IBM Security Verify Product Tour

Begin your tour →

IBM

Securely connect any user to anything

IBM Security Verify brings context and intelligence to decisions about who should have access to what, allowing your organization to give the right people the right access at the right time.

Explore the demo and learn how to master the balance between security and user experience.

Employee

Business manager

IT administrator

Developer

Employee

Easily access the apps you need to do your job from any device, without password hassles.

Employees need quick access to the tools they need to do their jobs, without feeling burdened by dozens of credentials. While enterprise security is expected, IT policies can still feel like an obstacle. Employees want to work efficiently, without roadblocks.

11

hours

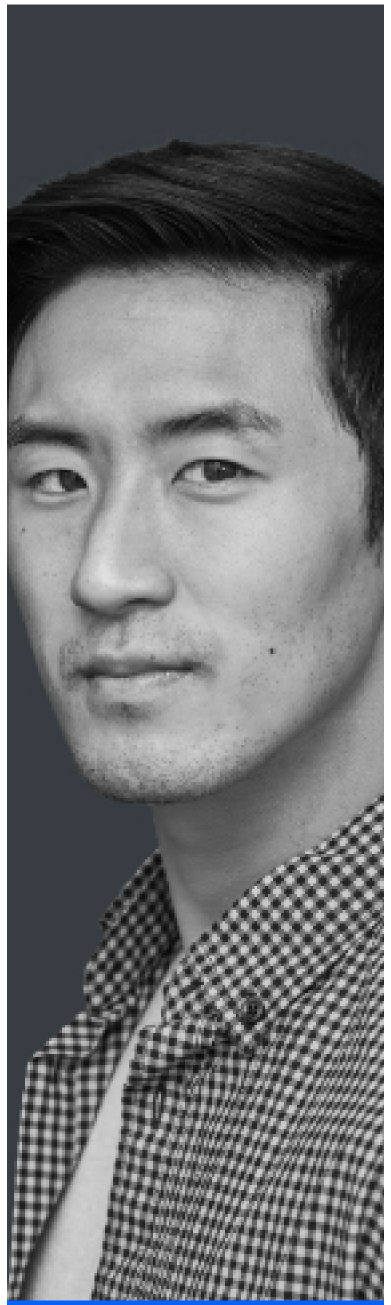
average time each year employees worldwide spend entering or resetting their password

World Economic Forum

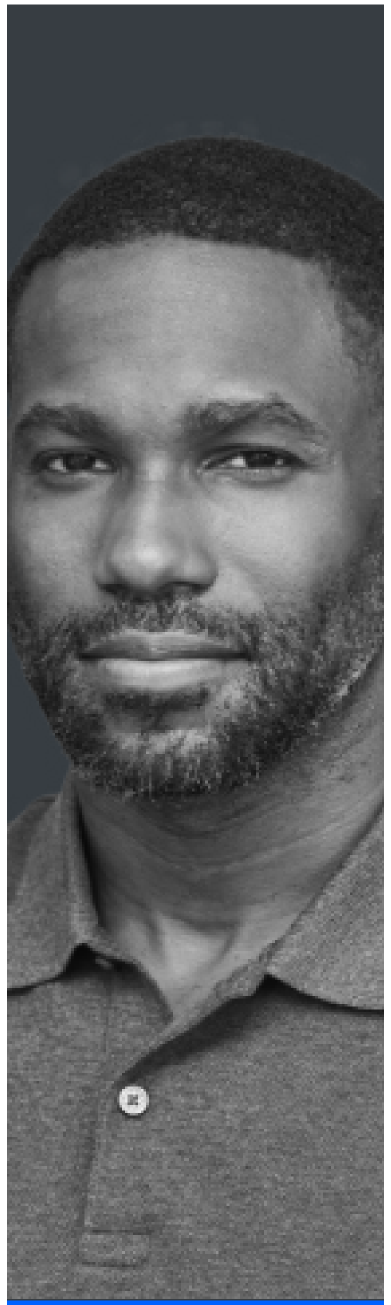
"Getting stalled by tools and systems when I'm just trying to get my work done is really frustrating."

Jessica, Employee

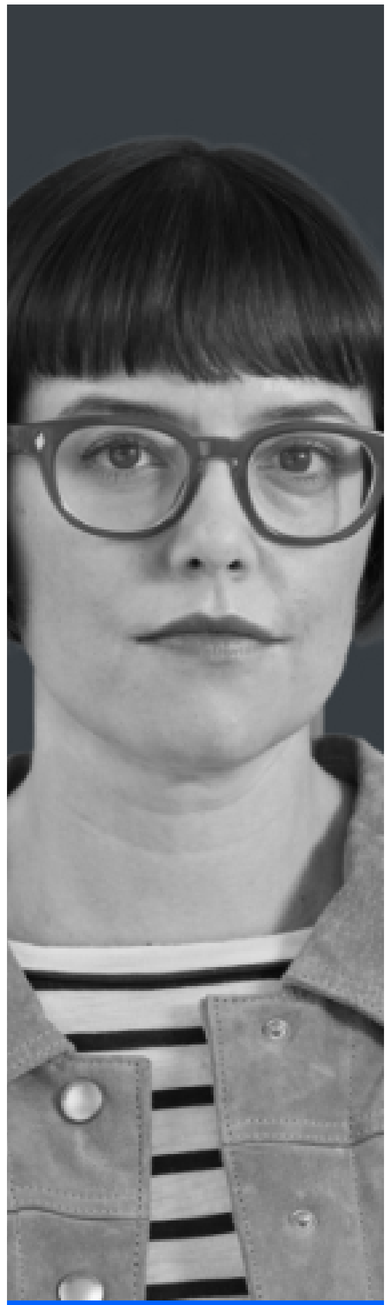
Employee



View



View



View

Begin with:
Branded sign-in page

← →

- ● **Employee**
- ○ Single sign-on
- ○ Request application access
- ○ Register and use MFA
- ○ **Business manager**
- ○ **IT administrator**
- ○ **Developer**

Employee

Easily access the apps you need to do your job from any device, without password hassles.

Employees need quick access to the tools they need to do their jobs, without feeling burdened by dozens of credentials. While enterprise security is expected, IT policies can still feel like an obstacle. Employees want to work efficiently, without roadblocks.

11

hours

average time each year employees worldwide spend entering or resetting their password

World Economic Forum

> *"Getting stalled by tools and systems when I'm just trying to get my work done is really frustrating."*
>
> **Jessica, Employee**

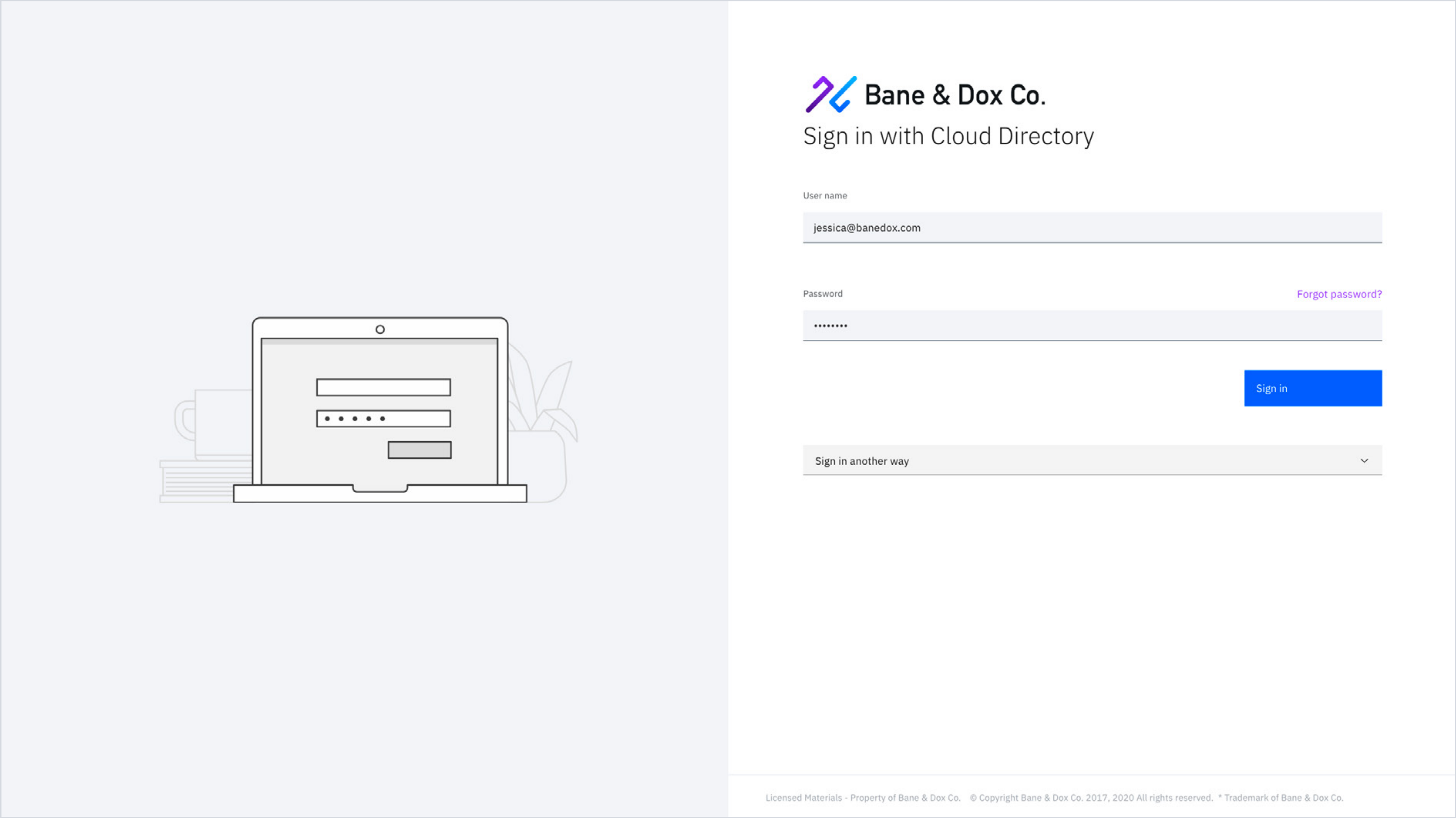
Employee

- **Employee**
- Single sign-on
  - Branded sign-in page
  - One-click access to apps
- Request application access
  - Search catalog
  - Write justification
  - Pending requests
  - New app in launchpad
- Register and use MFA
  - Add new authentication device
  - Set up mobile app
  - Choose MFA method
- **Business manager**
- **IT administrator**
- **Developer**

Employee: 1 of 2
Single sign-on

Branded sign-in page

Employees need quick access to the tools they need to do their jobs, without feeling burdened by dozens of credentials. While enterprise security is expected, IT policies can still feel like an obstacle. Employees want to work efficiently, without roadblocks.



Bane & Dox Co.

Sign in with Cloud Directory

User name

jessica@banedox.com

Password

••••••••

Licensed Materials - Property of Bane & Dox Co.   © Copyright Bane & Dox Co. 2017, 2020 All rights reserved. * Trademark of Bane & Dox Co.

Next:
One-click access to apps

← →

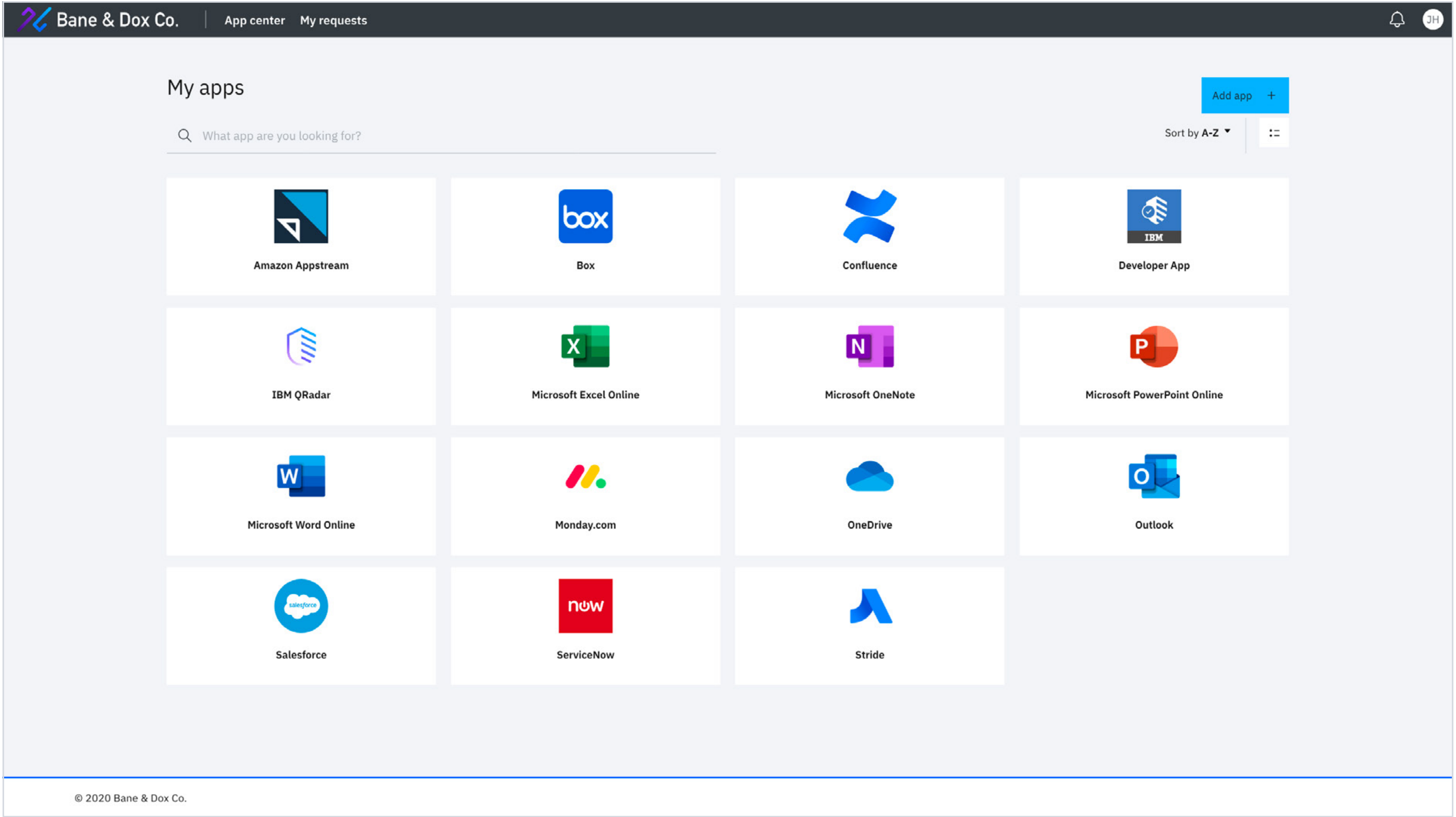
● Employee ◉ **Single sign-on** ○ Request application access ○ Register and use MFA ○ Business manager ○ IT administrator ○ Developer

Employee: 2 of 2

Single sign-on

One-click access to apps

From her launchpad, Jessica can access all the apps she is entitled to use. Depending on how the IT administrator configures her settings, most applications will have one-click access.



Next:
Search catalog

← →

● Employee ◉ **Single sign-on** ○ Request application access ○ Register and use MFA ○ Business manager ○ IT administrator ○ Developer

Back Next

IBM **Security** Verify

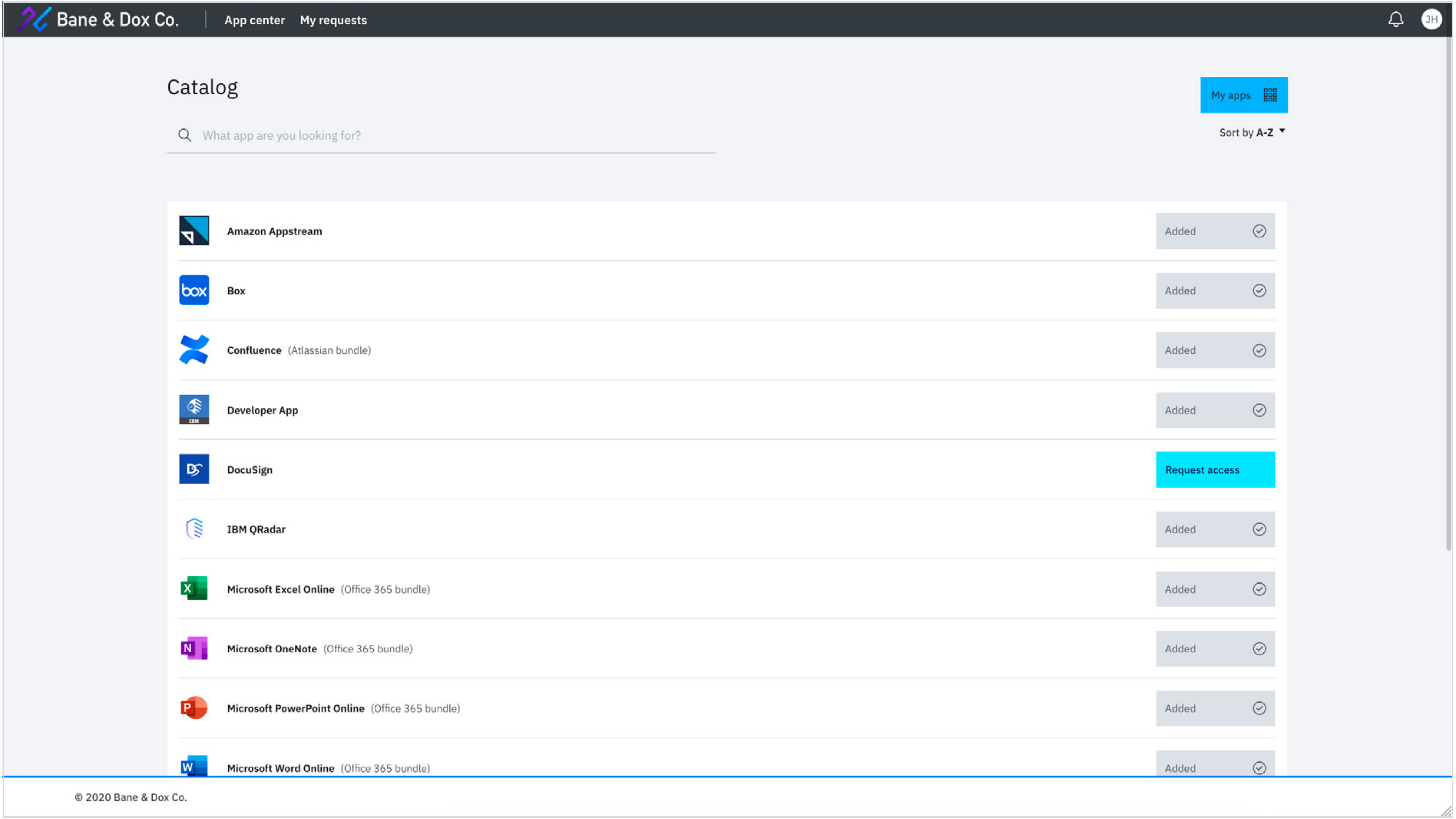
Try Verify Now

Employee: 1 of 4

Request application access

Search catalog

From her launchpad, Jessica can access all the apps she is entitled to use. Depending on how the IT administrator configures her settings, most applications will have one-click access.



Catalog

What app are you looking for?

Sort by **A-Z**

Amazon Appstream	Added ✓
Box	Added ✓
Confluence (Atlassian bundle)	Added ✓
Developer App	Added ✓
DocuSign	Request access
IBM QRadar	Added ✓
Microsoft Excel Online (Office 365 bundle)	Added ✓
Microsoft OneNote (Office 365 bundle)	Added ✓
Microsoft PowerPoint Online (Office 365 bundle)	Added ✓
Microsoft Word Online (Office 365 bundle)	Added ✓

© 2020 Bane & Dox Co.

Next:
Write justification

← →

● Employee ● Single sign-on ◉ **Request application access** ○ Register and use MFA ○ Business manager ○ IT administrator ○ Developer

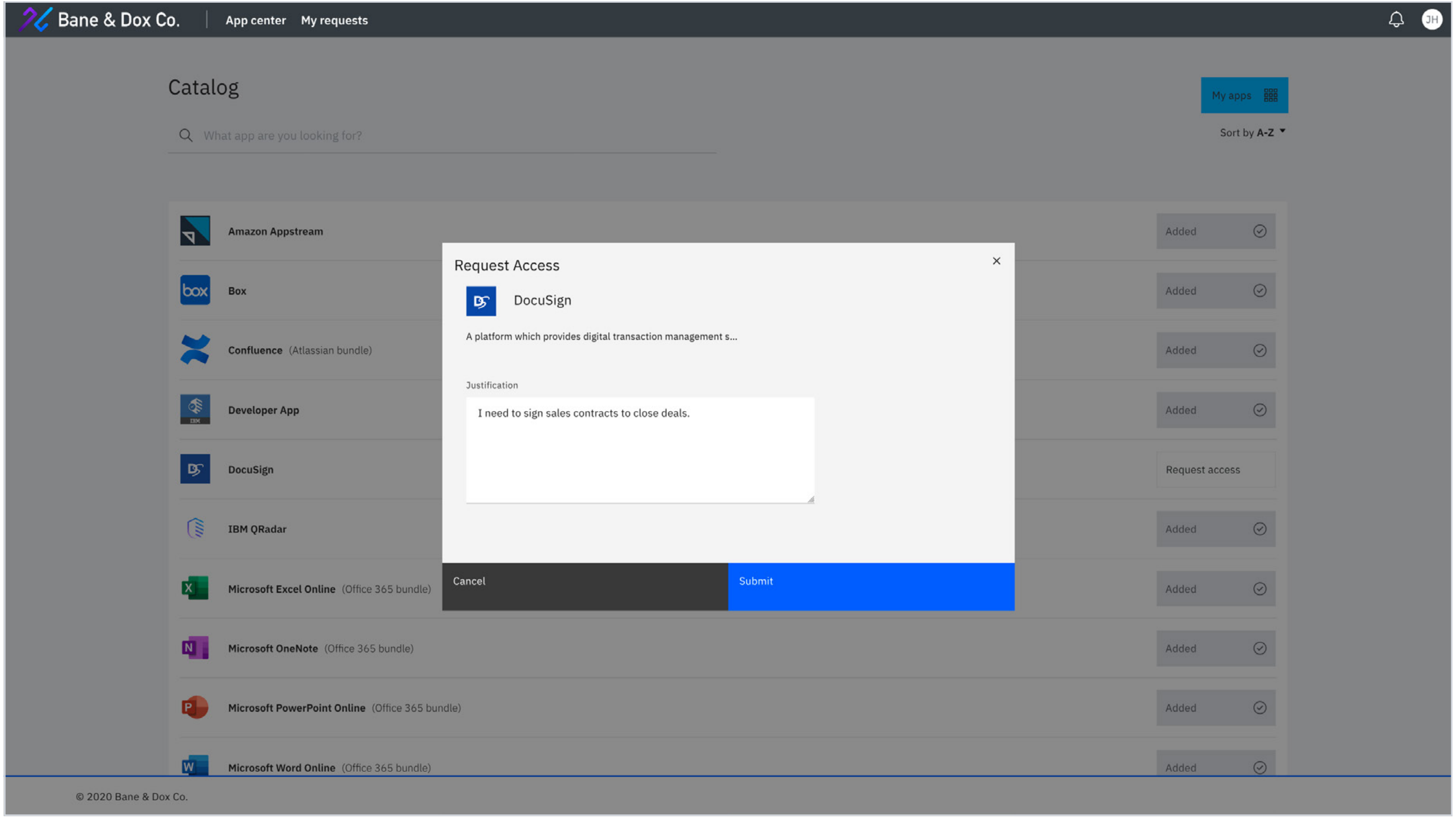
Back Next

Employee: 2 of 4

Request application access

Write justification

She selects XYZ and writes a business justification for why she needs access.



Catalog

What app are you looking for?

Amazon Appstream	Added
Box	Added
Confluence (Atlassian bundle)	Added
Developer App	Added
DocuSign	Request access
IBM QRadar	Added
Microsoft Excel Online (Office 365 bundle)	Added
Microsoft OneNote (Office 365 bundle)	Added
Microsoft PowerPoint Online (Office 365 bundle)	Added
Microsoft Word Online (Office 365 bundle)	Added

Request Access ×

DocuSign

A platform which provides digital transaction management s...

Justification

I need to sign sales contracts to close deals.

Cancel | Submit

© 2020 Bane & Dox Co.

Next:
Pending requests

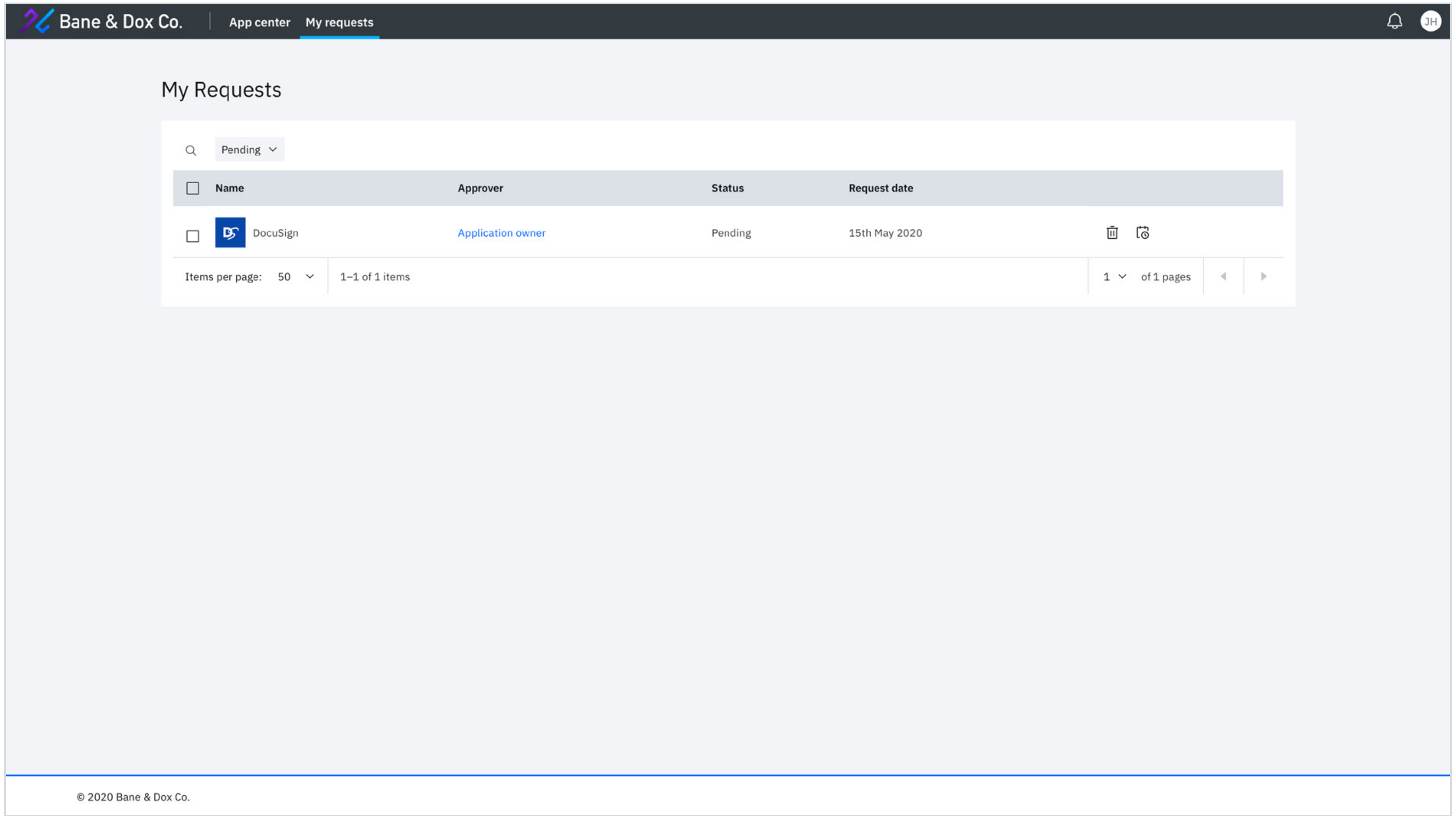
← →

- Employee
- Single sign-on
- **Request application access**
- Register and use MFA
- Business manager
- IT administrator
- Developer

Employee: 3 of 4
Request application access

Pending requests

In her pending requests page, Jessica can see her pending access requests, who they are assigned to and current status. If needed, she can check back here to add additional details to her justification.



My Requests

Pending

□ Name	Approver	Status	Request date
□ DocuSign	Application owner	Pending	15th May 2020

Items per page: 50 | 1–1 of 1 items | 1 of 1 pages

© 2020 Bane & Dox Co.

Next:
New app in launchpad

← →

Employee
Single sign-on
Request application access
Register and use MFA
Business manager
IT administrator
Developer

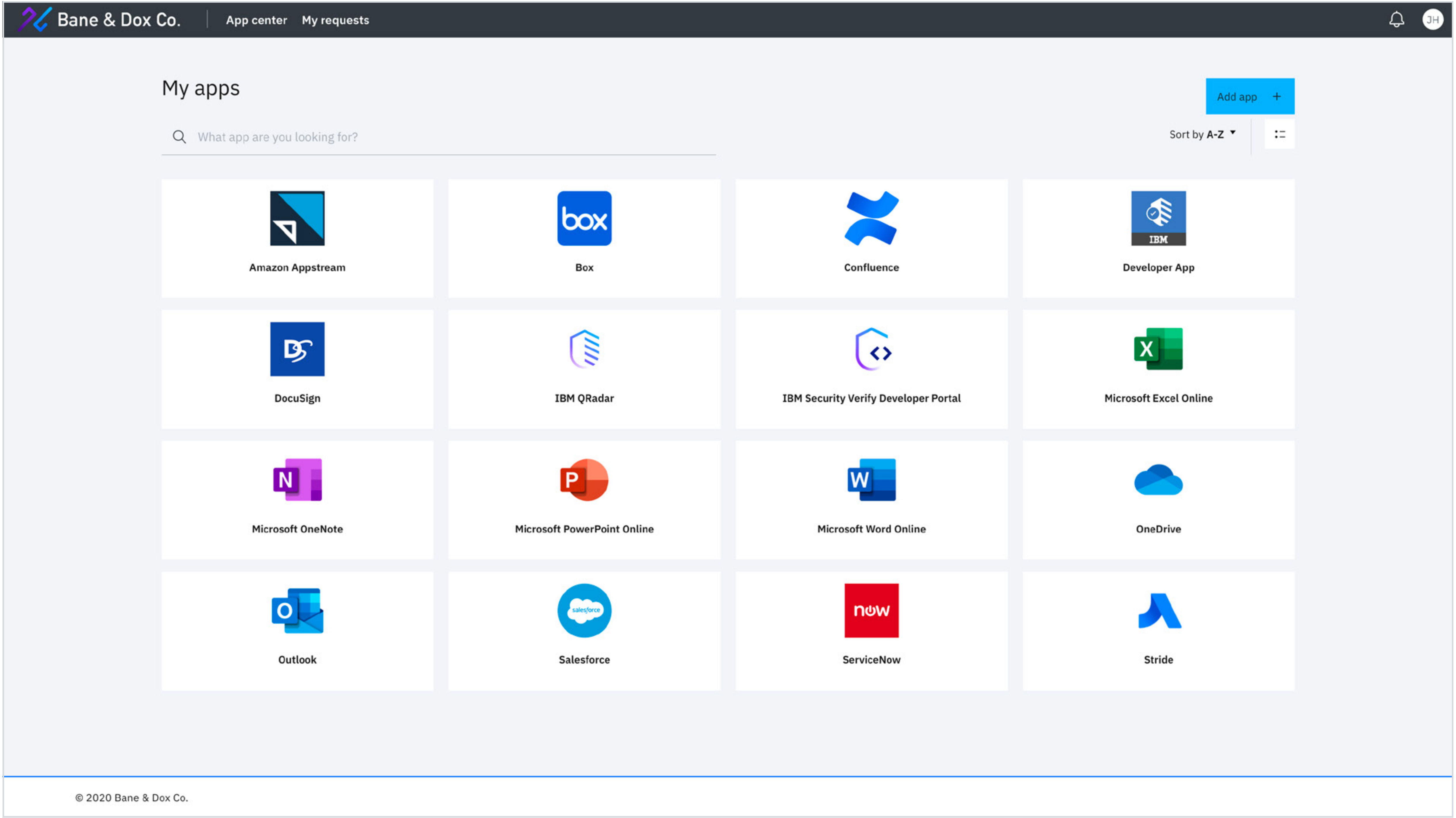
IBM **Security** Verify

Try Verify Now

Employee: 4 of 4
Request application access

New app in launchpad

Once the request is approved by the application owner, she will see XYZ added to her launchpad.



Next:
Add new authentication device launchpad

← →

● Employee
● Single sign-on
◉ **Request application access**
○ Register and use MFA
○ Business manager
○ IT administrator
○ Developer

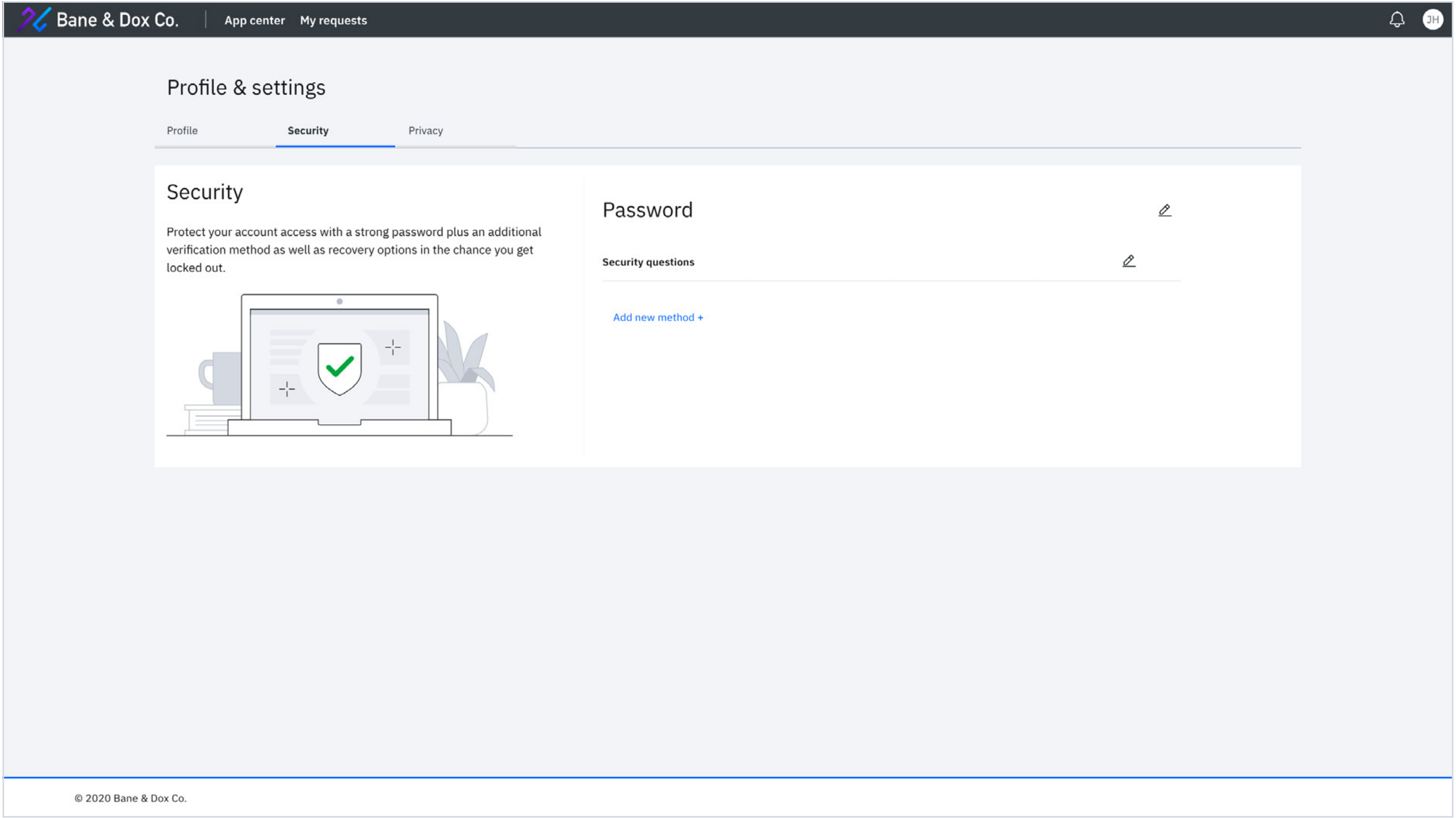
Back

Next

Employee: 1 of 3
Register and use MFA

Add new authentication device launchpad

Jessica can add devices and resources to use for authentication challenges on her security settings page. She can register her mobile phone for use with the IBM Security Verify mobile app to complete MFA challenges or choose any of the other available methods.



Profile & settings

Security

Protect your account access with a strong password plus an additional verification method as well as recovery options in the chance you get locked out.

Password

Security questions

© 2020 Bane & Dox Co.

Next:
MFA registration

← →

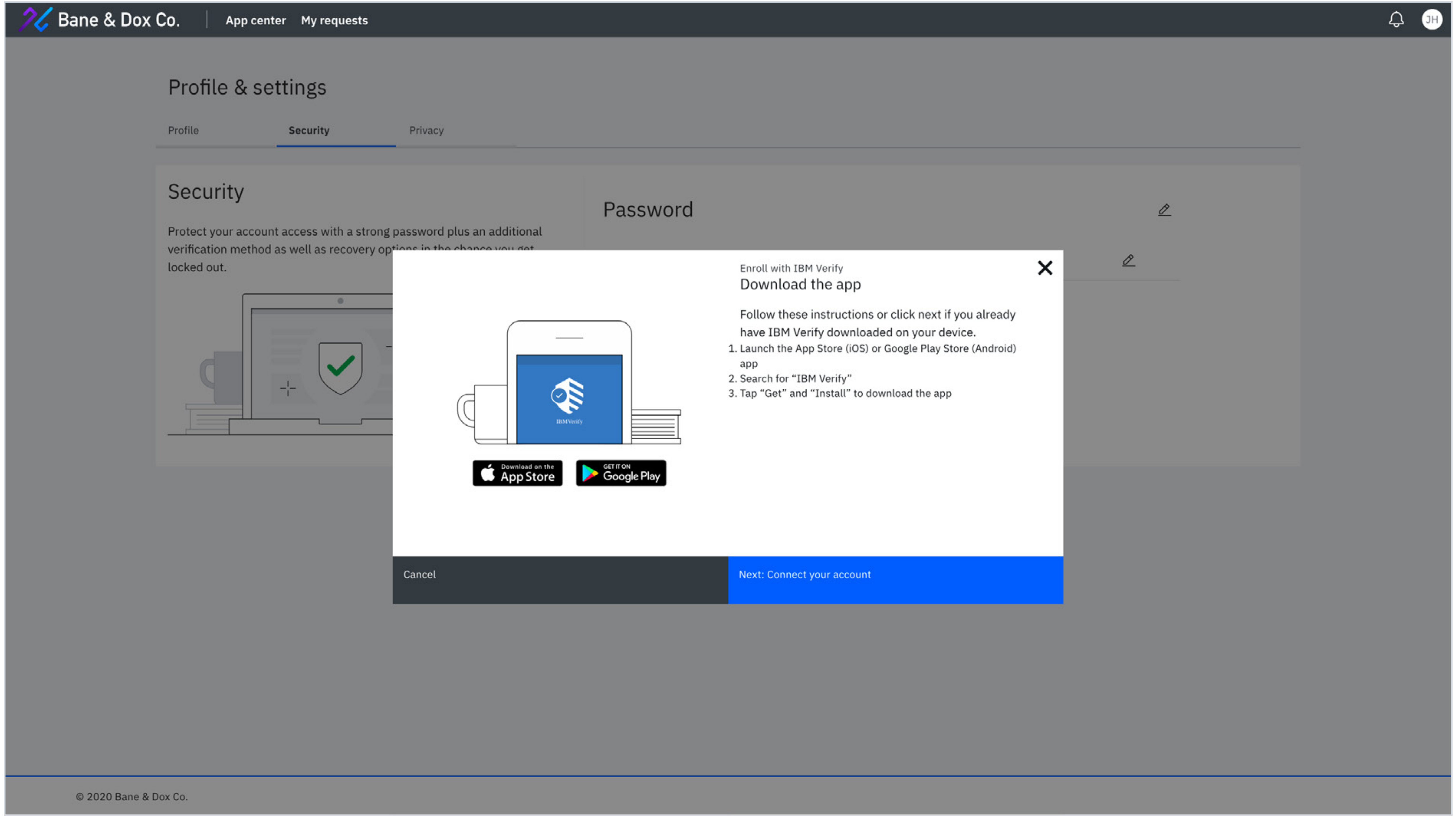
● Employee — ● Single sign-on — ● Request application access — ◉ **Register and use MFA** — ○ Business manager — ○ IT administrator — ○ Developer

Back
Next

Employee: 2 of 3
Register and use MFA

Set up mobile app

Jessica can add devices and resources to use for authentication challenges on her security settings page. She can register her mobile phone for use with the IBM Security Verify mobile app to complete MFA challenges or choose any of the other available methods.



Profile & settings

Security

Protect your account access with a strong password plus an additional verification method as well as recovery options in the chance you get locked out.

Password

Enroll with IBM Verify

Download the app

Follow these instructions or click next if you already have IBM Verify downloaded on your device.

1. Launch the App Store (iOS) or Google Play Store (Android) app
2. Search for “IBM Verify”
3. Tap “Get” and “Install” to download the app

© 2020 Bane & Dox Co.

Next:
Choose MFA method

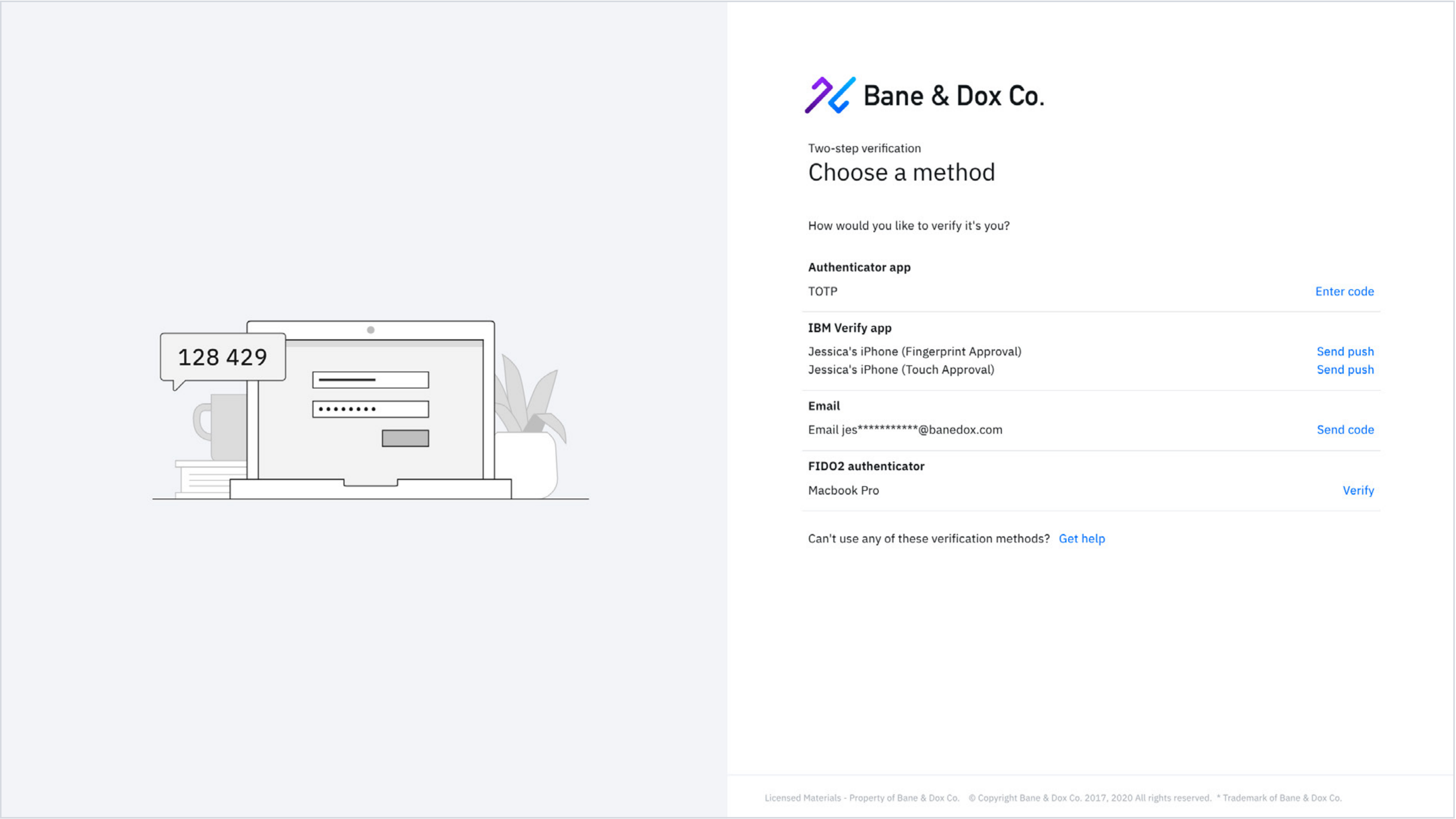
← →

Employee
Single sign-on
Request application access
Register and use MFA
Business manager
IT administrator
Developer

Employee: 3 of 3
Register and use MFA

Choose MFA method

Now, when Jessica logs into an app that requires MFA, she can choose the supported authentication method that is most convenient to her.



Bane & Dox Co.

Two-step verification

Choose a method

How would you like to verify it's you?

Authenticator app
TOTP — Enter code

IBM Verify app
Jessica's iPhone (Fingerprint Approval) — Send push
Jessica's iPhone (Touch Approval) — Send push

Email
Email jes***********@banedox.com — Send code

FIDO2 authenticator
Macbook Pro — Verify

Can't use any of these verification methods? Get help

Licensed Materials - Property of Bane & Dox Co. © Copyright Bane & Dox Co. 2017, 2020 All rights reserved. * Trademark of Bane & Dox Co.

Next:
Line of business manager

← →

Employee — Single sign-on — Request application access — **Register and use MFA** — Business manager — IT administrator — Developer

Line of business manager

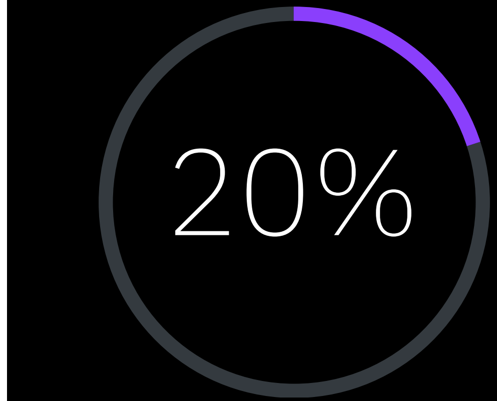
Manage team specific application entitlements with delegated controls.

Line of business managers need to deliver new services to employees and customers quickly in order to stay competitive. They need to move at the speed of business, without waiting on IT.

Begin with:
Pending notifcation in launchpad

← →

View



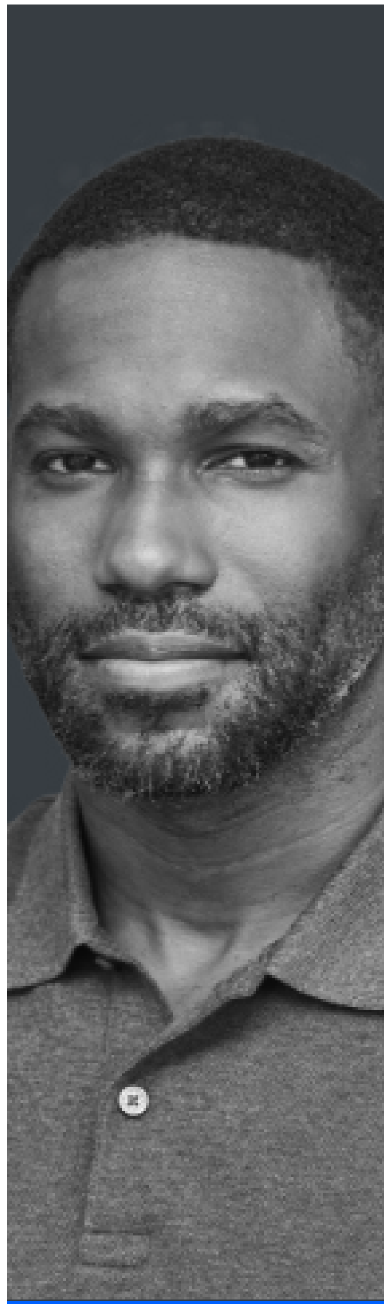
20% to 50% of all calls to the IT helpdesk concern password resets

World Economic Forum

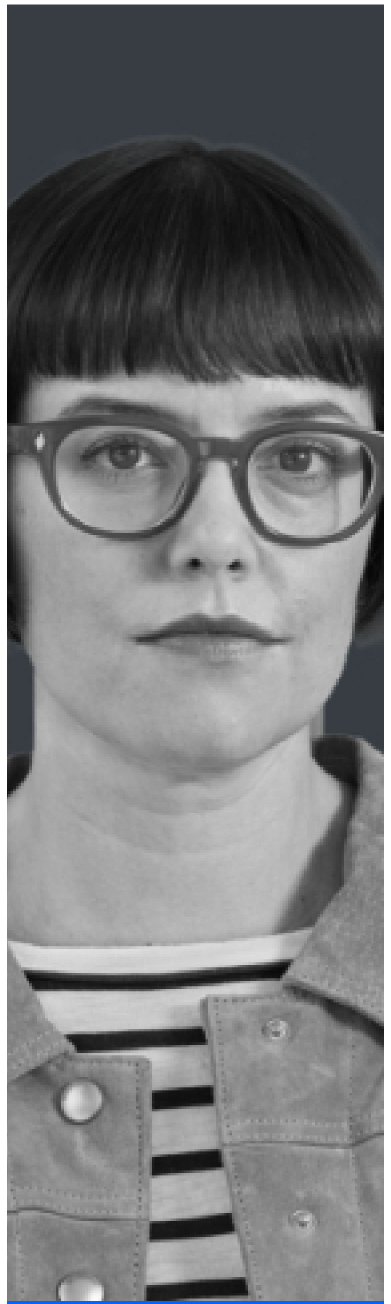
"Getting stalled by tools and systems when I'm just trying to get my work done is really frustrating."

Jacob, Employee

Business manager



View



View

○ Employee ● **Business manager** ○ Process access requests ○ IT administrator ○ Developer

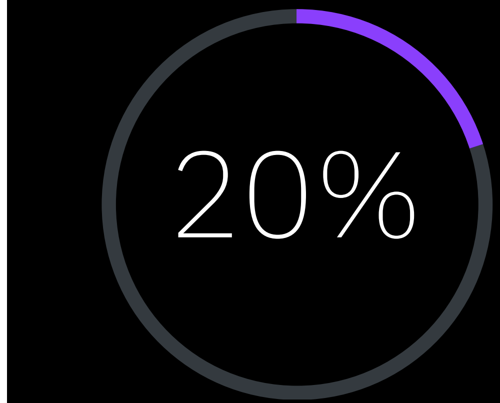
IBM **Security** Verify

Try Verify Now

Line of business manager

Manage team specific application entitlements with delegated controls.

Line of business managers need to deliver new services to employees and customers quickly in order to stay competitive. They need to move at the speed of business, without waiting on IT.



20% to 50% of all calls to the IT helpdesk concern password resets

World Economic Forum

> *"Getting stalled by tools and systems when I'm just trying to get my work done is really frustrating."*
>
> **Jacob, Employee**

Business manager

- ○ **Employee**
- ● **Business manager**
  - ○ Process access requests
    - Pending notification in launchpad
    - View request details
    - Request additional justification
    - Approve/reject the request
- ○ **IT administrator**
- ○ **Developer**

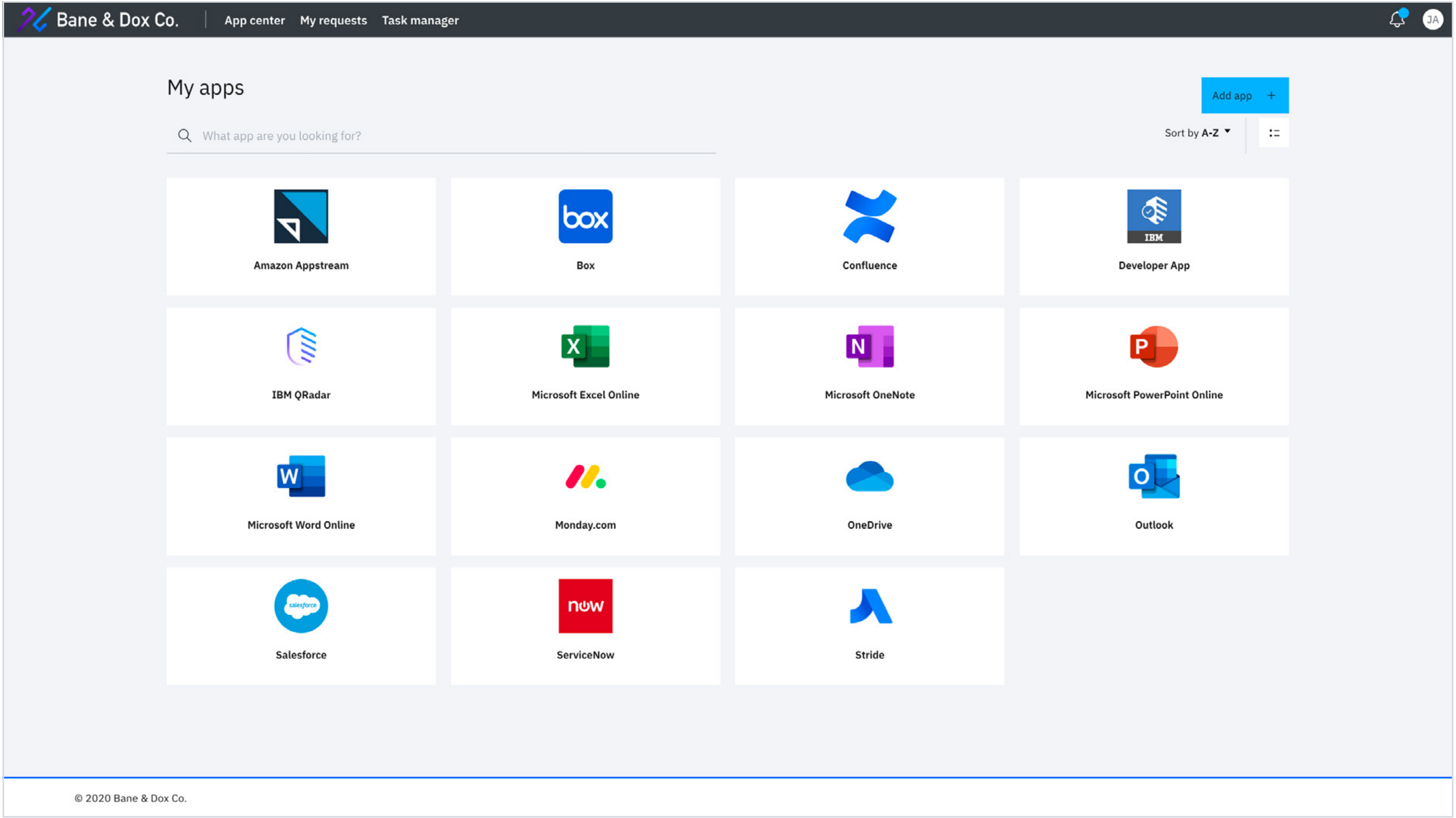
Back to team

Begin business manager path

Line of business manager: 1 of 4
Process access requests

Pending notification in launchpad

Jacob is the manager of the Bane & Dox Co. sales team. When he logs in to IBM Security Verify, he'll be able to see all the applications he can access. Jacob has been delegated permissions to manage DocuSign for the organization and approve employee access requests without waiting on IT. Here, he can view pending notifications for app requests.



Next:
View request details

← →

○ Employee

● Business manager

● **Process access requests**

○ IT administrator

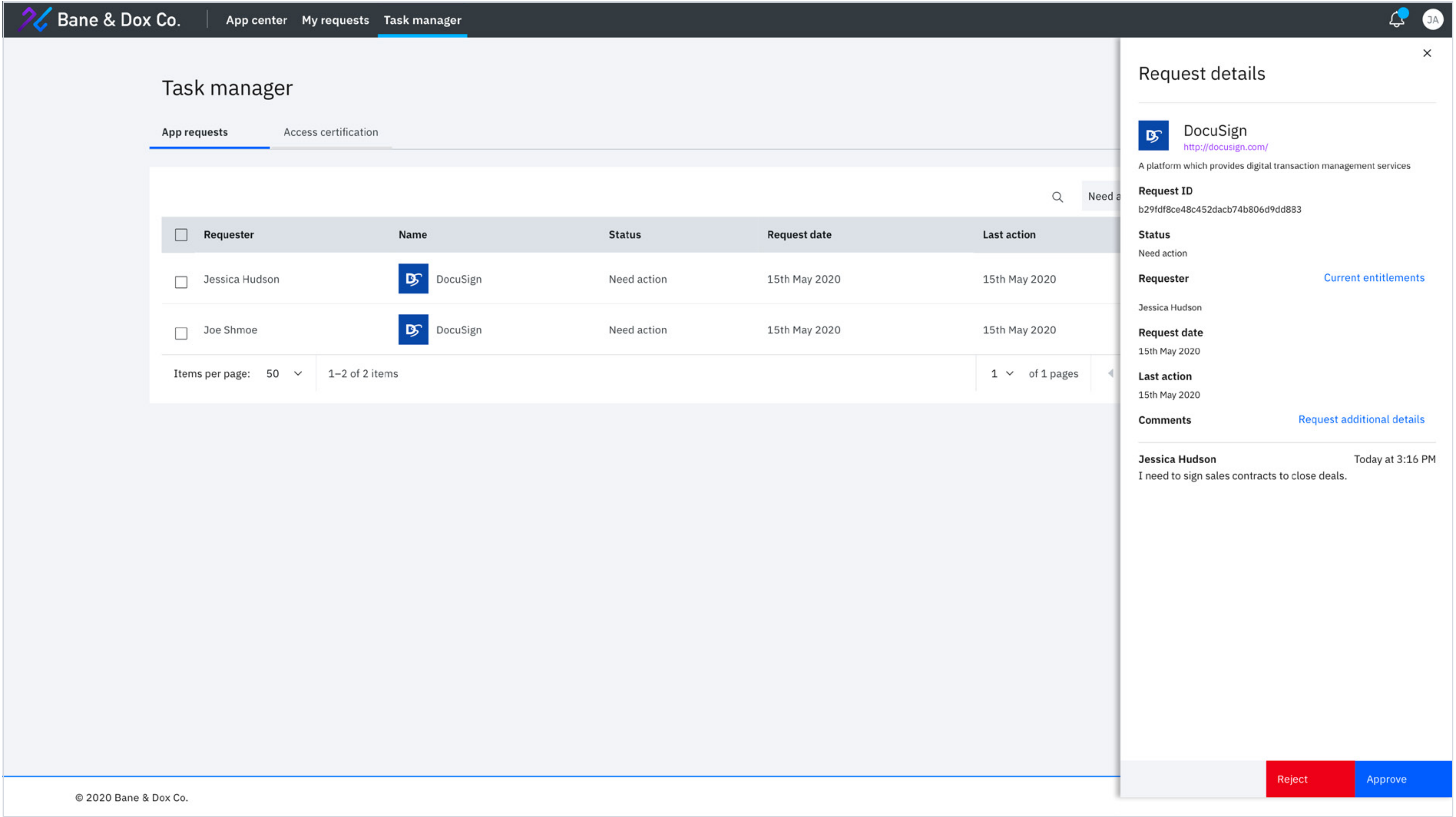
○ Developer

Line of business manager: 2 of 4

Process access requests

View request details

From the applications request tab, Jacob can view the details of Jessica's request. If needed, he can ask Jessica for additional justification for her request.



Task manager

App requests | Access certification

Need a

☐	Requester	Name	Status	Request date	Last action
☐	Jessica Hudson	DocuSign	Need action	15th May 2020	15th May 2020
☐	Joe Shmoe	DocuSign	Need action	15th May 2020	15th May 2020

Items per page: 50 | 1–2 of 2 items | 1 of 1 pages

© 2020 Bane & Dox Co.

Request details

DocuSign
http://docusign.com/

A platform which provides digital transaction management services

Request ID
b29fdf8ce48c452dacb74b806d9dd883

Status
Need action

Requester — Current entitlements
Jessica Hudson

Request date
15th May 2020

Last action
15th May 2020

Comments — Request additional details

Jessica Hudson Today at 3:16 PM
I need to sign sales contracts to close deals.

Next:
Request additional justification

← →

○ Employee ● Business manager ● **Process access requests** ○ IT administrator ○ Developer

IBM **Security** Verify

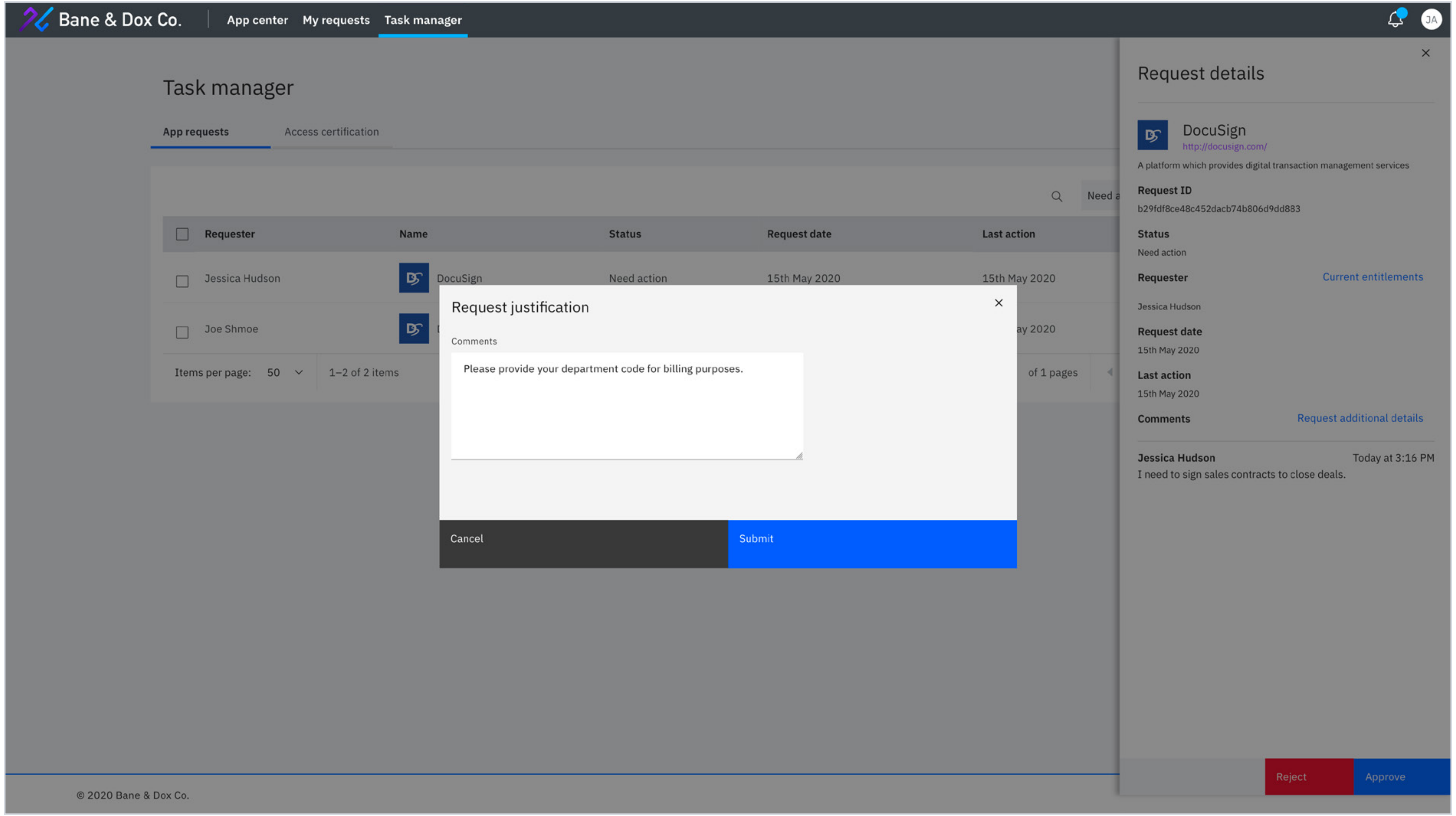
Try Verify Now

Line of business manager: 3 of 4

Process access requests

Request additional justification

He can send the request back for more justification.



Bane & Dox Co. | App center | My requests | **Task manager**

JA

Task manager

App requests | Access certification

Need a

□	Requester	Name	Status	Request date	Last action
□	Jessica Hudson	DocuSign	Need action	15th May 2020	15th May 2020
□	Joe Shmoe				ay 2020

Items per page: 50 | 1–2 of 2 items | of 1 pages

Request justification ×

Comments

Please provide your department code for billing purposes.

Cancel | Submit

© 2020 Bane & Dox Co.

Request details ×

DocuSign
http://docusign.com/

A platform which provides digital transaction management services

Request ID
b29fdf8ce48c452dacb74b806d9dd883

Status
Need action

Requester Current entitlements

Jessica Hudson

Request date
15th May 2020

Last action
15th May 2020

Comments Request additional details

Jessica Hudson Today at 3:16 PM
I need to sign sales contracts to close deals.

Reject | Approve

Next:
Approve/reject the request

← →

○ Employee
● Business manager
● **Process access requests**
○ IT administrator
○ Developer

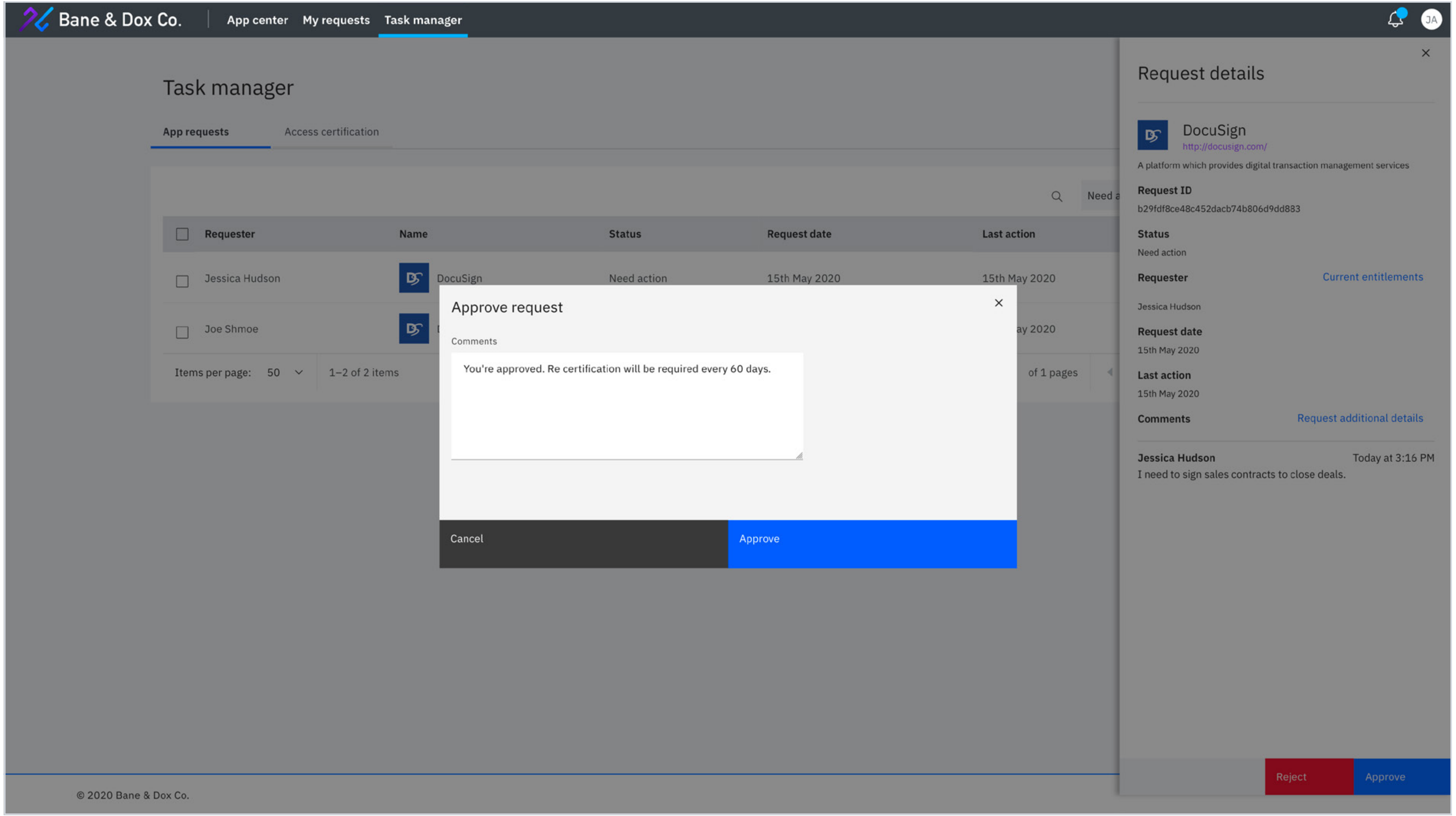
Back | Next

Line of business manager: 4 of 4

Process access requests

Approve/reject the request

Or, he can approve/reject the request. By owning access approvals for his direct reports, Jacob enables his team to move at the speed of business without feeling burdened by IT logistics.



Task manager

App requests | Access certification

Need a

□	Requester	Name	Status	Request date	Last action
□	Jessica Hudson	DocuSign	Need action	15th May 2020	15th May 2020
□	Joe Shmoe				ay 2020

Items per page: 50 | 1–2 of 2 items | of 1 pages

Approve request

Comments

You're approved. Re certification will be required every 60 days.

Request details

DocuSign
http://docusign.com/

A platform which provides digital transaction management services

Request ID
b29fdf8ce48c452dacb74b806d9dd883

Status
Need action

Requester Current entitlements

Jessica Hudson

Request date
15th May 2020

Last action
15th May 2020

Comments Request additional details

Jessica Hudson Today at 3:16 PM
I need to sign sales contracts to close deals.

© 2020 Bane & Dox Co.

IBM **Security** Verify

Try Verify Now

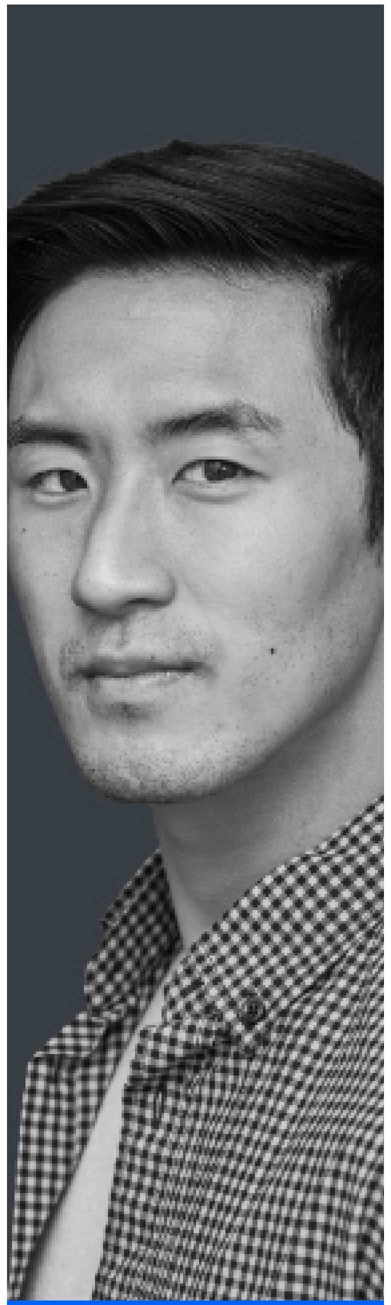
IT administrator

Simplify configuration, scale on a common platform and automate risk protection.

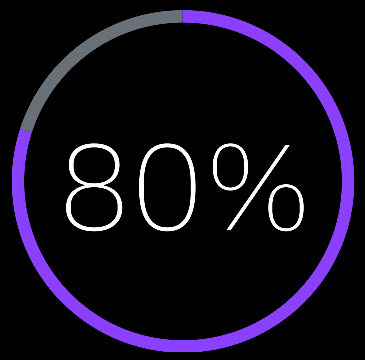
IT administrators need to satisfy business demands for easy access while protecting the organization against credential misuse — despite any lack of time, skills or resources they may be facing. Teams can also feel a loss of control when incorporating cloud applications from a wide variety of vendors, so an integrated workflow for SSO and MFA becomes paramount.

Begin with:
Live dashboard

View



View



80%

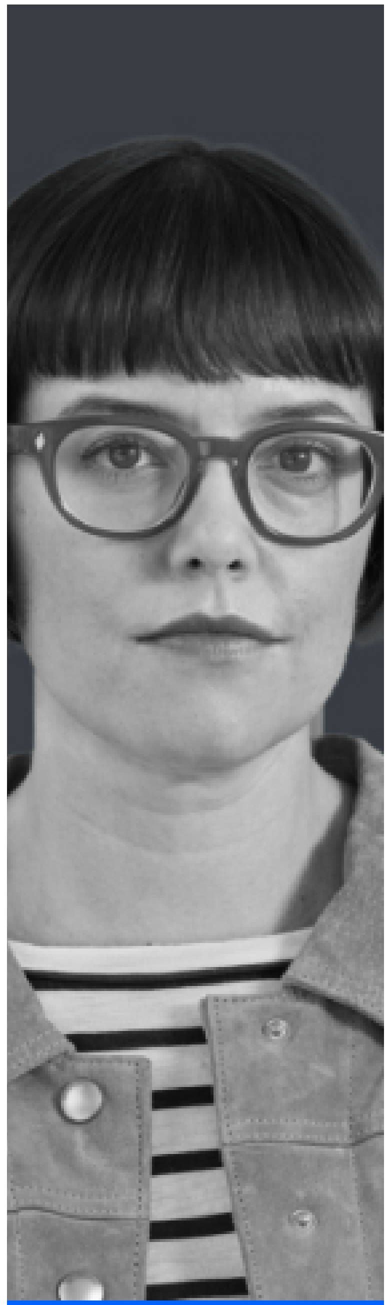
of hacking-related breaches involve compromised and weak credentials

World Economic Forum

"I need to enable my organization's productivity, keep my colleagues safe and account for all aspects of identity and access related risks along the way - all at the same time. "

Scott, IT Admin

IT administrator



View

← →

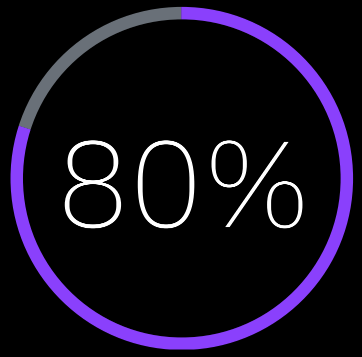
○ Employee ○ Business manager ● **IT administrator** ○ Monitor activity ○ Customize policies ○ Manage users and identities ○ Add applications ○ Analyze risk ○ Developer

Back Next

IT administrator

Simplify configuration, scale on a common platform and automate risk protection.

IT administrators need to satisfy business demands for easy access while protecting the organization against credential misuse — despite any lack of time, skills or resources they may be facing. Teams can also feel a loss of control when incorporating cloud applications from a wide variety of vendors, so an integrated workflow for SSO and MFA becomes paramount.



of hacking-related breaches involve compromised and weak credentials

World Economic Forum

"I need to enable my organization's productivity, keep my colleagues safe and account for all aspects of identity and access related risks along the way - all at the same time. "

Scott, IT Admin

IT administrator

○ **Employee**

○ **Business manager**

● **IT administrator**

○ Monitor activity
- Live dashboard
- Create activity reports
- Adaptive Access activity report

○ Customize policies
- Policy editor
- Add rule to policy
- Adaptive Access

○ Manage users and identities
- Manager users
- Manage groups
- Manage user attributes
- Active Directory and LDAP
- Social login

○ Add applications
- View applications
- Search for application to add
- Add owner for access approvals
- Configure sign-on settings
- Configure entitlements
- Set periodic access recertification

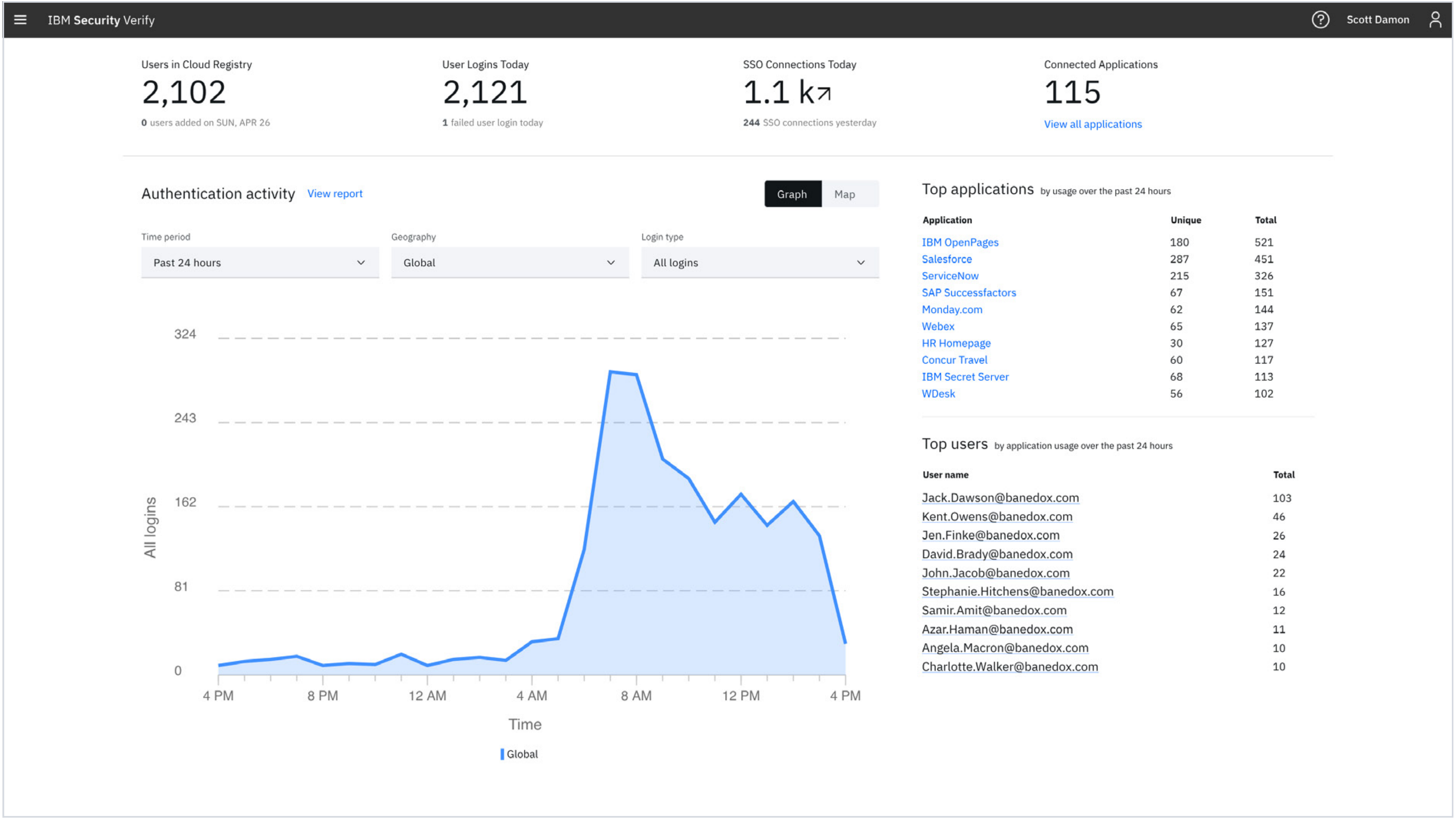
○ Analyze risk
- Analytics report
- View ranked policy violations
- Take suggested remediation actions

○ **Developer**

IT administrator: 1 of 3
Monitor activity

Live dashboard

IBM Security Verify's administrative dashboard provides a global overview of authentication activity within an organization. Scott, an IT administrator, can filter for time period or geography to better understand user trends.



Users in Cloud Registry	User Logins Today	SSO Connections Today	Connected Applications
2,102	2,121	1.1 k↗	115
0 users added on SUN, APR 26	**1** failed user login today	**244** SSO connections yesterday	View all applications

Authentication activity View report

Time period: Past 24 hours
Geography: Global
Login type: All logins

Top applications by usage over the past 24 hours

Application	Unique	Total
IBM OpenPages	180	521
Salesforce	287	451
ServiceNow	215	326
SAP Successfactors	67	151
Monday.com	62	144
Webex	65	137
HR Homepage	30	127
Concur Travel	60	117
IBM Secret Server	68	113
WDesk	56	102

Top users by application usage over the past 24 hours

User name	Total
Jack.Dawson@banedox.com	103
Kent.Owens@banedox.com	46
Jen.Finke@banedox.com	26
David.Brady@banedox.com	24
John.Jacob@banedox.com	22
Stephanie.Hitchens@banedox.com	16
Samir.Amit@banedox.com	12
Azar.Haman@banedox.com	11
Angela.Macron@banedox.com	10
Charlotte.Walker@banedox.com	10

Next:
Create activity reports

← →

○ Employee ○ Business manager ● IT administrator ● **Monitor activity** ○ Customize policies ○ Manage users and identities ○ Add applications ○ Analyze risk ○ Developer

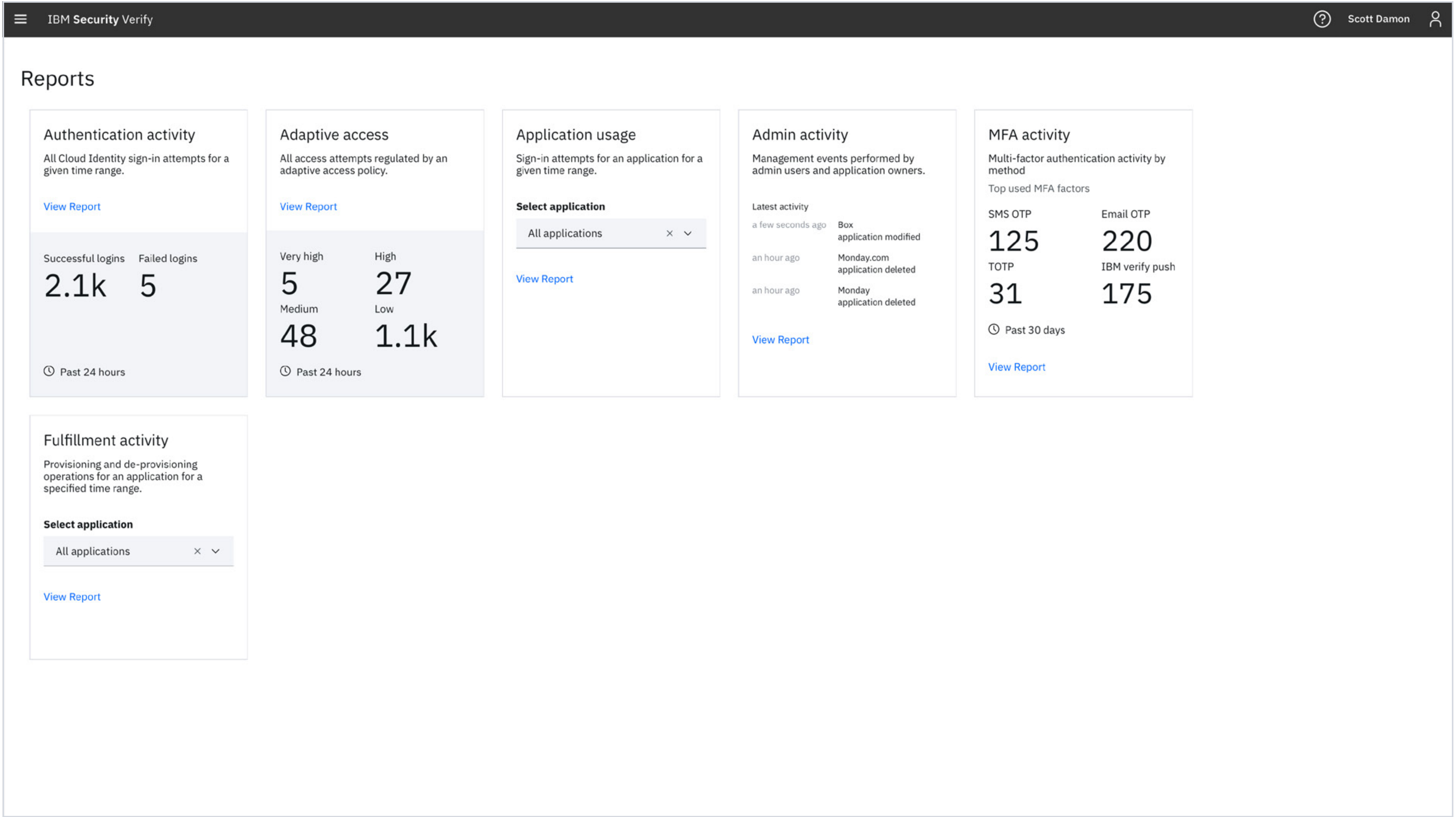
Back Next

IT administrator: 2 of 3

Monitor activity

Create activity reports

Verify's reporting interface enables Scott to filter recent activity data live to quickly diagnose problems. Across authentication activity, Adaptive Access, application usage, admin activity and MFA activity, he can dive deep into his organization's access and authentication data to collect insights and troubleshoot events.



Reports

Authentication activity

All Cloud Identity sign-in attempts for a given time range.

View Report

Successful logins: 2.1k

Failed logins: 5

Past 24 hours

Adaptive access

All access attempts regulated by an adaptive access policy.

View Report

Very high: 5

High: 27

Medium: 48

Low: 1.1k

Past 24 hours

Application usage

Sign-in attempts for an application for a given time range.

Select application: All applications

View Report

Admin activity

Management events performed by admin users and application owners.

Latest activity

a few seconds ago — Box application modified

an hour ago — Monday.com application deleted

an hour ago — Monday application deleted

View Report

MFA activity

Multi-factor authentication activity by method

Top used MFA factors

SMS OTP: 125

Email OTP: 220

TOTP: 31

IBM verify push: 175

Past 30 days

View Report

Fulfillment activity

Provisioning and de-provisioning operations for an application for a specified time range.

Select application: All applications

View Report

Next:
Adaptive Access activity reports

← →

Employee · Business manager · IT administrator · **Monitor activity** · Customize policies · Manage users and identities · Add applications · Analyze risk · Developer

Back Next

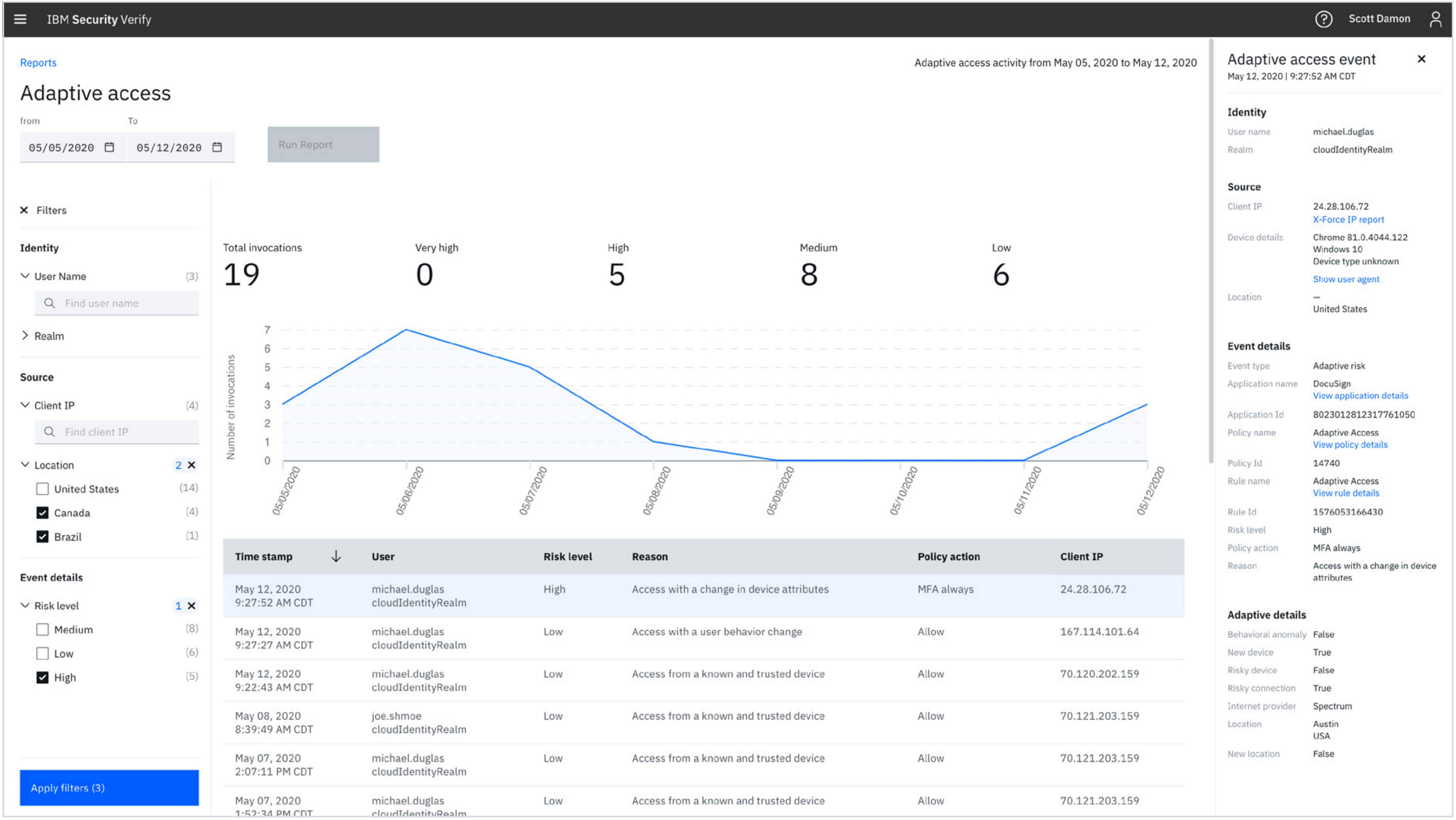
IT administrator: 3 of 3

Monitor activity

Adaptive access activity report

In an Adaptive Access report for instance, Scott can see all recent logins from applications using an Adaptive Access policy and documented event parameters. Using reports in Verify, he can diagnose and troubleshoot high risk events and take action if needed.

Adaptive Access Interactive Demo



Adaptive access activity from May 05, 2020 to May 12, 2020

Adaptive access

from 05/05/2020 To 05/12/2020

Identity

- User Name (3)
- Realm

Source

- Client IP (4)
- Location 2 ×
  - ☐ United States (14)
  - ☑ Canada (4)
  - ☑ Brazil (1)

Event details

- Risk level 1 ×
  - ☐ Medium (8)
  - ☐ Low (6)
  - ☑ High (5)

Total invocations	Very high	High	Medium	Low
19	0	5	8	6

Time stamp ↓	User	Risk level	Reason	Policy action	Client IP
May 12, 2020 9:27:52 AM CDT	michael.duglas cloudIdentityRealm	High	Access with a change in device attributes	MFA always	24.28.106.72
May 12, 2020 9:27:27 AM CDT	michael.duglas cloudIdentityRealm	Low	Access with a user behavior change	Allow	167.114.101.64
May 12, 2020 9:22:43 AM CDT	michael.duglas cloudIdentityRealm	Low	Access from a known and trusted device	Allow	70.120.202.159
May 08, 2020 8:39:49 AM CDT	joe.shmoe cloudIdentityRealm	Low	Access from a known and trusted device	Allow	70.121.203.159
May 07, 2020 2:07:11 PM CDT	michael.duglas cloudIdentityRealm	Low	Access from a known and trusted device	Allow	70.121.203.159
May 07, 2020 1:52:34 PM CDT	michael.duglas cloudIdentityRealm	Low	Access from a known and trusted device	Allow	70.121.203.159

Adaptive access event ×

May 12, 2020 | 9:27:52 AM CDT

Identity

User name	michael.duglas
Realm	cloudIdentityRealm

Source

Client IP	24.28.106.72 X-Force IP report
Device details	Chrome 81.0.4044.122 Windows 10 Device type unknown Show user agent
Location	— United States

Event details

Event type	Adaptive risk
Application name	DocuSign View application details
Application Id	8023012812317761050
Policy name	Adaptive Access View policy details
Policy Id	14740
Rule name	Adaptive Access View rule details
Rule Id	1576053166430
Risk level	High
Policy action	MFA always
Reason	Access with a change in device attributes

Adaptive details

Behavioral anomaly	False
New device	True
Risky device	False
Risky connection	True
Internet provider	Spectrum
Location	Austin USA
New location	False

Next:
Policy editor

← →

Employee · Business manager · IT administrator · **Monitor activity** · Customize policies · Manage users and identities · Add applications · Analyze risk · Developer

Back Next

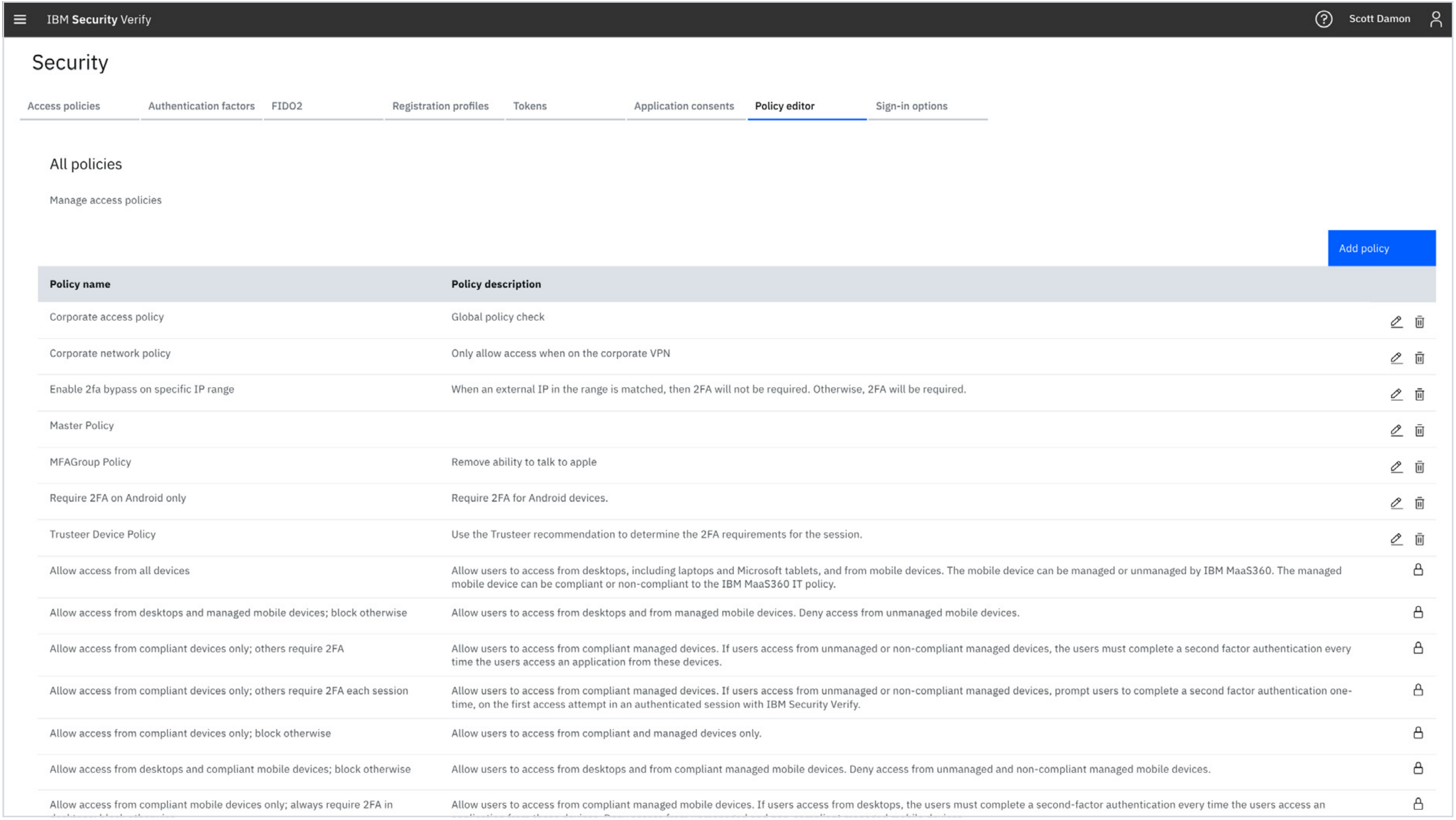
IBM **Security** Verify

Try Verify Now

IT administrator: 1 of 3
Customize policies

Policy editor

In the access policy editor, Scott can create additional custom access policies to use with his organization's applications. Some policies are included by default, such as always allowing access, always requiring 2FA, or requiring 2FA at the beginning of each new session.



Security

All policies

Manage access policies

Policy name	Policy description
Corporate access policy	Global policy check
Corporate network policy	Only allow access when on the corporate VPN
Enable 2fa bypass on specific IP range	When an external IP in the range is matched, then 2FA will not be required. Otherwise, 2FA will be required.
Master Policy	
MFAGroup Policy	Remove ability to talk to apple
Require 2FA on Android only	Require 2FA for Android devices.
Trusteer Device Policy	Use the Trusteer recommendation to determine the 2FA requirements for the session.
Allow access from all devices	Allow users to access from desktops, including laptops and Microsoft tablets, and from mobile devices. The mobile device can be managed or unmanaged by IBM MaaS360. The managed mobile device can be compliant or non-compliant to the IBM MaaS360 IT policy.
Allow access from desktops and managed mobile devices; block otherwise	Allow users to access from desktops and from managed mobile devices. Deny access from unmanaged mobile devices.
Allow access from compliant devices only; others require 2FA	Allow users to access from compliant managed devices. If users access from unmanaged or non-compliant managed devices, the users must complete a second factor authentication every time the users access an application from these devices.
Allow access from compliant devices only; others require 2FA each session	Allow users to access from compliant managed devices. If users access from unmanaged or non-compliant managed devices, prompt users to complete a second factor authentication one-time, on the first access attempt in an authenticated session with IBM Security Verify.
Allow access from compliant devices only; block otherwise	Allow users to access from compliant and managed devices only.
Allow access from desktops and compliant mobile devices; block otherwise	Allow users to access from desktops and from compliant managed mobile devices. Deny access from unmanaged and non-compliant managed mobile devices.
Allow access from compliant mobile devices only; always require 2FA in	Allow users to access from compliant managed mobile devices. If users access from desktops, the users must complete a second-factor authentication every time the users access an

Next:
Add rule to policy

← →

Employee | Business manager | IT administrator | Monitor activity | **Customize policies** | Manage users and identities | Add applications | Analyze risk | Developer

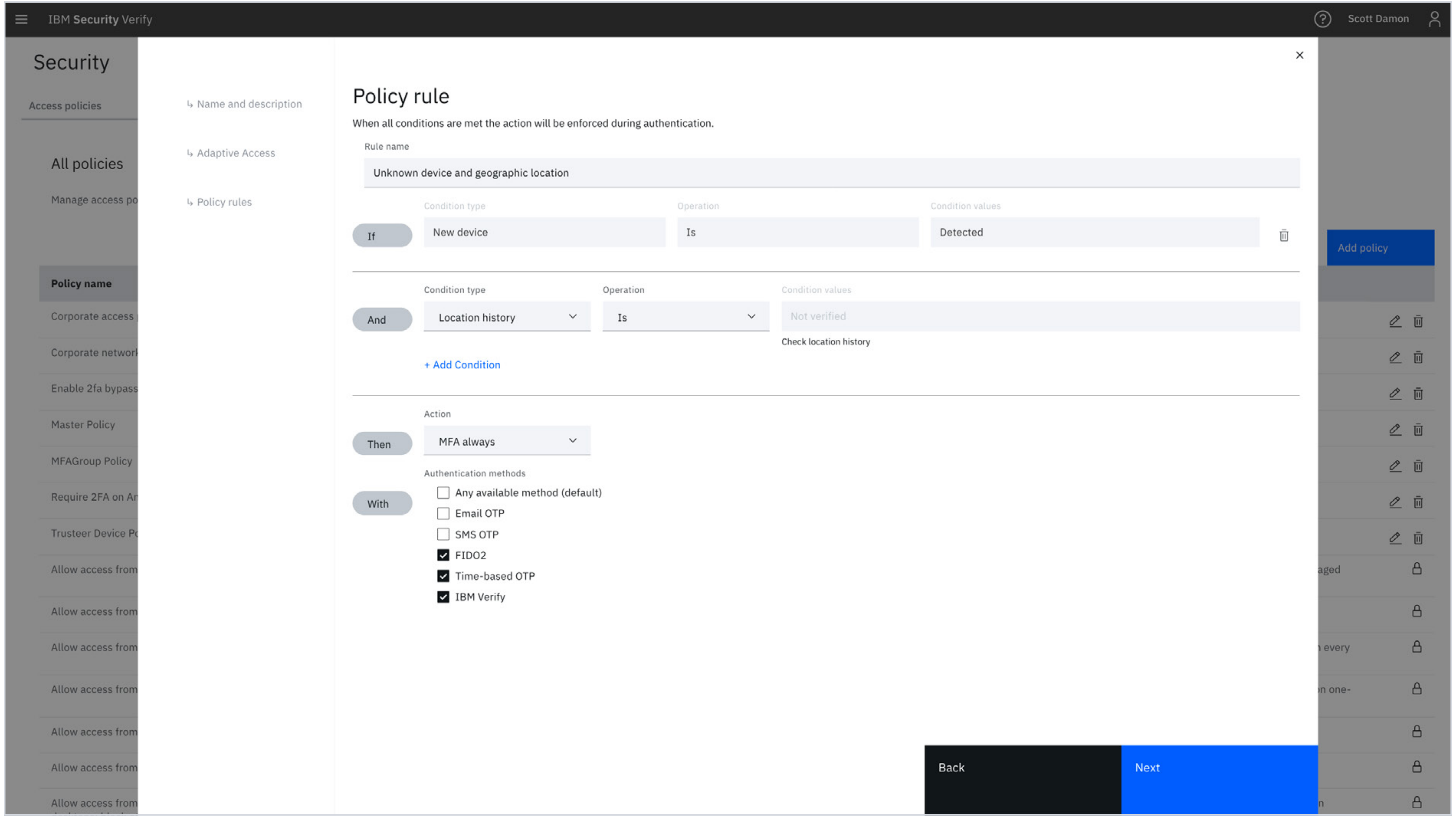
Back

Next

IT administrator: 2 of 3
Customize policies

Add rule to policy

Scott can easily configure rules based on conditions like device, group membership, IP and geolocation that either allow or block access or challenge with MFA.



Policy rule

When all conditions are met the action will be enforced during authentication.

Rule name: Unknown device and geographic location

If — Condition type: New device — Operation: Is — Condition values: Detected

And — Condition type: Location history — Operation: Is — Condition values: Not verified
Check location history

+ Add Condition

Then — Action: MFA always

With — Authentication methods
- ☐ Any available method (default)
- ☐ Email OTP
- ☐ SMS OTP
- ☑ FIDO2
- ☑ Time-based OTP
- ☑ IBM Verify

Next:
Adaptive Access

← →

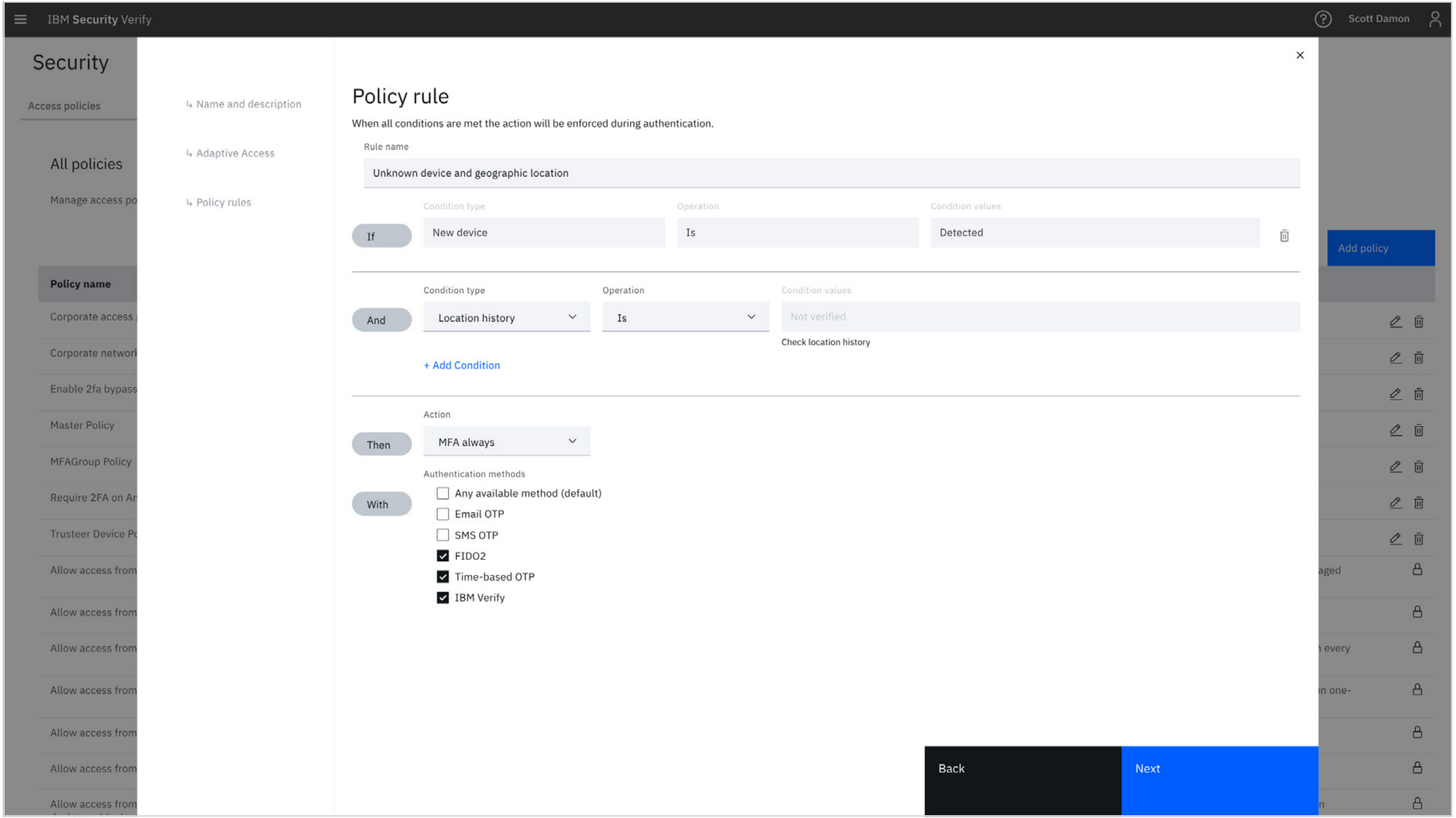
Employee · Business manager · IT administrator · Monitor activity · **Customize policies** · Manage users and identities · Add applications · Analyze risk · Developer

IT administrator: 3 of 3
Customize policies

Adaptive Access

He can also choose to automatically consider deep user, device, activity, environment, and behavior context by enabling risk-based authentication through an Adaptive Access policy. Adaptive Access determines an overall level of risk across a robust set of contextual parameters, powered by AI. With continuous authentication, low-risk users are granted frictionless access while higher risk users are automatically challenged or blocked.

Adaptive Access Interactive Demo



Policy rule

When all conditions are met the action will be enforced during authentication.

Rule name: Unknown device and geographic location

If — Condition type: New device — Operation: Is — Condition values: Detected

And — Condition type: Location history — Operation: Is — Condition values: Not verified — Check location history

+ Add Condition

Then — Action: MFA always

With — Authentication methods:
- □ Any available method (default)
- □ Email OTP
- □ SMS OTP
- ☑ FIDO2
- ☑ Time-based OTP
- ☑ IBM Verify

Next:
Manager users

← →

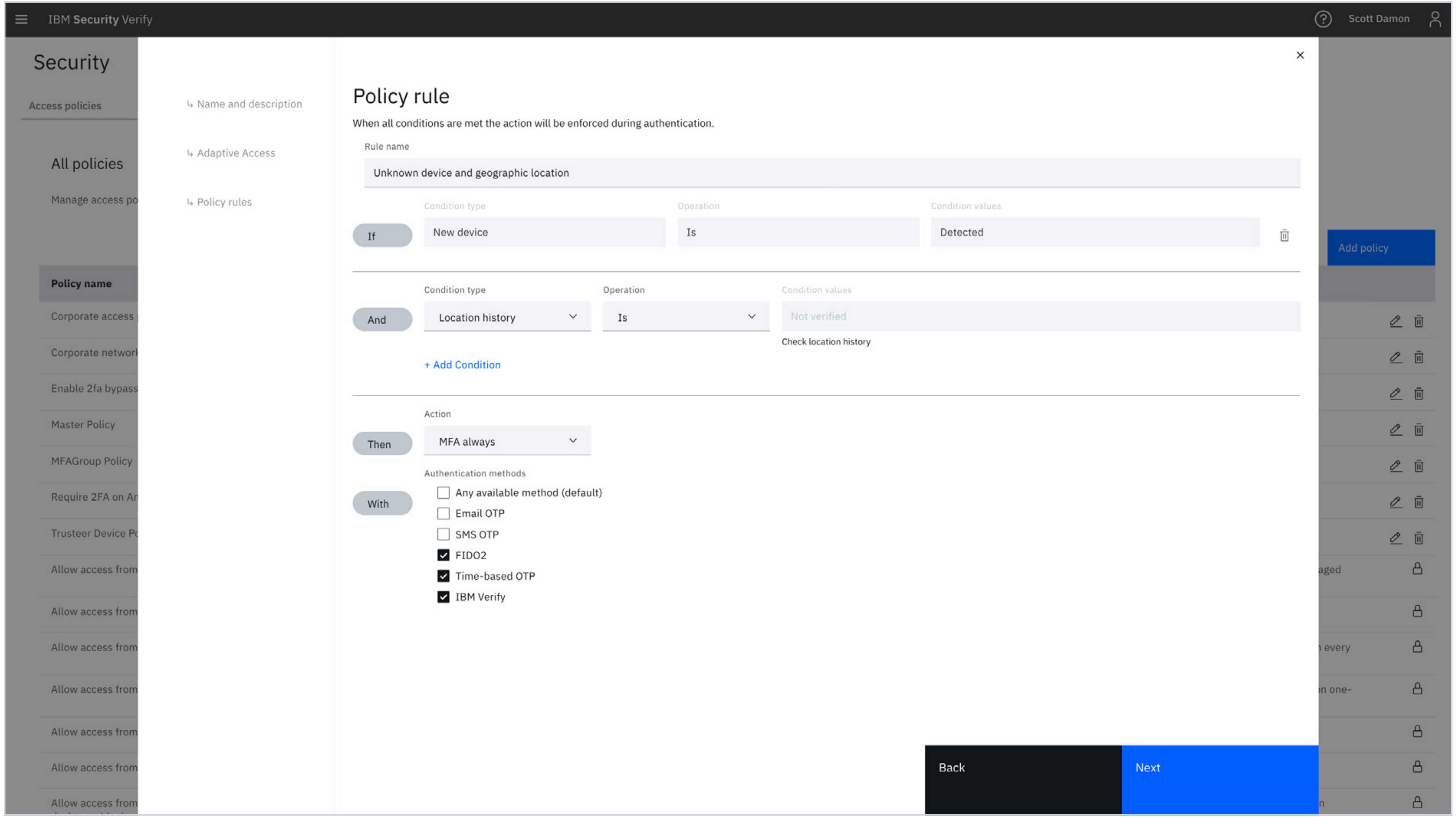
Employee | Business manager | IT administrator | Monitor activity | **Customize policies** | Manage users and identities | Add applications | Analyze risk | Developer

Back
Next

IT administrator: 1 of 5
Manage users and identity sources

Manager users

Scott can onboard new users with a simple configuration interface. He can add attributes from scratch or choose to pull in data from various identity sources like the Cloud Directory, Active Directory, or an IBMid.



Policy rule

When all conditions are met the action will be enforced during authentication.

Rule name: Unknown device and geographic location

	Condition type	Operation	Condition values
If	New device	Is	Detected
And	Location history	Is	Not verified Check location history

+ Add Condition

Then — Action: MFA always

With — Authentication methods

- ☐ Any available method (default)
- ☐ Email OTP
- ☐ SMS OTP
- ☑ FIDO2
- ☑ Time-based OTP
- ☑ IBM Verify

Next:
Manage groups

← →

Employee — Business manager — IT administrator — Monitor activity — Customize policies — **Manage users and identities** — Add applications — Analyze risk — Developer

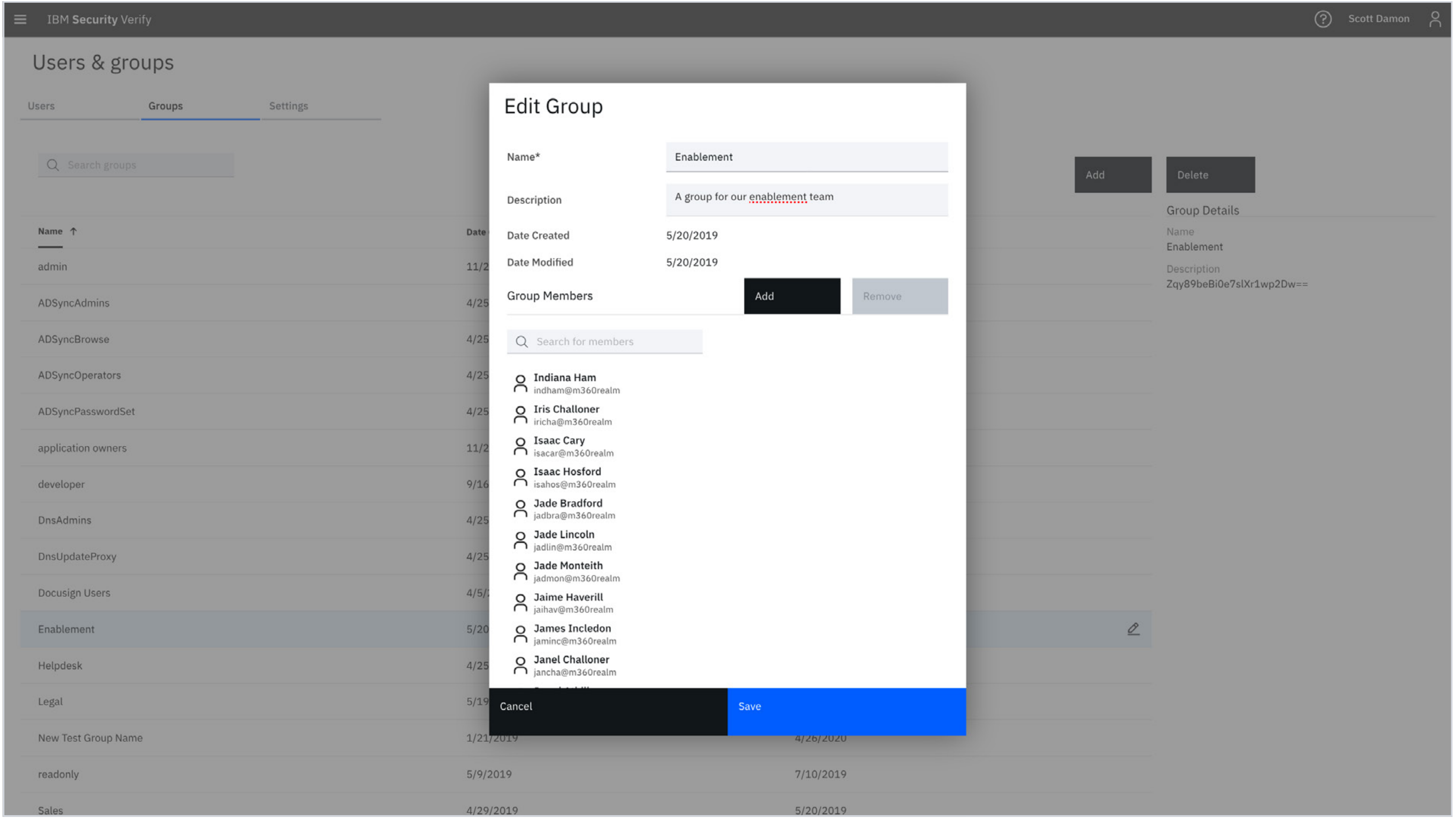
IBM **Security** Verify

Try Verify Now

IT administrator: 2 of 5
Manage users and identity sources

Manage groups

Whether organized by department, role, or a more unique attribute, groups can help make access more modular within an organization. For instance, Scott can add a new Bane & Dox Co. Sales group to help that collection of individuals access common sales applications. If he integrates an existing directory into Verify, that directory's groups will be preserved.



Users & groups

Users | Groups | Settings

Search groups

Name ↑	Date	
admin	11/2	
ADSyncAdmins	4/25	
ADSyncBrowse	4/25	
ADSyncOperators	4/25	
ADSyncPasswordSet	4/25	
application owners	11/2	
developer	9/16	
DnsAdmins	4/25	
DnsUpdateProxy	4/25	
Docusign Users	4/5/	
Enablement	5/20	
Helpdesk	4/25	
Legal	5/19	
New Test Group Name	1/21/2019	4/26/2020
readonly	5/9/2019	7/10/2019
Sales	4/29/2019	5/20/2019

Add Delete

Group Details
Name
Enablement
Description
Zqy89beBi0e7slXr1wp2Dw==

Edit Group

Name*: Enablement
Description: A group for our enablement team
Date Created: 5/20/2019
Date Modified: 5/20/2019

Group Members — Add | Remove

Search for members

- Indiana Ham indham@m360realm
- Iris Challoner iricha@m360realm
- Isaac Cary isacar@m360realm
- Isaac Hosford isahos@m360realm
- Jade Bradford jadbra@m360realm
- Jade Lincoln jadlin@m360realm
- Jade Monteith jadmon@m360realm
- Jaime Haverill jaihav@m360realm
- James Incledon jaminc@m360realm
- Janel Challoner jancha@m360realm

Cancel | Save

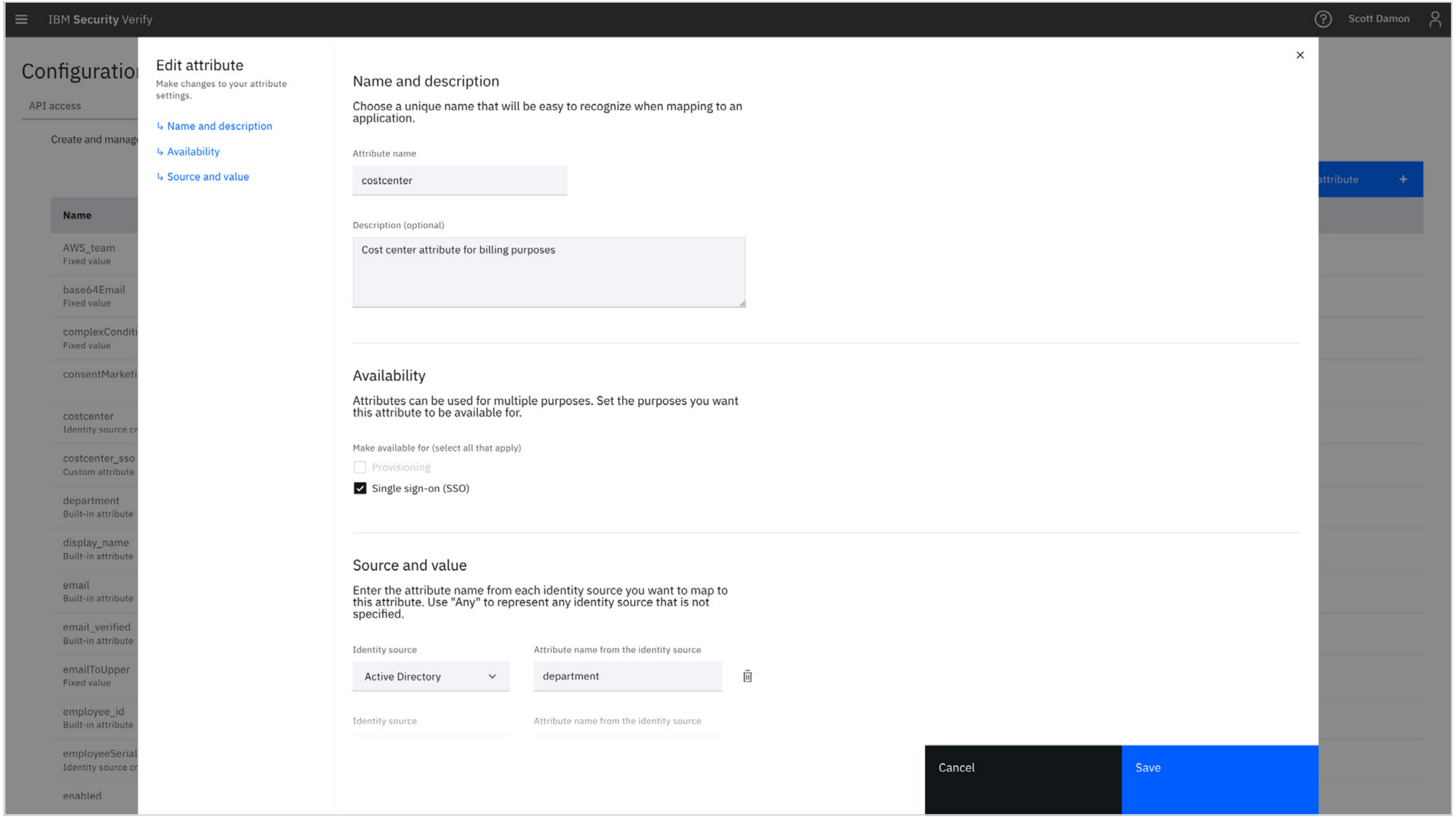
Next:
Manage user attributes

← →

IT administrator: 3 of 5
Manage users and identity sources

Manage user attributes

While Verify includes dozens of the most common user attributes by default, Scott can link additional attributes from any of his connected identity sources or create custom attributes when needed. These attributes can then be referenced in identity sources and applications for single sign-on, provisioning, creating profiles, and more.



Edit attribute
Make changes to your attribute settings.

↳ Name and description
↳ Availability
↳ Source and value

Name and description

Choose a unique name that will be easy to recognize when mapping to an application.

Attribute name: costcenter

Description (optional): Cost center attribute for billing purposes

Availability

Attributes can be used for multiple purposes. Set the purposes you want this attribute to be available for.

Make available for (select all that apply)

□ Provisioning
☑ Single sign-on (SSO)

Source and value

Enter the attribute name from each identity source you want to map to this attribute. Use "Any" to represent any identity source that is not specified.

Identity source	Attribute name from the identity source
Active Directory	department
Identity source	Attribute name from the identity source

Cancel Save

Next:
Active Directory and LDAP

← →

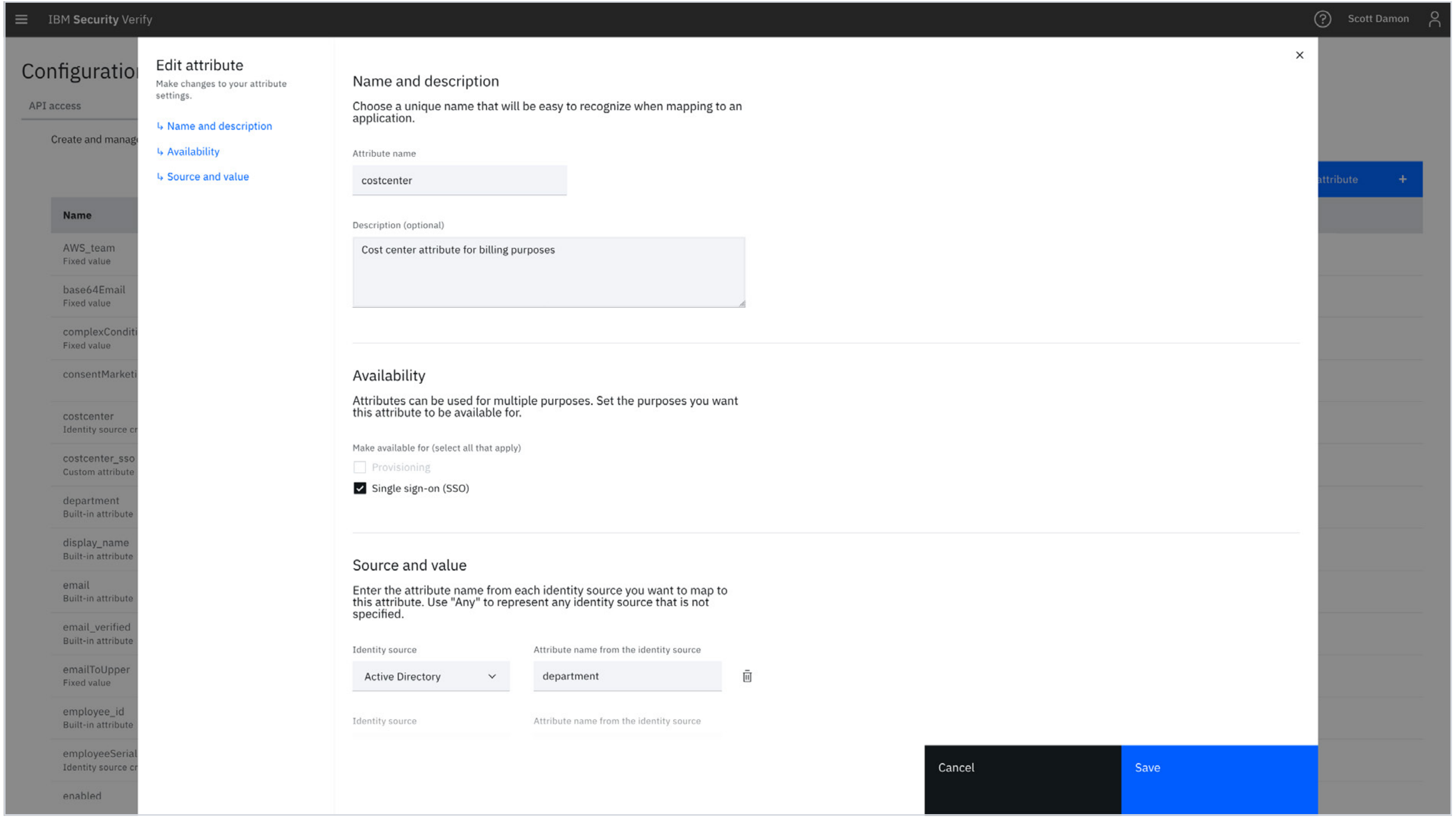
Employee
Business manager
IT administrator
Monitor activity
Customize policies
Manage users and identities
Add applications
Analyze risk
Developer

IT administrator: 4 of 5

Manage users and identity sources

Active directory and LDAP

Scott can configure Verify to connect to an existing Active Directory or LDAP identity source or even non-standard directories, databases, or external services.



Configuratio

API access

Create and manag

Name
AWS_team Fixed value
base64Email Fixed value
complexConditi Fixed value
consentMarketi
costcenter Identity source cr
costcenter_sso Custom attribute
department Built-in attribute
display_name Built-in attribute
email Built-in attribute
email_verified Built-in attribute
emailToUpper Fixed value
employee_id Built-in attribute
employeeSerial Identity source cr
enabled

Edit attribute

Make changes to your attribute settings.

Name and description

Choose a unique name that will be easy to recognize when mapping to an application.

Attribute name: costcenter

Description (optional): Cost center attribute for billing purposes

Availability

Attributes can be used for multiple purposes. Set the purposes you want this attribute to be available for.

Make available for (select all that apply)

- □ Provisioning
- ☑ Single sign-on (SSO)

Source and value

Enter the attribute name from each identity source you want to map to this attribute. Use "Any" to represent any identity source that is not specified.

Identity source	Attribute name from the identity source
Active Directory	department

Identity source

Attribute name from the identity source

Next:

Social login

← →

Employee · Business manager · IT administrator · Monitor activity · Customize policies · **Manage users and identities** · Add applications · Analyze risk · Developer

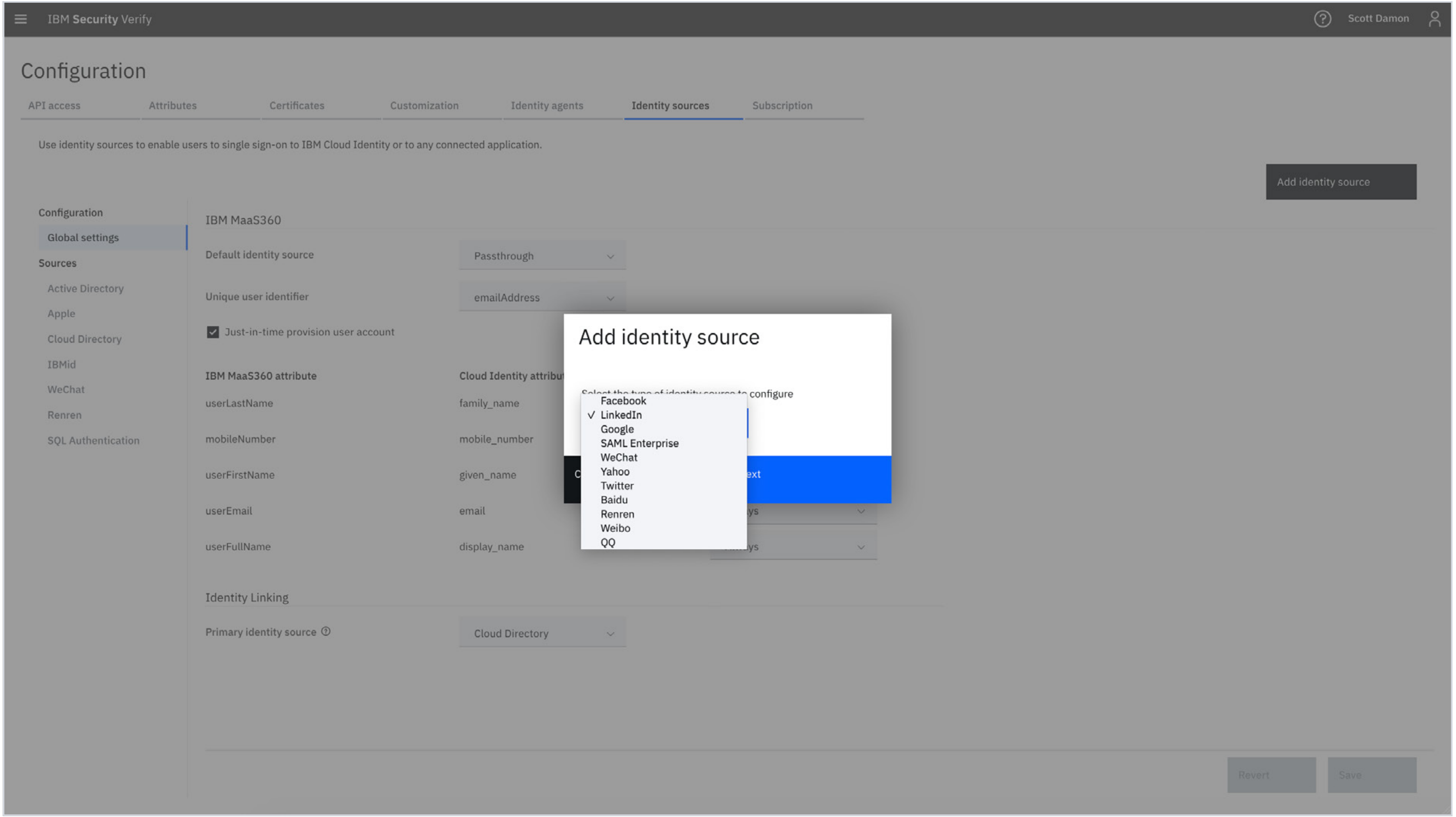
Back

Next

IT administrator: 5 of 5
Manage users and identity sources

Social login

Scott can also link a wide array of social login providers to offer more options for his users, from Google and LinkedIn to more region-specific providers.



Use identity sources to enable users to single sign-on to IBM Cloud Identity or to any connected application.

IBM MaaS360

Default identity source: Passthrough

Unique user identifier: emailAddress

☑ Just-in-time provision user account

IBM MaaS360 attribute	Cloud Identity attribu
userLastName	family_name
mobileNumber	mobile_number
userFirstName	given_name
userEmail	email
userFullName	display_name

Identity Linking

Primary identity source: Cloud Directory

Add identity source

Select the type of identity source to configure

- Facebook
- ✓ LinkedIn
- Google
- SAML Enterprise
- WeChat
- Yahoo
- Twitter
- Baidu
- Renren
- Weibo
- QQ

Next:
View applications

← →

Employee
Business manager
IT administrator
Monitor activity
Customize policies
Manage users and identities
Add applications
Analyze risk
Developer

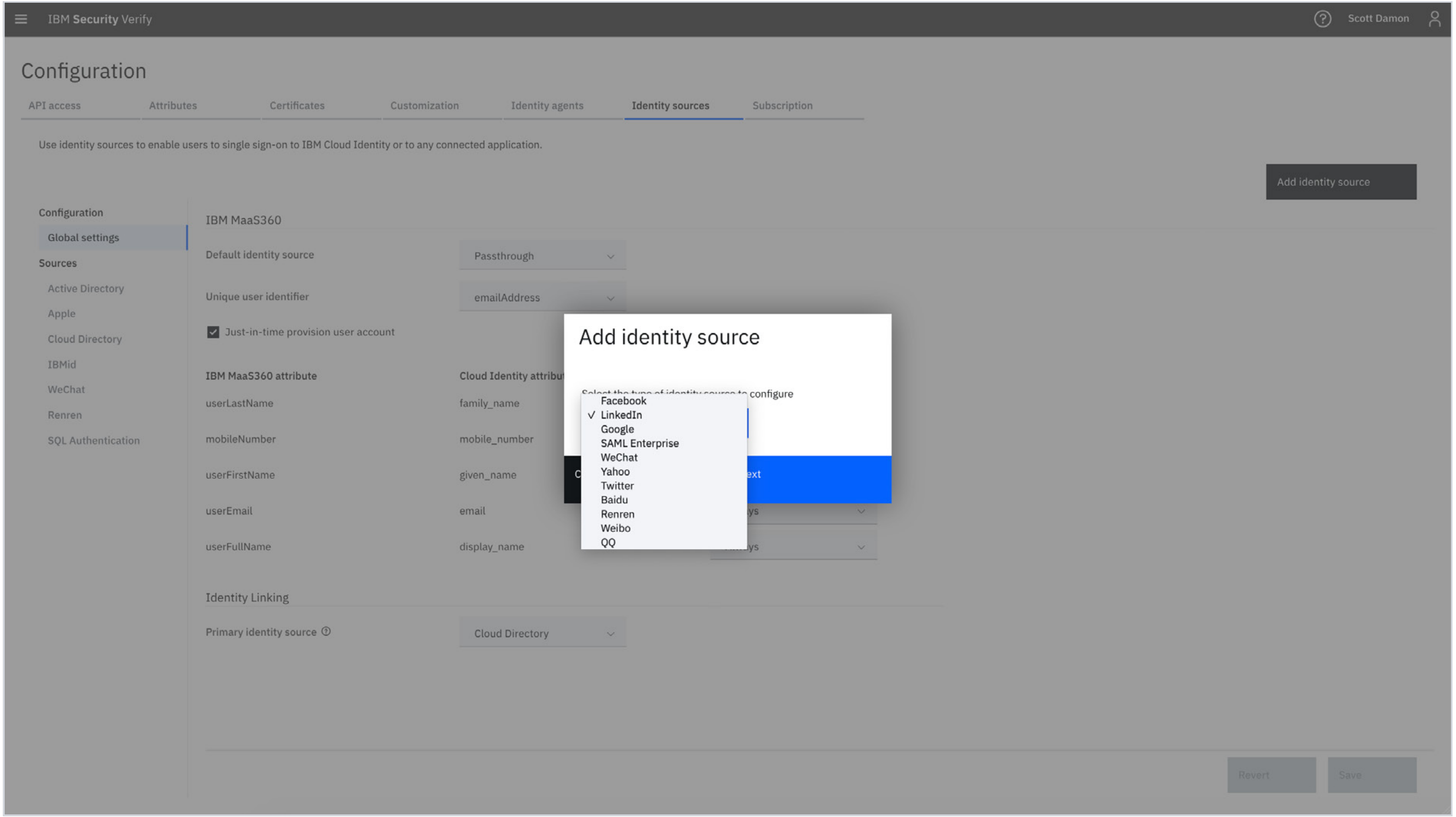
IBM **Security** Verify

Try Verify Now

IT administrator: 1 of 6
Add applications

View applications

Verify supports hundreds of SaaS applications out of the box, enables streamlined integration of custom apps, and provides a lightweight application gateway to extend support to on-premises apps as well. Scott can manage all of his organization's apps from a single interface.



Configuration

Use identity sources to enable users to single sign-on to IBM Cloud Identity or to any connected application.

IBM MaaS360

Default identity source: Passthrough

Unique user identifier: emailAddress

☑ Just-in-time provision user account

IBM MaaS360 attribute	Cloud Identity attribu
userLastName	family_name
mobileNumber	mobile_number
userFirstName	given_name
userEmail	email
userFullName	display_name

Identity Linking

Primary identity source: Cloud Directory

Add identity source

Select the type of identity source to configure

Next:
Search for application to add

←　→

○ Employee
○ Business manager
● IT administrator
● Monitor activity
● Customize policies
● Manage users and identities
● **Add applications**
○ Analyze risk
○ Developer

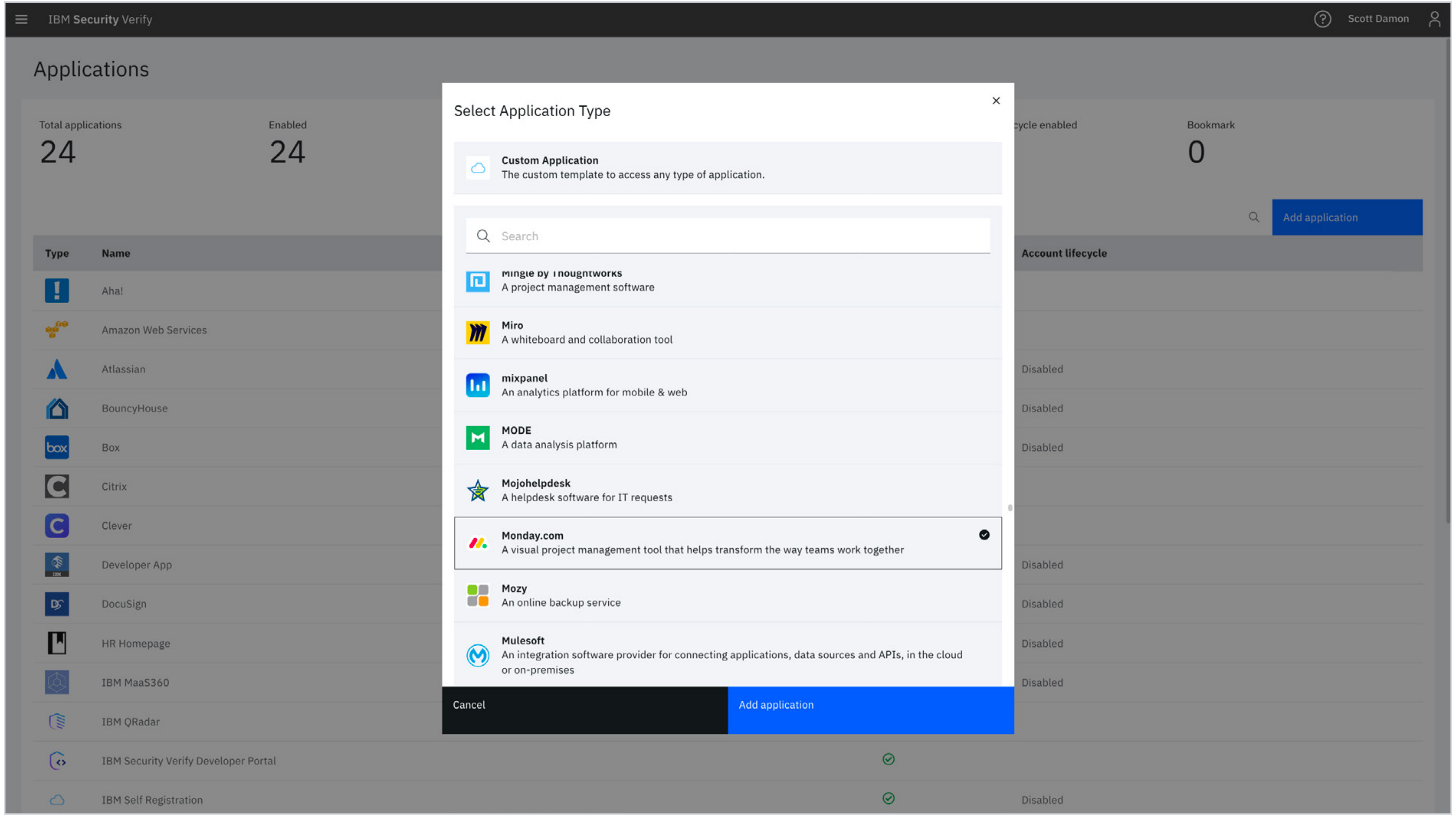
Back
Next

IT administrator: 2 of 6

Add applications

Search for application to add

Scott can search for a new application to add, like Monday.com. With pre-built SaaS connectors, integrating new applications into federated single sign-on is straightforward.



Applications

Total applications 24

Enabled 24

...cycle enabled

Bookmark 0

Type	Name		Account lifecycle
	Aha!		
	Amazon Web Services		
	Atlassian		Disabled
	BouncyHouse		Disabled
	Box		Disabled
	Citrix		
	Clever		
	Developer App		Disabled
	DocuSign		Disabled
	HR Homepage		Disabled
	IBM MaaS360		Disabled
	IBM QRadar		
	IBM Security Verify Developer Portal	✓	
	IBM Self Registration	✓	Disabled

Select Application Type

Custom Application
The custom template to access any type of application.

Search

Mingle by Thoughtworks
A project management software

Miro
A whiteboard and collaboration tool

mixpanel
An analytics platform for mobile & web

MODE
A data analysis platform

Mojohelpdesk
A helpdesk software for IT requests

Monday.com ✓
A visual project management tool that helps transform the way teams work together

Mozy
An online backup service

Mulesoft
An integration software provider for connecting applications, data sources and APIs, in the cloud or on-premises

Next:
Add owner for access approvals

← →

○ Employee
○ Business manager
● IT administrator
● Monitor activity
● Customize policies
● Manage users and identities
● **Add applications**
○ Analyze risk
○ Developer

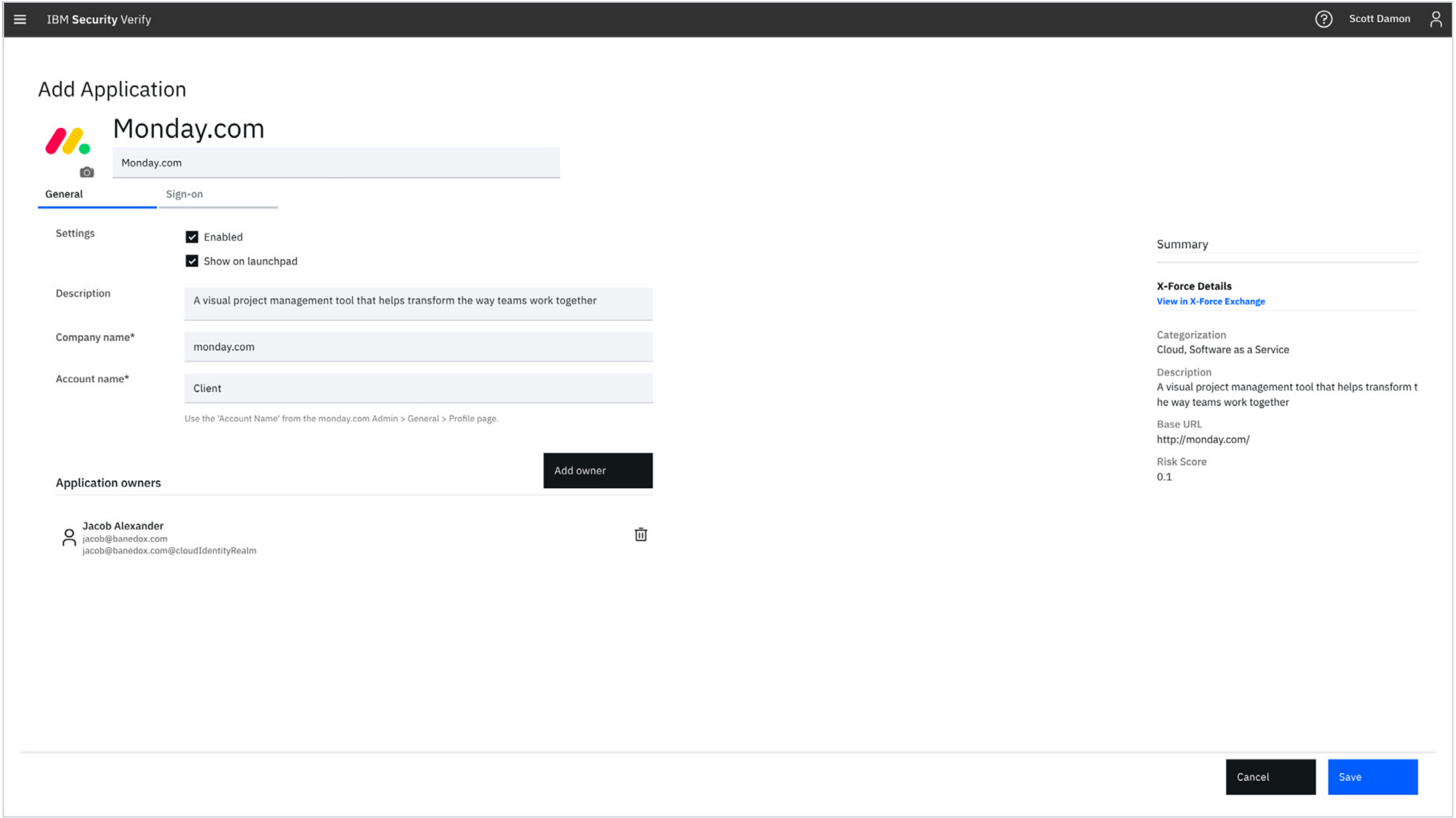
IBM **Security** Verify

Try Verify Now

IT administrator: 3 of 6
Add applications

Add owner for access approvals

To manage ongoing operations with the app, Scott can assign an application owner and approver(s) for access requests.



IBM **Security** Verify — Scott Damon

Add Application

Monday.com

Monday.com

General | Sign-on

Settings
☑ Enabled
☑ Show on launchpad

Description: A visual project management tool that helps transform the way teams work together

Company name*: monday.com

Account name*: Client

Use the 'Account Name' from the monday.com Admin > General > Profile page.

Application owners — Add owner

Jacob Alexander
jacob@banedox.com
jacob@banedox.com@cloudIdentityRealm

Summary

X-Force Details
View in X-Force Exchange

Categorization
Cloud, Software as a Service

Description
A visual project management tool that helps transform t he way teams work together

Base URL
http://monday.com/

Risk Score
0.1

Cancel | Save

Next:
Configure sign-on settings

← →

Employee | Business manager | IT administrator | Monitor activity | Customize policies | Manage users and identities | **Add applications** | Analyze risk | Developer

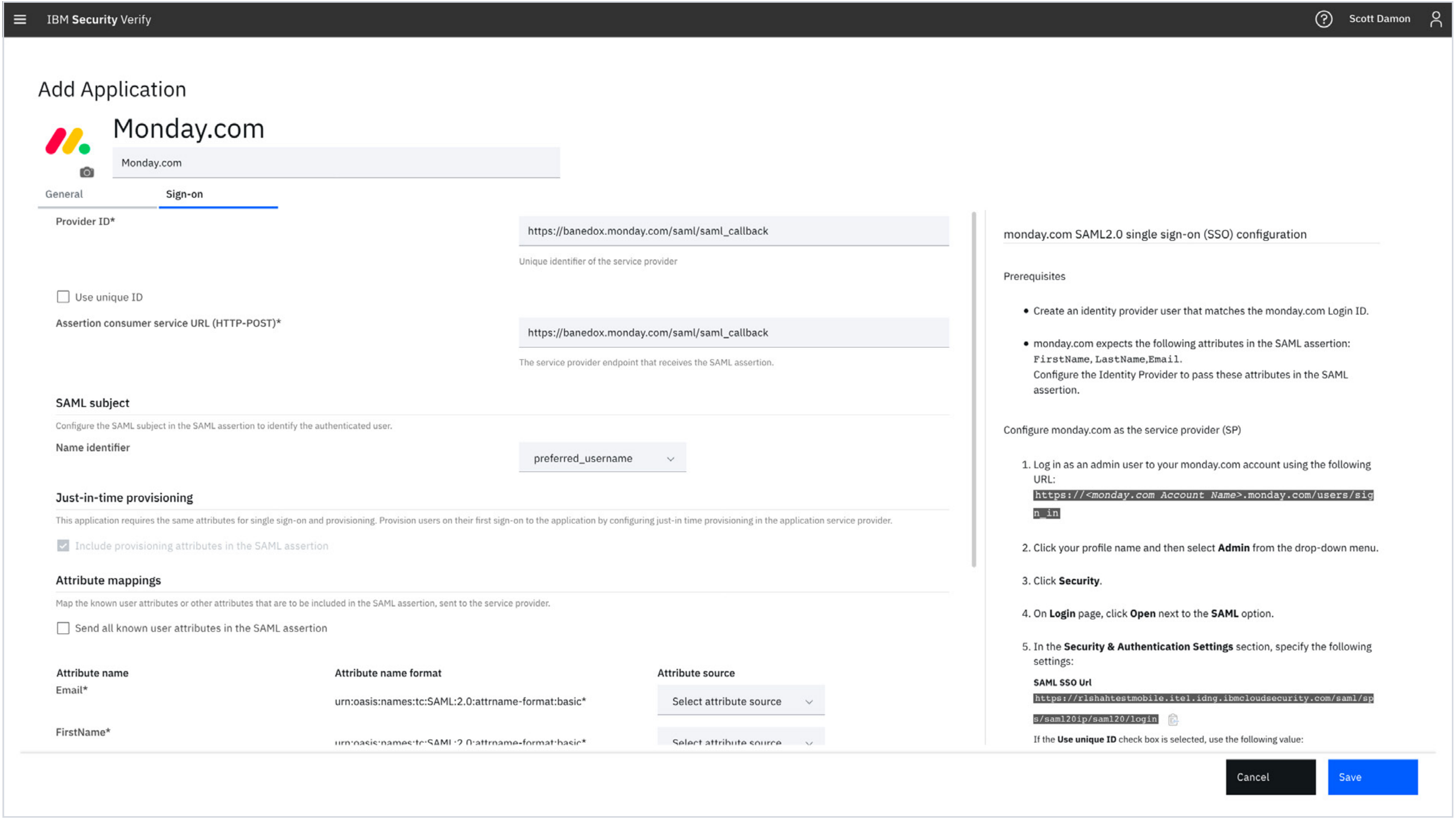
Back | Next

IT administrator: 4 of 6
Add applications

Configure sign-on settings

In the Sign-on tab, Scott can configure the required parameters for the application to appropriately integrate with Verify, with application-specific instructions to help. Further down the page, he can configure other aspects of the integration like mapping which attributes are to be sent to the service provider, as well the access policy to apply to the application.

Next:
Configure entitlements



Add Application

Monday.com

Monday.com

Provider ID* https://banedox.monday.com/saml/saml_callback
Unique identifier of the service provider

□ Use unique ID

Assertion consumer service URL (HTTP-POST)* https://banedox.monday.com/saml/saml_callback
The service provider endpoint that receives the SAML assertion.

SAML subject
Configure the SAML subject in the SAML assertion to identify the authenticated user.
Name identifier preferred_username

Just-in-time provisioning
This application requires the same attributes for single sign-on and provisioning. Provision users on their first sign-on to the application by configuring just-in time provisioning in the application service provider.
☑ Include provisioning attributes in the SAML assertion

Attribute mappings
Map the known user attributes or other attributes that are to be included in the SAML assertion, sent to the service provider.
□ Send all known user attributes in the SAML assertion

Attribute name	Attribute name format	Attribute source
Email*	urn:oasis:names:tc:SAML:2.0:attrname-format:basic*	Select attribute source
FirstName*	urn:oasis:names:tc:SAML:2.0:attrname-format:basic*	Select attribute source

monday.com SAML2.0 single sign-on (SSO) configuration

Prerequisites

- Create an identity provider user that matches the monday.com Login ID.
- monday.com expects the following attributes in the SAML assertion: `FirstName, LastName,Email`.
  Configure the Identity Provider to pass these attributes in the SAML assertion.

Configure monday.com as the service provider (SP)

1. Log in as an admin user to your monday.com account using the following URL: `https://<monday.com Account Name>.monday.com/users/sign_in`
2. Click your profile name and then select **Admin** from the drop-down menu.
3. Click **Security**.
4. On **Login** page, click **Open** next to the **SAML** option.
5. In the **Security & Authentication Settings** section, specify the following settings:
   SAML SSO Url
   `https://rlshahtestmobile.itel.idng.ibmcloudsecurity.com/saml/sps/saml20ip/saml20/login`
   If the **Use unique ID** check box is selected, use the following value:

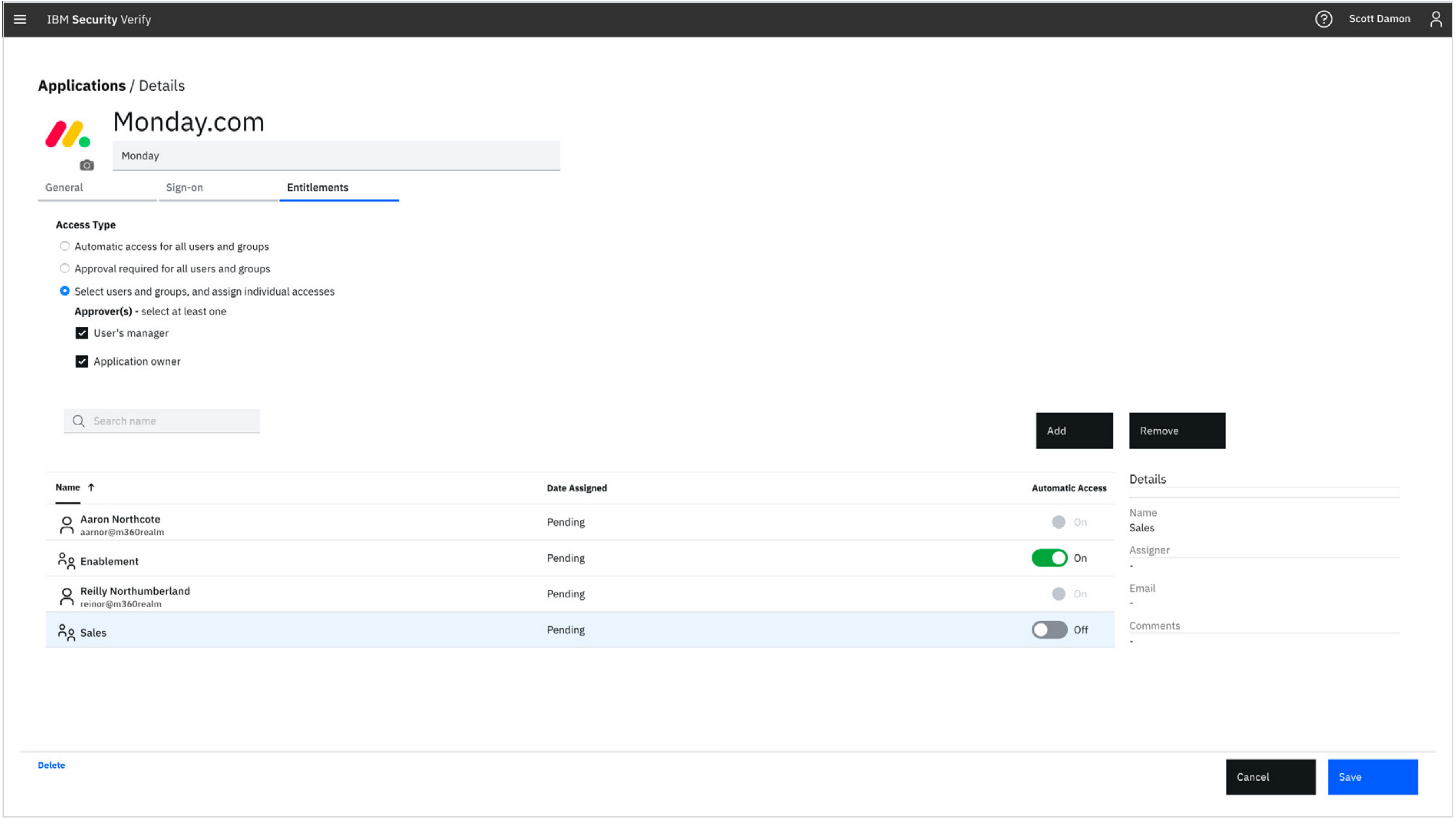
Employee
Business manager
IT administrator
Monitor activity
Customize policies
Manage users and identities
Add applications
Analyze risk
Developer

IT administrator: 5 of 6

Add applications

Configure entitlements

In the Entitlements tab, Scott can configure the level of access and approval logistics appropriate for the application. In this case, he chooses a particular set of users and groups.



Applications / Details

Monday.com

Monday

Access Type

○ Automatic access for all users and groups

○ Approval required for all users and groups

● Select users and groups, and assign individual accesses

Approver(s) - select at least one

☑ User's manager

☑ Application owner

Name ↑	Date Assigned	Automatic Access
Aaron Northcote aarnor@m360realm	Pending	On
Enablement	Pending	On
Reilly Northumberland reinor@m360realm	Pending	On
Sales	Pending	Off

Details

Name
Sales

Assigner
-

Email
-

Comments
-

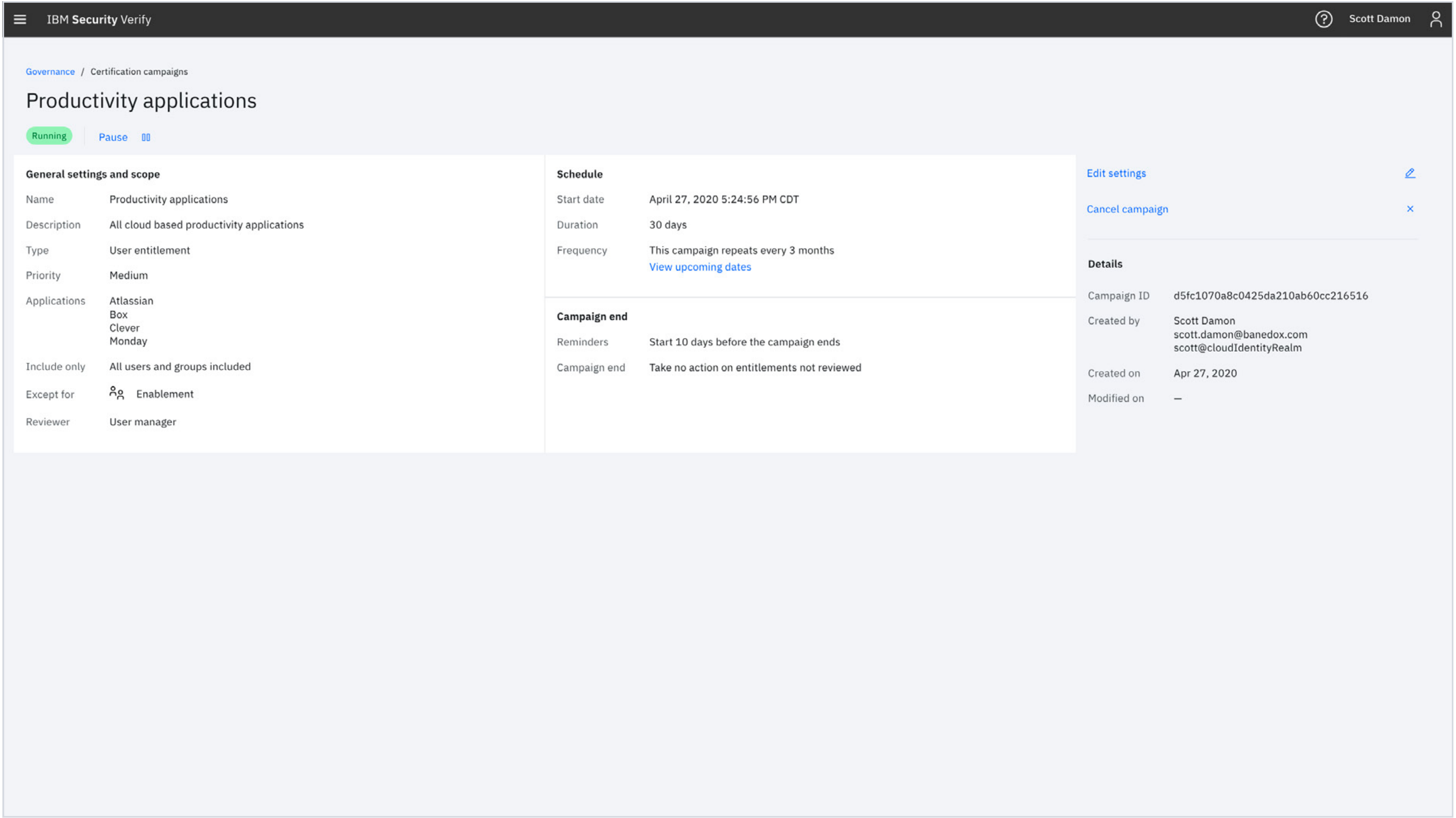
Next:
Set periodic access recertification

IT administrator: 6 of 6

Add applications

Set periodic access recertification

Over time, it can be difficult for an organization to efficiently recertify applications to ensure levels of access are still appropriate. To ensure this important step isn't missed, Scott can set periodic recertification campaigns on a per-app basis to automate this aspect of identity governance.



Productivity applications

General settings and scope

Name	Productivity applications
Description	All cloud based productivity applications
Type	User entitlement
Priority	Medium
Applications	Atlassian Box Clever Monday
Include only	All users and groups included
Except for	Enablement
Reviewer	User manager

Schedule

Start date	April 27, 2020 5:24:56 PM CDT
Duration	30 days
Frequency	This campaign repeats every 3 months View upcoming dates

Campaign end

Reminders	Start 10 days before the campaign ends
Campaign end	Take no action on entitlements not reviewed

Details

Campaign ID	d5fc1070a8c0425da210ab60cc216516
Created by	Scott Damon scott.damon@banedox.com scott@cloudIdentityRealm
Created on	Apr 27, 2020
Modified on	—

Next:
Analytics dashboard

← →

Employee · Business manager · IT administrator · Monitor activity · Customize policies · Manage users and identities · **Add applications** · Analyze risk · Developer

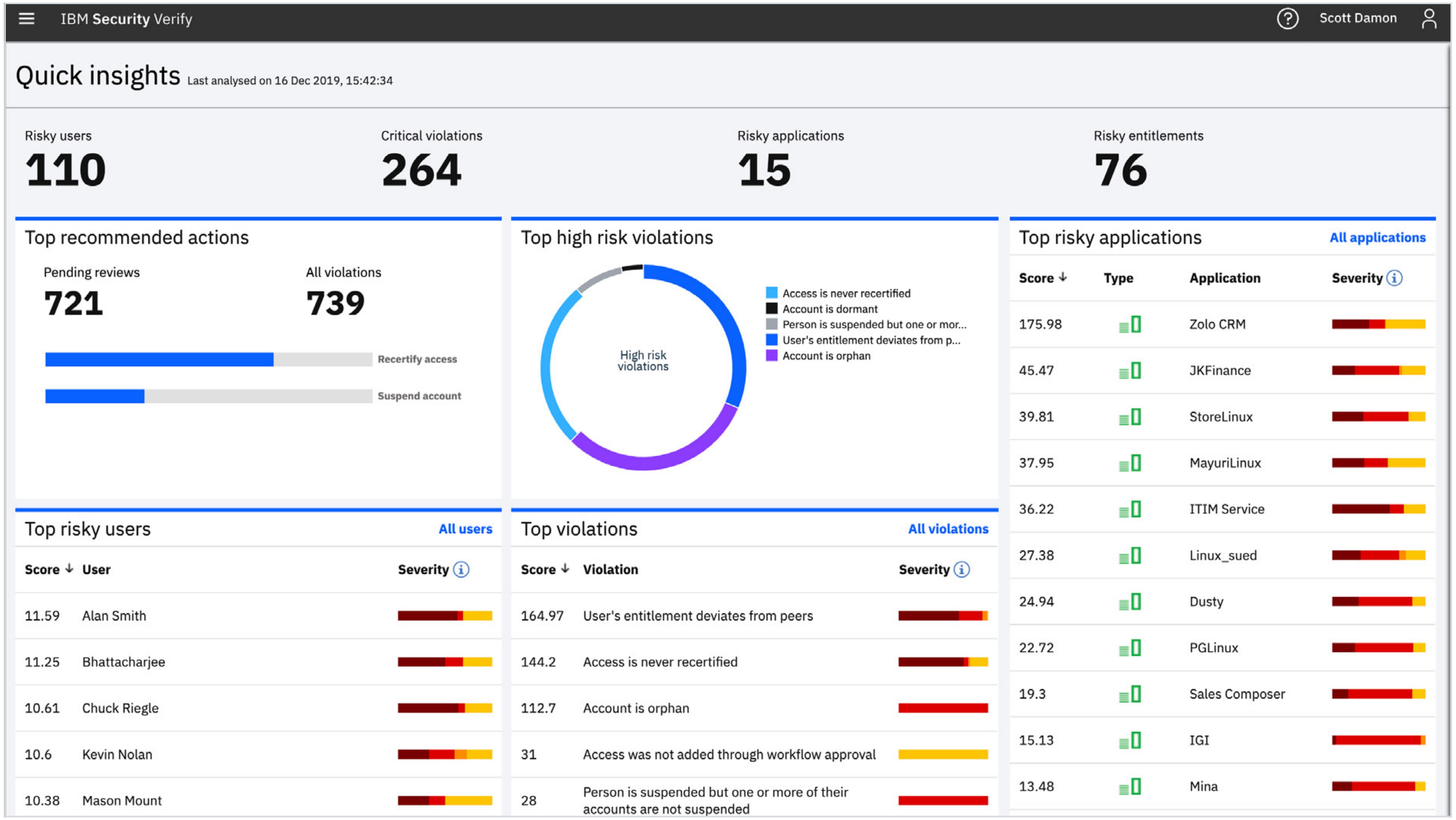
IBM **Security** Verify

Try Verify Now

IT administrator: 1 of 3
Analyze risk

Analytics dashboard

Scott can review the overall health of his IAM environment in the identity analytics dashboard, where he can quickly scan for identity-related risks across users, entitlements, and applications. He can dig deeper into individual users and applications for further insight into violations and accumulated risk scores.



IBM Security Verify — Scott Damon

Quick insights

Last analysed on 16 Dec 2019, 15:42:34

Risky users	Critical violations	Risky applications	Risky entitlements
110	264	15	76

Top recommended actions

Pending reviews	All violations
721	739

Recertify access
Suspend account

Top high risk violations

High risk violations
Access is never recertified
Account is dormant
Person is suspended but one or mor...
User's entitlement deviates from p...
Account is orphan

Top risky applications

All applications

Score ↓	Type	Application	Severity ⓘ
175.98		Zolo CRM	
45.47		JKFinance	
39.81		StoreLinux	
37.95		MayuriLinux	
36.22		ITIM Service	
27.38		Linux_sued	
24.94		Dusty	
22.72		PGLinux	
19.3		Sales Composer	
15.13		IGI	
13.48		Mina	

Top risky users

All users

Score ↓	User	Severity ⓘ
11.59	Alan Smith	
11.25	Bhattacharjee	
10.61	Chuck Riegle	
10.6	Kevin Nolan	
10.38	Mason Mount	

Top violations

All violations

Score ↓	Violation	Severity ⓘ
164.97	User's entitlement deviates from peers	
144.2	Access is never recertified	
112.7	Account is orphan	
31	Access was not added through workflow approval	
28	Person is suspended but one or more of their accounts are not suspended	

Next:
View ranked policy violations

← →

Employee · Business manager · IT administrator · Monitor activity · Customize policies · Manage users and identities · Add applications · **Analyze risk** · Developer

Back Next

IBM **Security** Verify

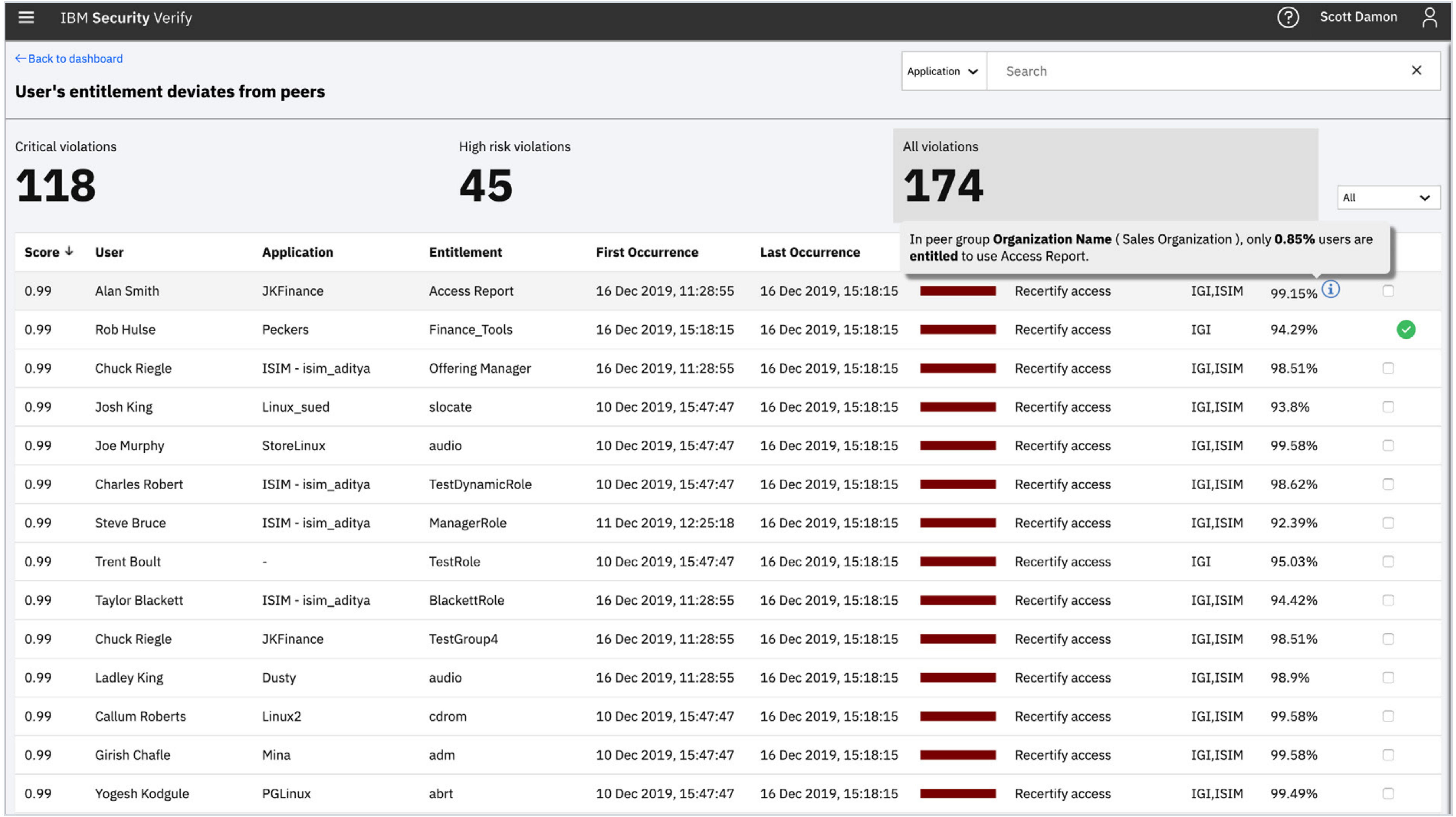
Try Verify Now

IT administrator: 2 of 3

Analyze risk

View ranked policy violations

Scott can highlight anomalies and view ranked violations within a policy category such as this “user’s entitlement deviates from peers” view. This particular policy within identity analytics performs peer group analysis to identify contextually atypical entitlements that may introduce additional risk.



User's entitlement deviates from peers

Critical violations **118**

High risk violations **45**

All violations **174**

All

In peer group **Organization Name** (Sales Organization), only **0.85%** users are **entitled** to use Access Report.

Score ↓	User	Application	Entitlement	First Occurrence	Last Occurrence					
0.99	Alan Smith	JKFinance	Access Report	16 Dec 2019, 11:28:55	16 Dec 2019, 15:18:15	▬	Recertify access	IGI,ISIM	99.15% ⓘ	□
0.99	Rob Hulse	Peckers	Finance_Tools	16 Dec 2019, 15:18:15	16 Dec 2019, 15:18:15	▬	Recertify access	IGI	94.29%	✓
0.99	Chuck Riegle	ISIM - isim_aditya	Offering Manager	16 Dec 2019, 11:28:55	16 Dec 2019, 15:18:15	▬	Recertify access	IGI,ISIM	98.51%	□
0.99	Josh King	Linux_sued	slocate	10 Dec 2019, 15:47:47	16 Dec 2019, 15:18:15	▬	Recertify access	IGI,ISIM	93.8%	□
0.99	Joe Murphy	StoreLinux	audio	10 Dec 2019, 15:47:47	16 Dec 2019, 15:18:15	▬	Recertify access	IGI,ISIM	99.58%	□
0.99	Charles Robert	ISIM - isim_aditya	TestDynamicRole	10 Dec 2019, 15:47:47	16 Dec 2019, 15:18:15	▬	Recertify access	IGI,ISIM	98.62%	□
0.99	Steve Bruce	ISIM - isim_aditya	ManagerRole	11 Dec 2019, 12:25:18	16 Dec 2019, 15:18:15	▬	Recertify access	IGI,ISIM	92.39%	□
0.99	Trent Boult	-	TestRole	10 Dec 2019, 15:47:47	16 Dec 2019, 15:18:15	▬	Recertify access	IGI	95.03%	□
0.99	Taylor Blackett	ISIM - isim_aditya	BlackettRole	16 Dec 2019, 11:28:55	16 Dec 2019, 15:18:15	▬	Recertify access	IGI,ISIM	94.42%	□
0.99	Chuck Riegle	JKFinance	TestGroup4	16 Dec 2019, 11:28:55	16 Dec 2019, 15:18:15	▬	Recertify access	IGI,ISIM	98.51%	□
0.99	Ladley King	Dusty	audio	16 Dec 2019, 11:28:55	16 Dec 2019, 15:18:15	▬	Recertify access	IGI,ISIM	98.9%	□
0.99	Callum Roberts	Linux2	cdrom	10 Dec 2019, 15:47:47	16 Dec 2019, 15:18:15	▬	Recertify access	IGI,ISIM	99.58%	□
0.99	Girish Chafle	Mina	adm	10 Dec 2019, 15:47:47	16 Dec 2019, 15:18:15	▬	Recertify access	IGI,ISIM	99.58%	□
0.99	Yogesh Kodgule	PGLinux	abrt	10 Dec 2019, 15:47:47	16 Dec 2019, 15:18:15	▬	Recertify access	IGI,ISIM	99.49%	□

Next:
Take suggested remediation actions

← →

○ Employee ○ Business manager ● IT administrator ● Monitor activity ● Customize policies ● Manage users and identities ● Add applications ● **Analyze risk** ○ Developer

Back Next

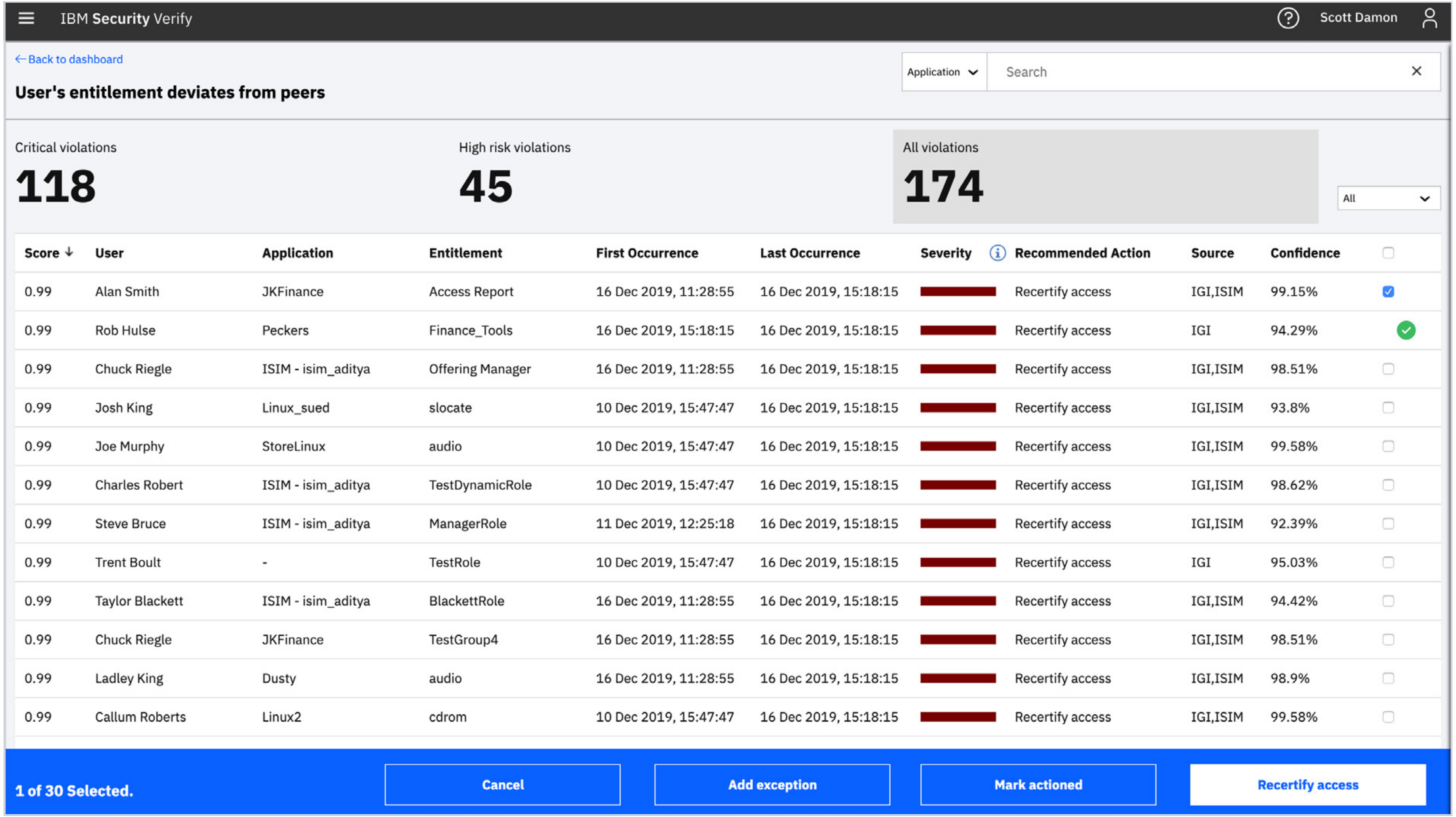
IBM **Security** Verify

Try Verify Now

IT administrator: 3 of 3
Analyze risk

Take suggested remediation actions

For each policy violation, Verify also suggests a remediation action like recertifying access, alongside AI-powered risk and confidence scores. Scott can perform the recertification request from within the identity analytics dashboard.



User's entitlement deviates from peers

Critical violations **118**

High risk violations **45**

All violations **174**

Score ↓	User	Application	Entitlement	First Occurrence	Last Occurrence	Severity ⓘ	Recommended Action	Source	Confidence	□
0.99	Alan Smith	JKFinance	Access Report	16 Dec 2019, 11:28:55	16 Dec 2019, 15:18:15	🟥	Recertify access	IGI,ISIM	99.15%	☑
0.99	Rob Hulse	Peckers	Finance_Tools	16 Dec 2019, 15:18:15	16 Dec 2019, 15:18:15	🟥	Recertify access	IGI	94.29%	✓
0.99	Chuck Riegle	ISIM - isim_aditya	Offering Manager	16 Dec 2019, 11:28:55	16 Dec 2019, 15:18:15	🟥	Recertify access	IGI,ISIM	98.51%	□
0.99	Josh King	Linux_sued	slocate	10 Dec 2019, 15:47:47	16 Dec 2019, 15:18:15	🟥	Recertify access	IGI,ISIM	93.8%	□
0.99	Joe Murphy	StoreLinux	audio	10 Dec 2019, 15:47:47	16 Dec 2019, 15:18:15	🟥	Recertify access	IGI,ISIM	99.58%	□
0.99	Charles Robert	ISIM - isim_aditya	TestDynamicRole	10 Dec 2019, 15:47:47	16 Dec 2019, 15:18:15	🟥	Recertify access	IGI,ISIM	98.62%	□
0.99	Steve Bruce	ISIM - isim_aditya	ManagerRole	11 Dec 2019, 12:25:18	16 Dec 2019, 15:18:15	🟥	Recertify access	IGI,ISIM	92.39%	□
0.99	Trent Boult	-	TestRole	10 Dec 2019, 15:47:47	16 Dec 2019, 15:18:15	🟥	Recertify access	IGI	95.03%	□
0.99	Taylor Blackett	ISIM - isim_aditya	BlackettRole	16 Dec 2019, 11:28:55	16 Dec 2019, 15:18:15	🟥	Recertify access	IGI,ISIM	94.42%	□
0.99	Chuck Riegle	JKFinance	TestGroup4	16 Dec 2019, 11:28:55	16 Dec 2019, 15:18:15	🟥	Recertify access	IGI,ISIM	98.51%	□
0.99	Ladley King	Dusty	audio	16 Dec 2019, 11:28:55	16 Dec 2019, 15:18:15	🟥	Recertify access	IGI,ISIM	98.9%	□
0.99	Callum Roberts	Linux2	cdrom	10 Dec 2019, 15:47:47	16 Dec 2019, 15:18:15	🟥	Recertify access	IGI,ISIM	99.58%	□

1 of 30 Selected.

Next:
Developer

← →

○ Employee ○ Business manager ● IT administrator ● Monitor activity ● Customize policies ● Manage users and identities ● Add applications ● **Analyze risk** ○ Developer

Back Next

Developer

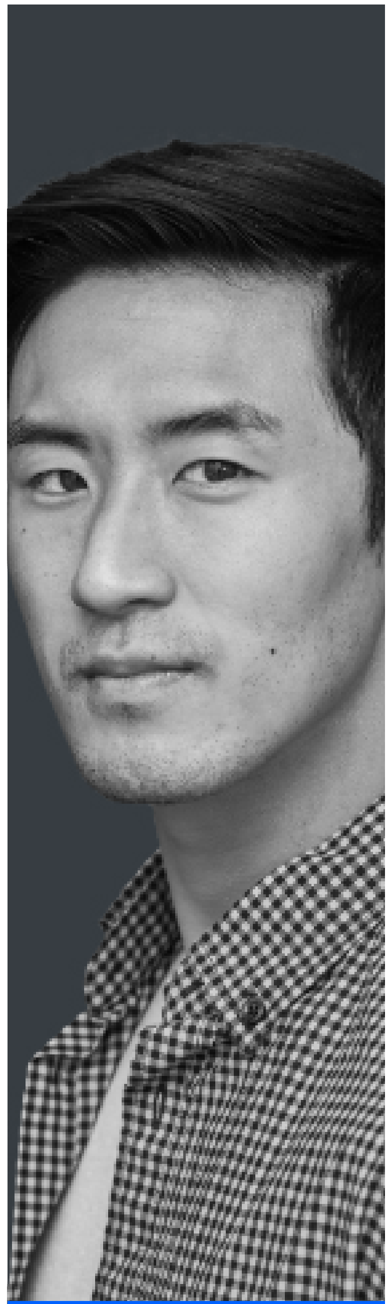
Embed access and authentication into custom applications with intuitive, purpose-built APIs.

Developers need to build run-time flows for authentication, give users registration capabilities, and embed MFA into their applications, without necessarily being an IAM expert. To do this efficiently, they need robust APIs and documentation, sample code, and guided instructions.

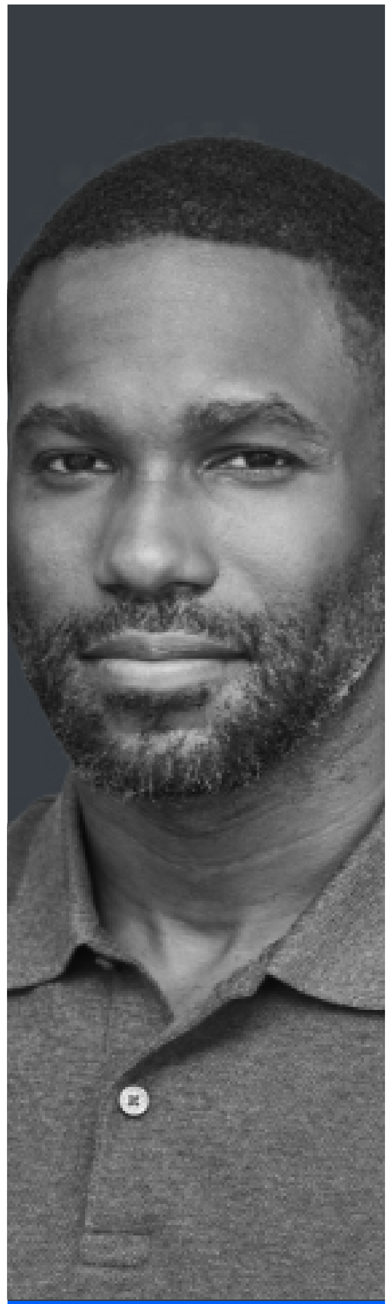
Begin with:
Developer portal

← →

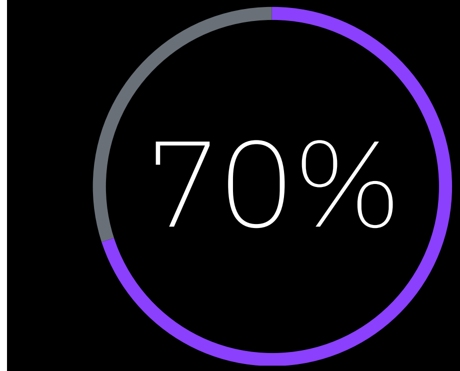
View



View



View



or more of all application access through access management solutions will leverage MFA by 2024

Gartner

"I need to embed authentication into my applications quickly, without this step becoming a roadblock for what I'm actually trying to accomplish"

Alice, Developer

Developer

○ Employee ○ Business manager ○ IT administrator ● **Developer** ○ Developer resources ○ Build custom applications ○ API configuration

Developer

Embed access and authentication into custom applications with intuitive, purpose-built APIs.

Developers need to build run-time flows for authentication, give users registration capabilities, and embed MFA into their applications, without necessarily being an IAM expert. To do this efficiently, they need robust APIs and documentation, sample code, and guided instructions.

70%

or more of all application access through access management solutions will leverage MFA by 2024

Gartner

“I need to embed authentication into my applications quickly, without this step becoming a roadblock for what I’m actually trying to accomplish”

Alice, Developer

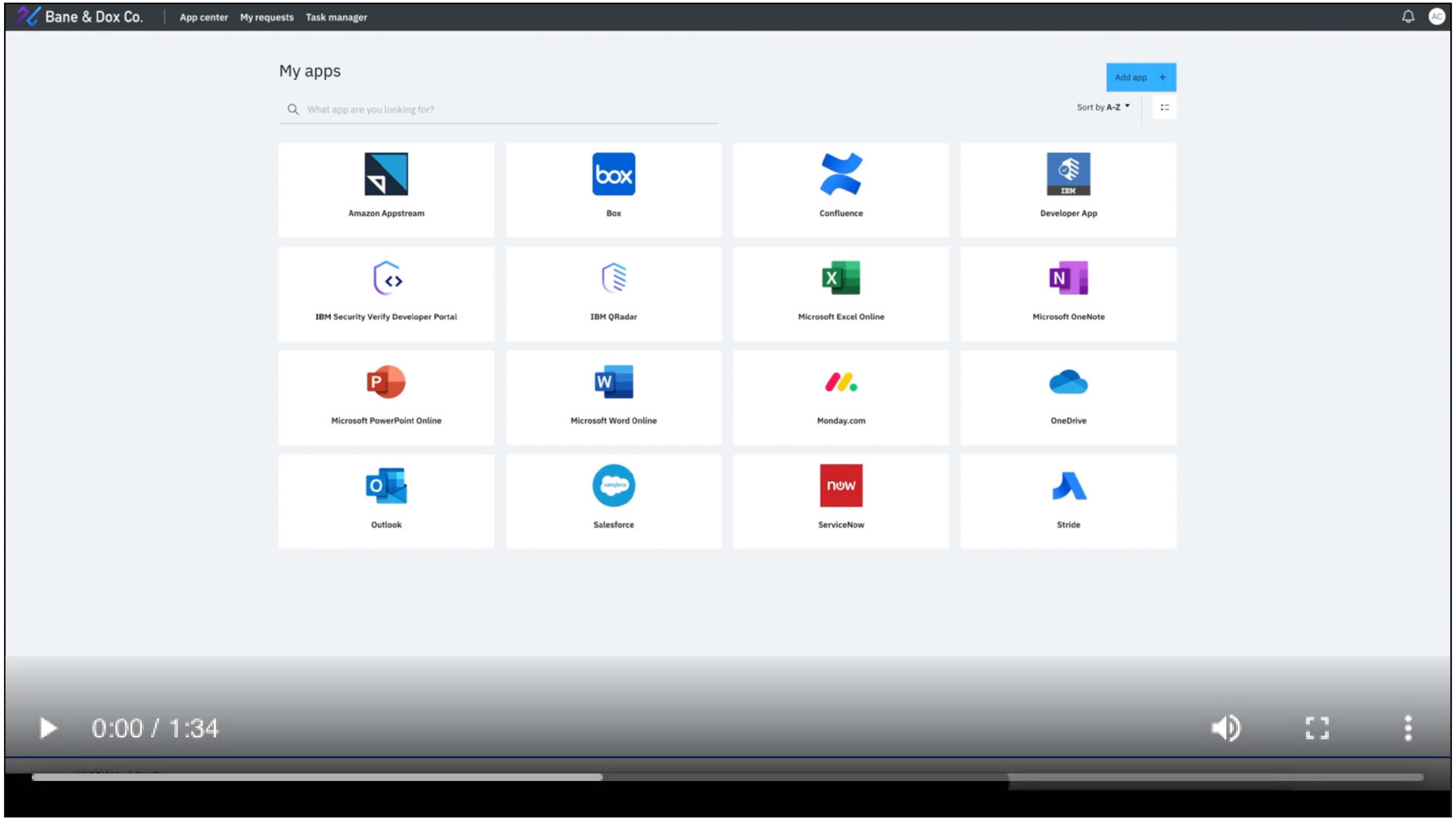
Developer

- ○ Employee
- ○ Business manager
- ○ IT administrator
- ● **Developer**
- ○ Developer resources
  - Developer portal
  - API help
- ○ Build custom applications
  - Add custom application template
  - Configure sign-on settings
  - Configure provisioning
  - Troubleshoot bugs
- ○ API configuration
  - Add API clients
  - Delegated administration

Developer: 1 of 2
Developer resources

Developer portal

The IBM Security Verify developer portal offers a wizard-like experience that guides developers through the process of integrating an application. The portal offers code snippets, step-by-step instructions, and sample applications, in addition to standard API documentation.



Next:
API help

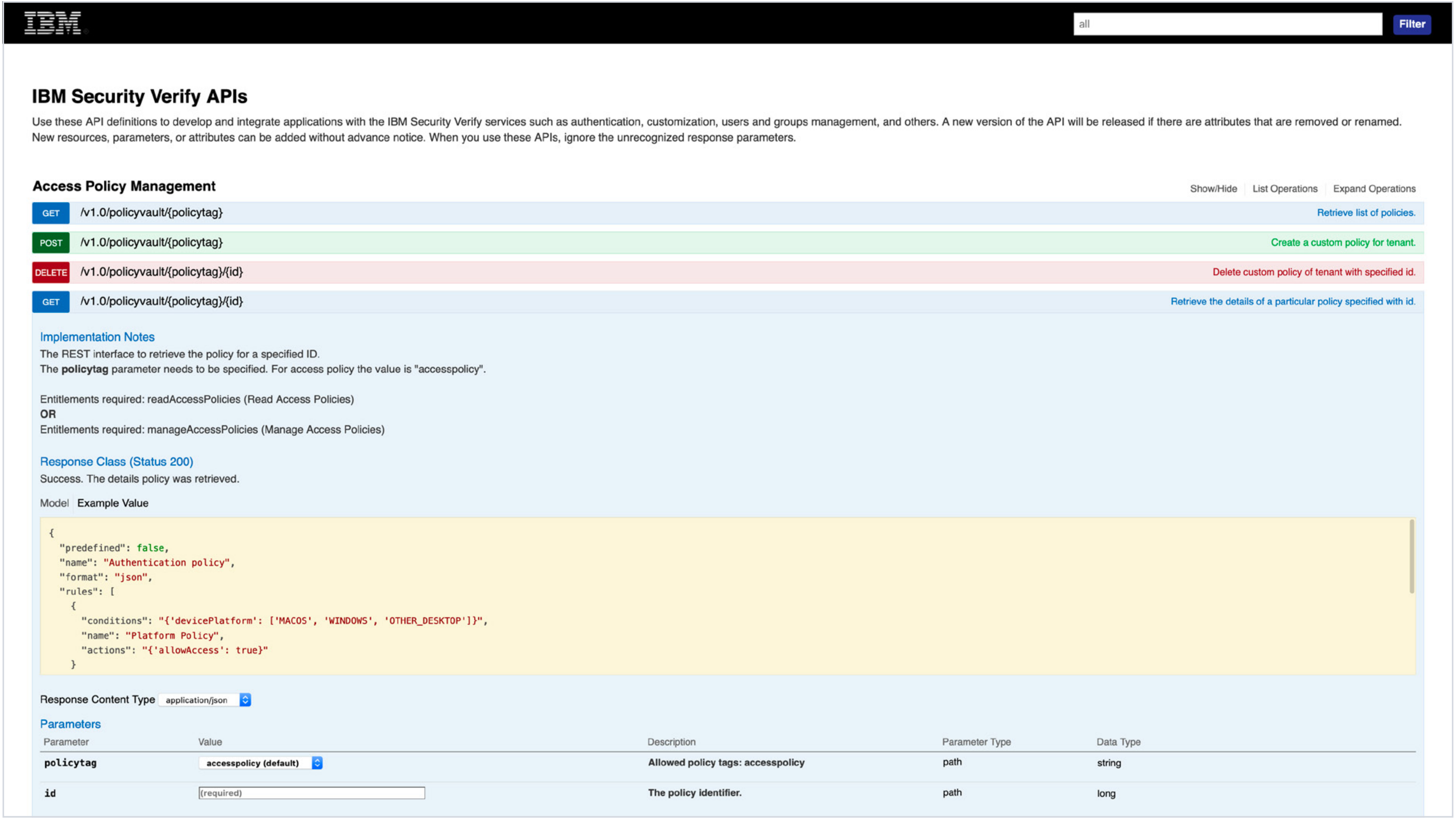
←
→

Employee
Business manager
IT administrator
Developer
Developer resources
Build custom applications
API configuration

Developer: 2 of 2
Developer resources

API help

Alice can use Verify’s APIs to integrate identity-related functions like user management and authentication into her applications. The Verify API Help provides guidance for implementation like required entitlements, parameters, and possible response messages. The Help documentation also includes an example implementation for each API call.



IBM Security Verify APIs

Use these API definitions to develop and integrate applications with the IBM Security Verify services such as authentication, customization, users and groups management, and others. A new version of the API will be released if there are attributes that are removed or renamed. New resources, parameters, or attributes can be added without advance notice. When you use these APIs, ignore the unrecognized response parameters.

Access Policy Management

GET	/v1.0/policyvault/{policytag}	Retrieve list of policies.
POST	/v1.0/policyvault/{policytag}	Create a custom policy for tenant.
DELETE	/v1.0/policyvault/{policytag}/{id}	Delete custom policy of tenant with specified id.
GET	/v1.0/policyvault/{policytag}/{id}	Retrieve the details of a particular policy specified with id.

Implementation Notes
The REST interface to retrieve the policy for a specified ID.
The **policytag** parameter needs to be specified. For access policy the value is "accesspolicy".

Entitlements required: readAccessPolicies (Read Access Policies)
OR
Entitlements required: manageAccessPolicies (Manage Access Policies)

Response Class (Status 200)
Success. The details policy was retrieved.

Model | **Example Value**

```
{
  "predefined": false,
  "name": "Authentication policy",
  "format": "json",
  "rules": [
    {
      "conditions": "{'devicePlatform': ['MACOS', 'WINDOWS', 'OTHER_DESKTOP']}",
      "name": "Platform Policy",
      "actions": "{'allowAccess': true}"
    }
```

Response Content Type application/json

Parameters

Parameter	Value	Description	Parameter Type	Data Type
policytag	accesspolicy (default)	**Allowed policy tags: accesspolicy**	path	string
id	(required)	**The policy identifier.**	path	long

Next:
Add custom application template

←　→

Employee
Business manager
IT administrator
Developer
Developer resources
Build custom applications
API configuration

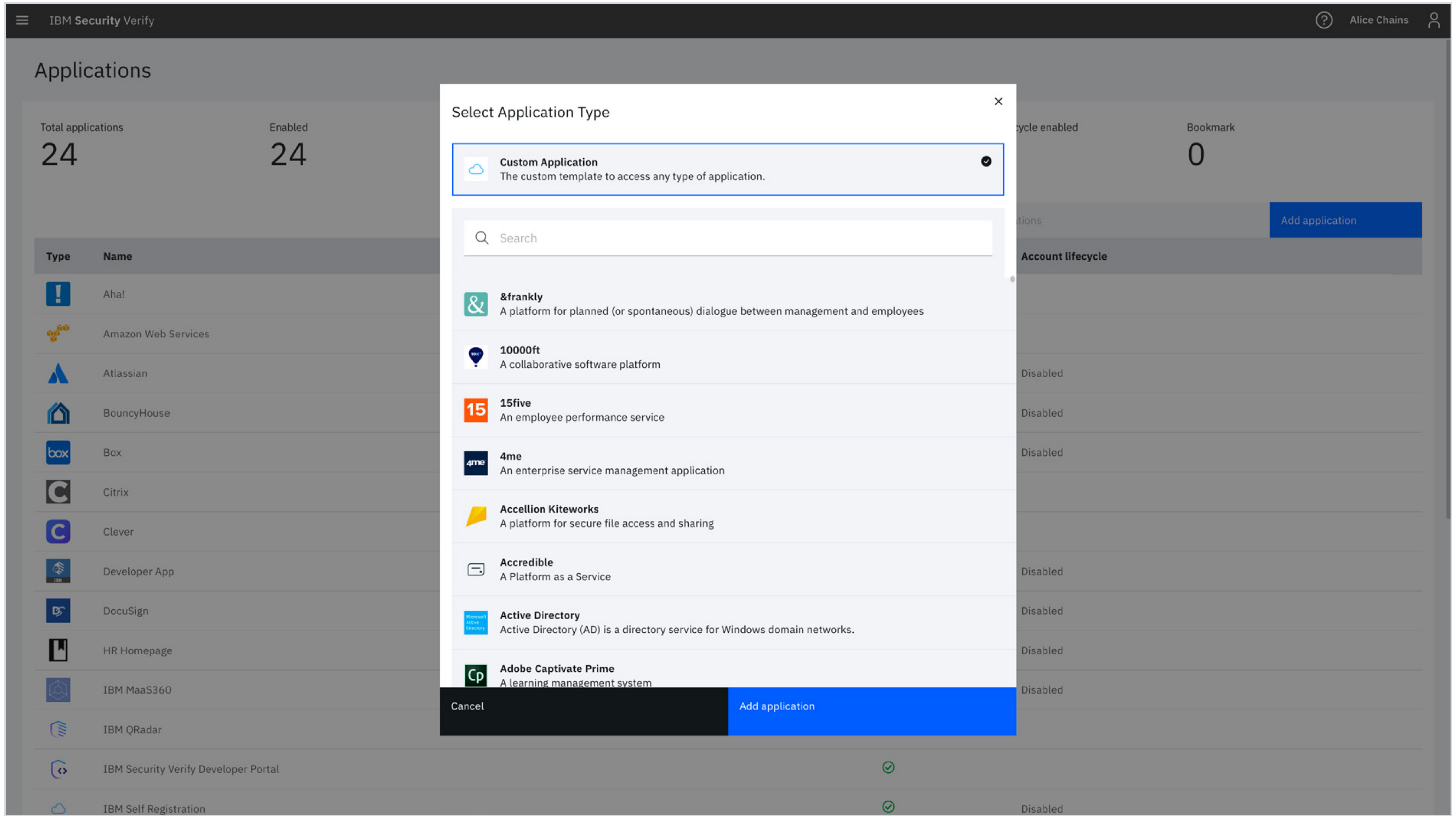
IBM **Security** Verify

Try Verify Now

Developer: 1 of 4
Build custom applications

Add custom application template

Alice can include her custom applications alongside the organization’s other SaaS and on-premises applications by integrating them into Verify’s federated single sign-on. To get started, she can add the custom application template to integrate new SAML or Open ID Connect applications.



IBM Security Verify — Alice Chains

Applications

Total applications 24 — Enabled 24 — ...ycle enabled — Bookmark 0

Add application

Type	Name		Account lifecycle
	Aha!		
	Amazon Web Services		
	Atlassian		Disabled
	BouncyHouse		Disabled
	Box		Disabled
	Citrix		
	Clever		
	Developer App		Disabled
	DocuSign		Disabled
	HR Homepage		Disabled
	IBM MaaS360		Disabled
	IBM QRadar		
	IBM Security Verify Developer Portal	✓	
	IBM Self Registration	✓	Disabled

Select Application Type

Custom Application ●
The custom template to access any type of application.

Search

&frankly
A platform for planned (or spontaneous) dialogue between management and employees

10000ft
A collaborative software platform

15five
An employee performance service

4me
An enterprise service management application

Accellion Kiteworks
A platform for secure file access and sharing

Accredible
A Platform as a Service

Active Directory
Active Directory (AD) is a directory service for Windows domain networks.

Adobe Captivate Prime
A learning management system

Next:
Configure sign-on settings

← →

Employee — Business manager — IT administrator — Developer — Developer resources — **Build custom applications** — API configuration

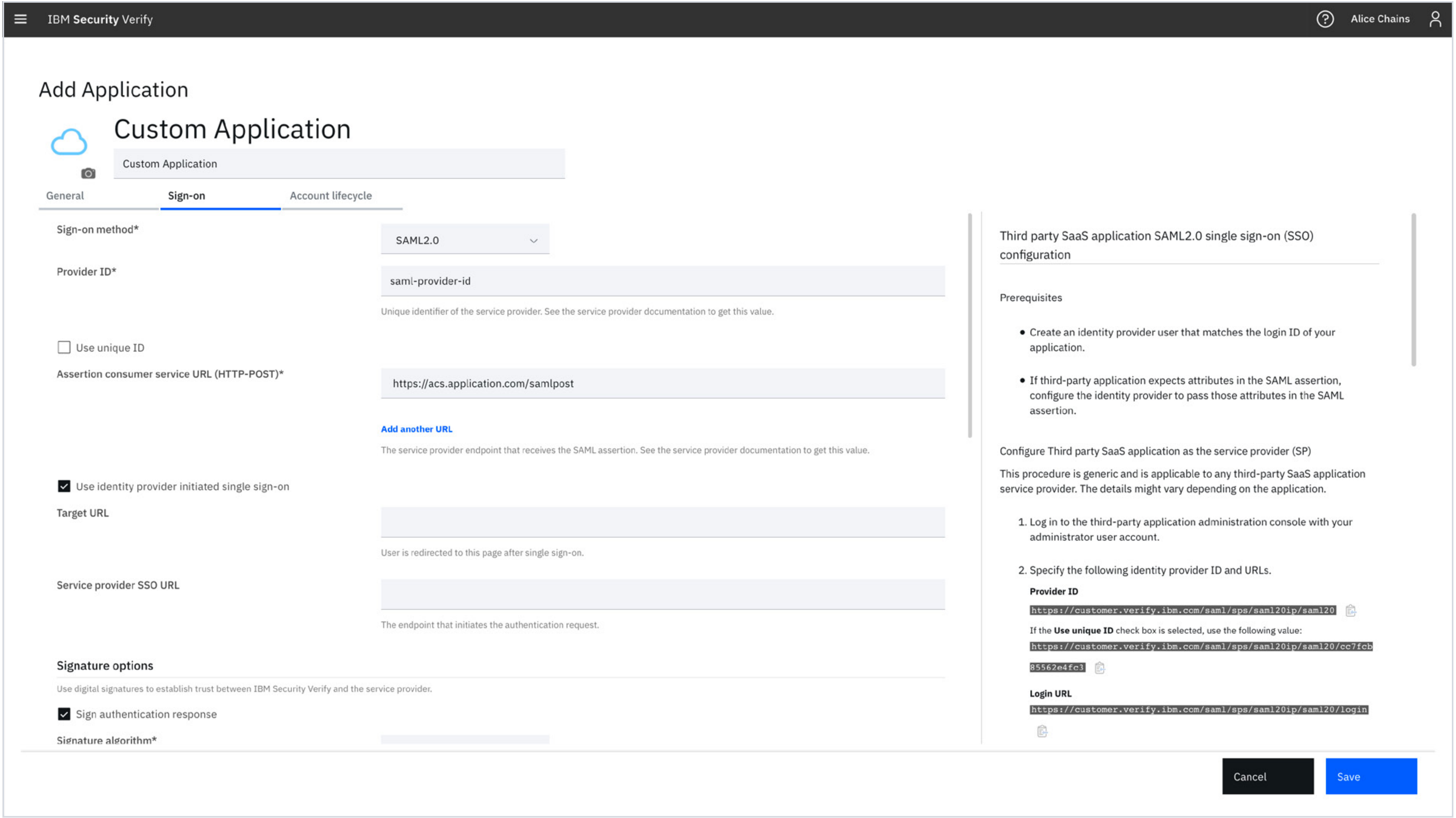
Back Next

Developer: 2 of 4

Build custom applications

Configure sign-on settings

In the application template, step-by-step instructions are provided to integrate the application.



Add Application

Custom Application

Custom Application

Sign-on method* SAML2.0

Provider ID* saml-provider-id

Unique identifier of the service provider. See the service provider documentation to get this value.

☐ Use unique ID

Assertion consumer service URL (HTTP-POST)* https://acs.application.com/samlpost

Add another URL

The service provider endpoint that receives the SAML assertion. See the service provider documentation to get this value.

☑ Use identity provider initiated single sign-on

Target URL

User is redirected to this page after single sign-on.

Service provider SSO URL

The endpoint that initiates the authentication request.

Signature options

Use digital signatures to establish trust between IBM Security Verify and the service provider.

☑ Sign authentication response

Signature algorithm*

Third party SaaS application SAML2.0 single sign-on (SSO) configuration

Prerequisites

- Create an identity provider user that matches the login ID of your application.
- If third-party application expects attributes in the SAML assertion, configure the identity provider to pass those attributes in the SAML assertion.

Configure Third party SaaS application as the service provider (SP)

This procedure is generic and is applicable to any third-party SaaS application service provider. The details might vary depending on the application.

1. Log in to the third-party application administration console with your administrator user account.
2. Specify the following identity provider ID and URLs.

   Provider ID

   `https://customer.verify.ibm.com/saml/sps/saml20ip/saml20`

   If the **Use unique ID** check box is selected, use the following value:

   `https://customer.verify.ibm.com/saml/sps/saml20ip/saml20/cc7fcb`
   `85562e4fc3`

   Login URL

   `https://customer.verify.ibm.com/saml/sps/saml20ip/saml20/login`

Next:
Configure provisioning

← →

○ Employee

○ Business manager

○ IT administrator

● Developer

● Developer resources

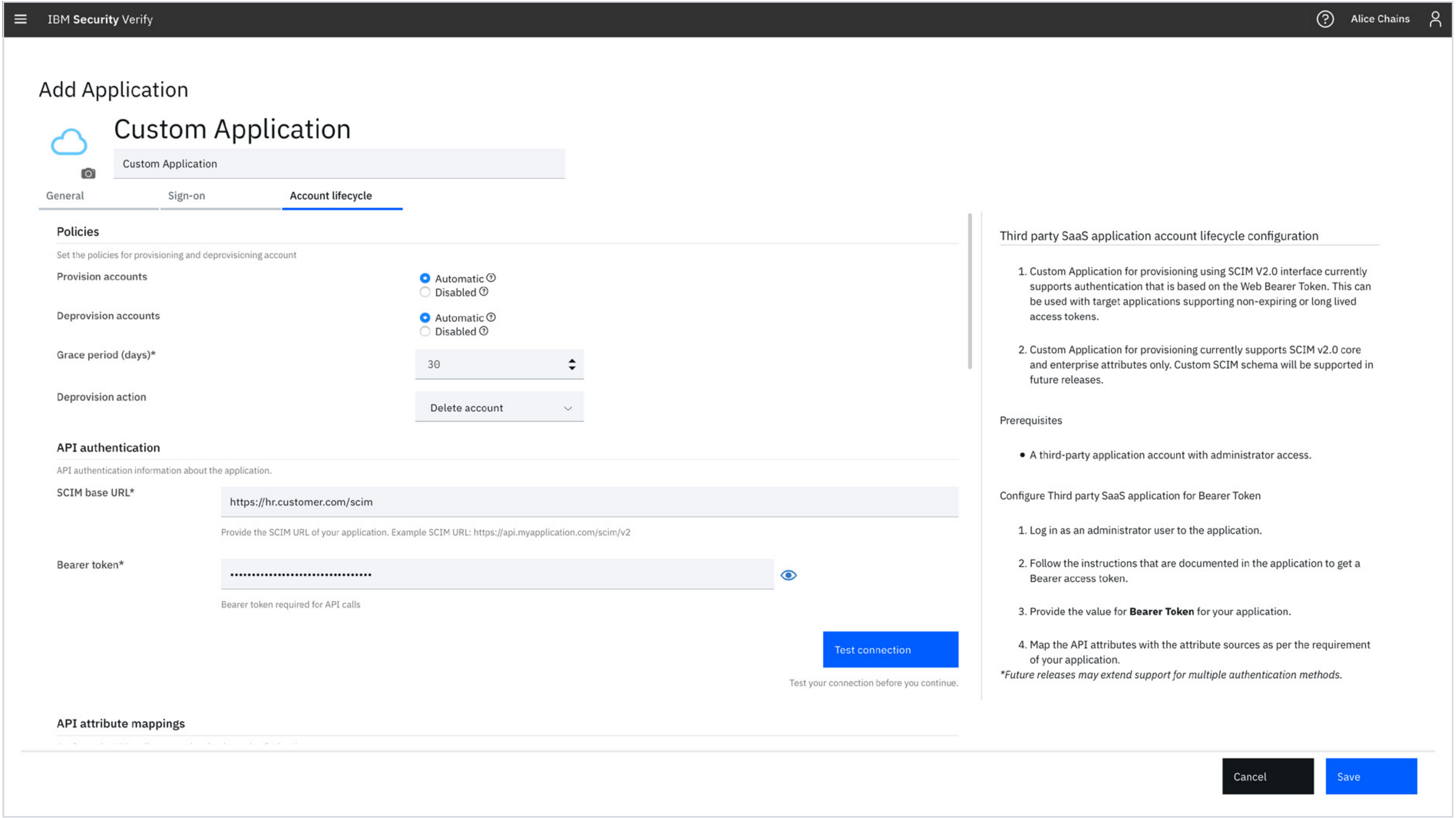
● **Build custom applications**

○ API configuration

Developer: 3 of 4
Build custom applications

Configure provisioning

She can also choose to enable automatic provisioning and deprovisioning for the application with SCIM.



Add Application

Custom Application

Custom Application

Policies

Set the policies for provisioning and deprovisioning account

Provision accounts: ● Automatic ○ Disabled

Deprovision accounts: ● Automatic ○ Disabled

Grace period (days)*: 30

Deprovision action: Delete account

API authentication

API authentication information about the application.

SCIM base URL*: https://hr.customer.com/scim

Provide the SCIM URL of your application. Example SCIM URL: https://api.myapplication.com/scim/v2

Bearer token*: ••••••••••••••••••••••••••••••••••

Bearer token required for API calls

Test your connection before you continue.

API attribute mappings

Third party SaaS application account lifecycle configuration

1. Custom Application for provisioning using SCIM V2.0 interface currently supports authentication that is based on the Web Bearer Token. This can be used with target applications supporting non-expiring or long lived access tokens.
2. Custom Application for provisioning currently supports SCIM v2.0 core and enterprise attributes only. Custom SCIM schema will be supported in future releases.

Prerequisites

- A third-party application account with administrator access.

Configure Third party SaaS application for Bearer Token

1. Log in as an administrator user to the application.
2. Follow the instructions that are documented in the application to get a Bearer access token.
3. Provide the value for **Bearer Token** for your application.
4. Map the API attributes with the attribute sources as per the requirement of your application.

**Future releases may extend support for multiple authentication methods.*

Next:
Troubleshoot bugs

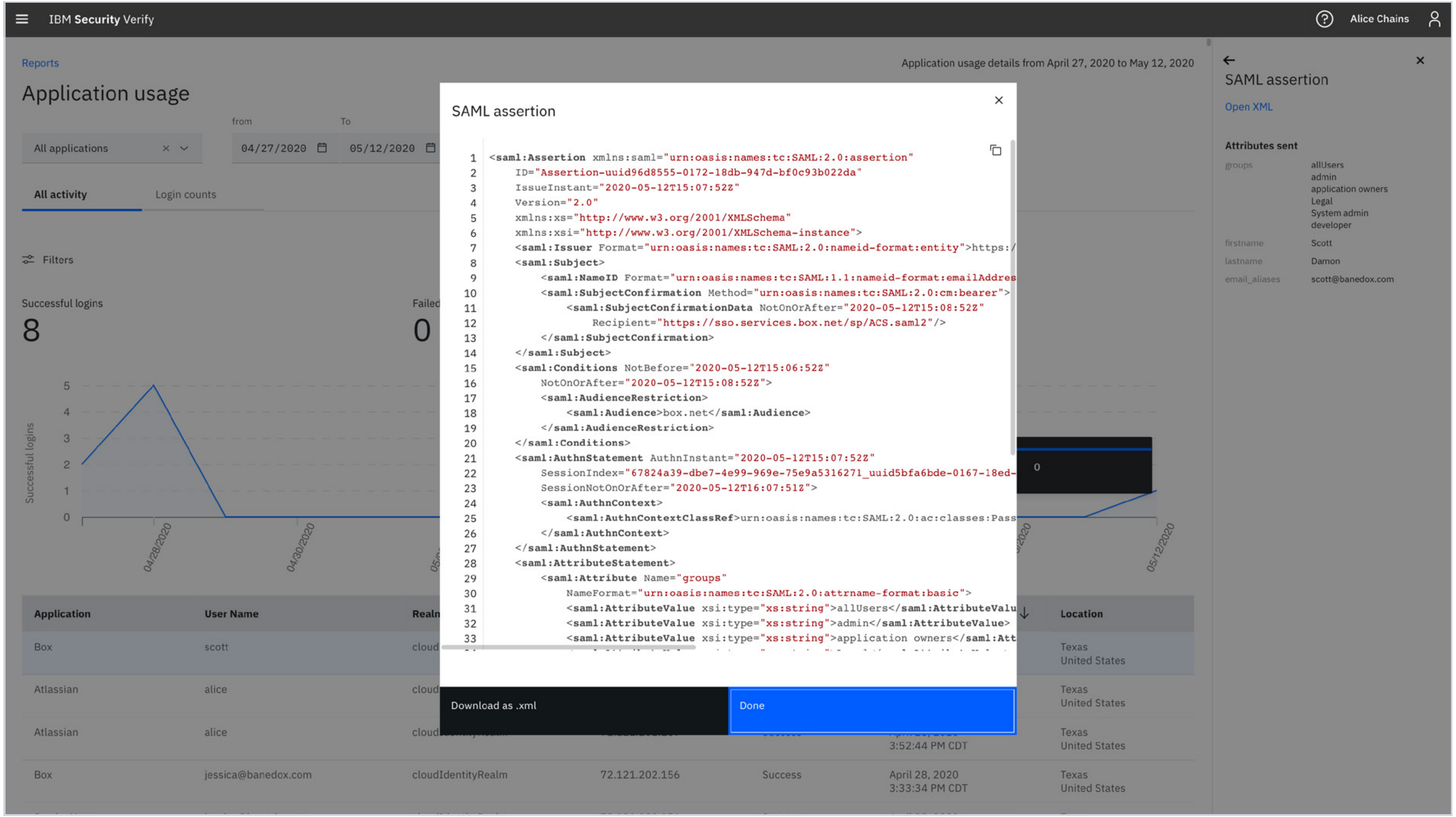
○ Employee ○ Business manager ○ IT administrator ● Developer ● Developer resources ● **Build custom applications** ○ API configuration

Developer: 4 of 4

Build custom applications

Troubleshoot bugs

Alice can monitor the performance of her application and dig into authentication event details to troubleshoot bugs.



SAML assertion

```
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="Assertion-uuid96d8555-0172-18db-947d-bf0c93b022da"
    IssueInstant="2020-05-12T15:07:52Z"
    Version="2.0"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">https:/
    <saml:Subject>
        <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddres
        <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml:SubjectConfirmationData NotOnOrAfter="2020-05-12T15:08:52Z"
                Recipient="https://sso.services.box.net/sp/ACS.saml2"/>
        </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Conditions NotBefore="2020-05-12T15:06:52Z"
        NotOnOrAfter="2020-05-12T15:08:52Z">
        <saml:AudienceRestriction>
            <saml:Audience>box.net</saml:Audience>
        </saml:AudienceRestriction>
    </saml:Conditions>
    <saml:AuthnStatement AuthnInstant="2020-05-12T15:07:52Z"
        SessionIndex="67824a39-dbe7-4e99-969e-75e9a5316271_uuid5bfa6bde-0167-18ed-
        SessionNotOnOrAfter="2020-05-12T16:07:51Z">
        <saml:AuthnContext>
            <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Pass
        </saml:AuthnContext>
    </saml:AuthnStatement>
    <saml:AttributeStatement>
        <saml:Attribute Name="groups"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <saml:AttributeValue xsi:type="xs:string">allUsers</saml:AttributeValu
            <saml:AttributeValue xsi:type="xs:string">admin</saml:AttributeValue>
            <saml:AttributeValue xsi:type="xs:string">application owners</saml:Att
```

SAML assertion

Open XML

Attributes sent

groups	allUsers admin application owners Legal System admin developer
firstname	Scott
lastname	Damon
email_aliases	scott@banedox.com

Application	User Name	Realn				Location
Box	scott	cloud				Texas United States
Atlassian	alice	cloud				Texas United States
Atlassian	alice	cloud			3:52:44 PM CDT	Texas United States
Box	jessica@banedox.com	cloudIdentityRealm	72.121.202.156	Success	April 28, 2020 3:33:34 PM CDT	Texas United States

Next:
Add API clients

← →

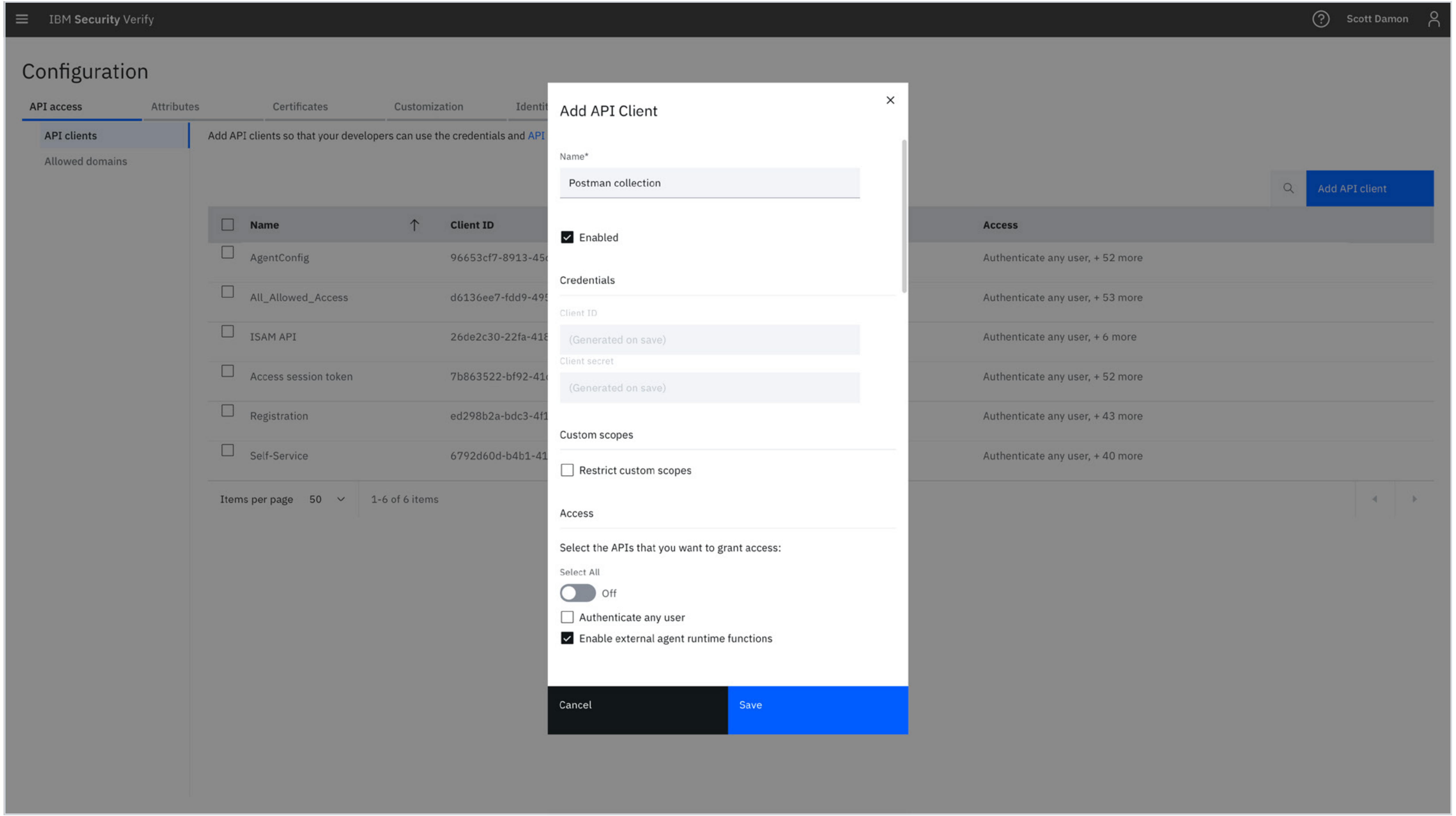
IBM **Security** Verify

Try Verify Now

Developer: 1 of 2
API configuration

Add API clients

Alice can select from a variety of API clients she might want to integrate into her applications.



Configuration

API access | Attributes | Certificates | Customization | Identi

API clients
Allowed domains

Add API clients so that your developers can use the credentials and API

Add API client

☐	Name ↑	Client ID	Access
☐	AgentConfig	96653cf7-8913-45	Authenticate any user, + 52 more
☐	All_Allowed_Access	d6136ee7-fdd9-495	Authenticate any user, + 53 more
☐	ISAM API	26de2c30-22fa-418	Authenticate any user, + 6 more
☐	Access session token	7b863522-bf92-41	Authenticate any user, + 52 more
☐	Registration	ed298b2a-bdc3-4f1	Authenticate any user, + 43 more
☐	Self-Service	6792d60d-b4b1-41	Authenticate any user, + 40 more

Items per page 50 | 1-6 of 6 items

Add API Client ×

Name*
Postman collection

☑ Enabled

Credentials

Client ID
(Generated on save)

Client secret
(Generated on save)

Custom scopes

☐ Restrict custom scopes

Access

Select the APIs that you want to grant access:

Select All
Off

☐ Authenticate any user
☑ Enable external agent runtime functions

Cancel | Save

Next:
Delegated administration

← →

Employee | Business manager | IT administrator | Developer | Developer resources | Build custom applications | **API configuration**

Back | Next

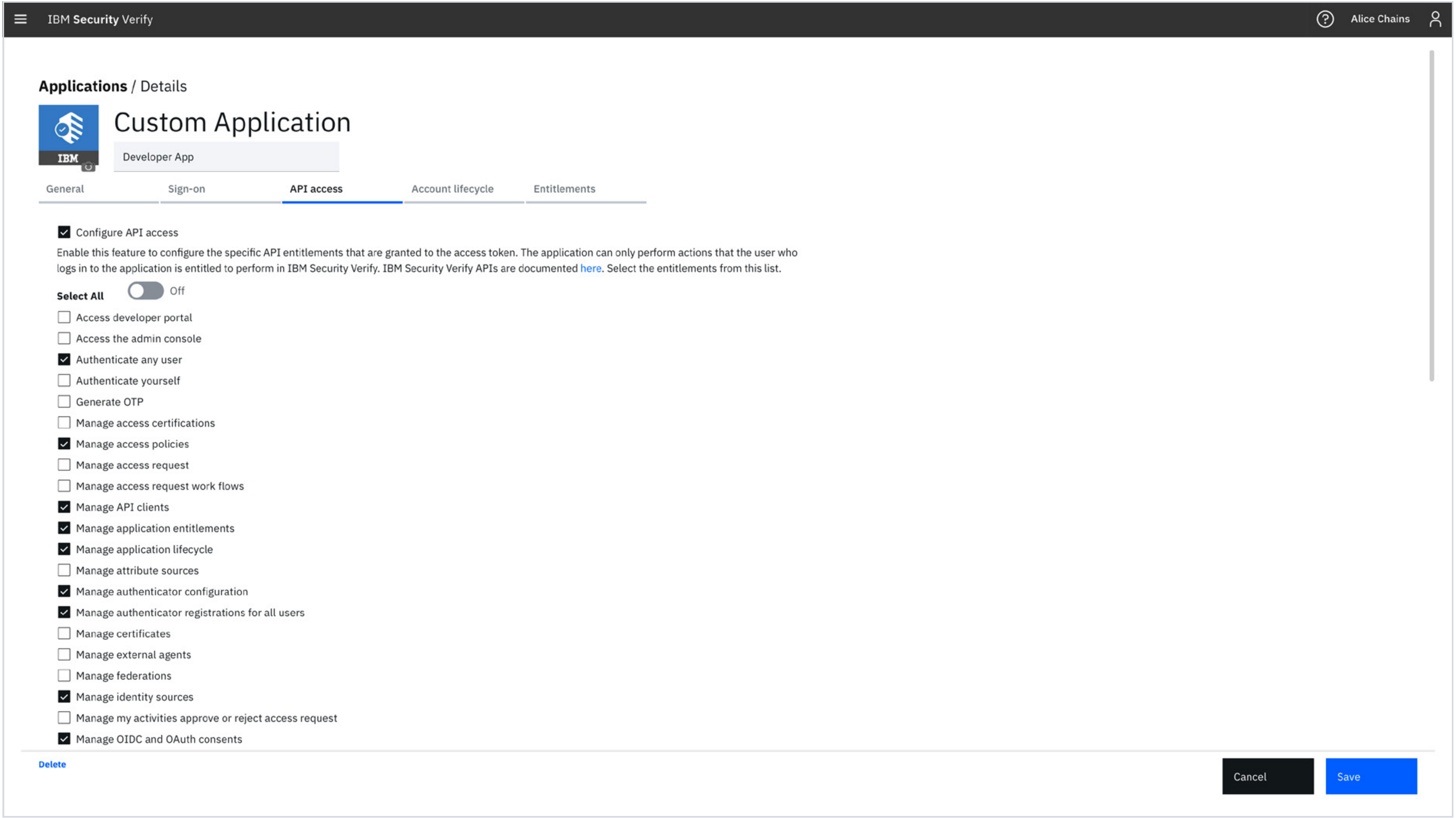
IBM **Security** Verify

Try Verify Now

Developer: 2 of 2
API configuration

Delegated administration

She can also give her application permission to call specific API entitlements that are granted to the access token.



Applications / Details

Custom Application

Developer App

☑ Configure API access

Enable this feature to configure the specific API entitlements that are granted to the access token. The application can only perform actions that the user who logs in to the application is entitled to perform in IBM Security Verify. IBM Security Verify APIs are documented here. Select the entitlements from this list.

Select All Off

- □ Access developer portal
- □ Access the admin console
- ☑ Authenticate any user
- □ Authenticate yourself
- □ Generate OTP
- □ Manage access certifications
- ☑ Manage access policies
- □ Manage access request
- □ Manage access request work flows
- ☑ Manage API clients
- ☑ Manage application entitlements
- ☑ Manage application lifecycle
- □ Manage attribute sources
- ☑ Manage authenticator configuration
- ☑ Manage authenticator registrations for all users
- □ Manage certificates
- □ Manage external agents
- □ Manage federations
- ☑ Manage identity sources
- □ Manage my activities approve or reject access request
- ☑ Manage OIDC and OAuth consents

Explore:
IBM Security Verify

←

Employee · Business manager · IT administrator · Developer · Developer resources · Build custom applications · **API configuration**

Back

Learn more

IBM Security

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
February 2021

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates. The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided. The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation. Statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

00000000USEN

IBM