager for Mobile. The following compatibility with earlier versions is supported:

- Policy server compatibility with servers in prior versions
- Compatibility with single sign-on targets
- Limited compatibility with earlier versions for session management

Policy server compatibility with servers in prior versions

The Version 9.0.* policy server is compatible with prior releases of other servers, as specified in the following table.

Table 5. Compatibility with earlier versions of servers

Compatible servers	Compatible versions
WebSEAL server	• Tivoli Access Manager for e-business, Version 6.1.1 and newer • Security Access Manager for Web, Version 7.0 and newer
Authorization server	
Web plug-ins	

Version 9.0.* interfaces are compatible with prior releases of the product, as specified in the following table.

Table 6. Compatibility with earlier versions of interfaces

Version 9.0.* interfaces	Compatible versions
C Administration	• Tivoli Access Manager for e-business, Version 6.1 and newer • Security Access Manager for Web, Version 7.0 and newer
Java Administration	
External Authentication	
C Authorization	
Java Authorization	
Registry Direct	• Tivoli Access Manager for e-business, Version 6.1.1 and newer • Security Access Manager for Web, Version 7.0 and newer

Compatibility with single sign-on targets

IBM Security Access Manager maintains compatibility with earlier versions for all single sign-on information that is sent over HTTP to applications behind WebSEAL junctions. Applications that are written to use single sign-on information that is supplied by previous versions of the product can use the same information that is provided by Version 9.0.*.

This compatibility applies to both custom applications and IBM applications such as the Trust Association Interceptor. The Trust Association interface is a service provider API that enables the integration of third-party security service (for example, a reverse proxy) with WebSphere Application Server. Security Access Manager, version 9.0.*, is compatible with all versions of the Trust Association Interceptor.

Limited compatibility with earlier versions of session management

IBM Security Access Manager for Web Version 8.0 introduced the Distributed Session Cache. This component replaces the Session Management Server that was provided in previous releases of the product.

The following limitations apply to deployments that combine IBM Security Access Manager, Version 9.0.* with prior versions, such as IBM Security Access Manager for Web, Version 7.0.0:

- You cannot use both the Distributed Session Cache and the Session Management Server in the same deployment.
- The IBM Security Access Manager Version 9.0.* WebSEAL server cannot communicate with the Session Management Server.
- IBM Security Access Manager for Web Version 7.0.* WebSEAL server can communicate with the Distributed Session Cache in Version 9.0, but only if IBM Security Access Manager for Web Fix Pack 2 (Version 7.0.0.2) or newer is applied.

Chapter 9. Documentation updates for known limitations

You can view the known software limitations, problems, and workarounds on the IBM® Security Access Manager Support site.

The Support site describes not only the limitations and problems that exist when the product is released, but also any additional items that are found after product release. As limitations and problems are discovered and resolved, the IBM Software Support team updates the online knowledge base. By searching the knowledge base, you can find workarounds or solutions to problems that you experience.

Also, check the Troubleshooting topics.

Known limitations for Security Access Manager

A system error is displayed briefly when the Mozilla Firefox browser is refreshed.

When you use the Mozilla Firefox browser to access the local management interface, sometimes a system error is displayed briefly during a browser refresh.

This error is displayed because the browser refresh causes an XMLHttpRequest (XHR) request to be canceled before the request finishes. The error does not indicate impact to normal operations and can be ignored.

Unable to remove local users or groups from authorization roles with Mozilla Firefox on Mac OS X.

When you use the local management interface through a Mozilla Firefox browser version on a Mac OS X system, you might not be able to remove a user or group from an authorization role.

On the Management Authorization page of the local management interface, when you click **Edit**, the Edit Local Members window is displayed. To remove a user or group, normally you uncheck the check box for that user or group and then click **OK** to save the changes. However, if you use Firefox on Mac OS X to complete such operation, the browser does not properly recognize the change and does not display any error messages. The user or group list remains unchanged after you click **OK**.

To avoid such issue on Mac OS X, you have two options:

- Use a different browser to access the local management interface.
- Use the REST API. See the REST API documentation and browse to **Manage: System Settings** > **System Settings** > **Management Authorization** > **Updating an authorization role**.

Lower throughput observed with certificate revocation list enabled

Enabling certificate revocation list (CRL) validation might result in a lower throughput from the system. If your certificate does not have a CRL, you might want to disable CRL checking by using the advanced configuration parameter **`kess.crlEnabled`**. Alternatively, you might want to reduce the frequency of CRL checking by using the advanced configuration parameter **`kess.crlInterval`**.

Client certificate authentication for federated directories is not supported for UsernameTokenSTSModule

When you configure a federated directory, do not select a client certificate.

In rare circumstances, an OAuth access token validation might fail.

These instances have been observed very shortly after a restart of the Advanced Access Control runtime server. The symptoms and conditions include:

1. Restart the Advanced Access Control runtime server.
2. Execute an OAuth flow, such as the Resource Owner Password Credential flow, to obtain a valid access and refresh token pair.
3. Attempt to use the access token to access a resource that is protected by the API Definition associated with the OAuth client that has been granted the access token.

Step 3 has been observed to fail on some rare occasions. The cause is due to delayed restart initialization of some internal Advanced Access Control runtime components. Normal successful processing has been observed when the request for the protected resource in step 3 is resubmitted.

Junction type for Security Access Manager Oracle PeopleSoft PeopleTools integration

When you access the PeopleSoft Workcenter Dashboard via WebSEAL using a standard junction type, the dashboard is not displayed correctly. The browser issues a message "Only secure content is displayed" with a button "Show all content". When this button is clicked, an Oracle authentication login panel is displayed.

Note that the full URI of the server is used instead of just the junction name. Because the content contains an absolute address that WebSEAL cannot filter when a standard junction type is used, for example:

```
<DIV id="ptasjs1"> http://hostaddress/cs/path/cache
/PT_PORTAL_UTIL_JS_MIN_1.js</DIV>
```

In this case, a virtual host junction type must be adopted to negate the limitations associated with the use of standard junction script filtering.

Tooltips display issue

Tooltips might not display if you use the keyboard (for example, the Tab key) to navigate to a field. Tooltips are displayed properly when you use a mouse to navigate to the field.

Creating PIP resource when the server connection for database and LDAP is not available returns the wrong response.

For example, when you use the following command:

```
curl -k -b whatigot -s -S --ciphers "DES-CBC3-SHA" -X "POST" -H
"Accept:application/json" -H "Content-Type: application/json"
--data-binary "{\"name\":\"tldap1234\",\"description\":\"\"\
"attributes\":[{\"name\":\"trusteer.pinpoint.csid\",\"selector\":\
"wrongtestLdap\"}]\"type\":\"LDAP\",\"predefined\":false,\
"properties\":[{\"datatype\":\"String\",\"readOnly\":false,\
"sensitive\":false,\"value\":\"objectclass=abc\",\"key\":\
"searchBaseDN\"},{\"datatype\":\"String\",\"readOnly\":false,\
"sensitive\":false,\"value\":\"cn=*\",\"key\":\"searchFilter\"},{\
"datatype\":\"String\",\"readOnly\":false,\"sensitive\":false,\
"value\":\"0cdebb0c-49d9-4179-a47a-52f759a4ff57\",\"key\":\
```

```
"dataSource\"}]}" --user admin:admin -D whatigot "https://
{appliance_host}/iam/access/v8/pips/"
```

The expected response is as follows:

```
HTTP/1.1 400 Bad Request
```

But the actual response is as follows:

```
HTTP/1.1 201 Created
```

The error message "illegal character" when you modify an SSO rule is always displayed in English.

The error message "illegal character" is always displayed in English no matter which locale your browser uses.

Audit events cannot be sent to the remote syslog server if certain information is not provided.

If you choose to send the audit events to a remote machine, you must specify the correct details on the Audit Configuration page for host, port, protocol, and certificates. Otherwise, the audit events cannot be sent to the remote machine.

Attribute sources that are being used by a federation or partner is deletable.

Users can accidentally delete attribute sources that are in use by a federation or partner. Such operation causes errors to the federation. You must ensure that an attribute source is not in use before you delete it.

Federation Module: The email address name ID format requires a mapping rule

If you use an email address name ID format in a SAML 2.0 federation, you must set the type of STS Universal User attribute, whose name is "name", to:

```
"urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
```

You can accomplish this by using a mapping rule. Following is an example:

```
// Get the current principal name.
var principalName = stsuu.getPrincipalName();
// Set the type of principal name attribute "name" to
//"urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress".
stsuu.addPrincipalAttribute(new Attribute("name",
"urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress", principalName));
```

Personal certificates are not included in the list of selections when you choose certificates to use for encryption or signature validation with the SAML 2.0 partner management GUI

If you use the local management interface to choose certificates to be used for encryption or signature validation, only signer certificates are available for selection. Personal certificates are not included in the list of selections. A work-around is to use the REST API for such operations.

Federation module: The RSA-OAEP key encryption algorithm is not supported with HSM keys

IBM Security Access Manager does not support decryption of SAML 2.0 messages using the RSA Optional Asymmetric Encryption Padding (RSA-OAEP) key transport algorithm with Hardware Security Module (HSM) keys. The RSA-OAEP algorithm is supported with software (non-HSM) keys. For more information on RSA-OAEP, see http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p.

The upgrade from Security Access Manager 8.0, 8.0.0.1, and 8.0.0.2 does not correctly migrate the authentication module policies for Security Access Manager

for Mobile.

The work-around is to create the default set of authentication policies with the local management interface or REST API.

The following link creates a customized query of the live Support knowledge base for items specific to IBM® Security Access Manager, Version 9.0, and its fix packs.

IBM Security Access Manager technical documents

You can also create your own search query on the IBM Support Portal. For example:

1. Go to the IBM Support Portal:http://www.ibm.com/support/entry/portal/support
2. In the "Search support and downloads" field, enter: `Access Manager`.

Chapter 10. Security Access Manager appliance FRU/CRU documentation

Read the IBM Security Access Manager Field Replacement Unit (FRU) parts and Customer Replacement Unit (CRU) parts documentation before you replace the relevant parts.

Disk Drive Assembly Replacement Instructions

This document helps you to complete the following tasks:

- Remove a failed disk drive and replace it with a new disk drive
- Verify that the new disk drive is working correctly

Important: Before you proceed with these instructions, review the *IBM Systems Safety Notices* provided in the *IBM Media Terms and Conditions CD* that is included with your appliance model.

Note: The illustrations in this document might differ slightly from your appliance model.

Supported appliances

The instructions in this document support IBM Security Access Manager (IBM Part Number: 01LK905).

Replacing a storage drive assembly

Before you begin

You must have a replacement storage drive assembly before you remove and replace the failed assembly.

About this task

Identifying the storage drive assembly

The front panel of the appliance contains the storage drive assembly, as highlighted in yellow in the following figure:

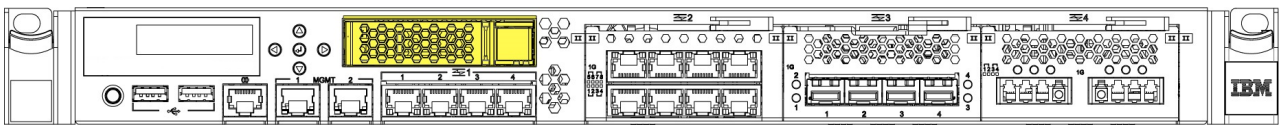


Figure 1. Location of the storage drive assembly on the front of the appliance

Procedure

1. Shut down the appliance by using the local management interface (LMI) or the command-line interface (CLI).
2. Unplug all of the power cords that are attached to the appliance.

3. Press the release button on the right side of the storage drive assembly to release the assembly lock.
4. Pull the drive handle lever to the left to pull the storage drive assembly from the drive bay, as shown in the following figure:

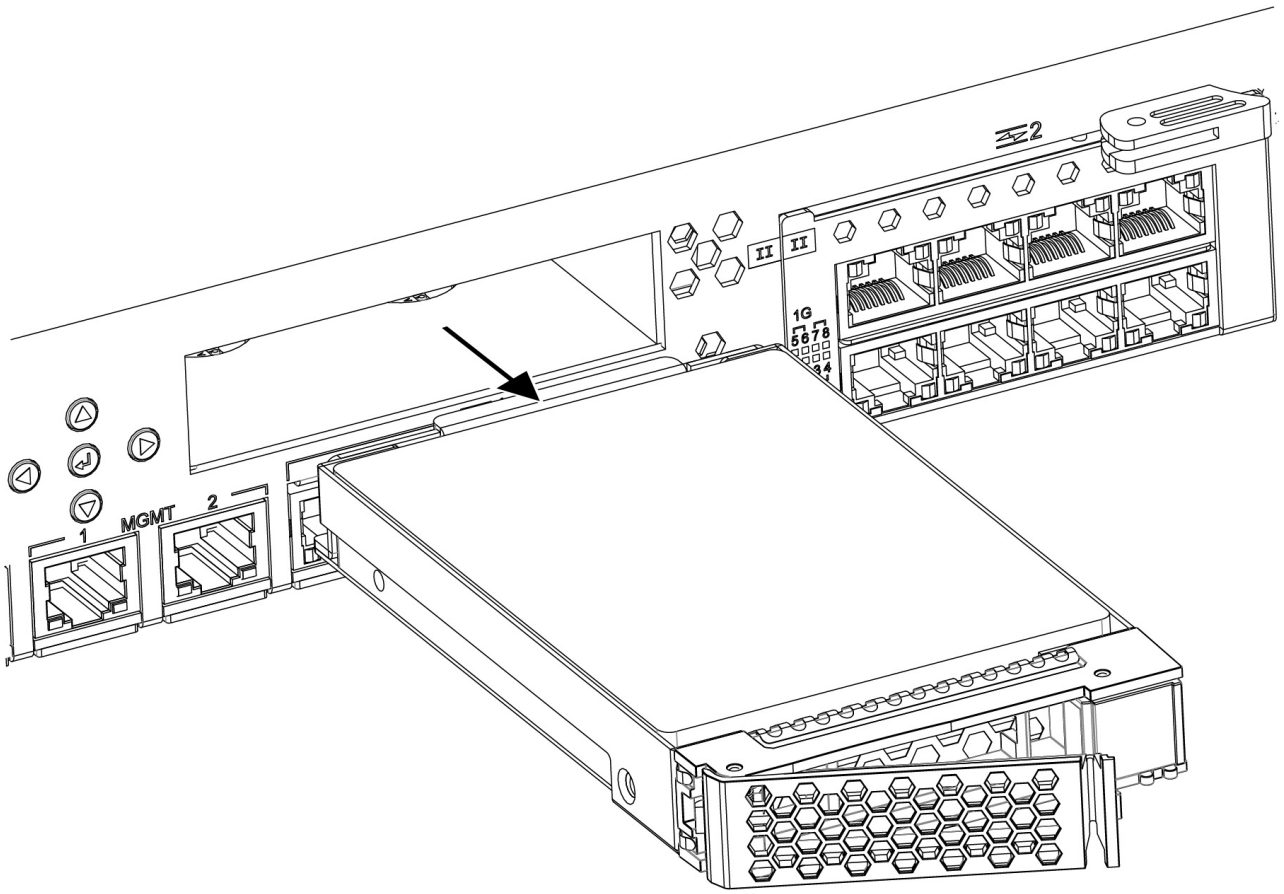


Figure 2. Removing the storage drive assembly from the drive bay

5. Place the new storage drive assembly in the drive bay.
6. Push the storage drive assembly into the drive bay until the lever locks into place.

What to do next

Turn on the appliance, and then reimage it.

Important: You must reimage the appliance after you replace the storage drive. If you do not reimage the appliance, the appliance can become inoperable.

Fan Assembly Replacement Instructions

Use these instructions to complete the following tasks:

- Remove a failed fan module from the appliance and replace it with a new one
- Verify that the new fan module is working correctly

Important: Before you proceed with these instructions, review the *IBM Systems Safety Notices* provided in the *IBM Media Terms and Conditions CD* that is included with your appliance model.

Note: The illustrations in this document might differ slightly from your appliance model.

Supported appliances

The instructions in this document support IBM Security Access Manager (IBM Part Number: 01LK905).

Replacing a fan assembly

Before you begin

You must have the applicable replacement fan assembly before you can remove and replace the failed fan assembly.

About this task

Identifying a failed fan assembly

The back panel of the appliance contains four user-accessible fan modules, as highlighted in yellow in the following figure:

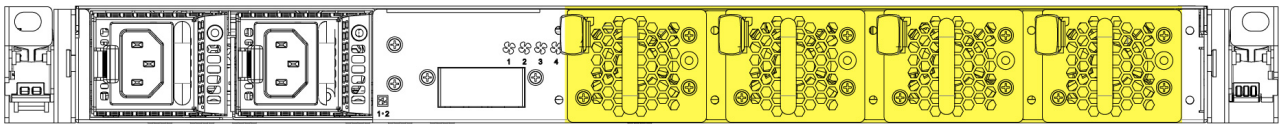


Figure 3. Location of the fan modules on the back of the appliance

During normal operation, the LED for the fan module is not illuminated. If one of the fan modules experiences a failure, the LED for the failed fan module is illuminated in amber.

Procedure

1. Pinch the orange retention clip on the fan module to release the fan assembly from the chassis.
2. Pull the fan assembly out of the chassis, as shown in the following figure:

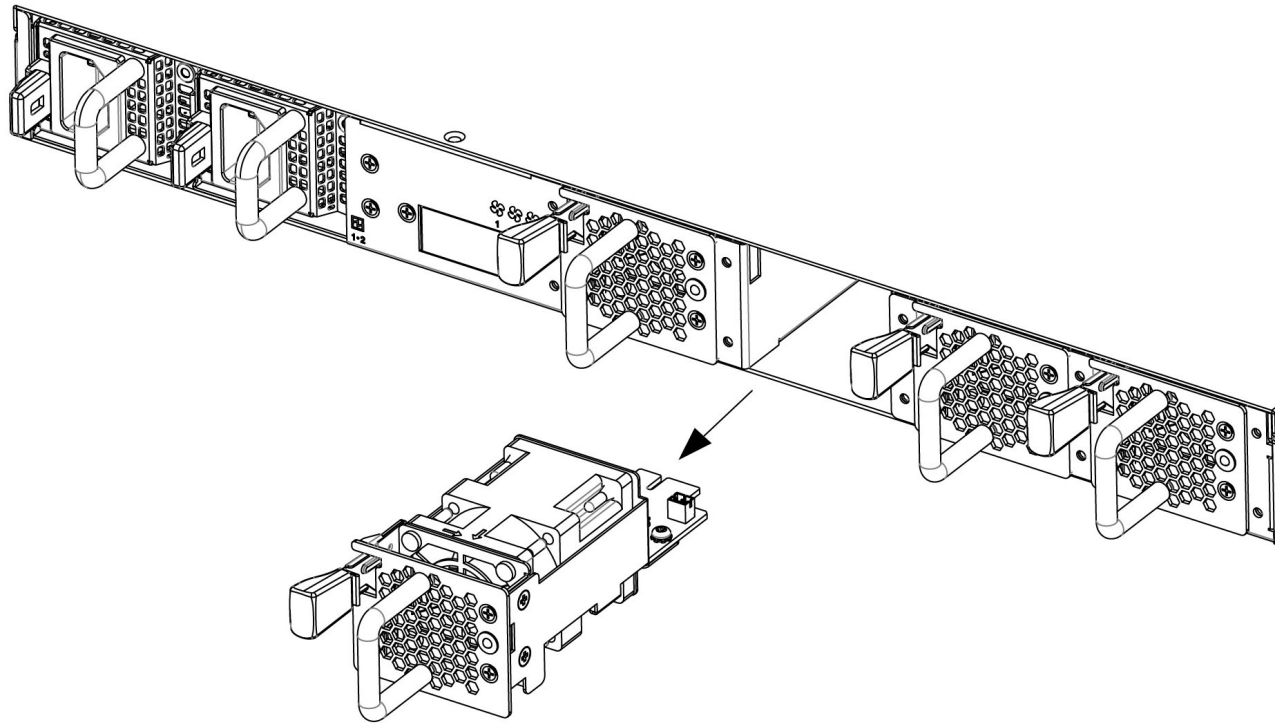


Figure 4. Removing a fan assembly from the back of the appliance

3. Slide the replacement fan assembly into the fan assembly bay. Make sure the fan assembly is secured in the chassis.

Results

The fan module LED is not illuminated in amber and the fan starts to circulate air.

Network Interface Module Replacement Instructions

This document helps you to complete the following tasks:

- Remove a failed network interface module and replace it with a new network interface module
- Verify that the replacement network interface module is working correctly

Best practice: Replace a failed network interface module as soon as possible.

Important: Before you proceed with these instructions, review the *IBM Systems Safety Notices* provided in the *IBM Media Terms and Conditions CD* that is included with your appliance model.

Note: The illustrations in this document might differ slightly from your appliance model.

Supported appliances

The instructions in this document support IBM Security Access Manager (IBM Part Number: 01LK905).

Replacing a failed network interface module

About this task

Identifying the network interface module

The front panel of the appliance contains the network interface modules, as highlighted in yellow in the following figure:

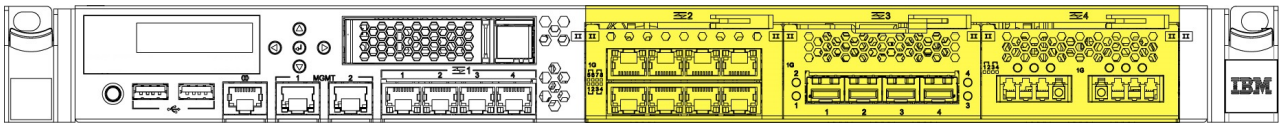


Figure 5. Location of the network interface modules on the front of the appliance

Procedure

1. Turn off the appliance by using the local management interface (LMI) or the command-line interface (CLI).
2. Unplug all of the power cords that are attached to the appliance.
3. Grasp the blue latch on the front of the appliance and pull it toward you.
4. Pull the lever on the failed module toward you, and then pull module from the chassis, as shown in the following figure:

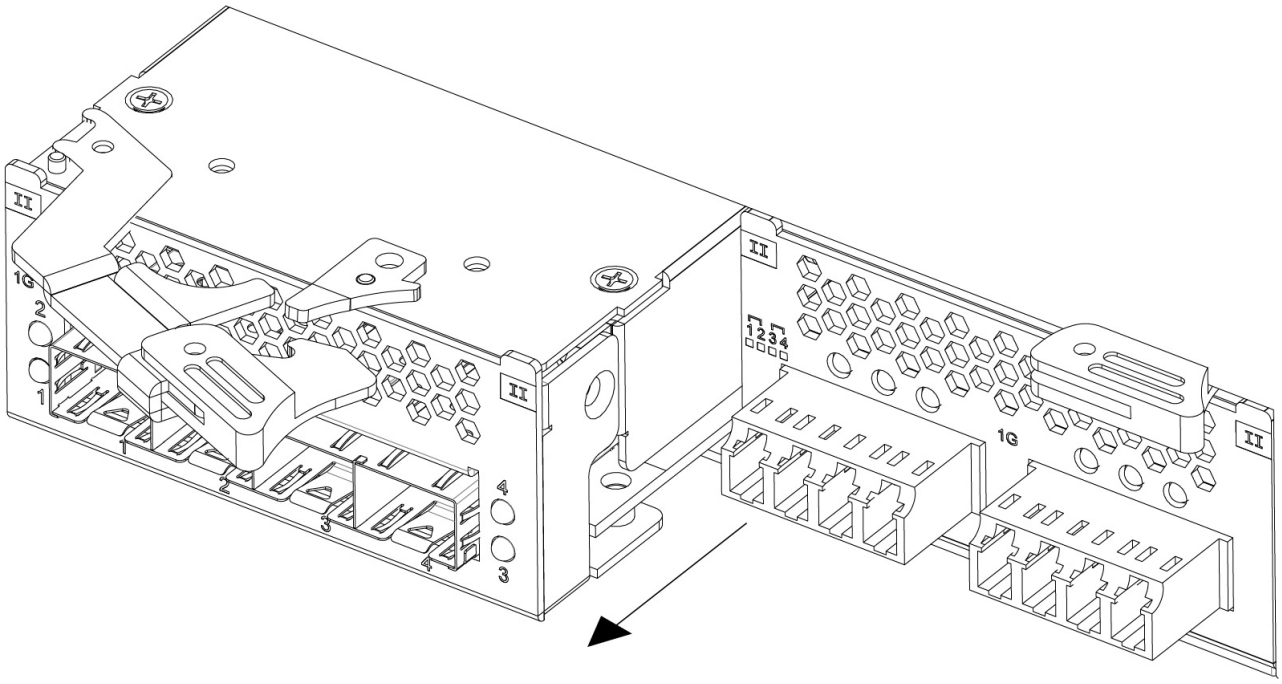


Figure 6. Removing a network interface module from the front of the appliance

5. Set aside the failed module.

Attention: As you unpack the replacement module, make sure that you do not touch the gold connectors on the back of the module, and do not let the gold connectors come in contact with the packing material. In addition, do not let these gold connectors touch the appliance while you are inserting the replacement module into the chassis. The gold connectors are extremely fragile and can be damaged if they touch anything.

6. Unpack the replacement module.
7. Carefully align the replacement module with the chassis, and then push the module into the chassis until the module is in place.
8. Push the blue latch on the front of appliance into place.
9. Plug in all of the power cords that are attached to the appliance.
10. Turn on the appliance by pressing the power button on the front.
11. Verify that the LCD panel on the front of the appliance is illuminated.

What to do next

Check whether the new module is working correctly by logging in to the appliance LMI and verifying that the new module was recognized by the appliance.

Power Supply Replacement Instructions

This document helps you to complete the following tasks:

- Identify a failed power supply
- Remove the failed power supply and replace it with a new power supply
- Verify that the replacement power supply is working correctly

Best practice: Replace a failed power supply as soon as possible.

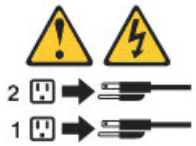
Important: Before you proceed with these instructions, review the *IBM Systems Safety Notices* provided in the *IBM Media Terms and Conditions CD* that is included with your appliance model.

Note: The illustrations in this document might differ slightly from your appliance model.

Supported appliances

The instructions in this document support IBM Security Access Manager (IBM Part Number: 01LK905).

CAUTION:
The power control button on the device and the power switch on the power supply do not turn off the electrical current supplied to the device. The device also might have more than one power cord. To remove all current from the device, ensure that all power cords are disconnected from the power source.



CAUTION:
Never remove the cover on a power supply or any part that has the following label attached.

Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, contact a service technician.

Identifying a failed power supply

The power supply unit uses an LED that indicates whether the unit is working as expected. The location of the LED is shown in the following figure:

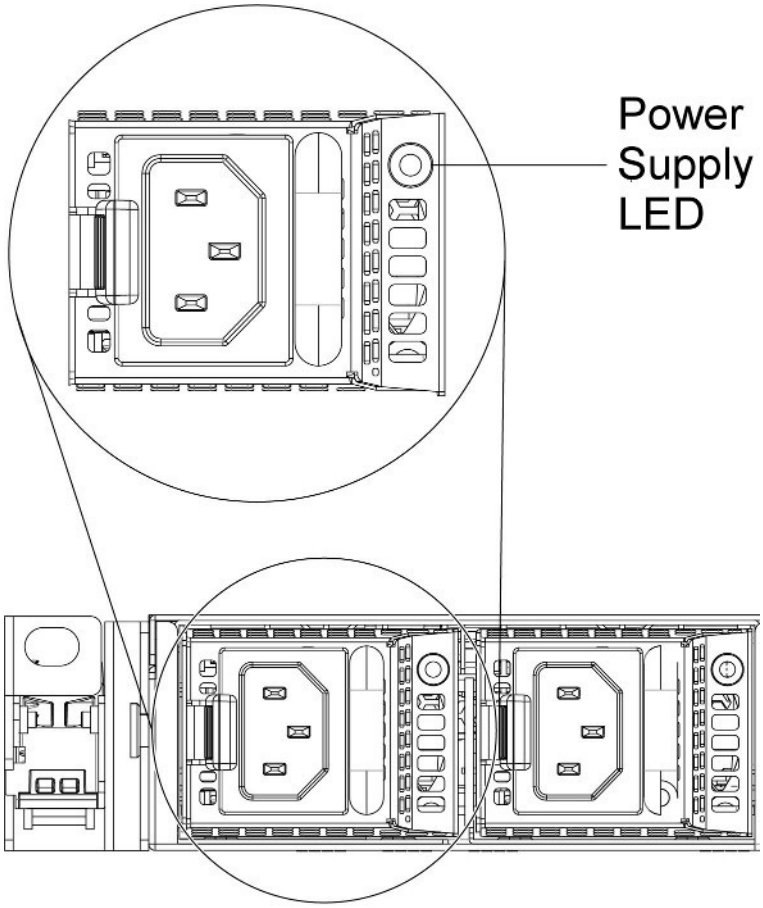


Figure 7. Power supply LED

The following table indicates the potential problems that can occur with the power supply:

Table 7. Power supply LED combinations for detecting potential problems

Power supply condition	**LED state**
Normal work	Green
No AC power to all the power supplies	Off
AC present / Only 12VSB on (PS off) or PS in CR state	1 Hz Blink Green
AC cord unplugged with a second power supply in parallel still with AC input power	0.5 Hz Blink Green
Power supply warning events where power supply continues to operate: high temp, high power, high current, slow fan	1 Hz Blink Red
Power supply critical event causing a shutdown, failure, OCP, OVP, Fan Fail	Red

Replacing a failed power supply

Before you begin

When you replace a failed power supply, do not unplug the power supply unit that is working. This action disrupts service to the appliance.

Procedure

1. Remove the failed power supply from the power supply bay by pinching the side clip and pulling the failed power supply from the bay, as shown in Figure 2.

   Important:

   During normal operation, each power supply bay must contain either a power supply or a power supply blank for proper cooling.

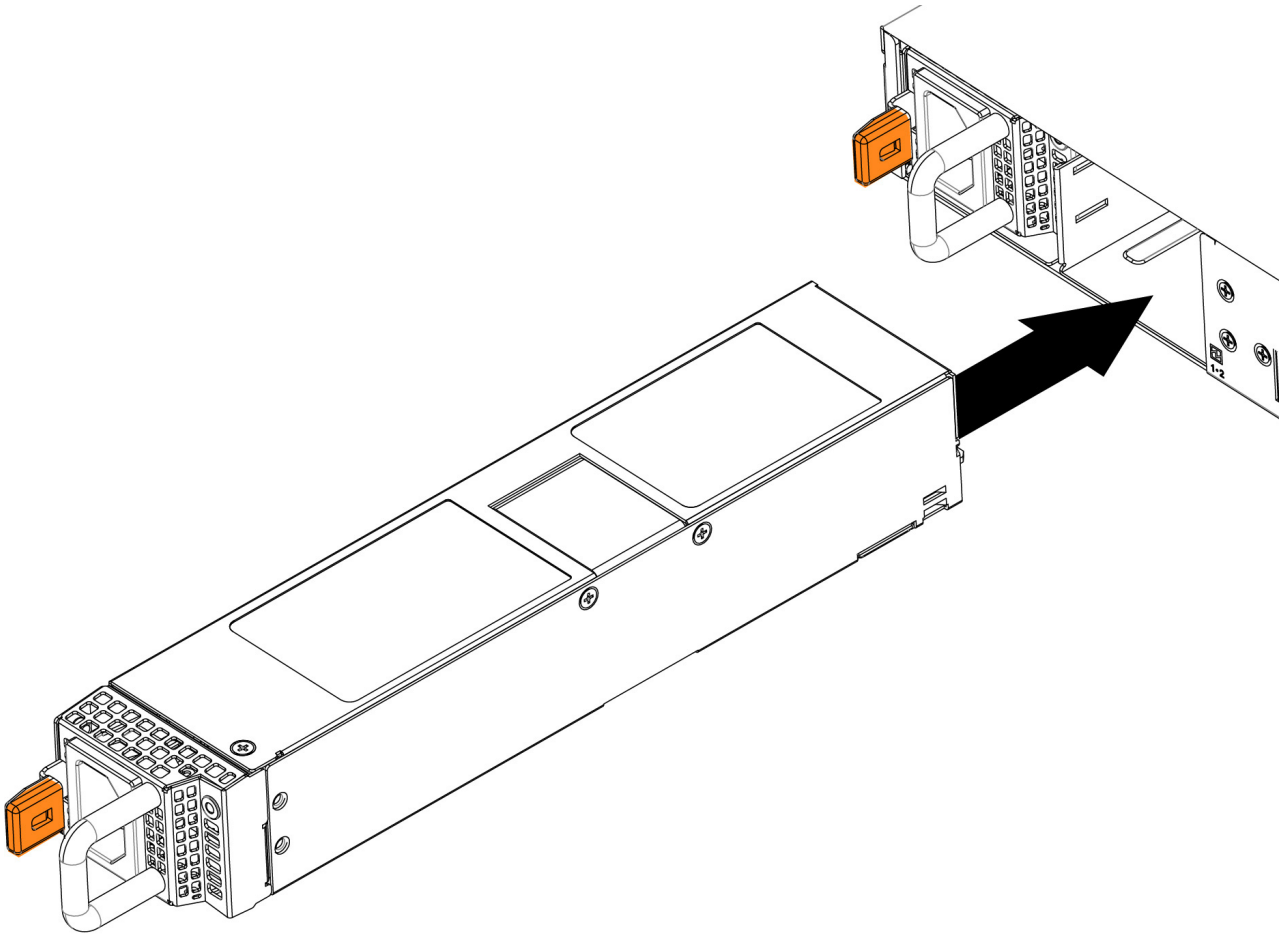


Figure 8. Removing the power supply from the back of the appliance

2. Slide the AC power supply into the bay until the retention latch clicks into place. Make sure that the power supply connects firmly to the power supply connector.
3. Connect the power cord for the new AC power supply to the power cord connector on the power supply. The AC power supply connectors on the back of the appliance are shown in the following figure:

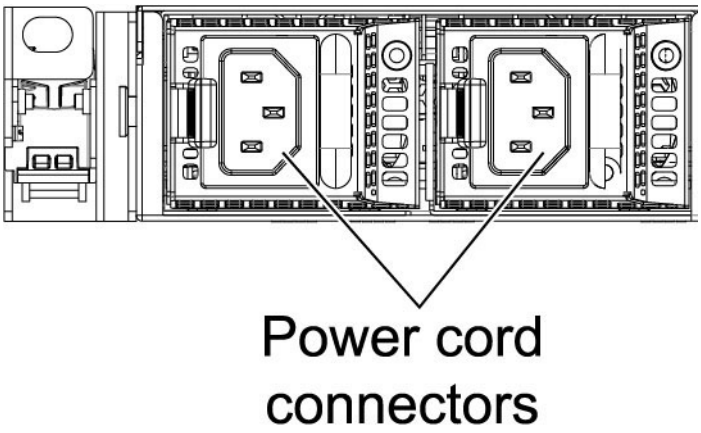


Figure 9. Identifying the power cord connectors

4. Route the power cord through the power supply handle and through any cable clamps on the back of the appliance to prevent the power cord from being accidentally pulled out when you slide the appliance into and out of the rack.
5. Connect the power cord to a properly grounded electrical outlet.

What to do next

Make sure that the AC power LED and the DC power LED on the AC power supply are illuminated, which indicates that the power supply is operating correctly. The two power LEDs are to the left of the power cord connector.

Chapter 11. Supporting content

Use these resources to better understand the product.

IBM IdentityDev for IBM Security Access Manager
https://developer.ibm.com/identitydev/

IBM Security Learning Academy
https://www.securitylearningacademy.com/local/navigator/index.php?level=iaam01

The IBM Security YouTube Channel
https://www.youtube.com/user/IBMSecuritySolutions

The IBM Security Support YouTube Channel
https://www.youtube.com/channel/UCIYjTUJjvRaolva6tiYU4Cg

DeveloperWorks Answers
https://developer.ibm.com/answers/topics/accessmanager/

DeveloperWorks Forum
https://www.ibm.com/developerworks/community/forums/html/forum?id=11111111-0000-0000-0000-000000000259

Index

Printed in USA