IBM Security Verify Produkttour

Beginnen Sie Ihre Tour →

IBM **Security** Verify

Versuchen Sie Verify jetzt

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

1. **Mitarbeiter**
2. Single Sign-on
3. Anwendungszugriff anfordern
4. MFA registrieren und verwenden
5. **Bereichsleiter**
6. **IT-Administrator**
7. **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.

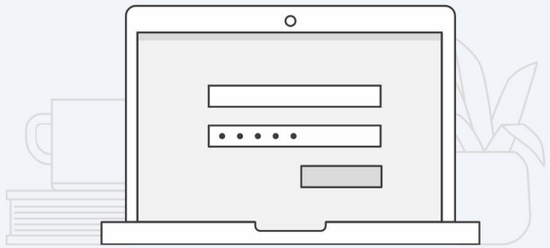
Mitarbeiter brauchen Schnellzugriff auf die Tools, die sie für ihre Arbeit benötigen, ohne sich durch Dutzende von Berechtigungsnachweisen belastet zu fühlen. Trotz hoher Erwartungen an die Unternehmenssicherheit, können sich IT-Richtlinien immer noch wie ein Hindernis anfühlen. Mitarbeiter wollen effizient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

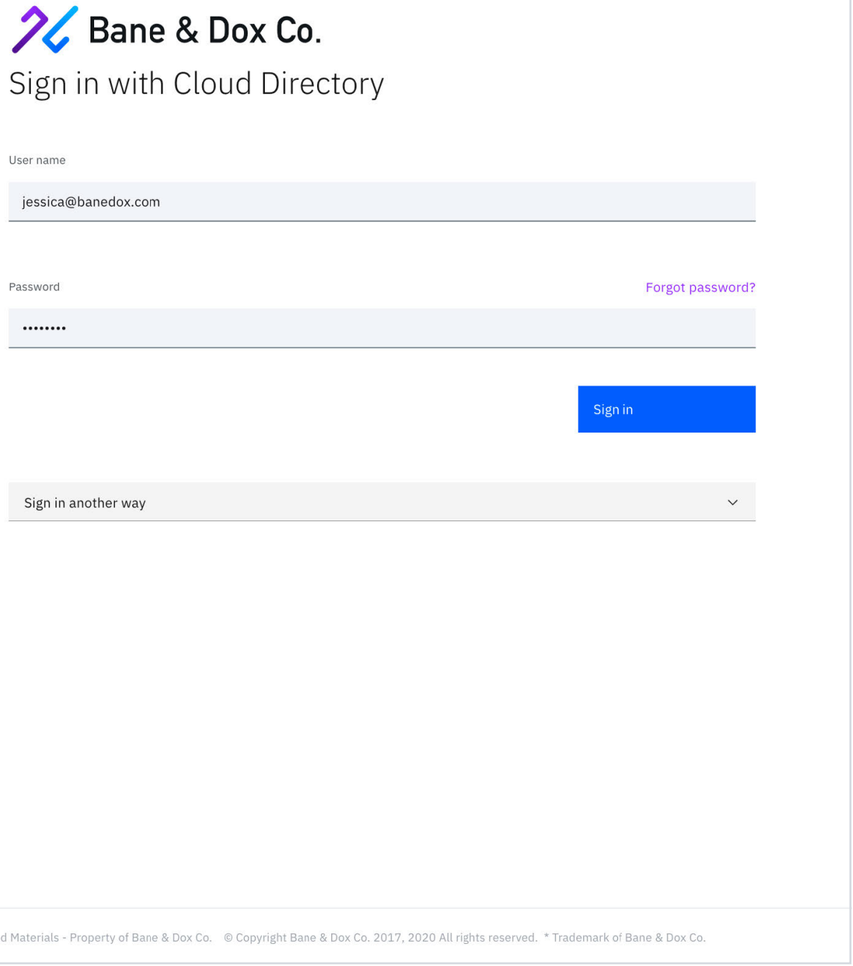
- **Mitarbeiter**
- Single Sign-on
  - Markenspezifische Anmeldeseite
  - Zugriff auf Apps mit einem Klick
- Anwendungszugriff anfordern
  - Katalog durchsuchen
  - Begründung erstellen
  - Offene Anfragen
  - Neue App in der Klickstartleiste
- MFA registrieren und verwenden
  - Neues Authentifizierungsgerät 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

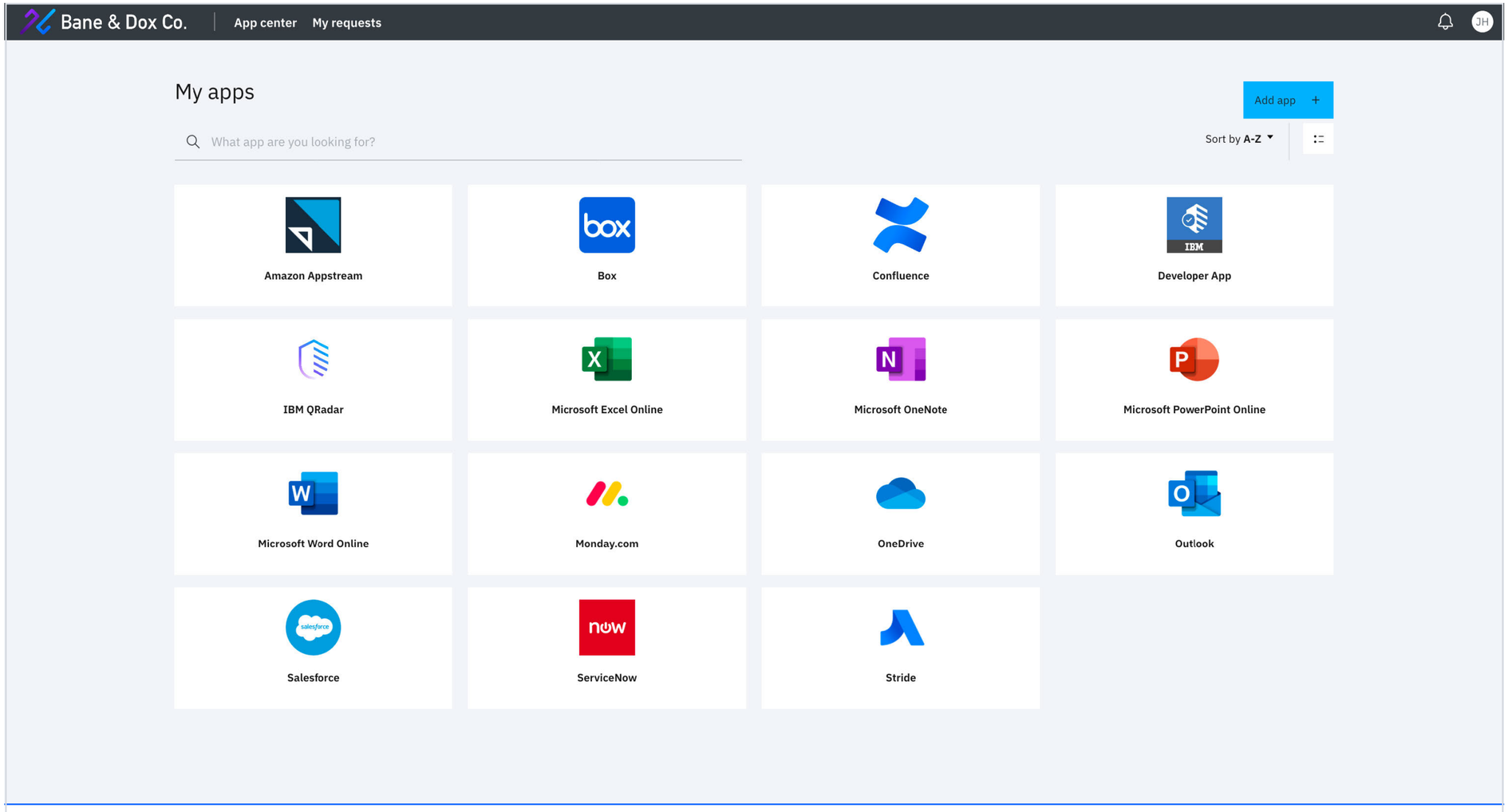
Mitarbeiter
Single Sign-on
Anwendungszugriff anfordern
MFA registrieren und verwenden
Bereichsleiter
IT-Administrator
Entwickler

Zurück
Weiter

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

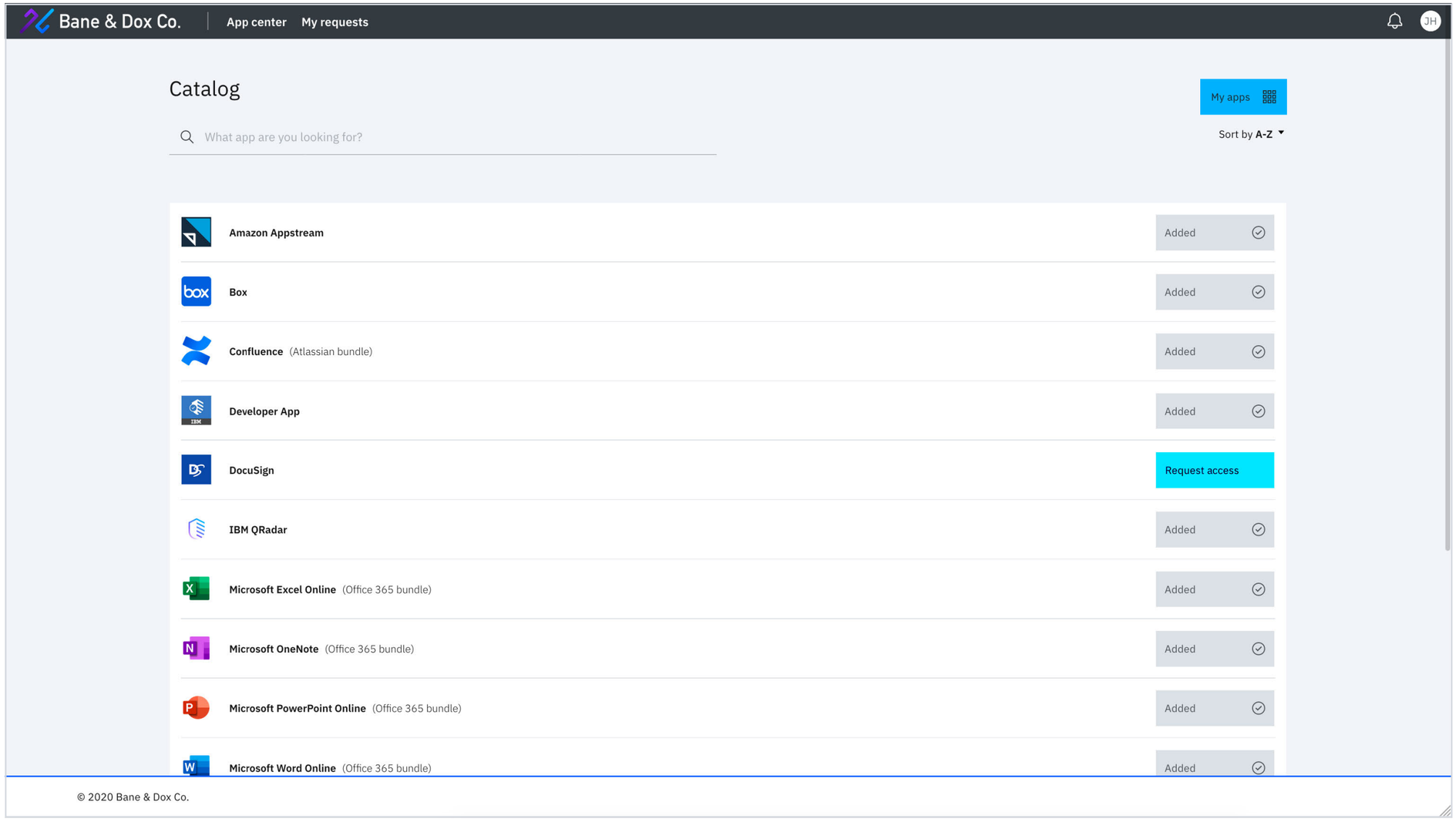
Mitarbeiter | **Single Sign-on** | Anwendungszugriff anfordern | MFA registrieren und verwenden | Bereichsleiter | IT-Administrator | Entwickler

Zurück | Weiter

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.

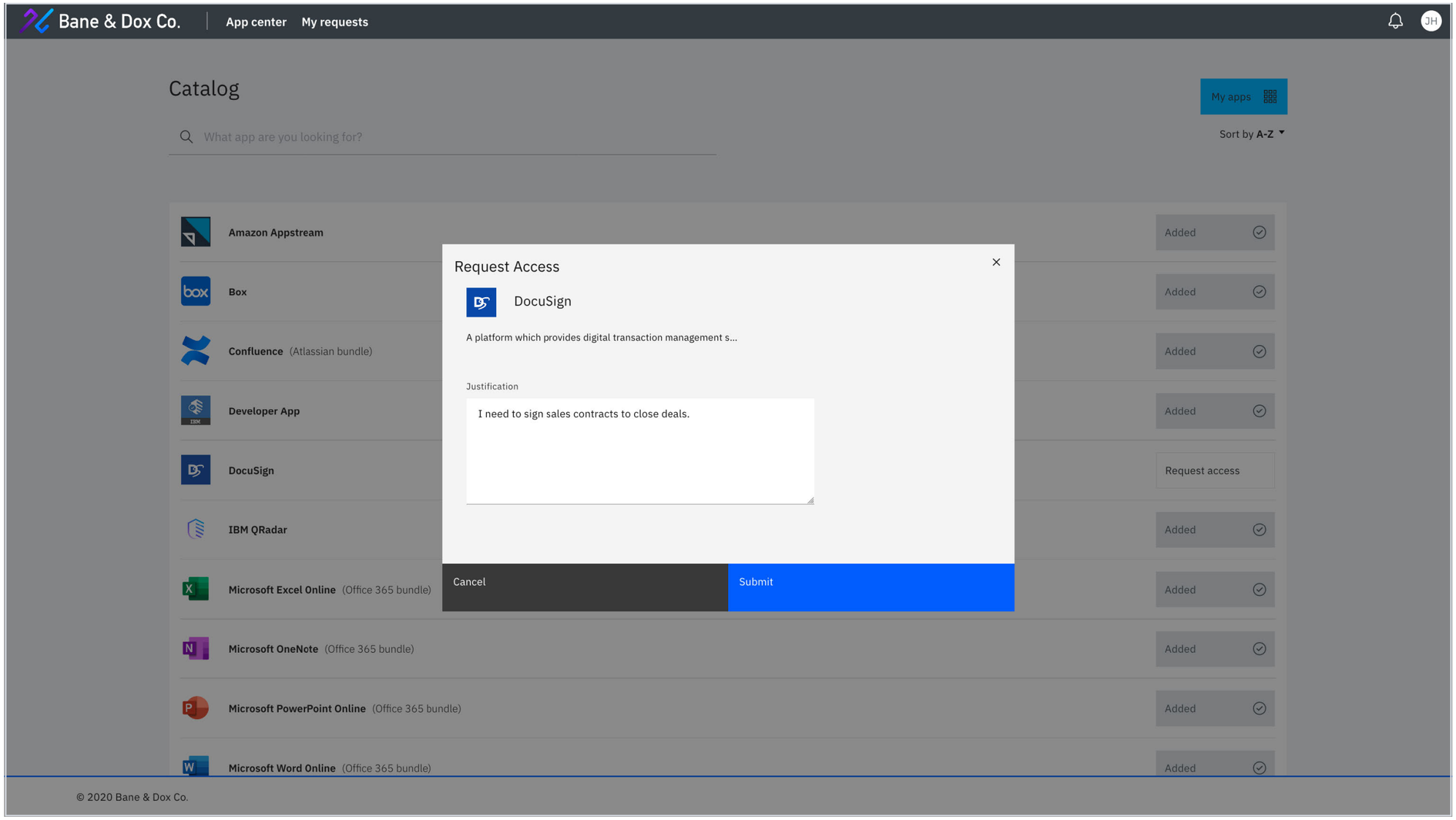


Weiter:
Begründung erstellen

Mitarbeiter: 2 von 4
Anwendungszugriff anfordern

Begründung erstellen

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



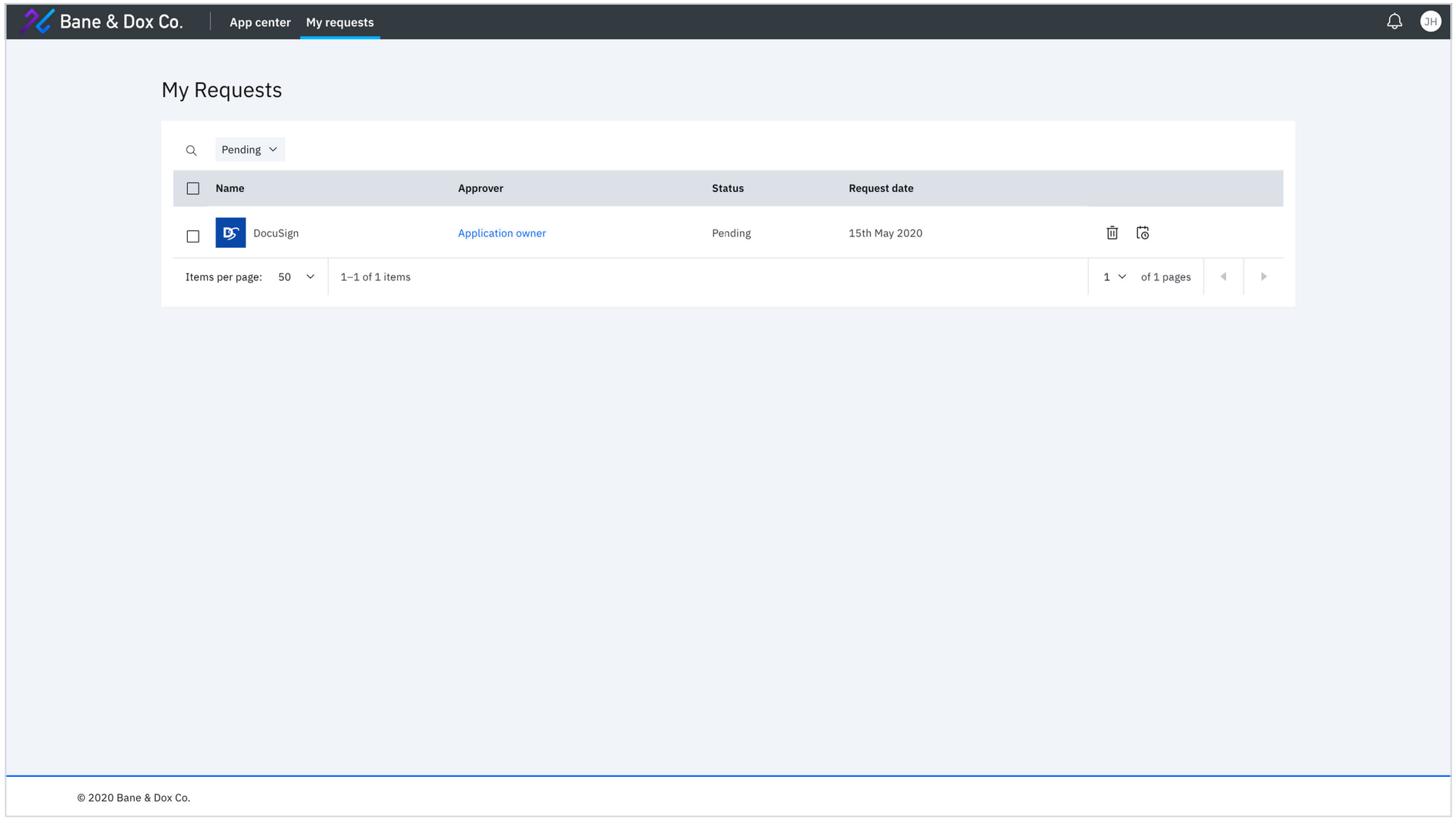
Weiter:
Offene Anfragen

Mitarbeiter
Single Sign-on
Anwendungszugriff anfordern
MFA registrieren und verwenden
Bereichsleiter
IT-Administrator
Entwickler

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.

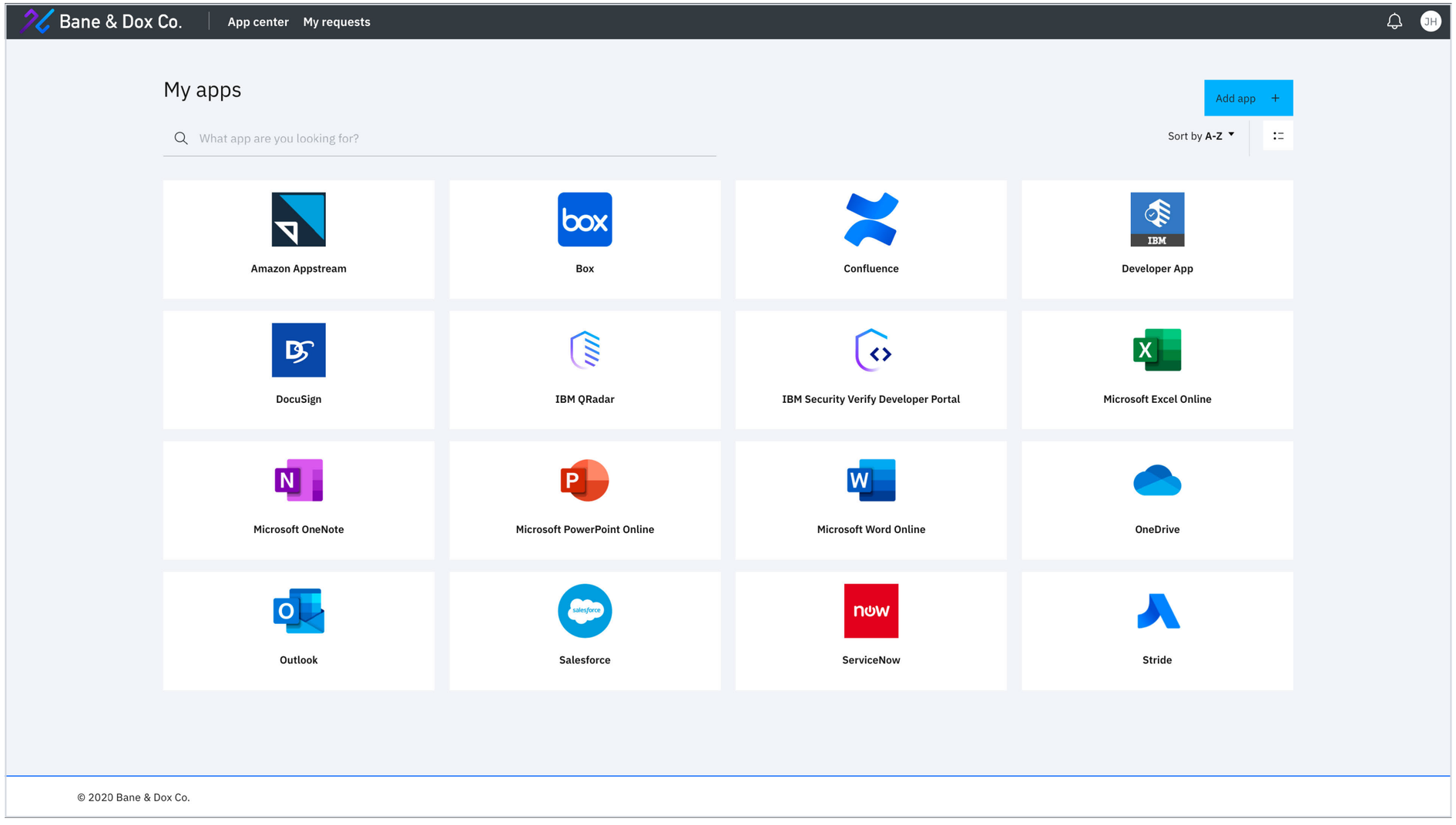


Weiter:
Neue App in der Klickstartleiste

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

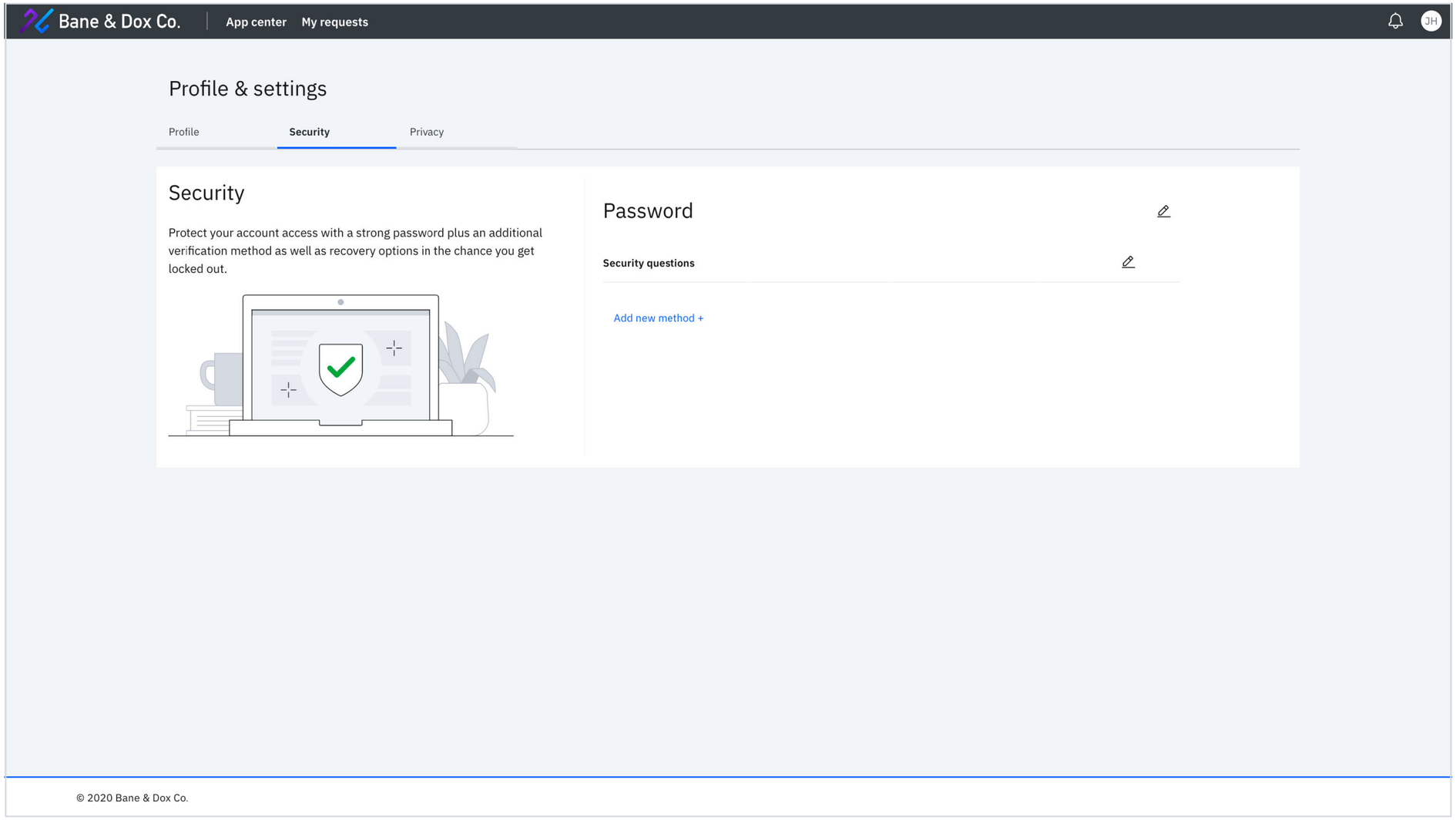
Mitarbeiter · Single Sign-on · **Anwendungszugriff anfordern** · MFA registrieren und verwenden · Bereichsleiter · IT-Administrator · Entwickler

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

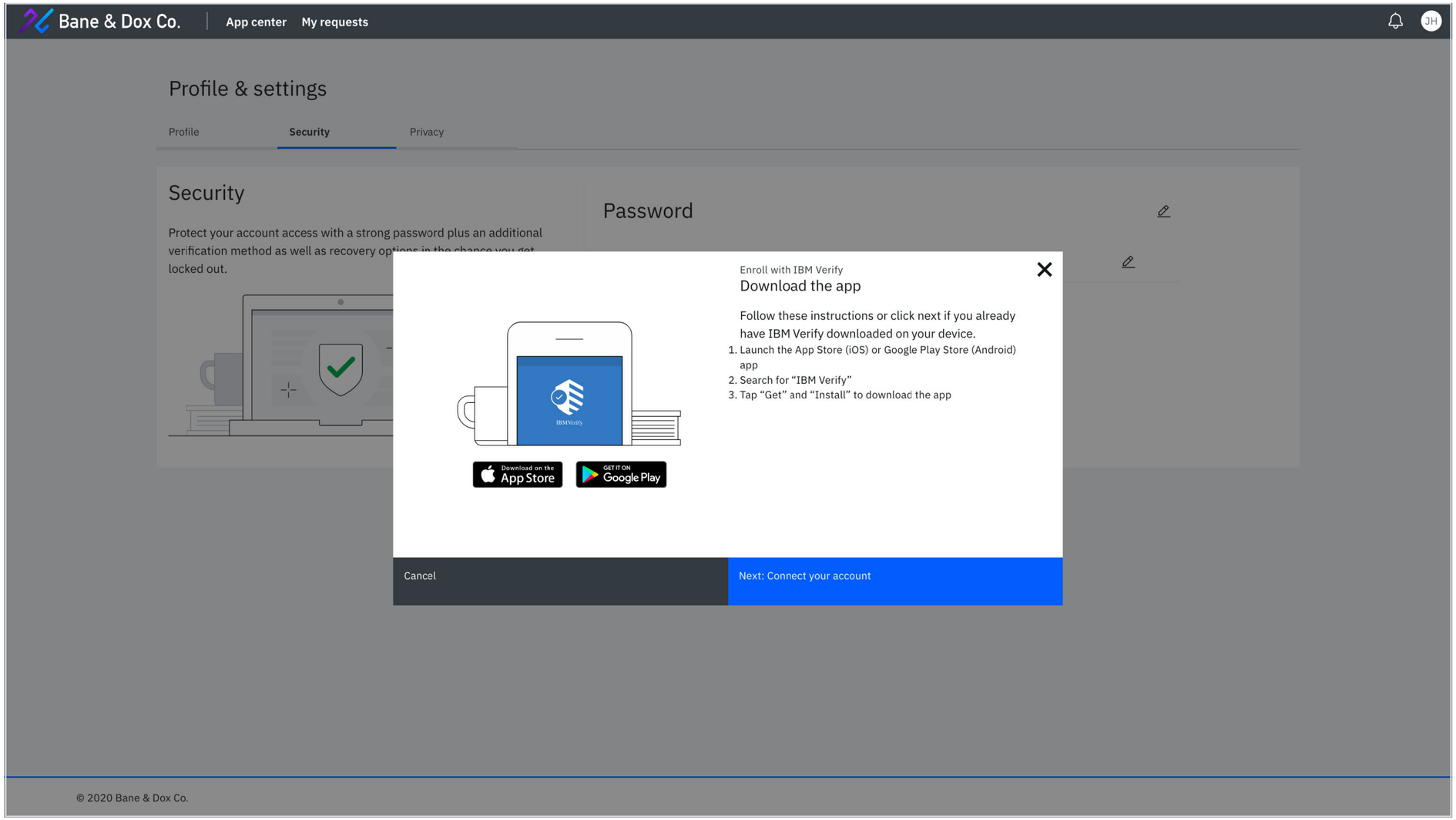
Mitarbeiter
Single Sign-on
Anwendungszugriff anfordern
MFA registrieren und verwenden
Bereichsleiter
IT-Administrator
Entwickler

Zurück
Weiter

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.

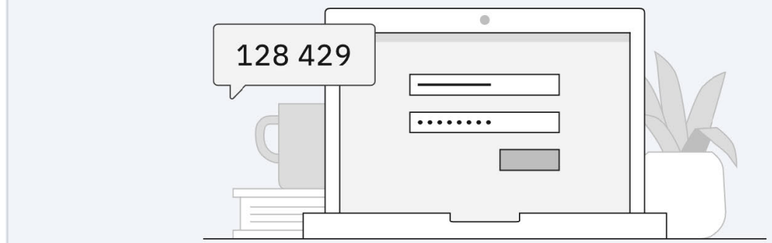


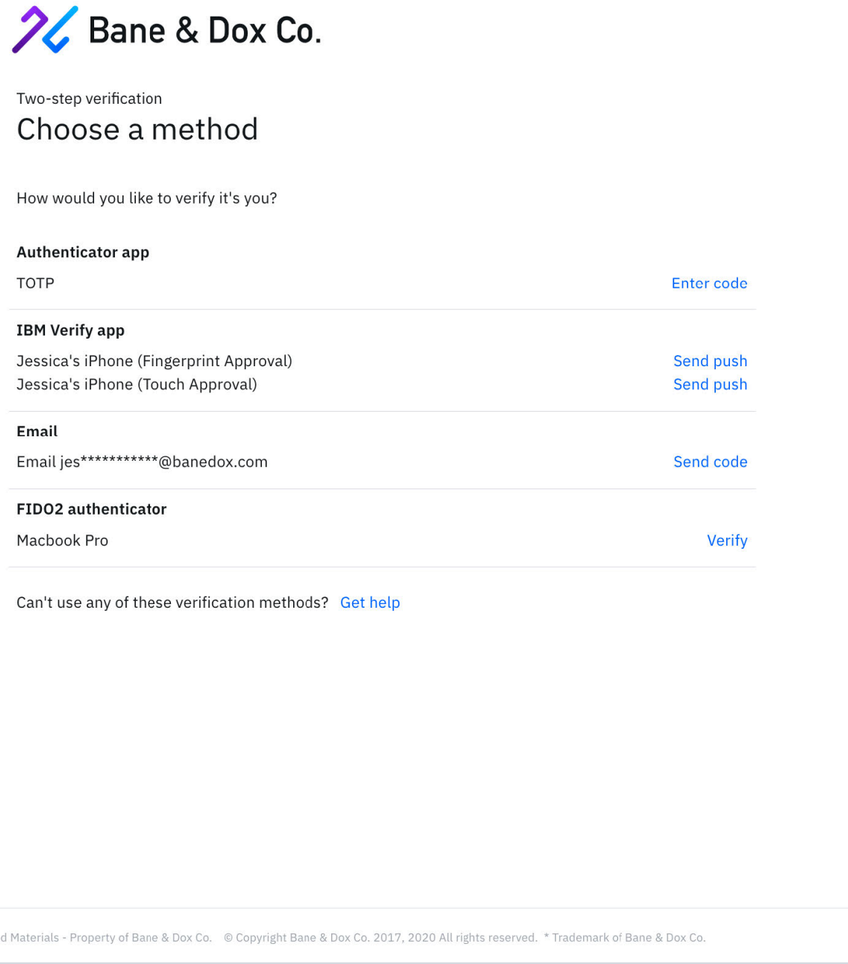
Weiter:
Wählen Sie die MFA Methode

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

Mitarbeiter
Single Sign-on
Anwendungszugriff anfordern
MFA registrieren und verwenden
Bereichsleiter
IT-Administrator
Entwickler

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

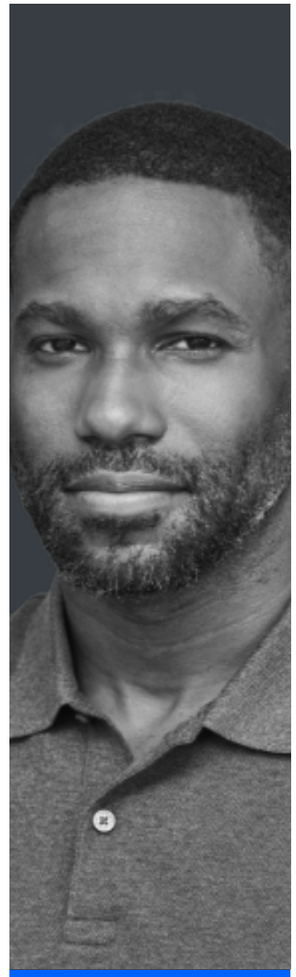
20 bis 50 % aller Anrufe beim IT-Helpdesk betreffen das Zurücksetzen von Kennwörtern

Weltwirtschaftsforum

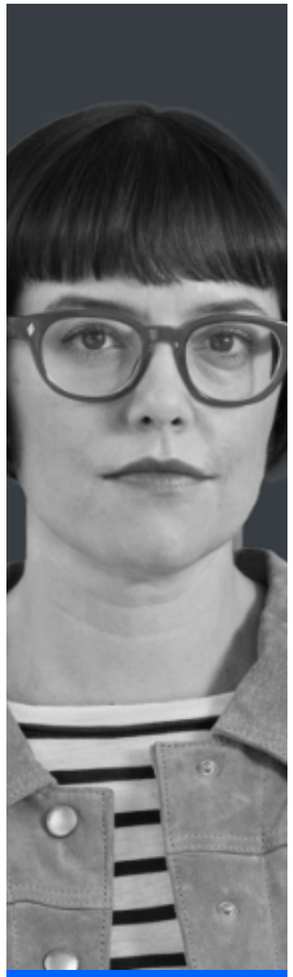
„Es ist wirklich frustrierend, von Tools und Systemen ausgebremst zu werden, wenn ich nur versuche, meine Arbeit zu erledigen.“

Jakob, Angestellter

Bereichsleiter



Anzeigen



Anzeigen

Mitarbeiter

Bereichsleiter

Zugriffsanfragen bearbeiten

IT-Administrator

Entwickler

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.

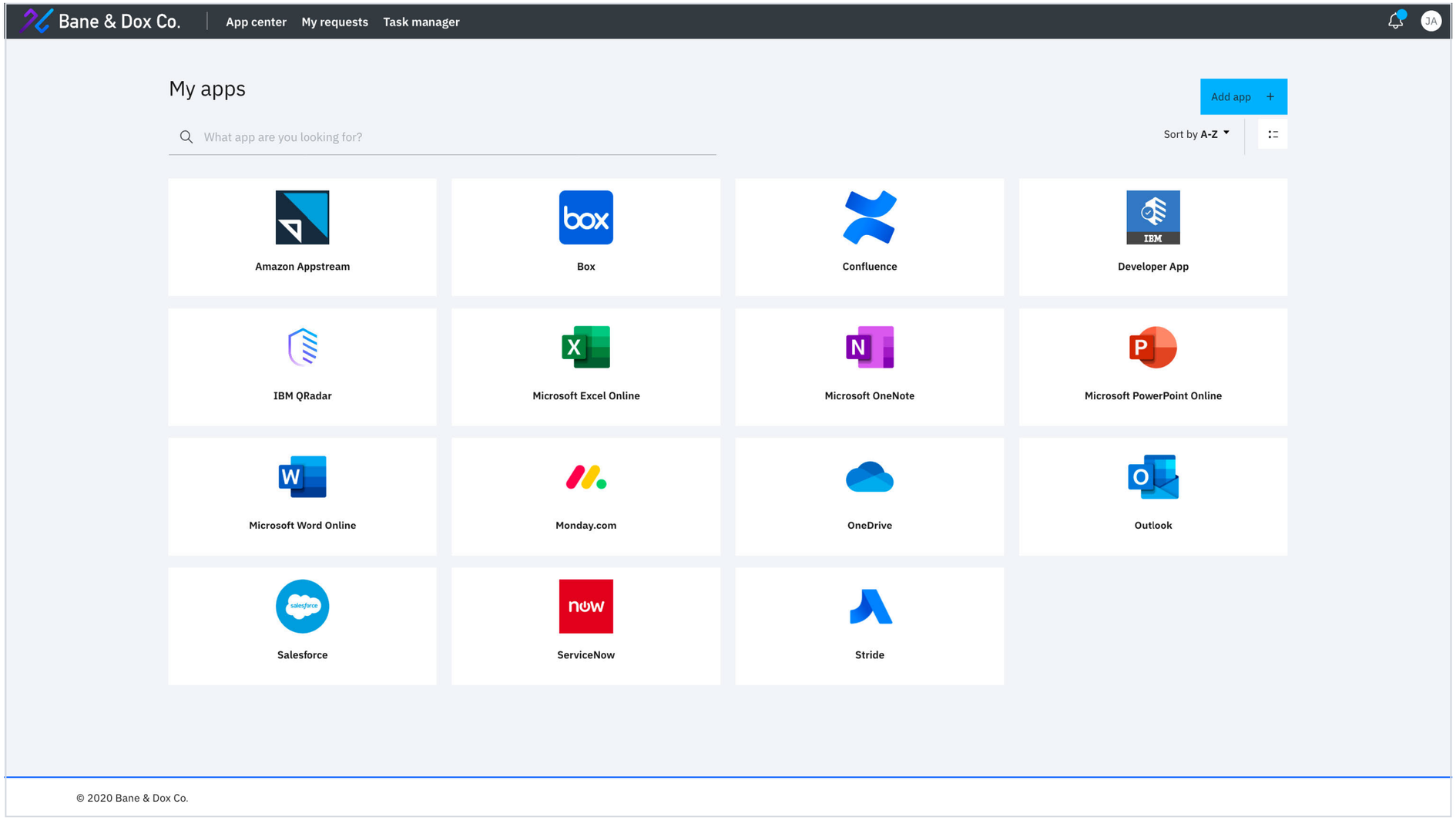
Bereichsleiter

- 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

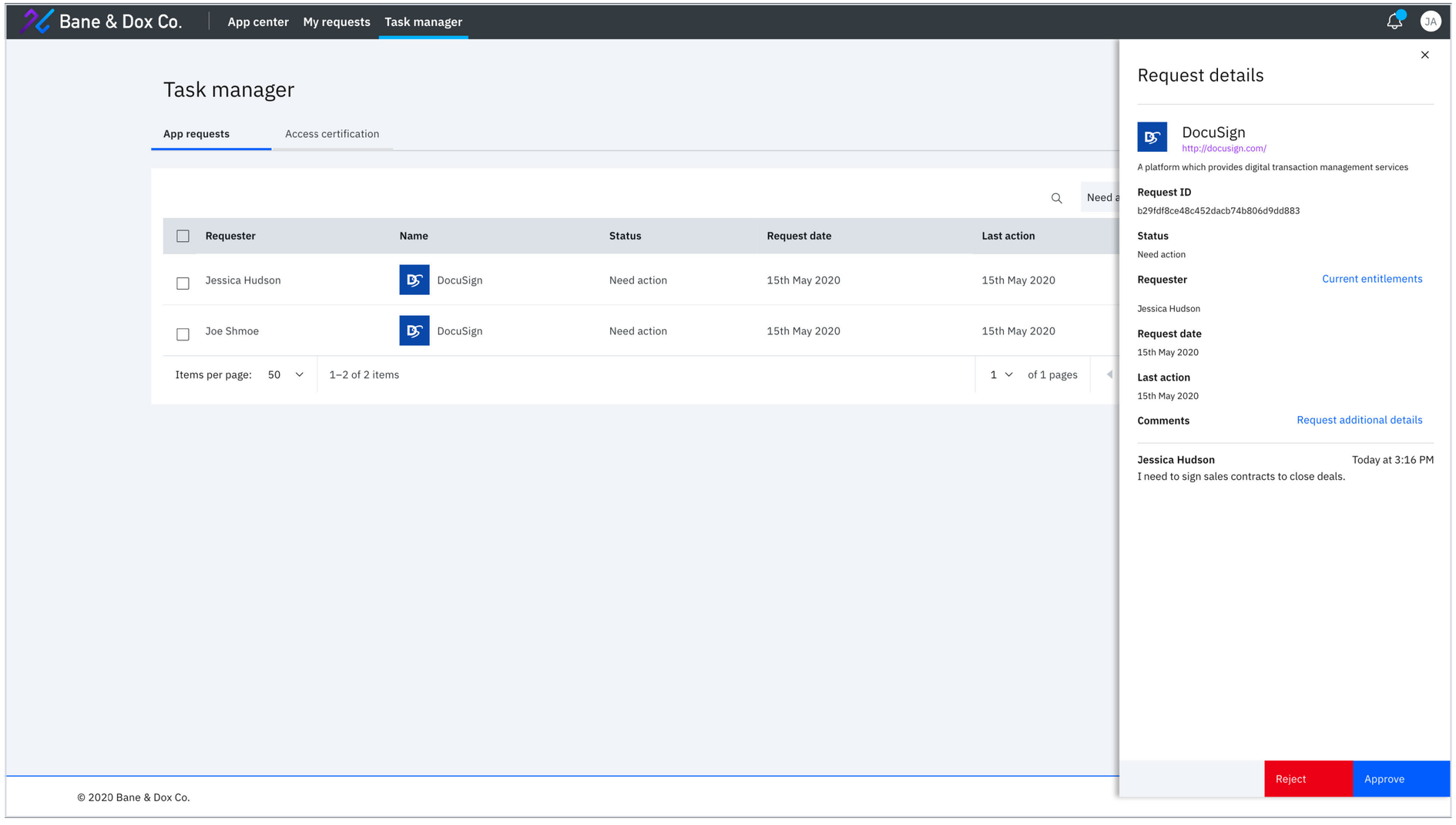
Mitarbeiter | Bereichsleiter | **Zugriffsanfragen bearbeiten** | IT-Administrator | Entwickler

Zurück | Weiter

Geschäftsbereichsmanager: 2 von 4
Zugriffsanfragen bearbeiten

Anfragedetails anzeigen

Auf der Registrierkarte Anfragen kann Jacob die Details von Jessicas Anfrage einsehen. Bei Bedarf kann er Jessica um zusätzliche Begründungen für ihre Anfrage bitten.



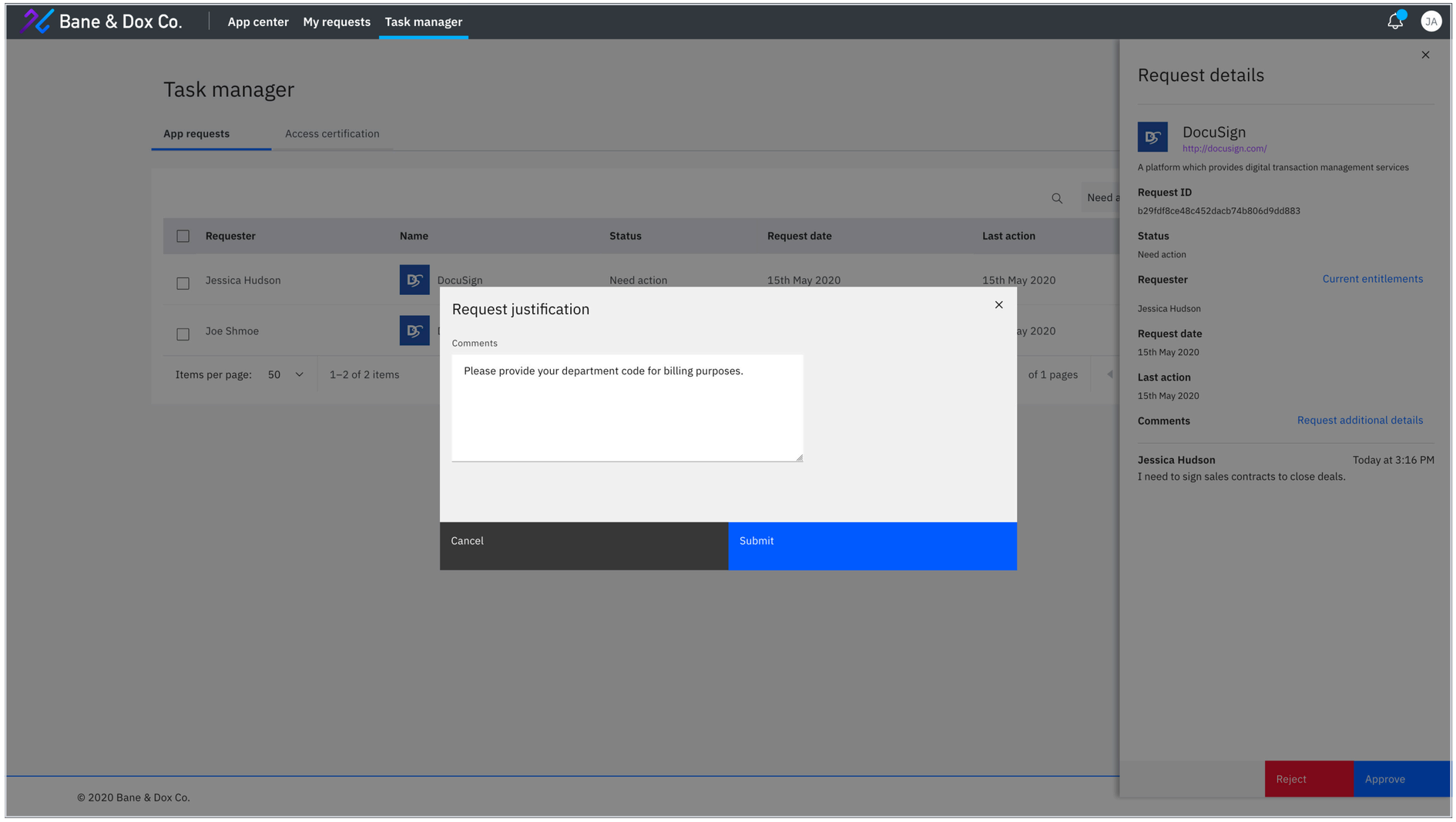
Weiter:
Zusätzliche Begründung anfordern

Mitarbeiter · Bereichsleiter · **Zugriffsanfragen bearbeiten** · IT-Administrator · Entwickler

Geschäftsbereichsmanager: 3 von 4
Zugriffsanfragen bearbeiten

Zusätzliche Begründung anfordern

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



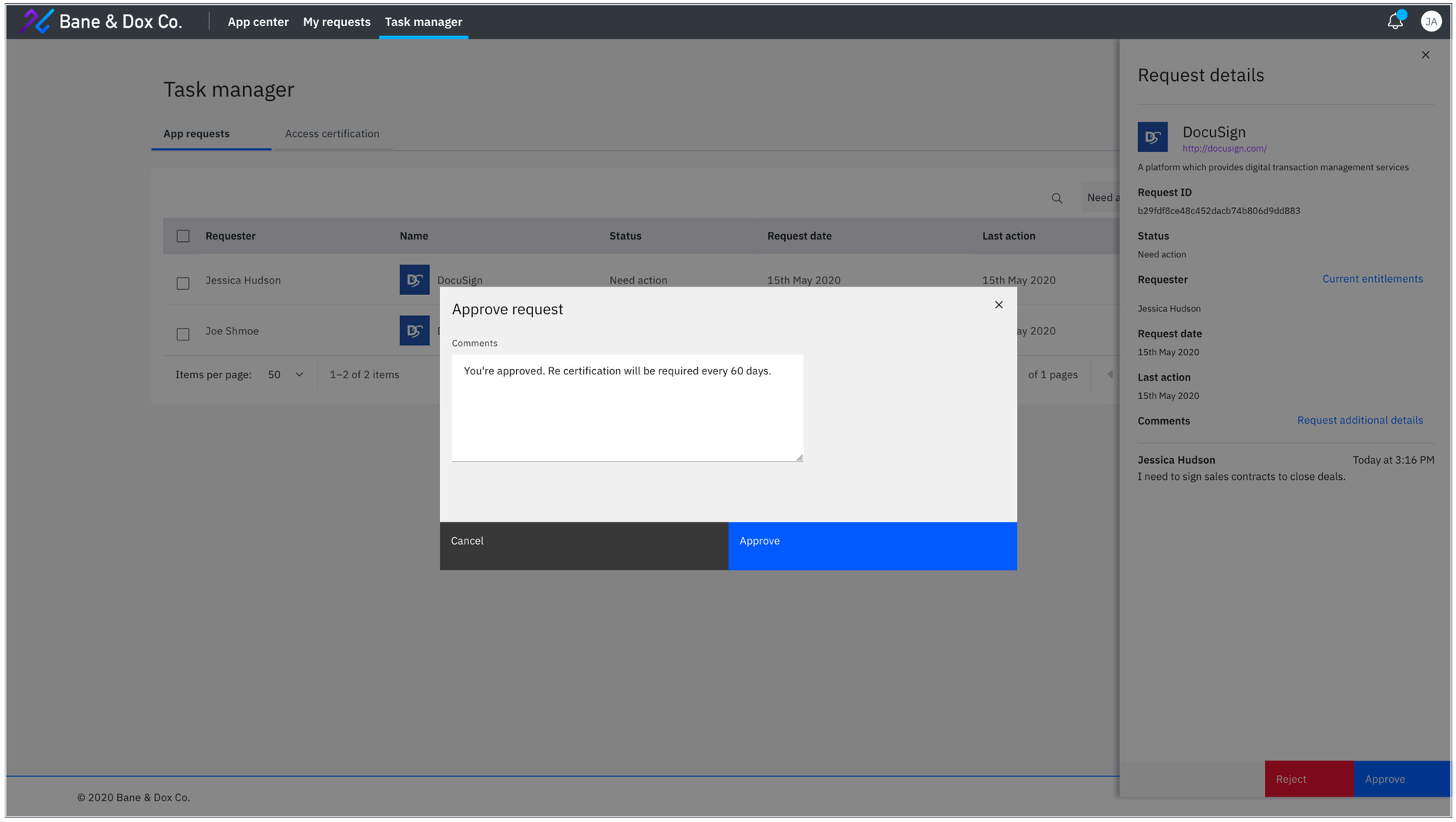
Weiter:
Anfrage genehmigen/ablehnen

Mitarbeiter
Bereichsleiter
Zugriffsanfragen bearbeiten
IT-Administrator
Entwickler

Geschäftsbereichsmanager: 4 von 4
Zugriffsanfragen bearbeiten

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

Mitarbeiter · Bereichsleiter · **Zugriffsanfragen bearbeiten** · IT-Administrator · Entwickler

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 %

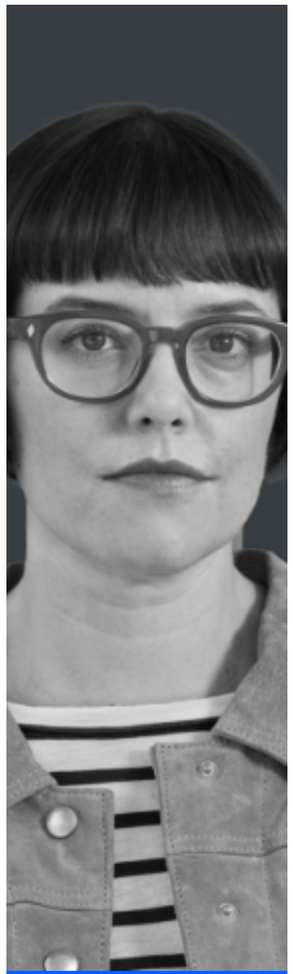
80 % der Hackerangriffe basieren auf kompromittierten und schwachen Berechtigungsnachweisen

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

Mitarbeiter · Bereichsleiter · **IT-Administrator** · Vorgang überwachen · Richtlinien anpassen · Benutzer und Identitäten verwalten · Anwendungen hinzufügen · Risiko analysieren · Entwickler

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.

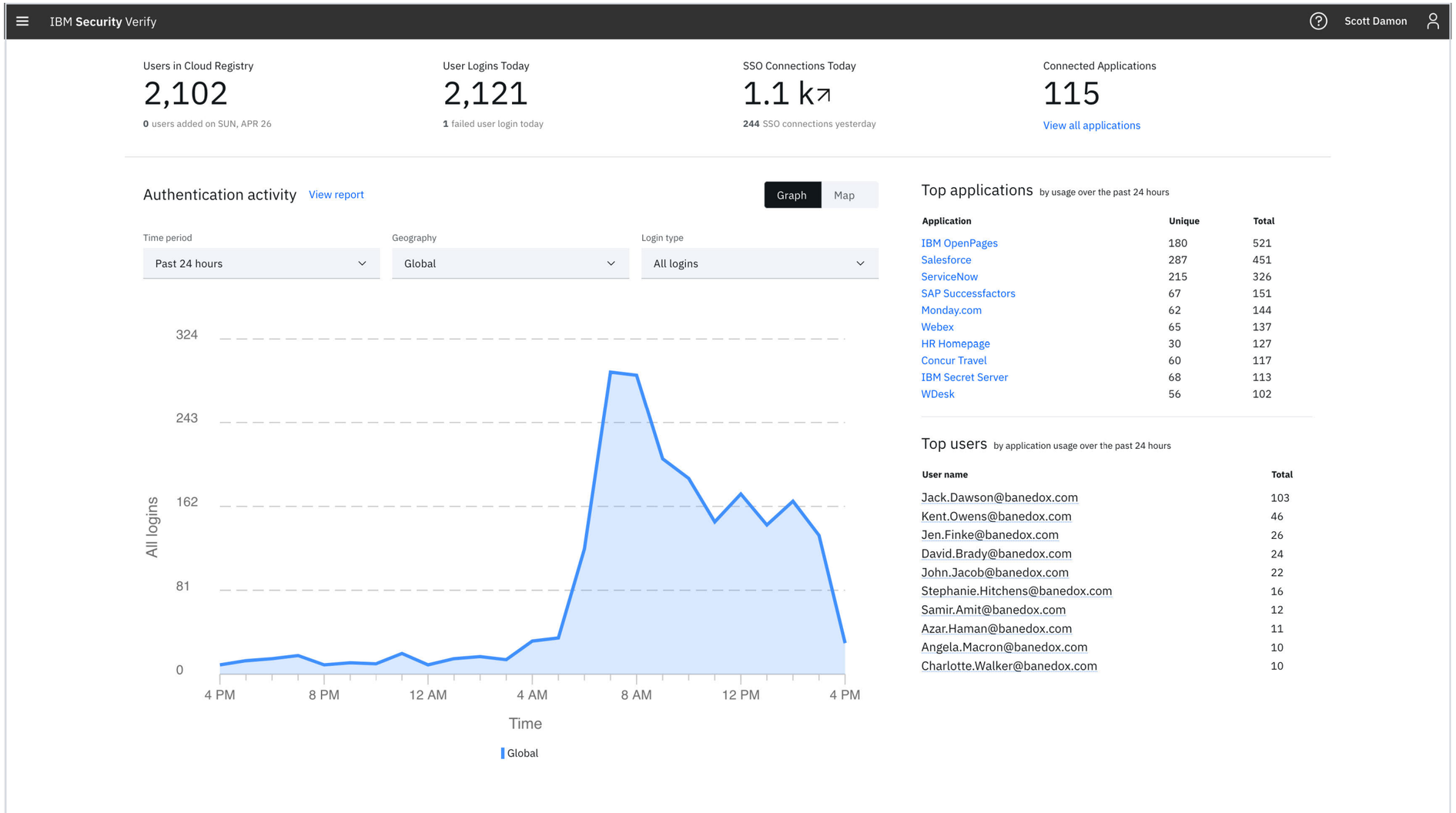
IT-Administrator

- Mitarbeiter
- Bereichsleiter
- **IT-Administrator**
  - Vorgang überwachen
    - Live-Anzeigefeld
    - Aktivitätsberichte erstellen
    - Aktivitätsbericht von Adaptive Access
  - Richtlinien anpassen
    - Richtlinieneditor
    - Regel zur Richtlinie hinzufügen
    - Adaptiver Zugriff
  - Benutzer und Identitäten verwalten
    - Management-Benutzer
    - Gruppen verwalten
    - Benutzerattribute verwalten
    - Active Directory und LDAP
    - Soziale Anmeldung
  - Anwendungen hinzufügen
    - Anwendungen anzeigen
    - Nach Anwendungen zum Hinzufügen suchen
    - Besitzer für Zugang hinzufügen Freigaben
    - Anmeldungseinstellungen konfigurieren
    - Berechtigungen konfigurieren
    - Regelmäßige erneute Zertifizierung des Zugangs festlegen
  - Risiko analysieren
    - Analyse melden
    - Eingestufte Richtlinienverstöße anzeigen
    - Ergreifen Sie vorgeschlagene Korrekturaktionen
- Entwickler

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.

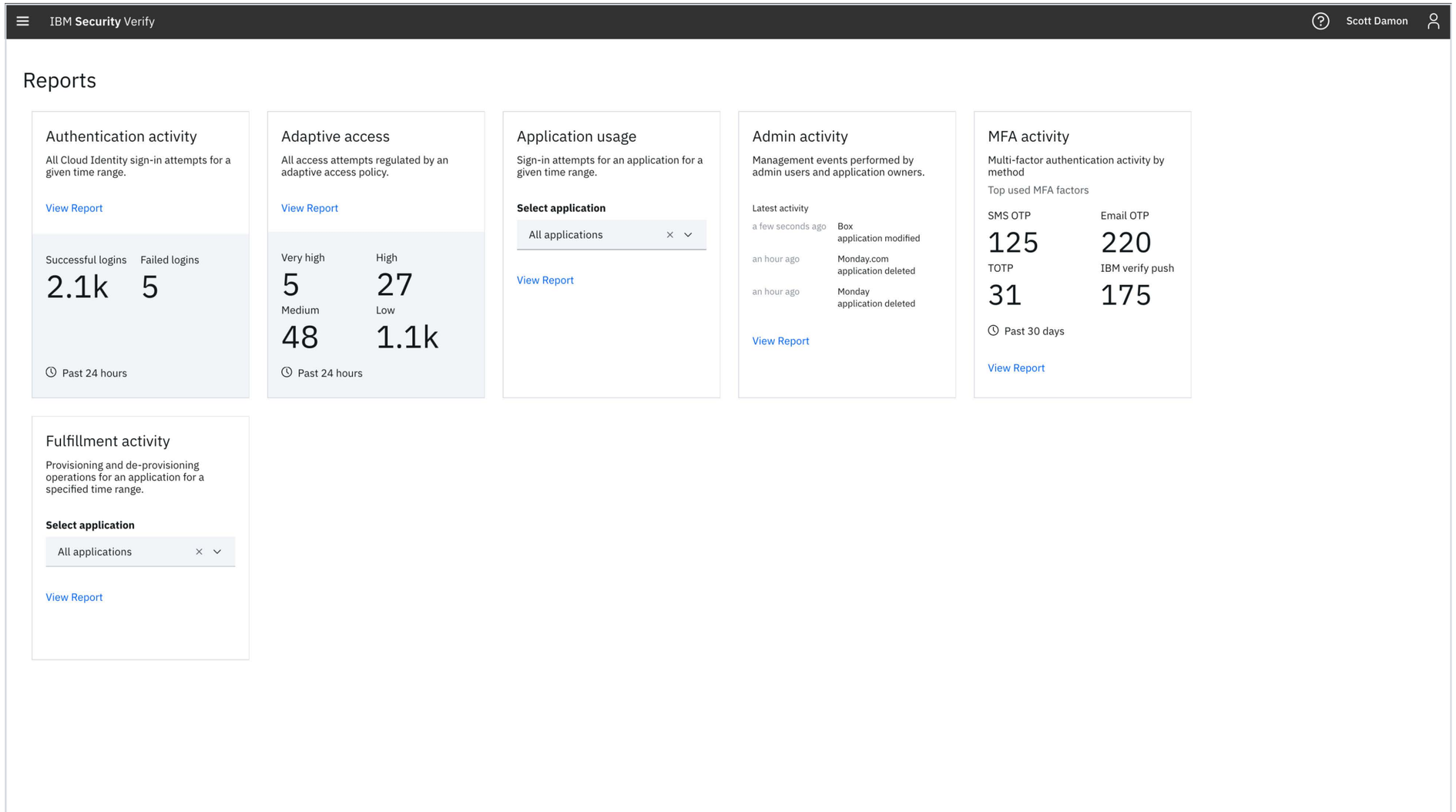


Weiter:
Aktivitätsberichte erstellen

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.



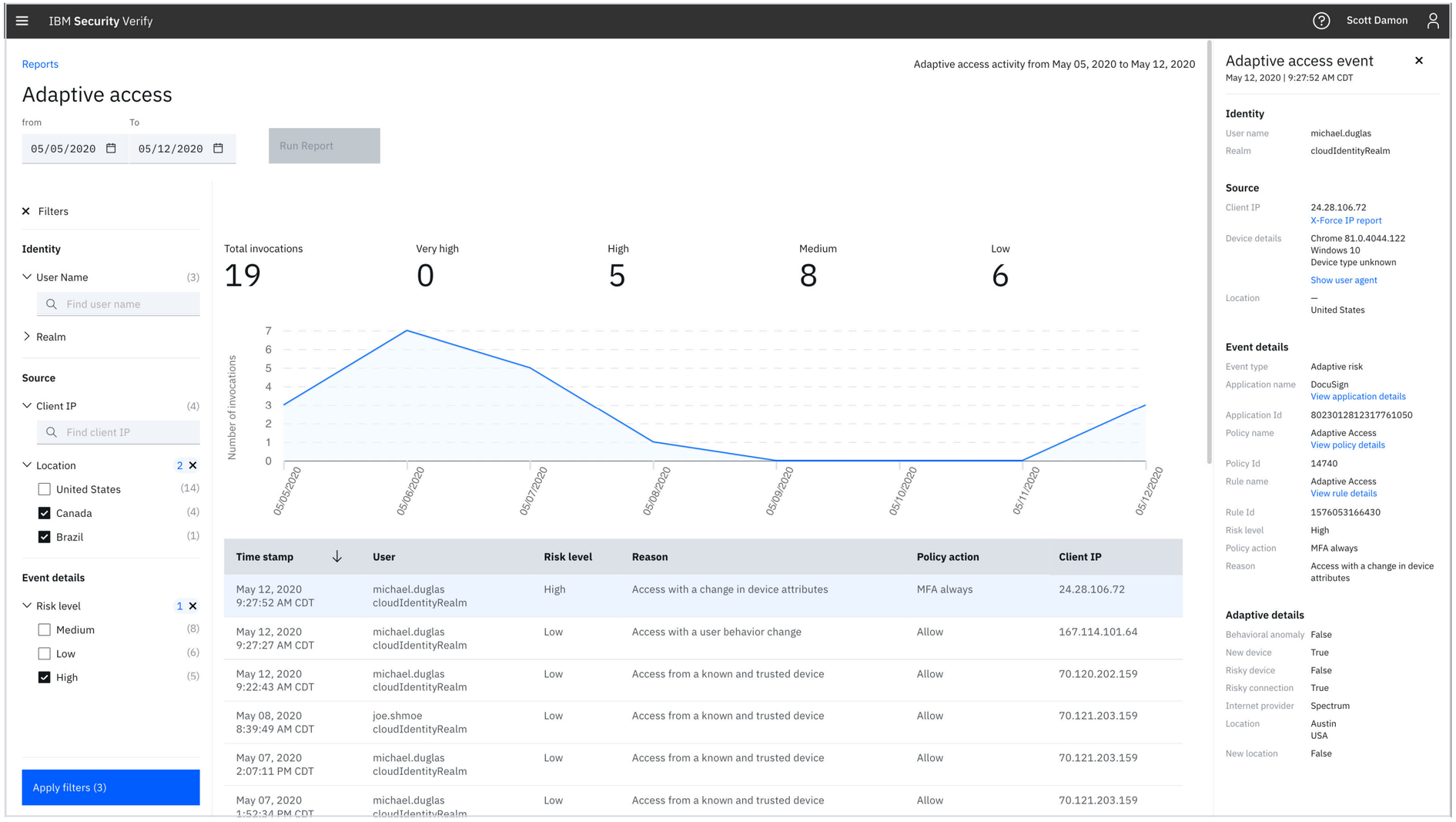
Weiter:
Aktivitätsberichte von Adaptive Access

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

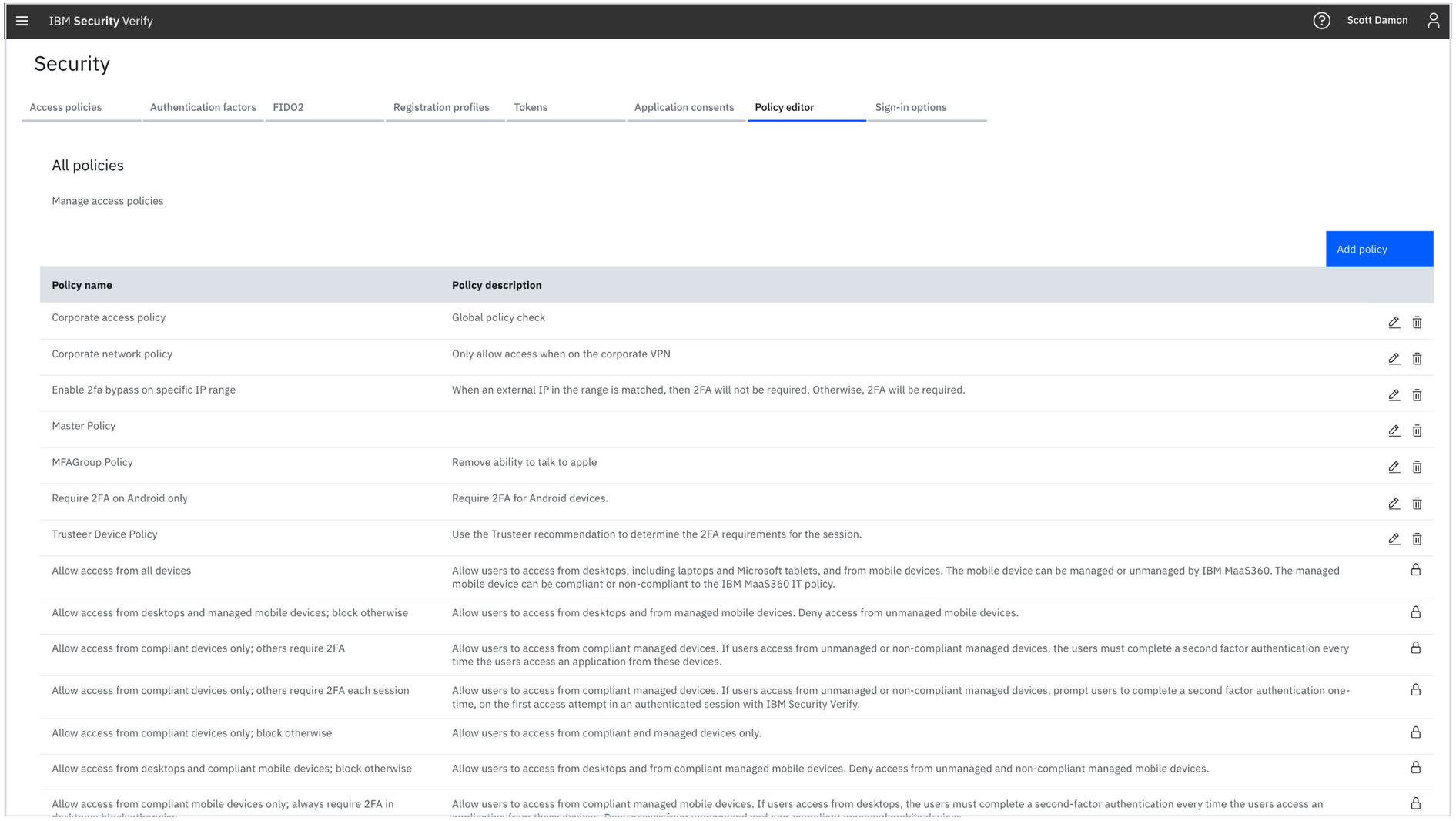
Mitarbeiter
Bereichsleiter
IT-Administrator
Überwachung Aktivität
Richtlinien anpassen
Benutzer und Identitäten verwalten
Anwendungen hinzufügen
Risiko analysieren
Entwickler

Zurück
Weiter

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

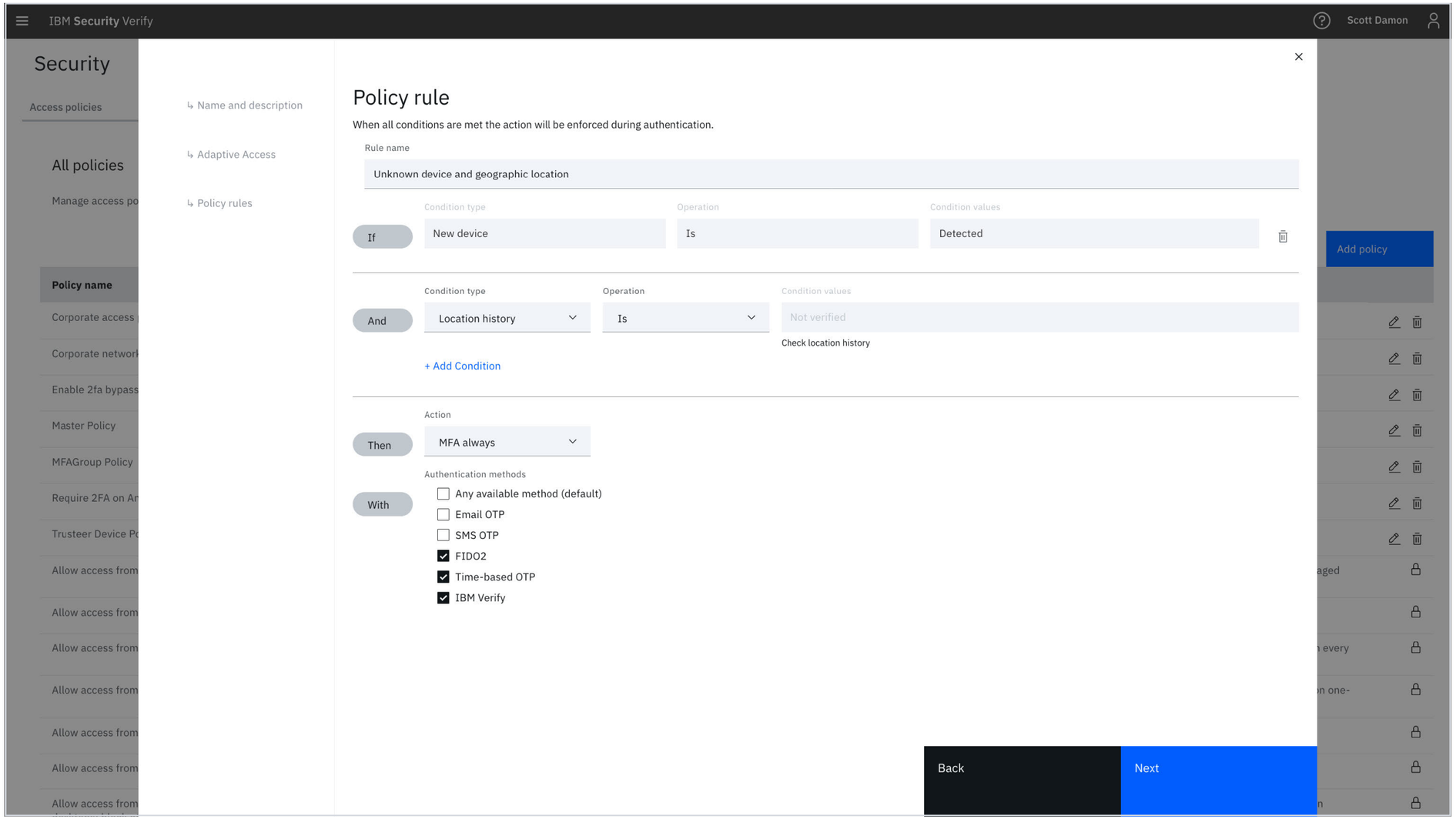
Mitarbeiter
Bereichsleiter
IT-Administrator
Überwachen Aktivität
Richtlinien anpassen
Benutzer und Identitäten verwalten
Anwendungen hinzufügen
Risiko analysieren
Entwickler

Zurück
Weiter

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

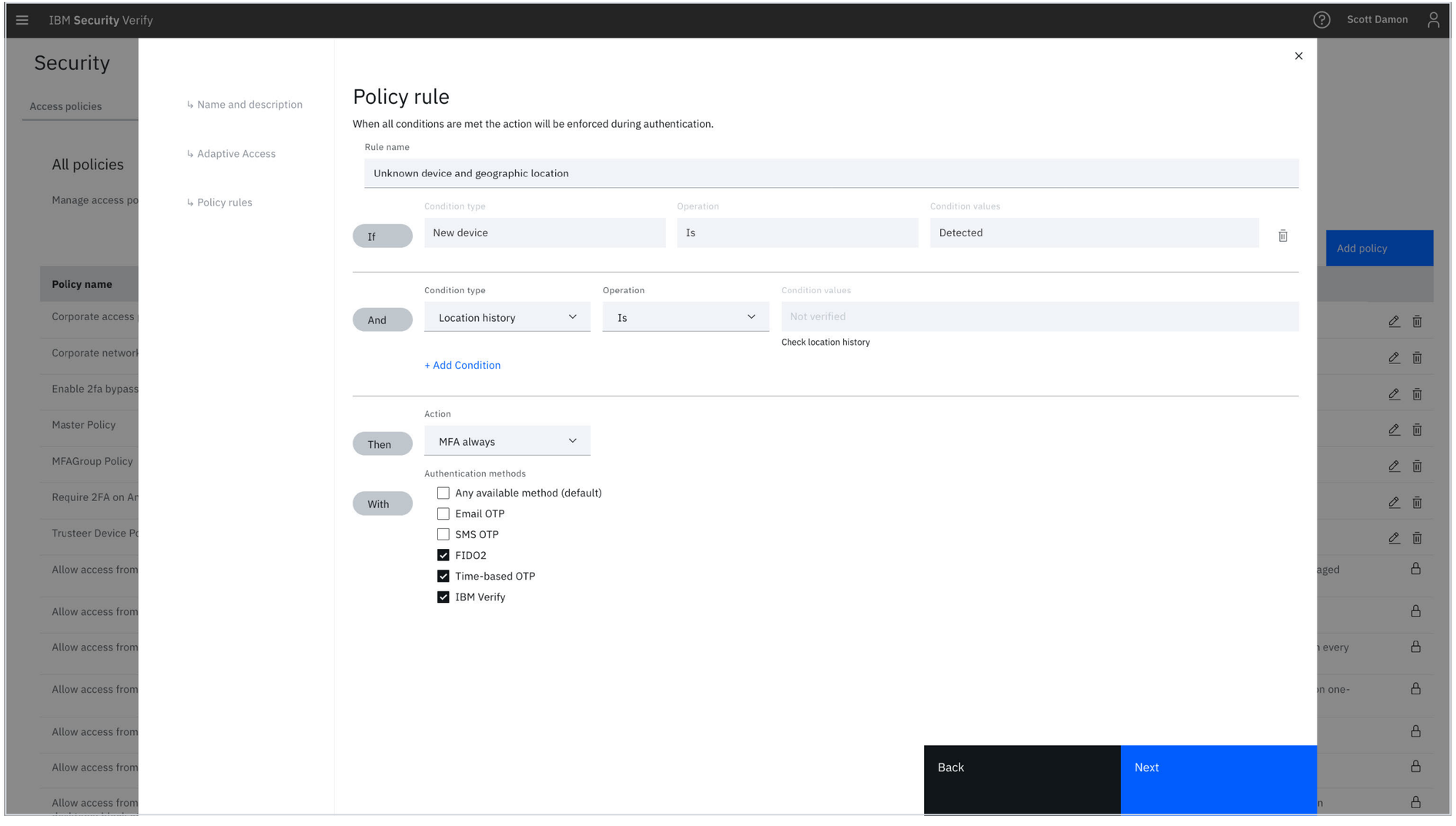
Mitarbeiter · Bereichsleiter · IT-Administrator · Vorgang überwachen · **Richtlinien anpassen** · Benutzer und Identitäten verwalten · Anwendungen hinzufügen · Risiko analysieren · Entwickler

IT-Administrator: 3 von 3
Richtlinien anpassen

Adaptiver Zugriff

Er kann sich auch dafür entscheiden, den Kontext von Benutzer, Gerät, Aktivität, Umgebung und Verhalten automatisch zu berücksichtigen, indem er die risikobasierte Authentifizierung über eine adaptive Zugriffsrichtlinie aktiviert. Adaptive Access bestimmt das Gesamtrisiko anhand einer Reihe von robusten, kontextbezogenen Parametern, die durch KI angetrieben werden. Durch kontinuierliche Authentifizierung erhalten Benutzer mit geringem Risiko einen reibungslosen Zugriff, während Benutzer mit höherem Risiko automatisch abgefragt oder geblockt werden.

Adaptive Access Interaktive Demo



Weiter:
Management-Benutzer

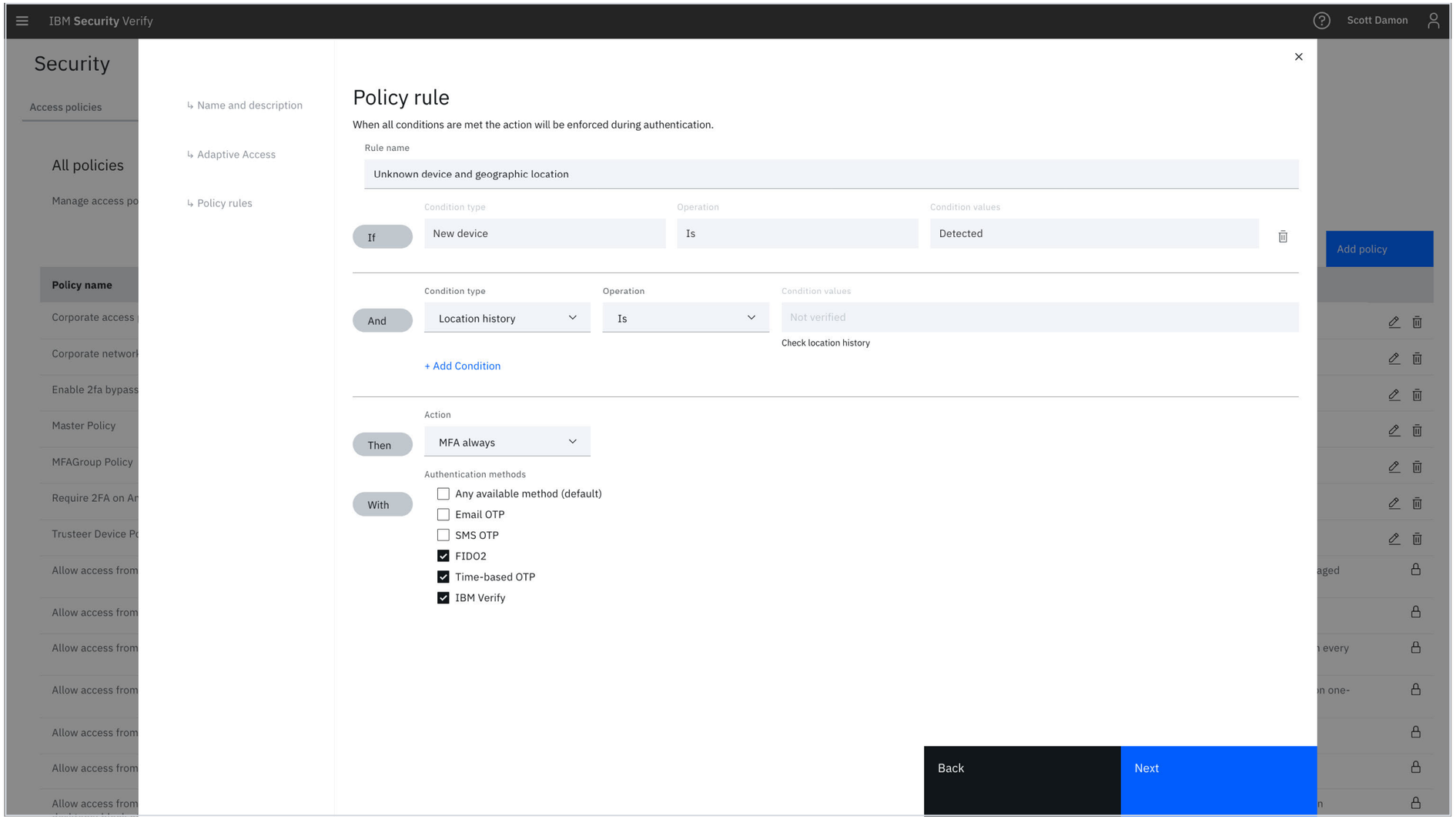
Mitarbeiter
Bereichsleiter
IT-Administrator
Vorgang überwachen
Richtlinien anpassen
Benutzer und Identitäten verwalten
Anwendungen hinzufügen
Risiko analysieren
Entwickler

Zurück
Weiter

IT-Administrator: 1 von 5
Verwalten Sie Benutzer und Identitätsquellen

Management-Benutzer

Scott kann neue Benutzer über eine einfache Konfigurationsschnittstelle integrieren. Er kann Attribute von Grund auf hinzufügen oder Daten aus verschiedenen Identitätsquellen wie dem Cloud Directory, Active Directory oder einer IBMid extrahieren.



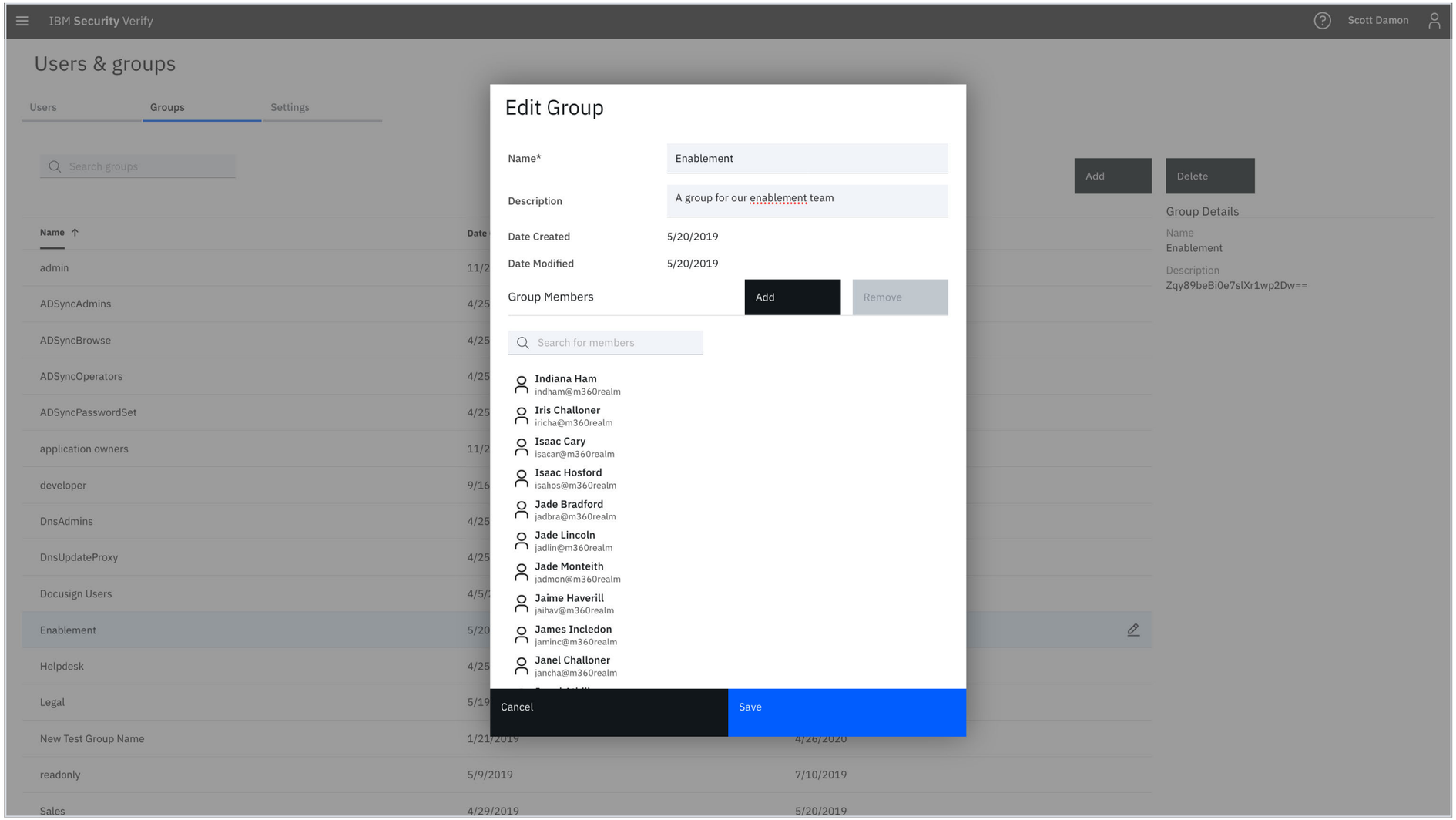
Weiter:
Gruppen verwalten

Mitarbeiter | Bereichsleiter | IT-Administrator | Vorgang überwachen | Richtlinien anpassen | **Benutzer und Identitäten verwalten** | Anwendungen hinzufügen | Risiko analysieren | Entwickler

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

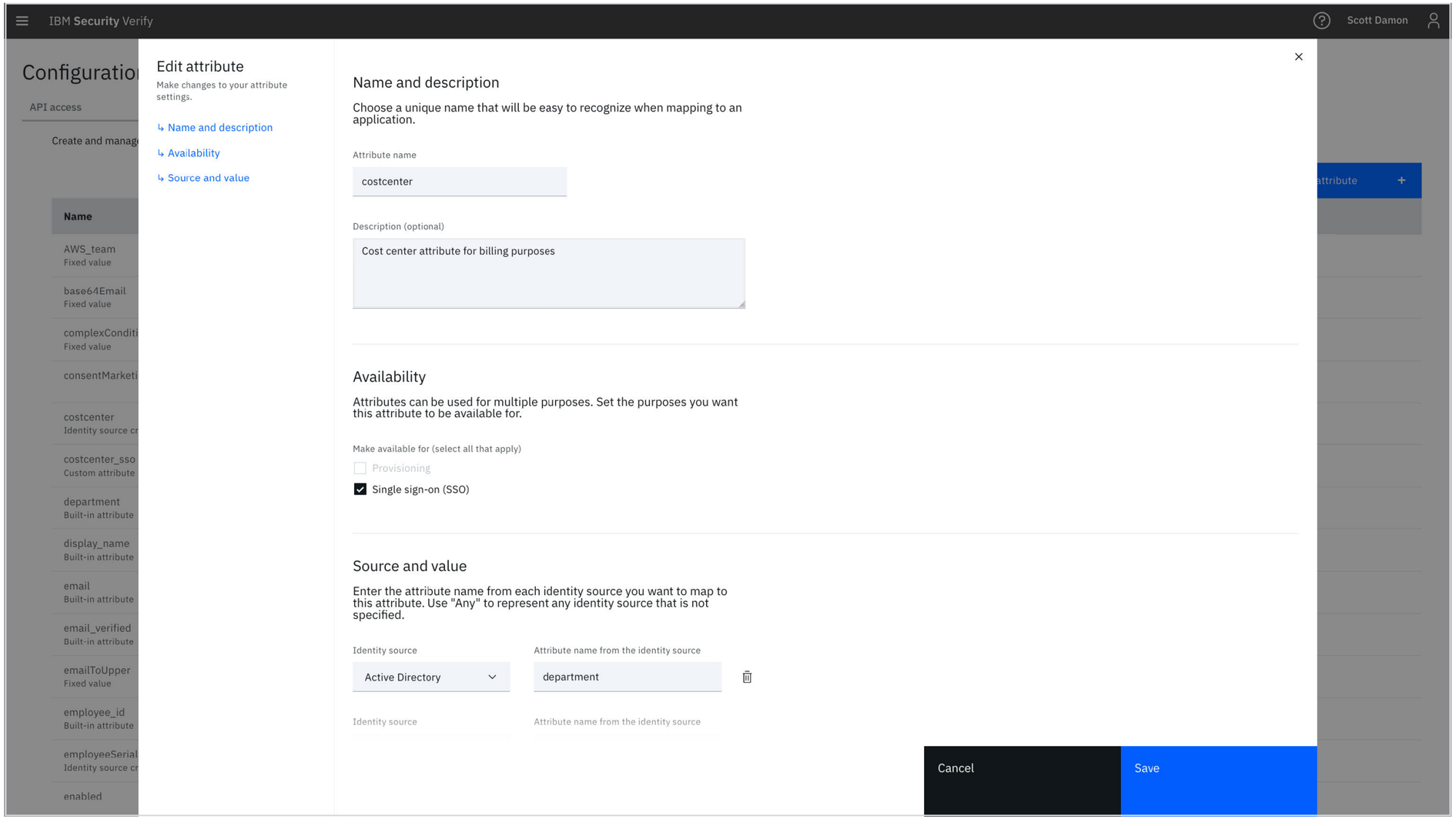
Mitarbeiter
Bereichsleiter
IT-Administrator
Vorgang überwachen
Richtlinien anpassen
Benutzer und Identitäten verwalten
Anwendungen hinzufügen
Risiko analysieren
Entwickler

Zurück
Weiter

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

Mitarbeiter
Bereichsleiter
IT-Administrator
Vorgang überwachen
Richtlinien anpassen
Benutzer und Identitäten verwalten
Anwendungen hinzufügen
Risiko analysieren
Entwickler

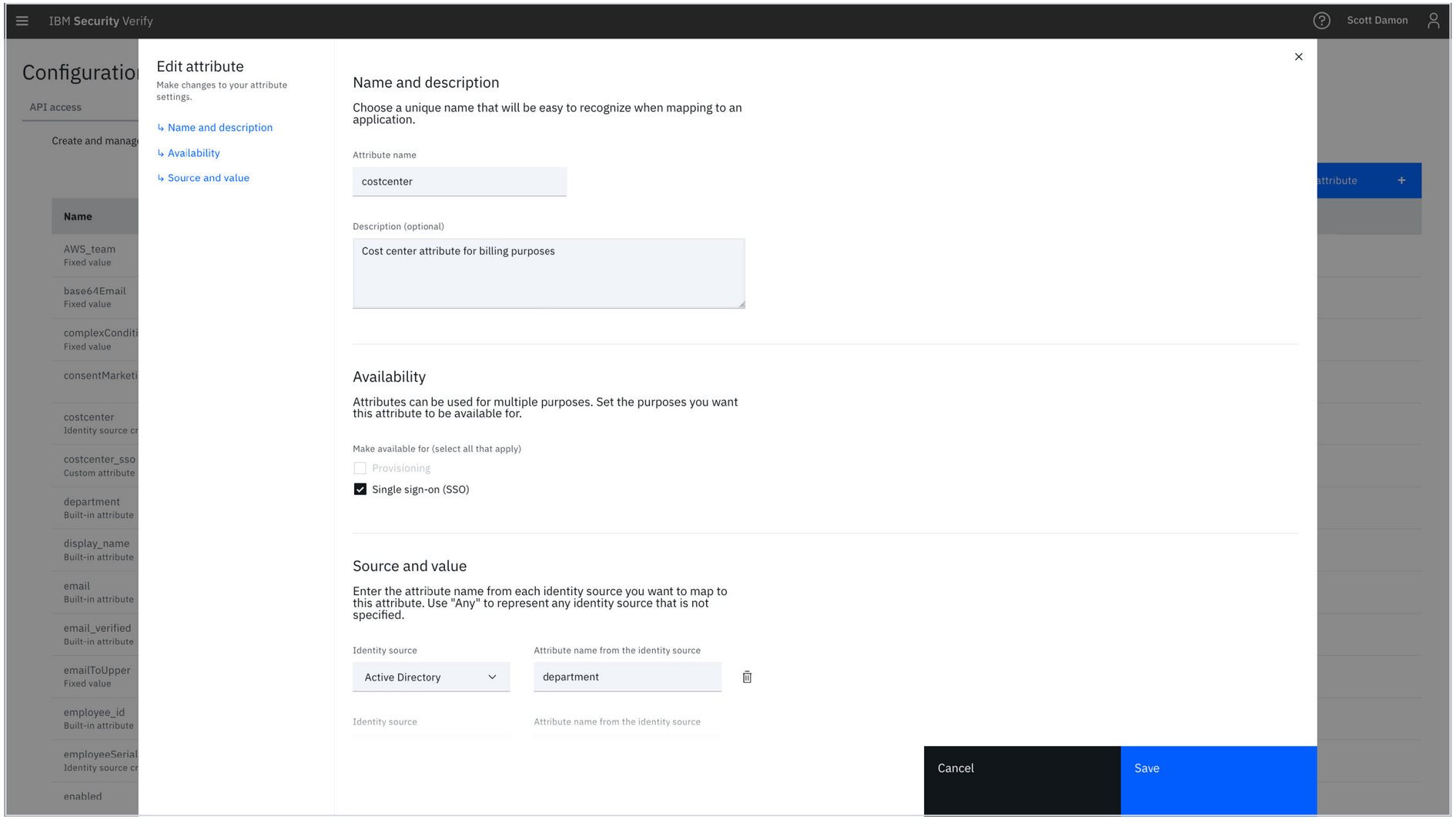
Zurück
Weiter

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.



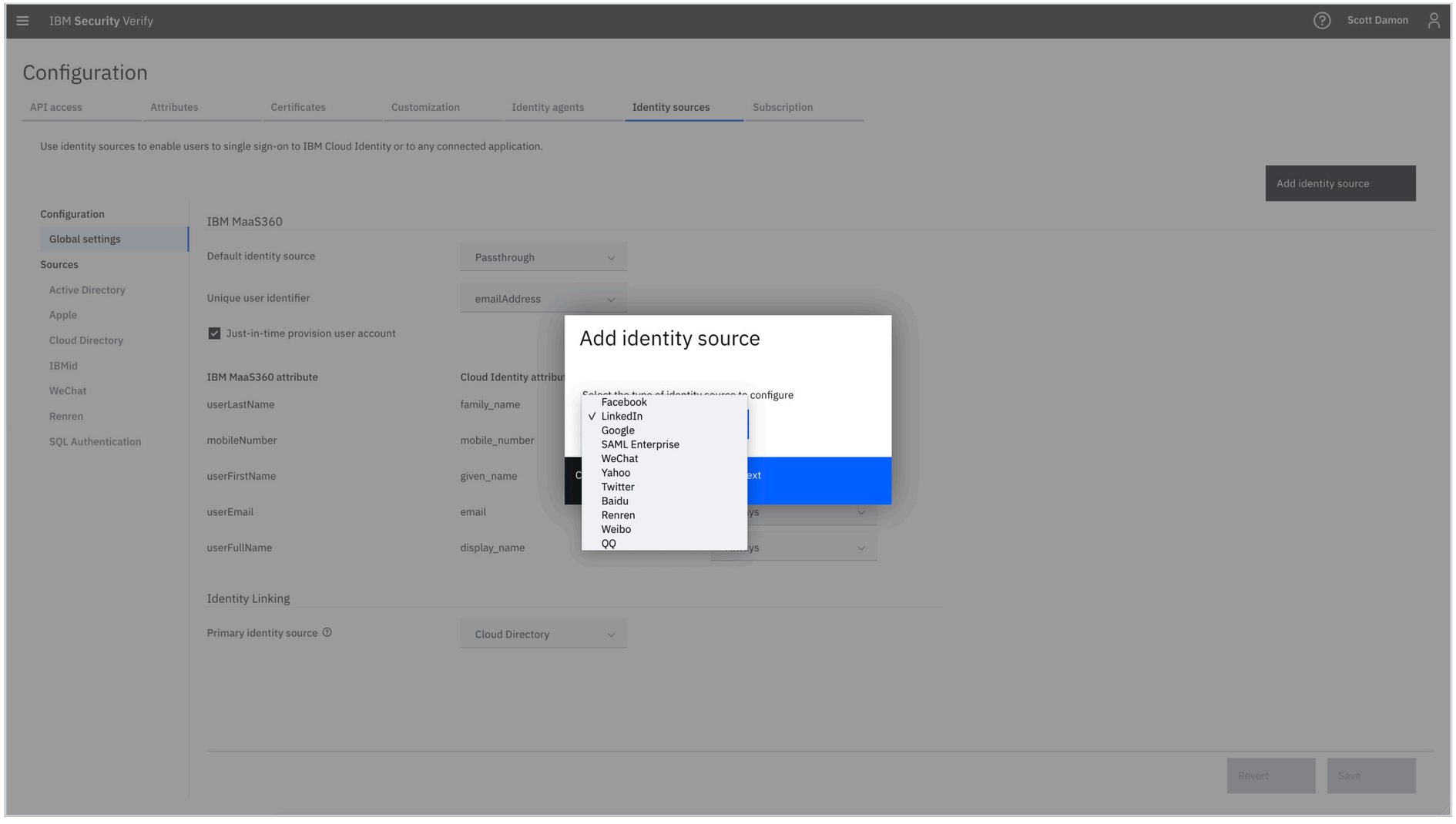
Weiter:
Soziale Anmeldung

Mitarbeiter | Bereichsleiter | **IT-Administrator** | Vorgang überwachen | Richtlinien anpassen | **Benutzer und Identitäten verwalten** | Anwendungen hinzufügen | Risiko analysieren | Entwickler

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.



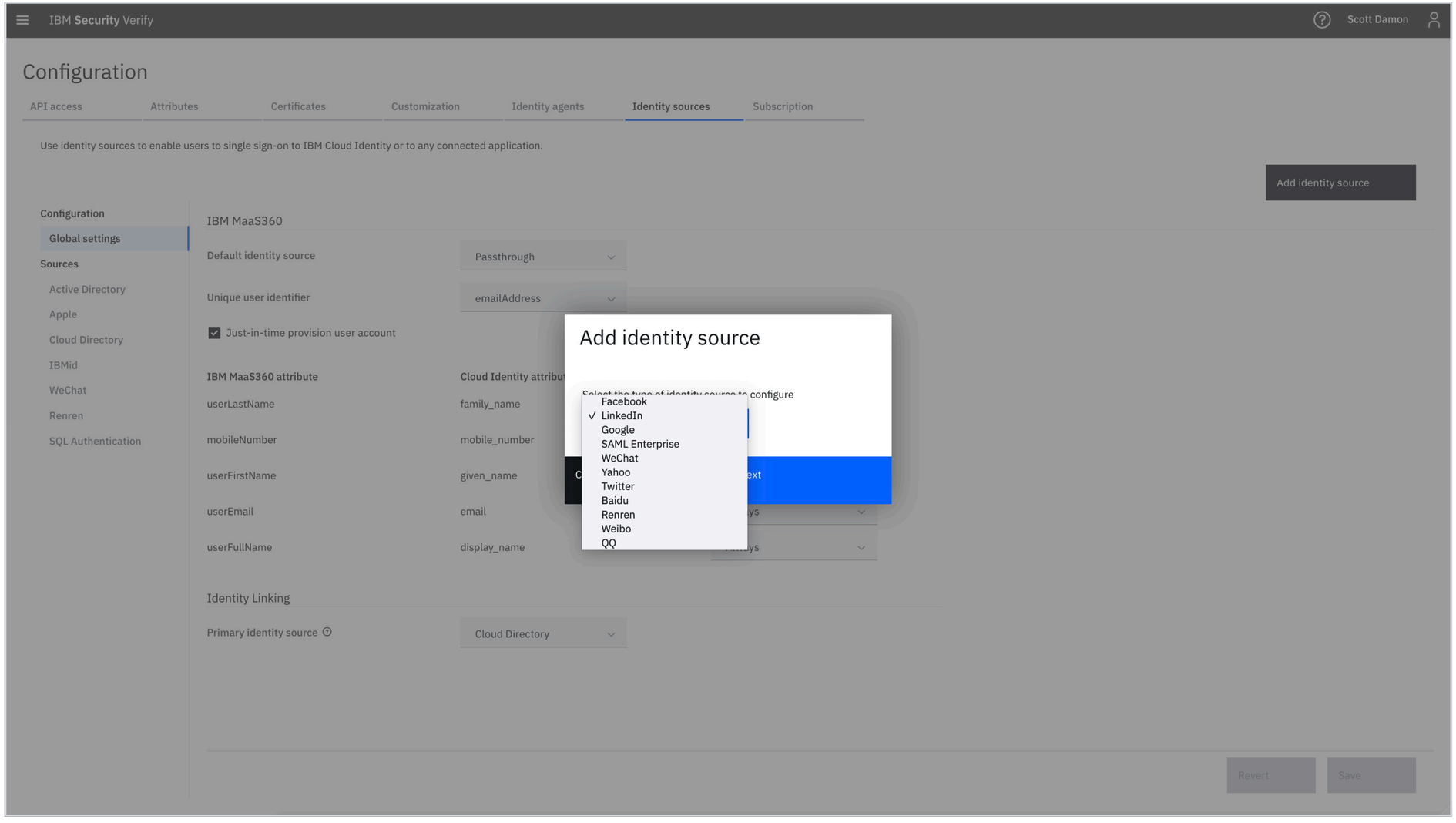
Weiter:
Anwendungen anzeigen

Mitarbeiter · Bereichsleiter · IT-Administrator · Vorgang überwachen · Richtlinien anpassen · **Benutzer und Identitäten verwalten** · Anwendungen hinzufügen · Risiko analysieren · Entwickler

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.



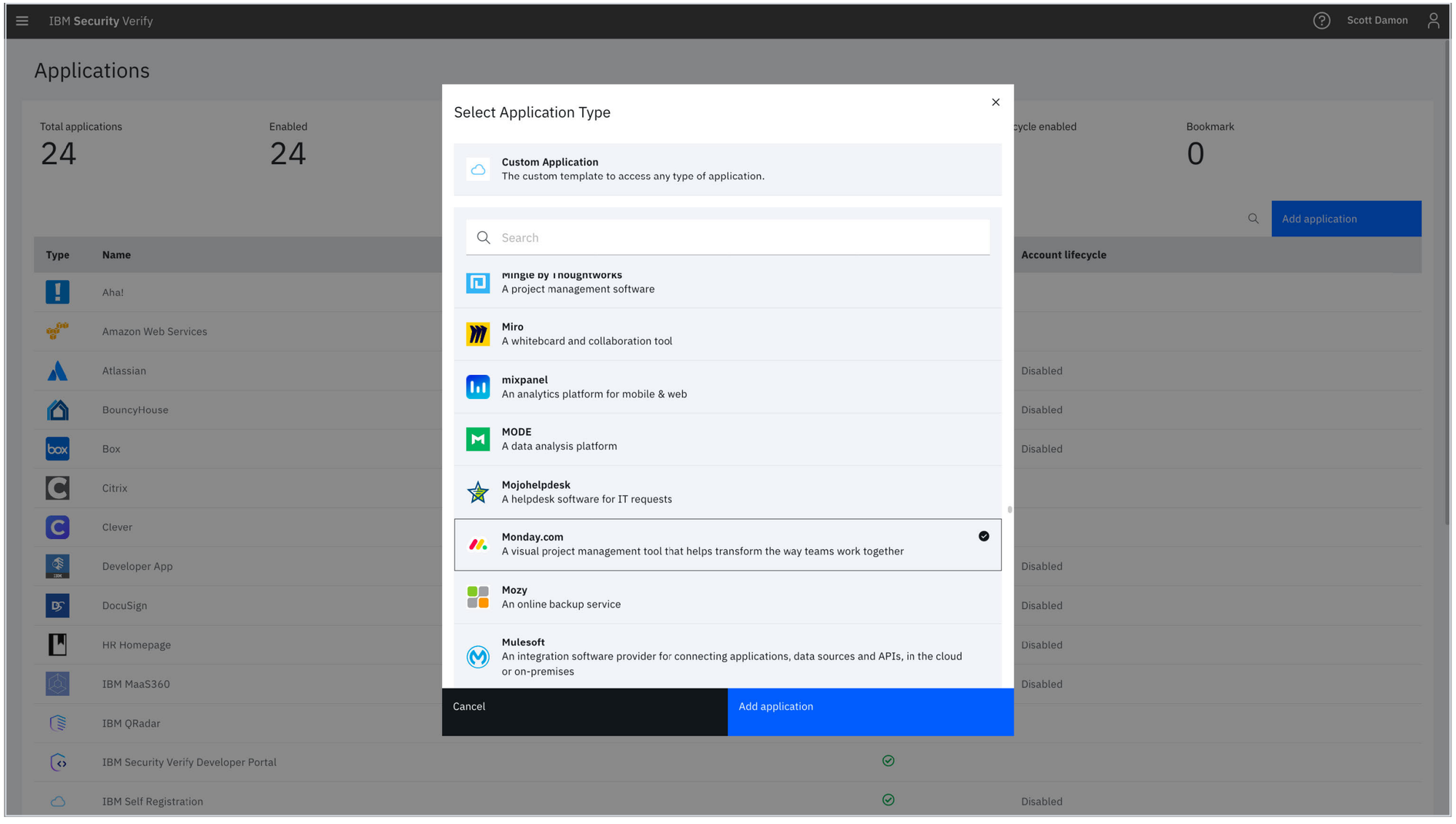
Weiter:
Nach Anwendungen zum Hinzufügen suchen

Mitarbeiter
Bereichsleiter
IT-Administrator
Vorgang überwachen
Richtlinien anpassen
Benutzer und Identitäten verwalten
Anwendungen hinzufügen
Risiko analysieren
Entwickler

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

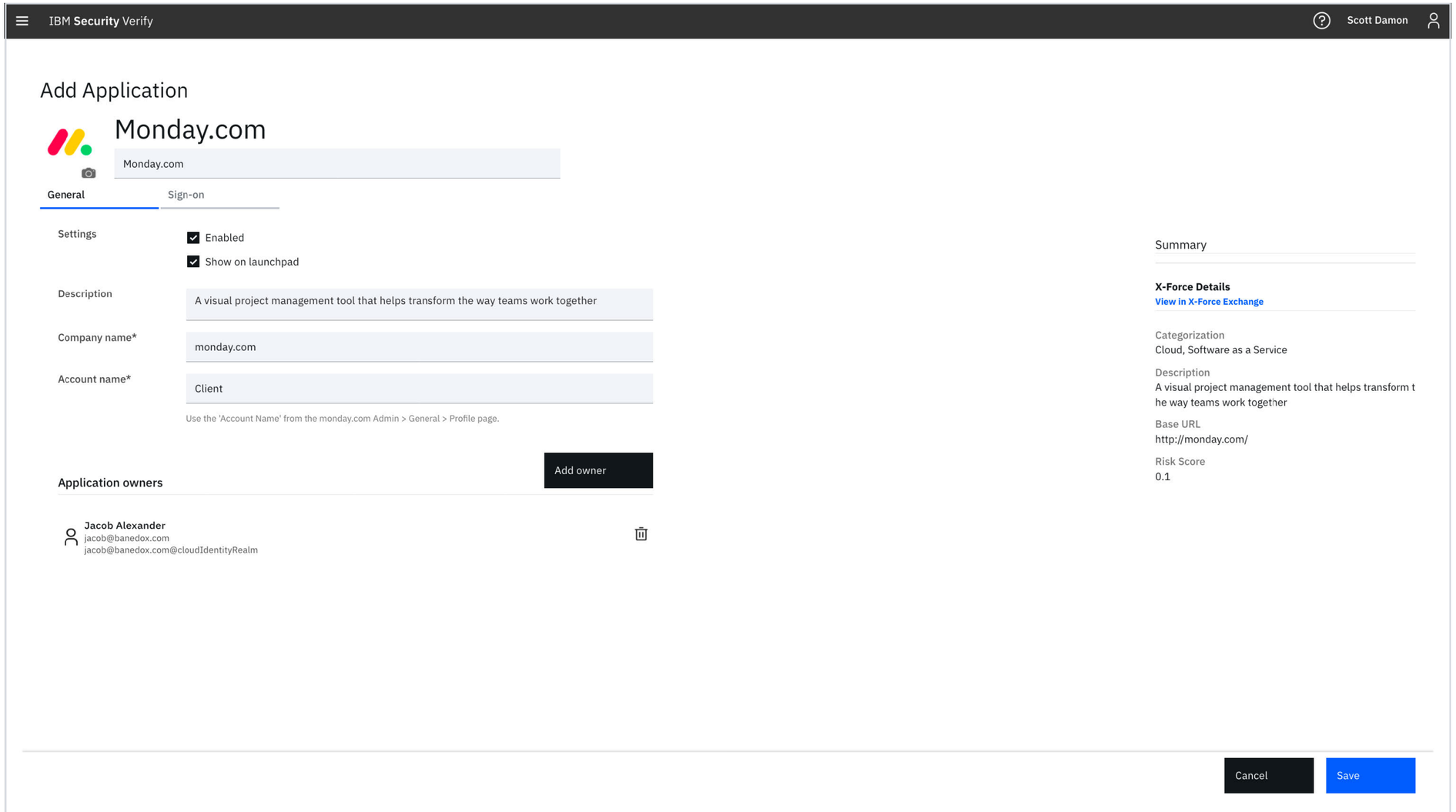
Mitarbeiter · Bereichsleiter · IT-Administrator · Vorgang überwachen · Richtlinien anpassen · Benutzer und Identitäten verwalten · **Anwendungen hinzufügen** · Risiko analysieren · Entwickler

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.

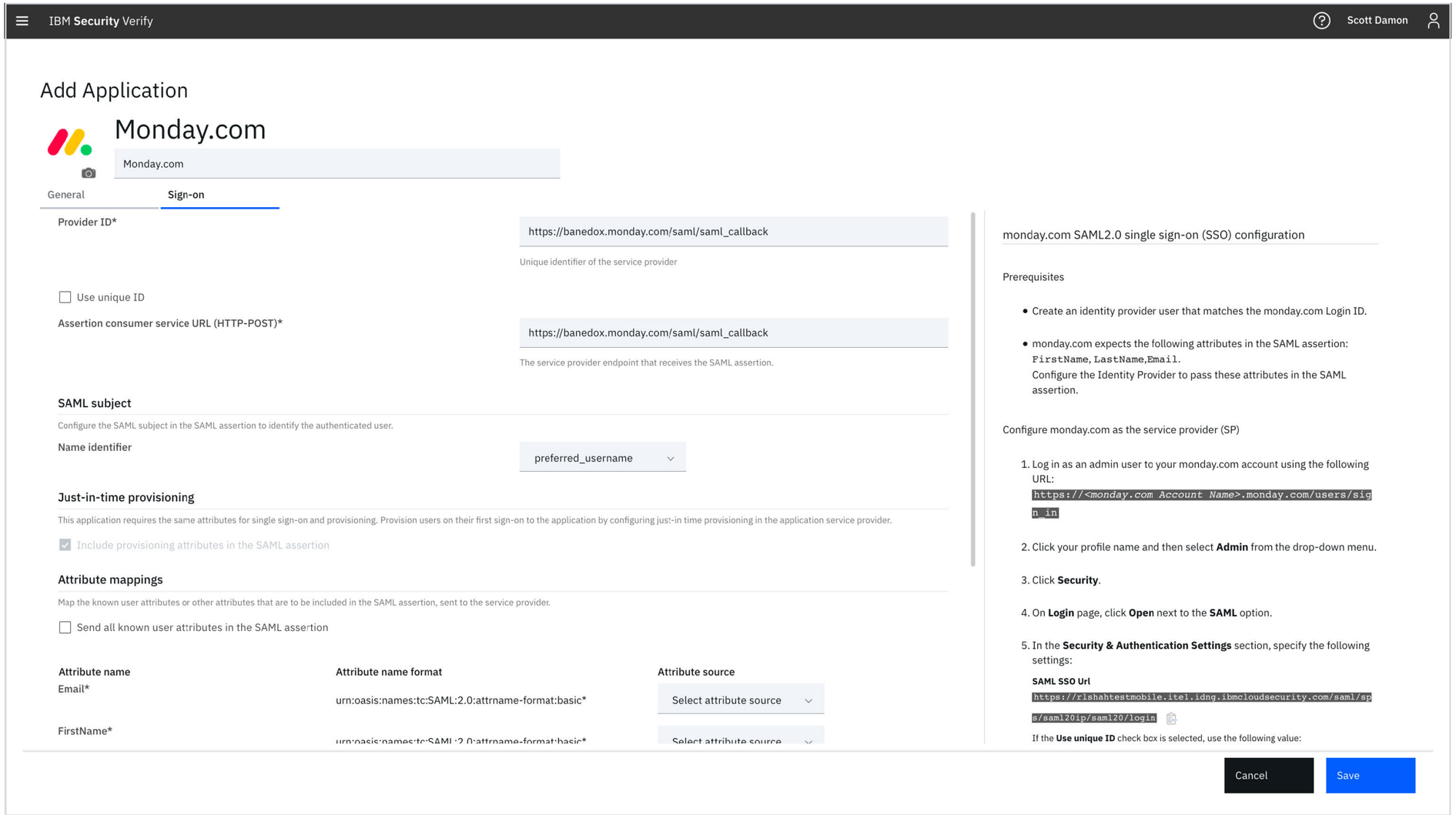


Weiter:
Anmeldungseinstellungen konfigurieren

IT-Administrator: 4 von 6
Anwendungen hinzufügen

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.

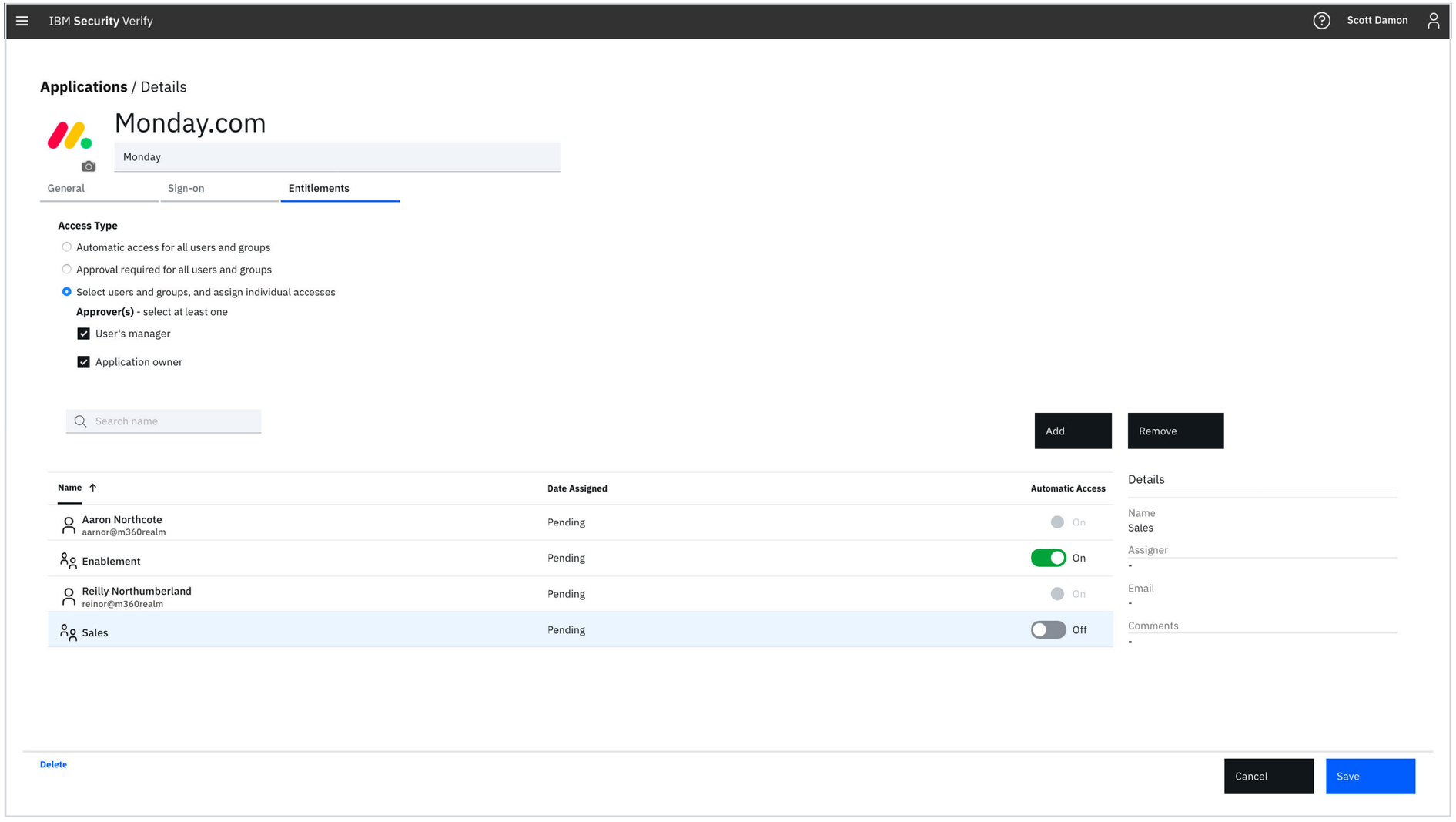


Weiter:
Berechtigungen konfigurieren

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

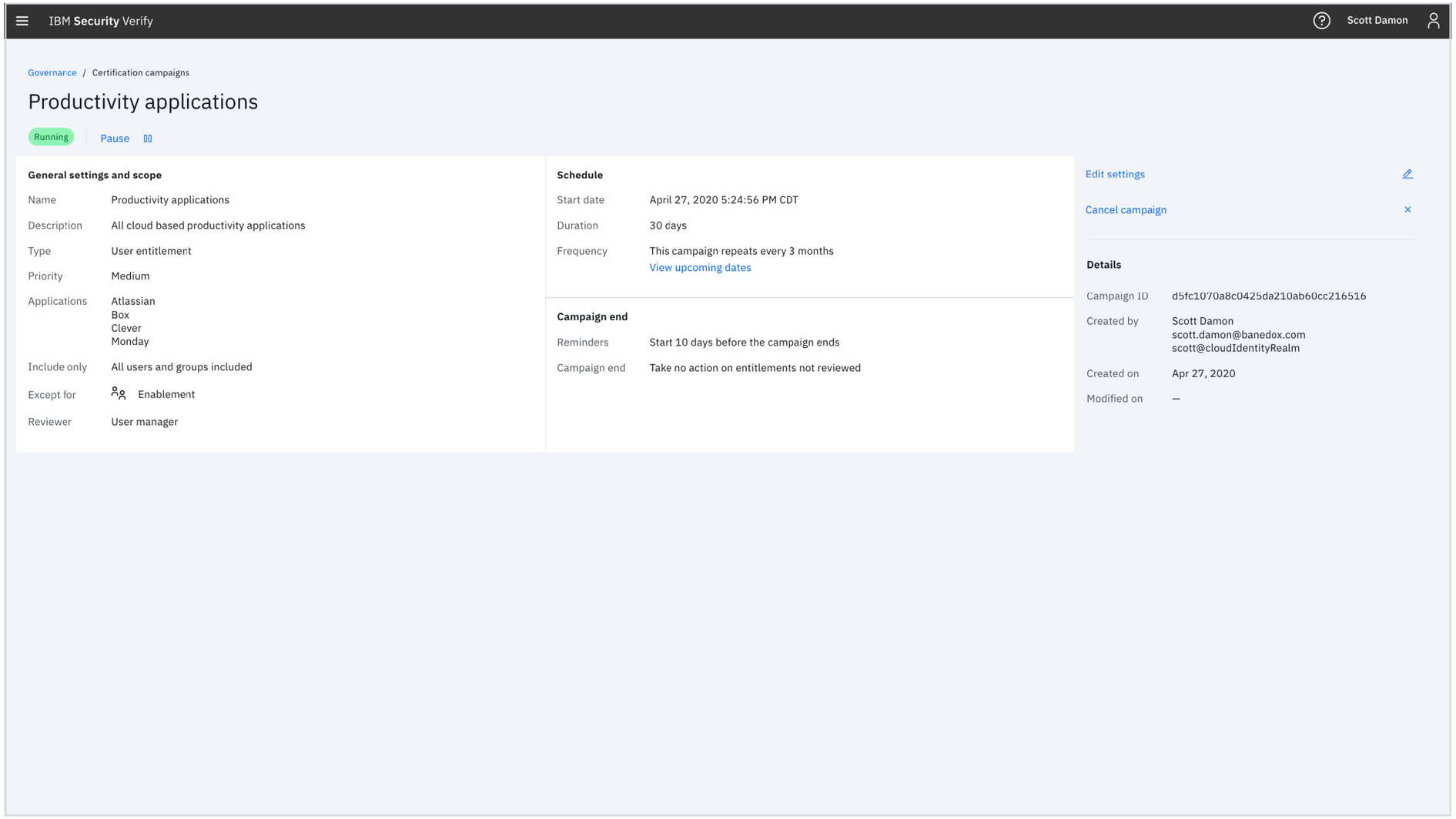
IT-Administrator: 6 von 6

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.

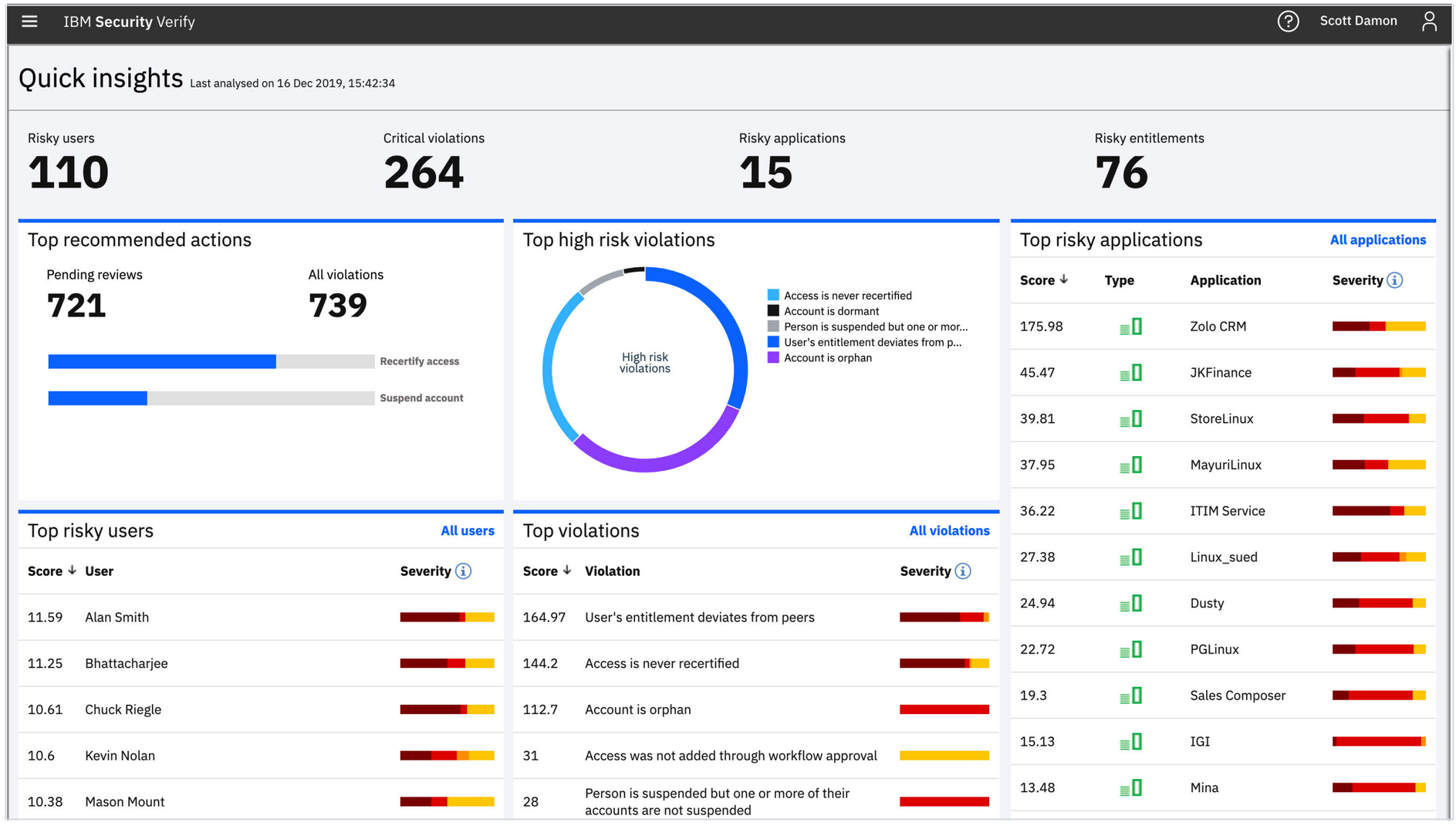
Weiter:
Analysedashboard



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.



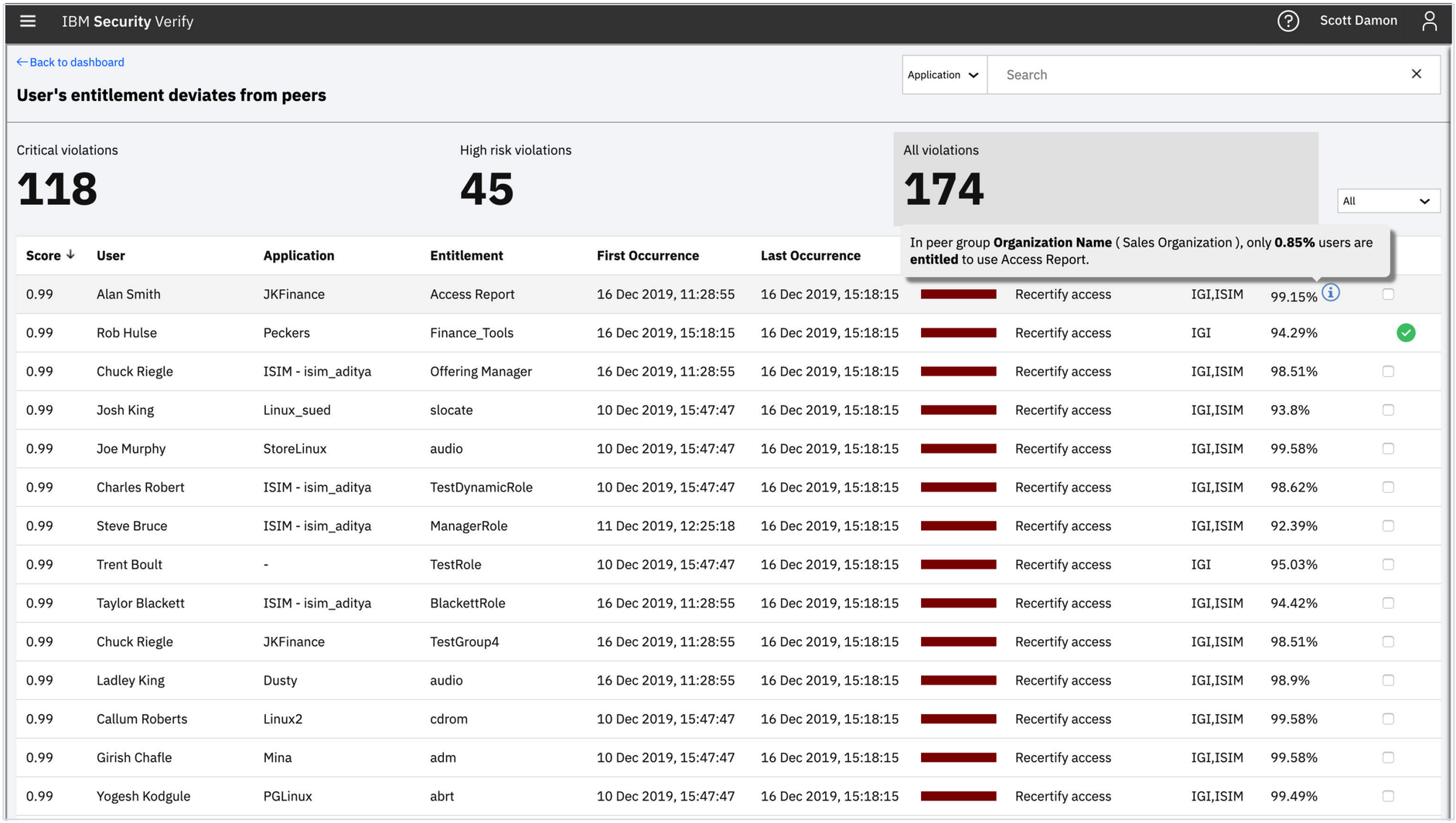
Weiter:
Eingestufte Richtlinienverstöße anzeigen

Mitarbeiter · Bereichsleiter · IT-Administrator · Vorgang überwachen · Richtlinien anpassen · Benutzer und Identitäten verwalten · Anwendungen hinzufügen · **Risiko analysieren** · Entwickler

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.



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%	

Weiter:
Ergreifen Sie vorgeschlagene Korrekturaktionen

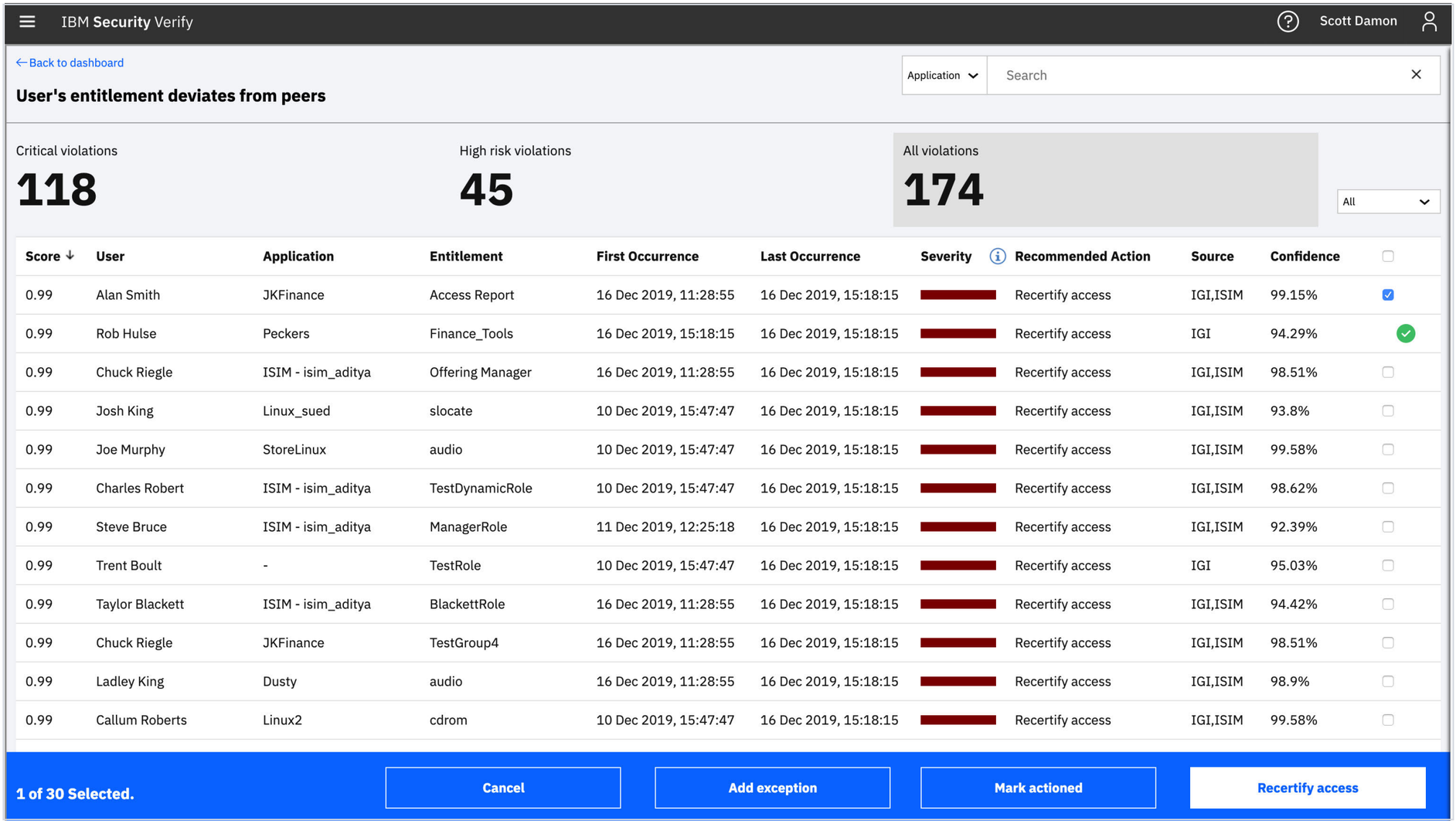
Mitarbeiter · Bereichsleiter · IT-Administrator · Vorgang überwachen · Richtlinien anpassen · Benutzer und Identitäten verwalten · Anwendungen hinzufügen · **Risiko analysieren** · Entwickler

Zurück
Weiter

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

Mitarbeiter · Bereichsleiter · IT-Administrator · Vorgang überwachen · Richtlinien anpassen · Benutzer und Identitäten verwalten · Anwendungen hinzufügen · **Risiko analysieren** · Entwickler

Zurück
Weiter

Entwickler

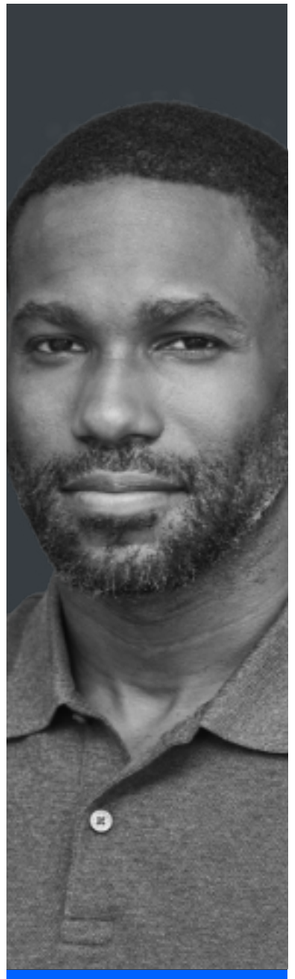
Integrieren Sie Zugriff und Authentifizierung in benutzerdefinierten Anwendungen mit intuitiven, speziell entwickelten APIs.

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%

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

Zurück
Weiter

Entwickler

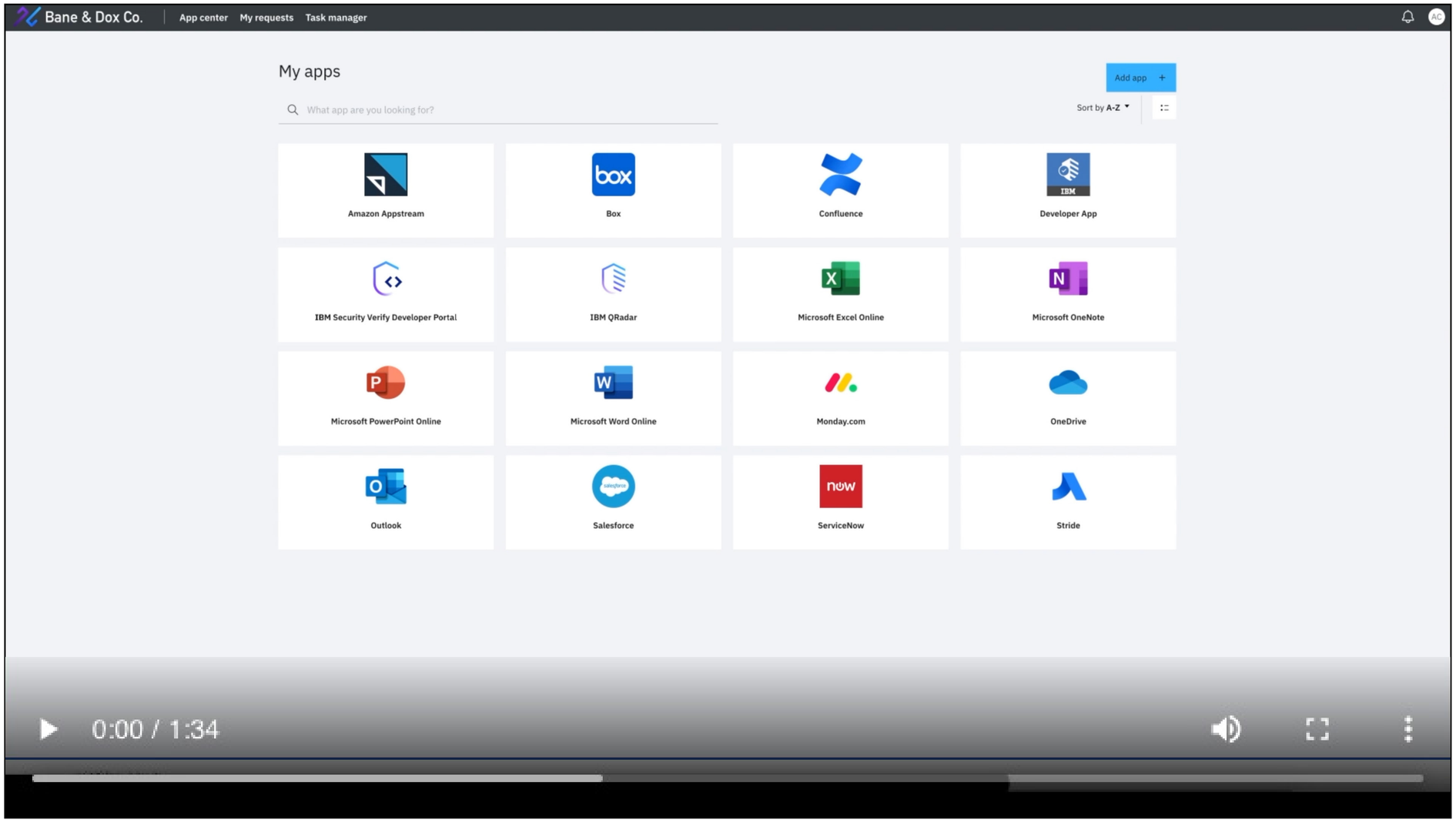
Integrieren Sie Zugriff und Authentifizierung in benutzerdefinierten Anwendungen mit intuitiven, speziell entwickelten APIs.

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.

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

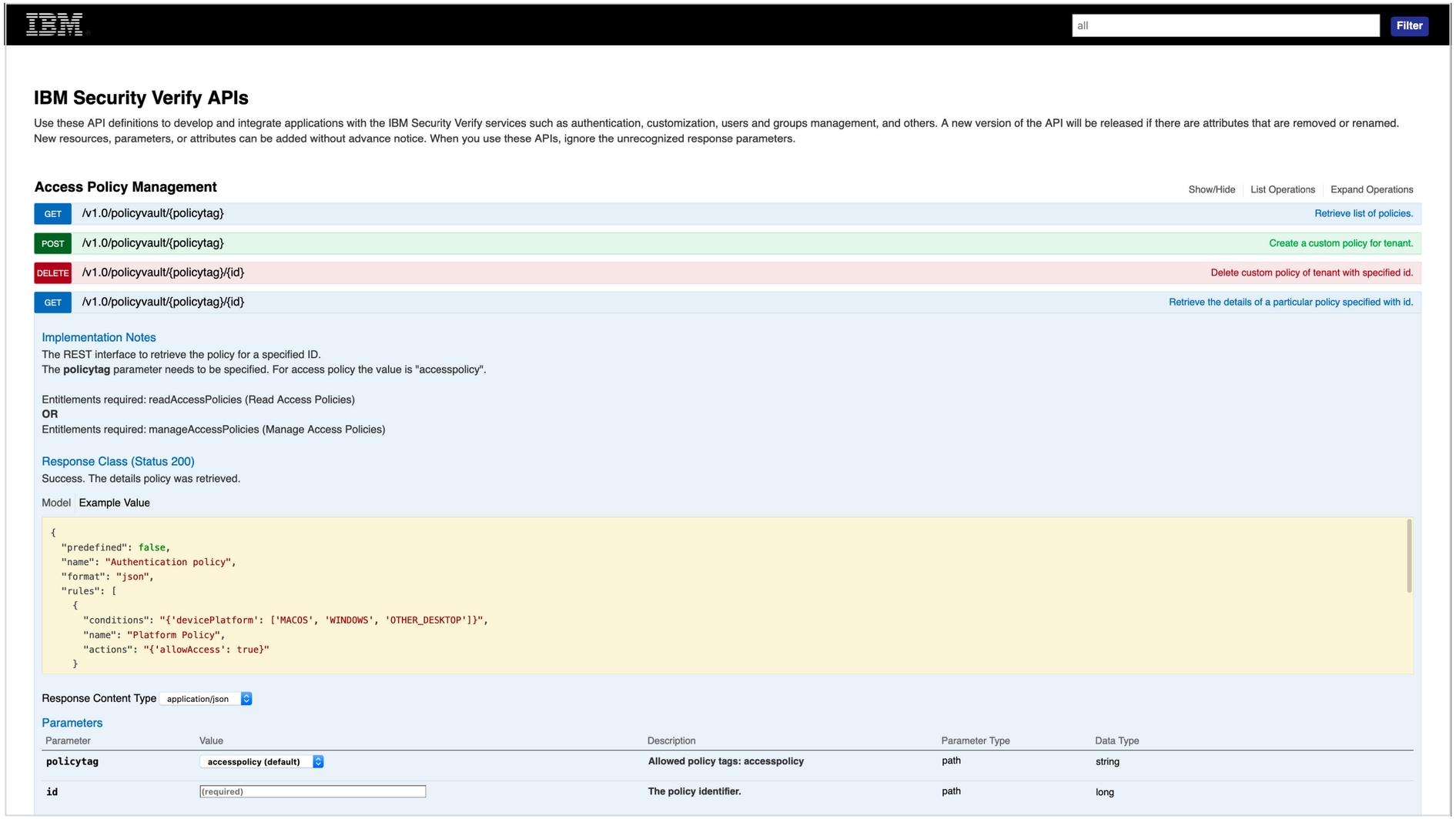
Mitarbeiter
Bereichsleiter
IT-Administrator
Entwickler
Entwickler-ressourcen
Benutzerdefinierte Anwendungen erstellen
API-Konfiguration

Zurück
Weiter

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.



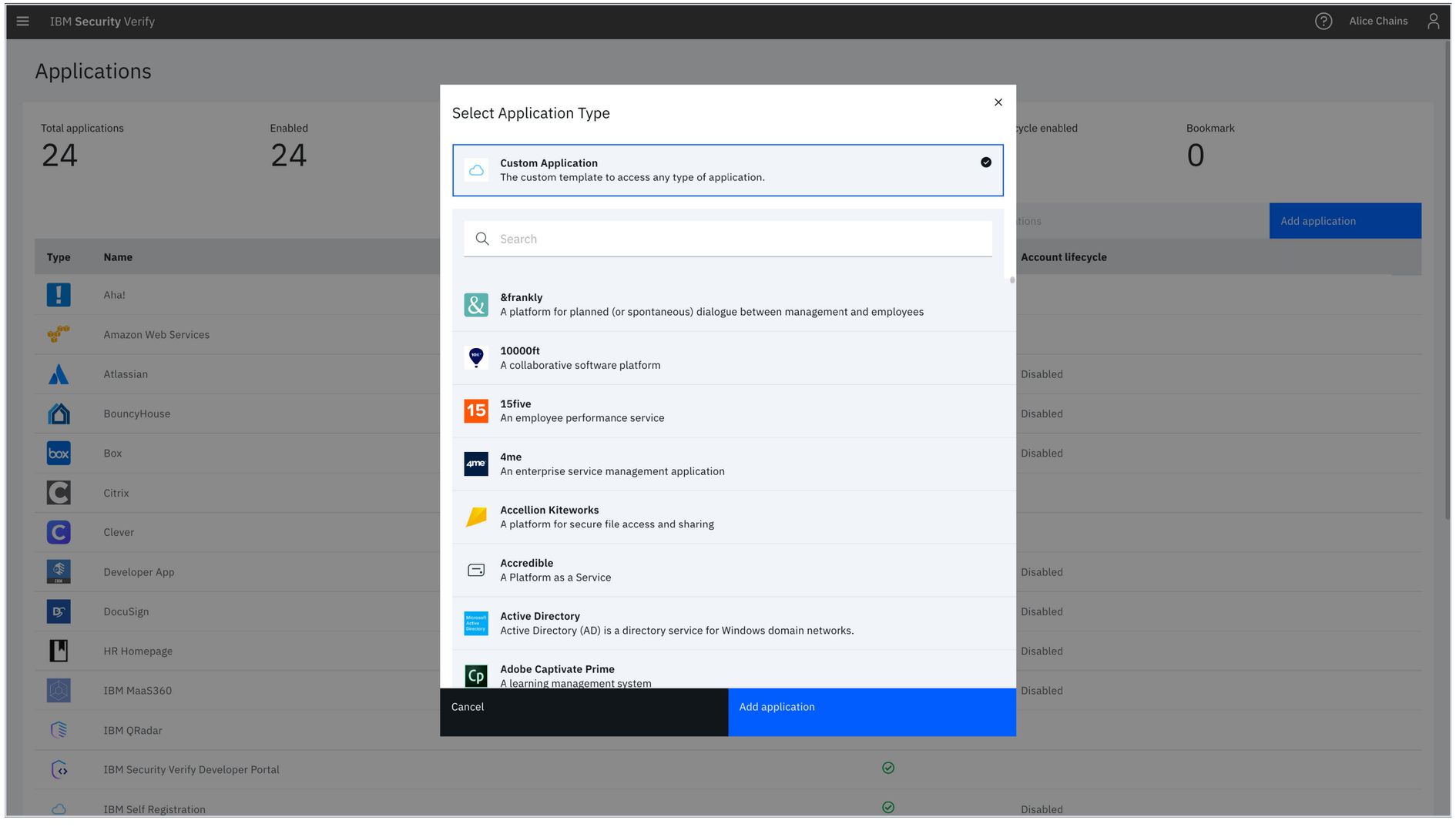
Weiter:
Benutzerdefinierte Anwendungsvorlage hinzufügen

Mitarbeiter · Bereichsleiter · IT-Administrator · Entwickler · **Entwickler-ressourcen** · Benutzerdefinierte Anwendungen erstellen · API-Konfiguration

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 föderiert einmalige Anmeldung von Verify integriert. Als Einstieg kann sie die benutzerdefinierte Anwendungsvorlage hinzufügen, um neue SAML- oder Open ID Connect-Anwendungen zu integrieren.



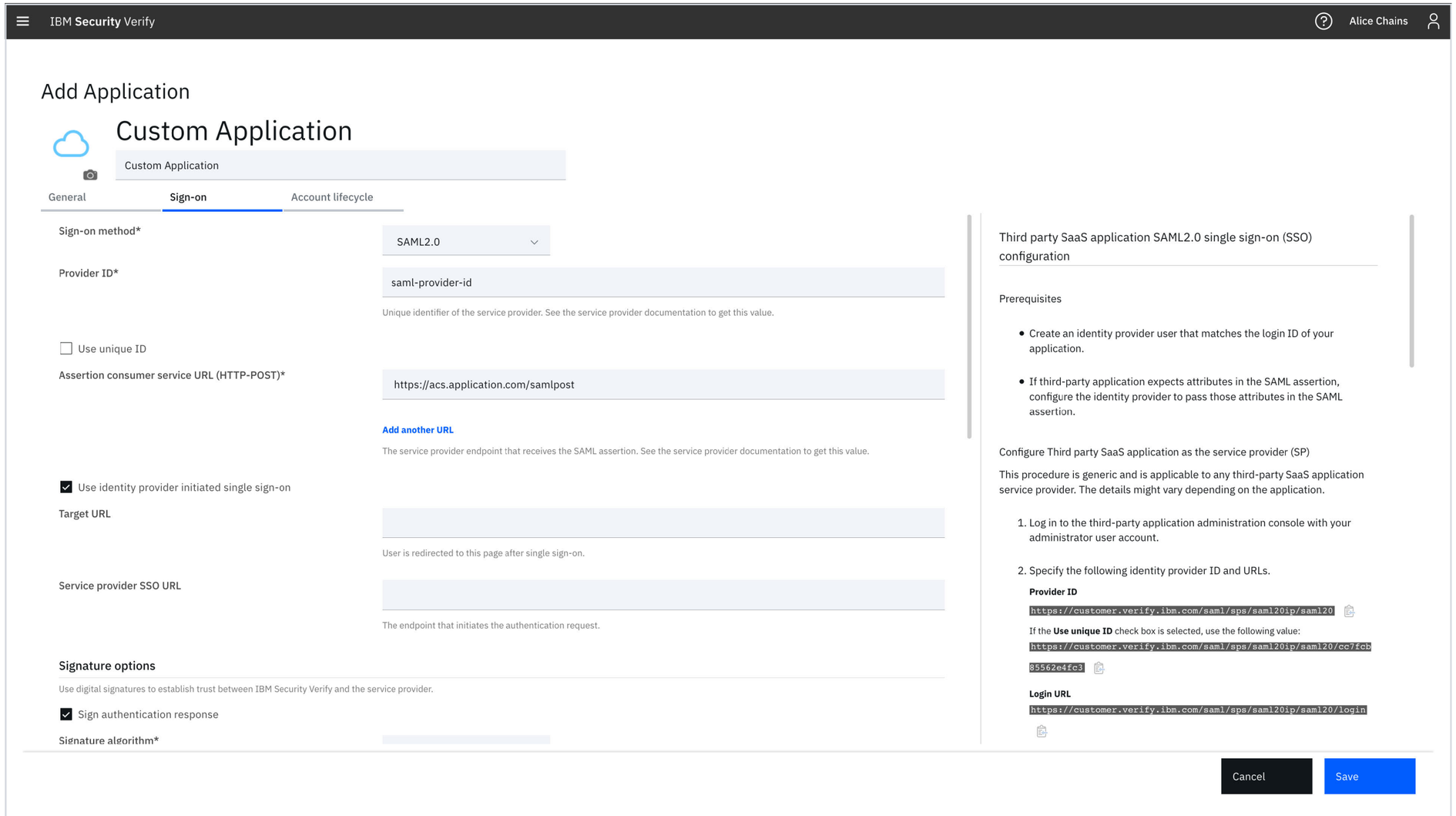
Weiter:
Anmeldungseinstellungen konfigurieren

Entwickler: 2 von 4

Benutzerdefinierte Anwendungen erstellen

Anmeldungs-einstellungen konfigurieren

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



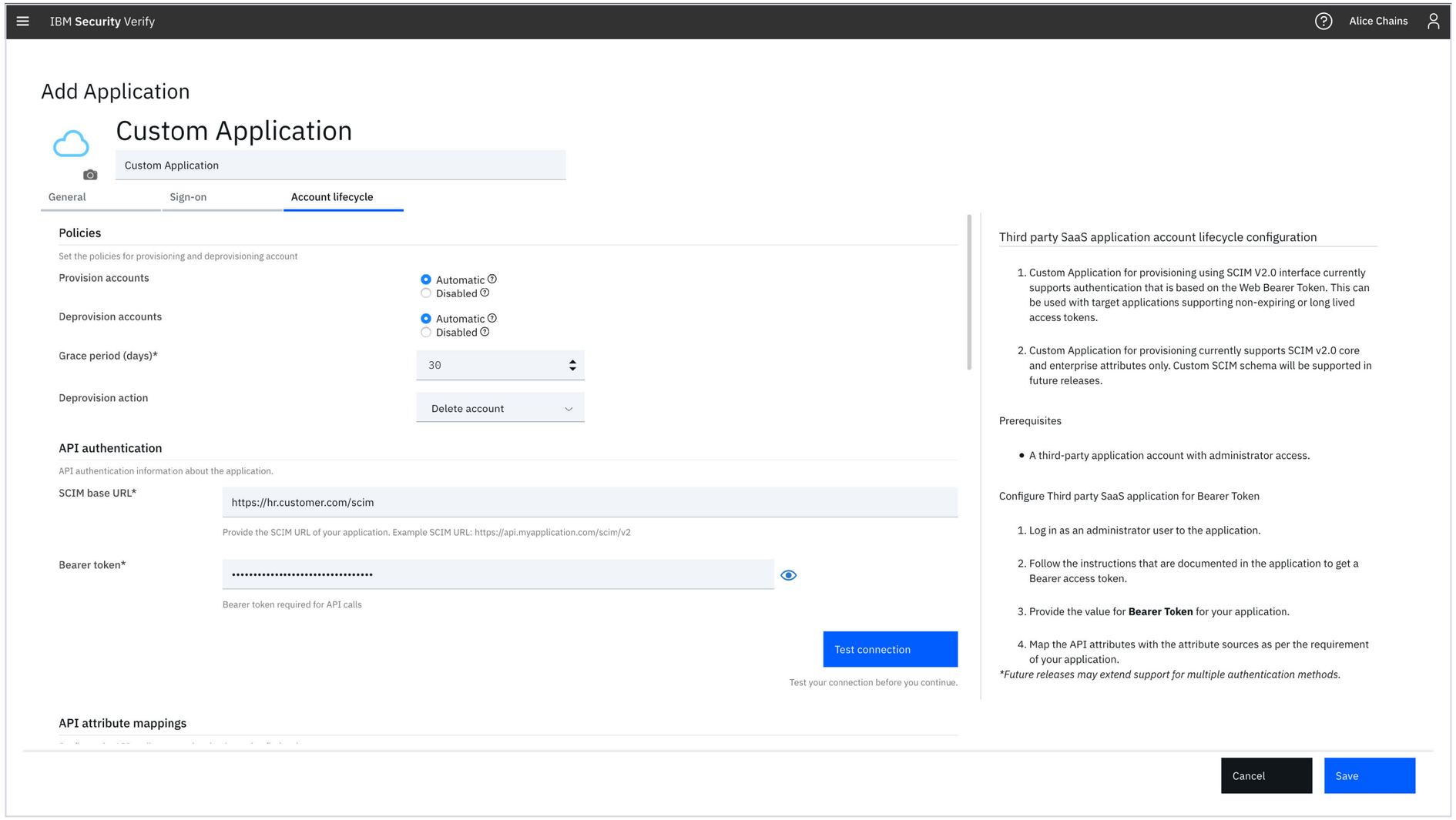
Weiter:
Bereitstellung konfigurieren

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

Mitarbeiter · Bereichsleiter · IT-Administrator · Entwickler · Entwickler-ressourcen · **Benutzerdefinierte Anwendungen erstellen** · API-Konfiguration

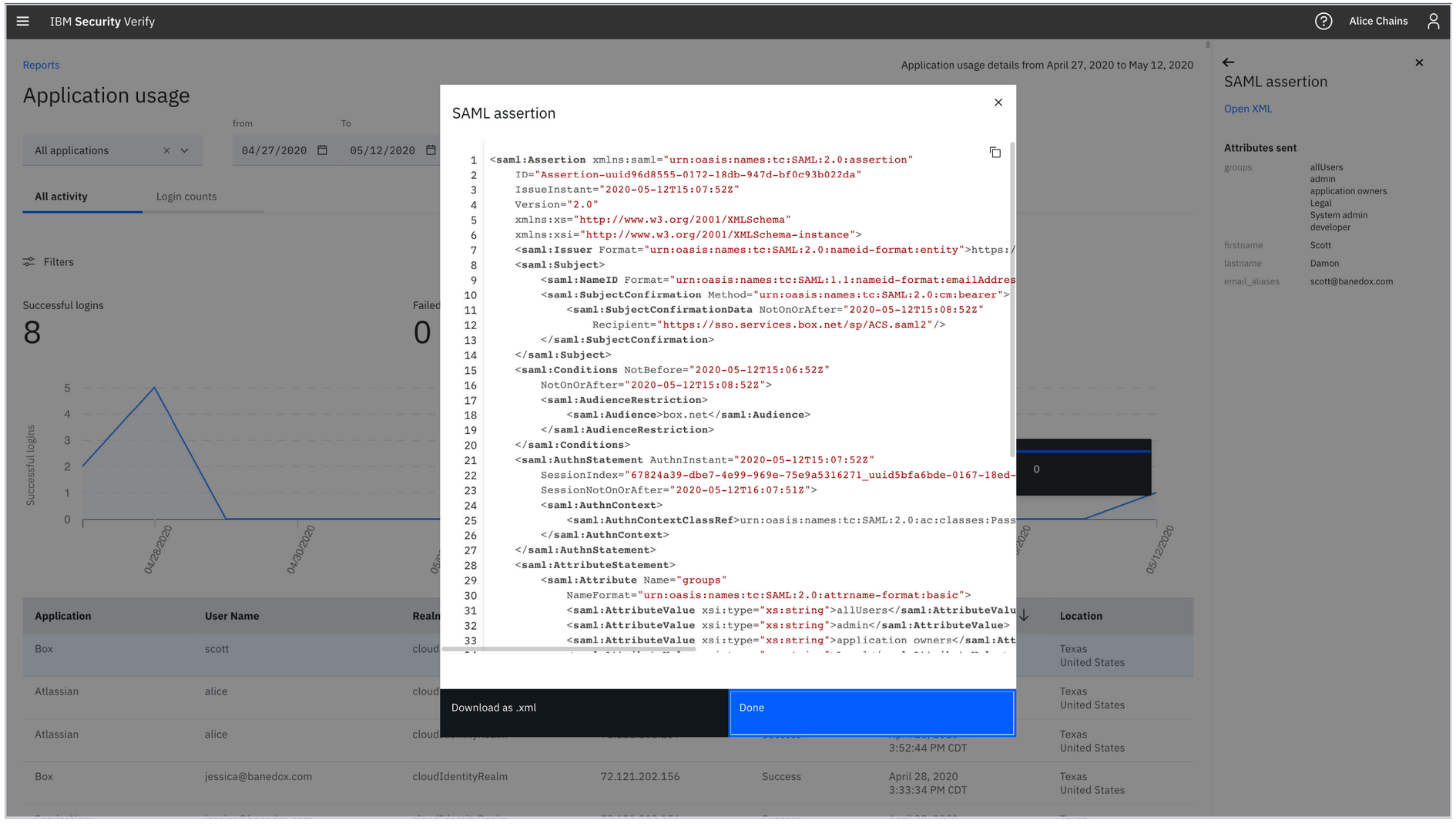
Zurück

Weiter

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.

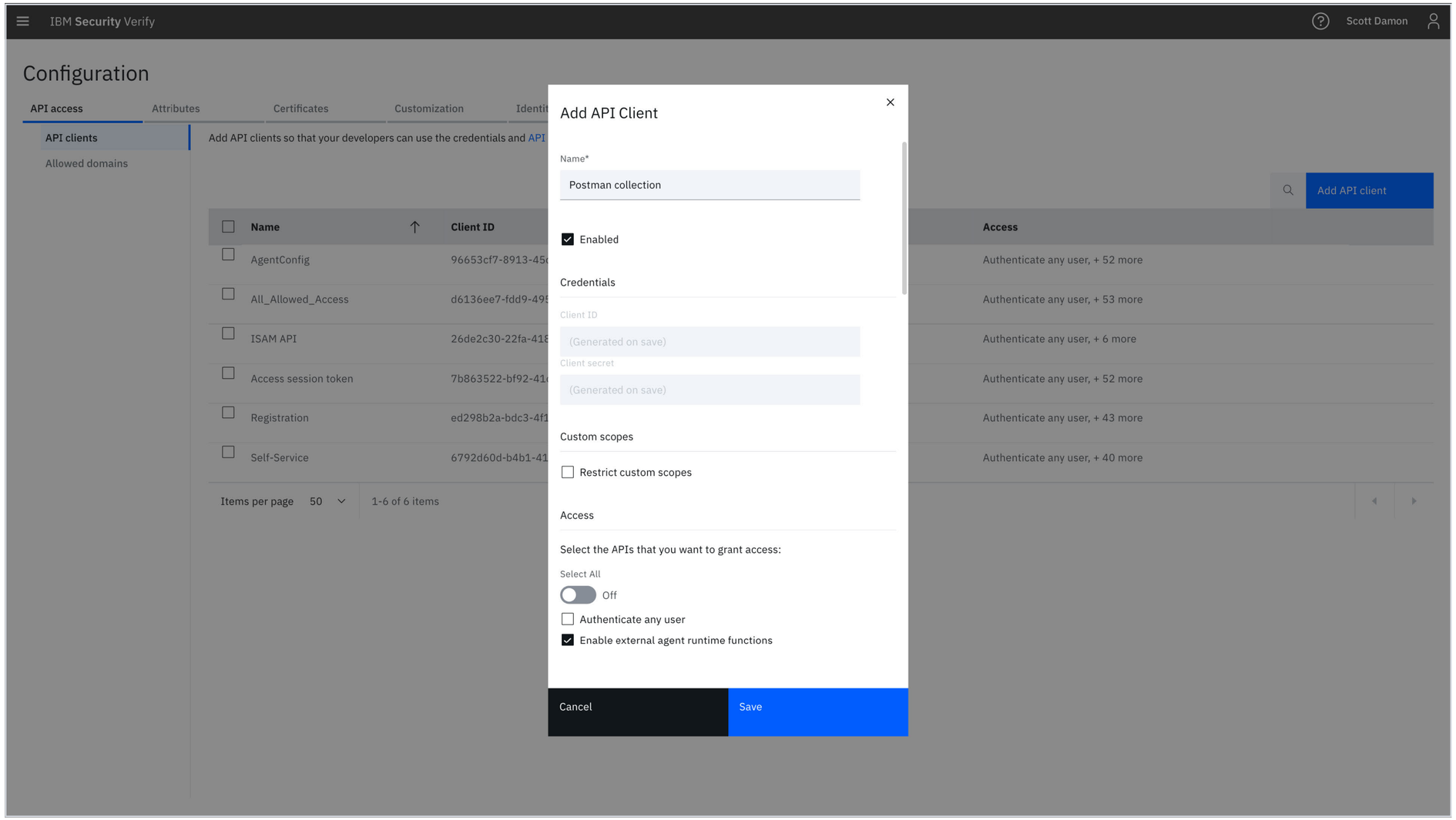


Weiter:
API-Clients hinzufügen

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.

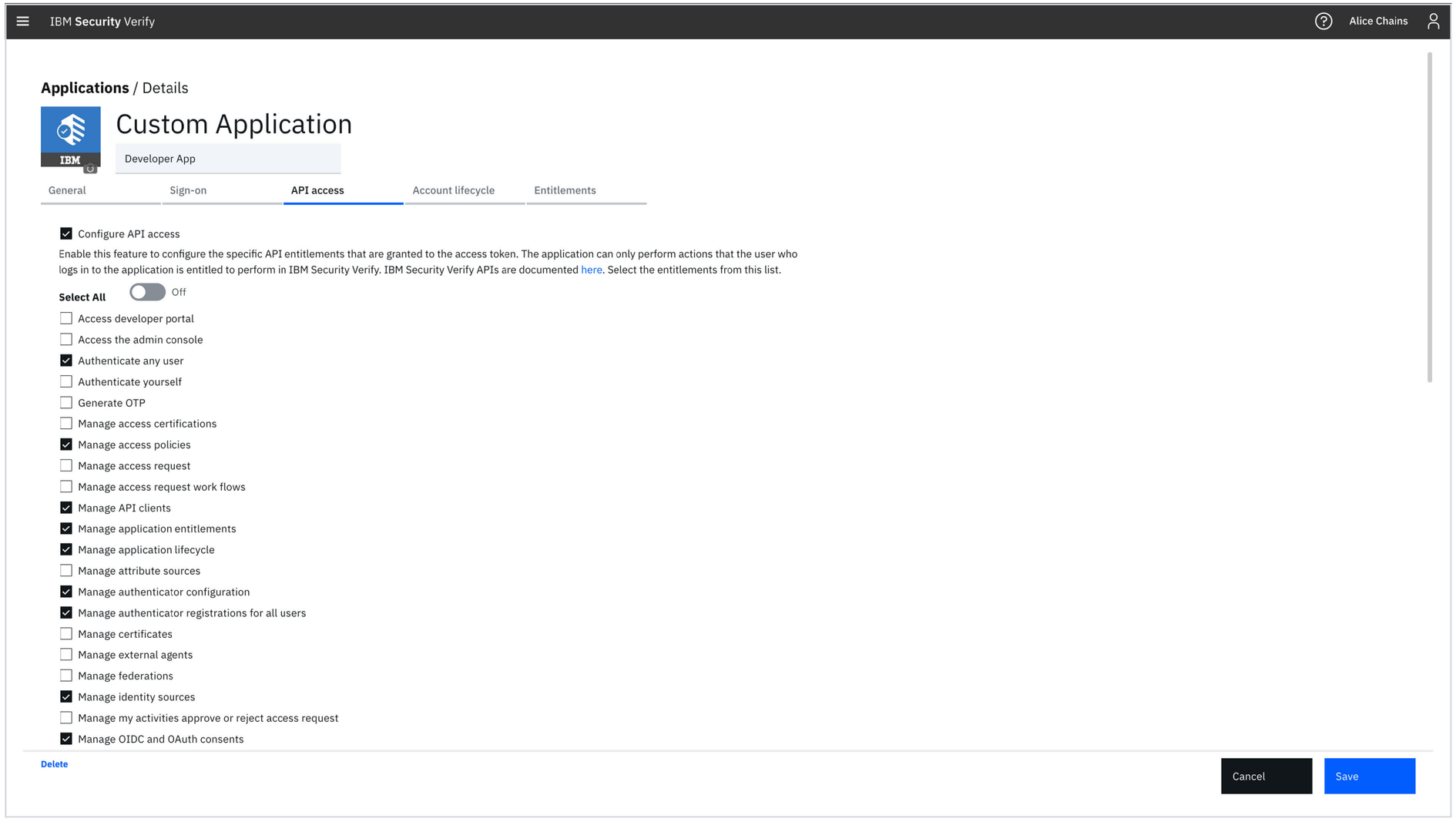


Weiter:
Stellvertreterverwaltung

Entwickler: 2 von 2
API-Konfiguration

Stellvertreterver-waltung

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



Informieren Sie sich über:
IBM Security Verify

Mitarbeiter
Bereichsleiter
IT-Administrator
Entwickler
Entwickler-ressourcen
Benutzerdefinierte Anwendungen erstellen
API-Konfiguration

Zurück
Weitere Informationen

IBM Security

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

00000000USEN

IBM