IBM Security Verify 产品展示

开始体验 →

IBM

IBM **Security** Verify

立即试用 Verify

将一切用户安全地连接到任何设备

IBM Security Verify 为有关谁应该有权访问哪些内容的决策提供上下文和情报，从而使您的组织能够在适当的时间为适当的人员提供适当的访问权限。

探索此展示，了解如何掌握安全与用户体验之间的平衡。

员工

业务经理

IT 管理员

开发者

员工

从任何设备轻松访问工作所需的应用，无需输入密码。

员工需要快速访问他们工作所需的工具，而不会被数十个凭证所累。企业安全是期望目标，但 IT 策略仍可能是实现目标的挡路石。员工希望无障碍地高效工作。

11

个小时

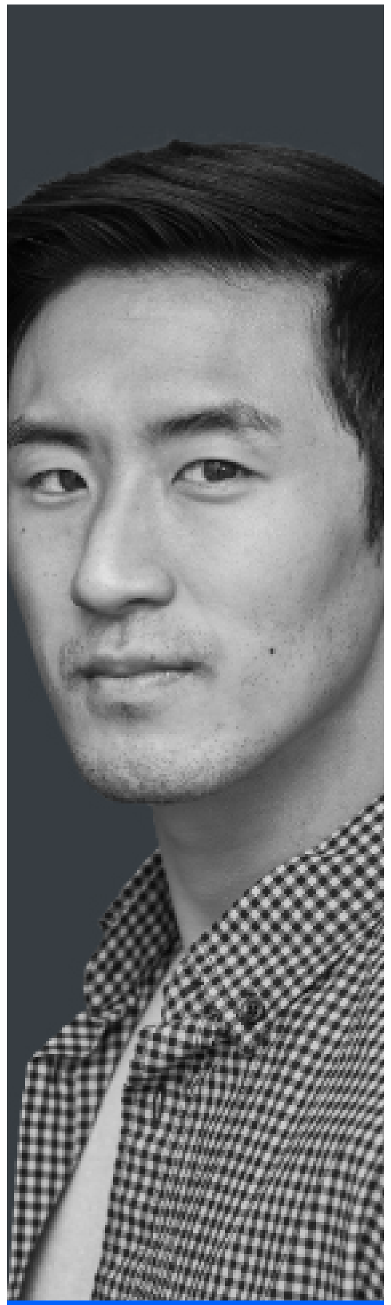
全球员工每年用在输入或重置密码上的平均时间

世界经济论坛

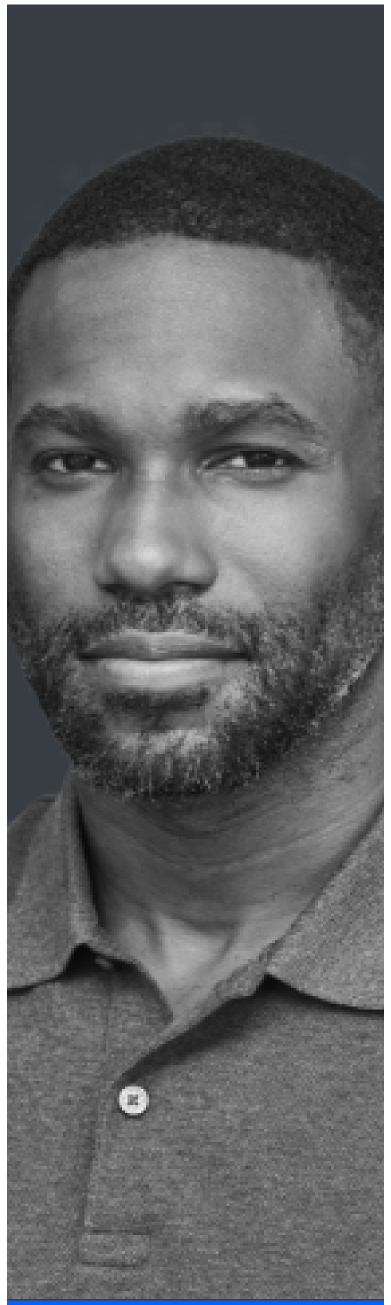
“我只是想把工作做完的时候，却因为工具和系统而停滞不前，真是令人沮丧。”

Jessica，员工

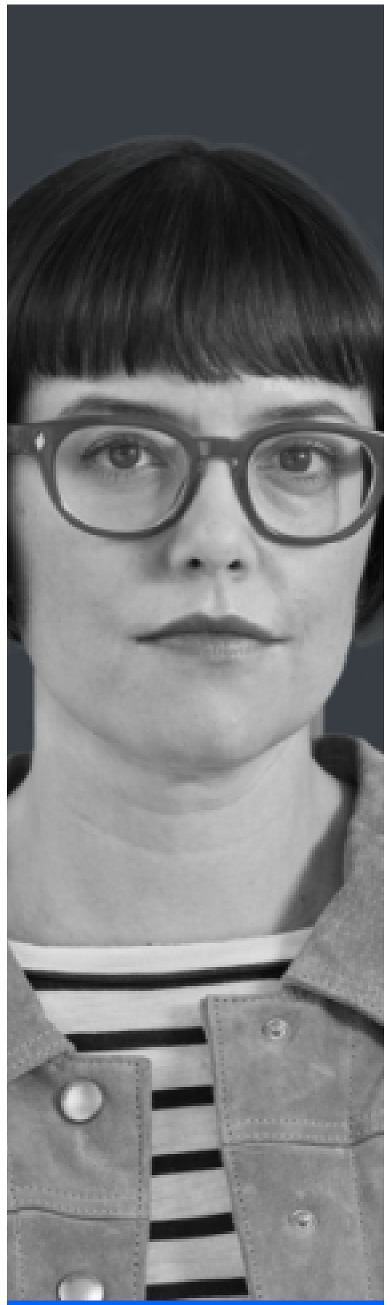
员工



查看



查看



查看

首先：
品牌登录页面

← →

○ **员工** ○ 单点登录 ○ 请求应用程序访问 ○ 注册并使用 MFA ○ 业务经理 ○ IT 管理员 ○ 开发者

员工

从任何设备轻松访问工作所需的应用，无需输入密码。

员工需要快速访问他们工作所需的工具，而不会被数十个凭证所累。企业安全是期望目标，但 IT 策略仍可能是实现目标的挡路石。员工希望无障碍地高效工作。

11

个小时

全球员工每年用在输入或重置密码上的平均时间

世界经济论坛

“我只是想把工作做完的时候，却因为工具和系统而停滞不前，真是令人沮丧。”

Jessica，员工

员工

- **员工**
- 单点登录
  - 品牌登录页面
  - 一键访问应用
- 请求应用程序访问
  - 搜索目录
  - 写下理由
  - 暂挂请求
  - 在启动板中新增应用
- 注册并使用 MFA
  - 添加新的身份验证设备
  - 设置移动应用
  - 选择 MFA 方法
- 业务经理
- IT 管理员
- 开发者

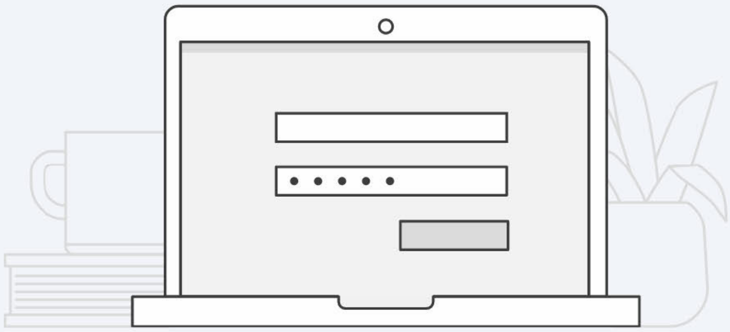
IBM **Security** Verify

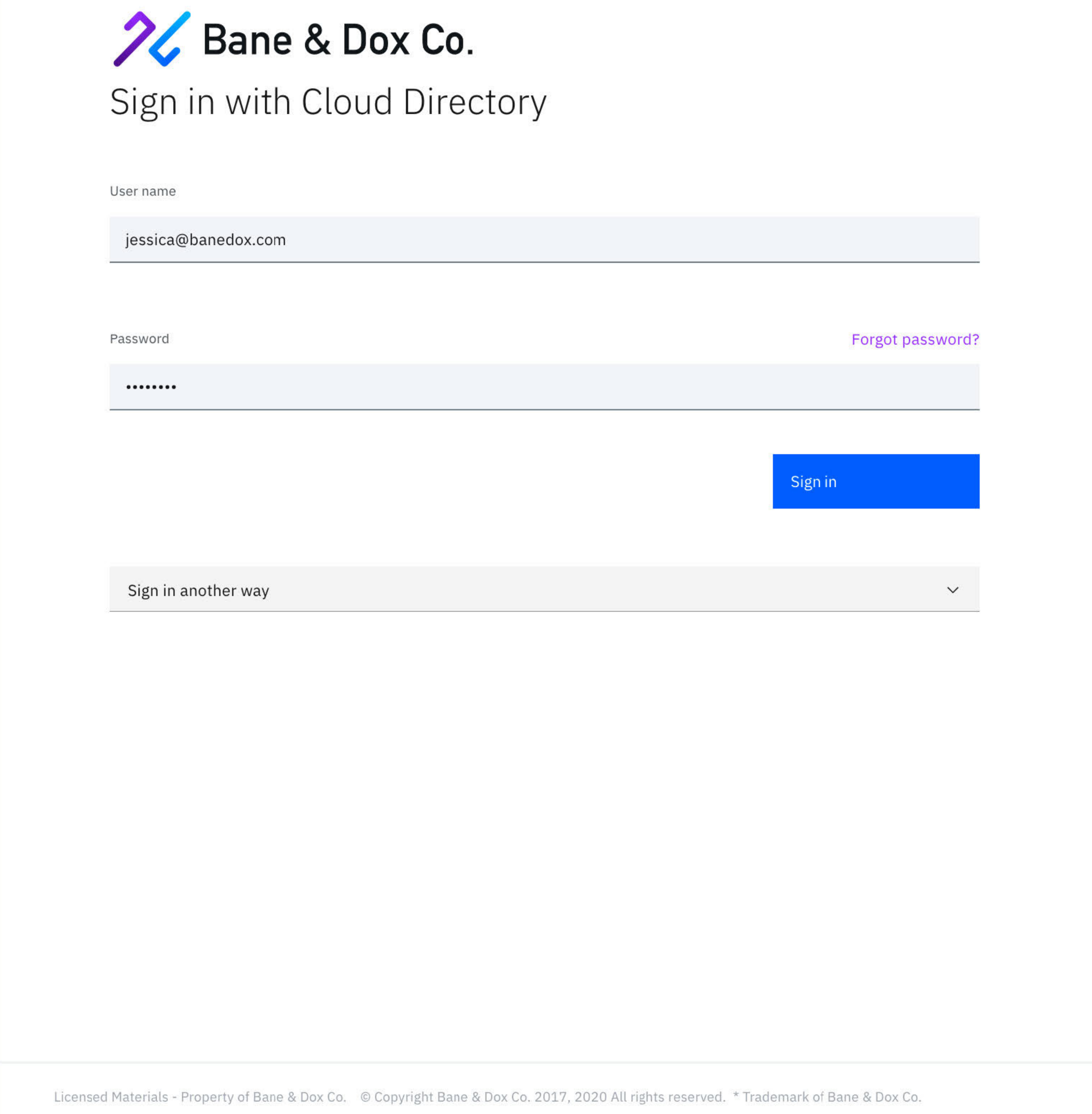
立即试用 Verify

员工：第 1 步（共 2 步）
单点登录

品牌登录页面

员工需要快速访问他们工作所需的工具，而不会被数十个凭证所累。企业安全是期望目标，但 IT 策略仍可能是实现目标的挡路石。员工希望无障碍地高效工作。





Bane & Dox Co.

Sign in with Cloud Directory

User name

jessica@banedox.com

Password

Forgot password?

••••••••

Sign in

Sign in another way

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

下一步：
一键访问应用

←　→

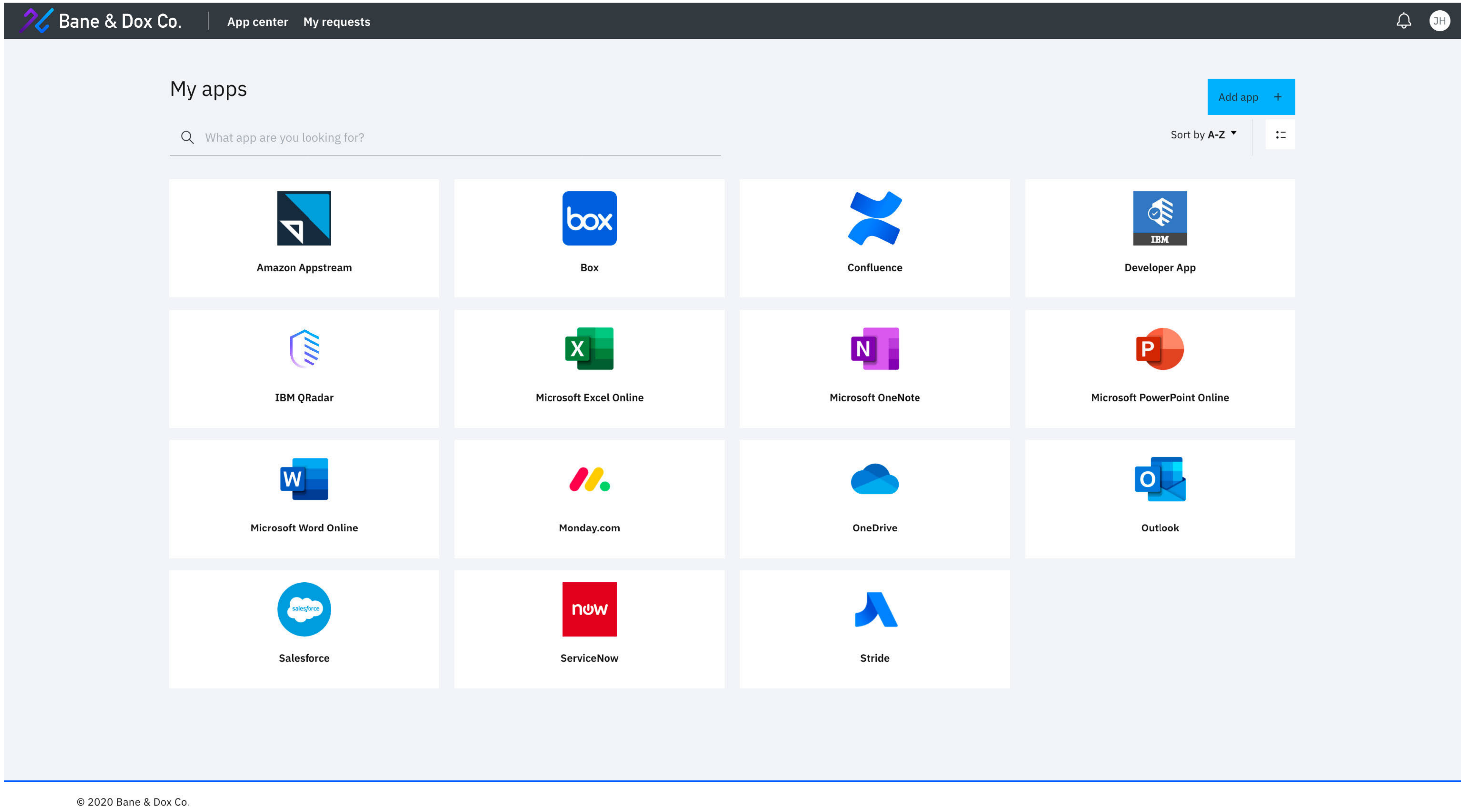
员工　**单点登录**　请求应用程序访问　注册并使用 MFA　业务经理　IT 管理员　开发者

上一页　下一页

员工：第 2 步（共 2 步）
单点登录

一键访问应用

Jessica 从启动板中可以访问她有权使用的所有应用。根据 IT 管理员对其环境的配置，大多数应用程序将支持一键访问。



下一步：
搜索目录

← →

员工 ● 单点登录 ○ 请求应用程序访问 ○ 注册并使用 MFA ○ 业务经理 ○ IT 管理员 ○ 开发者

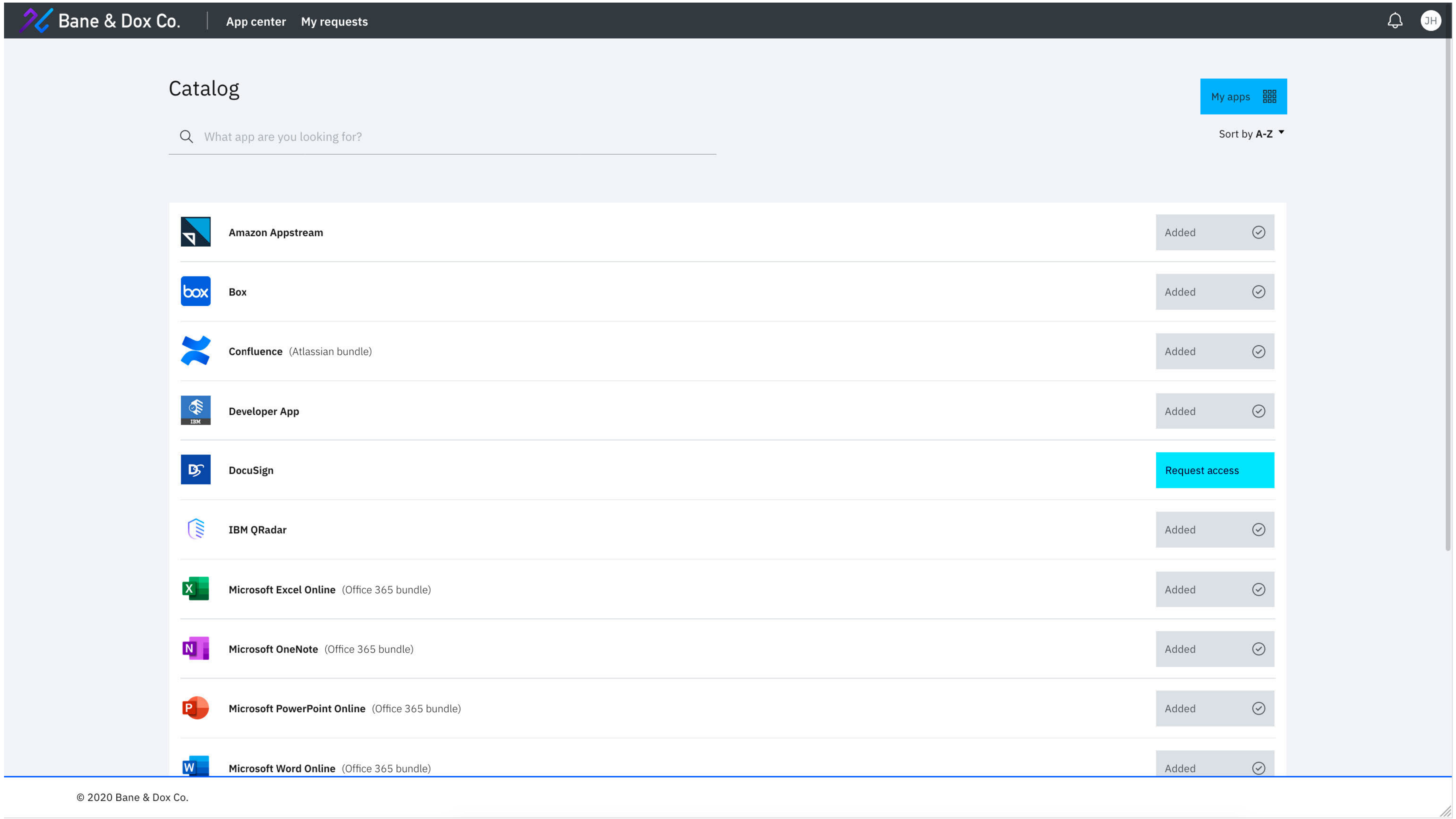
上一页 下一页

员工：第 1 步（共 4 步）
请求应用程序访问

搜索目录

Jessica 从启动板中可以访问她有权使用的所有应用。根据 IT 管理员对其环境的配置，大多数应用程序将支持一键访问。

下一步：
写下理由



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

© 2020 Bane & Dox Co.

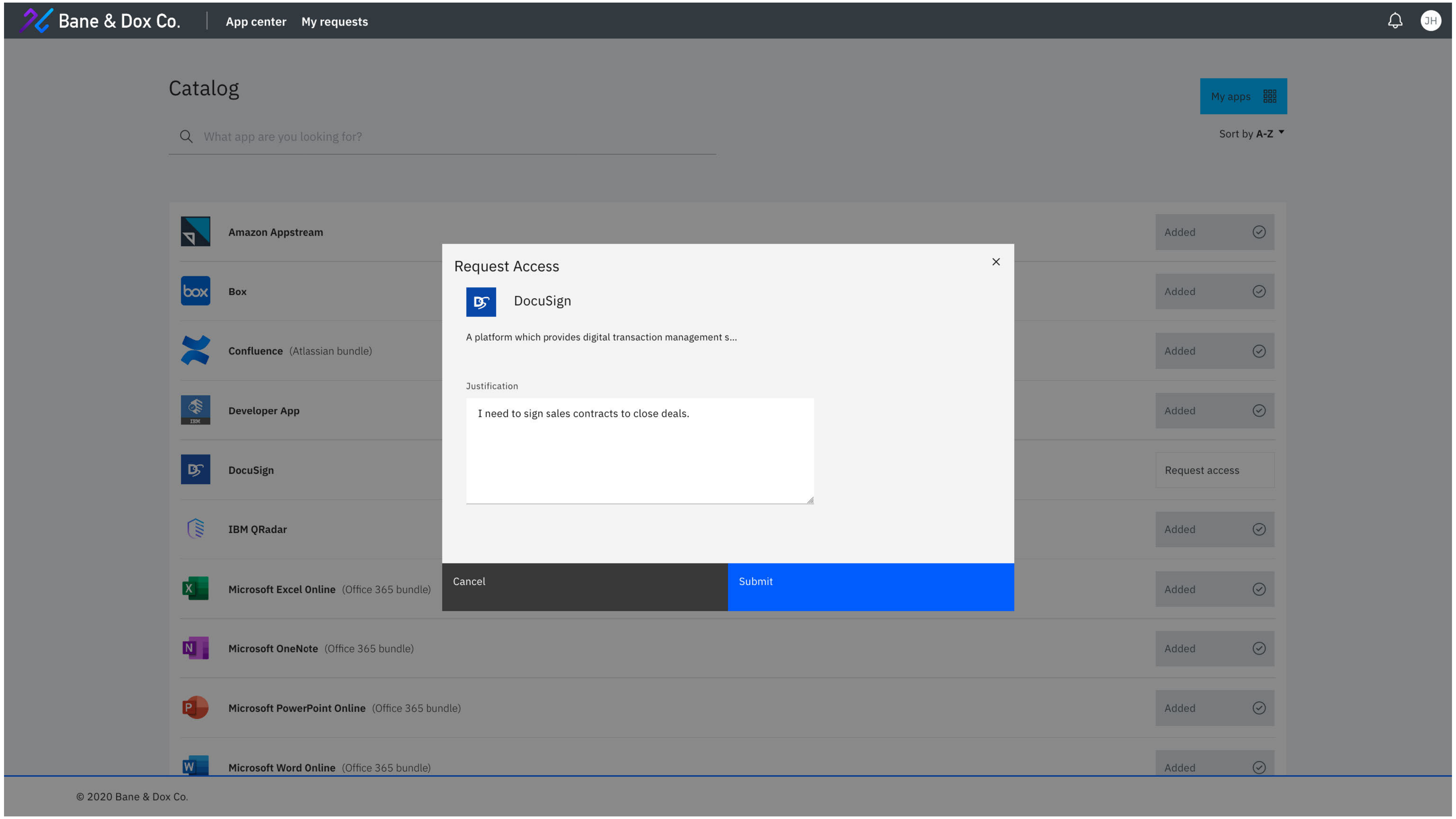
IBM **Security** Verify

立即试用 Verify

员工：第 2 步（共 4 步）
请求应用程序访问

写下理由

她选择了 XYZ，并写下一个业务理由来说明她为何需要访问。


Bane & Dox Co.
App center
My requests
JH
Catalog
My apps
What app are you looking for?
Sort by A-Z
Amazon Appstream
Box
Confluence (Atlassian bundle)
Developer App
DocuSign
IBM QRadar
Microsoft Excel Online (Office 365 bundle)
Microsoft OneNote (Office 365 bundle)
Microsoft PowerPoint Online (Office 365 bundle)
Microsoft Word Online (Office 365 bundle)
Added
Request access
Cancel
Submit
© 2020 Bane & Dox Co.

Request Access

DocuSign

A platform which provides digital transaction management s...

Justification

I need to sign sales contracts to close deals.

下一步：
暂挂请求

← →

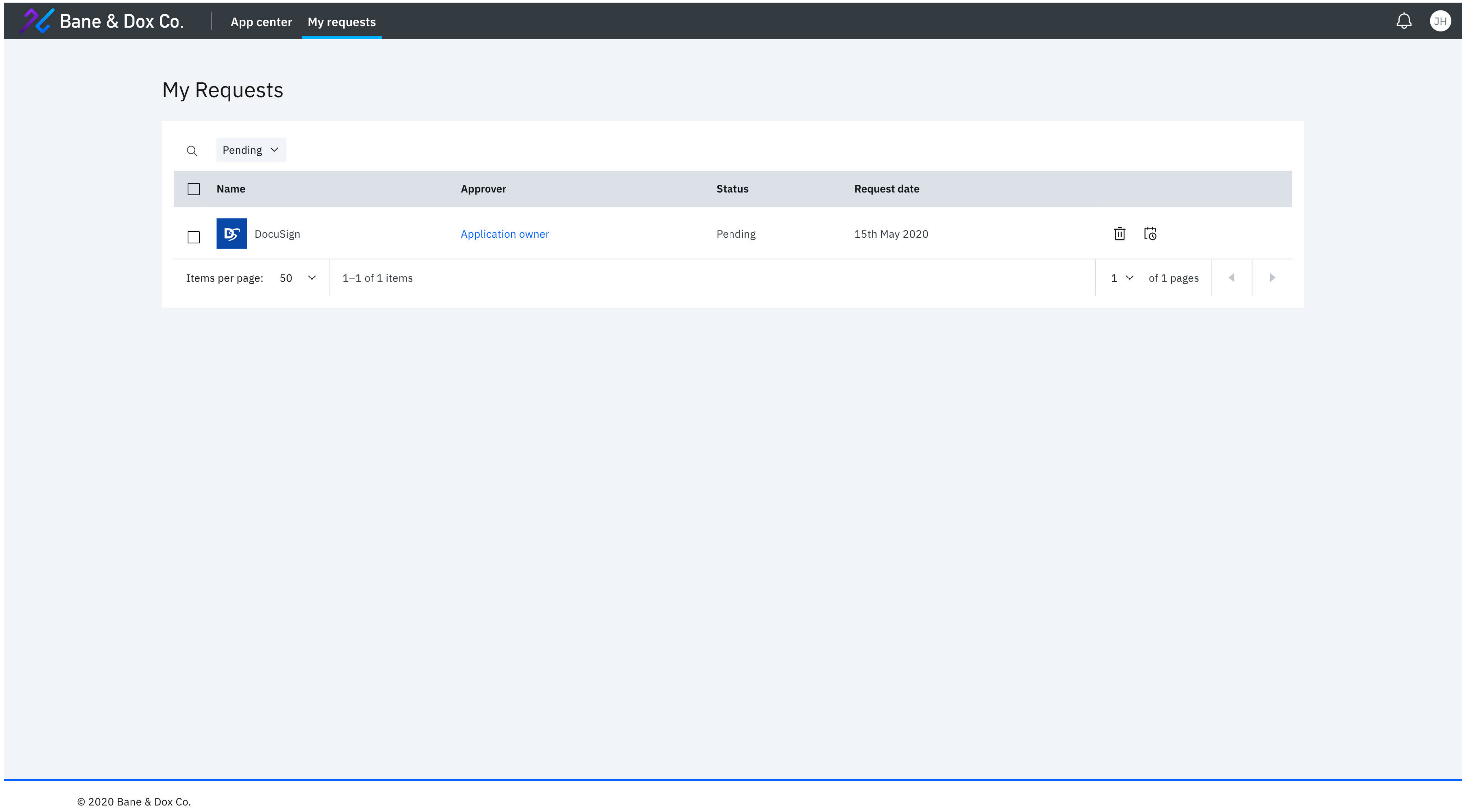
员工 · 单点登录 · **请求应用程序访问** · 注册并使用 MFA · 业务经理 · IT 管理员 · 开发者

上一页 下一页

员工：第 3 步（共 4 步）
请求应用程序访问

待审核申请

在待审核申请页面中，Jessica 可以查看她的待审核访问请求、这些请求已分配给谁以及当前状态。如果需要，她可以返回此处查看以添加更多详细信息来说明理由。



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.

下一步：
在启动板中新增应用

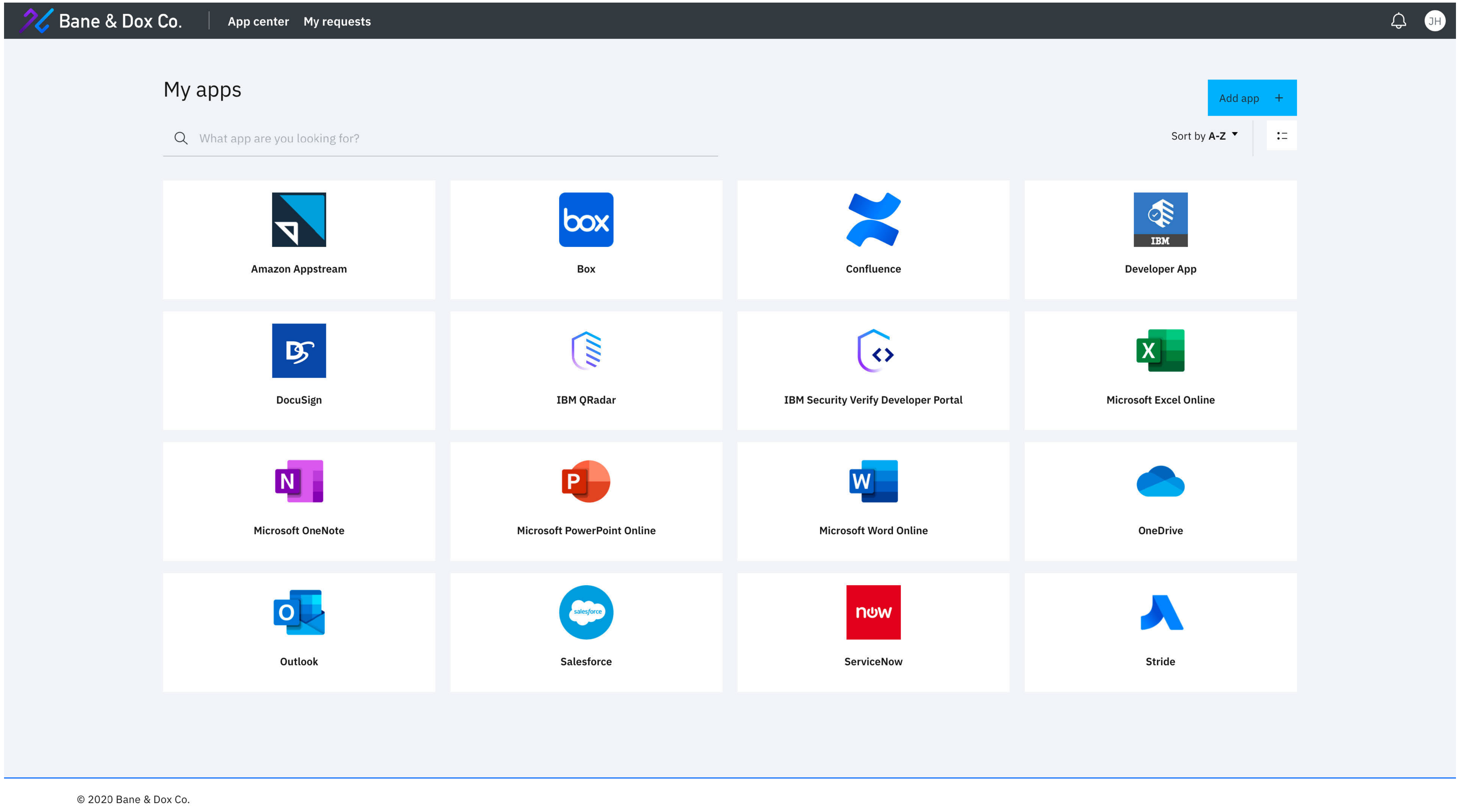
← →

员工 · 单点登录 · **请求应用程序访问** · 注册并使用 MFA · 业务经理 · IT 管理员 · 开发者

员工：第 4 步（共 4 步）
请求应用程序访问

在启动板中新增应用

一旦请求被应用负责人核准，她将看到 XYZ 已添加到启动板。

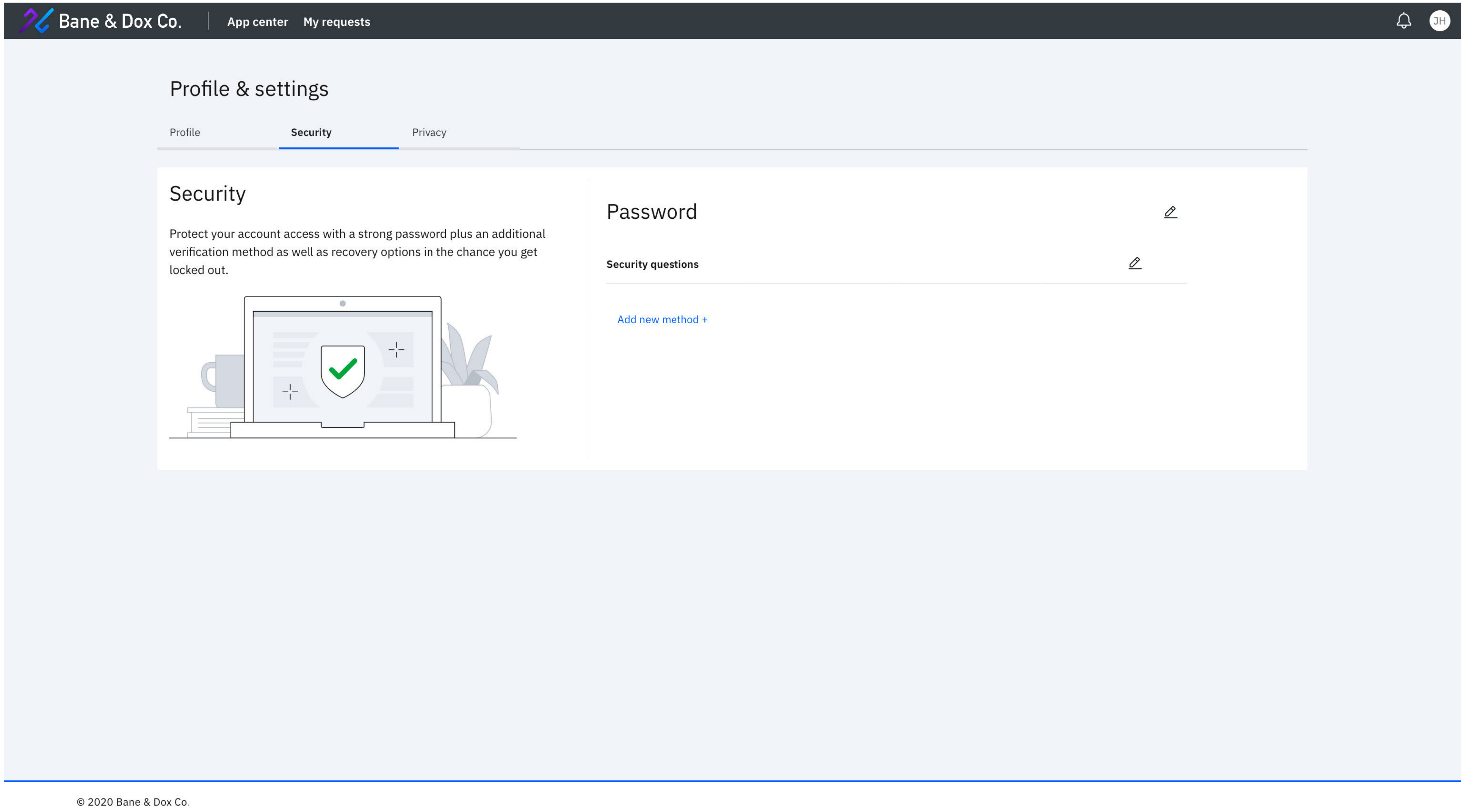


下一步：
向启动板添加新的身份验证设备

员工：第 1 步（共 3 步）
注册并使用 MFA

向启动板添加新的身份验证设备

Jessica 可以在安全设置页面上添加用于解决身份验证难题的设备和资源。她可以在手机上注册以使用 IBM Security Verify 移动应用来解决 MFA 难题或选择任何其他可用方法。



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

Add new method +

© 2020 Bane & Dox Co.

下一步：
MFA 注册

← →

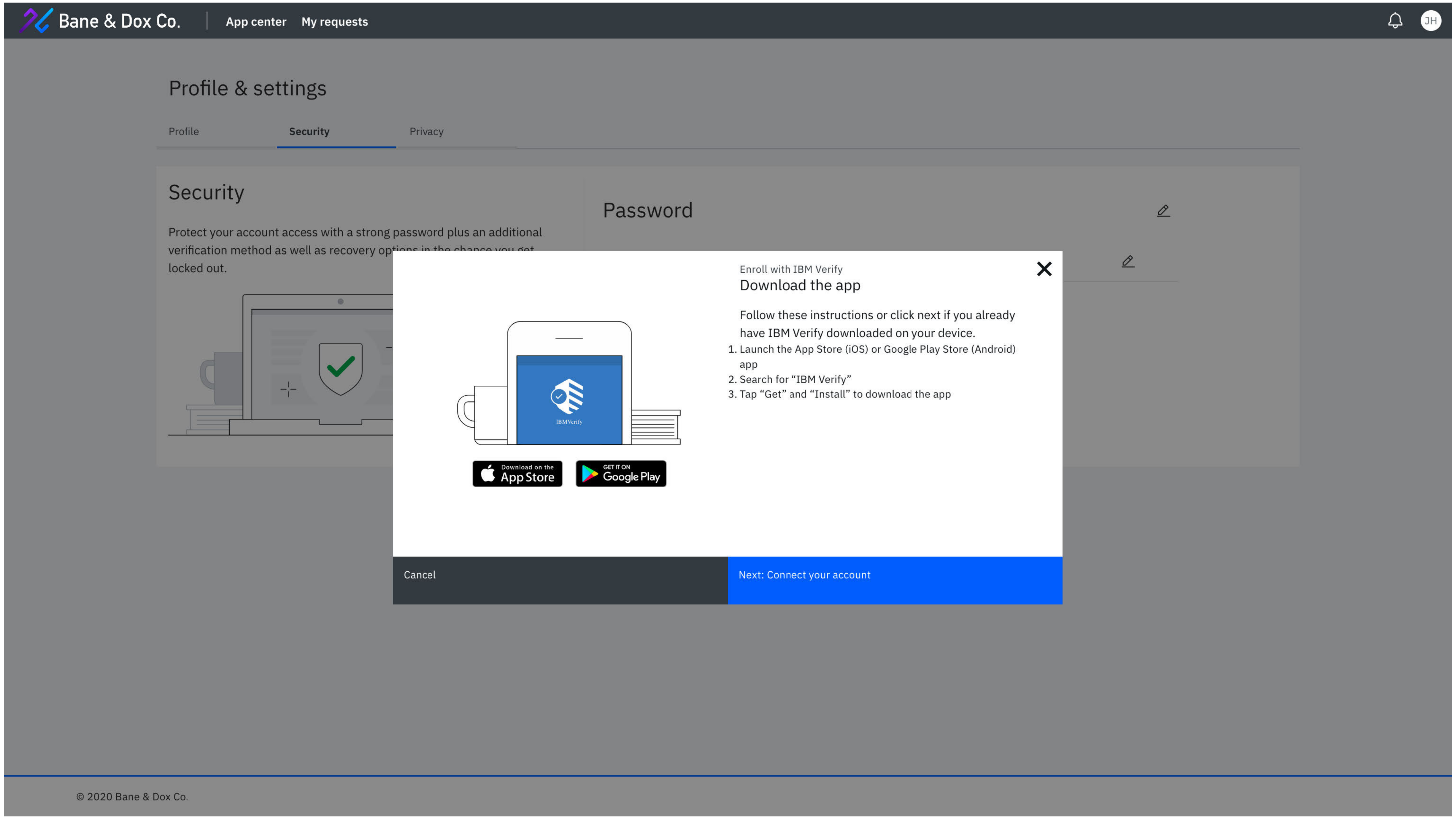
员工 — 单点登录 — 请求应用程序访问 — **注册并使用 MFA** — 业务经理 — IT 管理员 — 开发者

上一页 下一页

员工：第 2 步（共 3 步）
注册并使用 MFA

设置移动应用

Jessica 可以在安全设置页面上添加用于解决身份验证难题的设备和资源。她可以在手机上注册以使用 IBM Security Verify 移动应用来解决 MFA 难题或选择任何其他可用方法。



Bane & Dox Co. | App center My requests JH

Profile & settings

Profile | **Security** | Privacy

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

Cancel | Next: Connect your account

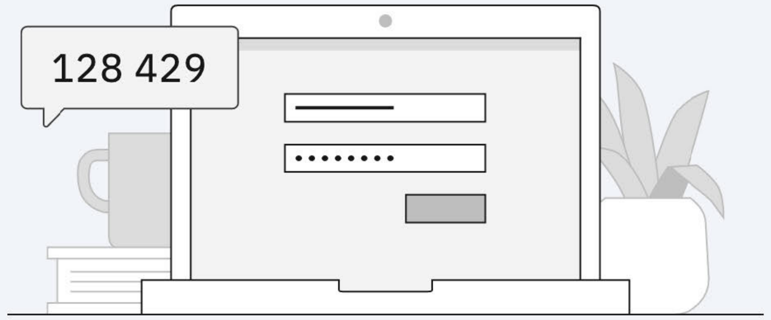
© 2020 Bane & Dox Co.

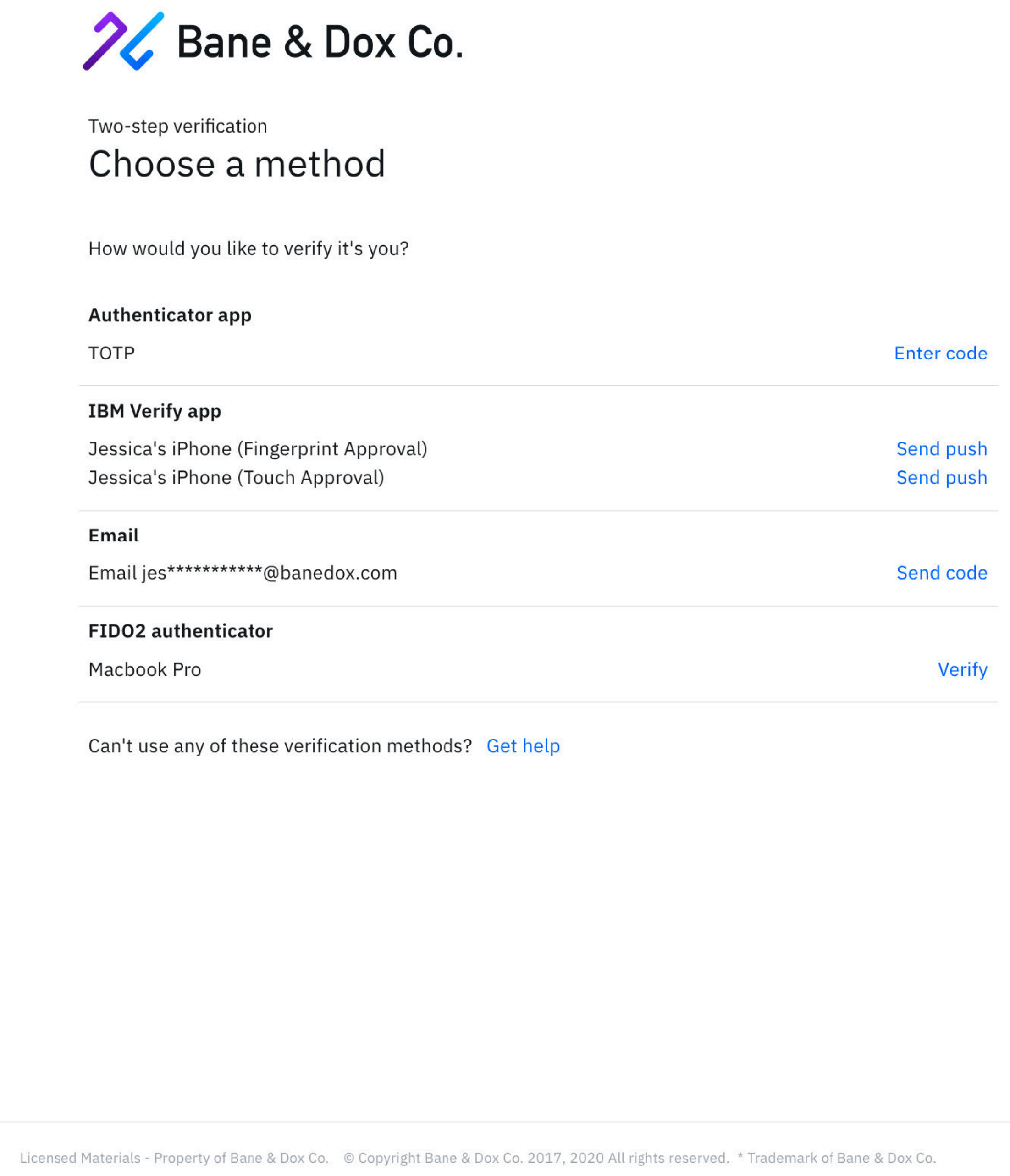
下一步：
选择 MFA 方法

员工：第 3 步（共 3 步）
注册并使用 MFA

选择 MFA 方法

现在，当 Jessica 登录到需要 MFA 的应用时，她可以选择对她来说最便捷的受支持身份验证方法。





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

下一步：
业务部门经理

IBM **Security** Verify

立即试用 Verify

业务部门经理

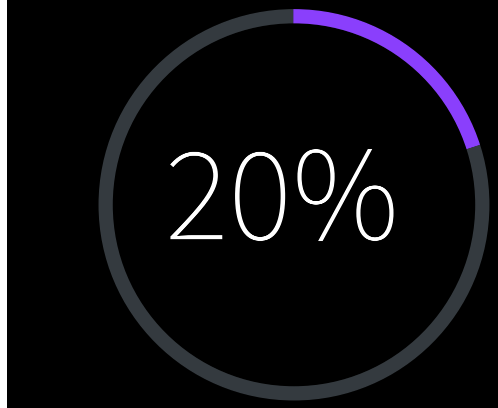
通过授权的控制来管理团队特定的应用程序权利。

业务部门经理需要快速向员工和客户提供新服务，以便保持竞争力。他们需要以业务的速度采取行动，而无需等待 IT。

首先：
在启动板待审核通知

←　→

查看



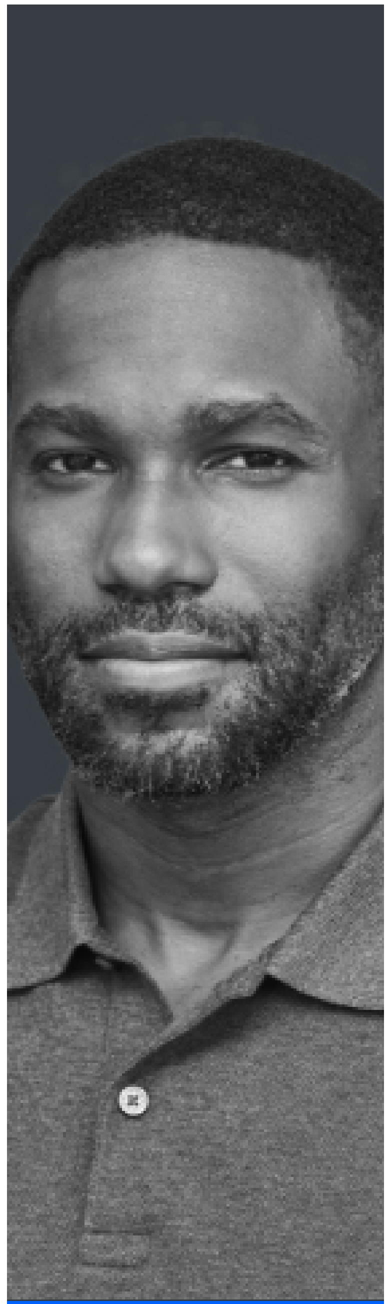
20% 到 50% 的 IT 帮助台呼叫与密码重置有关

世界经济论坛

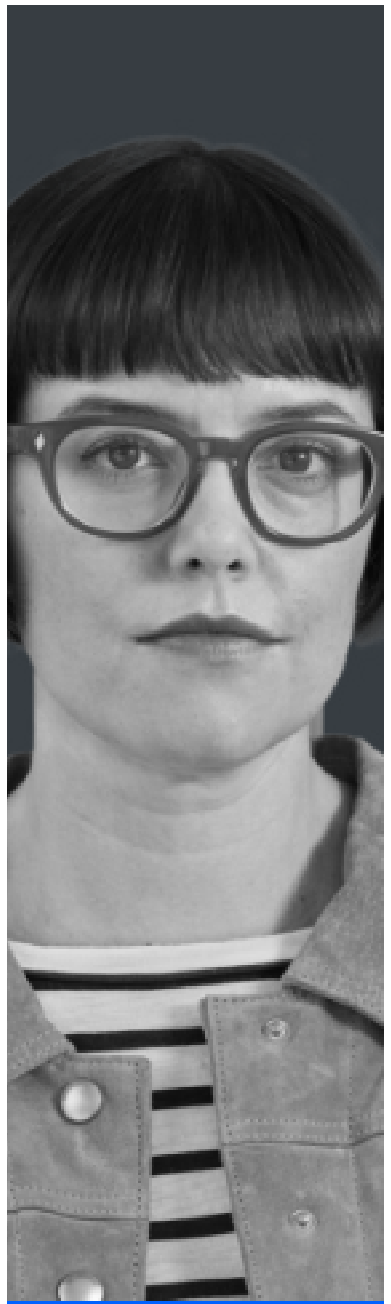
“我只是想把工作做完的时候，却因为工具和系统而停滞不前，真是令人沮丧。”

Jacob，员工

业务经理



查看



查看

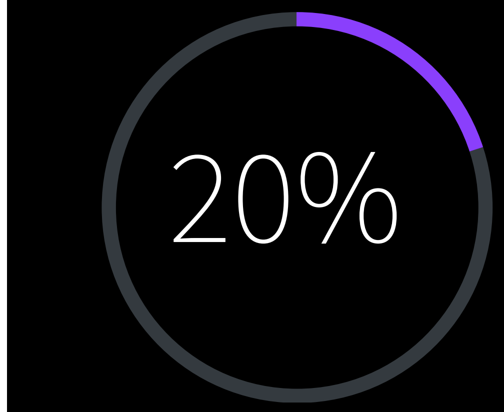
○ 员工　● **业务经理**　○ 处理访问请求　○ IT 管理员　○ 开发者

上一页　下一页

业务部门经理

通过授权的控制来管理团队特定的应用程序权利。

业务部门经理需要快速向员工和客户提供新服务，以便保持竞争力。他们需要以业务的速度采取行动，而无需等待 IT。



20% 到 50% 的 IT 帮助台呼叫与密码重置有关

世界经济论坛

“我只是想把工作做完的时候，却因为工具和系统而停滞不前，真是令人沮丧。”

Jacob，员工

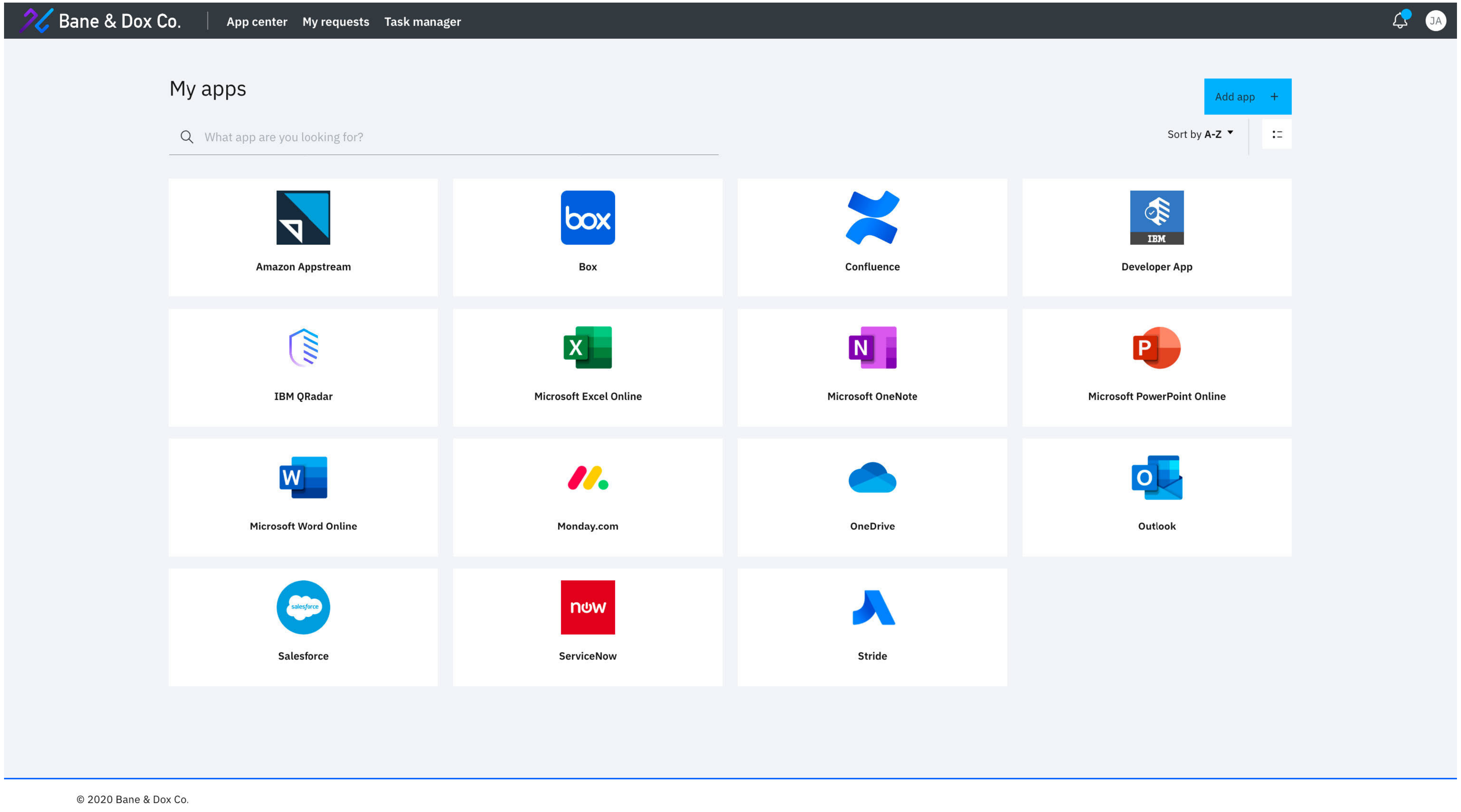
业务经理

- 员工
- **业务经理**
- 处理访问请求
  - 在启动板暂挂通知
  - 查看请求详细信息
  - 请求提供额外的理由
  - 核准/拒绝请求
- IT 管理员
- 开发者

业务部门经理：第 1 步（共 4 步）
处理访问请求

在启动板待审核通知

Jacob 是 Bane & Dox Co. 销售团队的经理。当登录到 IBM Security Verify 时，他将能够查看自己可以访问的所有应用程序。Jacob 已被授权管理组织的 DocuSign 并核准员工访问请求，而无需等待 IT。在这里，他可以查看应用请求的待审核通知。



下一步：
查看请求详细信息

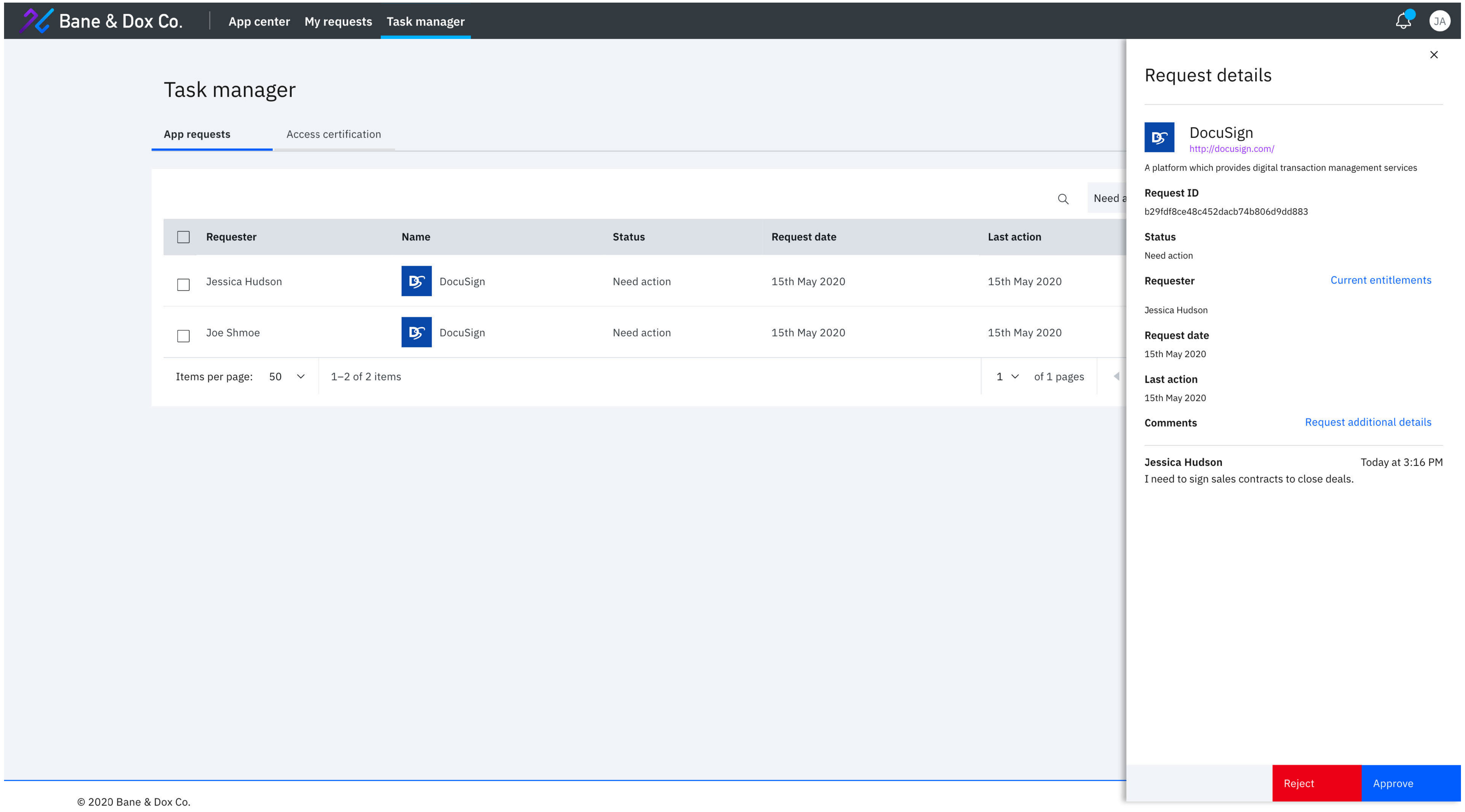
← →

○ 员工 ● 业务经理 ● **处理访问请求** ○ IT 管理员 ○ 开发者

业务部门经理：第 2 步（共 4 步）
处理访问请求

查看请求详细信息

从应用程序请求选项卡中，Jacob 可以查看 Jessica 的请求详细信息。如果需要，他可以要求 Jessica 为她的请求提供额外的理由。



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.

下一步：
请求提供额外的理由

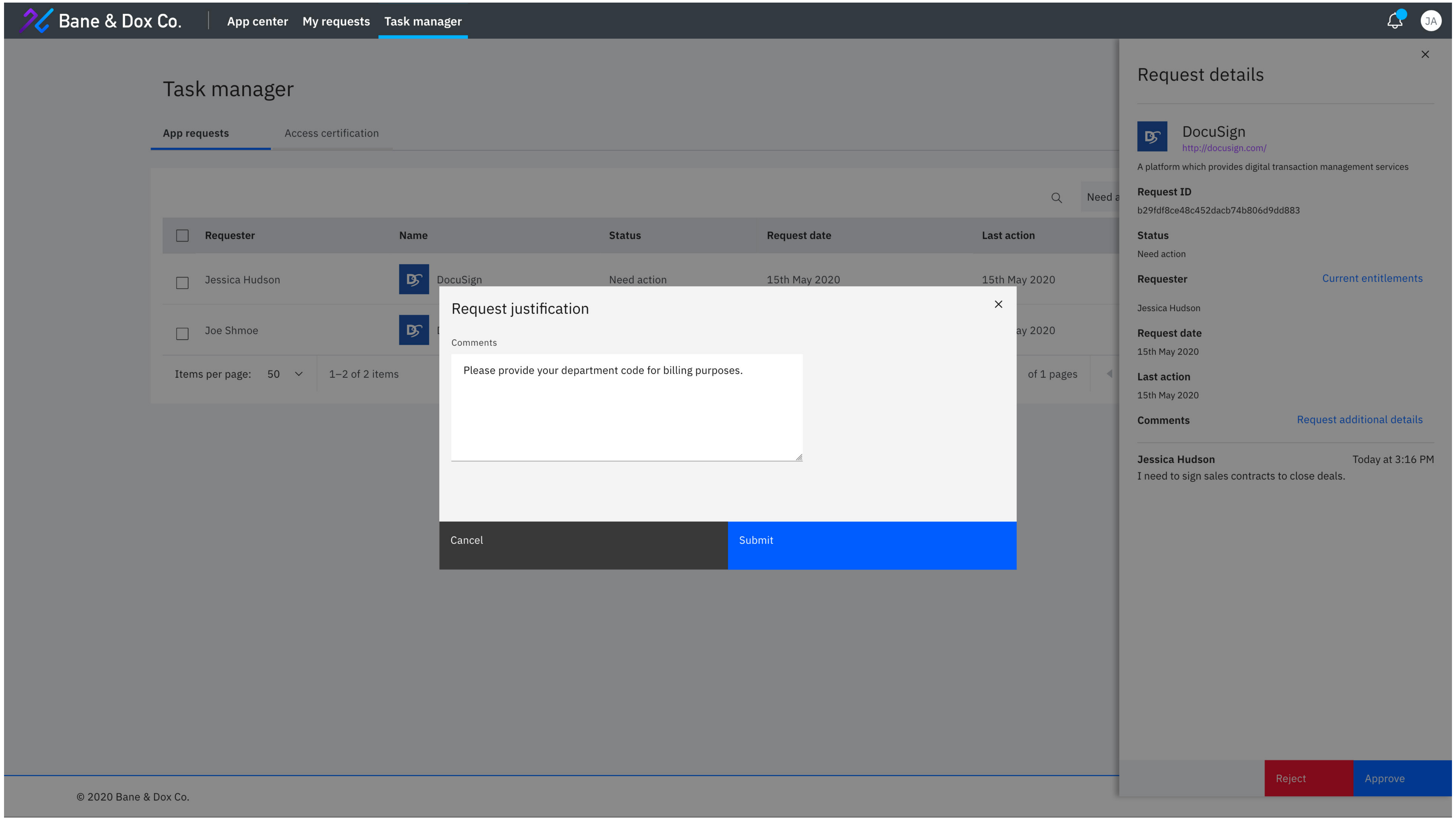
← →

员工 | 业务经理 | **处理访问请求** | IT 管理员 | 开发者

业务部门经理：第 3 步（共 4 步）
处理访问请求

请求提供额外的理由

他可以将请求退回，要求提供更多理由。



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	D			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

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

© 2020 Bane & Dox Co.

下一步：
核准/拒绝请求

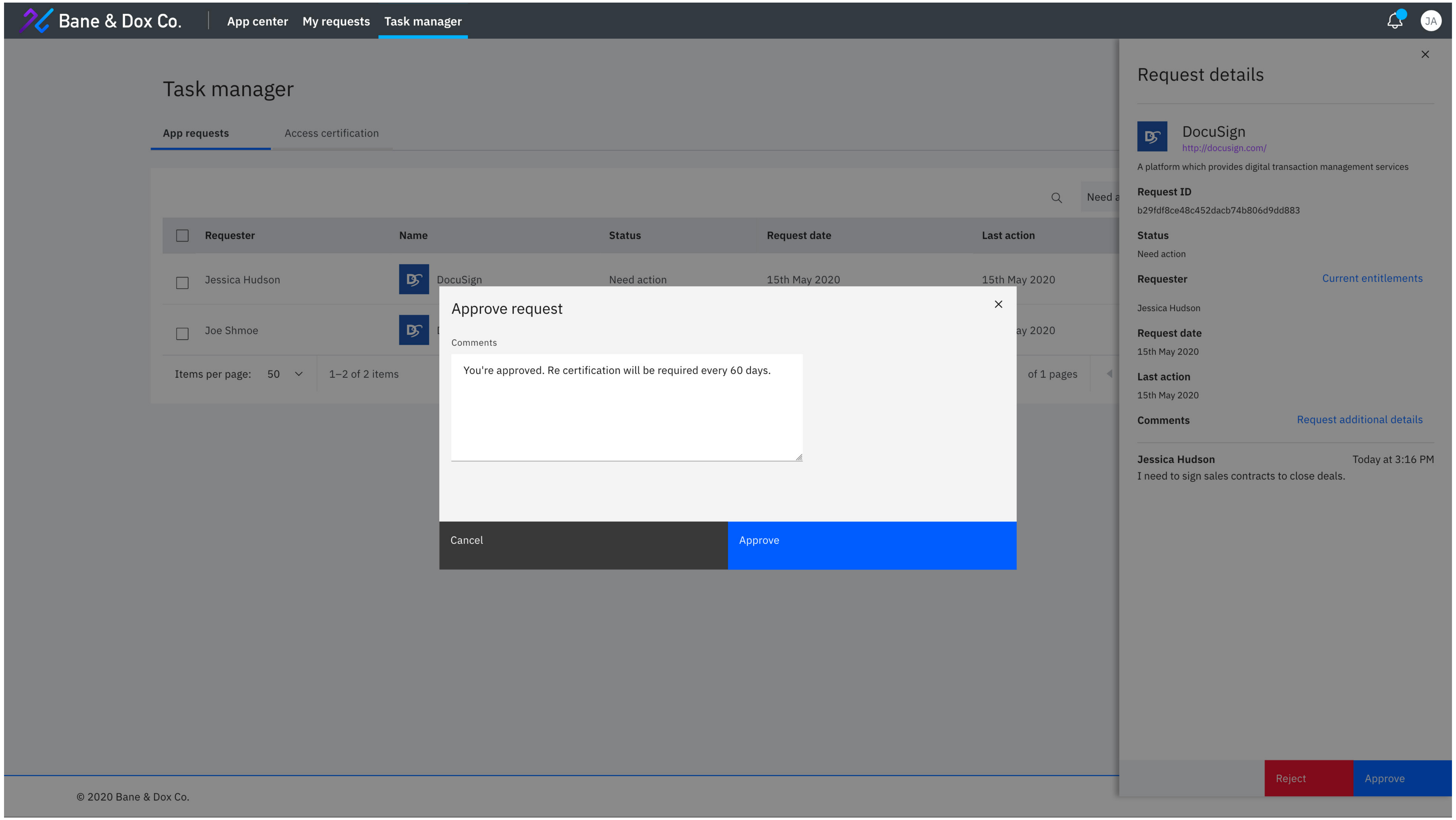
← →

员工 业务经理 **处理访问请求** IT 管理员 开发者

业务部门经理：第 4 步（共 4 步）
处理访问请求

核准/拒绝请求

或者，他可以核准/拒绝该请求。通过负责核准直接下属的访问权限，Jacob 使他的团队能够以业务的速度采取行动，而不会被 IT 流程所累。



Task manager

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

下一步：
IT 管理员

←　→

员工　业务经理　**处理访问请求**　IT 管理员　开发者

上一页　下一页

IT 管理员

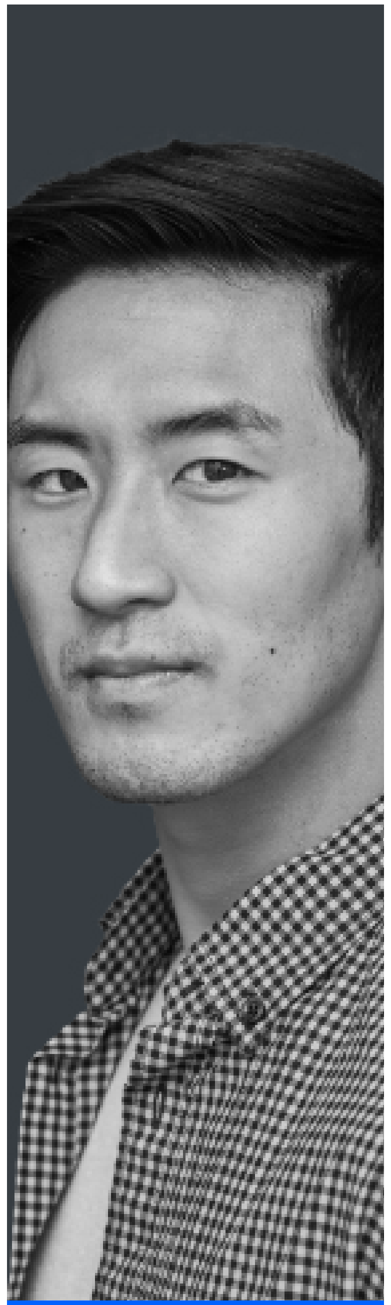
简化配置、在通用平台上扩展和自动进行风险保护。

IT 管理员需要满足轻松访问的业务需求，同时保护组织不受凭证滥用的影响 — 尽管他们可能面临时间、技能或资源的缺乏问题。在整合来自各种供应商的云应用程序时，团队也会感到手足无措，因此 SSO 和 MFA 的集成工作流变得至关重要。

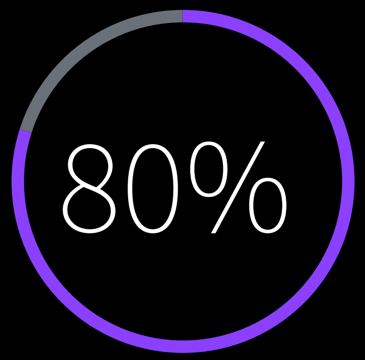
首先：
实时仪表板

← →

查看



查看



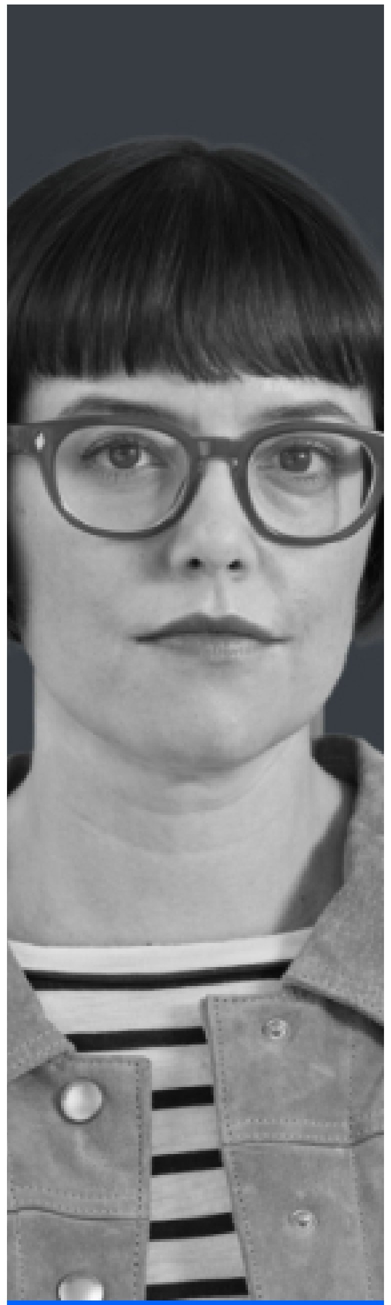
80% 由黑客攻击引起的违规与泄露和脆弱的凭证有关

世界经济论坛

“我需要提高组织的生产力，确保同事安全，并在此过程中考虑身份和访问相关风险的方方面面 — 所有一切同步进行。”

Scott，IT 管理员

IT 管理员



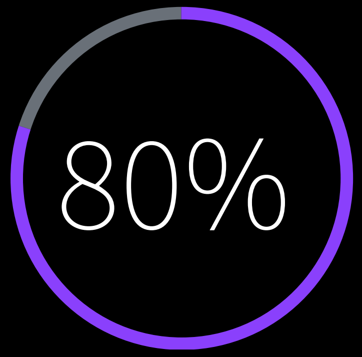
查看

○ 员工 ○ 业务经理 ● **IT 管理员** ○ 监控活动 ○ 自定义策略 ○ 管理用户和身份 ○ 添加应用程序 ○ 分析风险 ○ 开发者

IT 管理员

简化配置、在通用平台上扩展和自动进行风险保护。

IT 管理员需要满足轻松访问的业务需求，同时保护组织不受凭证滥用的影响 — 尽管他们可能面临时间、技能或资源的缺乏问题。在整合来自各种供应商的云应用程序时，团队也会感到手足无措，因此 SSO 和 MFA 的集成工作流变得至关重要。



80% 由黑客攻击引起的违规与泄露和脆弱的凭证有关

世界经济论坛

“我需要提高组织的生产力，确保同事安全，并在此过程中考虑身份和访问相关风险的方方面面 — 所有一切同步进行。” ”

Scott, IT 管理员

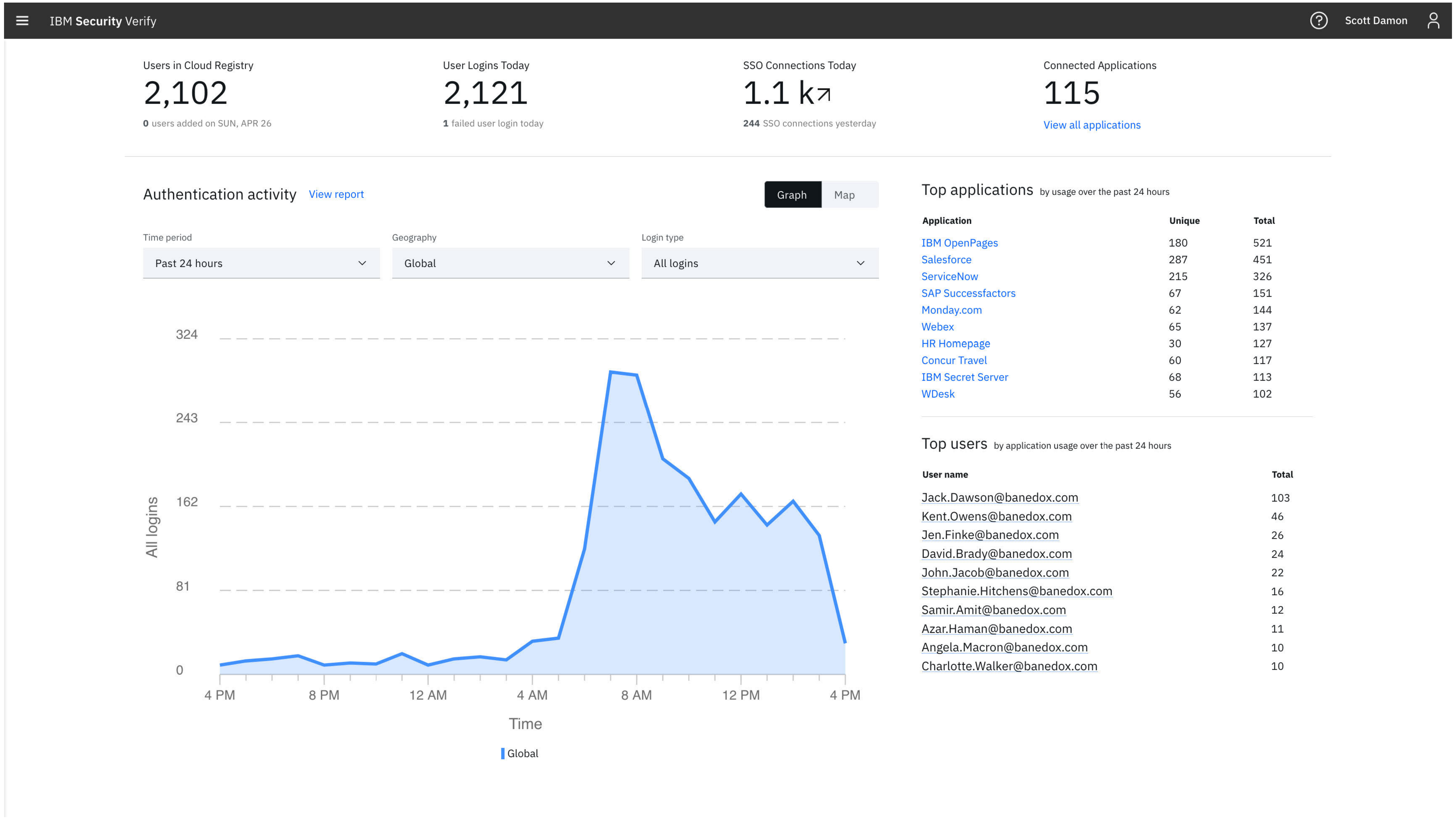
IT 管理员

- 员工
- 业务经理
- **IT 管理员**
  - 监控活动
    - 实时仪表板
    - 创建活动报告
    - 自适应访问活动报告
  - 自定义策略
    - 策略编辑器
    - 将规则添加到策略
    - 自适应访问
  - 管理用户和身份
    - 管理用户
    - 管理群组
    - 管理用户属性
    - Active Directory 和 LDAP
    - 社交登录
  - 添加应用程序
    - 查看应用程序
    - 搜索要添加的应用程序
    - 添加核准访问权限的负责人
    - 配置登录设置
    - 配置权利
    - 设置定期重新认证访问权限
  - 分析风险
    - 分析报告
    - 查看排列好的策略违规行为
    - 采取建议的补救措施
- 开发者

IT 管理员：第 1 步（共 3 步）
监控活动

实时仪表板

IBM Security Verify 的管理仪表板提供组织内身份验证活动的全局概览。Scott 是一名 IT 管理员，他可以按时段或地域进行筛选，以便更好地了解用户趋势。



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

Graph Map

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

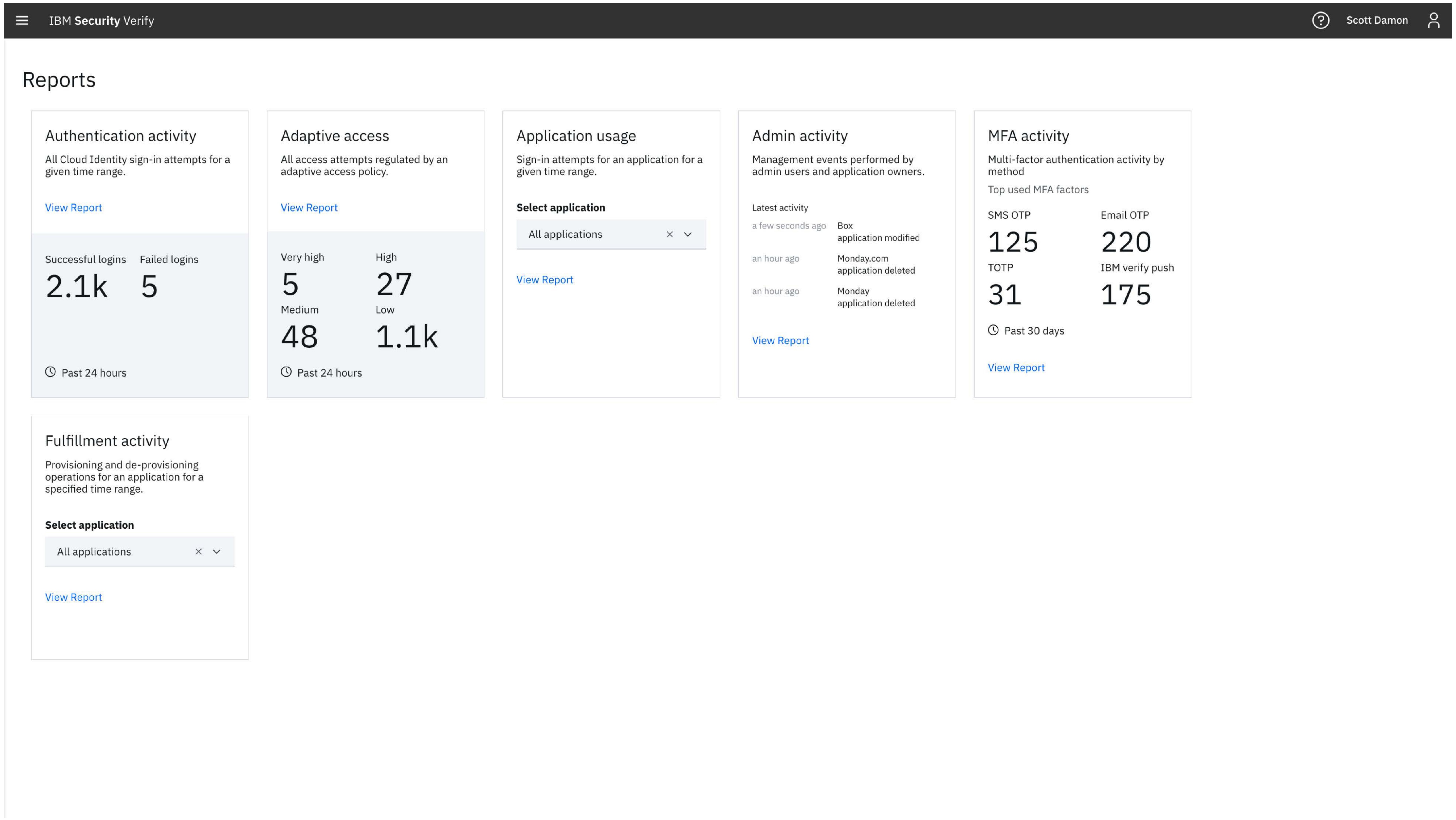
下一步：
创建活动报告

← →

IT 管理员：第 2 步（共 3 步）
监控活动

创建活动报告

Verify 的报告界面使 Scott 能够实时筛选最近的活动数据以快速诊断问题。在身份验证活动、自适应访问、应用程序使用、管理员活动和 MFA 活动中，他可以深入了解其组织的访问和身份验证数据，从而收集洞察并进行故障诊断。



Reports

Authentication activity
All Cloud Identity sign-in attempts for a given time range.
View Report

Successful logins	Failed logins
2.1k	5

Past 24 hours

Adaptive access
All access attempts regulated by an adaptive access policy.
View Report

Very high	High
5	27
Medium	**Low**
48	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	Email OTP
125	220
TOTP	**IBM verify push**
31	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

下一步：
自适应访问活动报告

← →

员工　业务经理　IT 管理员　**监控活动**　自定义策略　管理用户和身份　添加应用程序　分析风险　开发者

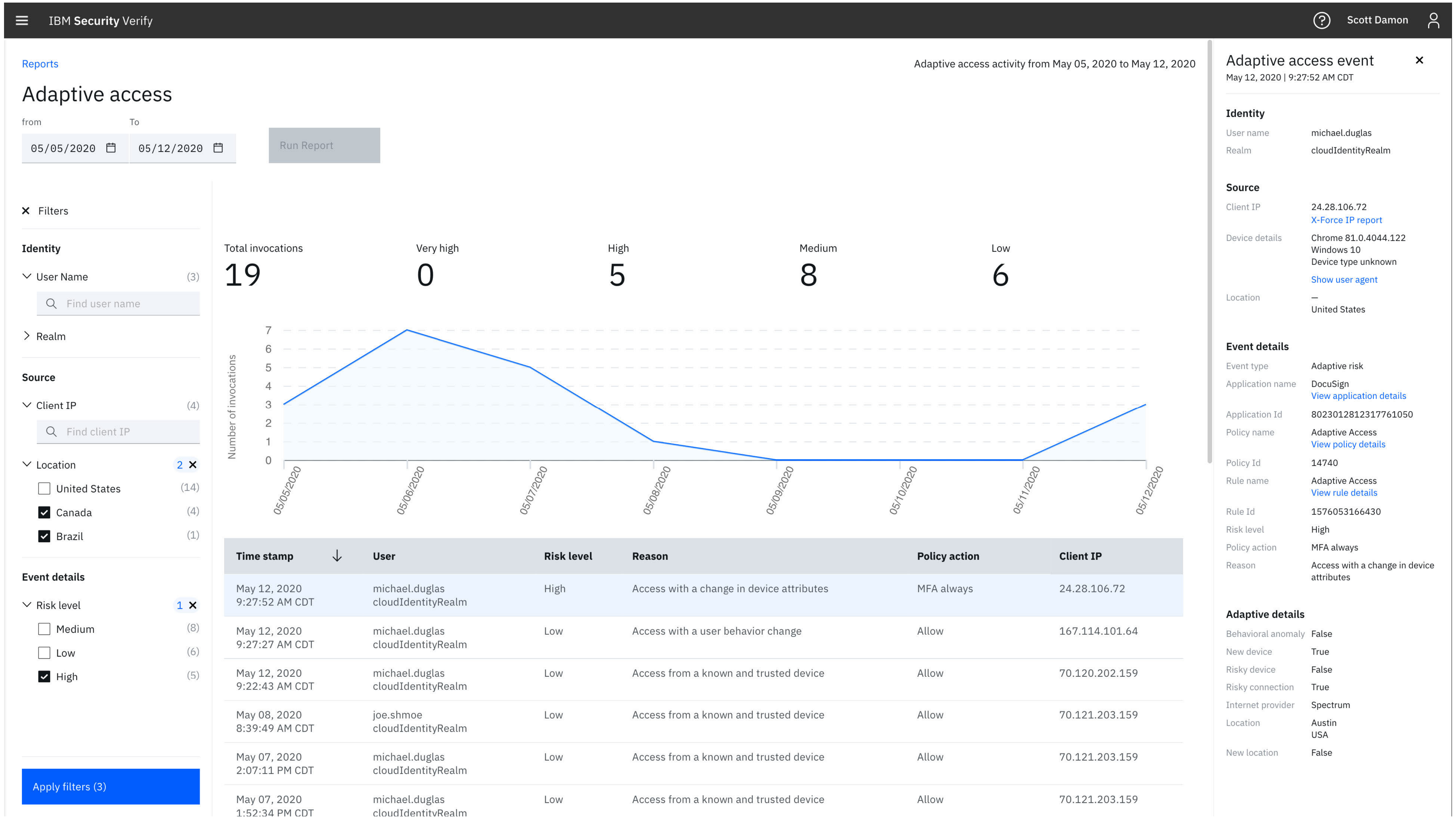
上一页　下一页

IT 管理员：第 3 步（共 3 步）
监控活动

自适应访问活动报告

例如，在自适应访问报告中，Scott 可以使用自适应访问策略和记录的事件参数查看应用程序的所有最近登录。通过使用 Verify 中的报告，他可以对高风险事件进行诊断和故障排除，并在必要时采取行动。

自适应访问交互式演示



IBM Security Verify | Scott Damon

Reports

Adaptive access

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

from 05/05/2020 | To 05/12/2020 | Run Report

✕ Filters

Identity

- User Name (3) — Find user name
- Realm

Source

- Client IP (4) — Find client IP
- Location 2 ✕
  - ☐ United States (14)
  - ☑ Canada (4)
  - ☑ Brazil (1)

Event details

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

Apply filters (3)

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

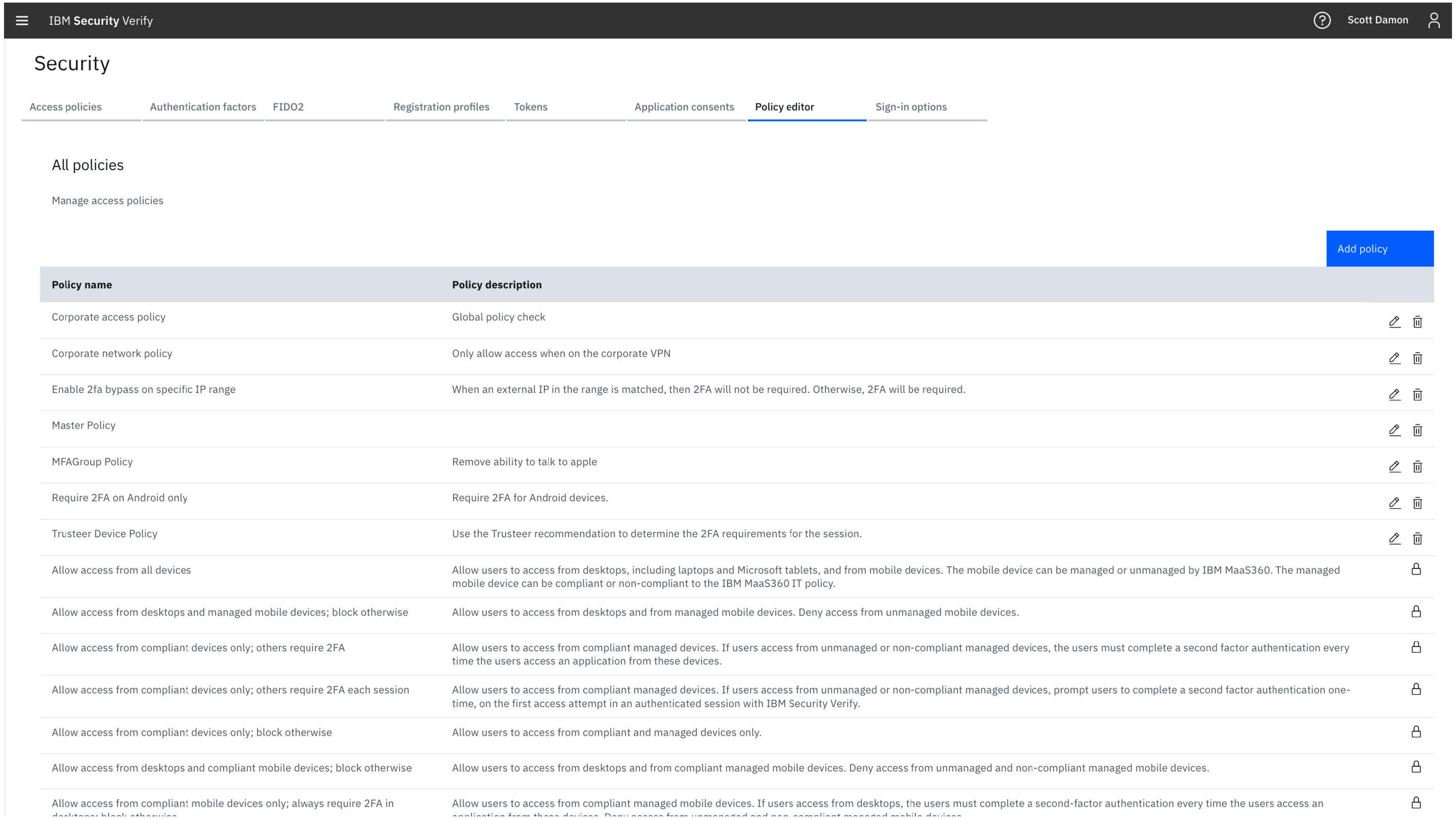
Behavioral anomaly	False
New device	True
Risky device	False
Risky connection	True
Internet provider	Spectrum
Location	Austin USA
New location	False

下一步：
策略编辑器

IT 管理员：第 1 步（共 3 步）
自定义策略

策略编辑器

在访问策略编辑器中，Scott 可以创建额外的自定义访问策略以使用其组织的应用程序。缺省情况下包含了一些策略，例如始终允许访问、始终需要 2FA 或开始每个新会话时需要 2FA。



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 desktops; block otherwise	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 application from these devices. Deny access from unmanaged and non-compliant managed mobile devices.

下一步：
将规则添加到策略

←　→

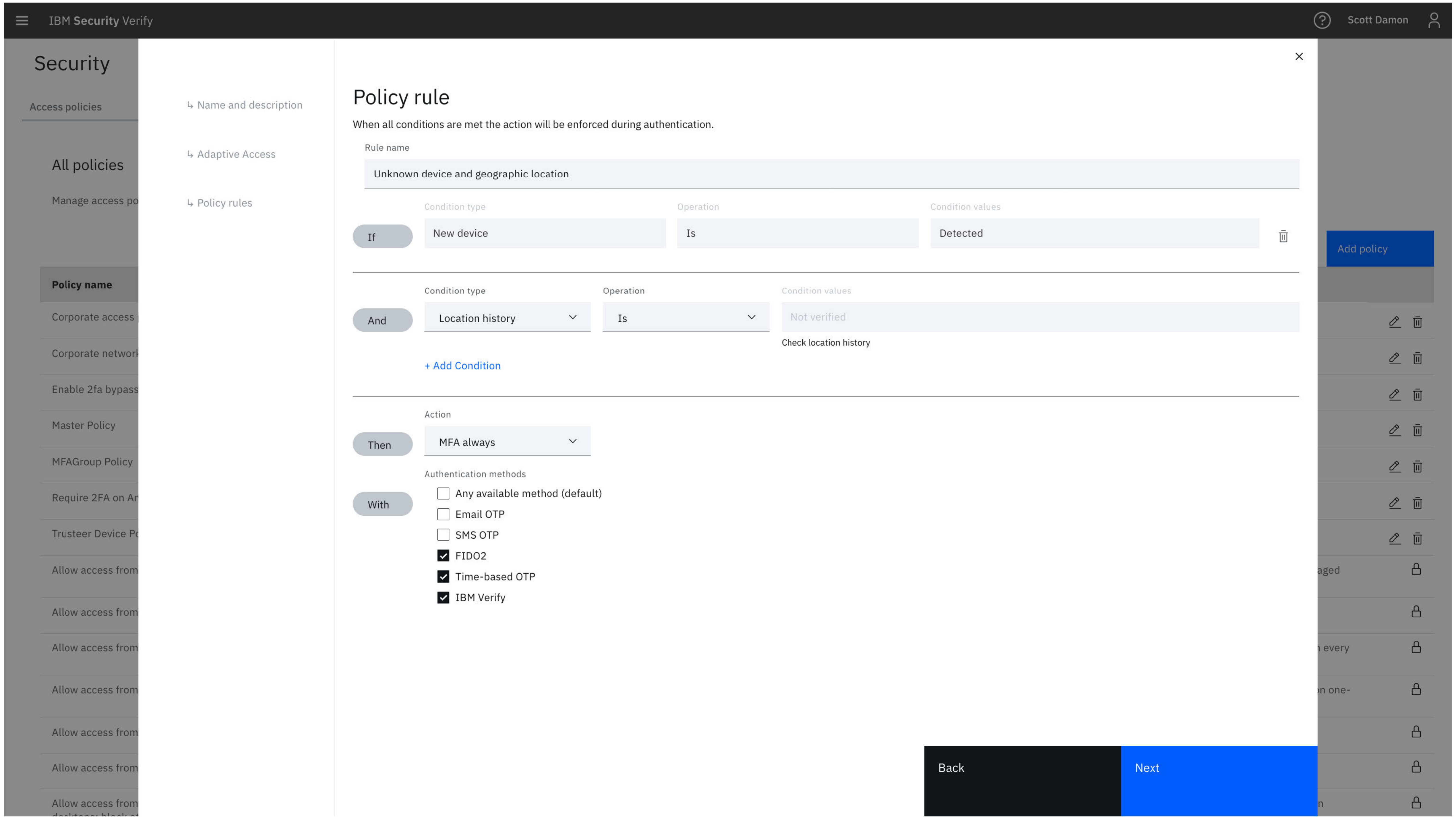
员工　业务经理　IT 管理员　监控活动　**自定义策略**　管理用户和身份　添加应用程序　分析风险　开发者

IT 管理员：第 2 步（共 3 步）

自定义策略

将规则添加到策略

Scott 可以根据设备、组成员资格、IP 和地理位置等条件轻松配置规则，允许或阻止访问或发起 MFA 质询。



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

下一步：
自适应访问

← →

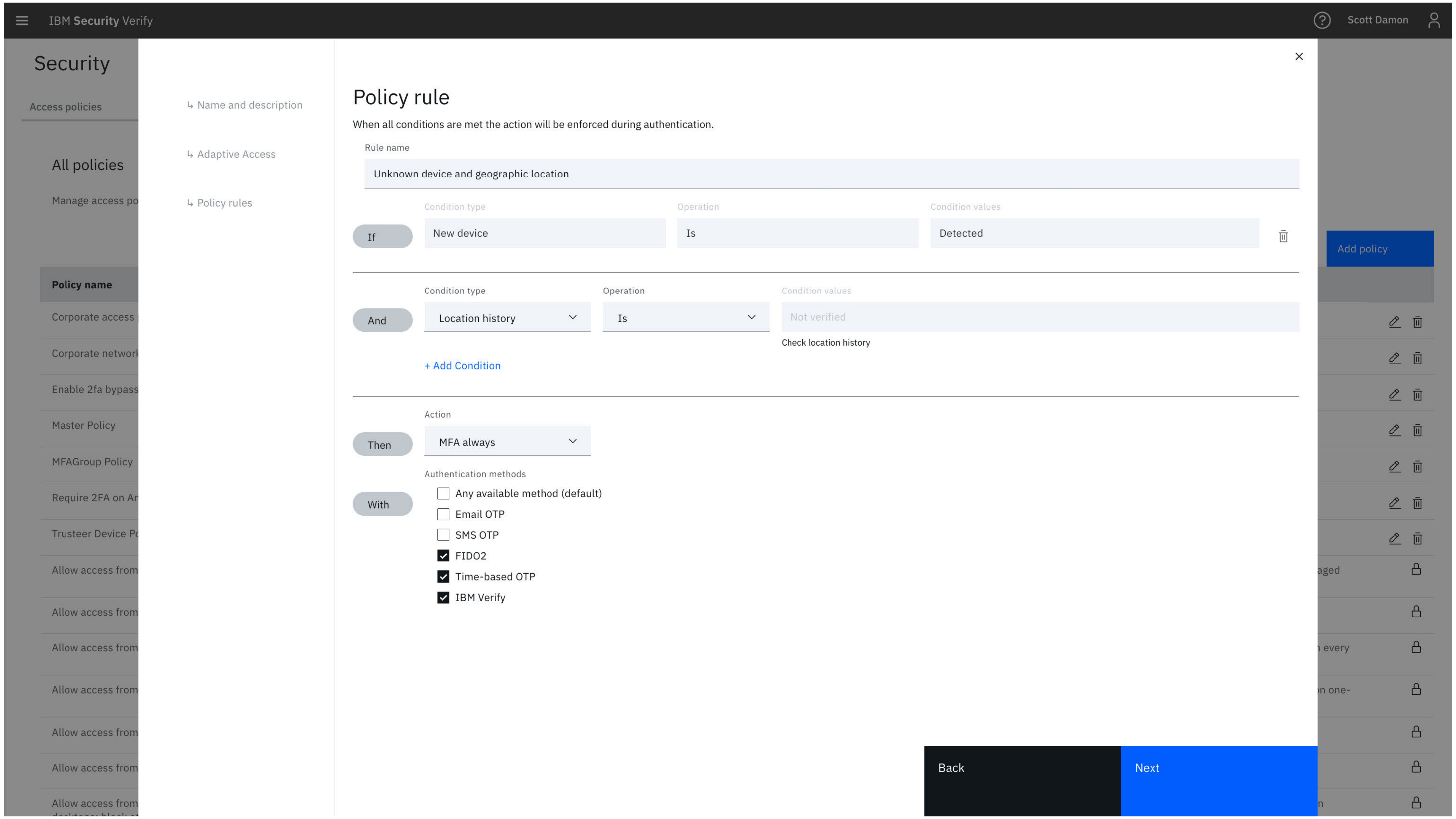
员工 · 业务经理 · IT 管理员 · 监控活动 · **自定义策略** · 管理用户和身份 · 添加应用程序 · 分析风险 · 开发者

IT 管理员：第 3 步（共 3 步）
自定义策略

自适应访问

他还可以选择通过自适应访问策略启用基于风险的身份验证，自动考虑深层的用户、设备、活动、环境和行为上下文。自适应访问通过由 AI 提供支持的一组强大的上下文参数确定总体风险水平。凭借持续的身份验证，低风险用户获得无障碍访问权限，而高风险用户被自动质询或阻止。

自适应访问交互式演示



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

下一步：
管理用户

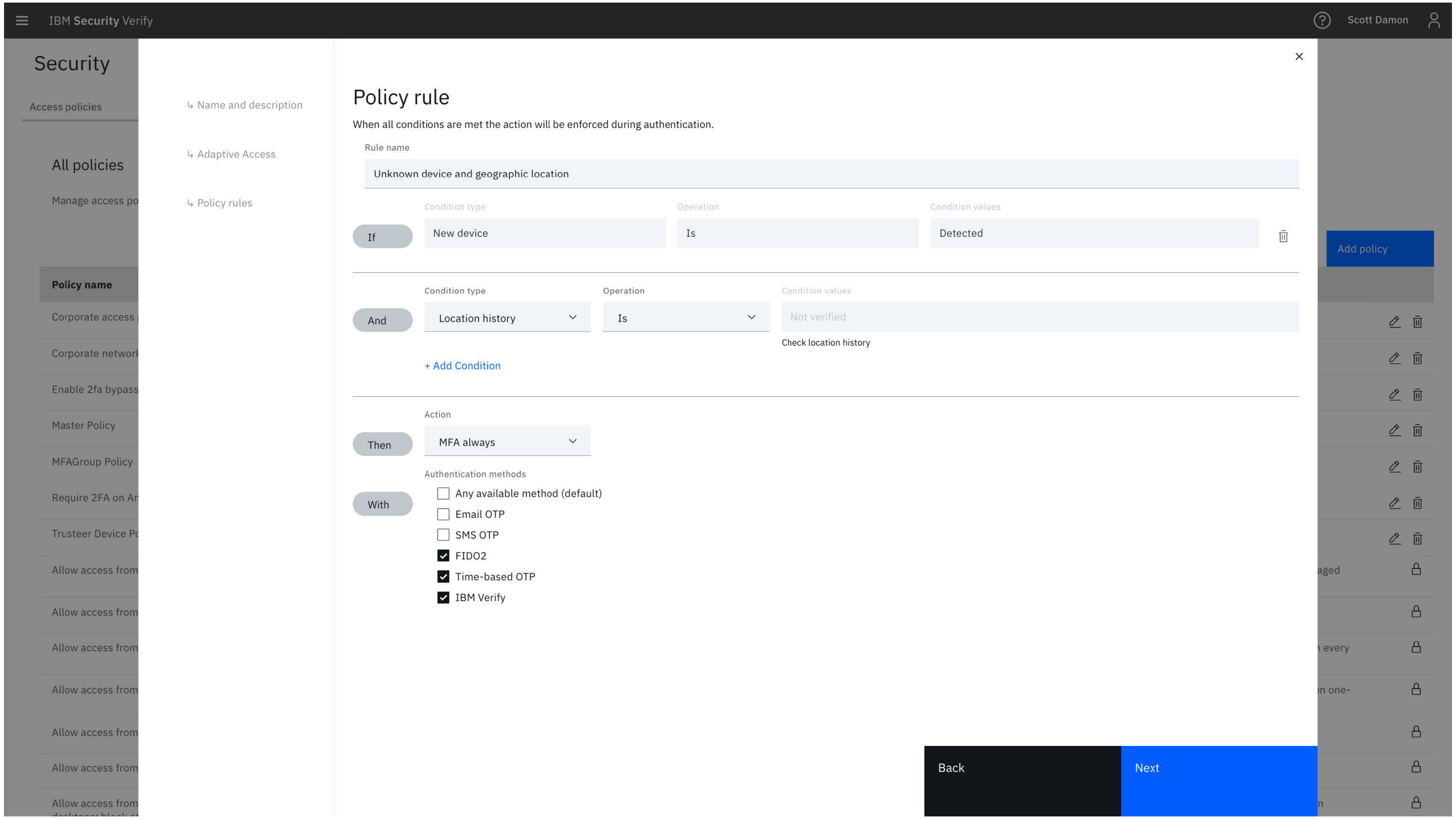
← →

员工 业务经理 IT 管理员 监控活动 **自定义策略** 管理用户和身份 添加应用程序 分析风险 开发者

IT 管理员：第 1 步（共 5 步）
管理用户和身份源

管理用户

Scott 可以使用简单的配置界面添加新用户。他可以从头开始添加属性，也可以选择从各种身份来源（如 Cloud Directory、Active Directory 或 IBMid）中提取数据。



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

下一步：
管理群组

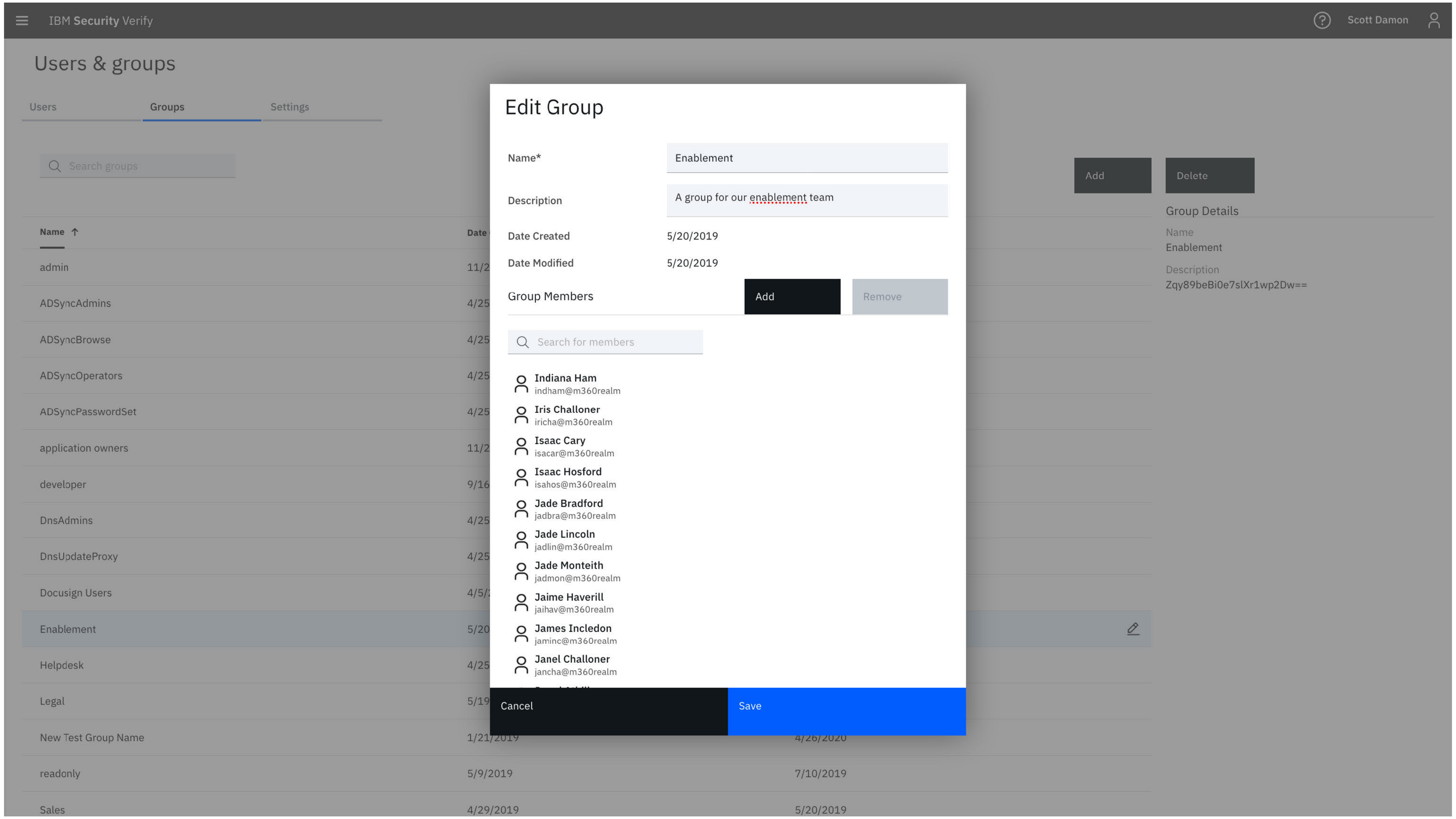
← →

○ 员工 ○ 业务经理 ● IT 管理员 ● 监控活动 ● 自定义策略 ● **管理用户和身份** ○ 添加应用程序 ○ 分析风险 ○ 开发者

IT 管理员：第 2 步（共 5 步）
管理用户和身份源

管理群组

无论是按部门、职务还是更独特的属性进行管理，群组都可以帮助使组织内的访问更加模块化。例如，Scott 可以添加一个新的 Bane & Dox Co.。销售群组有助于该集合的个人访问常见销售应用程序。如果他将现有目录整合到 Verify 中，则该目录的群组将被保留。



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

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

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

下一步：
管理用户属性

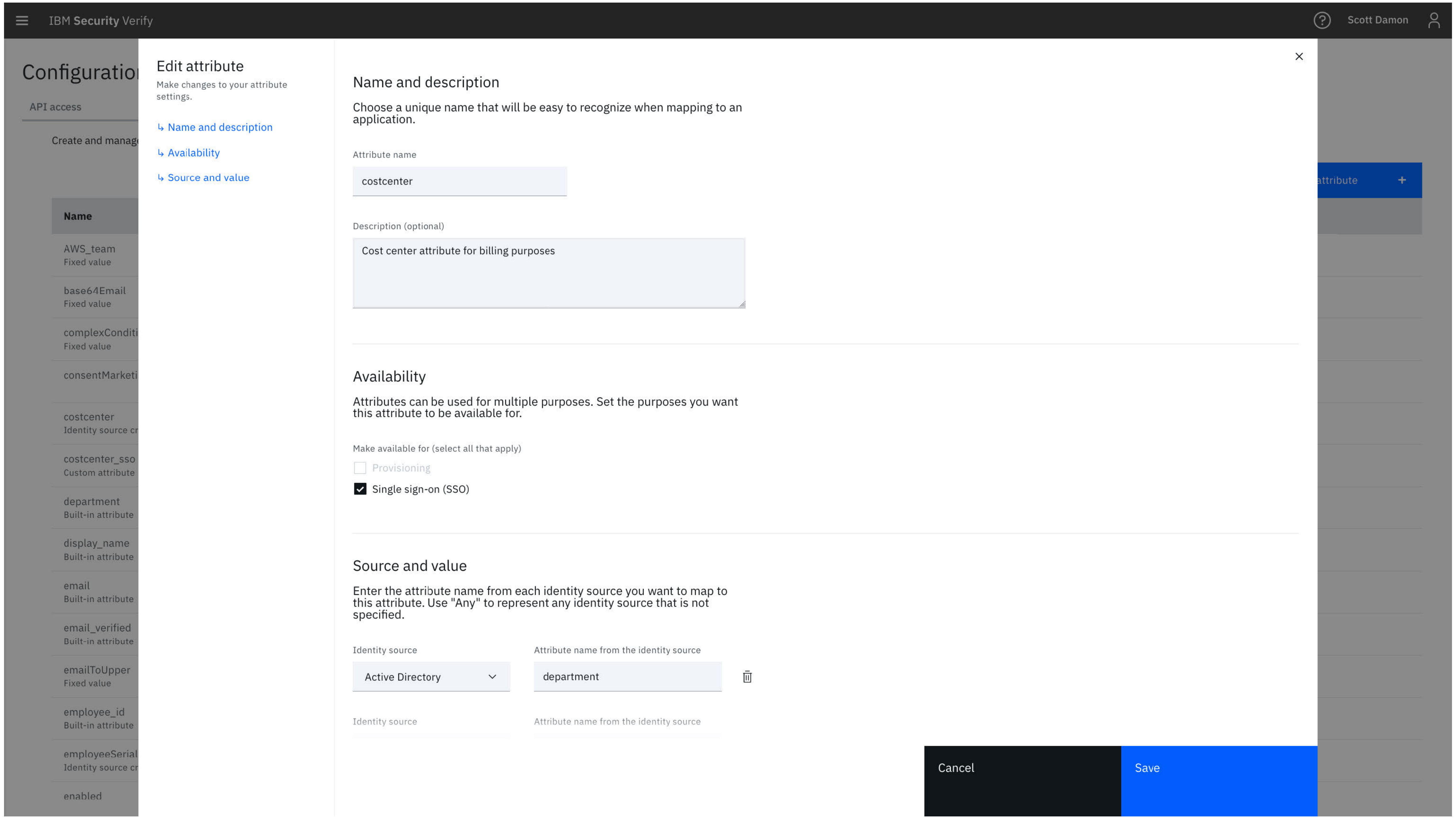
←　→

员工　业务经理　IT 管理员　监控活动　自定义策略　**管理用户和身份**　添加应用程序　分析风险　开发者

IT 管理员：第 3 步（共 5 步）
管理用户和身份源

管理用户属性

尽管 Verify 缺省包含数十种最常见的用户属性，Scott 还可以从他连接的任何身份源链接其他属性，或者在需要时创建自定义属性。然后可以在身份源和应用程序中引用这些属性，用于单点登录、配置、创建概要文件等。



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

下一步：
Active Directory 和 LDAP

← →

员工　业务经理　IT 管理员　监控活动　自定义策略　管理用户和身份份　添加应用程序　分析风险　开发者

上一页　下一页

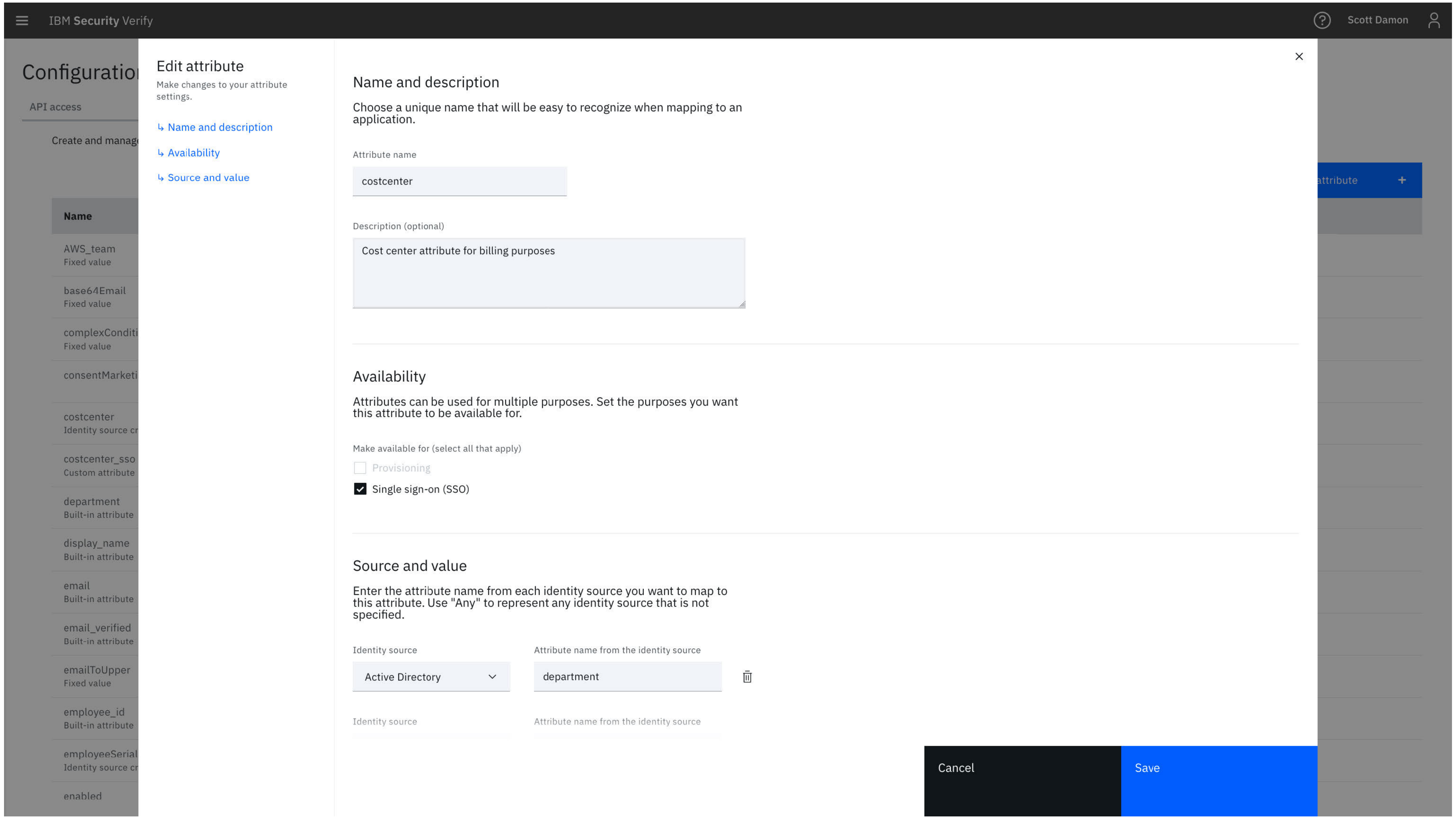
IBM **Security** Verify

立即试用 Verify

IT 管理员：第 4 步（共 5 步）
管理用户和身份源

Active Directory 和 LDAP

Scott 可以将 Verify 配置为连接到现有的 Active Directory 或 LDAP 身份源，甚至是非标准目录、数据库或外部服务。



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

下一步：
社交登录

← →

员工 业务经理 IT 管理员 监控活动 自定义策略 **管理用户和身份** 添加应用程序 分析风险 开发者

上一页 下一页

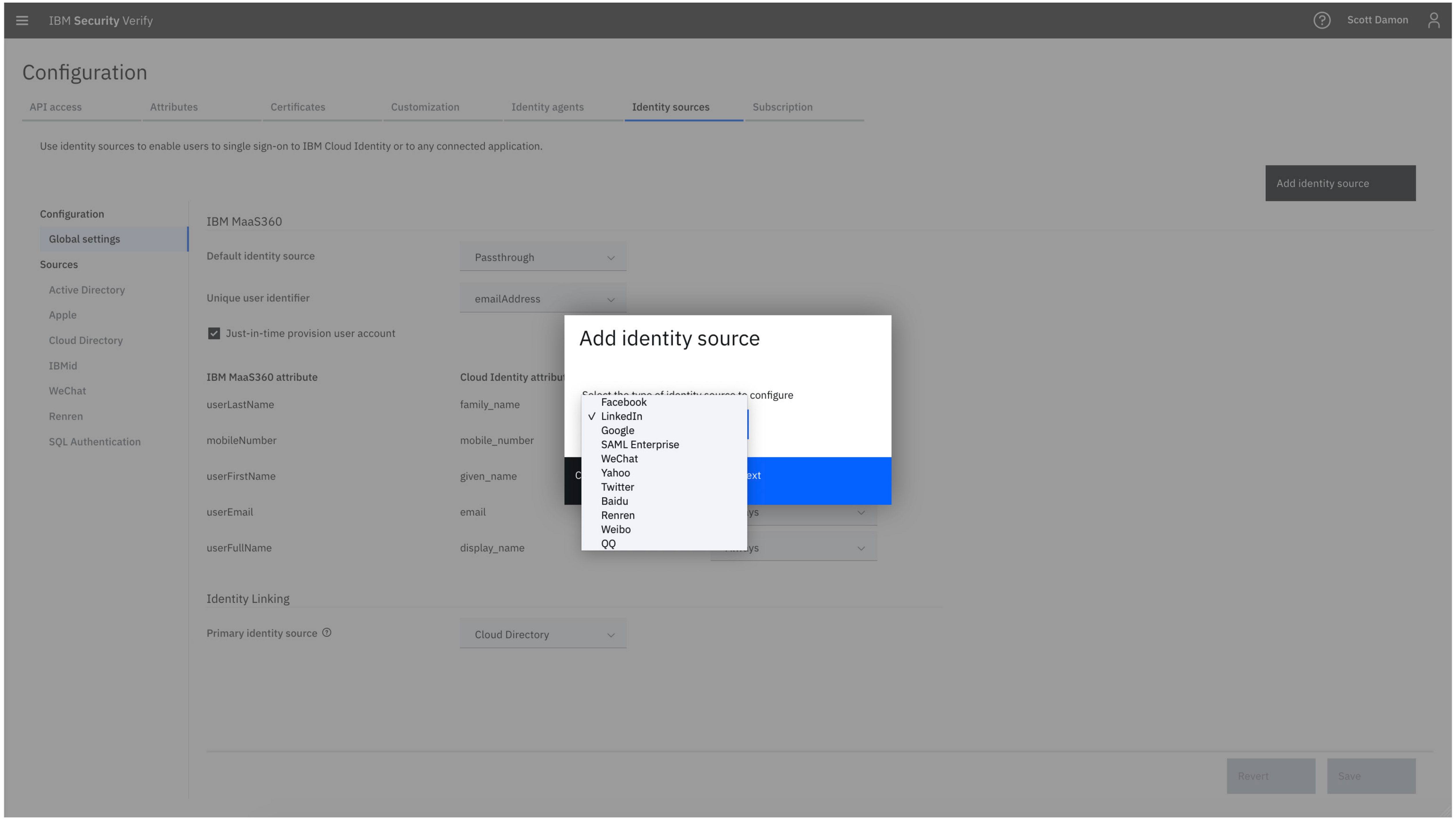
IBM **Security** Verify

立即试用 Verify

IT 管理员：第 5 步（共 5 步）
管理用户和身份源

社交登录

Scott 还可以链接各种社交登录提供商，为他的用户提供更多选择，包括 Google 和 LinkedIn 等特定地区提供商。



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 attribut
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

下一步：
查看应用程序

← →

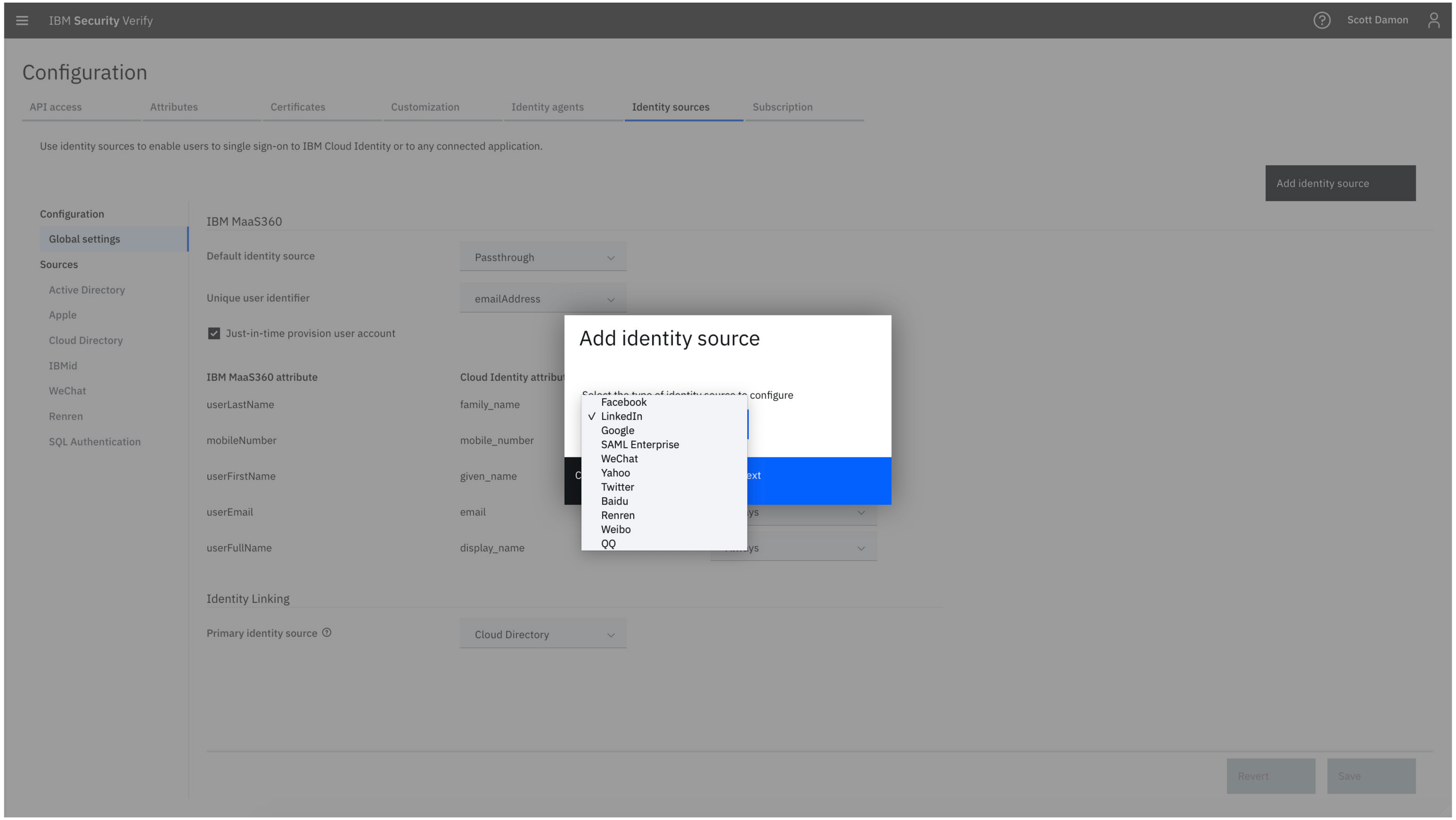
员工　业务经理　IT 管理员　监控活动　自定义策略　**管理用户和身份**　添加应用程序　分析风险　开发者

上一页　下一页

IT 管理员：第 1 步（共 6 步）
添加应用程序

查看应用程序

Verify 支持数百个开箱即用的 SaaS 应用程序，实现了自定义应用的简化集成，并提供轻量级应用程序网关以扩展对本地应用的支持。Scott 可以从单一界面管理其组织的所有应用。



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 attribut
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

下一步：
搜索要添加的应用程序

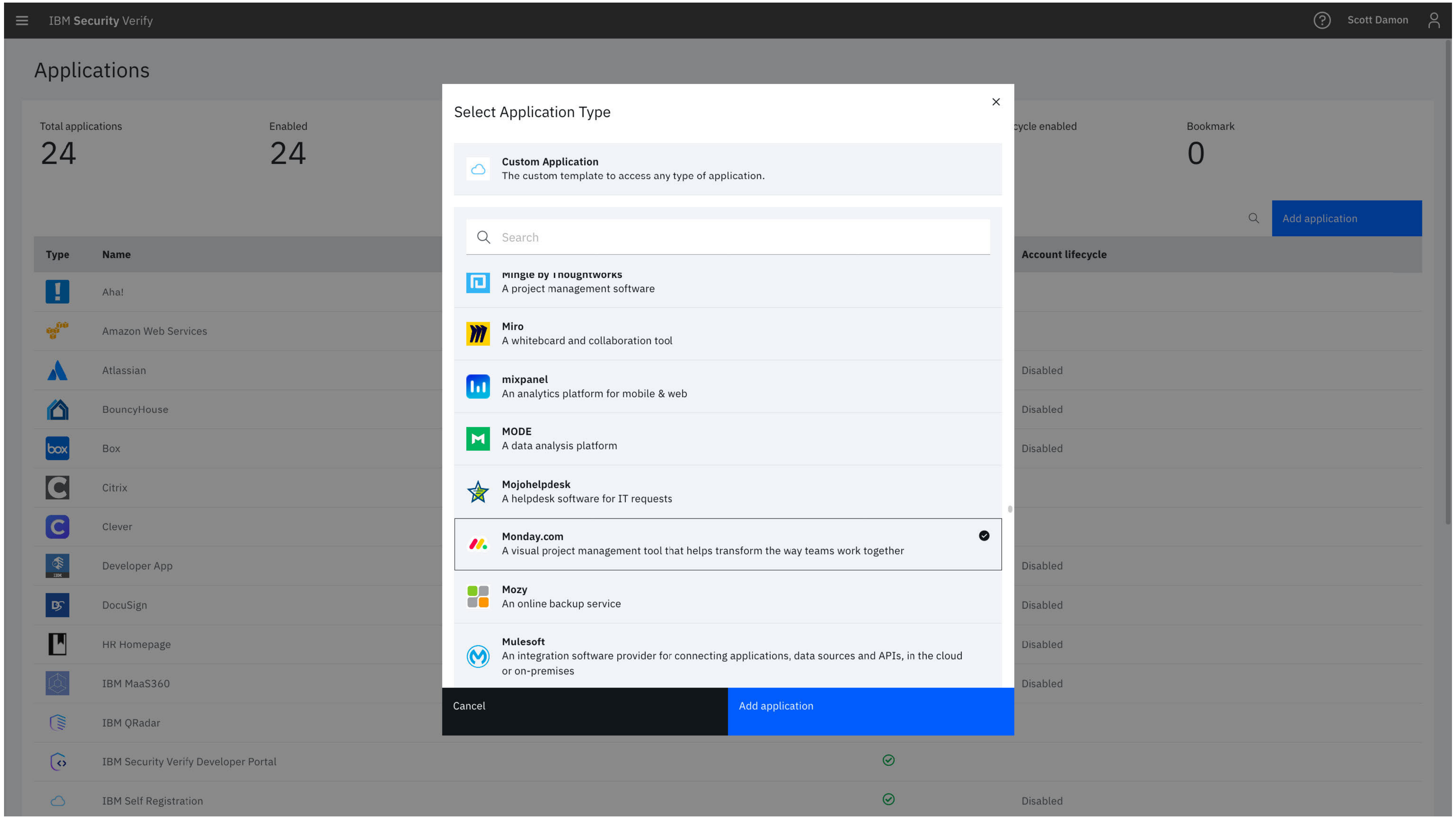
← →

○ 员工 ○ 业务经理 ● IT 管理员 ● 监控活动 ● 自定义策略 ● 管理用户和身份 ● **添加应用程序** ○ 分析风险 ○ 开发者

IT 管理员：第 2 步（共 6 步）
添加应用程序

搜索要添加的应用程序

Scott 可以搜索要添加的新应用程序，例如 Monday.com。通过预构建的 SaaS 连接器，将新应用程序集成到联合单点登录中非常简单。



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.

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

下一步：
添加审批访问权限的负责人

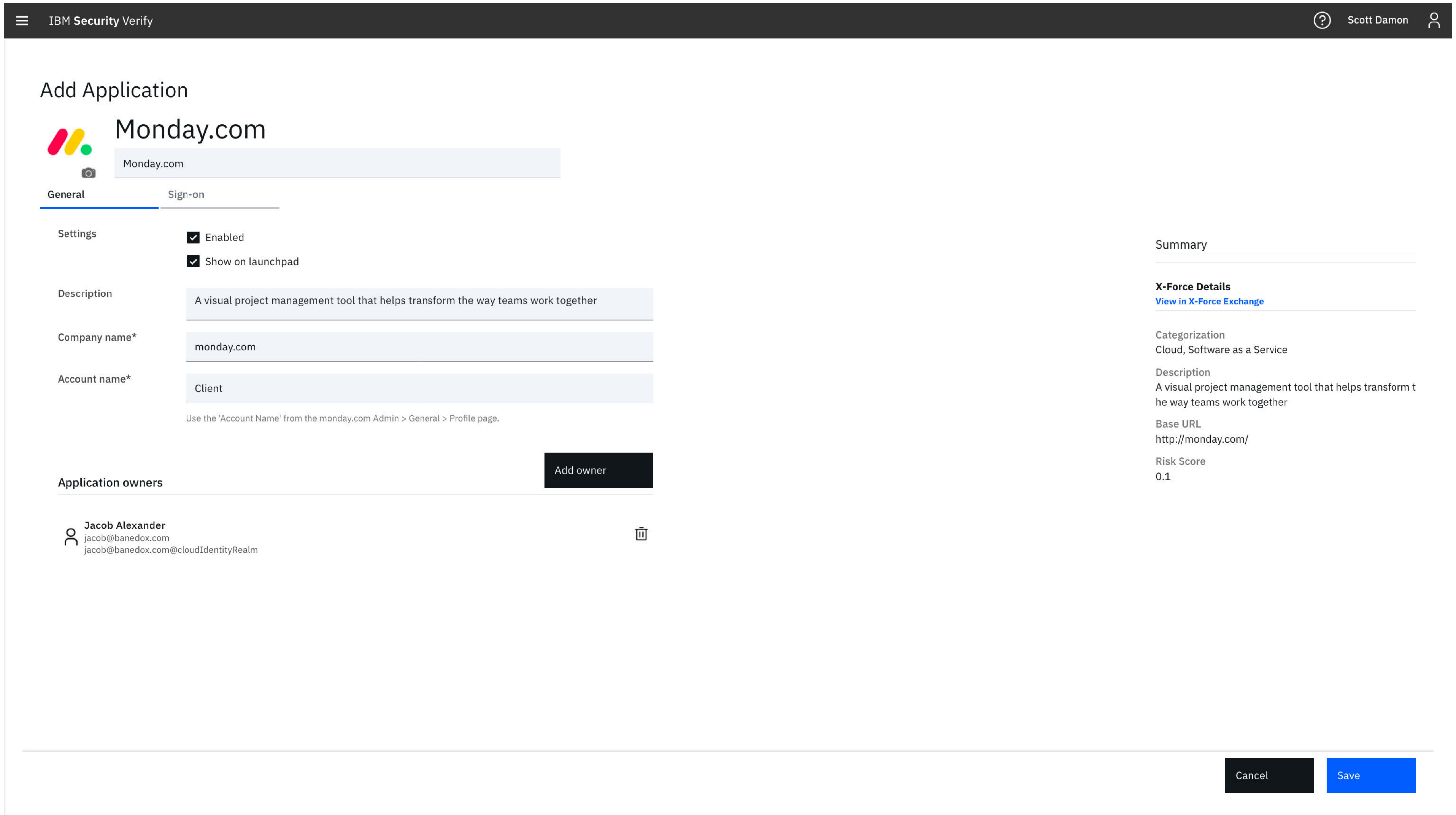
←　→

IT 管理员：第 3 步（共 6 步）

添加应用程序

添加审批访问权限的负责人

为了管理应用的持续操作，Scott 可以分配处理访问请求的应用程序负责人和审批人。



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 the way teams work together

Base URL
http://monday.com/

Risk Score
0.1

Cancel | Save

下一步：
配置登录设置

← →

员工 | 业务经理 | IT 管理员 | 监控活动 | 自定义策略 | 管理用户和身份 | **添加应用程序** | 分析风险 | 开发者

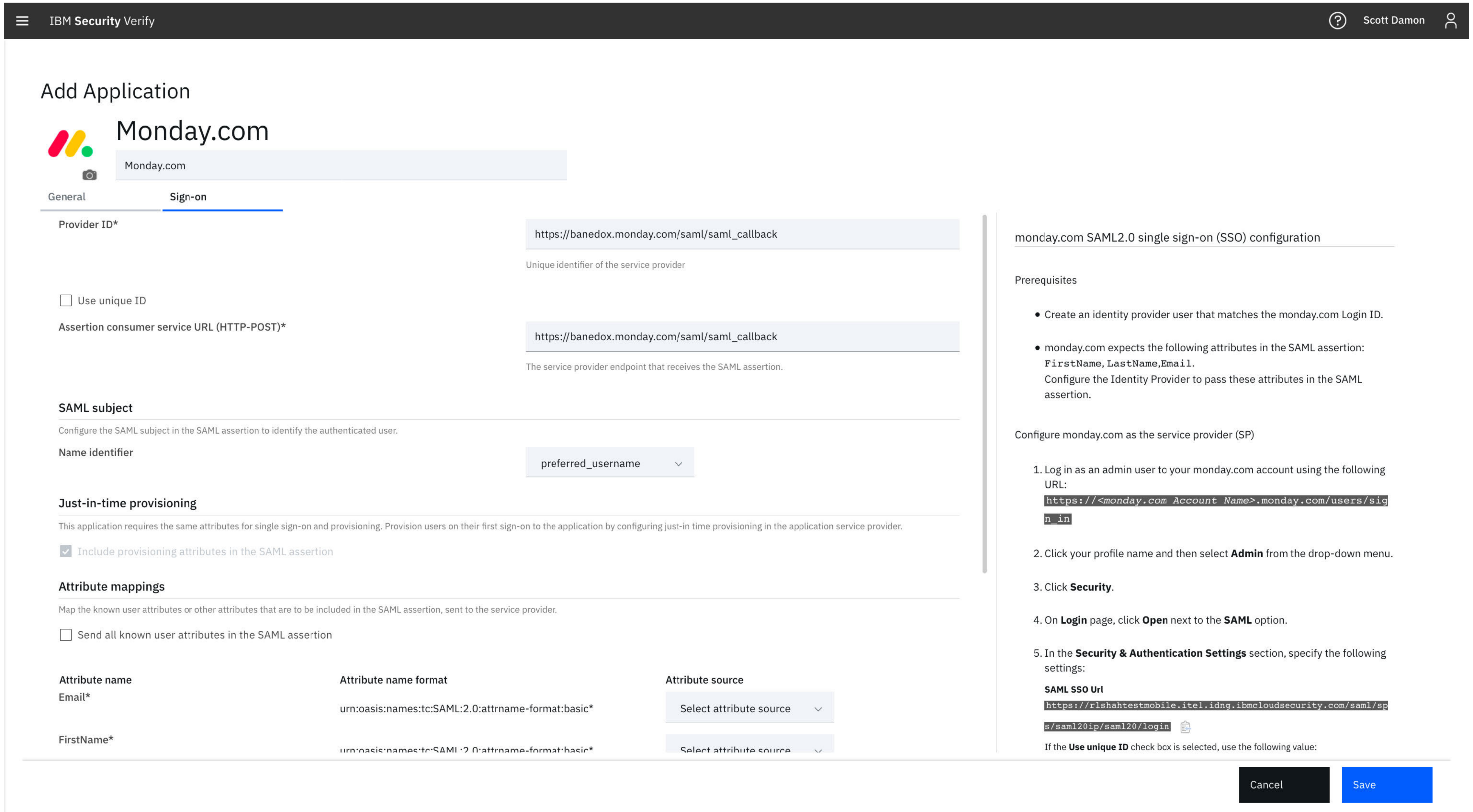
上一页 | 下一页

IT 管理员：第 4 步（共 6 步）

添加应用程序

配置登录设置

在“登录”选项卡中，Scott 可以配置应用程序所需的参数以适当地与 Verify 集成，并通过应用程序特定说明来提供帮助。在此页面的下方，他可以配置集成的其他方面，例如映射将要发送给服务提供商的属性，以及应用到应用程序的访问策略。



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.ite1.idng.ibmcloudsecurity.com/saml/sps/saml20ip/saml20/login`

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

下一步：
配置权利

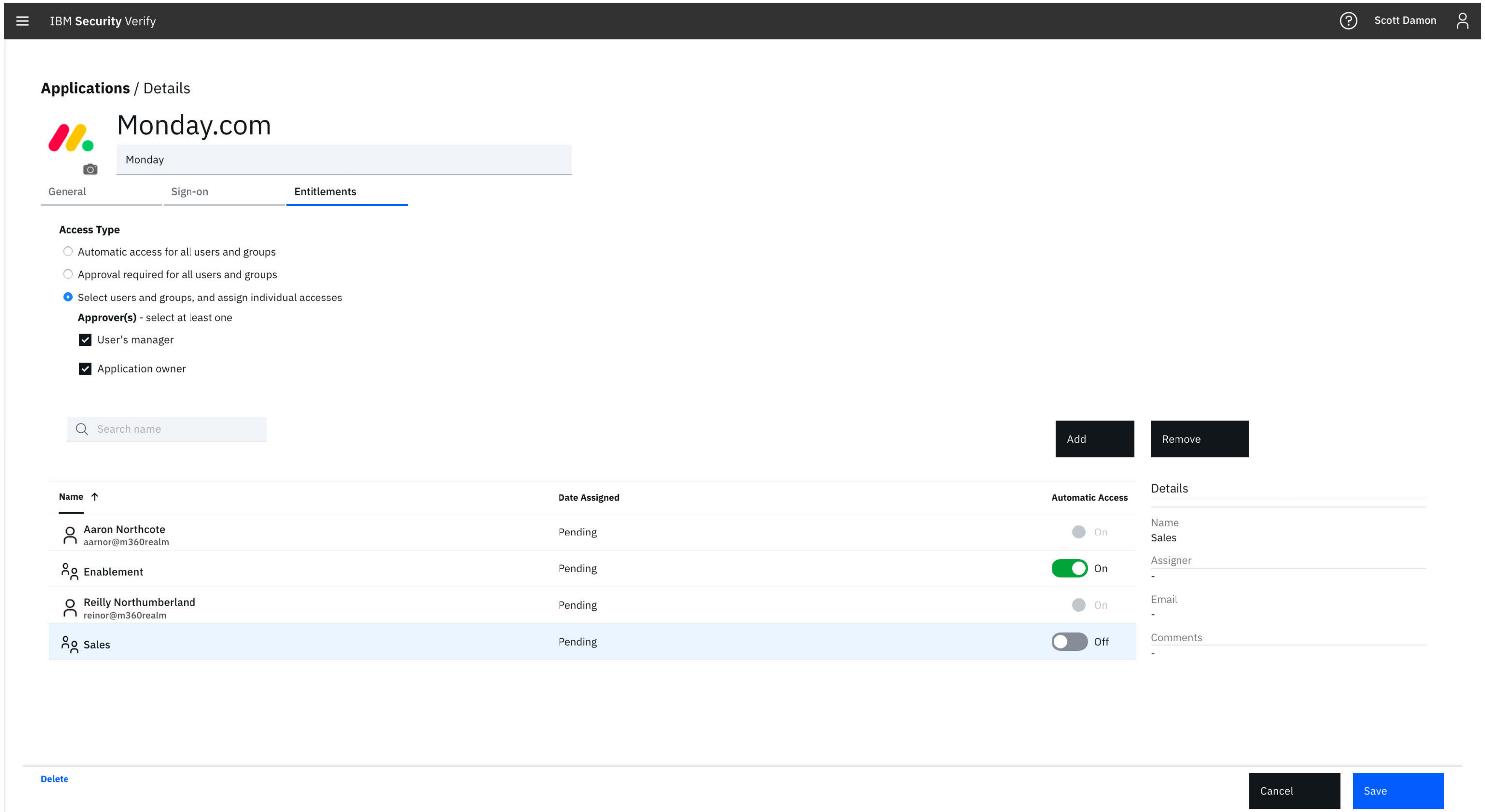
←
→

员工 业务经理 IT 管理员 监控活动 自定义策略 管理用户和身份 **添加应用程序** 分析风险 开发者

IT 管理员：第 5 步（共 6 步）
添加应用程序

配置权利

在“权利”选项卡中，Scott 可以配置适合应用程序的访问级别和审批流程。在这种情况下，他可以选择一组特定的用户和群组。



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
-

下一步：
设置定期重新认证访问权限

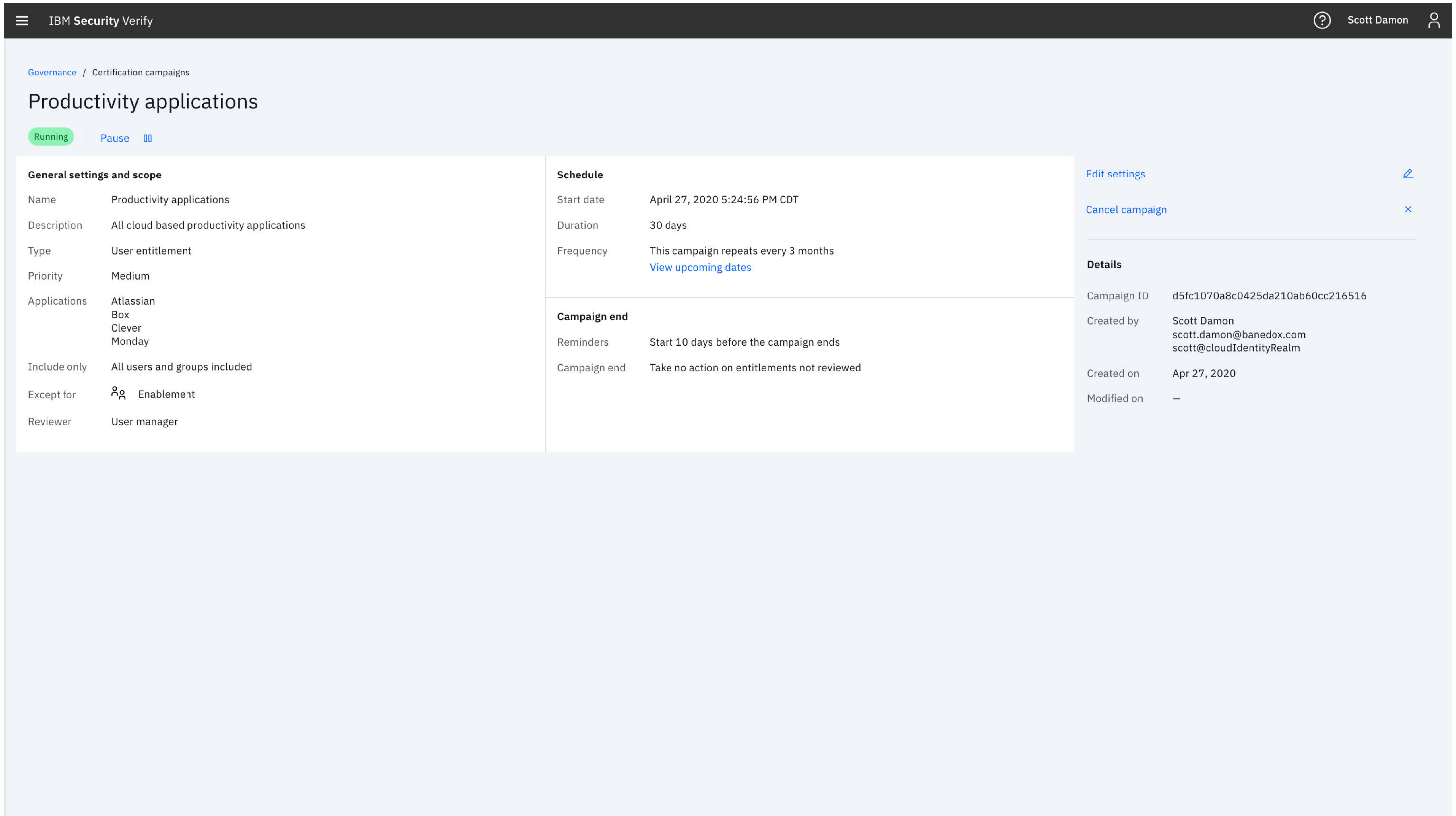
IT 管理员：第 6 步（共 6 步）

添加应用程序

设置定期重新认证访问权限

随着时间的推移，组织可能难以有效地重新认证应用程序，以确保访问级别仍然合适。为确保不漏掉这一重要步骤，Scott 可以针对每个应用设置定期重新认证活动，使身份治理这个方面实现自动化。

下一步：
分析仪表板



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	—

员工 业务经理 IT 管理员 监控活动 自定义策略 管理用户和身份 **添加应用程序** 分析风险 开发者

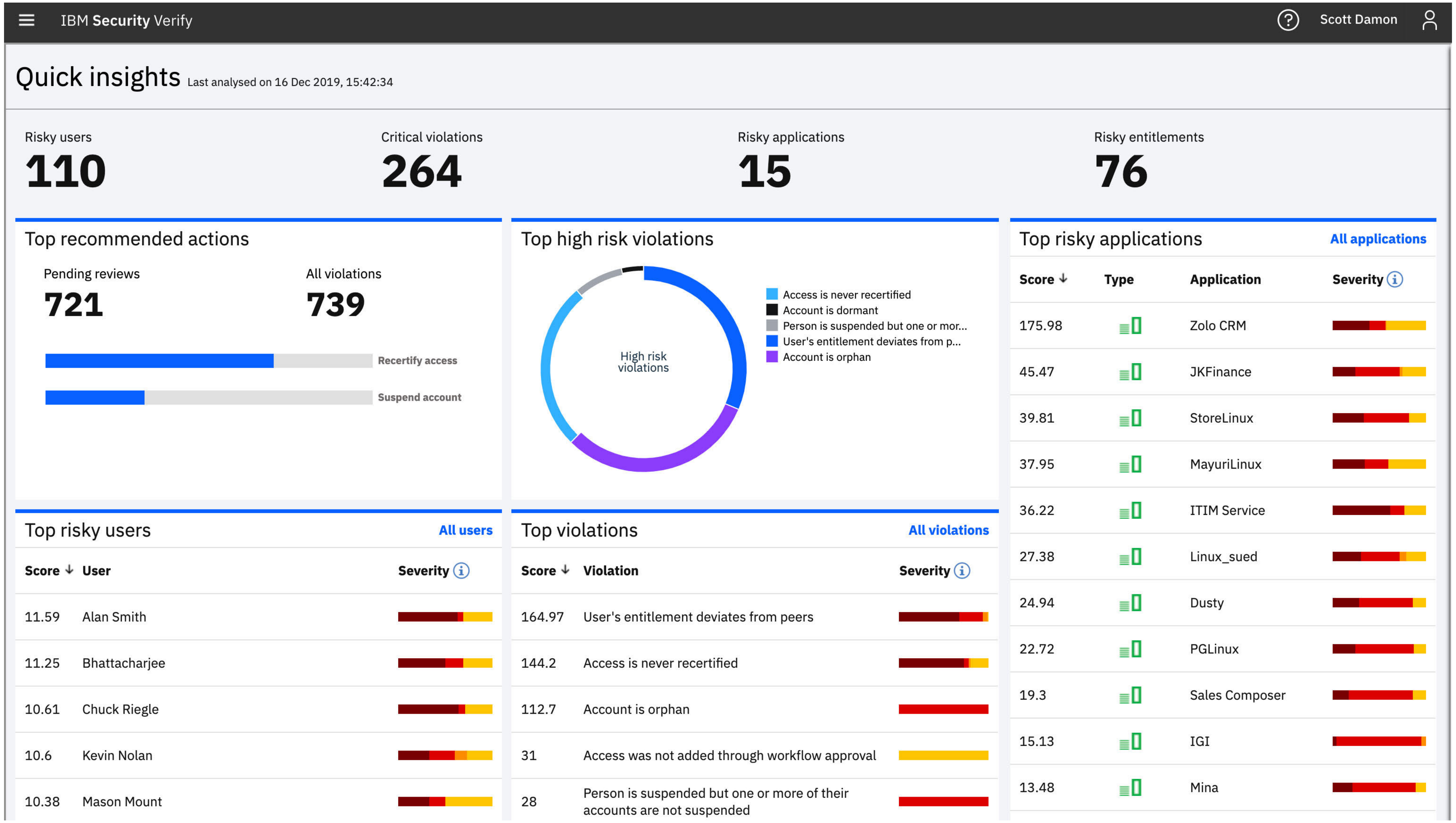
IBM **Security** Verify

立即试用 Verify

IT 管理员：第 1 步（共 3 步）
分析风险

分析仪表板

Scott 可以在身份分析仪表板中查看其 IAM 环境的整体运行状况，在这个仪表板中，他还可以快速扫描用户、权利和应用程序中与身份相关的风险。他可以更深入地探究每个用户和应用程序，进一步了解违规行为和累积风险评分。



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

Top 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	

下一步：
查看排列好的策略违规行为

← →

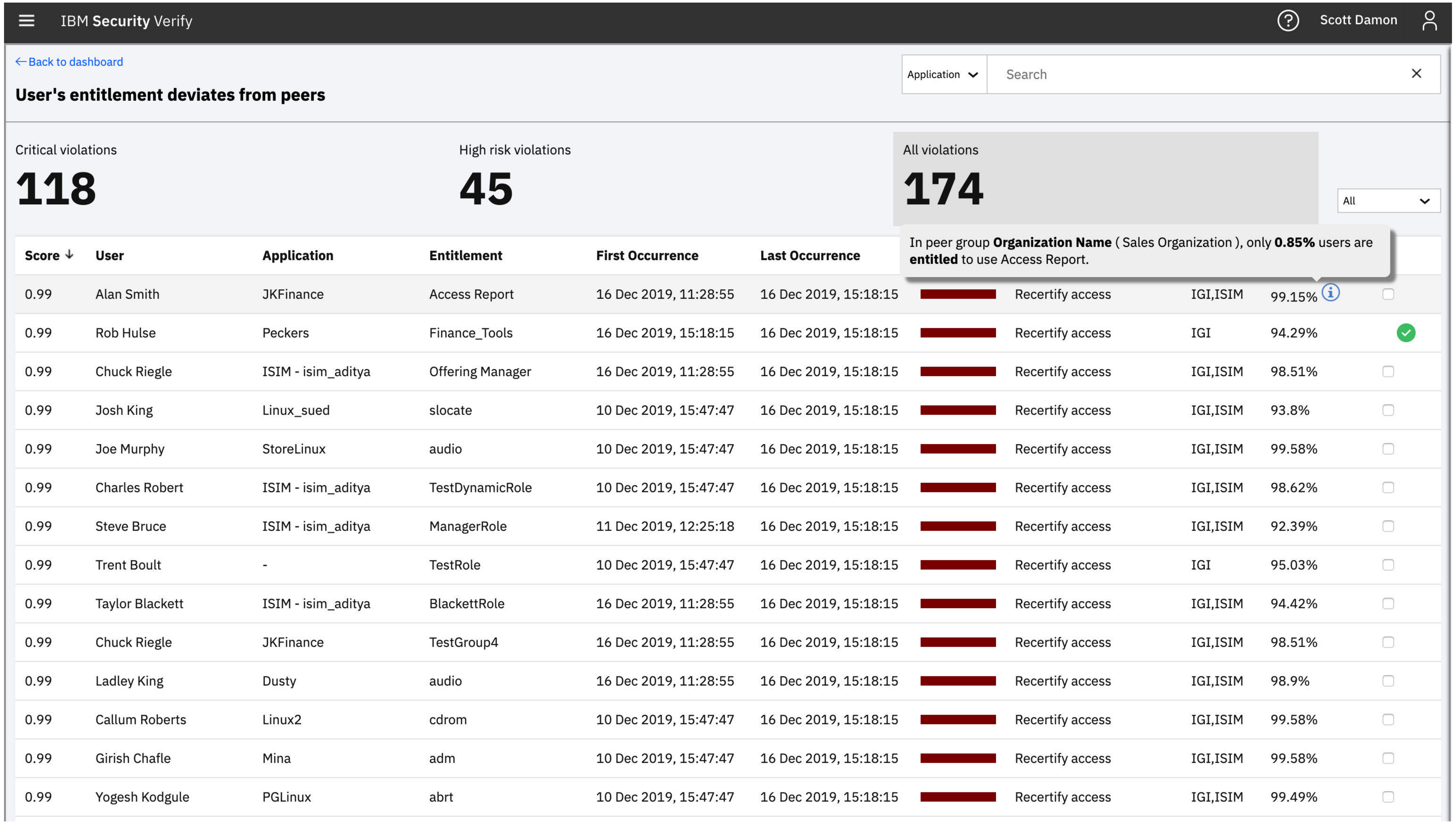
○ 员工 ○ 业务经理 ● IT 管理员 ● 监控活动 ● 自定义策略 ● 管理用户和身份 ● 添加应用程序 ● **分析风险** ○ 开发者

上一页 下一页

IT 管理员：第 2 步（共 3 步）
分析风险

查看排列好的策略违规行为

Scott 可以突出显示异常并查看策略类别中排列好的违规行为，例如“用户的权利与其他用户不同”这个视图。身份分析中的这种特定策略执行对等组分析，用于识别可能引入额外风险的上下文非典型权利。



User's entitlement deviates from peers

Critical violations **118**

High risk violations **45**

All violations **174**

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

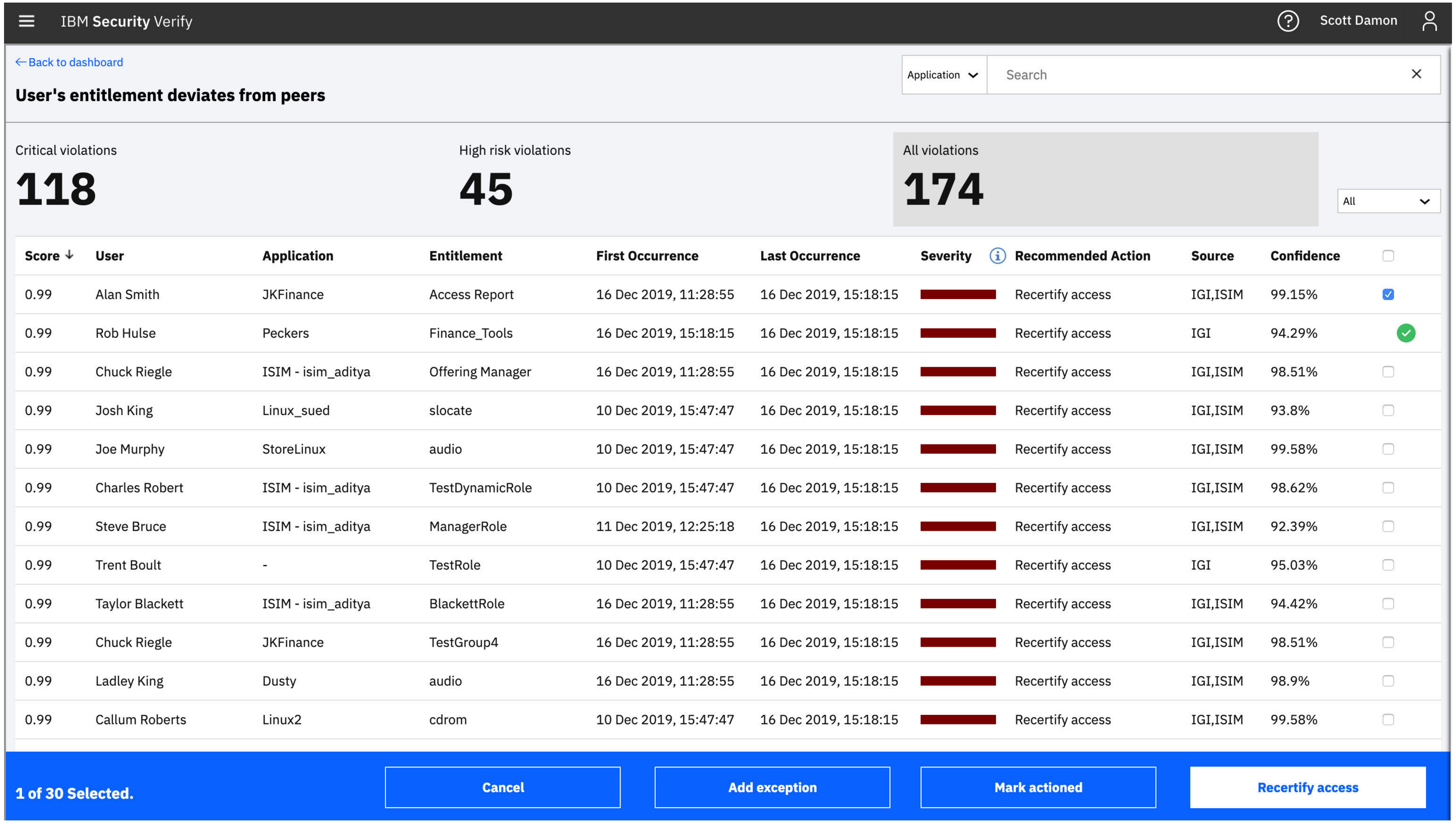
Score ↓	User	Application	Entitlement	First Occurrence	Last Occurrence					
0.99	Alan Smith	JKFinance	Access Report	16 Dec 2019, 11:28:55	16 Dec 2019, 15:18:15	■	Recertify access	IGI,ISIM	99.15% ⓘ	☐
0.99	Rob Hulse	Peckers	Finance_Tools	16 Dec 2019, 15:18:15	16 Dec 2019, 15:18:15	■	Recertify access	IGI	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%	☐

下一步：
采取建议的补救措施

IT 管理员：第 3 步（共 3 步）
分析风险

采取建议的补救措施

对于每项策略违规，Verify 还建议采取补救措施，例如重新认证访问权限，以及进行 AI 支持的风险和置信度评分。Scott 可以在身份分析仪表板中执行重新认证请求。



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.

下一步：
开发者

← →

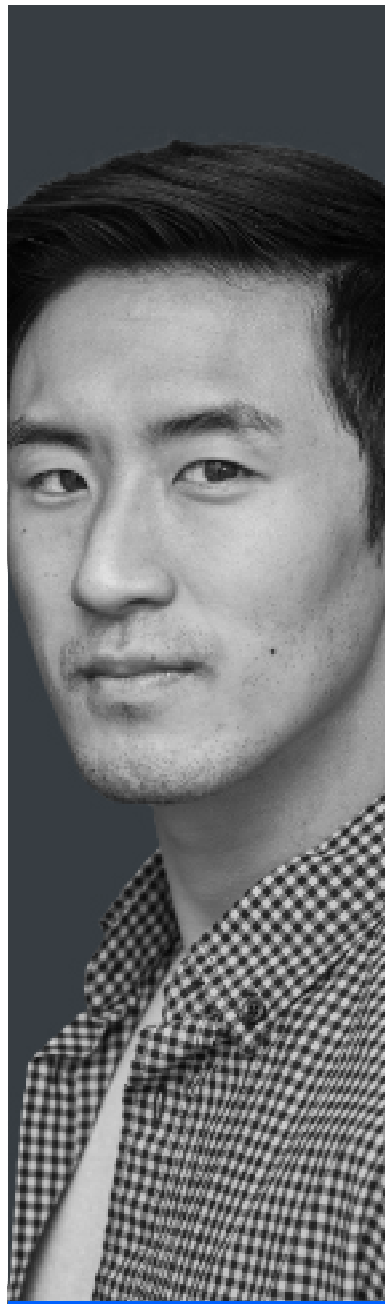
○ 员工 ○ 业务经理 ● IT 管理员 ● 监控活动 ● 自定义策略 ● 管理用户和身份 ● 添加应用程序 ● **分析风险** ○ 开发者

开发者

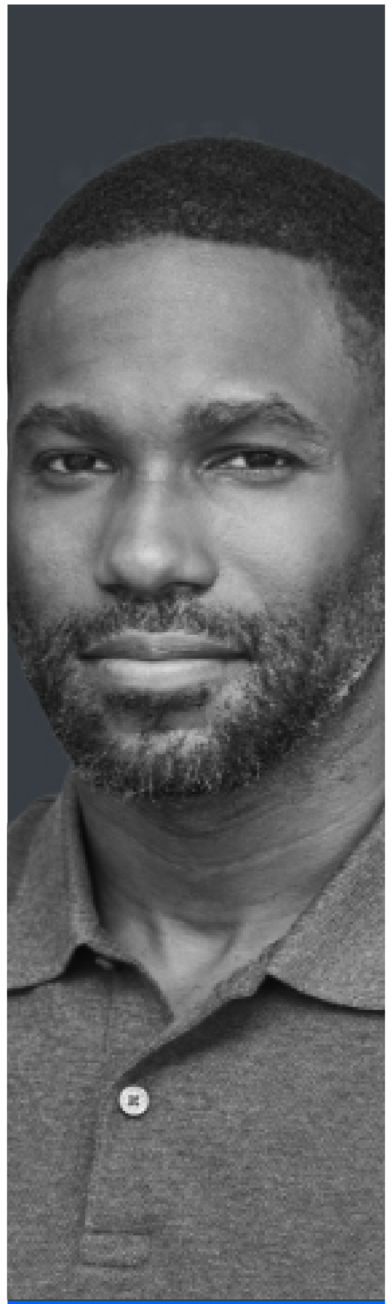
使用直观的专用 API 将访问和身份验证嵌入到自定义应用程序中。

开发者需要构建用于身份验证的运行时流程，为用户提供注册功能，并将 MFA 嵌入到他们的应用程序中，而不必成为 IAM 专家。为了有效地做到这一点，他们需要强大的 API 和文档、示例代码和指导说明。

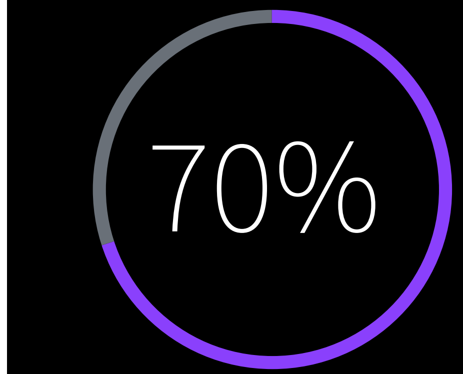
查看



查看



查看



到 2024 年，70% 甚至更多通过访问管理解决方案访问的应用程序将利用 MFA

Gartner

“我需要快速将身份验证嵌入到应用程序中，而不是让这一步成为我真正想要完成的任务的障碍”

Alice，开发者

开发者

首先：
开发者门户

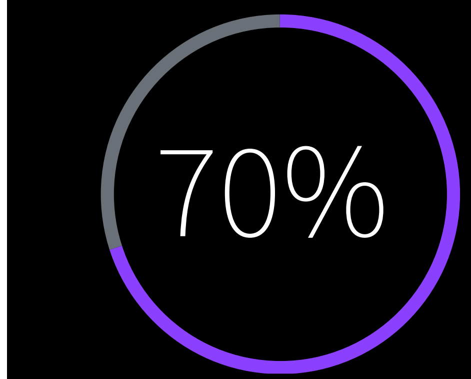
←　→

○ 员工　○ 业务经理　○ IT 管理员　● **开发者**　○ 开发人员资源　○ 构建自定义应用程序　○ API 配置

开发者

使用直观的专用 API 将访问和身份验证嵌入到自定义应用程序中。

开发者需要构建用于身份验证的运行时流程，为用户提供注册功能，并将 MFA 嵌入到他们的应用程序中，而不必成为 IAM 专家。为了有效地做到这一点，他们需要强大的 API 和文档、示例代码和指导说明。



到 2024 年，70% 甚至更多通过访问管理解决方案访问的应用程序将利用 MFA

Gartner

“我需要快速将身份验证嵌入到应用程序中，而不是让这一步成为我真正想要完成的任务的障碍”

Alice，开发者

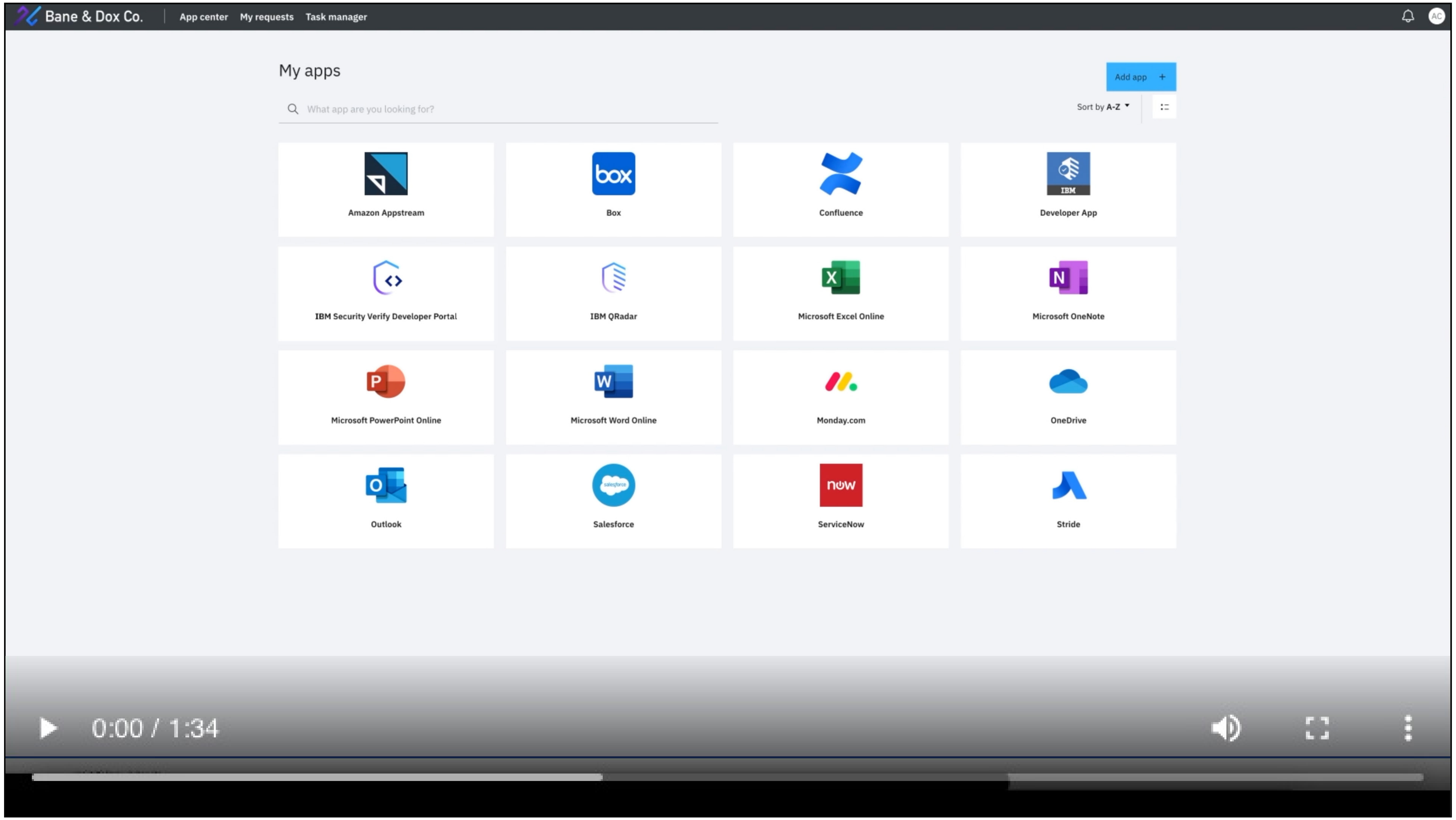
开发者

- 员工
- 业务经理
- IT 管理员
- **开发者**
- 开发人员资源
  - 开发者门户
  - API 帮助
- 构建自定义应用程序
  - 添加自定义应用程序模板
  - 配置登录设置
  - 进行配置
  - 排查漏洞
- API 配置
  - 添加 API 客户端
  - 委托管理

开发者：第 1 步（共 2 步）
开发人员资源

开发者门户

IBM Security Verify 开发者门户提供一种类似向导的体验，可指导开发者完成集成应用程序的过程。除标准 API 文档外，该门户还提供代码片段、分步说明和示例应用程序。



下一步：
API 帮助

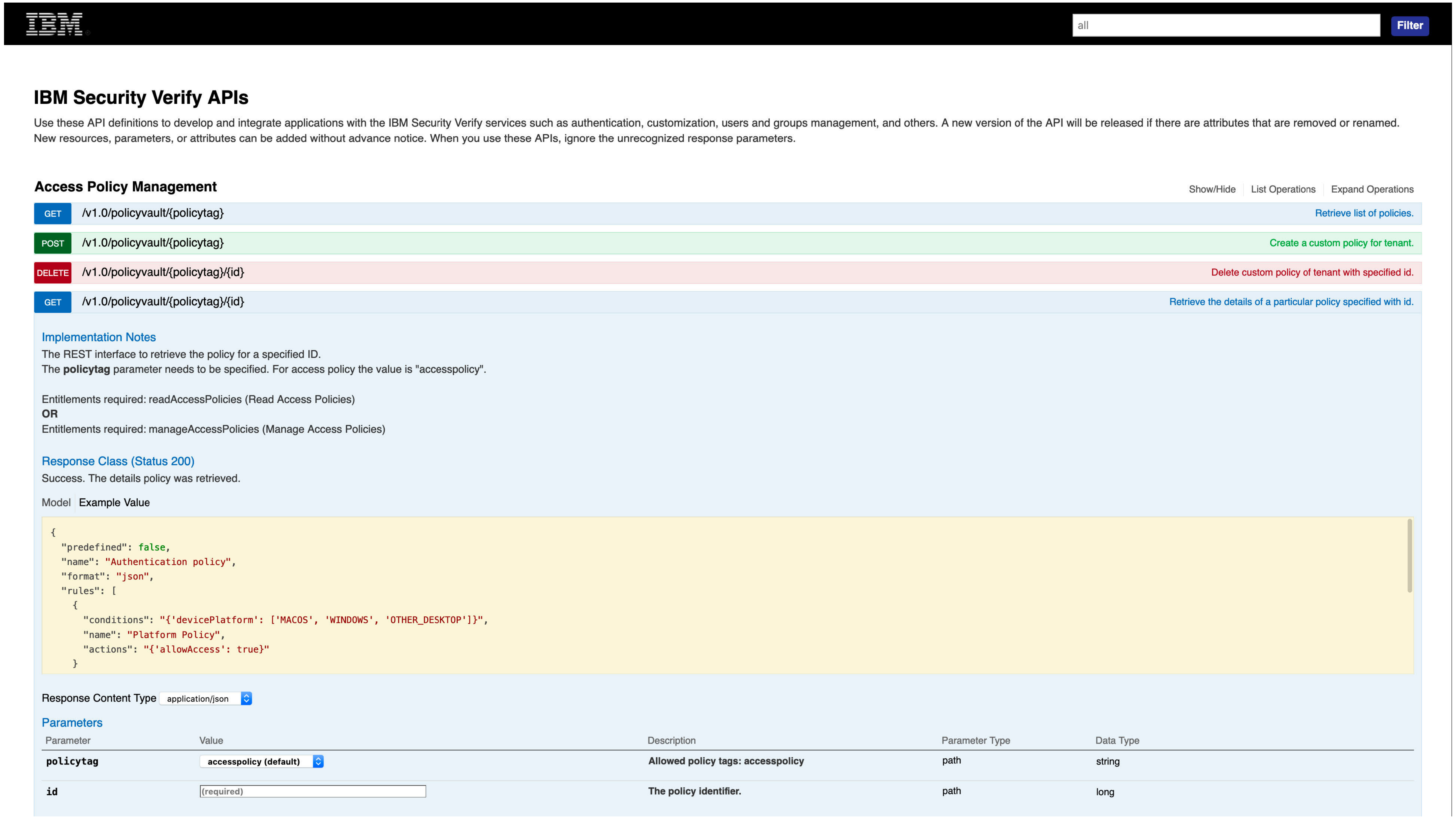
← →

员工 业务经理 IT 管理员 开发者 开发人员资源 构建自定义应用程序 API 配置

开发者：第 2 步（共 2 步）
开发人员资源

API 帮助

Alice 可以使用 Verify 的 API 将用户管理和身份验证等身份相关功能集成到她的应用程序中。Verify API 帮助提供实现指南，例如所需权利、参数和可能的响应消息。帮助文档还包含了每个 API 调用的实现示例。



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

下一步：
添加自定义应用程序模板

←　→

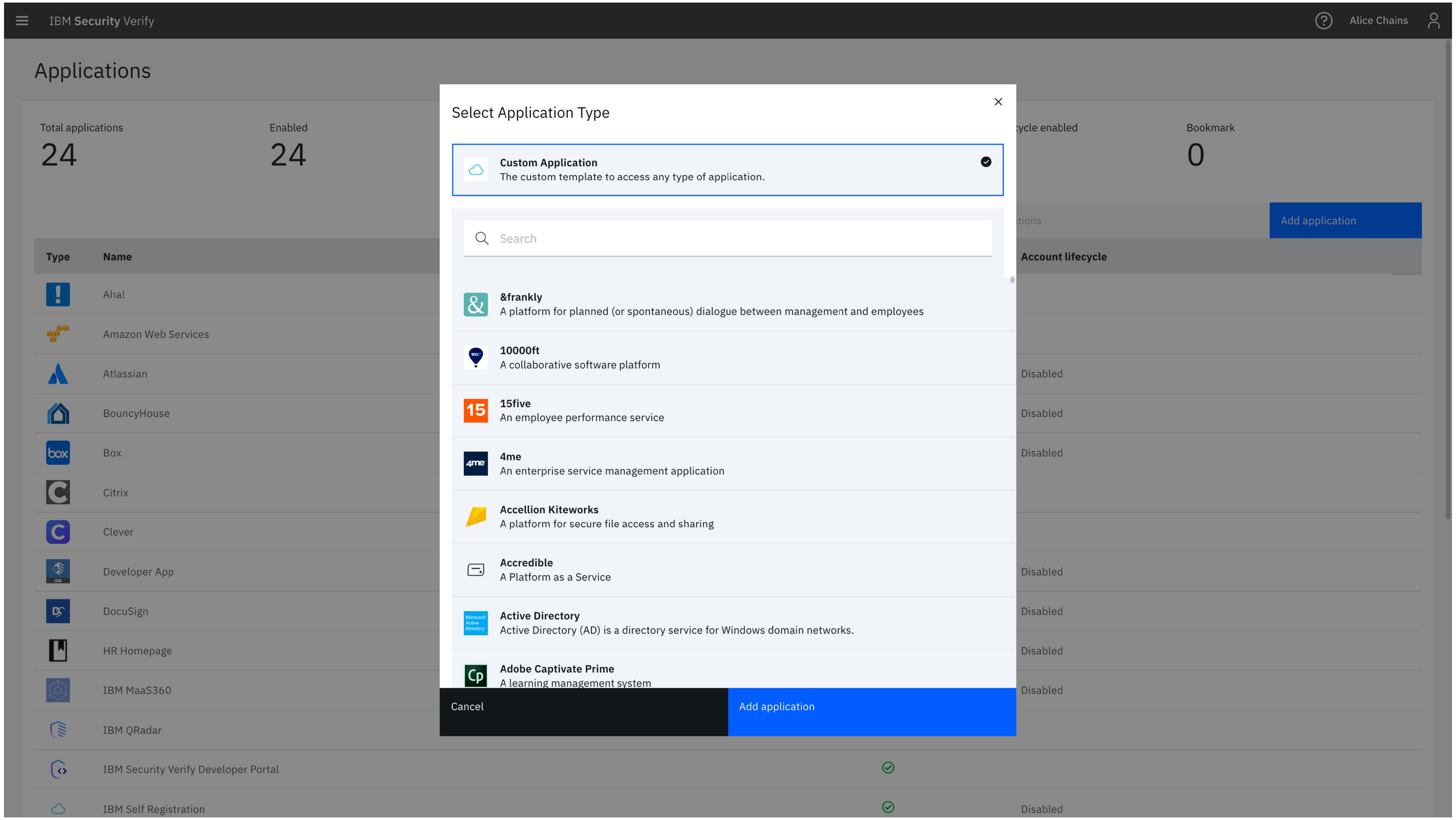
员工　业务经理　IT 管理员　开发者　**开发人员资源**　构建自定义应用程序　API 配置

上一页　下一页

开发者：第 1 步（共 4 步）
构建自定义应用程序

添加自定义应用程序模板

Alice 可以通过将其自定义应用程序与组织的其他 SaaS 和本地应用程序集成到 Verify 的联合单点登录中，将它们全部包含在内。首先，她可以添加自定义应用程序模板来集成新的 SAML 或 Open ID Connect 应用程序。



IBM **Security** Verify — Alice Chains

Applications

Total applications 24 | Enabled 24 | …cycle 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

Cancel | Add application

下一步：
配置登录设置

← →

员工 — 业务经理 — IT 管理员 — 开发者 — 开发人员资源 — **构建自定义应用程序** — API 配置

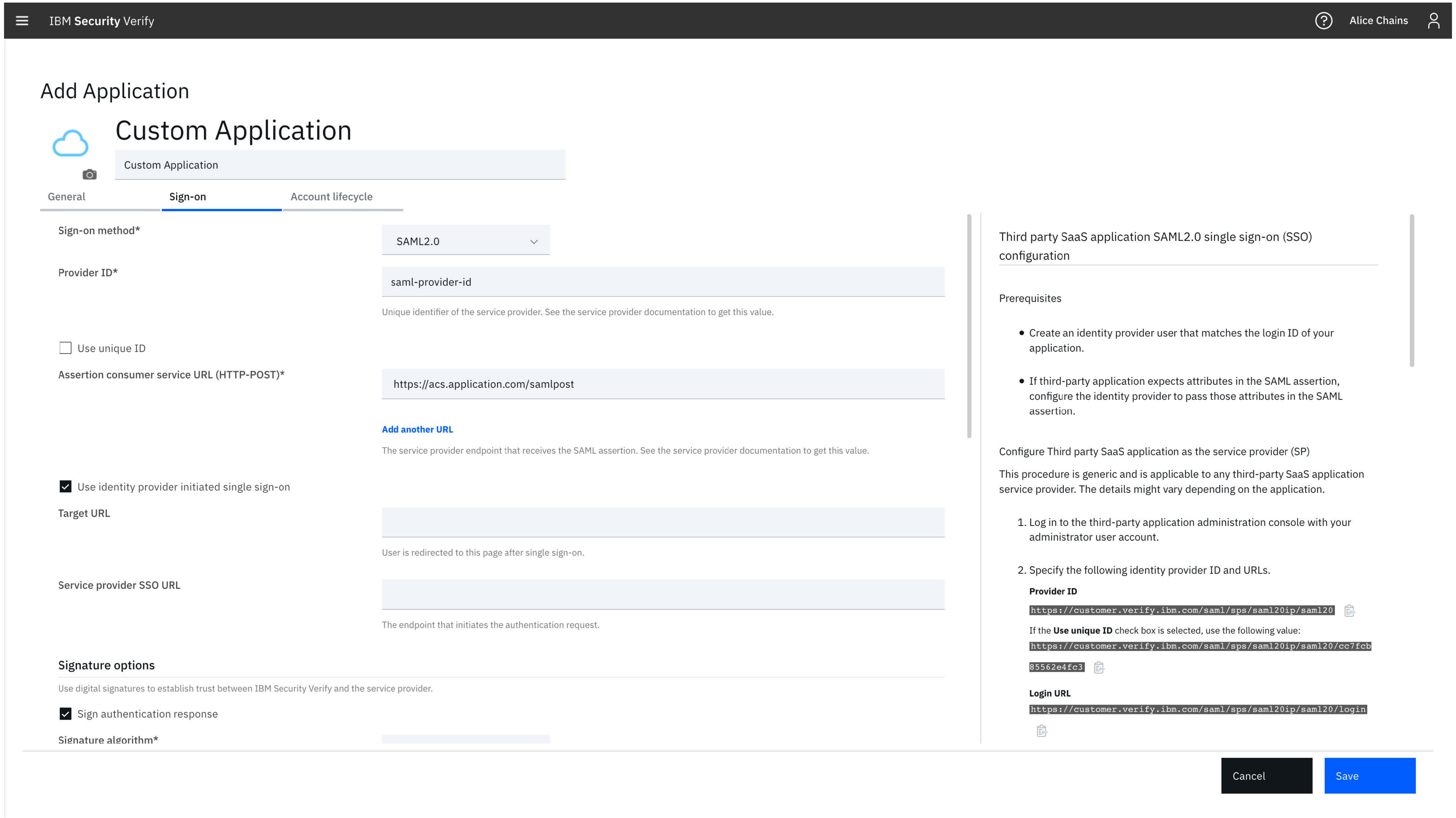
上一页 | 下一页

开发者：第 2 步（共 4 步）

构建自定义应用程序

配置登录设置

在应用程序模板中，提供了集成应用程序的分步说明。



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

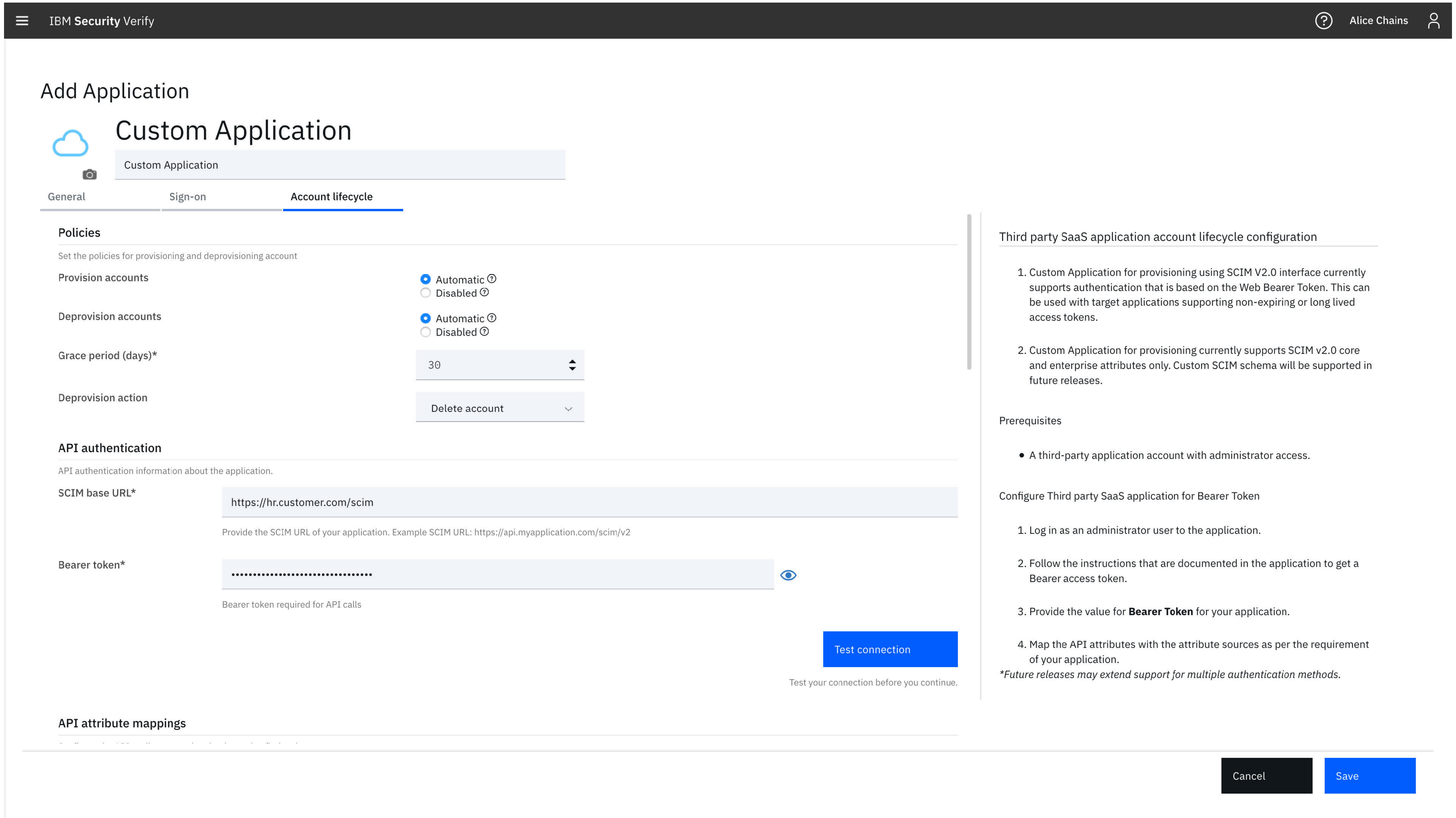
   `https://customer.verify.ibm.com/saml/sps/saml20ip/saml20/login`

下一步：
进行配置

开发者：第 3 步（共 4 步）
构建自定义应用程序

进行配置

她还可以使用 SCIM 选择为应用程序启用自动配置和取消配置。



≡ IBM **Security** Verify ⓘ Alice Chains

Add Application

Custom Application

Custom Application

General | Sign-on | **Account lifecycle**

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 connection

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.*

Cancel | Save

下一步：
排查漏洞

← →

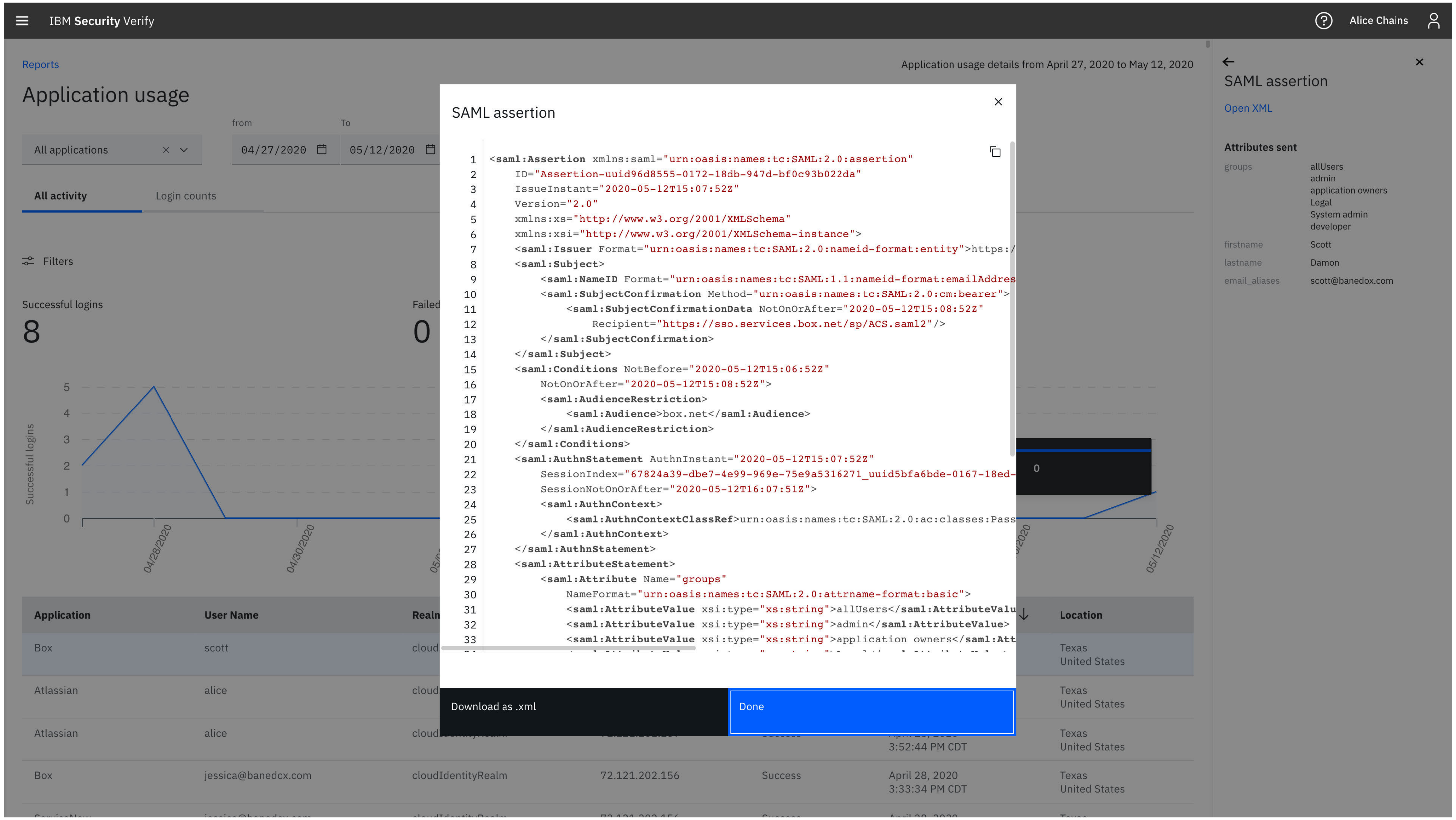
员工 | 业务经理 | IT 管理员 | 开发者 | 开发人员资源 | **构建自定义应用程序** | API 配置

开发者：第 4 步（共 4 步）

构建自定义应用程序

排查漏洞

Alice 可以监控应用程序的性能并深入了解身份验证事件的详细信息以排查漏洞。



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

[下一步：添加 API 客户端](#)

← →

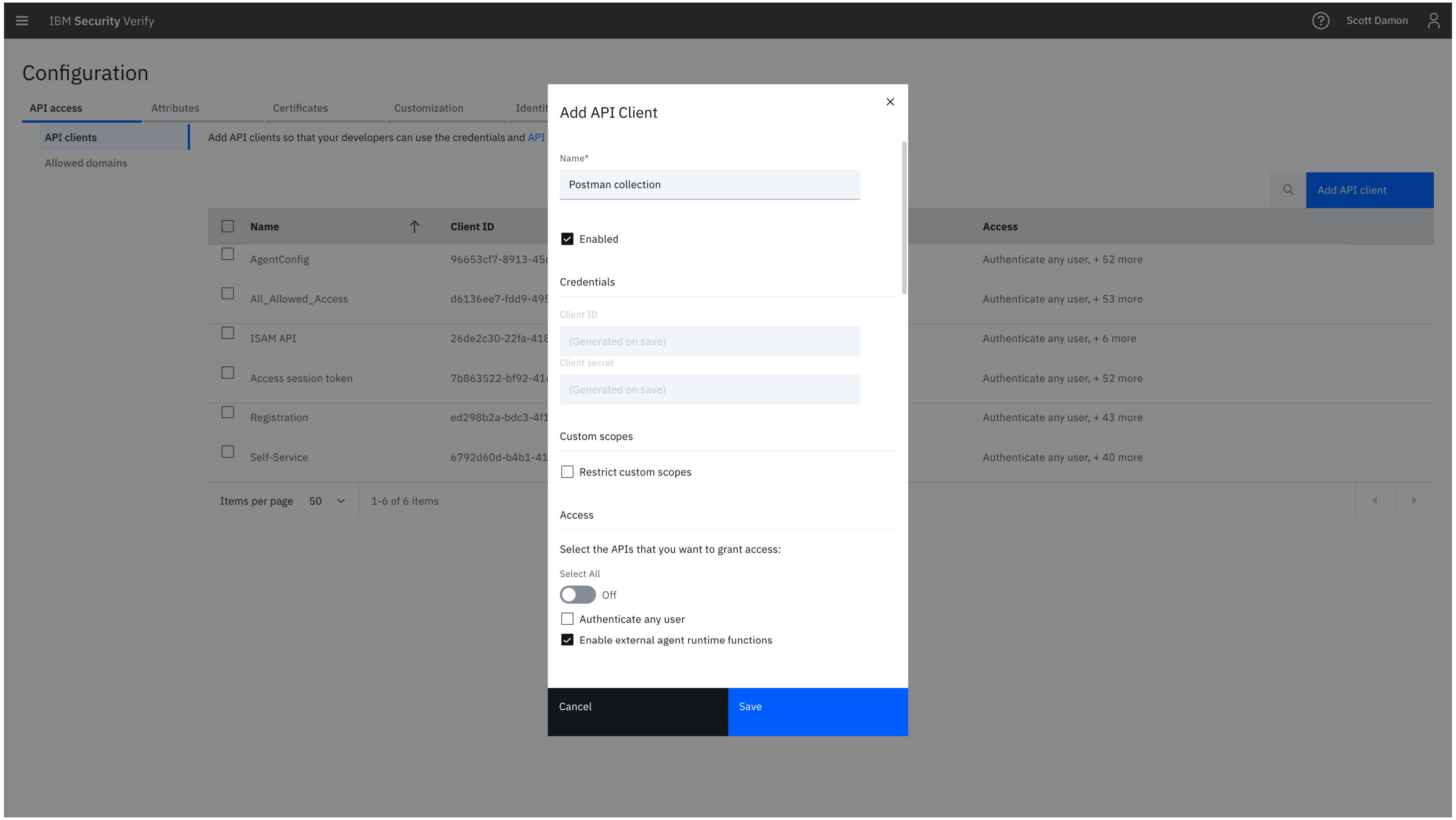
员工 业务经理 IT 管理员 开发者 开发人员资源 **构建自定义应用程序** API 配置

开发者：第 1 步（共 2 步）

API 配置

添加 API 客户端

Alice 可以从她想要集成到应用程序中的各种 API 客户端中进行选择。



Configuration

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

☐	Name ↑	Client ID	Access
☐	AgentConfig	96653cf7-8913-45	Authenticate any user, + 52 more
☐	All_Allowed_Access	d6136ee7-fdd9-49	Authenticate any user, + 53 more
☐	ISAM API	26de2c30-22fa-41	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

下一步：
委托管理

← →

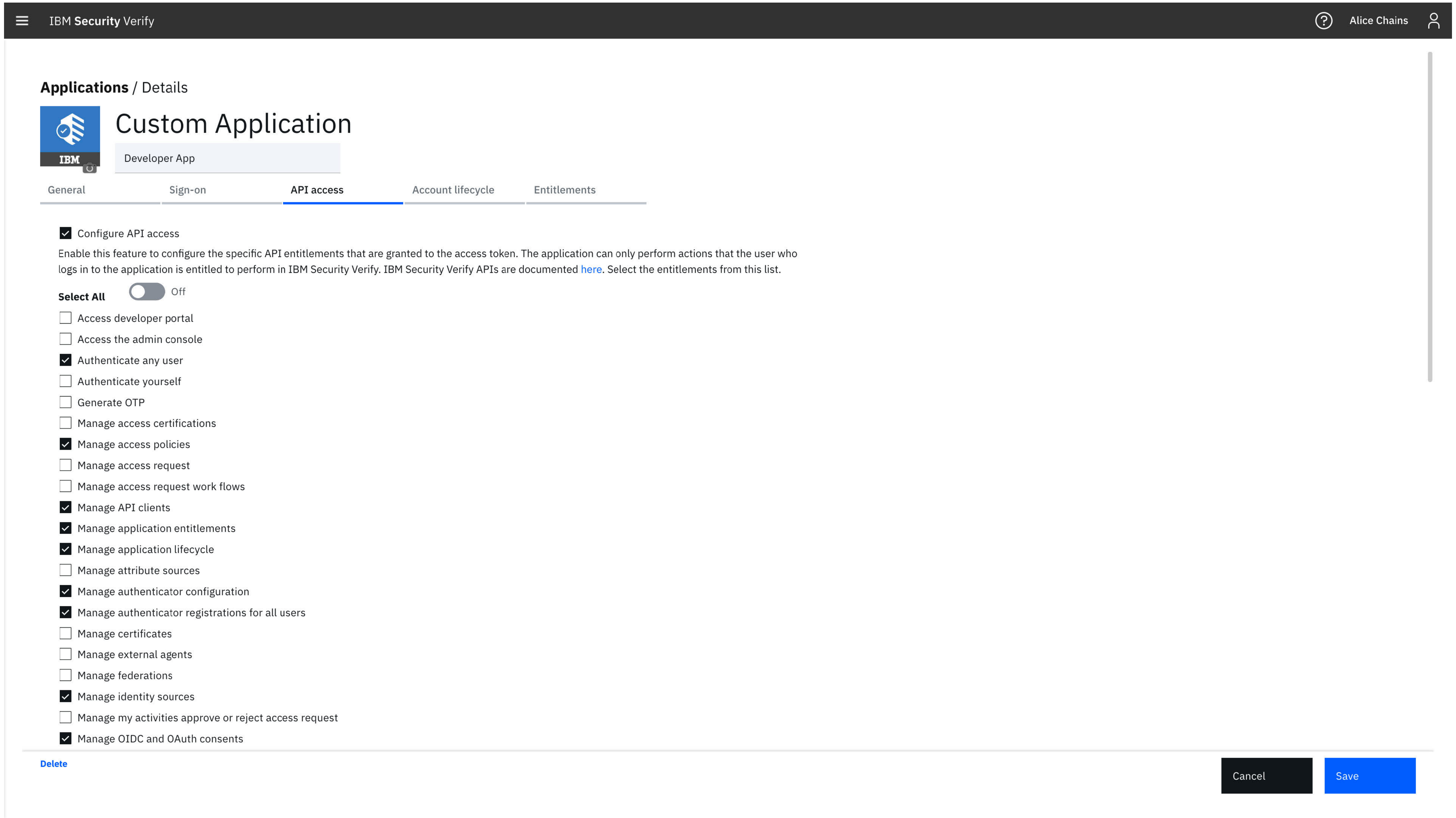
员工 业务经理 IT 管理员 开发者 开发人员资源 构建自定义应用程序 **API 配置**

上一页 下一页

开发者：第 2 步（共 2 步）
API 配置

委托管理

她还可以允许其应用程序调用授予访问令牌的特定 API 权利。



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

探索：
IBM Security Verify

IBM Security

国际商业机器（中国）有限公司
北京市朝阳区金和东路 20 号院 3 号楼
正大中心南塔 12 层
邮编：100020

美国出品
2021 年 2 月

本文档为自最初公布日期起的最新版本，IBM 可随时对其进行修改。IBM 并不一定在开展业务的所有国家或地区提供所有产品或服务。效能資料和客戶示例引用僅供說明之用。实际性能结果可能因具体配置和运行条件而异。

本文档内的信息“按现状”提供，不附有任何种类的（无论是明示的还是默示的）保证，包括不附有关于适销性、适用于某种特定用途的任何保证以及非侵权的任何保证或条件。

IBM 产品根据其提供时所依据协议的条款和条件获得保证。客户应遵守适用的法律法规。IBM 不提供法律建议或表述或保证其服务或产品会确保客户符合法律法规的规定。有关 IBM 未来发展方向及意图的声明如有变更或撤销，恕不另行通知，且仅用于说明目标之用。

00000000CNZH

IBM