



Jamf Connect : Identity and Secure Access All-In-One



Nicholas McGillivray

Senior Sales Engineer, Security



Sean Rabbitt

Senior Consulting Engineer, Identity

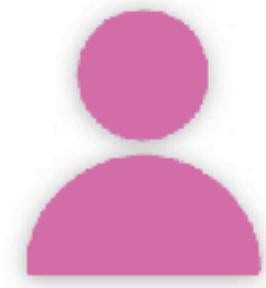


Jamf Connect: Identity and Secure Access

- What is Jamf Connect today?
- Tools + Requirements
- Deployment
- Demo



What is Connect Today?



Identity & Access Management

Provide users with a seamless experience from onboarding to access, based upon their existing cloud identity.



Zero Trust Network Access

Ensure only trusted users on sanctioned, safe devices are authorized to access work apps and data.



Identity & Access Management + Key Challenges



Time consuming
preparation by IT



Lack of **user management**
and insights

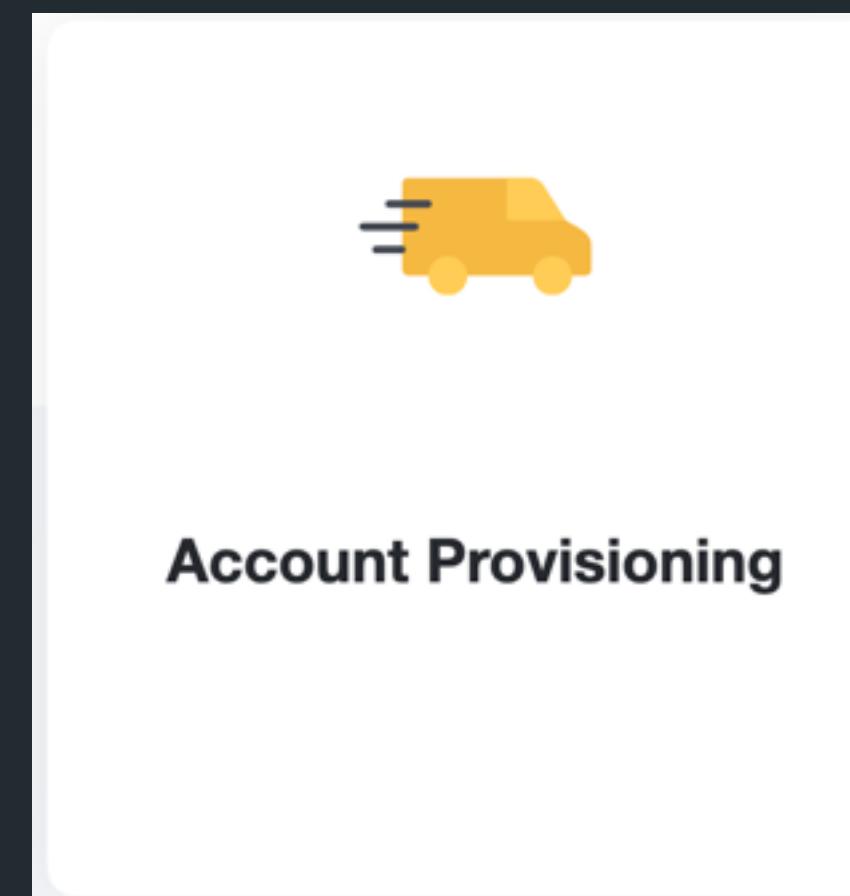


End user frustration with
password fatigue

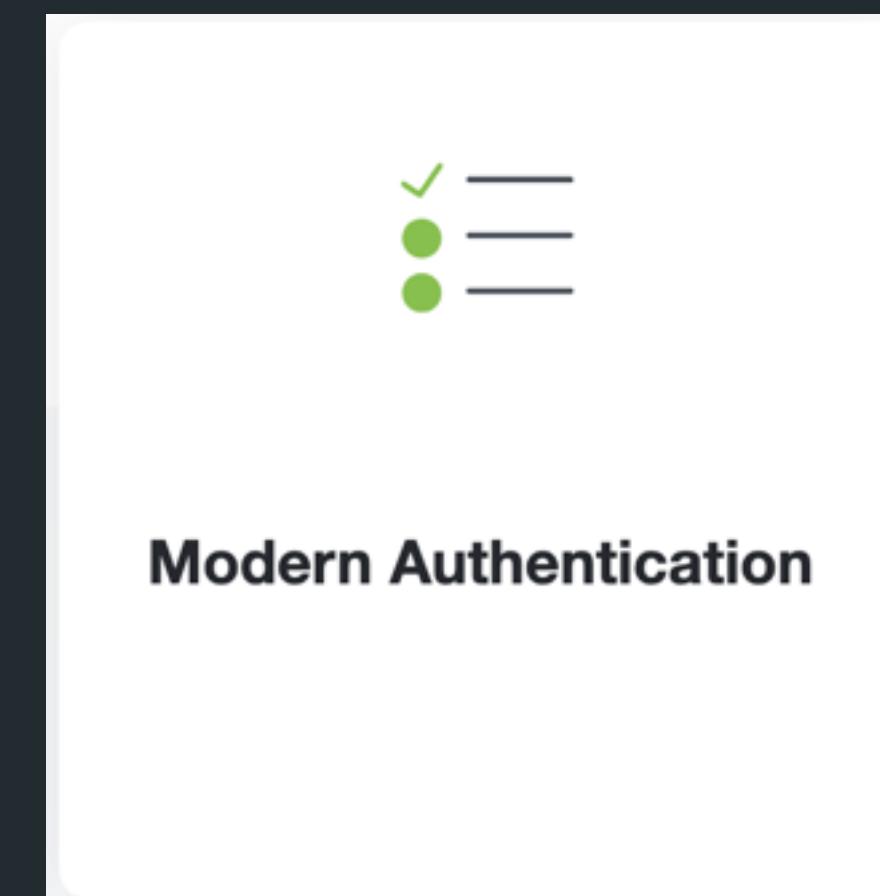


Identity & Access Management

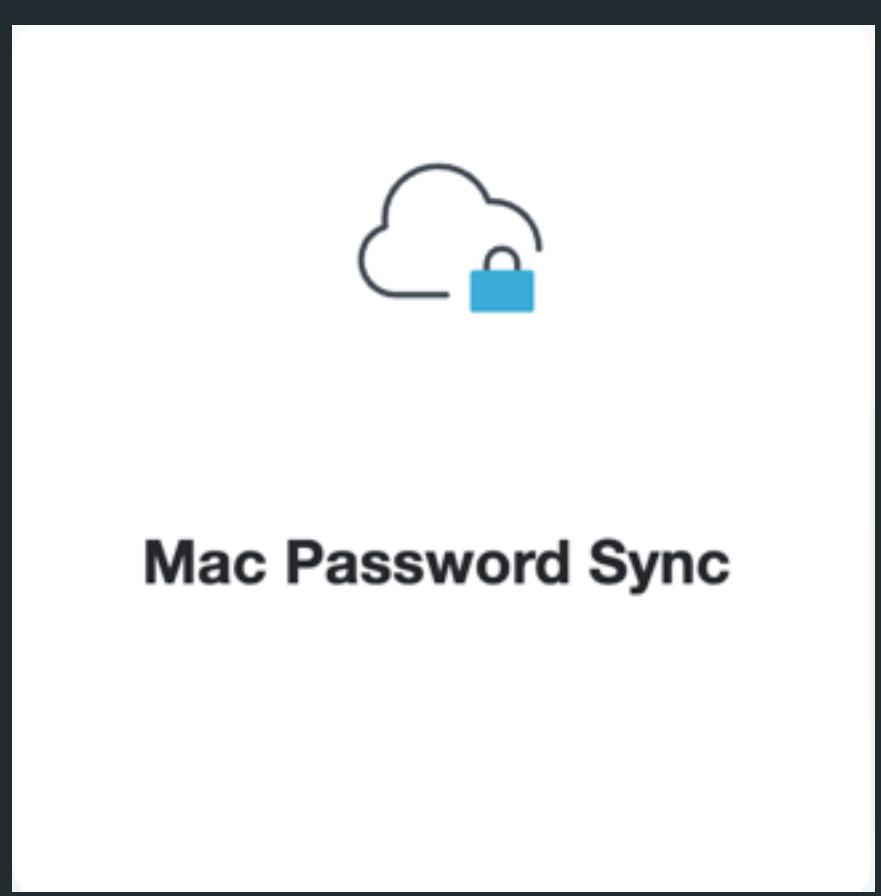
Connect Benefits



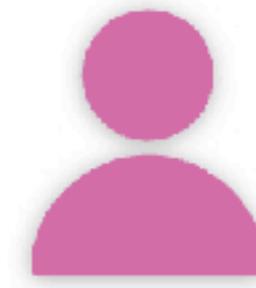
+



+



What is Connect Today?



Identity & Access Management

Provide users with a seamless experience from onboarding to access, based upon their existing cloud identity.

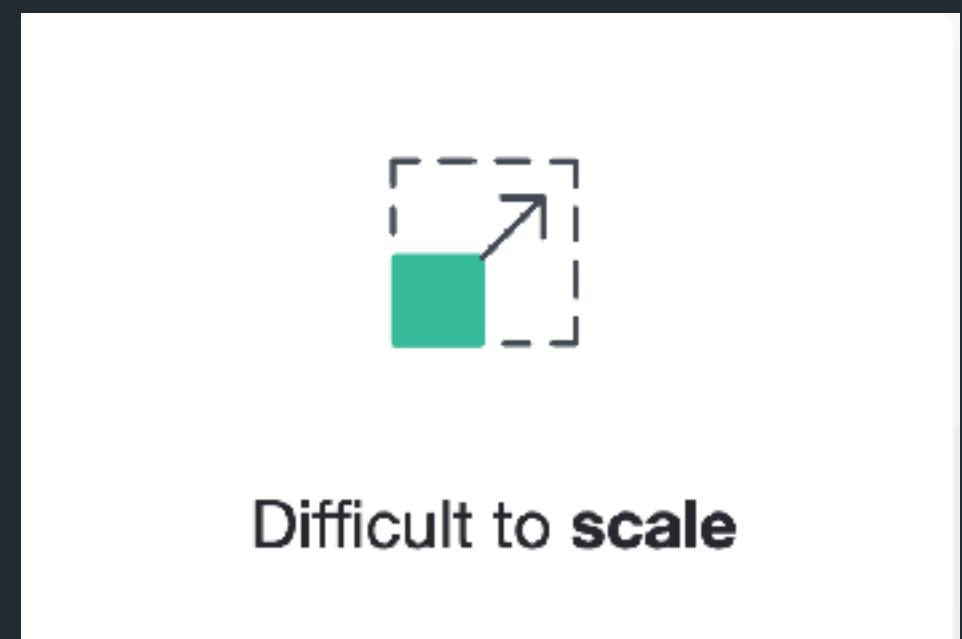


Zero Trust Network Access

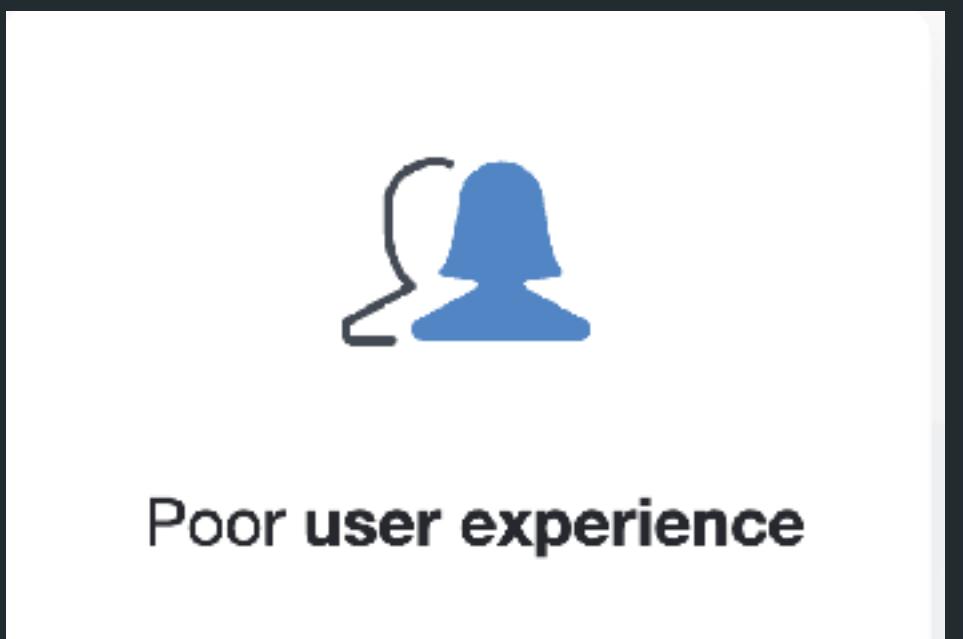
Ensure only trusted users on sanctioned, safe devices are authorized to access work apps and data.



Main issues With legacy VPN



+



+

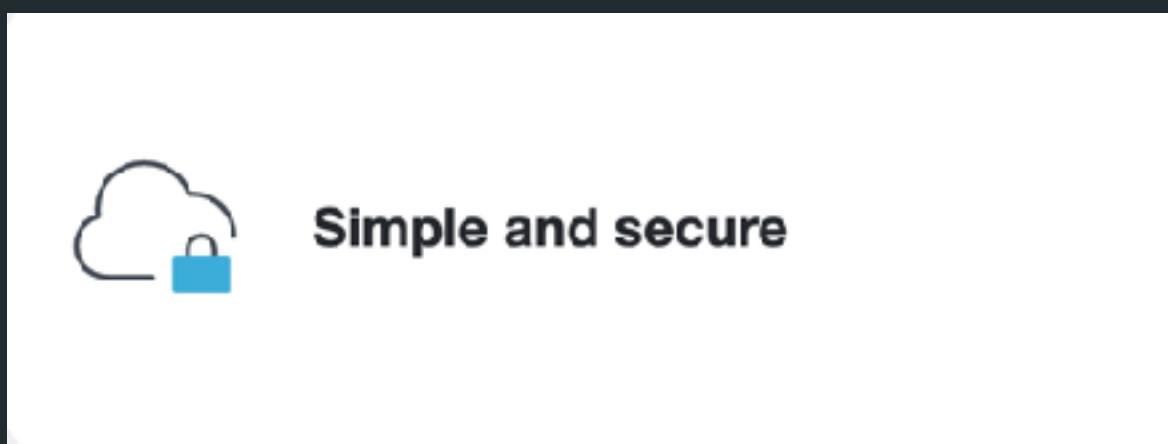


Inadequate **security**

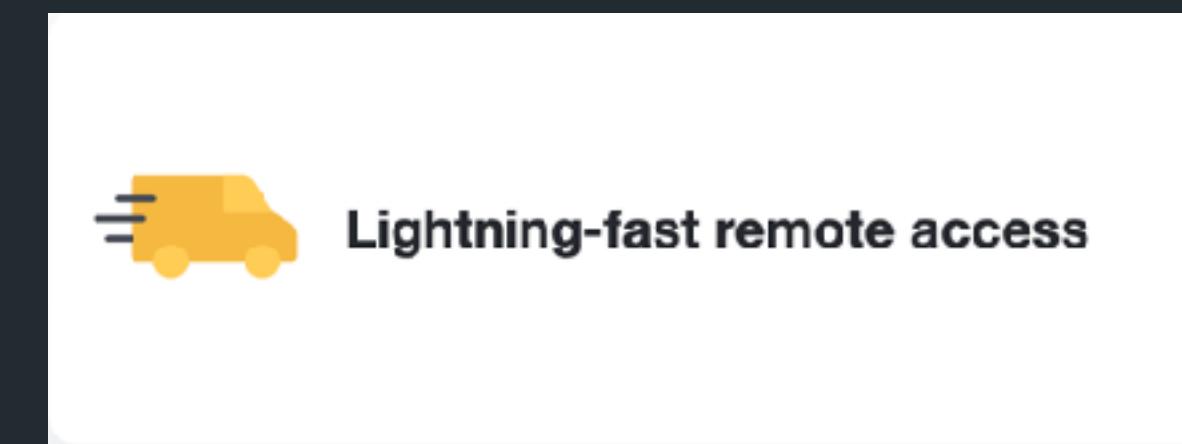


Key Benefits

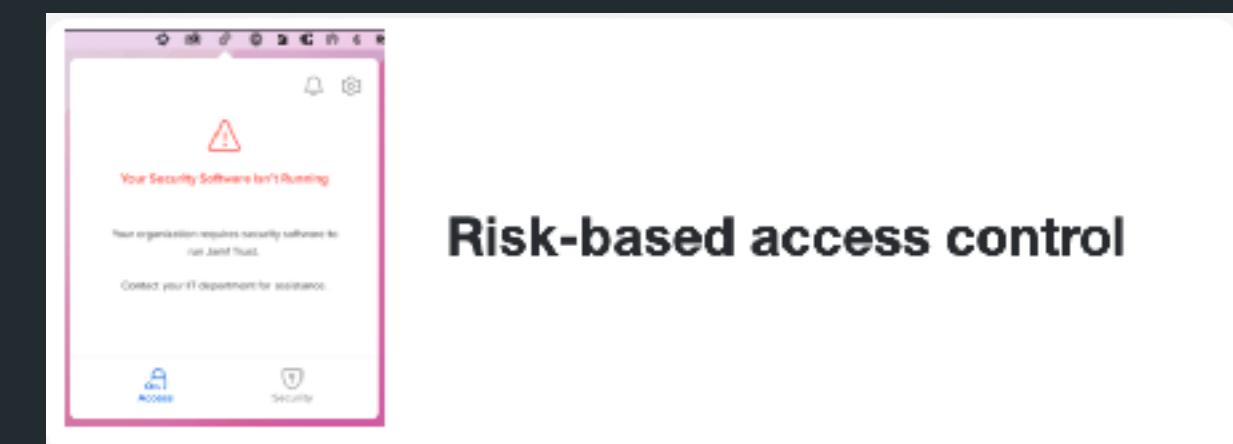
Zero Trust Network Access



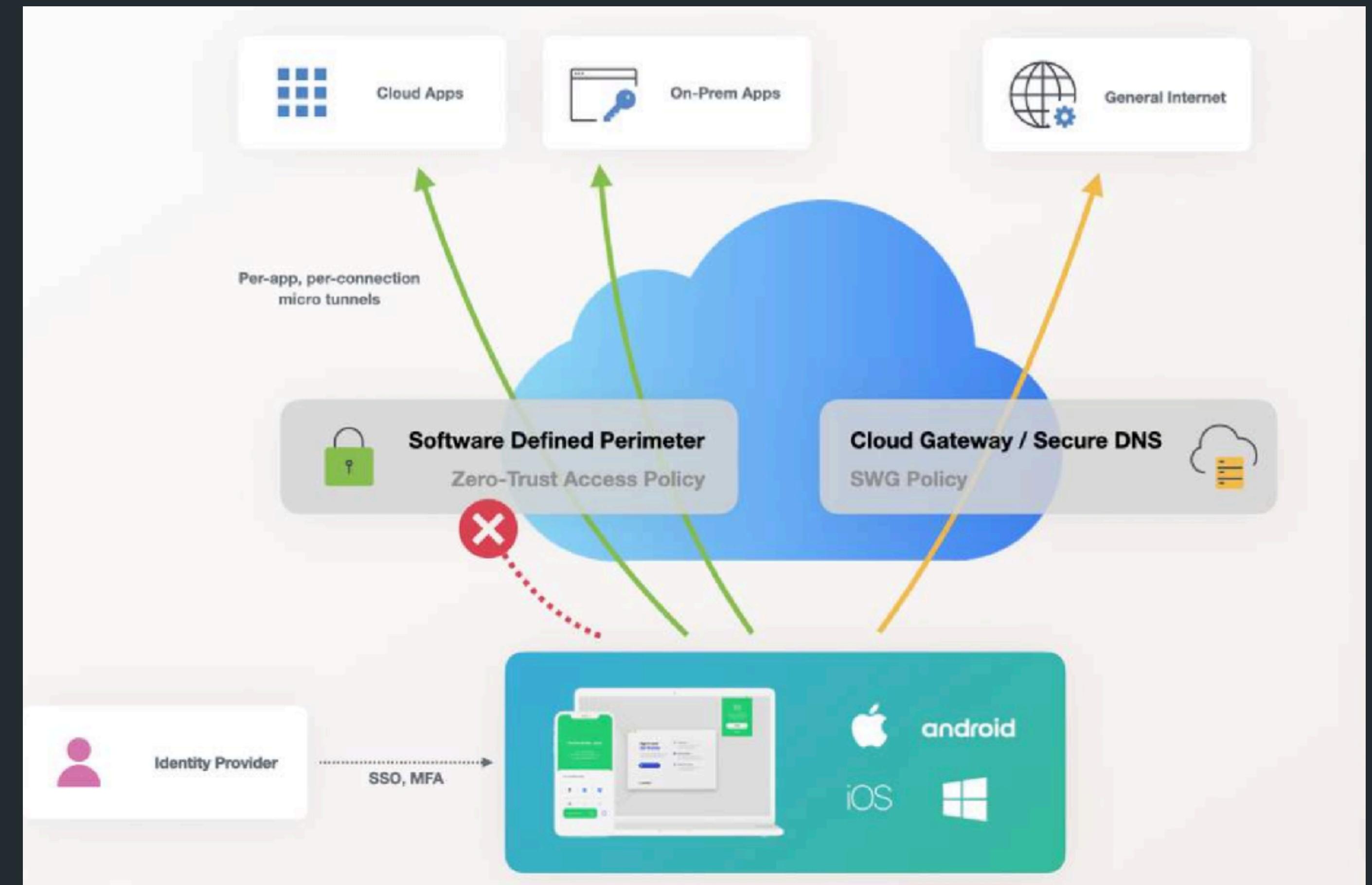
+



+



Scenarios: Dynamic Split Tunnel



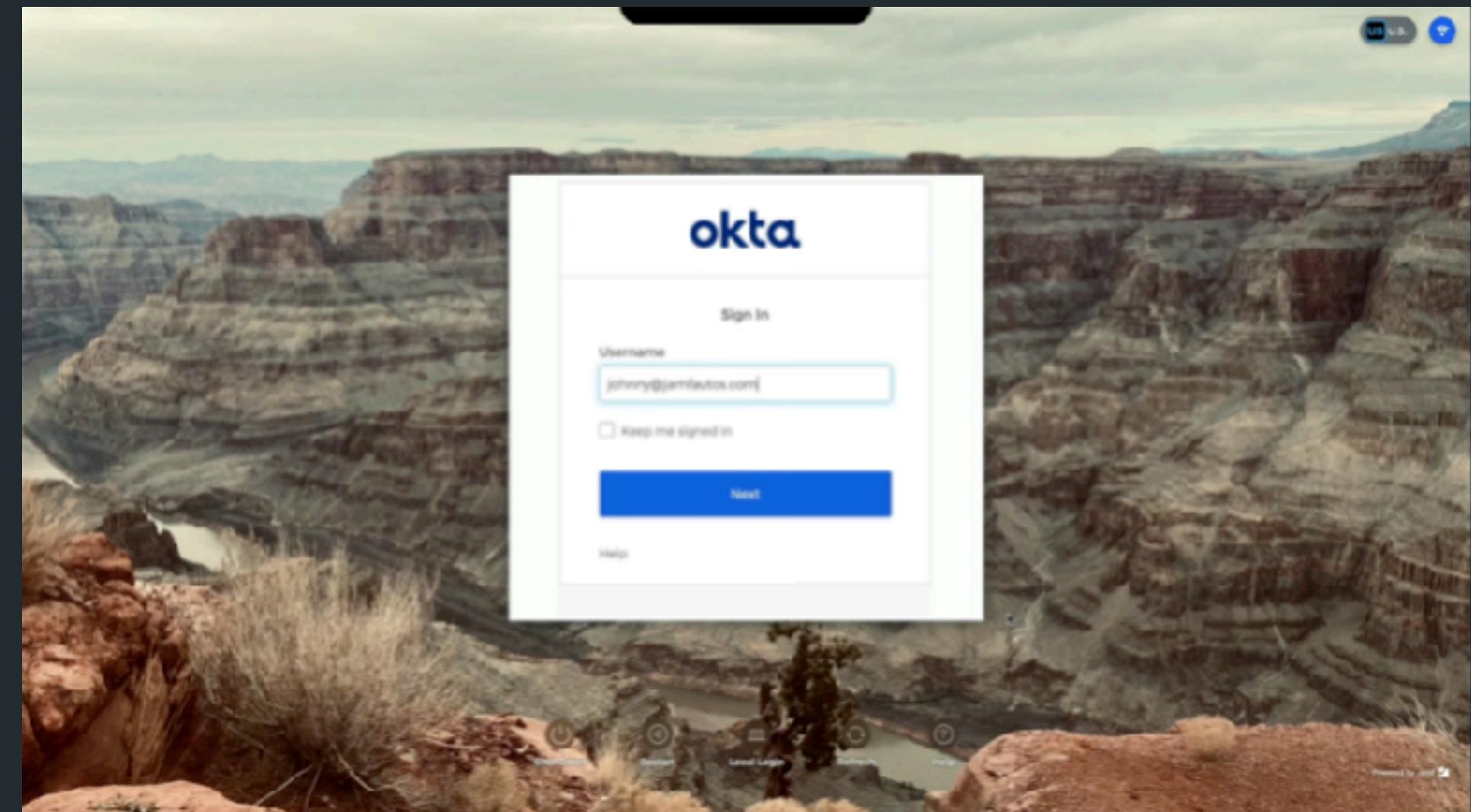
Tools + Requirements

- Included Tools
- Device, Identity Provider,
& collaboration requirements



Included Tools

- Jamf Connect
 - Login
 - Menu
 - Configuration
- Jamf Trust
- Jamf Security Cloud (Radar)



Requirements

Device/OS

- macOS 11
- iOS / iPadOS 15
- Windows 10
- Android 8

+

Identity Provider

- Azure
- Google
- Okta
- Many other IdPs

+

Collaboration

- Identity Team
- Security Team
- Network Team



Deployment

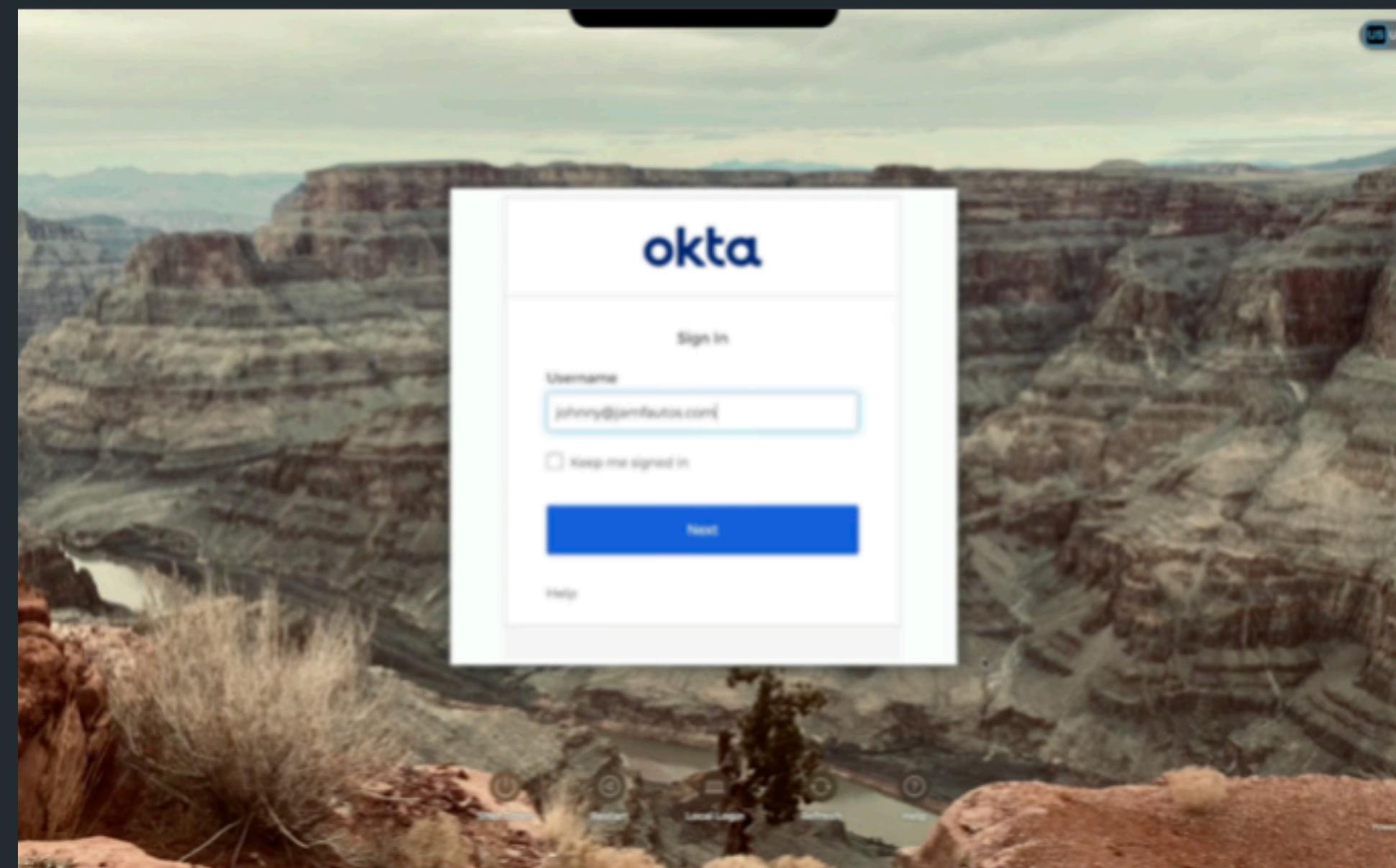
- Jamf Connect configuration for macOS
- Jamf Trust
- Jamf Security Cloud (Radar)



Deployment Step 1:

Connect Configuration

- Configuration settings
- App catalog
- Smart groups
- Pre Stage



Identity Provider

 **Jamf Connect - Okta as OIDC**

Active View Logs

[General](#) [Sign On](#) [Assignments](#) [Okta API Scopes](#) [Application Rate Limits](#)

Client Credentials [Edit](#)

Client ID: Ooa6f51dlkx5dlBoK1d7 [Edit](#)
Public identifier for the client that is required for all OAuth flows.

Client authentication: None Client secret Public key / Private key

Proof Key for Code Exchange (PKCE): Require PKCE as additional verification

General Settings [Edit](#)

APPLICATION



<https://jamf.it/jcIDP>



Mac Configuration Profiles

Jamf Connect Configuration

Identity provider: Okta (OIDC)

OIDC client ID: 0oa6f51dlkx5dIBoK1d7

ROPG client ID: 0oa6f

Tenant: jamfse-oie

You got tokens!

You have successfully authenticated to your Open ID Connect provider.

Auth endpoint: <https://jamfse-oie.oktapreview.com/oauth2/v1/authorize>

Token endpoint: <https://jamfse-oie.oktapreview.com/oauth2/v1/token>

User info endpoint: <https://jamfse-oie.oktapreview.com/oauth2/v1/userinfo>

Access token:

```
eyJraWQiOiJWZWtRN25yT2JCblRZOFZPLWR2SC1DWmxoMWJOZVBCd0
```

Refresh token:

```
eyJraWQiOiJuRGhzZXVpODNGeW4yRW8wal83elRxWndCQWI4ZjROODg
```

ID token:

```
eyJraWQiOiJuRGhzZXVpODNGeW4yRW8wal83elRxWndCQWI4ZjROODg
jti: ID.R0g6WZchffMy4IPseB7H8JkWBk8jLMAQeK2qykQnVts
aud: 0oa6f51dlkx5dIBoK1d7
at_hash: W-kiz5IKxRGsKS00AmDnRw
iss: https://jamfse-oie.oktapreview.com
sub: 00u4nnsi24jyMH98J1d7
email: user.connect@jamf.com
name: User Connect
```

Supported scopes:

```
["openid", "email", "profile", "address", "phone", "offline_access", "group"]
```

Save

The screenshot shows the Jamf Connect Configuration interface on a Mac. On the left, a sidebar lists various configuration profiles. The 'Okta as OIDC' profile is selected and highlighted. The main window displays configuration fields for an Okta identity provider, including the client ID and tenant. A central modal window titled 'You got tokens!' indicates a successful authentication. To the right, a 'Preview' pane shows the acquired OAuth2 tokens and their claims. The footer contains a copyright notice for Jamf from 2002-2023.

Mac Configuration Profiles

Identity provider | Login | Connect :: />

User creation

Initial password: Create a separate local password

User creation: Create all new users as local administrators
 Convert existing mobile accounts to local users
 Ignore roles DemobilizeUsers

Admin roles: groups

Admin attribute: macadmin

Short name: given_name

Full name: full_name

Account migration: Connect existing local users to a network account
 Hide the "Create new user" option from user interface

Hide users: username one, username two, username three

FileVault: Enable FileVault for first user
 Save FileVault recovery key
/usr/local/filevault

Keychain: Create Jamf Connect keychain

Authentication

ROPG client ID: 0oa6f51dlkx5dIBoK1d7

ROPG tenant: jamfse-oie.oktapreview.com

Discovery URL: https://example/.well-known/openid-configuration

Client secret: Your-Client-Secret

Success codes: ADDSTS50012

ROPG scopes: openid+profile+email+groups

Sign in

Sign in logo: /path/logo.png

Username label: E-Mail

Password label: Okta password

Window title: Sync your password with Okta

One-time password message: Enter your verification code

MFA excluded: push,question

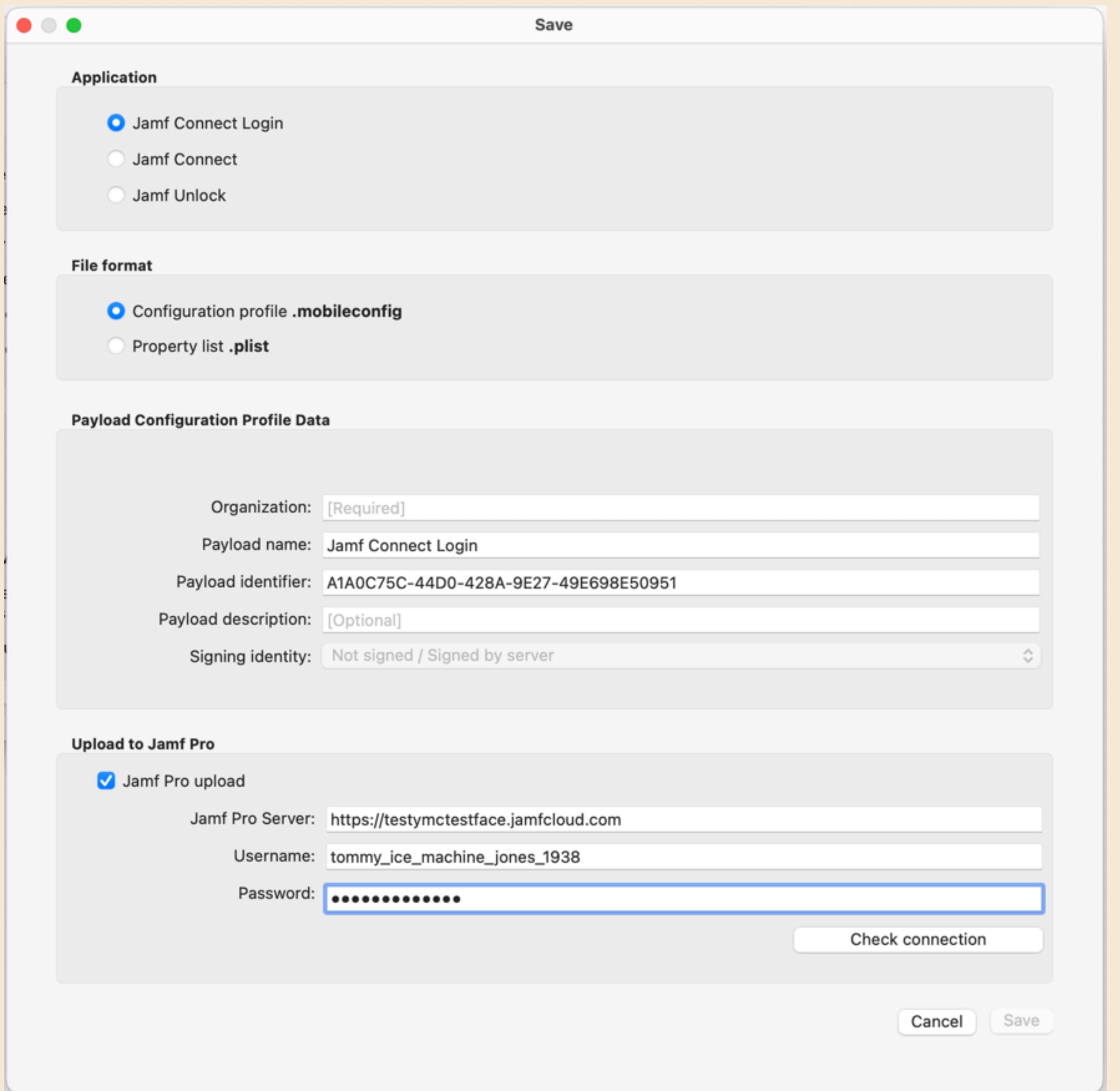
MFA rename: +



<https://jamf.it/jcstart>



Import to Jamf Pro



Deploy to existing machines

Smart Computer Groups and Mac Apps

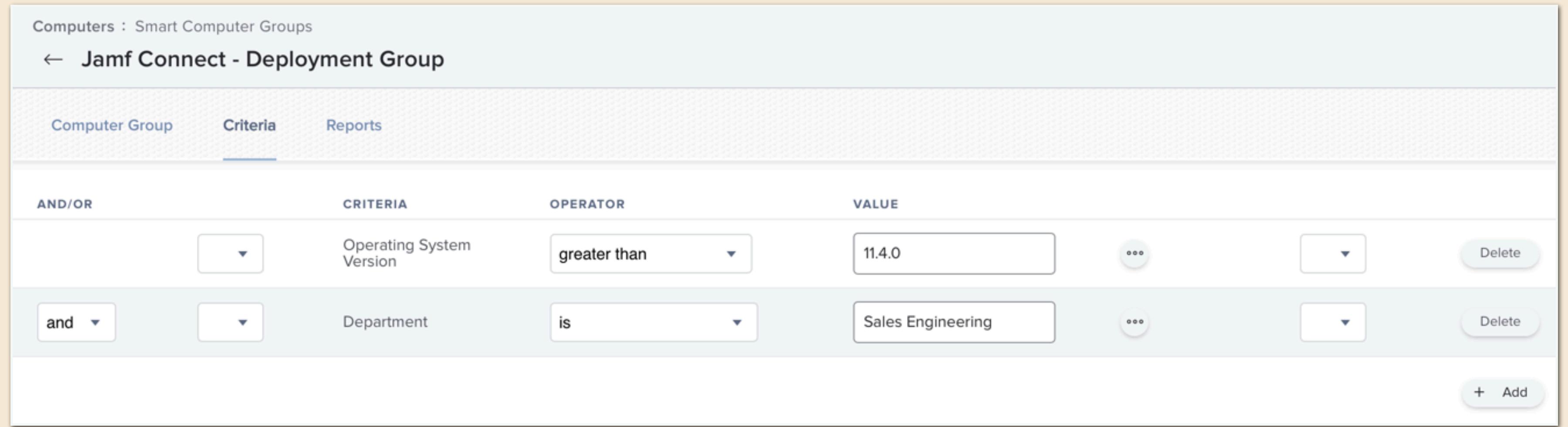
Computers : Smart Computer Groups

← Jamf Connect - Deployment Group

Computer Group Criteria Reports

AND/OR	CRITERIA	OPERATOR	VALUE	...	▼	Delete
	Operating System Version	greater than	11.4.0	...	▼	Delete
and	Department	is	Sales Engineering	...	▼	Delete

+ Add



Deploy to existing machines

Smart Computer Groups and Mac Apps

The screenshot shows the Jamf Connect Deployment interface for Mac Apps. On the left, there's a sidebar titled "Computers : Smart Computer Groups" with a "Jamf Connect - Deployment" section. The main area is titled "Computers" and "Mac Apps". It displays the "Jamf Connect Deployment" configuration settings.

Configuration settings:

- Display Name:** Jamf Connect (Required)
- Category:** None
- Target Group:** Jamf Connect - Deployment Group
- Distribution Method:** Install automatically (selected)
- Install supporting configuration profiles:** (checked) Automatically install supporting configuration profiles during deployment of this App Installer. Jamf recommends enabling this option.
 - (i) Jamf Pro will automatically install configuration profiles with all required settings to successfully deploy this App Installer. These profiles cannot be previewed or removed.
 - [More information ↗](#)

At the bottom right, there are "Cancel" and "Save" buttons.

Deploy via Zero Touch enrollment

Computers : PreStage Enrollments

← Jamf Connect with Okta (FileVault and LAPSUser workflow for macOS Catalina)

Options Scope

General

Account Settings

Create a local administrator account before the Setup Assistant
Local administrator account to create before the Setup Assistant for computers enrolled with this PreStage enrollment

Username: jamfManagement

Password:
Verify Password:

Hide managed administrator account in Users & Groups

Make the local administrator account MDM-enabled

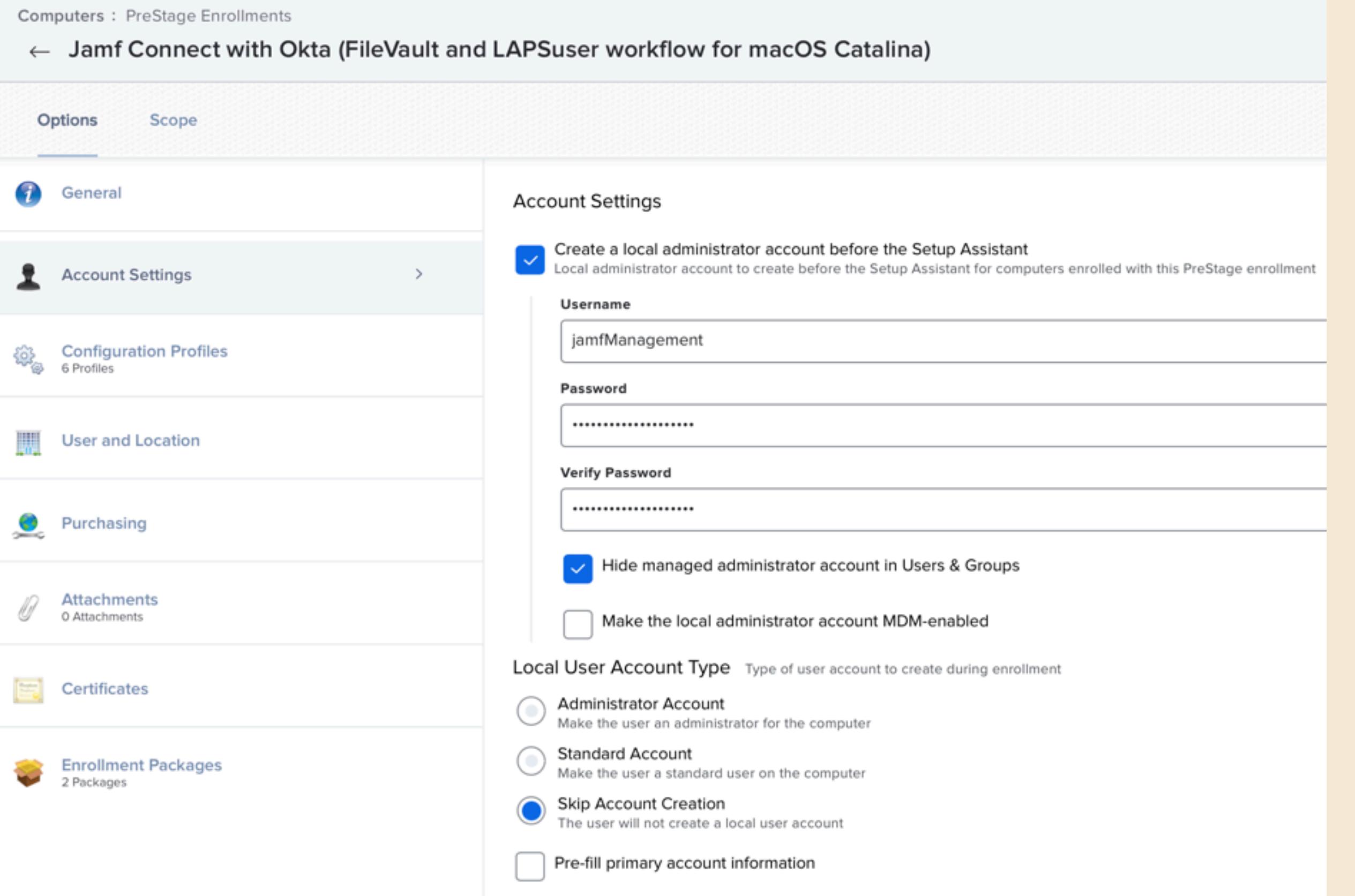
Local User Account Type Type of user account to create during enrollment

Administrator Account
Make the user an administrator for the computer

Standard Account
Make the user a standard user on the computer

Skip Account Creation
The user will not create a local user account

Pre-fill primary account information



Deploy via Zero Touch enrollment

Computers : PreStage Enrollments

← Jamf Connect

Options Scope

General Account Settings Configuration Profiles User and Location Purchasing Attachments Certificates Enrollment Packages

Computers : PreStage Enrollments

← Jamf Connect with Okta (FileVault and LAPSUser workflow for macOS Catalina)

Options Scope

General Account Settings Configuration Profiles User and Location Purchasing Attachments Certificates Enrollment Packages

Configuration Profiles

CONFIGURATION PROFILE SCOPE
To ensure the selected configuration profiles remain installed on computers after enrollment, ensure the scope of the configuration profile includes the computers in the scope of the PreStage enrollment.

NAME	SCOPE
Jamf Connect	
Jamf Connect - Deny Local	No scope defined
Jamf Connect - Enable FileVault for first user	Prestage - Jamf Connect with Okta (FileVault and LAPSUser workflow for macOS Catalina)
Jamf Connect - Enrollment Identity	Prestage - Jamf Connect with Okta (FileVault and LAPSUser workflow for macOS Catalina), Jamf Connect - First run done - notify mechanism complete excluded
Jamf Connect - LAPSUser for FileVault (macOS Catalina only)	Prestage - Jamf Connect with Okta (FileVault and LAPSUser workflow for macOS Catalina)
Jamf Connect - License	All computers
Jamf Connect - Okta - Version 2.0 or greater	1 computer, 2 computer groups
Jamf Connect - Run only once at launch	2 computer groups, Jamf Connect - First run done - notify mechanism complete excluded
Jamf Unlock - Enable and Require Pin	All computers
Test - Unlock	All computers
Jamf Trust	
Jamf Trust - Just Activation Part	No scope defined
Jamf Trust Bootstrap - macOS with Okta	Jamf Trust - macOS Okta - Private access, threat defense, secure DNS - valid email and prestige

Cancel Save

Deploy via Zero Touch enrollment

The screenshot shows the Jamf Connect configuration profile scope dialog. It includes a sidebar with navigation links like General, Account Settings, Configuration Profiles, User and Location, Purchasing, Attachments, Certificates, and Enrollment Packages. The main area displays a list of configuration profiles under the heading "Configuration Profiles". A callout box highlights the "CONFIGURATION PROFILE SCOPE" section, which contains the instruction: "To ensure the selected configuration profiles remain installed on computers after enrollment, ensure the scope of the configuration profile includes the computers in the scope of the PreStage enrollment". Below this, a list of profiles is shown with checkboxes. Several profiles are checked, including "Jamf Connect" and several "Jamf Connect" profiles under "Attachments".

Enrollment Packages

Distribution Point Distribution point to download the package(s) from

None

Cloud Distribution Point (Jamf Cloud)

JamfConnect.pkg

Deploy via Zero Touch enrollment

Computers : Smart Computer Groups

← Prestage - Jamf Connect with Okta (FileVault and LAPSUser workflow for macOS Catalina)

Computer Group Criteria Reports

AND/OR	CRITERIA	OPERATOR	VALUE	
▼	Enrollment Method: PreStage enrollment	is	Jamf Connect with Okta (F	⋮ Delete + Add



<https://jamf.it/jcstart>



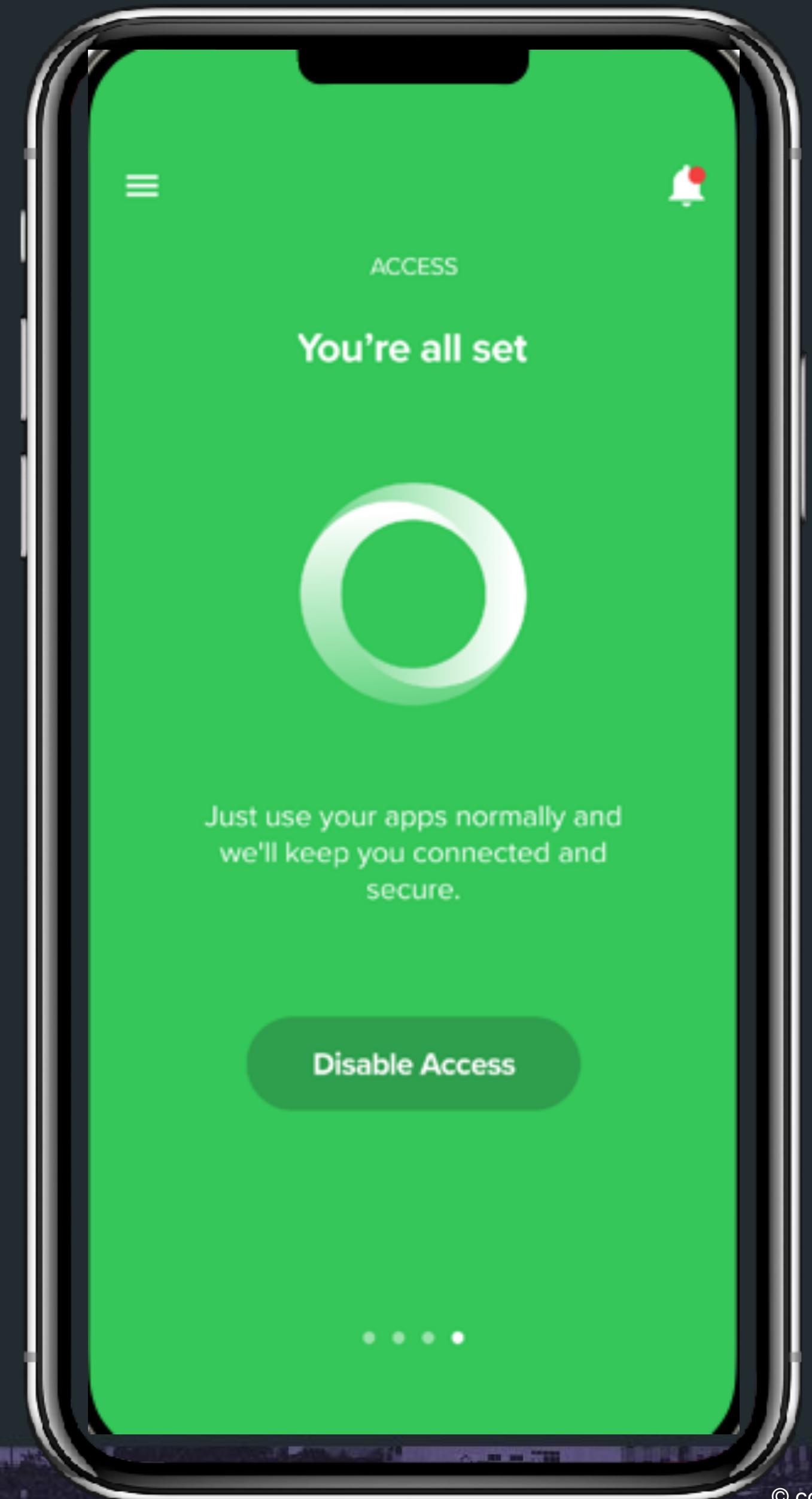


<https://jamf.it/jcstart>



Deployment Step 2: Jamf Trust

- VPP Jamf Pro
- Identity Provider Connection
- Activation Profile
- App Config, Config Profile



Computers : Mac Apps

← Jamf Trust ⓘ

General Scope Managed Distribution

Display Name Display name for the app

Jamf Trust

Enabled

Category Category to add the app to

Jamf Trust

Version Version of the app

11.15.0

Bundle Identifier Bundle identifier for the app

com.jamf.trust

Free
App is free

Schedule Jamf Pro to automatically check the App Store for app updates

Automatically update app description, icon, and version in Jamf Pro

App Store Country Or Region Country or region to use when syncing app with the App Store

United States

App Store Sync Time Time to sync with the App Store each day to automatically update app description, icon, and version in Jamf P

5 : 00 p.m.

Automatically Force App Updates

Automatically force updates for this app on computers (Managed Distribution)

Force App Update Force update for this app on computers (Managed Distribution)

Force Update

App URL URL of the app's App Store Preview page (e.g. "https://apps.apple.com/us/app/name-of-app/id123456789?mt=8")

https://apps.apple.com/us/app/jamf-trust/id1608041266?uo=4

Distribution Method Method to use for distributing the app

Install Automatically/Prompt Users to Install

Mobile Devices : Mobile Device Apps

← Jamf Trust

General Scope Managed Distribution App Configuration

Display Name Display name for the app

Jamf Trust

Enabled

Category Category to add the app to

Account Driven User Enrollment

Short Version Short Version of the app

11.4.0

Bundle Identifier Bundle identifier for the app

com.jamf.trust

Free
App is free

Distribution Method Method to use for distributing the app

Install Automatically/Prompt Users to Install

Display app in Self Service after it is installed

Require tethered network connection for app installation (iOS 10.3 or later)
Require the device to have a tethered network connection to download the app

Schedule Jamf Pro to automatically check the App Store for app updates
Automatically update app description, icon, and version in Jamf Pro

Automatically Force App Updates
Automatically force updates for this app on mobile devices (Managed Distribution or free apps)

Make app managed when possible
Make the app managed when managed app requirements are met

Convert unmanaged app to managed
Manage the app if already installed. If unsupervised, users must accept app management prompt. Conversion is not supported on devices enrolled via User Enrollment.

Remove app when MDM profile is removed

Prevent backup of app data

Allow users to remove app (iOS 14 or later)
Allows the user to remove this app from a device. The app is not removed from the App Catalog in Jamf Pro.



Dashboard

Reports

Devices

Policies

Integrations

UEM Connect

Access providers

Identity providers

Data streams

Risk API

Access gateways

Custom DNS

Settings

Manage your identity providers

Define and manage the connections to your identity providers. For more information see our [documentation](#).

Note: Currently, only Microsoft Azure, Okta and Google are supported. Other identity providers can be federated with Azure. Contact Jamf support for assistance.

Microsoft Microsoft identity services

1 of 1 tenants active

Add connection

Linked tenants

Connection

Status

Tenant ID

hello123.com



970823ed-e994-4ea4-8610-4a282c715d61

Actions

Okta Okta identity services

0 of 0 organizations active

Google Google identity services

1 of 1 organizations active

Add connection

Linked organizations

Status

Google tenant

Connection

Nicks Google workspace account



nmgilli123.com

Actions



Open enrollment

(i) You can use [identity-based provisioning](#) with this activation profile. This allows users to activate via other services.

Shareable link

You can distribute the shareable link or QR code via email or another text messaging service to allow end users to activate their devices.

<https://e.wandera.com/vfm9j7on>



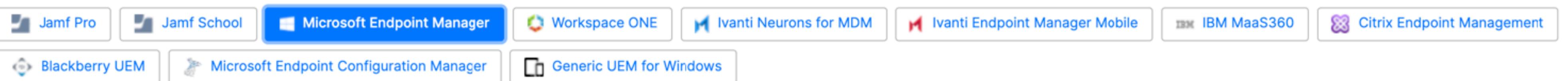
Managed deployment

You can deploy activation profiles to managed devices via your UEM solution or package manager.

Configuration varies by device platform and UEM solution.

(i) To manage device lifecycle settings and sync additional device metadata, configure [UEM Connect](#).

Select your UEM



Select your OS



iOS and iPadOS supervised (16 or later) on Microsoft Endpoint Manager

(i) Only supervised devices on iOS and iPadOS 16 or later support IP address filtering and per-site usage reporting.

Push a traffic vectoring profile below to your Apple devices. For more information, see our [documentation](#) on Apple device configuration.

Deploy and configure Jamf Trust app using the keys and values below. See our [documentation](#) for more information on how to deploy Jamf Trust to iOS and iPadOS devices.



Configuration profiles



Computers : Configuration Profiles

← Jamf Trust Bootstrap - macOS with Okta

Options Scope

Search... General

Name Display name of the profile
Jamf Trust Bootstrap - macOS with Okta

Description Brief explanation of the content or purpose of the profile

Application & Custom Settings ▾
Payloads configured: 6

Upload

Certificate
1 payload configured

DNS Settings
1 payload configured

VPN
1 payload configured

Mobile Devices : Mobile Device Apps

← Jamf Trust

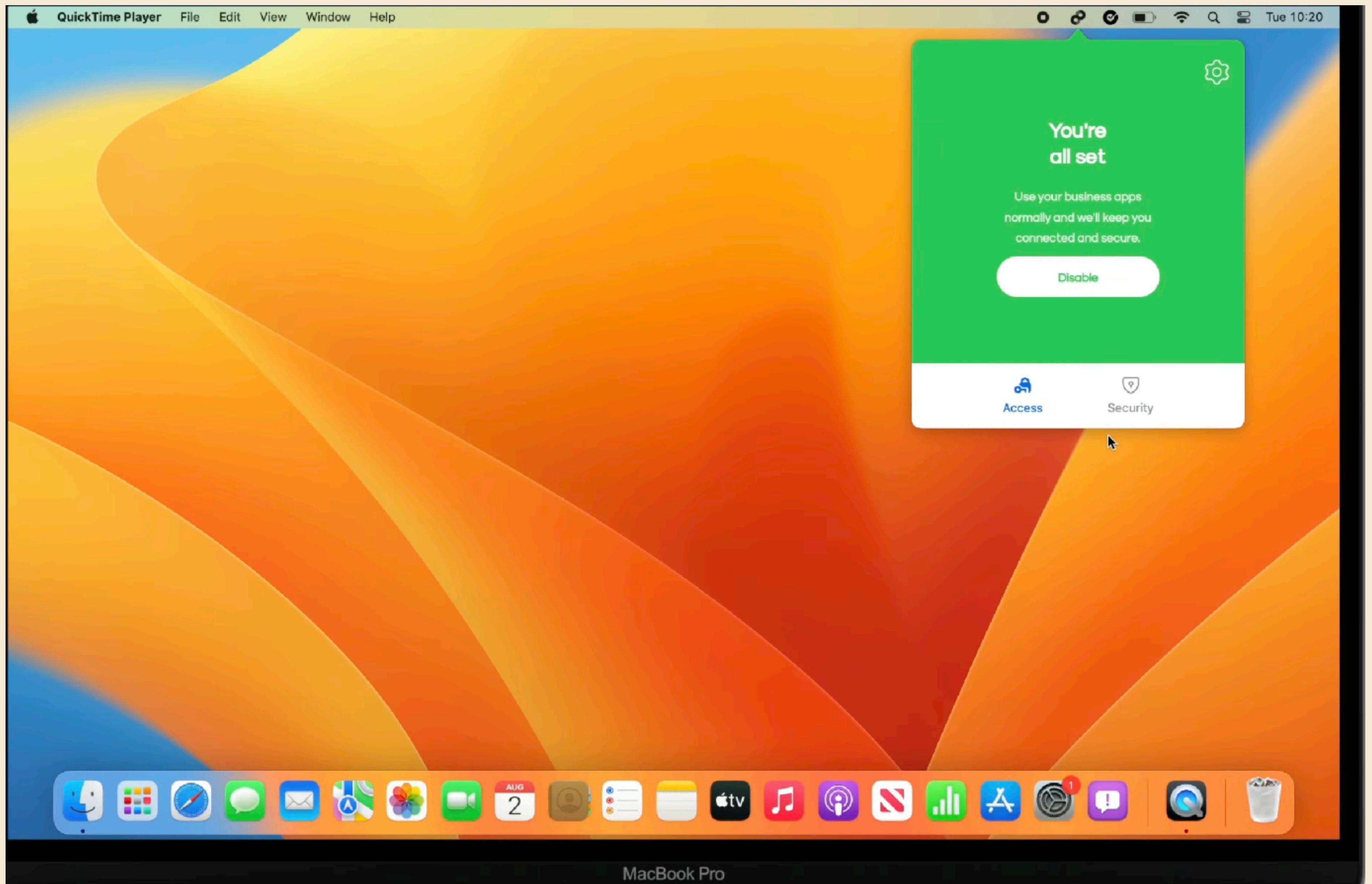
General Scope Self Service Managed Distribution App Configuration

Preferences Configuration dictionary to be applied to the app on mobile devices with iOS 7 or later

```
<dict>
<key>activationType</key>
<string>AP</string>
<key>activationProfileUrl</key>
<string>https://e.wandera.com/iI9xjvj7</string>
<key>apiKey</key>
<string>9c7c8704-e51b-412d-9a37-c308b73d25cb</string>
<key>secretKey</key>
<string>jddxkO6hdFlyOnQFMsqbECZnoio956Y5qlbiKA6rUIFpnLtjaOqkZc+6YrdYjpuoYsbm9xcaMQGnPFigDu7igg==</string>
<key>externalId</key>
<string>$UDID</string>
<key>email</key>
<string>$EMAIL</string>
<key>firstName</key>
<string>$FULLNAME</string>
</dict>
```

① For help generating the PLIST file for preferences, use the [AppConfig Generator](#)





MacBook Pro

© copyright 2002-2023 Jamf

2023
JAMF
UNIVERSE

Deployment Step 3: Jamf Security Cloud (Radar)

- SaaS + Enterprise
- Least Privilege Access
- Risk-based access control
- Routing options
- Reporting

Access policy
Define and manage the SaaS and Enterprise applications used by your organization. Once defined, these applications are used for defining policy and visibility in reporting.

New app policy Export | Edit selected

<input type="checkbox"/>	Application	Category	App type	Group assignments	Routing	Risk-based access	Edit
<input type="checkbox"/>	 Adobe	Uncategorized	SaaS	Agents and 23 more ?	Nearest Data Center	Medium and lower	Edit
<input type="checkbox"/>	 Atlassian Cloud	Uncategorized	SaaS	Everyone	Shared IP Pool: North America - USA East	Medium and lower	Edit
<input type="checkbox"/>	 BlueJeans	Uncategorized	SaaS	Everyone	Nearest Data Center	Medium and lower	Edit
<input type="checkbox"/>	 Box	Technology	SaaS	Directors and 2 more ?	Nearest Data Center	Medium and lower	Edit
<input type="checkbox"/>	 DocuSign	Uncategorized	SaaS	None	Nearest Data Center	Medium and lower	Edit
<input type="checkbox"/>	 Facebook	Social	SaaS	Marketing	Shared IP Pool: Europe - UK	Low and secure	Edit
<input type="checkbox"/>	 File Server	Technology	Enterprise	Everyone	Nearest Data Center	Off	Edit
<input type="checkbox"/>	 GitHub	Productivity	SaaS	Market	Default device routing	Medium and lower	Edit
<input type="checkbox"/>	 Google Apps	Business & Industry	SaaS	Everyone	Default device routing	Low and secure	Edit
<input type="checkbox"/>	 Microsoft 365	Technology	SaaS	Directors	Nearest Data Center	Medium and lower	Edit

1 2 3 4 5 6 7 >



[Return to Access policies](#) < Select app type

Cancel

New app policy



SaaS Apps

Applications hosted by software vendors in the public cloud.



Create policy



Enterprise Apps

Applications operated on your own infrastructure on-premise, in a data center, or private cloud.



Create policy

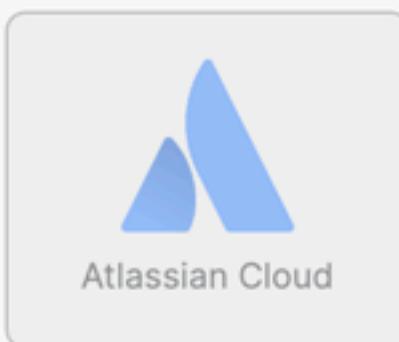


Add application

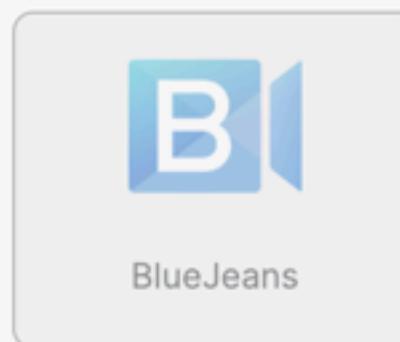
Select a pre-defined app...



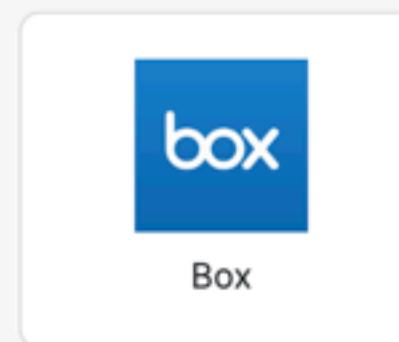
Adobe



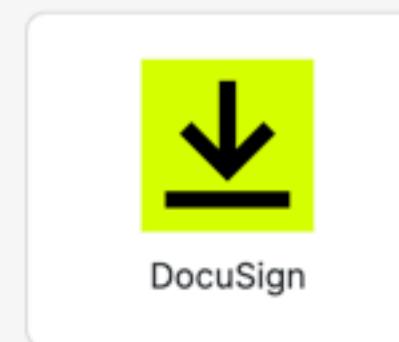
Atlassian Cloud



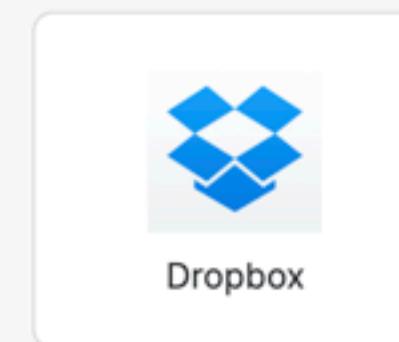
BlueJeans



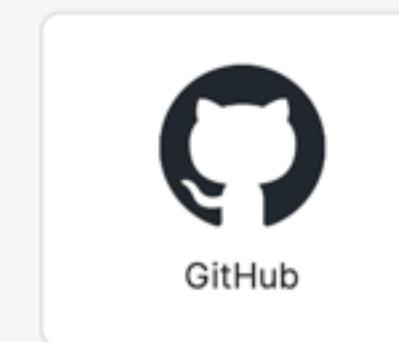
Box



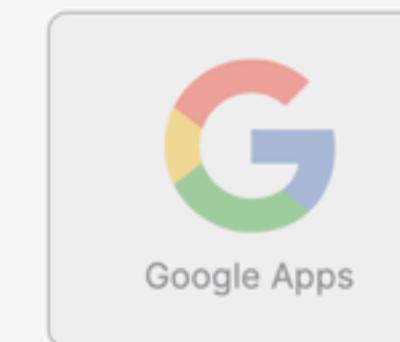
DocuSign



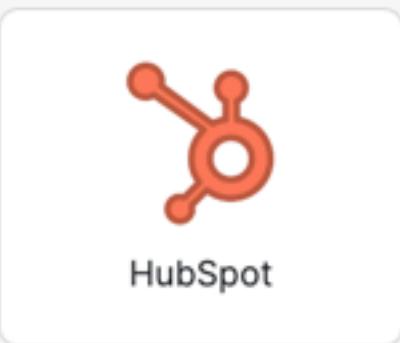
Dropbox



Github



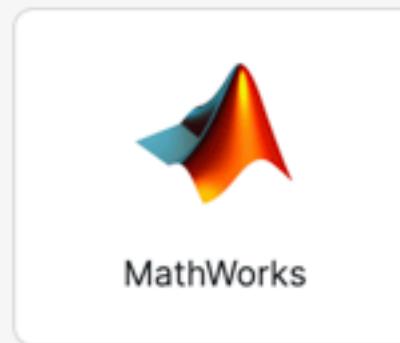
Google Apps



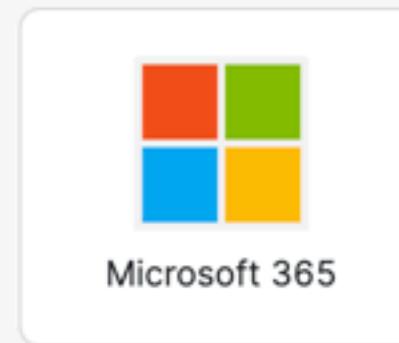
HubSpot



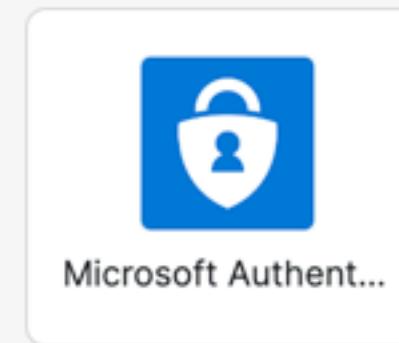
MailChimp



MathWorks



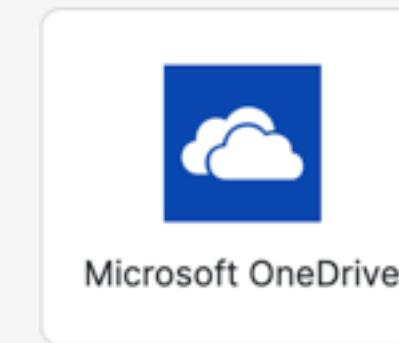
Microsoft 365



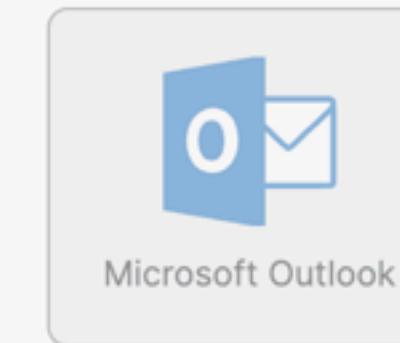
Microsoft Authent...



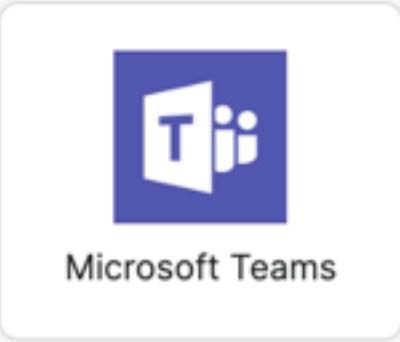
Microsoft Endpoi...



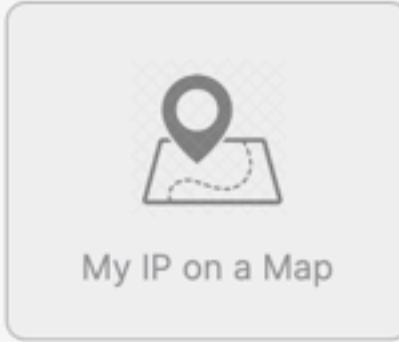
Microsoft OneDrive



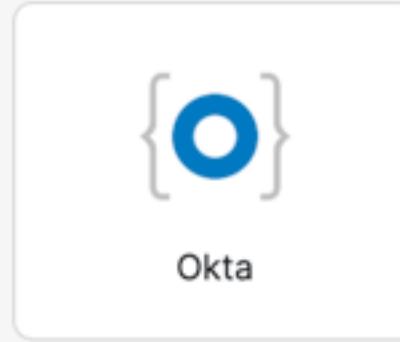
Microsoft Outlook



Microsoft Teams



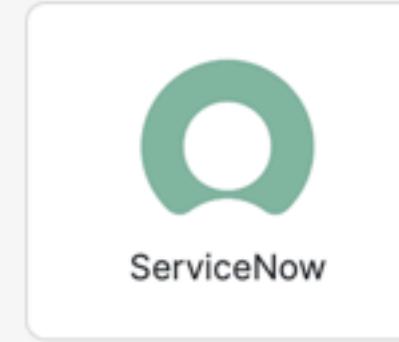
My IP on a Map



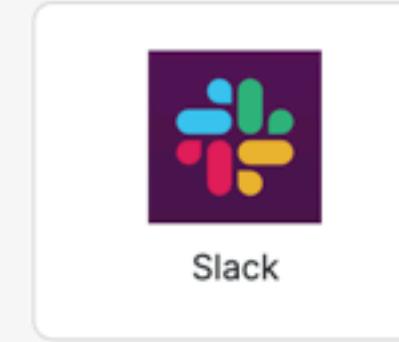
Okta



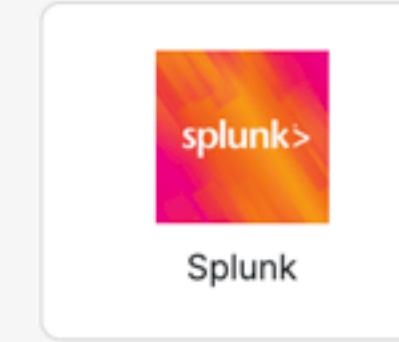
Salesforce



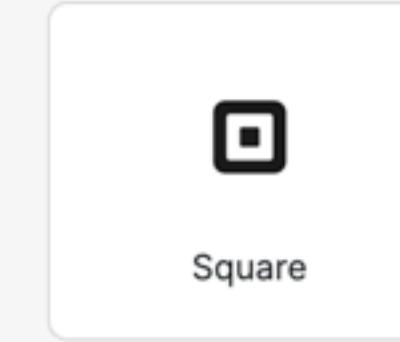
ServiceNow



Slack



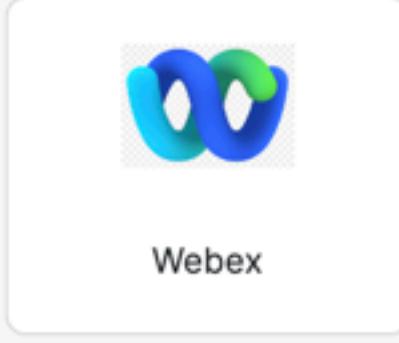
Splunk



Square



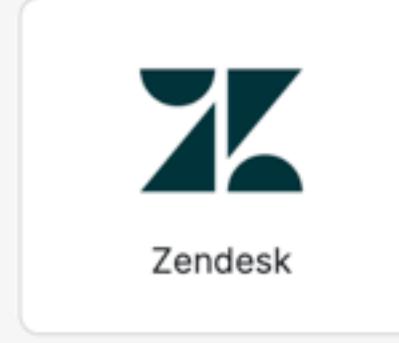
Twilio



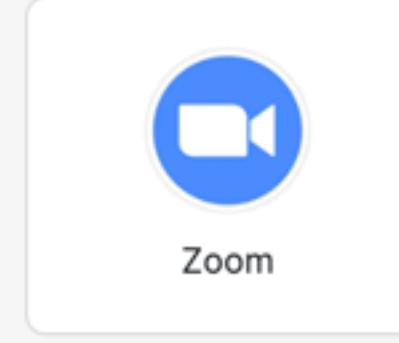
Webex



Workday



Zendesk



Zoom



Access policy

Define and manage the SaaS and Enterprise applications used by your organization. Once defined, these applications are used for defining policy and visibility in reporting.

New app policy							Export	Edit selected
<input type="checkbox"/>	Application	Category	App type	Group assignments	Routing	Direct IPs	Custom hostnames	⋮
<input type="checkbox"/>	AS Apache site	Technology	Enterprise	Everyone	Nick's RSA Gateway IPSec	10.0.10.146/32		Edit
<input type="checkbox"/>	EA Enterprise App	Technology	Enterprise	Contractors	Nick's RSA Gateway IPSec	10.0.10.0/24	*.company.com and 1 more ?	Edit
<input type="checkbox"/>	RA RSA app (hostname)	Uncategorized	Enterprise	Everyone	Nick's RSA Gateway IPSec		*.jamfse.io	Edit



Status
Active

Last Status Change
10 days ago
Jul 20, 2023 15:21

Last Edited
last year
May 18, 2022 15:34

[Return to Access gateways](#) < [Gateway detail](#)

[Status](#) [Settings](#)

Nick's RSA Gateway

ID	EGRESS REGION	TYPE OF EGRESS	EMAIL ALERT NOTIFICATIONS
b6be	North America - USA West	IPSec	N/A

New DNS zone

ⓘ Misconfiguring a zone may result in lost connectivity to some or all of your private applications and workloads for your end users. If in doubt, refer to our documentation for more information.

Zone name
JNUC 2023

Domains
Define the domains that will match this DNS zone. You can specify subdomains with a wildcard, but you must explicitly include the parent domain as well. That is, "company.com" will only cover the parent domain, and "*company.com" will only cover the subdomains.

Domain name	
*.company.com	Remove
*.jamfse.io	Remove
<input type="text"/>	Add new domain

Authoritative name servers
Specify the IP addresses of your authoritative name servers that are able to resolve hostnames for the domains defined in this zone. Ensure that each name server is reachable via the specified gateway.

Name server IP address	Reachable via
192.0.1.0	Nick's dedicated gateway

Edit Atlassian Cloud

General Traffic matching Users and groups **Security** Routing

Device risk-based access control



Access requires device risk validation

Deny access to devices with at least the following risk level:

High

Device push notifications

Notify users when access is denied

Restrict access when Jamf Trust is disabled



(i) This feature works only for managed Apple devices with the network threat protection profile installed (using DNS over HTTPS)

Device push notifications

Notify users when access is denied



Web content

Mode ⓘ	Threat category	Severity ⓘ	Affects device risk ⓘ	Alerts ⓘ	Auto response
<input checked="" type="checkbox"/> Active	Phishing ⓘ		<input checked="" type="checkbox"/> High	User, Admin	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Active	Data leaks		<input checked="" type="checkbox"/> Medium	User	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Active	Malware network traffic ⓘ	1 ignored	<input checked="" type="checkbox"/> Medium	User, Admin	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Active	Cryptojacking ⓘ		<input checked="" type="checkbox"/> Medium	User	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Active	Spam ⓘ		<input checked="" type="checkbox"/> Medium	User	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Active	Third-party app store traffic ⓘ		<input checked="" type="checkbox"/> Low	User	<input checked="" type="checkbox"/>

App

Mode ⓘ	Threat category	Severity ⓘ	Affects device risk ⓘ	Alerts ⓘ	Auto response
<input checked="" type="checkbox"/> Active	Malware		<input checked="" type="checkbox"/> High	User	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Active	Device admin app installed ⓘ		<input checked="" type="checkbox"/> Medium	User	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Active	Sideloaded app installed ⓘ		<input checked="" type="checkbox"/> Medium	User	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Active	Third-party app stores installed ⓘ		<input checked="" type="checkbox"/> Low	User	<input checked="" type="checkbox"/>

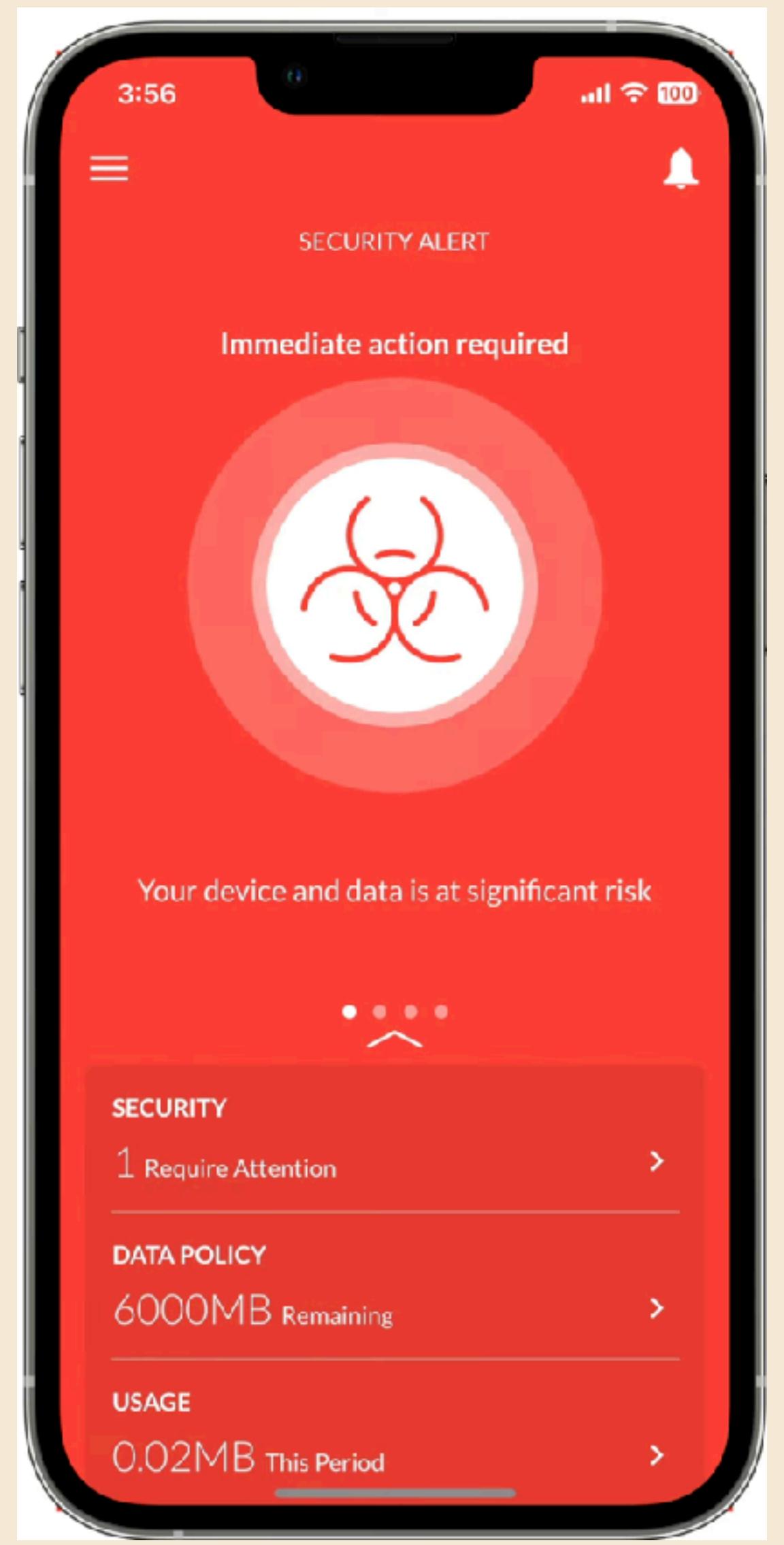
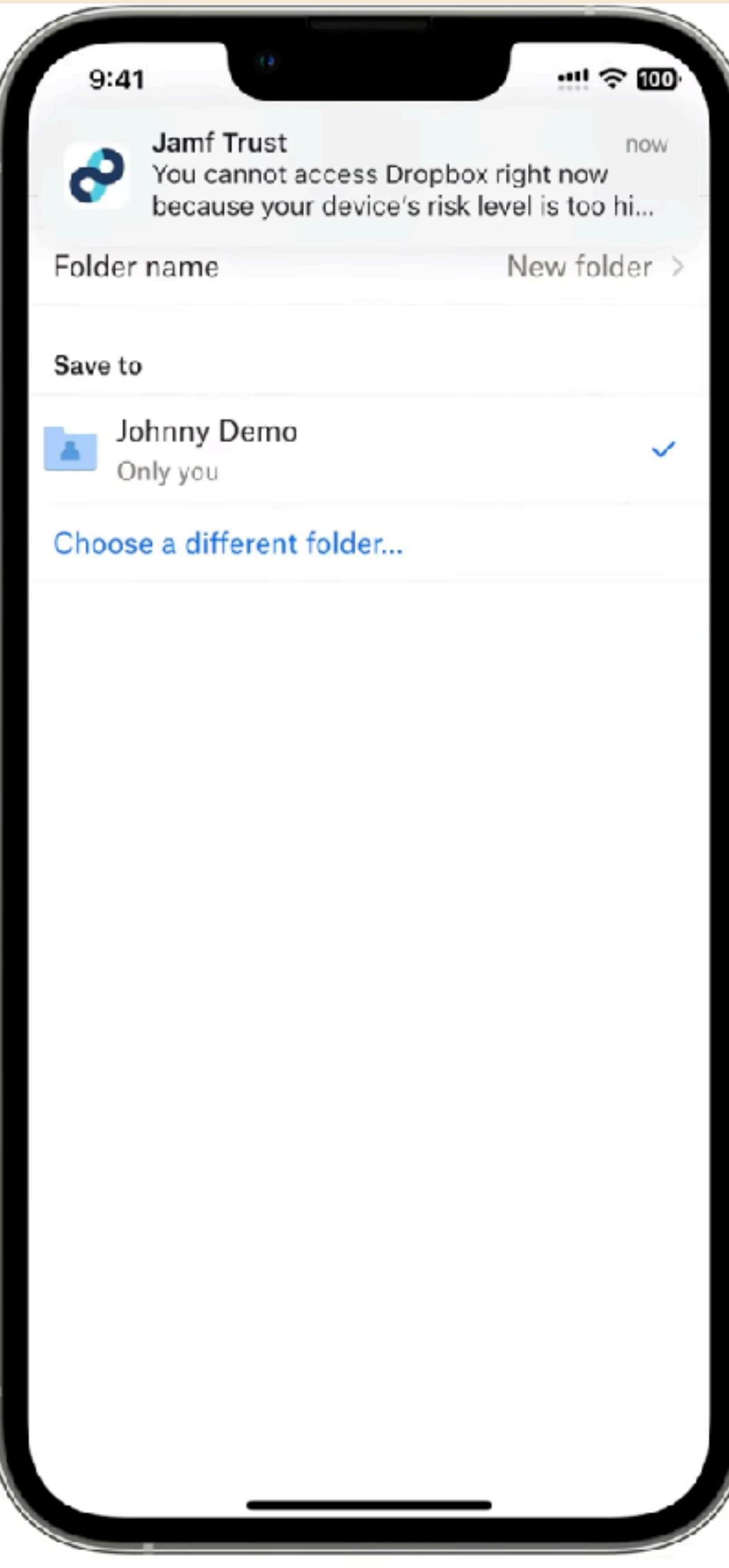
Network

Mode ⓘ	Threat category	Severity ⓘ	Affects device risk ⓘ	Alerts ⓘ	Auto response
<input checked="" type="checkbox"/> Active	Dangerous certificate ⓘ		<input checked="" type="checkbox"/> High	User	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Active	Adversary-in-the-Middle		<input checked="" type="checkbox"/> High	User	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Active	Risky hotspots ⓘ		<input checked="" type="checkbox"/> Medium	User	<input checked="" type="checkbox"/>

Device

Mode ⓘ	Threat category	Severity ⓘ	Affects device risk ⓘ	Alerts ⓘ	Auto response
<input checked="" type="checkbox"/> Active	Jailbreak ⓘ		<input checked="" type="checkbox"/> High	User, Admin	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Active	Out-of-date OS ⓘ	1 ignored	<input checked="" type="checkbox"/> High	User, Summary	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Active	Vulnerable OS (major) ⓘ		<input checked="" type="checkbox"/> High	User, Admin	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Active	Vulnerable OS (minor) ⓘ		<input checked="" type="checkbox"/> High	User	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Active	User password disabled ⓘ		<input checked="" type="checkbox"/> Medium	Select alert(s)	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Active	App inactivity ⓘ		<input type="checkbox"/>	Select alert(s)	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Active	Device encryption disabled ⓘ		<input checked="" type="checkbox"/> Medium	User	<input checked="" type="checkbox"/>





Edit Atlassian Cloud

General Traffic matching Users and groups Security Routing

Application Traffic Routing

Indicate how authorized devices should route their traffic to reach this application's servers. For more information see our [documentation](#).

To create and manage secure routes to private infrastructure, such as IPSec tunnels, use the [Infrastructure Integrations](#) settings.

Encrypt and route via ZTNA:

Nearest data center

Nearest data center

Nick's dedicated gateway Dedicated

Nick's RSA Gateway IPSec

Routing mode

Specify the traffic routing mode that

Only select IPv4 if the end-

on end-user devices

Edit Apache site

General Traffic matching Users and groups Security Routing

Application Traffic Routing

Indicate how authorized devices should route their traffic to reach this application's servers. For more information see our [documentation](#).

To create and manage secure routes to private infrastructure, such as IPSec tunnels, use the [Infrastructure Integrations](#) settings.

Encrypt and route via ZTNA:

Default device routing

Routing mode

Specify the traffic routing mode that

Only select IPv4 if the end-

Nick's RSA Gateway

Nearest data center

Nick's dedicated gateway Dedicated

Nick's RSA Gateway IPSec

Shared IP Pool: Asia - Hong Kong

Shared IP Pool: Asia - India

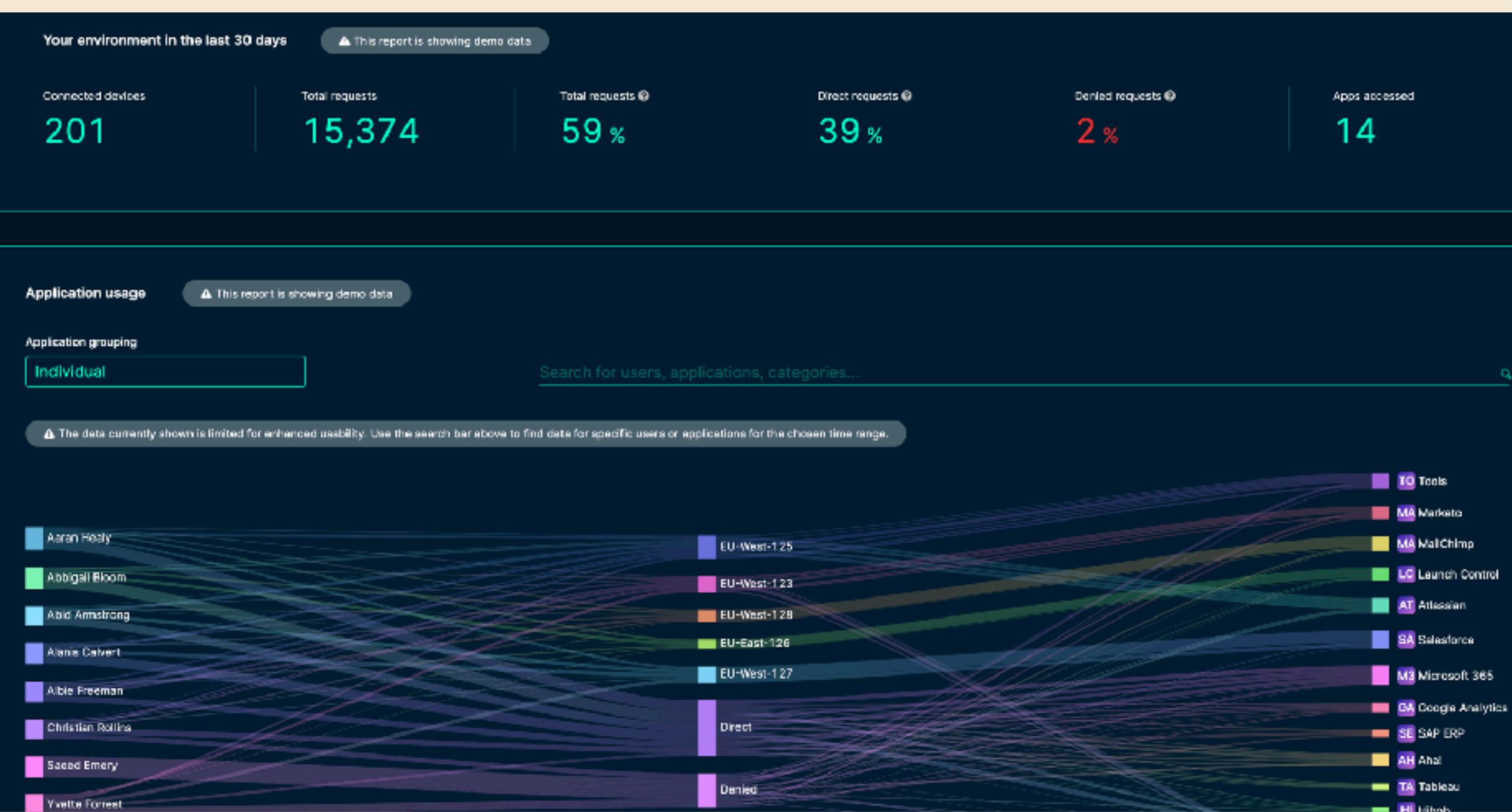
Shared IP Pool: Asia - Japan



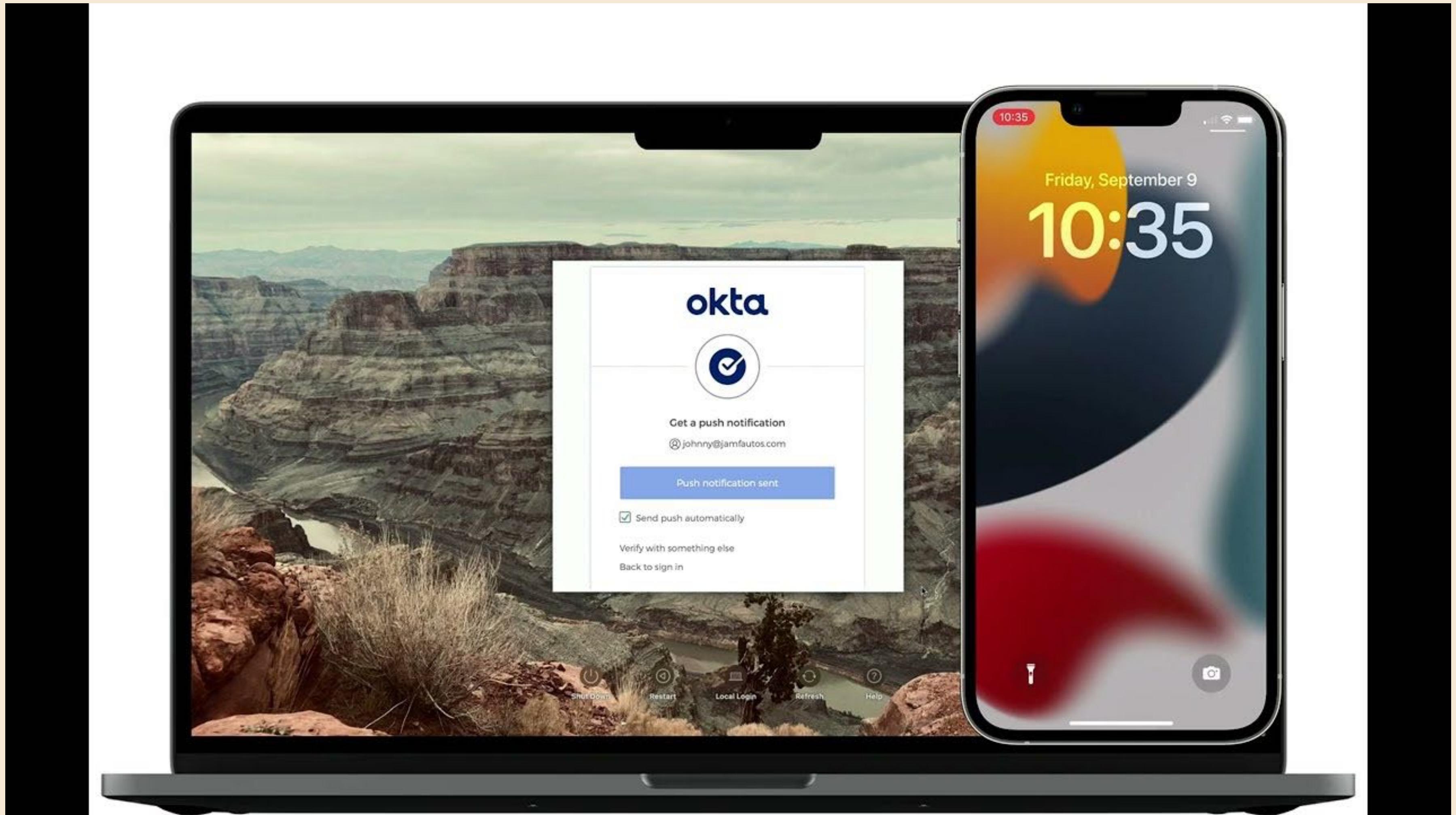
Event log

Jul 24, 2023 - Jul 31, 2023

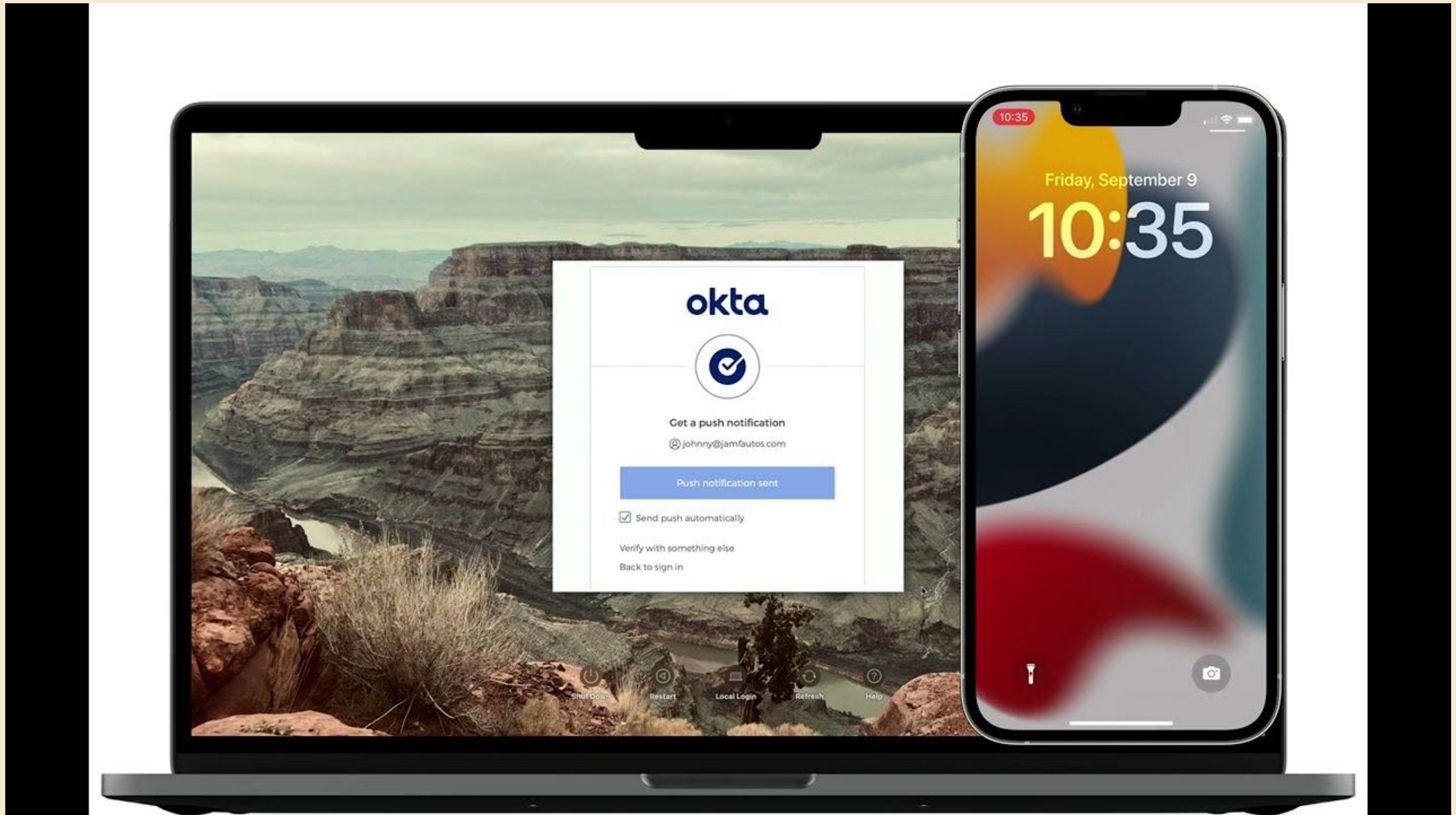
Timestamp Application User Device Route Action Hostname

+ Jul 31, 2023 14:55:05	Google Analytics	Jimmy Erickson	Windows 10	Direct	Allow	analytics.google.com
+ Jul 31, 2023 14:48:40	Marketo	Aaron Healy	Apple Mac	EU-East-124	Allow	app-icon63.marketo.com
+ Jul 31, 2023 14:40:49	Microsoft 365	Tammy House	Windows 10	Direct	Allow	outlook.office.com
+ Jul 31, 2023 14:22:56	Salesforce	Zahraa Collins	Other Android	EU-West-126	Allow	help.salesforce.com
+ Jul 31, 2023 14:16:22	Hacksw	Jolyon Meyer	Windows 10	EU-East-125	Allow	
+ Jul 31, 2023 14:11:33	Invision	Lucinda Barton	Apple	Direct	Allow	invisionapp.com
+ Jul 31, 2023 14:06:10	Google Analytics	Murray Travers	Other Android	Direct	Allow	analytics.google.com
+ Jul 31, 2023 14:04:34	Tableau	No Lloyd	Other Android	Direct	Allow	tableau.com
+ Jul 31, 2023 14:02:02	Tools	Jameson Mill	phone	EU-West-128	Allow	tools.wandera.net
+ Jul 31, 2023 14:01:24	Atlassian	Caelan Dorsey	Apple	EU-East-124	Allow	snapp.atlassian.net
+ Jul 31, 2023 14:00:28	Atlassian	Tyson Mackie	Windows 10	EU-East-124	Allow	
+ Jul 31, 2023 13:56:29	Launch Control	Jamal Hall	Apple Mac	EU-East-126	Allow	launch-control-console.osx.wandera.net
+ Jul 31, 2023 13:55:20	Microsoft 365	Elaia Whitmore	Apple Mac	Direct	Allow	outlook.office.com
+ Jul 31, 2023 13:50:47	Salesforce	Johanna Rowe	Apple Mac	EU-West-126	Allow	help.salesforce.com
+ Jul 31, 2023 13:49:34	Ahal	Mani Rivera	phone	Direct	Allow	
+ Jul 31, 2023 13:47:23	Invision	Jennie Sadler	phone	Direct	Allow	invisionapp.com


Demo



Demo





<https://jamf.it/jnuctrust>



Jamf Connect: Identity and Secure Access

- What is Jamf Connect today?
- Tools + Requirements
- Deployment
- Demo



Thank you for
listening!

