



IBM Security Verify Produkttour

Beginnen Sie Ihre Tour →



Verbinden Sie alle Benutzer sicher mit allem

IBM Security Verify liefert Kontext und geschäftsrelevantes Wissen für Entscheidungen darüber, wer auf was zugreifen darf. So kann Ihr Unternehmen den richtigen Personen zum richtigen Zeitpunkt den richtigen Zugriff gewähren.

Erkunden Sie die Demo und lernen Sie, wie Sie die Balance zwischen Sicherheit und Benutzerfreundlichkeit meistern.



Mitarbeiter



Bereichsleiter



IT-Administrator



Entwickler



Mitarbeiter

Greifen sie von jedem Gerät aus auf die Apps zu, die sie für ihre Tätigkeit benötigen, ohne sich um Kennwörter kümmern zu müssen.

Mitarbeiter brauchen Schnellzugriff auf die Tools, die sie für ihre Arbeit benötigen, ohne sich durch Dutzende von Berechtigungsnachweisen belastet zu fühlen. Trotz hoher Erwartungen an die Unternehmenssicherheit, können sich IT-Richtlinien immer noch wie ein Hindernis anfühlen. Mitarbeiter wollen effizient und ohne Hindernisse arbeiten.

Beginnen Sie mit:
Markenspezifische Anmeldeseite

11

Stunden

Die durchschnittliche Zeit, die Mitarbeiter weltweit jedes Jahr mit der Eingabe oder dem Zurücksetzen ihres Kennworts verbringen

Weltwirtschaftsforum

„Es ist wirklich frustrierend, von Tools und Systemen ausgebremst zu werden, wenn ich nur versuche, meine Arbeit zu erledigen.“

Jessica, Angestellte



Mitarbeiter



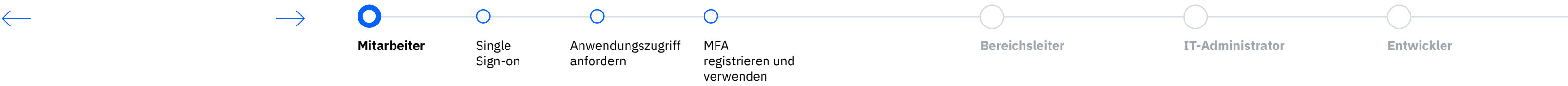
Anzeigen



Anzeigen



Anzeigen



Mitarbeiter

Greifen sie von jedem Gerät aus auf die Apps zu, die sie für ihre Tätigkeit benötigen, ohne sich um Kennwörter kümmern zu müssen.

Mitarbeiter brauchen Schnellzugriff auf die Tools, die sie für ihre Arbeit benötigen, ohne sich durch Dutzende von Berechtigungsnachweisen belastet zu fühlen. Trotz hoher Erwartungen an die Unternehmenssicherheit, können sich IT-Richtlinien immer noch wie ein Hindernis anfühlen. Mitarbeiter wollen effizient und ohne Hindernisse arbeiten.

11

Stunden

Die durchschnittliche Zeit, die Mitarbeiter weltweit jedes Jahr mit der Eingabe oder dem Zurücksetzen ihres Kennworts verbringen

Weltwirtschaftsforum

„Es ist wirklich frustrierend, von Tools und Systemen ausgebremst zu werden, wenn ich nur versuche, meine Arbeit zu erledigen.“

Jessica, Angestellte



Mitarbeiter

- Mitarbeiter

Single Sign-on

Markenspezifische Anmeldeseite

Zugriff auf Apps mit einem Klick

Anwendungszugriff anfordern

Katalog durchsuchen

Begründung erstellen

Offene Anfragen

Neue App in der Klickstartleiste

MFA registrieren und verwenden

Neues Authentifizierungsgerät hinzufügen

Mobile App einstellen

Wählen Sie die MFA Methode

Bereichsleiter

IT-Administrator

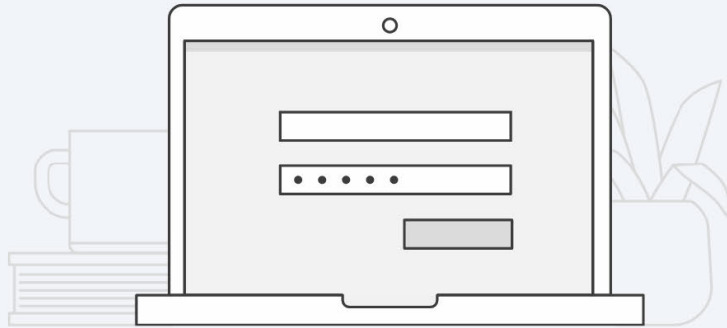
Entwickler

Mitarbeiter: 1 von 2
Single Sign-on

Markenspezifische Anmeldeseite

Mitarbeiter brauchen Schnellzugriff auf die Tools, die sie für ihre Arbeit benötigen, ohne sich durch Dutzende von Berechtigungsnachweisen belastet zu fühlen. Trotz hoher Erwartungen an die Unternehmenssicherheit, können sich IT-Richtlinien immer noch wie ein Hindernis anfühlen. Mitarbeiter wollen effizient und ohne Hindernisse arbeiten.

Weiter:
Zugriff auf Apps mit einem Klick



 **Bane & Dox Co.**

Sign in with Cloud Directory

User name

jessica@banedox.com

Password

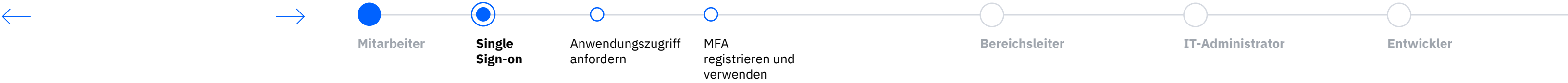
.....

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.



Mitarbeiter: 2 von 2
Single Sign-on

Zugriff auf Apps mit einem Klick

Über ihre Klickstartleiste kann Jessica auf alle Apps zugreifen, zu deren Verwendung sie berechtigt ist. Je nachdem, wie der IT-Administrator ihre Einstellungen konfiguriert, hat sie auf die meisten Anwendungen per Mausklick Zugriff.

Weiter:
Katalog durchsuchen

 Bane & Dox Co.

App centerMy requests



My apps

+

Add app

Sort by A-Z

⋮


Amazon Appstream


Box


Confluence


Developer App


IBM QRadar


Microsoft Excel Online


Microsoft OneNote


Microsoft PowerPoint Online


Microsoft Word Online


Monday.com


OneDrive

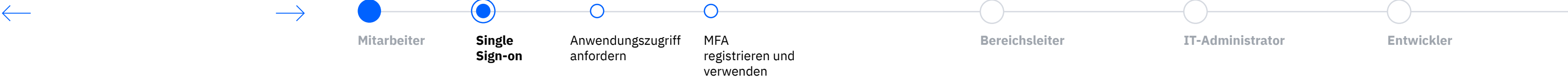

Outlook


Salesforce


ServiceNow


Stride

© 2020 Bane & Dox Co.



Mitarbeiter: 1 von 4

Anwendungszugriff anfordern

Katalog durchsuchen

Über ihre Klickstartleiste kann Jessica auf alle Apps zugreifen, zu deren Verwendung sie berechtigt ist. Je nachdem, wie der IT-Administrator ihre Einstellungen konfiguriert, hat sie auf die meisten Anwendungen per Mausklick Zugriff.

Weiter:

Begründung erstellen

 Bane & Dox Co.

App centerMy requests

Catalog

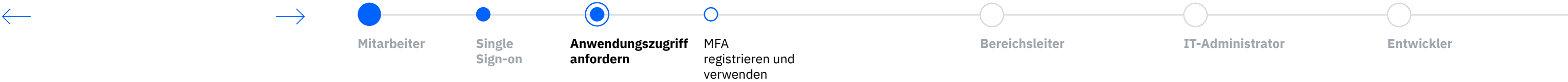
 What app are you looking for?

My apps

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.



Mitarbeiter: 2 von 4

Anwendungszugriff anfordern

Begründung erstellen

Sie wählt XYZ aus und schreibt eine geschäftliche Begründung, warum sie Zugang benötigt.

Weiter:

Offene Anfragen

Bane & Dox Co.

App center

My requests

Catalog

What app are you looking for?

My apps

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

Request Access

DocuSign

A platform which provides digital transaction management s...

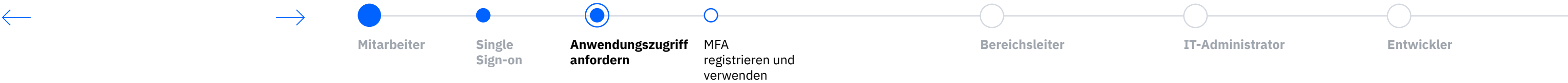
Justification

I need to sign sales contracts to close deals.

Cancel

Submit

© 2020 Bane & Dox Co.



Mitarbeiter: 3 von 4

Anwendungszugriff anfordern

Offene Anfragen

Auf der Seite mit den offenen Anfragen kann Jessica ihre offenen Zugriffsanfragen sehen, wem sie zugewiesen sind und welchen Status sie haben. Bei Bedarf kann sie hier noch einmal nachsehen, um ihrer Begründung weitere Details hinzuzufügen.

Weiter:

Neue App in der Klickstartleiste

 Bane & Dox Co.

App center

My requests

My Requests

Q

Pending

▼

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

Items per page: 50

▼

1–1 of 1 items

1

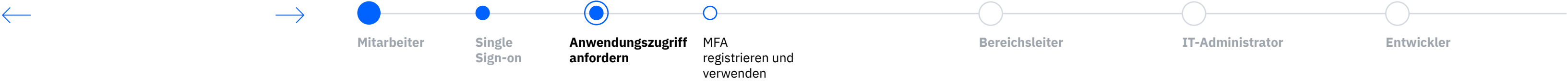
▼

of 1 pages

◀

▶

© 2020 Bane & Dox Co.



Mitarbeiter: 4 von 4

Anwendungszugriff anfordern

Neue App in der Klickstartleiste

Sobald die Anfrage vom Eigentümer der Anwendung genehmigt wurde, sieht sie, dass XYZ zu ihrer Klickstartleiste hinzugefügt wurde.

Weiter:
Neue Klickstartleiste für Authentifizierungsgerät hinzufügen

 Bane & Dox Co.

App centerMy requests

My apps

Add app +

Sort by A-Z ▾



What app are you looking for?



Amazon Appstream



Box



Confluence



Developer App



DocuSign



IBM QRadar



IBM Security Verify Developer Portal



Microsoft Excel Online



Microsoft OneNote



Microsoft PowerPoint Online



Microsoft Word Online



OneDrive



Outlook



Salesforce

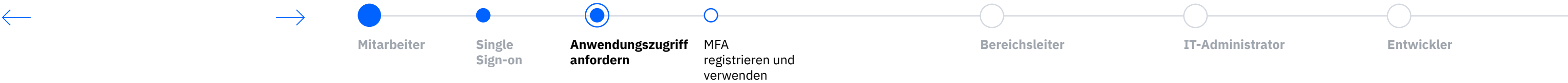


ServiceNow



Stride

© 2020 Bane & Dox Co.



Mitarbeiter: 1 von 3

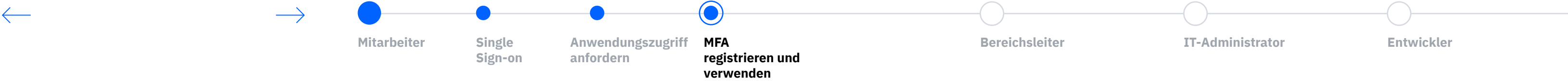
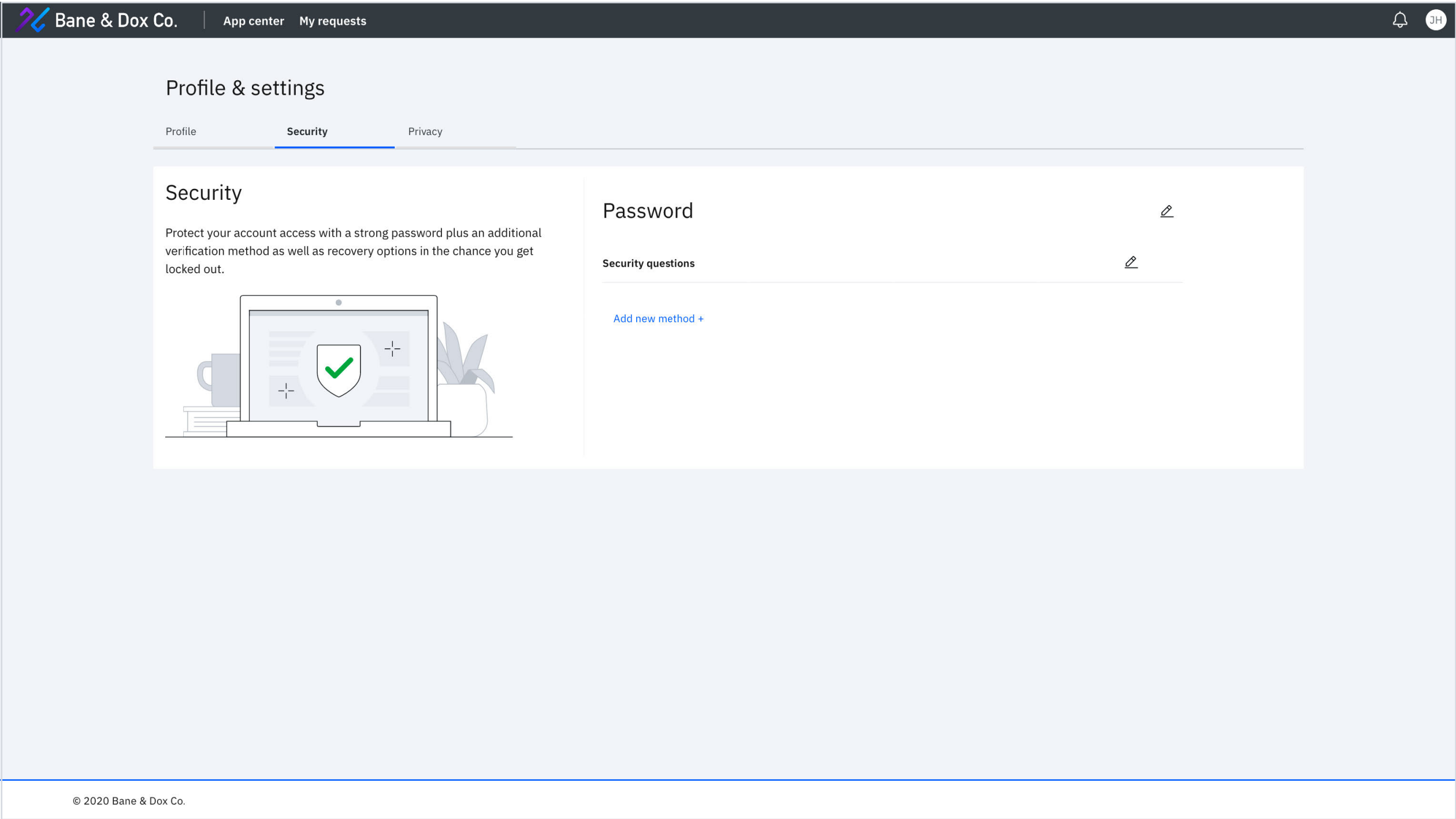
MFA registrieren und verwenden

Neue Klickstartleiste für Authentifizierungs- gerät hinzufügen

Jessica kann auf ihrer Seite mit den Sicherheitseinstellungen Geräte und Ressourcen hinzufügen, die für Authentifizierungsherausforderungen verwendet werden sollen. Sie kann ihr Mobiltelefon für die Verwendung mit der IBM Security Verify Mobile App registrieren, um MFA-Anforderungen zu erfüllen, oder eine der anderen verfügbaren Methoden wählen.

Weiter:

MFA Registrierung



Mitarbeiter: 2 von 3

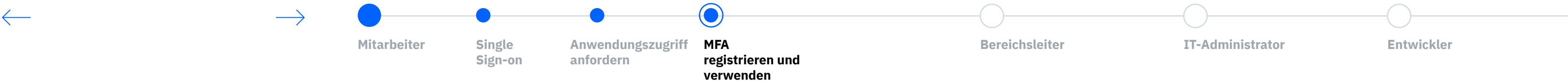
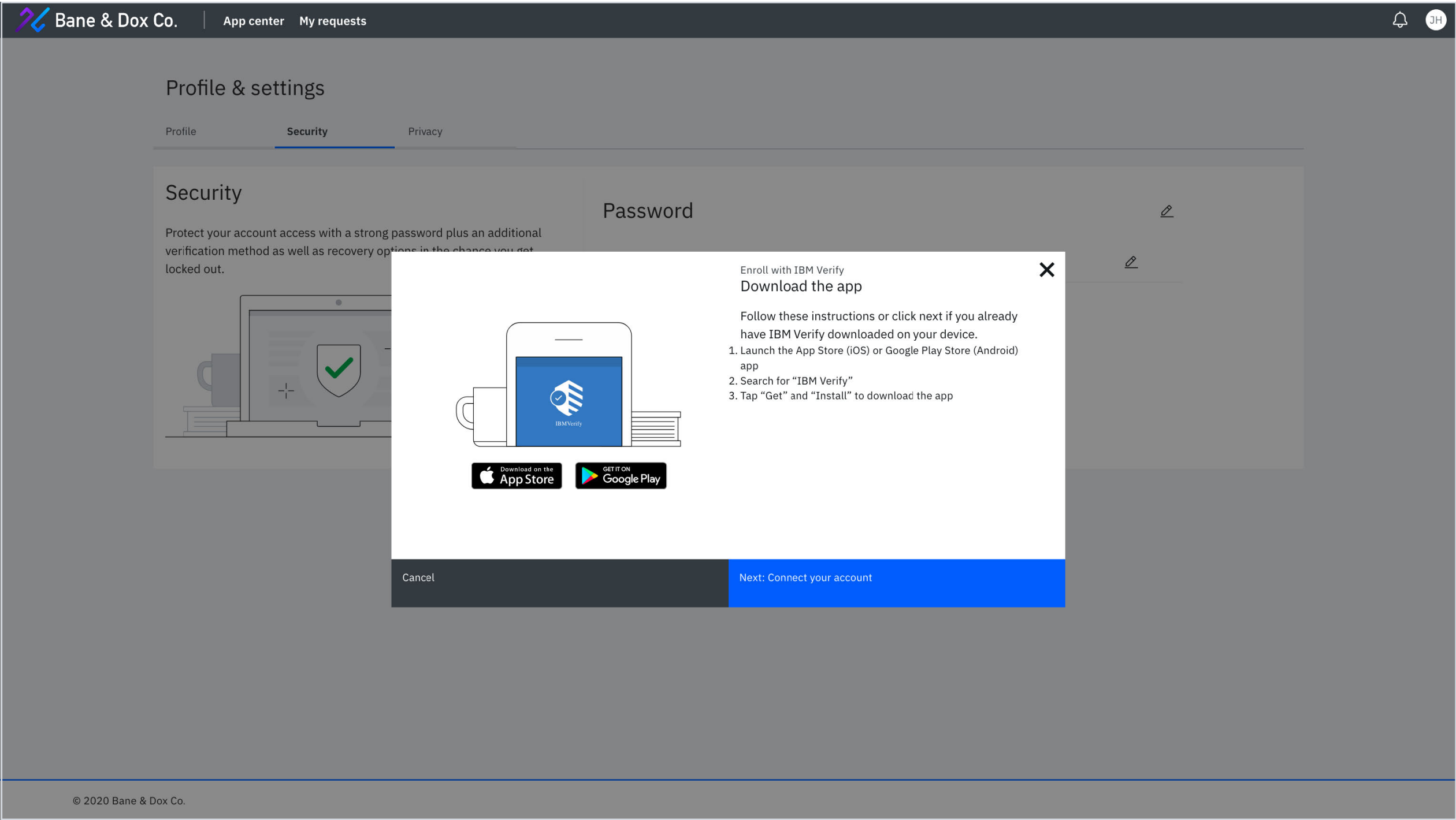
MFA registrieren und verwenden

Mobile App einstellen

Jessica kann auf ihrer Seite mit den Sicherheitseinstellungen Geräte und Ressourcen hinzufügen, die für Authentifizierungsherausforderungen verwendet werden sollen. Sie kann ihr Mobiltelefon für die Verwendung mit der IBM Security Verify Mobile App registrieren, um MFA-Anforderungen zu erfüllen, oder eine der anderen verfügbaren Methoden wählen.

Weiter:

Wählen Sie die MFA Methode



Mitarbeiter: 3 von 3

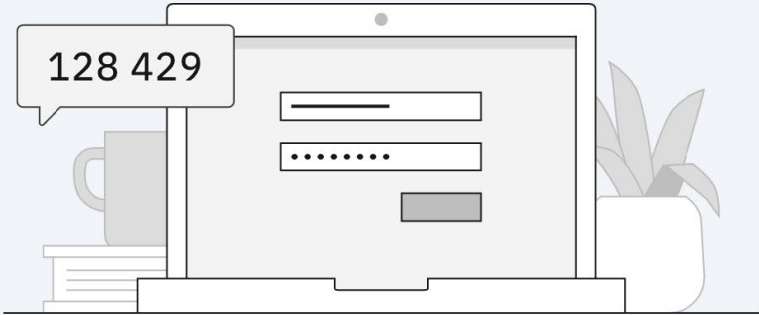
MFA registrieren und verwenden

Wählen Sie die MFA Methode

Wenn sich Jessica nun bei einer App anmeldet, die MFA erfordert, kann sie die unterstützte Authentifizierungsmethode wählen, die für sie am bequemsten ist.

Weiter:

Geschäftsbereichsmanager



 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)

Jessica's iPhone (Touch Approval)

Send push

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.

Geschäftsbereichs- manager

Verwalten Sie teamspezifische
Anwendungsberechtigungen mit
delegierten Steuerelementen.

Um wettbewerbsfähig zu bleiben, müssen
die Geschäftsbereichsmanager ihren
Mitarbeitern und Kunden schnell neue
Dienste anbieten. Sie müssen mit der
Geschwindigkeit ihres Geschäfts Schritt
halten, ohne auf die IT zu warten.

Beginnen Sie mit:
**Offene
Benachrichtigung in
der Klickstartleiste**



Anzeigen

20 %

20 bis 50 % aller Anrufe
beim IT-Helpdesk betreffen
das Zurücksetzen von
Kennwörtern

Weltwirtschaftsforum

*„Es ist wirklich frustrierend,
von Tools und Systemen
ausgebremst zu werden,
wenn ich nur versuche,
meine Arbeit zu erledigen.“*

Jakob, Angestellter

Bereichsleiter

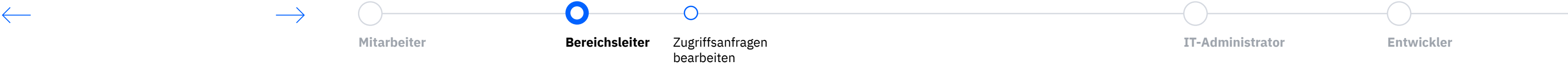




Anzeigen



Anzeigen



Geschäftsbereichs- manager

**Verwalten Sie teamspezifische
Anwendungsberechtigungen mit
delegierten Steuerelementen.**

Um wettbewerbsfähig zu bleiben, müssen
die Geschäftsbereichsmanager ihren
Mitarbeitern und Kunden schnell neue
Dienste anbieten. Sie müssen mit der
Geschwindigkeit ihres Geschäfts Schritt
halten, ohne auf die IT zu warten.

20 %

20 bis 50 % aller Anrufe
beim IT-Helpdesk betreffen
das Zurücksetzen von
Kennwörtern

Weltwirtschaftsforum

*„Es ist wirklich frustrierend,
von Tools und Systemen
ausgebremst zu werden,
wenn ich nur versuche,
meine Arbeit zu erledigen.“*

Jakob, Angestellter

Bereichsleiter





- Mitarbeiter

Bereichsleiter

Zugriffsanfragen bearbeiten

Offene Benachrichtigung in der Klickstartleiste

Anfragedetails anzeigen

Zusätzliche Begründung anfordern

Anfrage genehmigen/ablehnen

IT-Administrator

Entwickler

Geschäftsbereichsmanager: 1 von 4
Zugriffsanfragen bearbeiten

Offene Benachrichtigung in der Klickstartleiste

Jacob ist der Manager des Verkaufsteams von Bane & Dox Co. Wenn er sich bei IBM Security Verify anmeldet, kann er alle Anwendungen sehen, auf die er Zugriff hat. Jacob hat die Berechtigung erhalten, DocuSign für das Unternehmen zu verwalten und Zugriffsanfragen von Mitarbeitern zu genehmigen, ohne auf die IT-Abteilung zu warten. Hier kann er offene Benachrichtigungen für App-Anfragen einsehen.

Weiter:
Anfragedetails anzeigen

App centerMy requestsTask manager

My apps

What app are you looking for?

Sort by A-Z

Add app


Amazon Appstream


Box


Confluence


Developer App


IBM QRadar


Microsoft Excel Online


Microsoft OneNote


Microsoft PowerPoint Online


Microsoft Word Online


Monday.com


OneDrive


Outlook


Salesforce


ServiceNow


Stride

© 2020 Bane & Dox Co.

←

→

Mitarbeiter

Bereichsleiter

Zugriffsanfragen bearbeiten

IT-Administrator

Entwickler



ZurückWeiter

Anfragedetails anzeigen

Weiter:
**Zusätzliche Begründung
anfordern**

Bane & Dox Co.

App center

My requests

Task manager

JA

Task manager

App requests

Access certification

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

Request details

DocuSign

<http://docusign.com/>

A platform which provides digital transaction management services

Request ID

b29fdf8ce48c452dacb74b806d9dd883

Status

Need action

Requester

Jessica Hudson

[Current entitlements](#)

Request date

15th May 2020

Last action

15th May 2020

Comments

Jessica Hudson

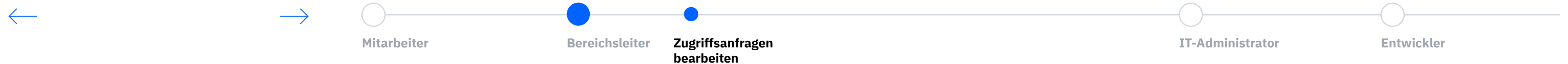
Today at 3:16 PM

I need to sign sales contracts to close deals.

Reject

Approve

© 2020 Bane & Dox Co.

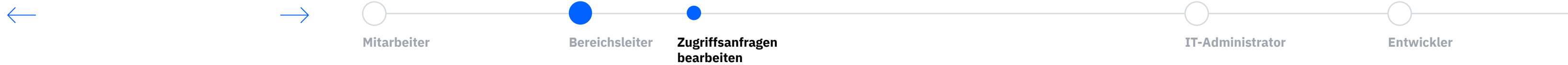
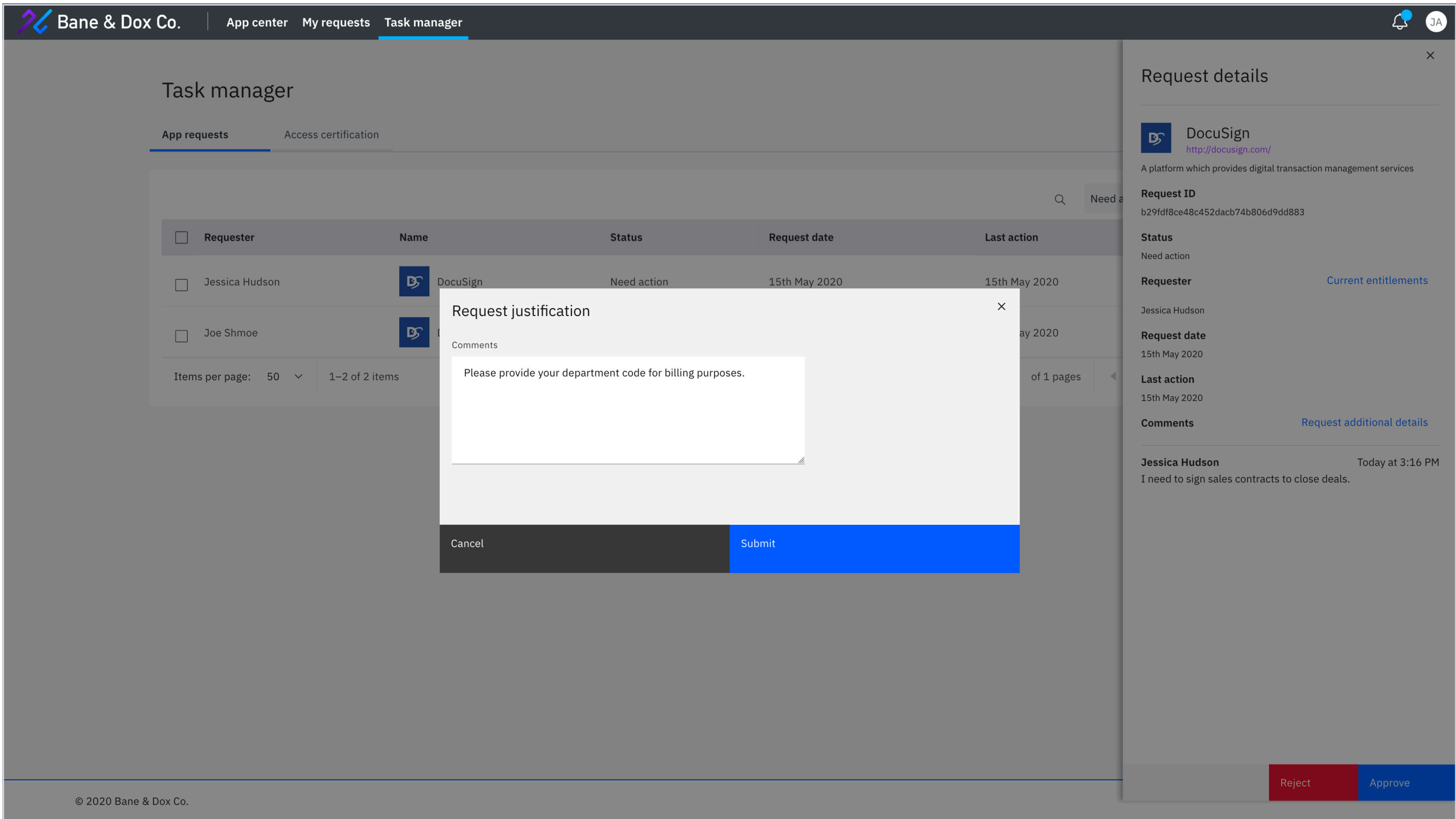


Geschäftsbereichsmanager: 3 von 4

Zusätzliche
Begründung
anfordern

Er kann die Anfrage zurückschicken, um weitere Begründungen zu erhalten.

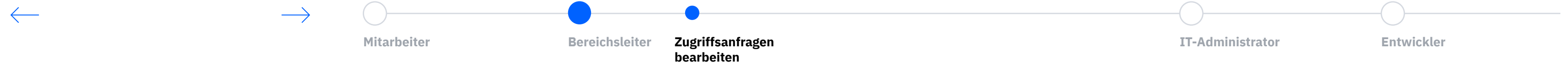
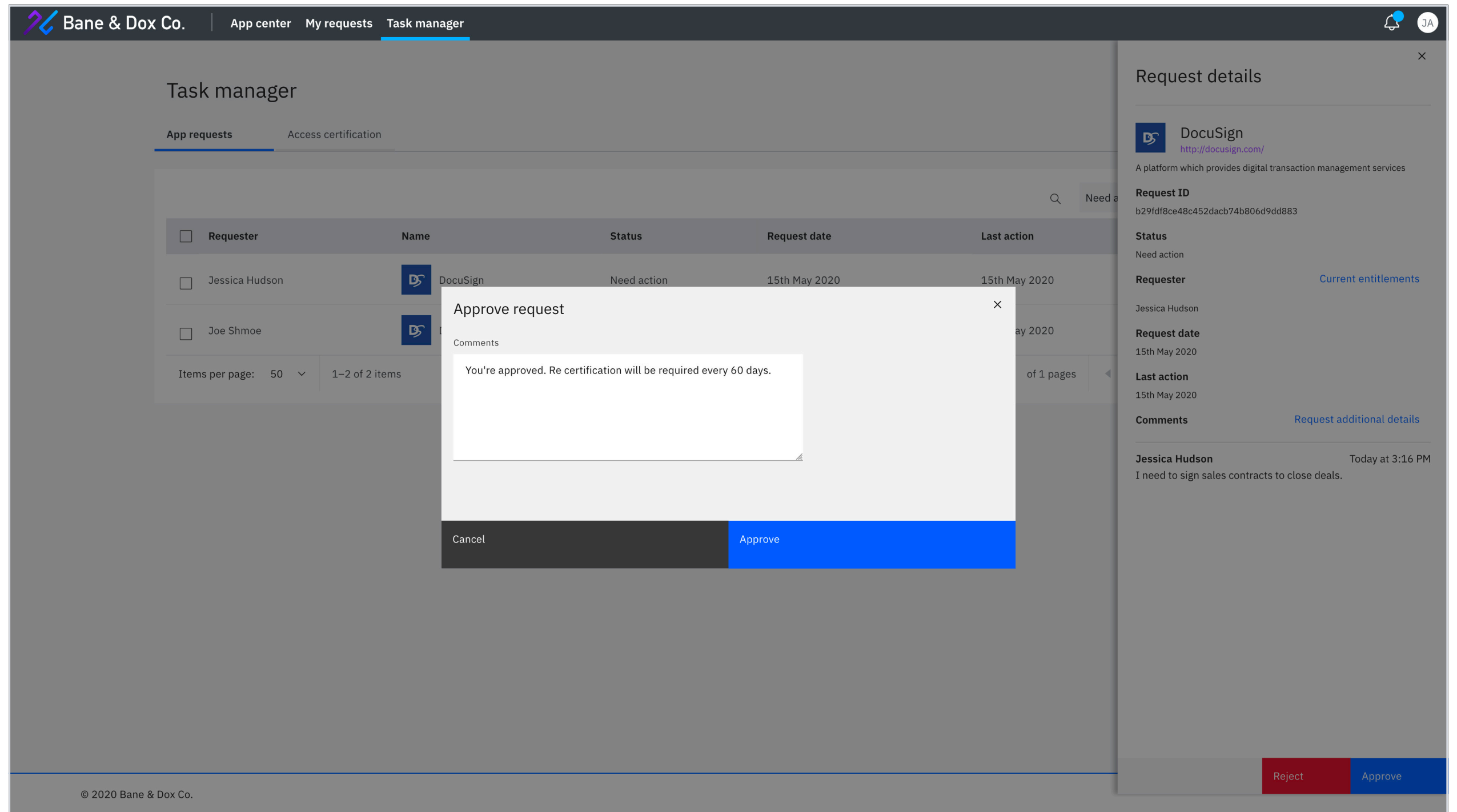
Weiter:
Anfrage genehmigen/ablehnen



Anfrage
genehmigen/
ablehnen

Oder er kann die Anfrage freigeben/
ablehnen. Da er die Zugriffsgenehmigungen
für seine direkten Mitarbeiter selbst in der
Hand hat, ermöglicht er es seinem Team,
mit dem aktuellen Geschäftstempo Schritt
zu halten, ohne sich durch die IT-Logistik
belastet zu fühlen.

Weiter:
IT-Administrator



IT-Administrator

Vereinfachen Sie die Konfiguration, skalieren Sie auf einer gemeinsamen Plattform und automatisieren Sie den Risikoschutz.

IT-Administratoren müssen die Geschäftsanforderungen nach einfachem Zugriff erfüllen und gleichzeitig ihre Organisation vor dem unsachgemäßen Gebrauch von Anmeldedaten schützen – obwohl es ihnen möglicherweise an Zeit, Fähigkeiten und Ressourcen mangelt. Teams können auch das Gefühl haben, die Kontrolle zu verlieren, wenn sie Cloud-Anwendungen von einer Vielzahl von Anbietern einbinden, so dass ein integrierter Ablauf für SSO und MFA von entscheidender Bedeutung wird.

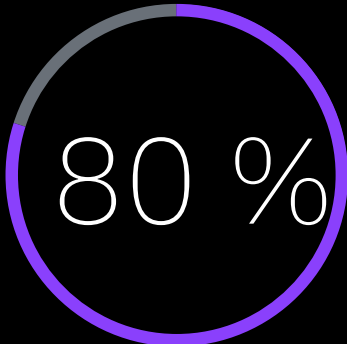
Beginnen Sie mit:
Live-Anzeigefeld



Anzeigen



Anzeigen



80 % der Hackerangriffe basieren auf kompromittierten und schwachen Berechtigungsnachweisen

Weltwirtschaftsforum

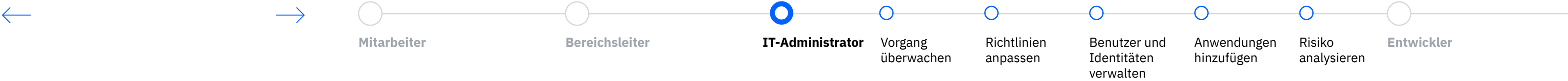
„Ich muss die Produktivität meines Unternehmens fördern, meine Kollegen schützen und alle Aspekte der identitäts- und zugangsbezogenen Risiken berücksichtigen – und das alles gleichzeitig.“

Scott, IT-Administrator

IT-Administrator



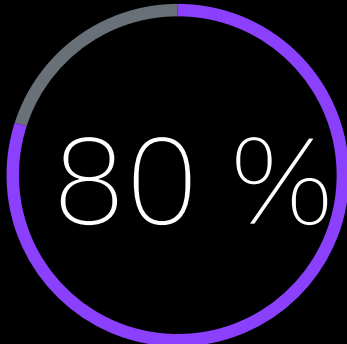
Anzeigen



IT-Administrator

Vereinfachen Sie die Konfiguration, skalieren Sie auf einer gemeinsamen Plattform und automatisieren Sie den Risikoschutz.

IT-Administratoren müssen die Geschäftsanforderungen nach einfachem Zugriff erfüllen und gleichzeitig ihre Organisation vor dem unsachgemäßen Gebrauch von Anmeldedaten schützen – obwohl es ihnen möglicherweise an Zeit, Fähigkeiten und Ressourcen mangelt. Teams können auch das Gefühl haben, die Kontrolle zu verlieren, wenn sie Cloud-Anwendungen von einer Vielzahl von Anbietern einbinden, so dass ein integrierter Ablauf für SSO und MFA von entscheidender Bedeutung wird.



80 % der Hackerangriffe basieren auf kompromittierten und schwachen Berechtigungsnachweisen

Weltwirtschaftsforum

„Ich muss die Produktivität meines Unternehmens fördern, meine Kollegen schützen und alle Aspekte der identitäts- und zugangsbezogenen Risiken berücksichtigen – und das alles gleichzeitig.“ ”

Scott, IT-Administrator



IT-Administrator

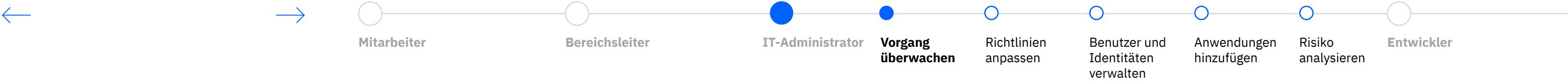
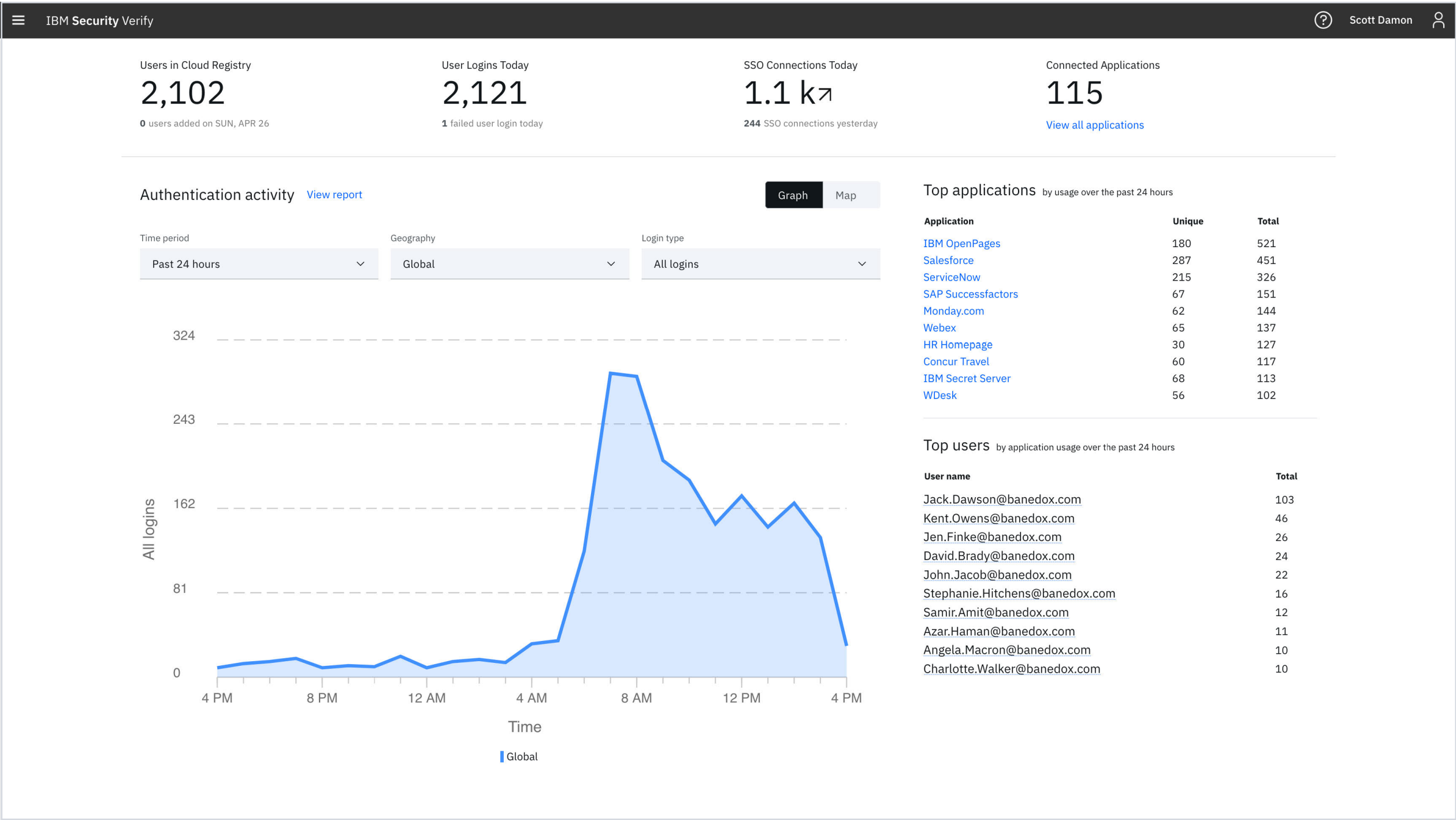


IT-Administrator: 1 von 3
Vorgang überwachen

Live-Anzeigefeld

Das administrative Anzeigefeld von IBM Security Verify bietet einen globalen Überblick über die Authentifizierungsaktivitäten innerhalb einer Organisation. Scott, ein IT-Administrator, kann nach Zeiträumen oder Regionen filtern, um Benutzer Trends besser zu verstehen.

Weiter:
Aktivitätsberichte erstellen



IT-Administrator: 2 von 3

Vorgang überwachen

Aktivitätsberichte erstellen

Die Berichtsschnittstelle von Verify ermöglicht es Scott, die jüngsten Aktivitätsdaten zeitnah zu filtern, um Probleme schnell zu diagnostizieren. Über Authentifizierungsaktivitäten, Adaptive Access, Anwendungsnutzung und Administrator- und MFA-Aktivitäten kann er tief in die Zugriffs- und Authentifizierungsdaten seines Unternehmens eintauchen, um Erkenntnisse zu sammeln und Fehler zu beheben.

Weiter:
Aktivitätsberichte von Adaptive Access

IBM Security Verify

?

Scott Damon

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

5

Medium

48

High

27

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

TOTP

31

Email OTP

220

IBM verify push

175

🕒

Past 30 days

[View Report](#)

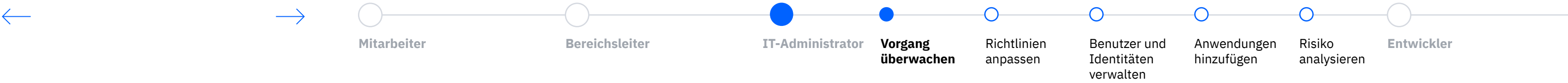
Fulfillment activity

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

Select application

All applications

[View Report](#)



IT-Administrator: 3 von 3
Vorgang überwachen

Aktivitätsbericht von Adaptive Access

In einem Adaptive Access-Bericht kann Scott beispielsweise alle jüngsten Anmeldungen von Anwendungen sehen, die eine Adaptive Access-Zugriffsrichtlinie und dokumentierte Ereignisparameter verwenden. Mithilfe der Berichte in Verify kann er Ereignisse mit hohem Risiko diagnostizieren und beheben und bei Bedarf Maßnahmen ergreifen.

Adaptive Access Interaktive Demo

Weiter:
Richtlinieneditor

IBM Security Verify

Reports

Adaptive access

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)

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

Total invocations 19

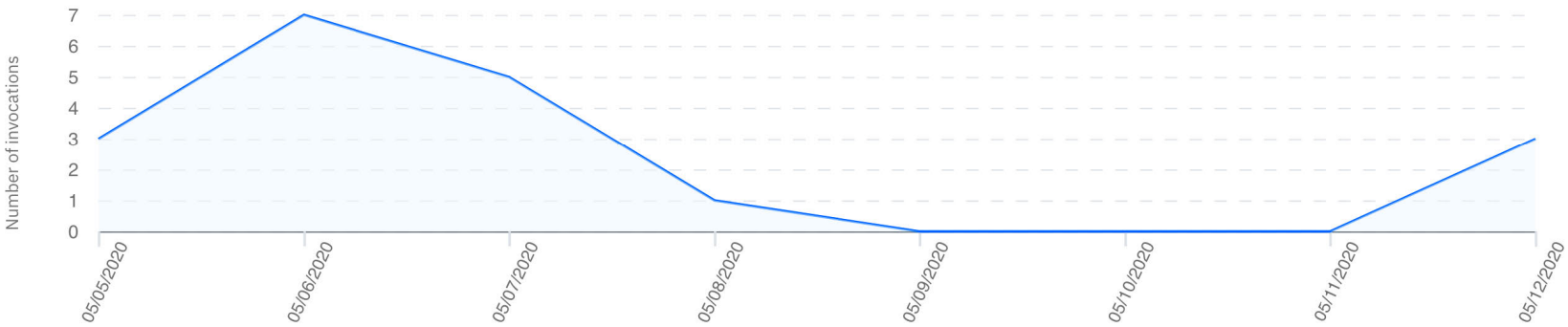
Very high 0

High 5

Medium 8

Low 6

Number of invocations



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

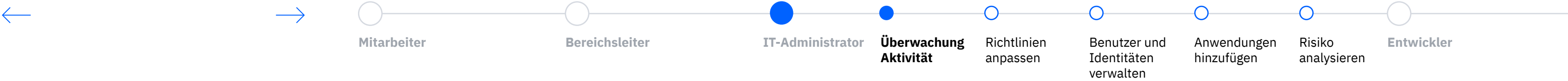
Risky device False

Risky connection True

Internet provider Spectrum

Location Austin
USA

New location False



IT-Administrator: 1 von 3
Richtlinien anpassen

Richtlinieneditor

Im Zugriffsrichtlinien-Editor kann Scott weitere benutzerdefinierte Zugriffsrichtlinien erstellen, die er für die Anwendungen seines Unternehmens verwenden kann. Einige Richtlinien sind standardmäßig enthalten, wie z. B. den Zugang immer zuzulassen, immer 2FA zu verlangen oder 2FA zu Beginn jeder neuen Sitzung zu verlangen.

Weiter:
Regel zur Richtlinie hinzufügen

IBM Security Verify

?

Scott Damon

Security

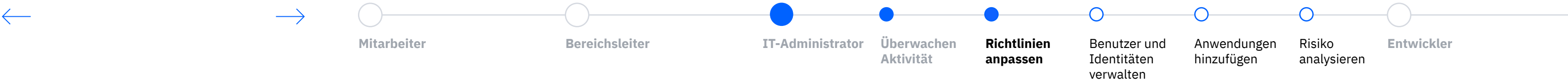
Access policiesAuthentication factorsFIDO2Registration profilesTokensApplication consentsPolicy editorSign-in options

All policies

Manage access policies

Add policy

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	



IT-Administrator: 2 von 3
Richtlinien anpassen

Regel zur Richtlinie hinzufügen

Scott kann auf einfache Weise Regeln konfigurieren, die auf Bedingungen wie Gerät, Gruppenzugehörigkeit, IP-Adresse und Geostandort basieren und die den Zugang oder die Abfrage mit MFA entweder erlauben oder blockieren.

Weiter:
Adaptiver Zugriff

IBM Security Verify

Security

Access policies

All policies

Manage access po

Policy name

Corporate access

Corporate network

Enable 2fa bypass

Master Policy

MFAGroup Policy

Require 2FA on Ar

Trusteer Device Po

Allow access from

Allow access from

Allow access from

Allow access from

Allow access from

Allow access from

Allow access from

Allow access from

Allow access from

↳ Name and description

↳ Adaptive Access

↳ Policy rules

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

+ Add Condition

Action

Then

MFA always

Authentication methods

Any available method (default)

Email OTP

SMS OTP

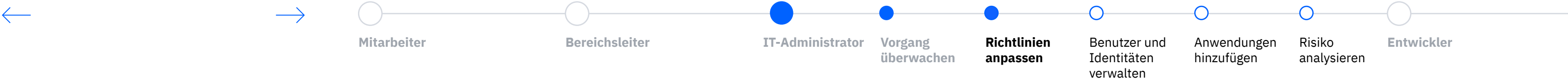
FIDO2

Time-based OTP

IBM Verify

Back

Next



Adaptiver Zugriff

Adaptive Access Interaktive Demo

Weiter:
Management-Benutzer

IBM Security Verify

?

Scott Damon

Security

Access policies

All policies

Manage access po

Policy name

Corporate access

Corporate network

Enable 2fa bypass

Master Policy

MFAGroup Policy

Require 2FA on Ar

Trusteer Device Po

Allow access from

Allow access from

Allow access from

Allow access from

Allow access from

Allow access from

Allow access from

Allow access from

↳ Name and description

↳ Adaptive Access

↳ Policy rules

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

Action

Then

MFA always

Authentication methods

☐ Any available method (default)

☐ Email OTP

☐ SMS OTP

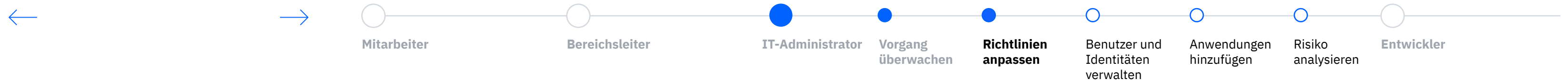
☒ FIDO2

☒ Time-based OTP

☒ IBM Verify

Back

Next



Management- Benutzer

Weiter: Gruppen verwalten

Security

Access policies

All policies

Manage access po

Policy name

Corporate access

Corporate network

Enable 2fa bypass

Master Policy

MFAGroup Policy

Require 2FA on An

Trusteer Device Po

Allow access from

Allow access from

Allow access from

Allow access from

Allow access from

Allow access from

Allow access from

Allow access from

↳ Name and description

↳ Adaptive Access

↳ Policy rules

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

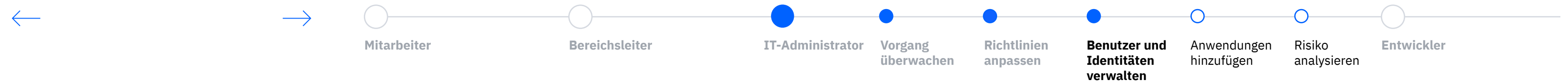
☒ FIDO2

☒ Time-based OTP

☒ IBM Verify

Back

Next



IT-Administrator: 2 von 5

Verwalten Sie Benutzer und Identitätsquellen

Gruppen verwalten

Ob nach Abteilungen, Rolle oder einem eindeutigen Attribut geordnet, können Gruppen dazu beitragen, den Zugriff innerhalb einer Organisation zu modularisieren. Scott kann zum Beispiel eine neue Bene & Dox Co. Vertriebsgruppe hinzufügen, damit diese Gruppe von Personen auf gemeinsame Vertriebsanwendungen zugreifen kann. Wenn er ein vorhandenes Verzeichnis in Verify integriert, bleiben die Gruppen dieses Verzeichnisses erhalten.

Weiter:

Benutzerattribute verwalten

IBM Security Verify

Users & groups

UsersGroupsSettings

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	4/5/1
Enablement	5/20
Helpdesk	4/25
Legal	5/19
New Test Group Name	1/21/2019
readonly	5/9/2019
Sales	4/29/2019

Edit Group

Name*

Enablement

Description

A group for our enablement team

Date Created

5/20/2019

Date Modified

5/20/2019

Group Members

AddRemove

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

AddDelete

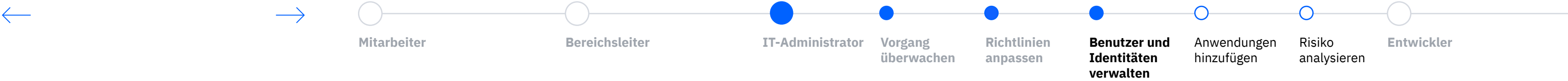
Group Details

Name

Enablement

Description

Zqy89beBi0e7slXr1wp2Dw==



IT-Administrator: 3 von 5
Verwalten Sie Benutzer und Identitätsquellen

Benutzerattribute verwalten

Während Verify standardmäßig Dutzende der gängigsten Benutzerattribute enthält, kann Scott bei Bedarf zusätzliche Attribute aus einer seiner verbundenen Identitätsquellen verknüpfen oder benutzerdefinierte Attribute erstellen. Diese Attribute können dann in Identitätsquellen und Anwendungen für die einmalige Anmeldung, die Bereitstellung, die Erstellung von Profilen und mehr referenziert werden.

Weiter:
Active Directory und LDAP

IBM Security Verify

Configuration

API access

Create and manage

Name
AWS_team Fixed value
base64Email Fixed value
complexCondi 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](#)

[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

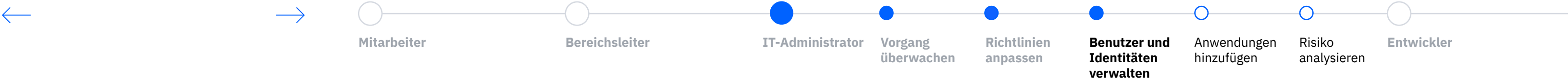
Enter the attribute name from each identity source you want to map to this attribute. Use "Any" to represent any identity source that is not specified.

Identity source	Attribute name from the identity source
Active Directory	department

Identity source	Attribute name from the identity source
-----------------	---

Cancel

Save



IT-Administrator: 4 von 5

Verwalten Sie Benutzer und Identitätsquellen

Active Directory und LDAP

Scott kann Verify so konfigurieren, dass es eine Verbindung zu einem vorhandenen Active Directory oder einer LDAP-Identitätsquelle oder sogar zu nicht standardmäßigen Verzeichnissen, Datenbanken oder externen Services herstellt.

Weiter:
Soziale Anmeldung

IBM Security Verify

Configuration

API access

Create and manage

Name
AWS_team Fixed value
base64Email Fixed value
complexCondi 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](#)

[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

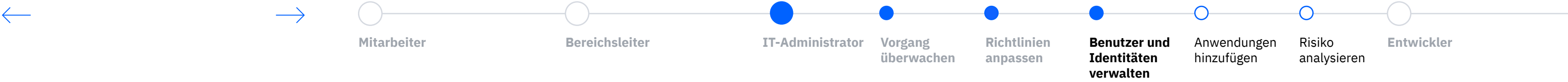
Enter the attribute name from each identity source you want to map to this attribute. Use "Any" to represent any identity source that is not specified.

Identity source	Attribute name from the identity source
Active Directory	department

Identity source	Attribute name from the identity source
-----------------	---

Cancel

Save

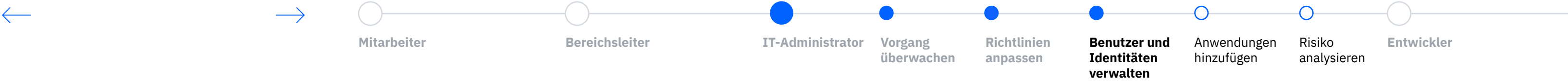
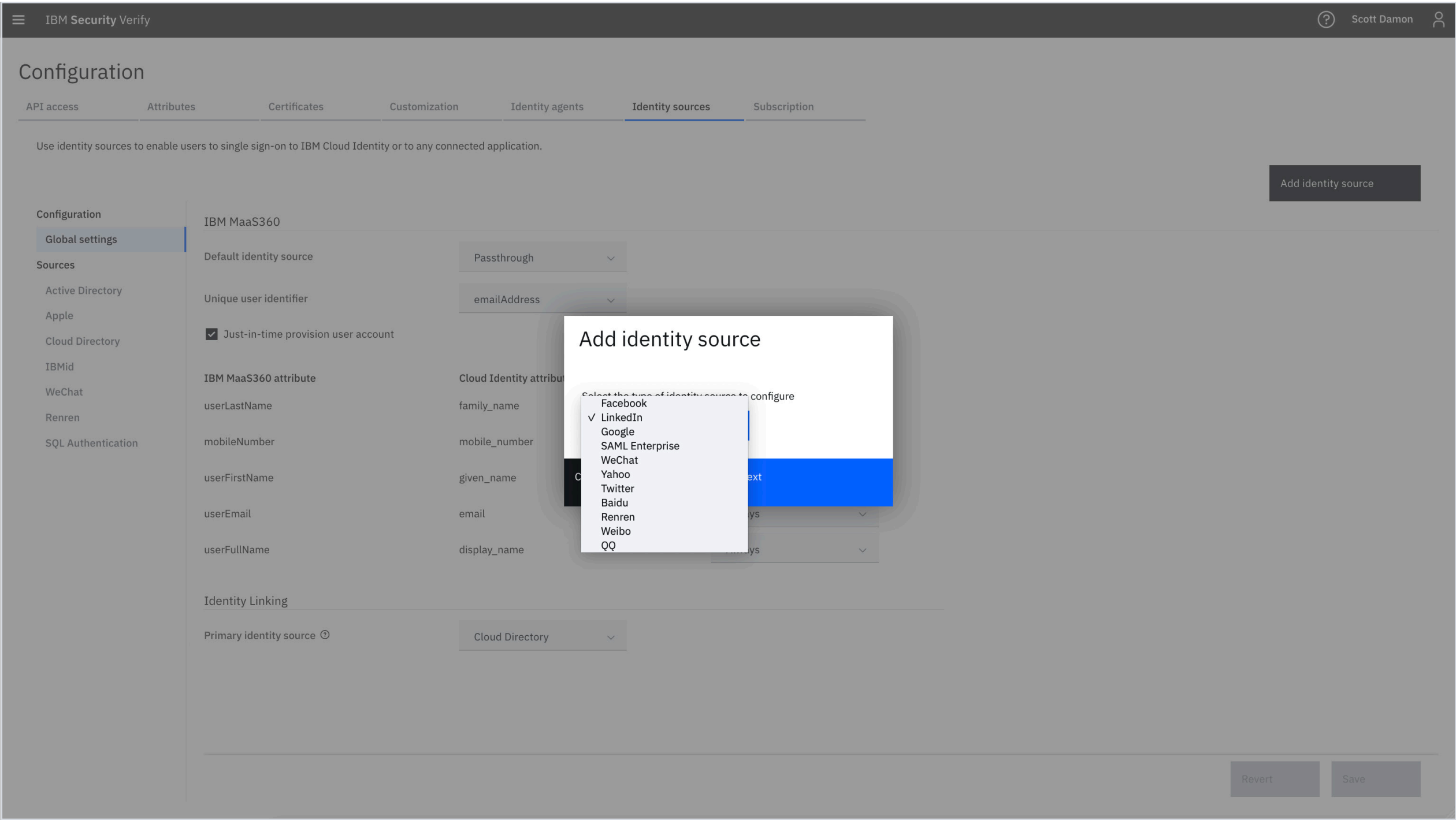


IT-Administrator: 5 von 5
Verwalten Sie Benutzer und
Identitätsquellen

Soziale Anmeldung

Scott kann auch eine Vielzahl von sozialen Anmeldeanbietern verknüpfen, um seinen Nutzern mehr Optionen zu bieten, von Google und LinkedIn bis hin zu regionalspezifischen Anbietern.

Weiter:
Anwendungen anzeigen



IT-Administrator: 1 von 6
Anwendungen hinzufügen

Anwendungen anzeigen

Verify unterstützt Hunderte von SaaS-Anwendungen, ermöglicht die rationelle Einbindung von benutzerdefinierten Anwendungen und bietet ein schlankes Application Gateway, um die Unterstützung auch auf lokale Anwendungen zu erweitern. Scott kann alle Anwendungen seiner Organisation über eine einzige Benutzerschnittstelle verwalten.

Weiter:
Nach Anwendungen zum Hinzufügen suchen

IBM Security Verify

?

Scott Damon

Configuration

API accessAttributesCertificatesCustomizationIdentity agentsIdentity sourcesSubscription

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

Add identity source

Configuration

Global settingsSourcesActive DirectoryAppleCloud DirectoryIBMidWeChatRenrenSQL Authentication

IBM MaaS360

Default identity sourcePassthrough

Unique user identifieremailAddress

☒ Just-in-time provision user account

IBM MaaS360 attribute

userLastNamefamily_name

mobileNumbermobile_number

userFirstNamegiven_name

userEmailemail

userFullNamedisplay_name

Identity Linking

Primary identity source ⓘCloud Directory

Select the type of identity source to configure

Facebook

✓ LinkedIn

Google

SAML Enterprise

WeChat

Yahoo

Twitter

Baidu

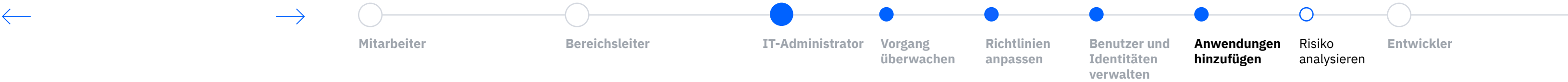
Renren

Weibo

QQ

Revert

Save



IT-Administrator: 2 von 6
Anwendungen hinzufügen

Nach Anwendungen zum Hinzufügen suchen

Scott kann nach einer neuen Anwendung, wie Monday.com, suchen, die er hinzufügen möchte. Mit vordefinierten SaaS-Konnektoren ist die Integration neuer Anwendungen in ein föderiertes Einzelanmeldesystem ein Kinderspiel.

Weiter:
Berechtigungsinhaber für Zugriffsgenehmigungen hinzufügen

IBM Security Verify

Applications

Total applications24

Enabled24

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

Select Application Type

Custom Application

The custom template to access any type of application.

Search

mingie by 1noughtworks

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

Cancel

Add application

Account lifecycle enabled

Bookmark0

Add application

Account lifecycle

Disabled

Disabled

Disabled

Disabled

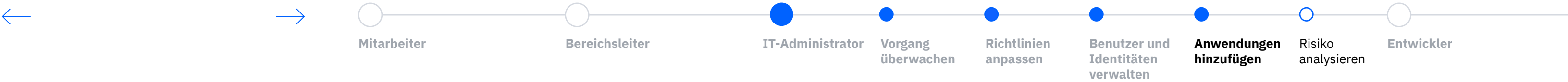
Disabled

Disabled

Disabled

Disabled

Disabled



IT-Administrator: 3 von 6

Anwendungen hinzufügen

Berechtigungsinhaber
für Zugriffs-
genehmigungen
hinzufügen

Um die laufenden Operationen mit der
Anwendung zu verwalten, kann Scott einen
Anwendungseigner und einen oder mehrere
Freigabeberechtigte für Zugriffsanfragen
zuweisen.

Weiter:
**Anmeldungseinstellungen
konfigurieren**

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



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



Add owner

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

Anmeldungs-einstellungen konfigurieren

Auf der Registerkarte Anmeldung kann Scott die erforderlichen Parameter für die Anwendung konfigurieren, damit diese ordnungsgemäß in Verify integriert werden kann, wobei anwendungsspezifische Anweisungen helfen. Weiter unten auf der Seite kann er andere Aspekte der Integration konfigurieren, z. B. die Zuordnung der Attribute, die an den Leistungserbringer gesendet werden sollen, sowie die Zugriffsrichtlinie, die für die Anwendung gelten soll.

Weiter:
Berechtigungen konfigurieren

IBM Security Verify

?

Scott Damon

Add Application



Monday.com

General

Sign-on

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)

- 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`
- Click your profile name and then select **Admin** from the drop-down menu.
- Click **Security**.
- On **Login** page, click **Open** next to the **SAML** option.
- In the **Security & Authentication Settings** section, specify the following settings:
SAML SSO Url
`https://rlshahtestmobile.itel.idng.ibmcloudsecurity.com/saml/sp/s/saml20ip/saml20/login`

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

Cancel

Save

IT-Administrator: 5 von 6
Anwendungen hinzufügen

Berechtigungen konfigurieren

Auf der Registerkarte Berechtigungen kann Scott die für die Anwendung geeignete Zugriffsebene und Freigabelogistik konfigurieren. In diesem Fall wählt er eine bestimmte Gruppe von Benutzern und Gruppen aus.

Weiter:
Regelmäßige erneute
Zertifizierung des Zugangs
festlegen

IBM Security Verify

?

Scott Damon

Applications / Details



Monday.com

Monday

General

Sign-on

Entitlements

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

Search name

Add

Remove

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

Delete

Cancel

Save

Details

Name

Sales

Assigner

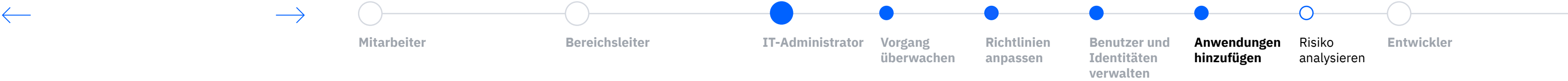
-

Email

-

Comments

-



IT-Administrator: 6 von 6
Anwendungen hinzufügen

Regelmäßige erneute Zertifizierung des Zugangs festlegen

Im Laufe der Zeit kann es für eine Organisation schwierig sein Anwendungen effizient zu rezertifizieren, um sicherzustellen, dass die Zugriffsebenen immer noch angemessen sind. Um sicherzustellen, dass dieser wichtige Schritt nicht verpasst wird, kann Scott regelmäßige Kampagnen zur Rezertifizierung auf Anwendungsbasis einrichten, um diesen Aspekt der Identitätsverwaltung zu automatisieren.

Weiter:
Analysedashboard

IBM Security Verify

?

Scott Damon

Governance / Certification campaigns

Productivity applications

RunningPause

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

Edit settings

Cancel campaign

Details

Campaign ID

d5fc1070a8c0425da210ab60cc216516

Created by

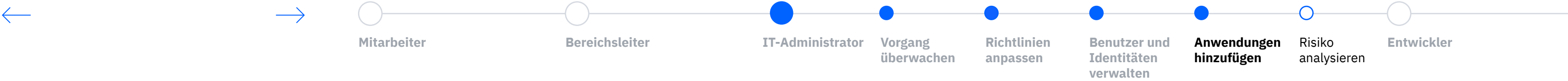
Scott Damon
scott.damon@banedox.com
scott@cloudIdentityRealm

Created on

Apr 27, 2020

Modified on

—



IT-Administrator: 1 von 3
Risiko analysieren

Analysedashboard

Scott kann den Gesamtzustand seiner IAM-Umgebung im Analysedashboard für Identitäten überprüfen, wo er schnell nach identitätsbezogenen Risiken für Benutzer, Berechtigungen und Anwendungen suchen kann. Er kann einzelne Benutzer und Anwendungen genauer unter die Lupe nehmen, um weitere Einsichten in Verstöße und kumulierte Risikowerte zu erhalten.

Weiter:
Eingestufte Richtlinienverstöße anzeigen

IBM Security Verify

Scott Damon

Quick insights

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

Risky users

110

Critical violations

264

Risky applications

15

Risky entitlements

76

Top recommended actions

Pending reviews

721

All violations

739

Recertify access

Suspend account

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

High risk violations

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 Riegler	
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	

Mitarbeiter

Bereichsleiter

IT-Administrator

Vorgang überwachen

Richtlinien anpassen

Benutzer und Identitäten verwalten

Anwendungen hinzufügen

Risiko analysieren

Entwickler



ZurückWeiter

IT-Administrator: 2 von 3
Risiko analysieren

Eingestufte Richtlinienverstöße anzeigen

Scott kann Anomalien hervorheben und abgestufte Verstöße innerhalb einer Richtlinienkategorie anzeigen, wie z. B. „Berechtigung des Benutzers weicht von der seiner Kollegen ab“. Diese spezielle Richtlinie innerhalb der Identitätsanalyse führt eine Peergruppenanalyse durch, um kontextuell atypische Berechtigungen zu identifizieren, die ein zusätzliches Risiko darstellen können.

Weiter:
Ergreifen Sie vorgeschlagene Korrekturaktionen

IBM Security Verify

Scott Damon

[← Back to dashboard](#)

Application

Search

User's entitlement deviates from peers

Critical violations

118

High risk violations

45

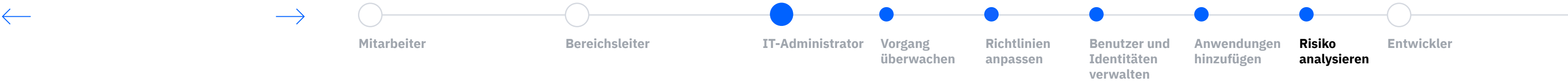
All violations

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 Riegler	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 Boulton	-	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 Riegler	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%		



IT-Administrator: 3 von 3
Risiko analysieren

Ergreifen Sie vorgeschlagene Korrekturaktionen

Für jeden Richtlinienverstoß schlägt Verify neben KI-gestützten Risiko- und Verlässlichkeitsscores auch Korrekturaktionen wie z. B. eine Neuzertifizierung des Zugangs vor. Scott kann die Anforderung für erneute Zertifizierung über das Dashboard der Identitätsanalyse ausführen.

Weiter:
Entwickler

IBM Security Verify

?

Scott Damon

← Back to dashboard

Application

▼

Search

×

User's entitlement deviates from peers

Critical violations

118

High risk violations

45

All violations

174

All

▼

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 Riegler	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 Boulton	-	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 Riegler	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.

Cancel

Add exception

Mark actioned

Recertify access

←→

Mitarbeiter

Bereichsleiter

IT-Administrator

Vorgang überwachen

Richtlinien anpassen

Benutzer und Identitäten verwalten

Anwendungen hinzufügen

Risiko analysieren

Entwickler



ZurückWeiter

Entwickler

Integrieren Sie Zugriff und Authentifizierung in benutzerdefinierten Anwendungen mit intuitiven, speziell entwickelten APIs.

Entwickler müssen Laufzeitabläufe für die Authentifizierung erstellen, Benutzern Registrierungsfunktionen zur Verfügung stellen und MFA in ihre Anwendungen einbetten, ohne unbedingt ein IAM-Experte zu sein. Um dies effizient zu tun, benötigen sie leistungsfähige APIs und Dokumentationen, Beispielcodes und geführte Anleitungen.

Beginnen Sie mit:
Developer Portal



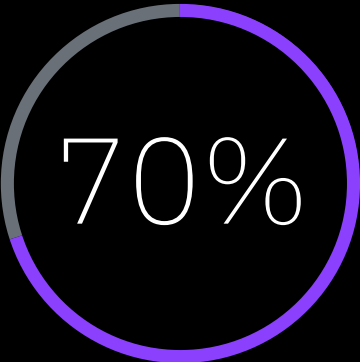
Anzeigen



Anzeigen



Anzeigen



70 % oder mehr aller Anwendungszugriff über Zugriffsmanagement-Lösungen werden bis 2024 MFA nutzen

Gartner

„Ich muss die Authentifizierung schnell in meine Anwendungen einbetten, ohne dass dieser Schritt zu einem Hindernis für das wird, was ich eigentlich erreichen möchte.“

Alice, Entwicklerin

Entwickler



Mitarbeiter



Bereichsleiter



IT-Administrator



Entwickler



Entwickler-ressourcen



Benutzerdefinierte Anwendungen erstellen



API-Konfiguration



Entwickler

Integrieren Sie Zugriff und Authentifizierung in benutzerdefinierten Anwendungen mit intuitiven, speziell entwickelten APIs.

Entwickler müssen Laufzeitabläufe für die Authentifizierung erstellen, Benutzern Registrierungsfunktionen zur Verfügung stellen und MFA in ihre Anwendungen einbetten, ohne unbedingt ein IAM-Experte zu sein. Um dies effizient zu tun, benötigen sie leistungsfähige APIs und Dokumentationen, Beispielcodes und geführte Anleitungen.

70%

70 % oder mehr aller Anwendungszugriff über Zugriffsmanagement-Lösungen werden bis 2024 MFA nutzen

Gartner

„Ich muss die Authentifizierung schnell in meine Anwendungen einbetten, ohne dass dieser Schritt zu einem Hindernis für das wird, was ich eigentlich erreichen möchte.“

Alice, Entwicklerin

Entwickler





Mitarbeiter

Bereichsleiter

IT-Administrator

Entwickler

Entwicklerressourcen

Developer Portal

API-Hilfe

Benutzerdefinierte Anwendungen erstellen

Benutzerdefinierte Anwendungsvorlage hinzufügen

Anmeldungseinstellungen konfigurieren

Bereitstellung konfigurieren

Softwarefehler beheben

API-Konfiguration

API-Clients hinzufügen

Stellvertreterverwaltung



Zurück zum Team

Starten Sie den Mitarbeiter Pfad

Entwickler: 1 von 2

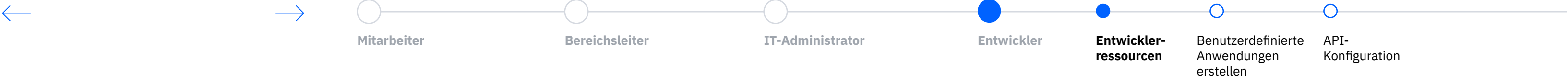
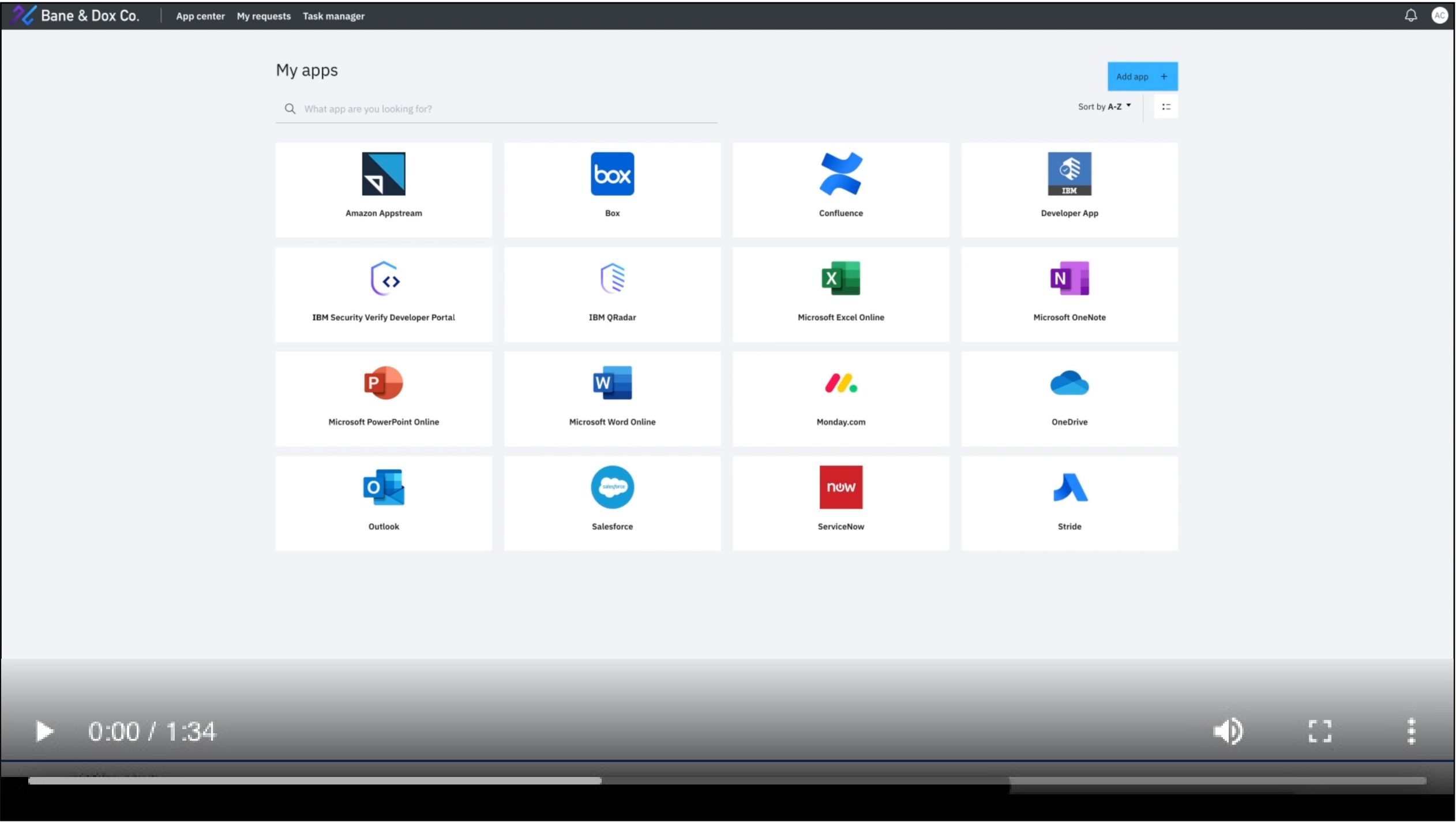
Entwicklerressourcen

Developer Portal

Das IBM Security Verify Developer Portal bietet eine assistentenähnliche Erfahrung, die Entwickler durch den Integrationsprozess einer Anwendung führt. Das Portal bietet neben Codeschnipsel auch Schritt-für-Schritt-Anleitungen und Beispielanwendungen.

Weiter:

API-Hilfe



Entwickler: 2 von 2
Entwicklerressourcen

API-Hilfe

Alice kann die APIs von Verify verwenden, um identitätsbezogene Funktionen wie Benutzermanagement und Authentifizierung in ihre Anwendungen zu integrieren. Die Verify-API-Hilfe bietet Anleitungen für die Implementierung, wie erforderliche Berechtigungen, Parameter und mögliche Antwortmeldungen. Die Hilfetext Dokumentation enthält auch eine Beispiel-Implementierung für jeden API-Aufruf.

Weiter:
Benutzerdefinierte
Anwendungsvorlage
hinzufügen

IBM

allFilter

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

Show/HideList OperationsExpand Operations

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.

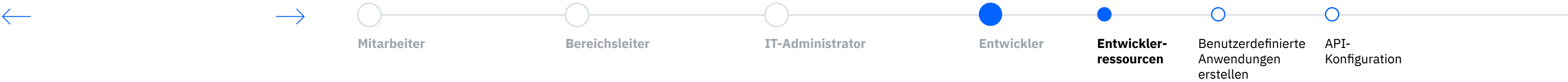
ModelExample Value

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

Response Content Typeapplication/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



Entwickler: 1 von 4
Benutzerdefinierte Anwendungen erstellen

Benutzerdefinierte Anwendungsvorlage hinzufügen

Alice kann ihre benutzerdefinierten Anwendungen neben den anderen lokalen und SaaS-Anwendungen des Unternehmens einbinden, indem sie sie in die fördert ein malige Anmeldung von Verify integriert. Als Einstieg kann sie die benutzerdefinierte Anwendungsvorlage hinzufügen, um neue SAML- oder Open ID Connect-Anwendungen zu integrieren.

Weiter:
Anmeldungseinstellungen konfigurieren

IBM Security Verify

Applications

Total applications24

Enabled24

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

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 Kitemworks

A platform for secure file access and sharing

Accredible

A Platform as a Service

Active Directory

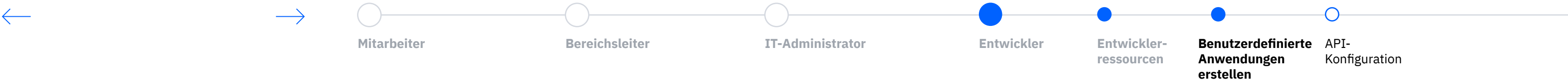
Active Directory (AD) is a directory service for Windows domain networks.

Adobe Captivate Prime

A learning management system

Cancel

Add application



Entwickler: 2 von 4
Benutzerdefinierte Anwendungen erstellen

Anmeldungs-einstellungen konfigurieren

In der Anwendungsvorlage werden Schritt-für-Schritt-Anleitungen zur Integration der Anwendung bereitgestellt.

Weiter:
Bereitstellung konfigurieren

IBM Security Verify

?

Alice Chains

Add Application



Custom Application

General

Sign-on

Account lifecycle

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.

- Log in to the third-party application administration console with your administrator user account.
- 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:

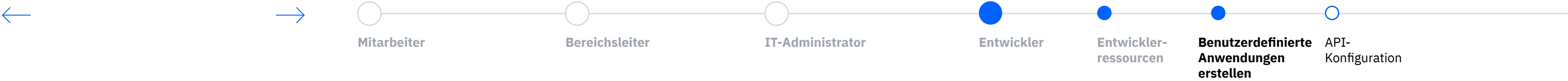
https://customer.verify.ibm.com/saml/sps/saml20ip/saml20/cc7fcb85562e4fc3

Login URL

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

Cancel

Save



Entwickler: 3 von 4

Benutzerdefinierte Anwendungen erstellen

Bereitstellung konfigurieren

Sie kann auch automatische Bereitstellung und Löschung für die Anwendung mit SCIM aktivieren.

Weiter:

Softwarefehler beheben

IBM Security Verify

?

Alice Chains

Add 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.

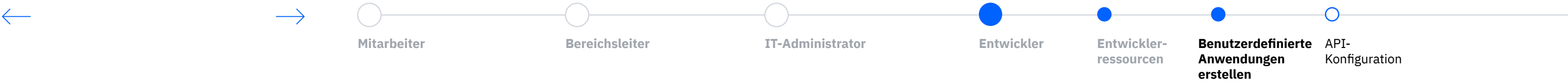
3. Provide the value for **Bearer Token** for your application.

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



Entwickler: 4 von 4
Benutzerdefinierte Anwendungen erstellen

Softwarefehler beheben

Alice kann die Leistung ihrer Anwendung überwachen und die Details von Authentifizierungsereignissen auswerten, um Fehler zu beheben.

Weiter:
API-Clients hinzufügen

IBM Security Verify

Application usage

Application usage details from April 27, 2020 to May 12, 2020

All applications

from 04/27/2020 To 05/12/2020

All activity

Login counts

Filters

Successful logins 8

Failed logins 0

Successful logins

04/28/2020 04/30/2020 05/01/2020

0 1 2 3 4 5

Application	User Name	Realn
Box	scott	cloud
Atlassian	alice	cloud
Atlassian	alice	cloud
Box	jessica@banedox.com	cloudIdentityRealm

SAML assertion

```
1 <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
2   ID="Assertion-uuid96d8555-0172-18db-947d-bf0c93b022da"
3   IssueInstant="2020-05-12T15:07:52Z"
4   Version="2.0"
5   xmlns:xs="http://www.w3.org/2001/XMLSchema"
6   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
7   <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">https://
8   <saml:Subject>
9     <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
10    <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
11      <saml:SubjectConfirmationData NotOnOrAfter="2020-05-12T15:08:52Z"
12        Recipient="https://sso.services.box.net/sp/ACS.saml2"/>
13    </saml:SubjectConfirmation>
14  </saml:Subject>
15  <saml:Conditions NotBefore="2020-05-12T15:06:52Z"
16    NotOnOrAfter="2020-05-12T15:08:52Z">
17    <saml:AudienceRestriction>
18      <saml:Audience>box.net</saml:Audience>
19    </saml:AudienceRestriction>
20  </saml:Conditions>
21  <saml:AuthnStatement AuthnInstant="2020-05-12T15:07:52Z"
22    SessionIndex="67824a39-dbe7-4e99-969e-75e9a5316271_uuid5bfa6bde-0167-18ed-
23    SessionNotOnOrAfter="2020-05-12T16:07:51Z">
24    <saml:AuthnContext>
25      <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Pass
26    </saml:AuthnContext>
27  </saml:AuthnStatement>
28  <saml:AttributeStatement>
29    <saml:Attribute Name="groups"
30      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
31      <saml:AttributeValue xsi:type="xs:string">allUsers</saml:AttributeValu
32      <saml:AttributeValue xsi:type="xs:string">admin</saml:AttributeValue>
33      <saml:AttributeValue xsi:type="xs:string">application owners</saml:Att
```

Download as .xml

Done

SAML assertion

Attributes sent

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



Entwickler: 1 von 2
API-Konfiguration

API-Clients hinzufügen

Alice kann aus einer Vielzahl von API-Clients wählen, die sie in ihre Anwendungen integrieren möchte.

Weiter:
Stellvertreterverwaltung

IBM Security Verify

?

Scott Damon

Configuration

API access

Attributes

Certificates

Customization

Identity

API clients

Allowed domains

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

☐	Name	↑	Client ID
☐	AgentConfig		96653cf7-8913-45e
☐	All_Allowed_Access		d6136ee7-fdd9-49f
☐	ISAM API		26de2c30-22fa-41f
☐	Access session token		7b863522-bf92-41f
☐	Registration		ed298b2a-bdc3-4f1
☐	Self-Service		6792d60d-b4b1-41f

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

Access

Authenticate any user, + 52 more

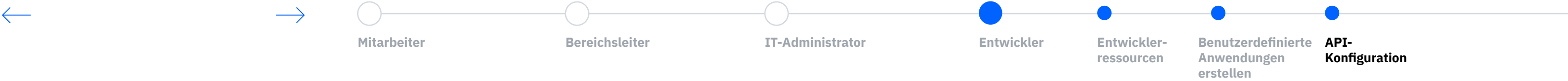
Authenticate any user, + 53 more

Authenticate any user, + 6 more

Authenticate any user, + 52 more

Authenticate any user, + 43 more

Authenticate any user, + 40 more



Entwickler: 2 von 2

API-Konfiguration

Stellvertreterverwaltung

Sie kann ihrer Anwendung auch die Erlaubnis erteilen, bestimmte API-Berechtigung aufzurufen, die den Zugriffstoken zugewiesen sind.

Informieren Sie sich über:
IBM Security Verify

IBM Security Verify

?

Alice Chains

Applications / Details



Developer App

General

Sign-on

API access

Account lifecycle

Entitlements

☒ 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

Delete

Cancel

Save



© Copyright IBM Corporation 2021

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Hergestellt in den USA
Februar 2021

IBM, das IBM Logo und ibm.com sind eingetragene Marken der International Business Machines Corporation in den USA und/oder anderen Ländern. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Unternehmen sein. Die aktuelle Liste der IBM Marken finden Sie auf der Webseite „Copyright and trademark information“ unter ibm.com/legal/copytrade.shtml.

Dieses Dokument ist zum Datum seiner Erstveröffentlichung aktuell und kann jederzeit von IBM geändert werden. Nicht alle IBM Angebote sind in jedem Land, in welchem IBM tätig ist, verfügbar. Leistungsdaten und Kundenbeispiele dienen nur zur Veranschaulichung. Die tatsächlichen Leistungsergebnisse können je nach spezifischen Konfigurationen und Betriebsbedingungen variieren.

Die Informationen in diesem Dokument werden auf der Grundlage des gegenwärtigen Zustands (auf „as-is“-Basis) ohne jegliche ausdrückliche oder stillschweigende Gewährleistung zur Verfügung gestellt, einschließlich, aber nicht beschränkt auf die Gewährleistungen für die Handelsüblichkeit, die Verwendungsfähigkeit für einen bestimmten Zweck oder die Freiheit von Rechten Dritter.

Für IBM Produkte gelten die Gewährleistungen, die in den Vereinbarungen vorgesehen sind, unter denen sie erworben werden. Der Kunde ist für die Einhaltung der maßgeblichen Gesetze und Vorschriften selbst verantwortlich. IBM erteilt keine Rechtsberatung und gibt keine Garantie bzw. Gewährleistung bezüglich der Konformität von IBM Produkten oder Services mit den geltenden Gesetzen oder gesetzlichen Bestimmungen. Jegliche Erklärungen bezüglich der Produktstrategien und Absichtserklärungen von IBM stellen die gegenwärtige Absicht von IBM dar, unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

00000000USEN