2023 JNUC

AUSTIN, TX

Jamf and Okta Device Trust

okta

okta

Jon Lehtinen

Okta

Sean Rabbitt

Jamf

2023 JNUC

Jamf and Okta Device Trust

okta

- What is Okta Device Trust
- The Okta at Okta experience
- Jamf Pro setup and deployment
- End user experience
- How does this affect Jamf Connect

2023 JNUC

Okta on Okta (at Okta)

okta

2023 JNUC

Okta on Okta (at Okta)

okta

Enable the Business

2023 JNUC

Okta on Okta (at Okta)

okta

Enable the Business

Evolve the Product

Okta on Okta (at Okta)

okta

Enable the Business

Evolve the Product

Showcase the Platform

okta

What is Okta Device Trust

2023 JNUC

What is Okta Device Trust

okta

Device Registration

- Okta Verify installed
- User trust established through authentication

What is Okta Device Trust

okta

Device Registration

- Okta Verify installed
- User trust established through authentication

Device Management

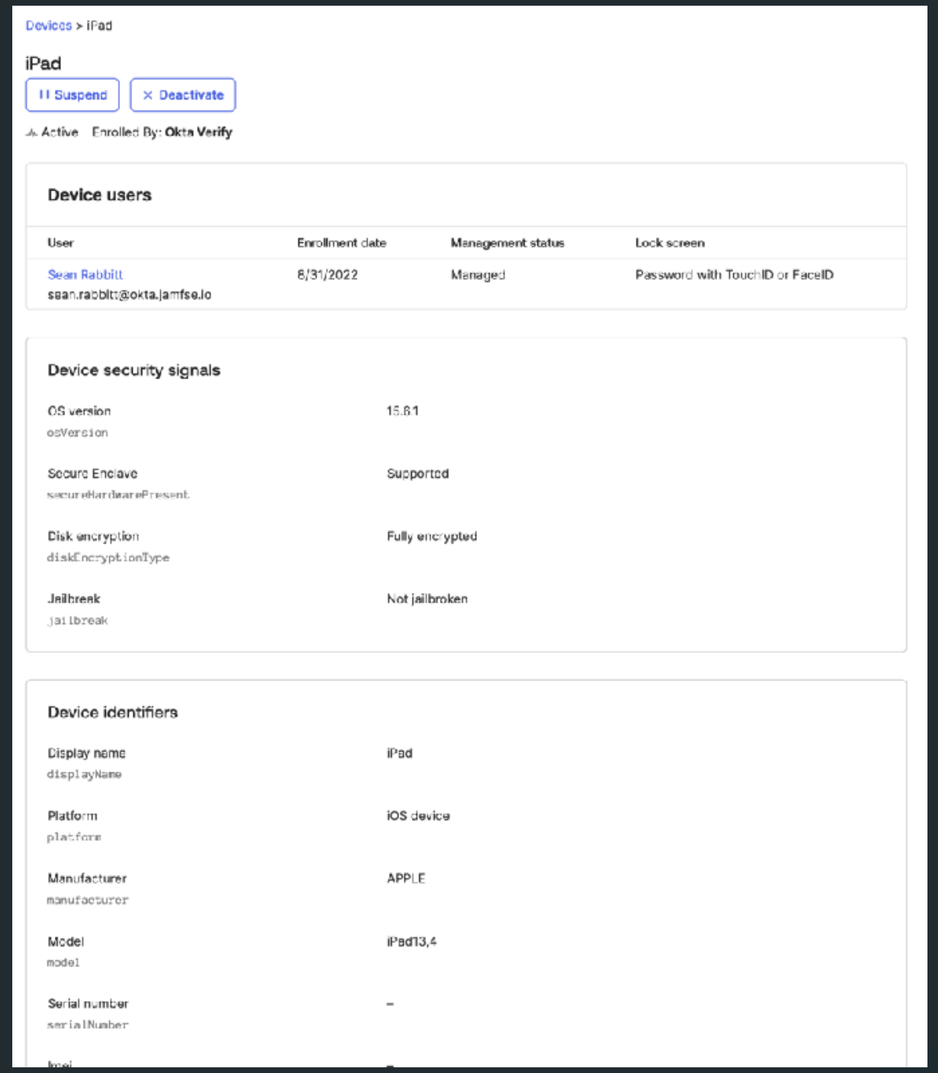
- Attestation that device has an MDM in control
- Works with multiple device enrollment methods and platforms

2023 JNUC

What is Okta Device Trust

What Okta Knows

- Basic Device Inventory information
- Trust established by MDM



What is Okta Device Trust

okta

What Okta Knows

- Basic Device Inventory information
- Trust established by MDM

What Jamf Knows

- Literally everything it can possibly gather
- Use Smart Computer/Device Group to scope SCEP profile or VPP app
- Trust calculated on any inventory update in Pro

What is Okta Device Trust

okta

How does Okta use this information

- Authenticators
  - What methods of authentication are permitted globally
- Global Session Policy
  - Rules established for ALL authentications
- Authentication Policies
  - Rules established for individual applications

2023 JNUC

Authenticators

okta

Authenticators

Authenticator documentation

Setup | Enrollment

Set up and manage authenticators used for authentication and recovery.

Add authenticator

Name	Factor type	Characteristics	Used for	Status	
Any TOTP Generator	Possession	Device bound	Authentication	Active	Actions ▾
Okta Verify	Possession Possession + Knowledge[1] Possession + Biometric[1]	Device bound Hardware protected Phishing resistant (Okta FastPass)[2]	Authentication Recovery (Push only)	Active	Actions ▾
Password	Knowledge		Authentication	Active	Actions ▾
FIDO2 (WebAuthn)	Possession Possession + Knowledge[1] Possession + Biometric[1]	Device bound Hardware protected Phishing resistant[2]	Authentication	Active	Actions ▾

2023 JNUC

Authenticators

okta

Okta Verify

After admins configure this authenticator, users are prompted to download and install the Okta Verify app. Once installed, Okta Verify uses your configuration to allow users to access protected resources. Learn more in documentation.

Used for

- Authentication (with time-based one-time password (TOTP), push notification, Okta FastPass)
- Self-service recovery (with push notification only)

Verification options

User can verify with

- TOTP (on by default) (Android and iOS only)
- Push notification (Android and iOS only)
- Okta FastPass (All platforms)

Okta FastPass

Sign-in page option

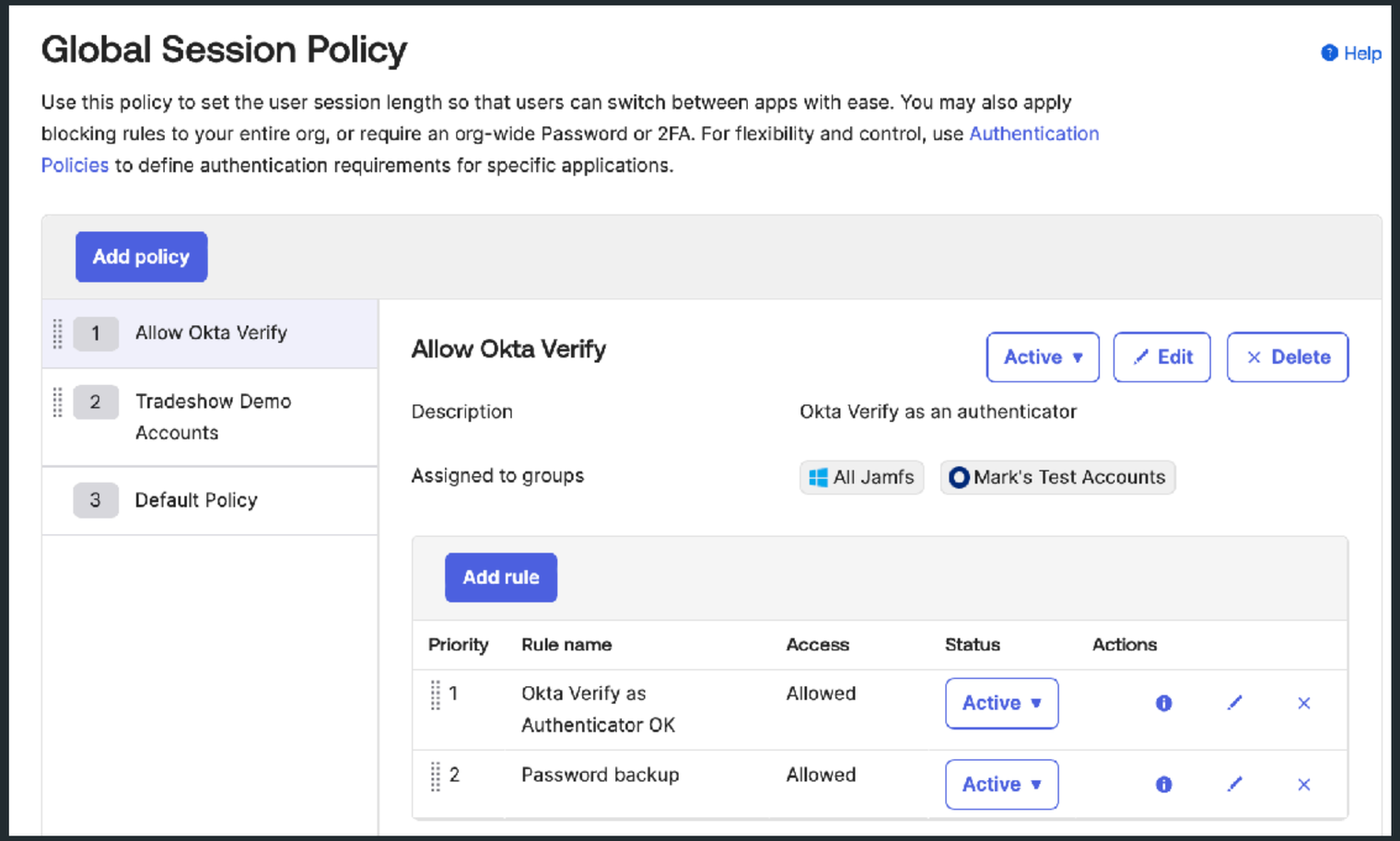
- Show the "Sign in with Okta FastPass" button

What does this button do?

2023 JNUC

Global Session Policy

okta



Global Session Policy

okta

Edit Rule

Rule name: Okta Verify as Authenticator OK

Exclude users: Exclude users

Policy settings

IF User's IP is: Anywhere

Manage configuration for Networks

AND Identity provider is: Any

AND Authenticates via: Any

AND Behavior is: Select behavior

AND Risk is: Any

THEN Access is: Allowed

Establish the user session with:

- (•) Any factor used to meet the Authentication Policy requirements
- ( ) A password

An IdP claim will satisfy either of these options. The Authentication Policy determines the authentication requirement for a request.

2023 JNUC

Add Rule

Rule name — TIP: Describe what this rule does

Exclude users — Exclude users

Policy settings

IF User's IP is — Anywhere

Manage configuration for Networks

AND Identity provider is — Any

AND Authenticates via — Any

AND Behavior is — Select behavior

AND Risk is — Any

THEN Access is — Allowed

Establish the user session with

- (•) Any factor used to meet the Authentication Policy requirements
- ( ) A password

An IdP claim will satisfy either of these options. The Authentication Policy determines the authentication requirement for a request.

okta

Multifactor authentication (MFA) is

- (•) Not required
- ( ) Required

You can use the Authentication Policy to define multifactor requirements and characteristics of the allowed authenticators.

- Custom integrations that use the Okta Classic APIs are affected by this setting. Learn more
- Verify that multifactor authentication for your key applications is turned on. Learn more

Session management

Maximum Okta session lifetime

- (•) No time limit
- ( ) Set time limit (Recommended)

The maximum session lifetime ensures that a session will expire after this maximum session time even if idle time never expires. Setting an upper bound minimizes the risk of session cookies misuse or hijacking.

Expire session after user has been idle on Okta for — 12 — Hours

User session will expire when the user has been inactive on Okta for the set time period, regardless of Max Okta session lifetime.

Persist session cookies across browser sessions — Disable (Recommended)

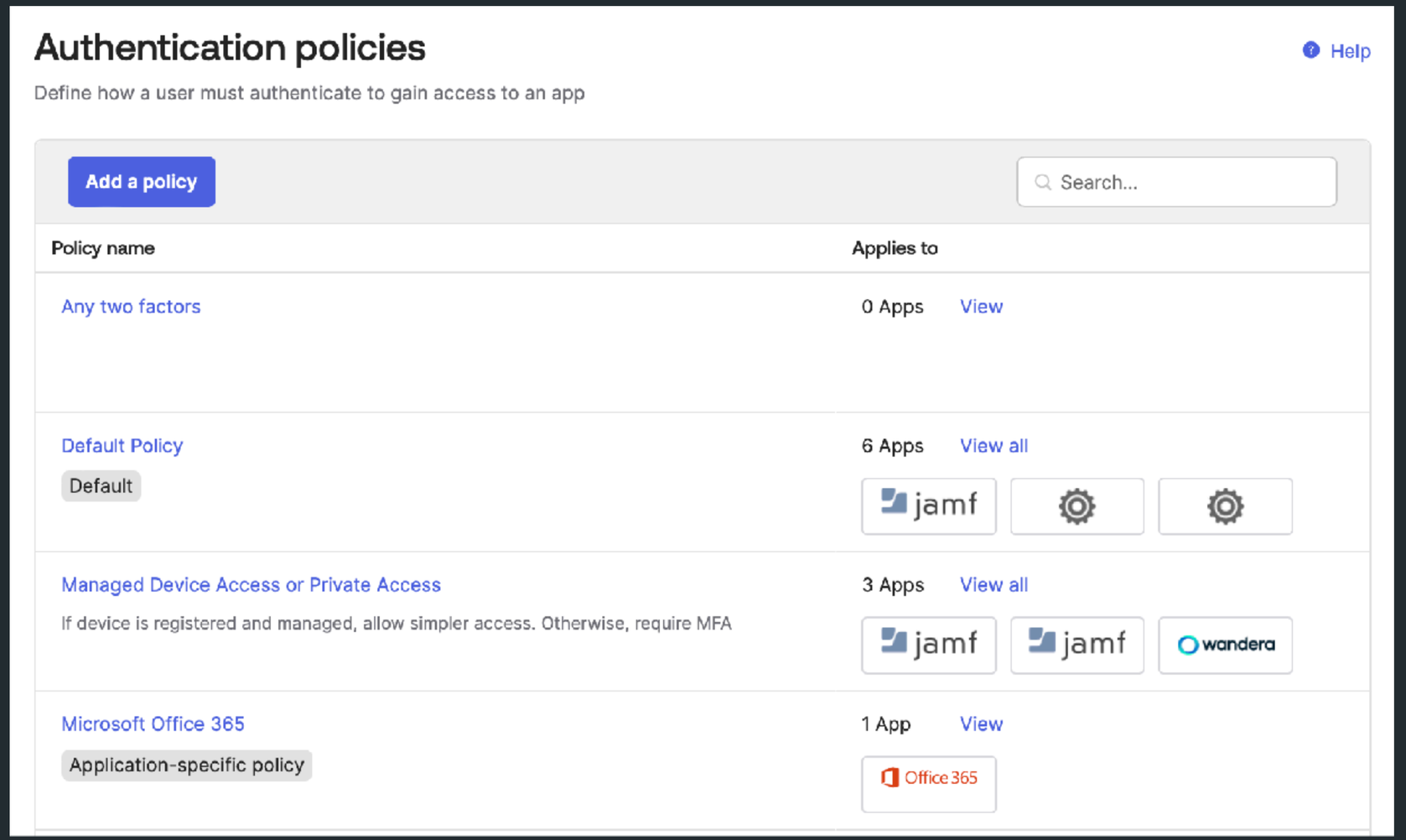
If enabled, when user reopens the same browser, they will not be asked to sign-in again if the session is still active. Learn more.

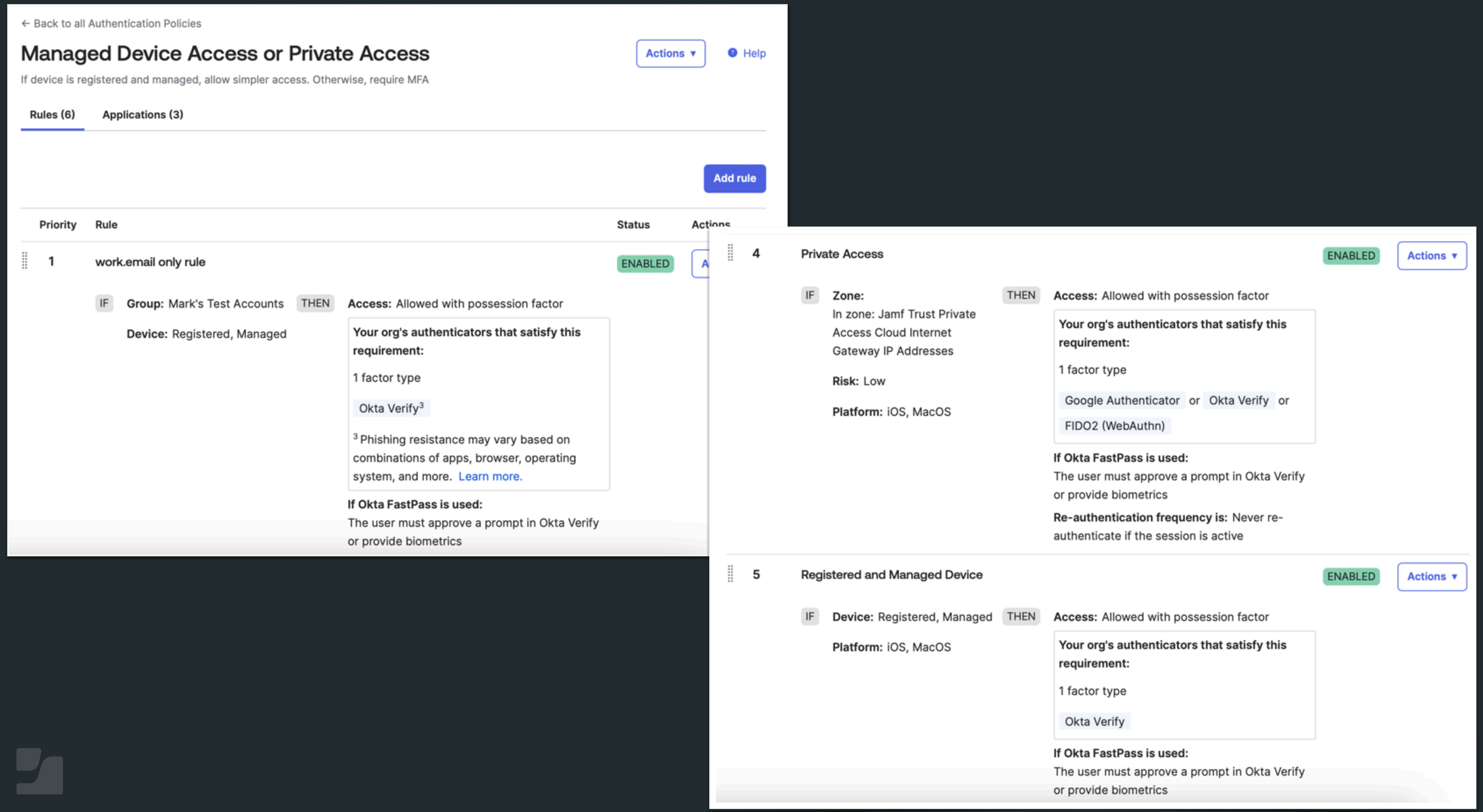
Create rule | Cancel

2023 JNUC

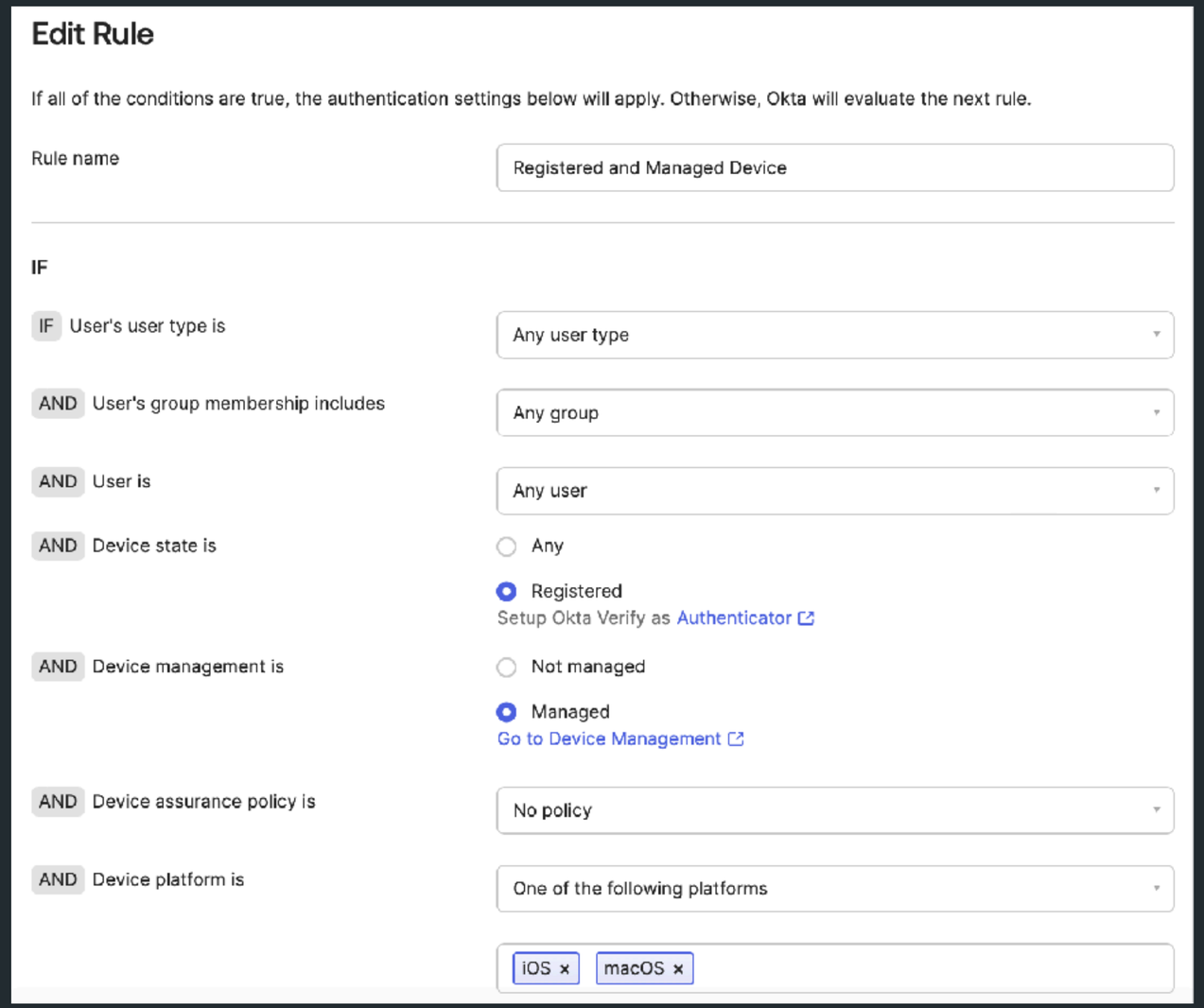
Authentication policies

okta





Authentication policies and device trust



Device state is:

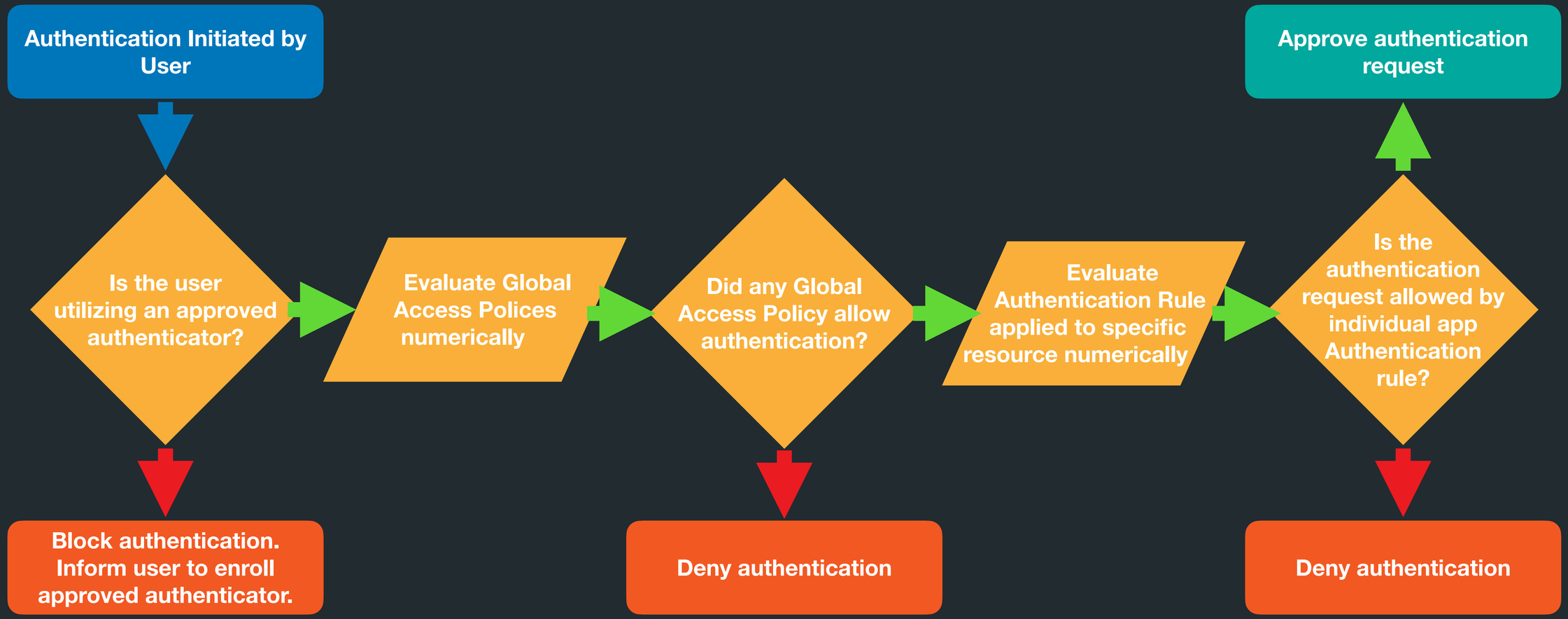
- Registered

Device management is:

- Managed

Device platform is:

- iOS (includes iPadOS)
- macOS



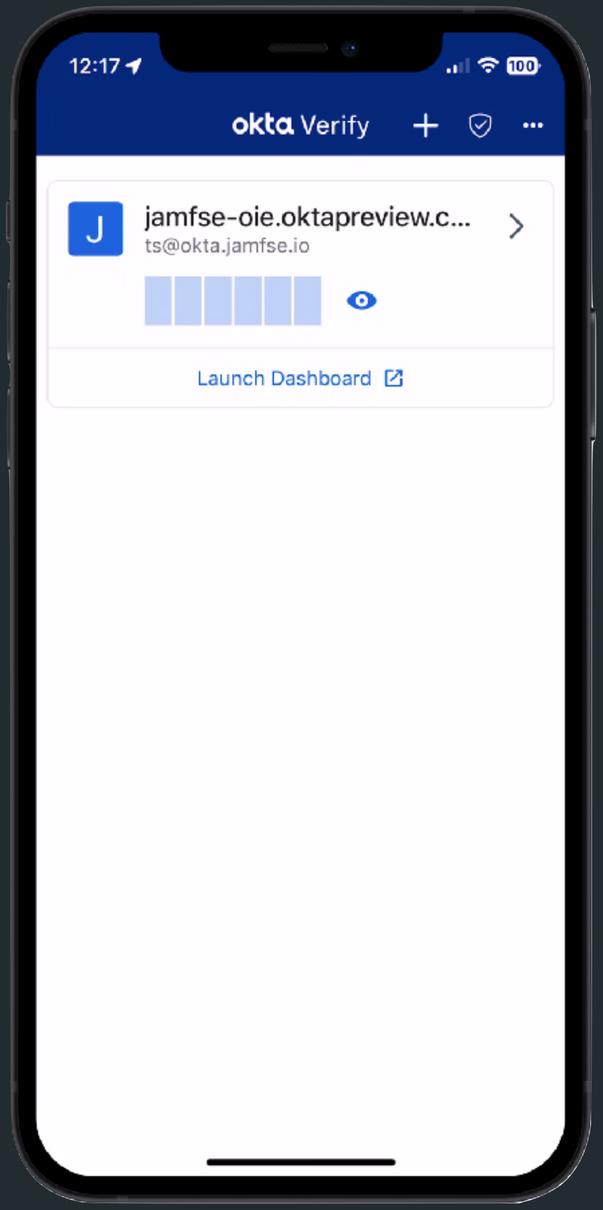
okta

Registered:

- Okta Verify installed
- User has logged in once
- macOS: Separate keychain created in ~/Library/Keychains

Managed:

- macOS - SCEP certificate pushed via MDM profile
- iOS - managementHint pushed in AppConfig via MDM



okta

2023 JNUC

okta

Okta Device Trust

@

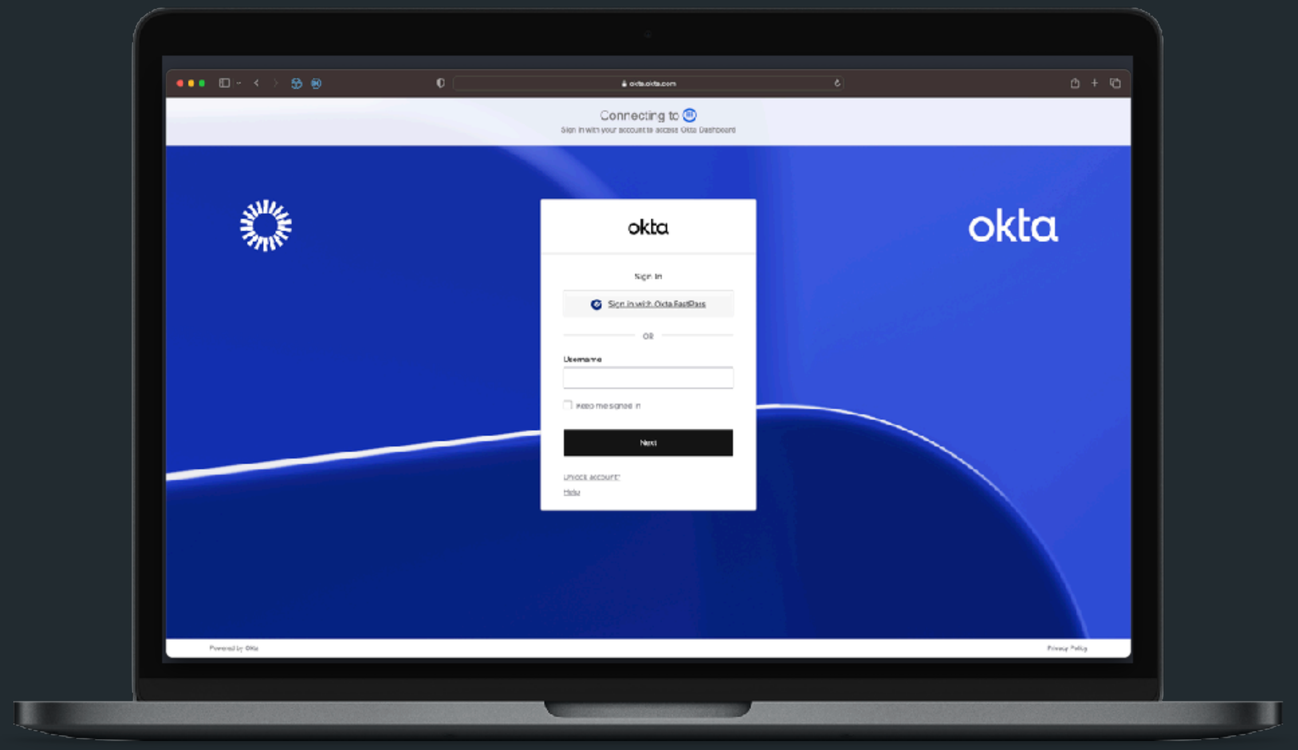
okta

2023 JNUC

Okta Device Trust & Authentication Policies

okta

- Unmanaged
- Low
- Medium
- Medium Productivity
- High



2023 JNUC

Okta Device Trust in Action at Okta- Unmanaged Device Policy

okta

Provides Access for:

Helpdesk

New employee onboarding (Jamf new device Mac registration)

Device Trust Features in Use:

Authenticators & App Policy:

Okta Device Trust in Action at Okta- Unmanaged Device Policy

okta

Provides Access for:

Helpdesk

New employee onboarding (Jamf new device Mac registration)

Device Trust Features in Use:

N/A - only policy to allow managed and unmanaged/unregistered devices

Authenticators & App Policy:

Okta Device Trust in Action at Okta- Unmanaged Device Policy

okta

Provides Access for:

Helpdesk

New employee onboarding (Jamf new device Mac registration)

Device Trust Features in Use:

N/A - only policy to allow managed and unmanaged/unregistered devices

Authenticators & App Policy:

Two of the following:

FastPass
WebAuthN
Password

Requires re-auth at each sign-on

Okta Device Trust in Action at Okta- Low Assurance Policy

okta

Provides Access for:

- Essential, low risk apps
- Training/LMS
- OktaTV
- Surveys
- Okta dashboard

Device Trust Features in Use:

Authenticators & App Policy:

2023 JNUC

Okta Device Trust in Action at Okta- Low Assurance Policy

okta

Provides Access for:

- Essential, low risk apps
- Training/LMS
- OktaTV
- Surveys
- Okta dashboard

Device Trust Features in Use:

- Behavior detection
- Crowdstrike ZTA <=60
- Registered - BYOD
- Managed - Work-issued

Authenticators & App Policy:

Okta Device Trust in Action at Okta- Low Assurance Policy

okta

Provides Access for:

- Essential, low risk apps
- Training/LMS
- OktaTV
- Surveys
- Okta dashboard

Device Trust Features in Use:

- Behavior detection
- Crowdstrike ZTA <=60
- Registered - BYOD
- Managed - Work-issued

Authenticators & App Policy:

- One of the following (Two if in Exception or trips Behavior Detection):
- FastPass (PR, no biometric required)
  WebAuthN (no pin/bio required)
- Session duration:
  12-hour re-challenge

2023 JNUC

Okta Device Trust in Action at Okta- Medium Assurance Policy

okta

Provides Access for:

Most applications used in day to day business operations

Design boards

Jira

Device Trust Features in Use:

Authenticators & App Policy:

Okta Device Trust in Action at Okta- Medium Assurance Policy

okta

Provides Access for:

- Most applications used in day to day business operations
- Design boards
- Jira

Device Trust Features in Use:

- Behavior detection
- Crowdstrike ZTA <=60
- Registered - BYOD
- Unmanaged device signals
- Managed - Work-issued
- Okta Verify device signals

Authenticators & App Policy:

Okta Device Trust in Action at Okta- Medium Assurance Policy

okta

Provides Access for:

- Most applications used in day to day business operations
- Design boards
- Jira

Device Trust Features in Use:

- Behavior detection
- Crowdstrike ZTA <=60
- Registered - BYOD
- Unmanaged device signals
- Managed - Work-issued
- Okta Verify device signals

Authenticators & App Policy:

One of the following combos:

- FastPass (PR + biometric)
  WebAuthN (Plus pin/ biometric)
  Password with FastPass or WebAuthnN

Session duration:
12-hour re-challenge

2023 JNUC

Okta Device Trust in Action at Okta- Medium Assurance Productivity Policy

okta

Provides Access for:

Collaboration and productivity apps

Apps used by field teams

Device Trust Features in Use:

Authenticators & App Policy:

Okta Device Trust in Action at Okta- Medium Assurance Productivity Policy

okta

Provides Access for:

- Collaboration and productivity apps
- Apps used by field teams

Device Trust Features in Use:

- Behavior detection
- Crowdstrike ZTA <=60
- Registered - BYOD
- Unmanaged device signals
- Managed - Work-issued
- Okta Verify device signals

Authenticators & App Policy:

Okta Device Trust in Action at Okta- Medium Assurance Productivity Policy

okta

Provides Access for:

- Collaboration and productivity apps
- Apps used by field teams

Device Trust Features in Use:

- Behavior detection
- Crowdstrike ZTA <=60
- Registered - BYOD
- Unmanaged device signals
- Managed - Work-issued
- Okta Verify device signals

Authenticators & App Policy:

One of the following combos:

FastPass (PR + biometric)
WebAuthN (Plus pin/ biometric)
Password with FastPass or WebAuthnN

Session duration:
12-hour re-challenge (Managed)
Requires re-auth at each sign-on

Okta Device Trust in Action at Okta- High Assurance Policy

okta

Provides Access for:

- Crown jewels
- Apps with PII
- Infrastructure/SRE

Device Trust Features in Use:

- Behavior detection
- Crowdstrike ZTA <=60
- Managed - Work-issued
- Okta Verify device signals

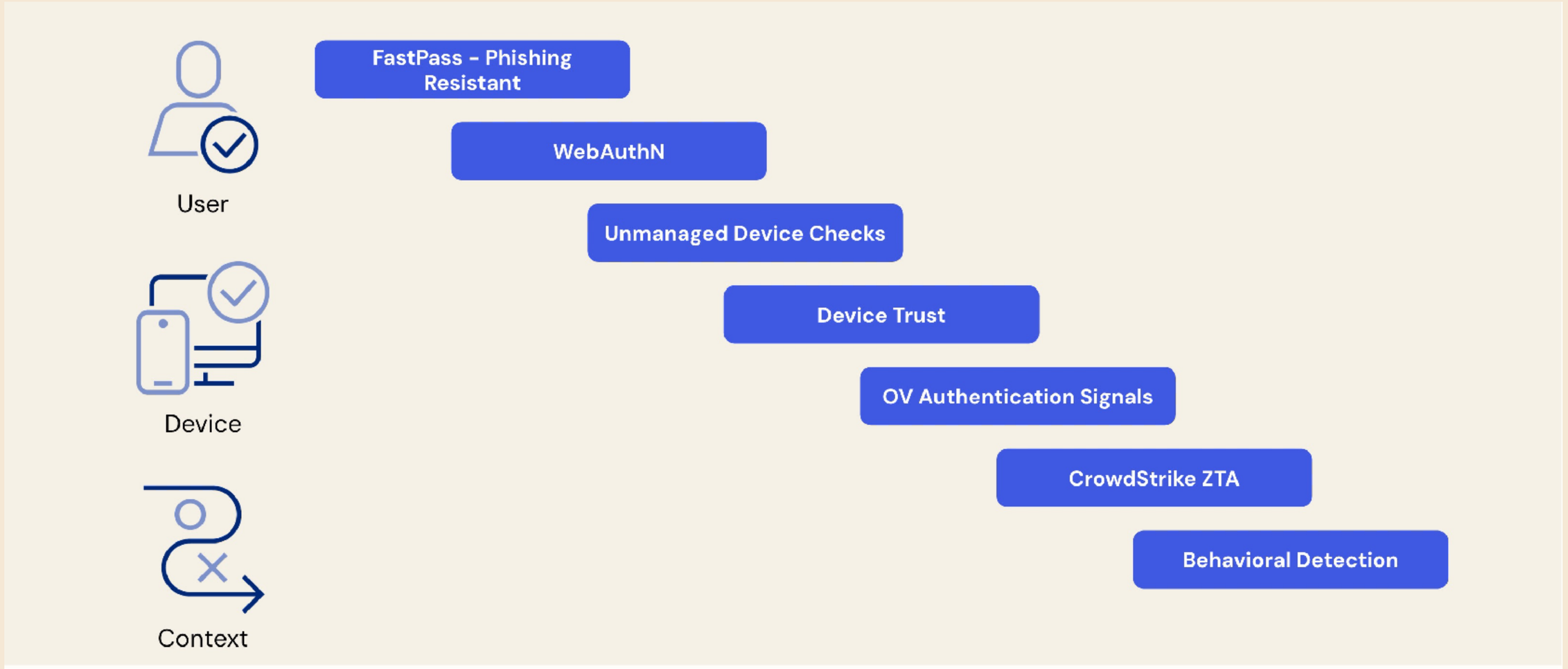
Authenticators & App Policy:

One of the following combos:

FastPass (PR + biometric)
WebAuthN (Plus pin/ biometric)
Password with FastPass (PR + biometric) or WebAuthN (Plus pin/biometric)

Session duration:
Requires re-auth at each sign-on

Defense in depth Zero Trust Architecture



okta

Configuring Okta Device Trust with Jamf Pro

2023 JNUC

Requirements

okta

Okta Identity Engine

CA provided by Okta / AppConfig secret pushed to iOS

Okta Verify app pushed via VPP

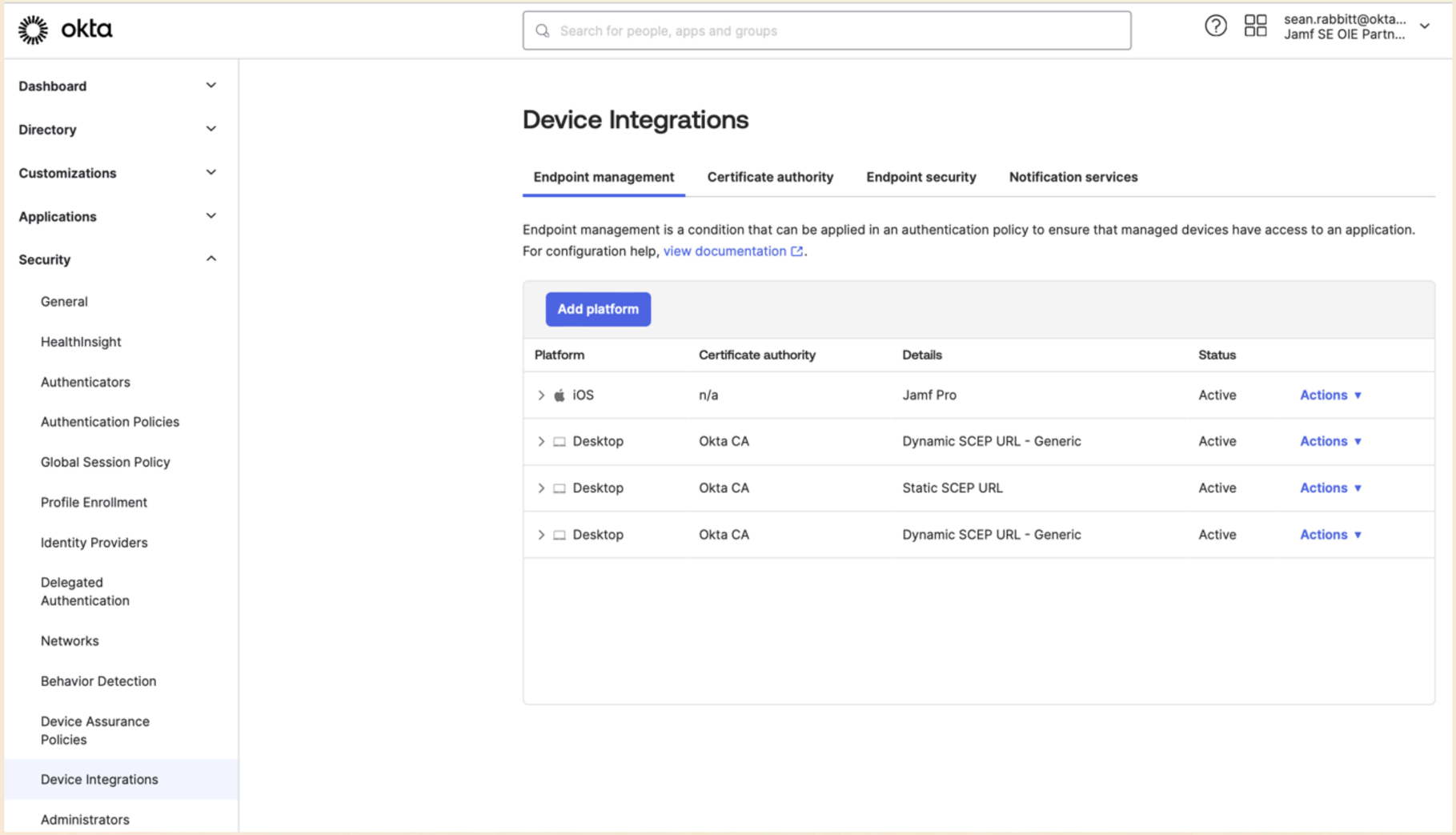
macOS 11 or greater

iOS or iPadOS 15.0 or greater

2023 JNUC

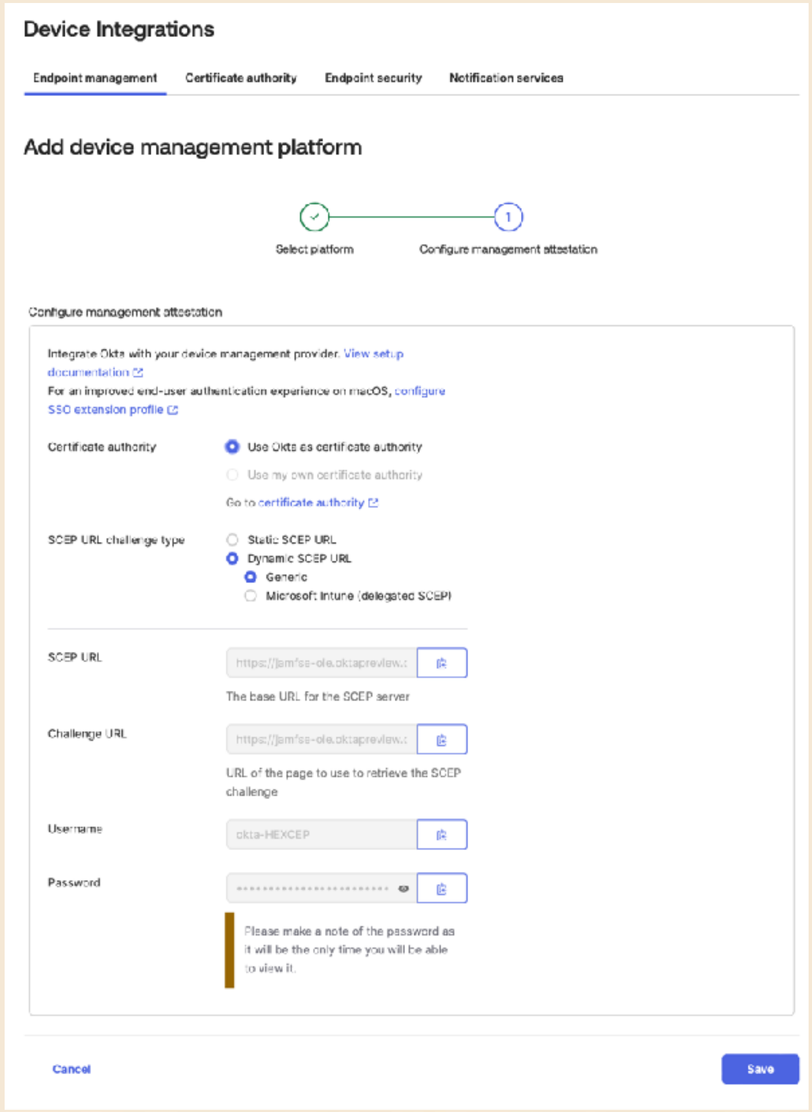
Configuring Okta Device Trust

SCEP server in Okta



Configuring Okta Device Trust

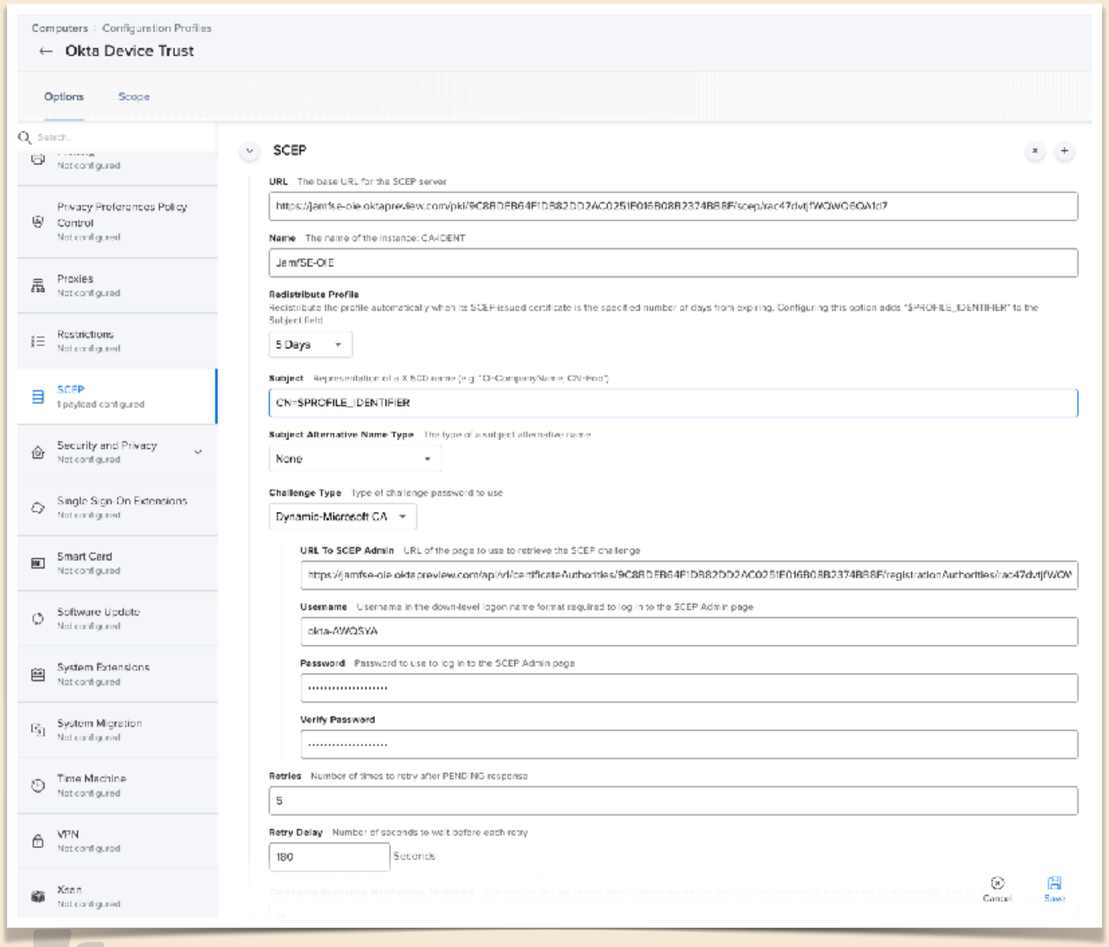
SCEP server in Okta

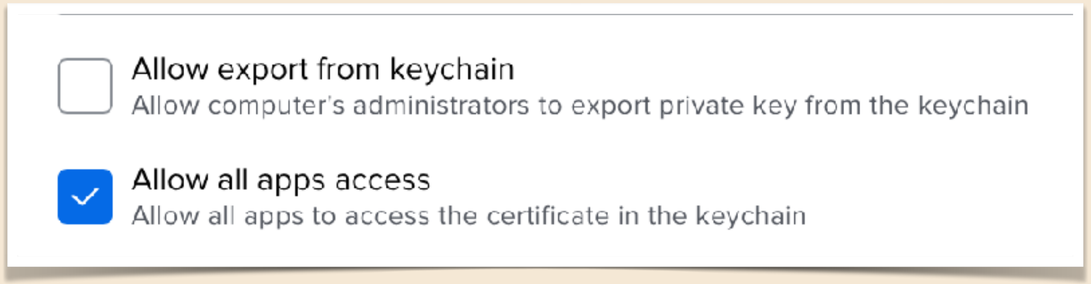


https://jamf.it/oktaCA

Configuring Okta Device Trust

SCEP Payload in Jamf Pro

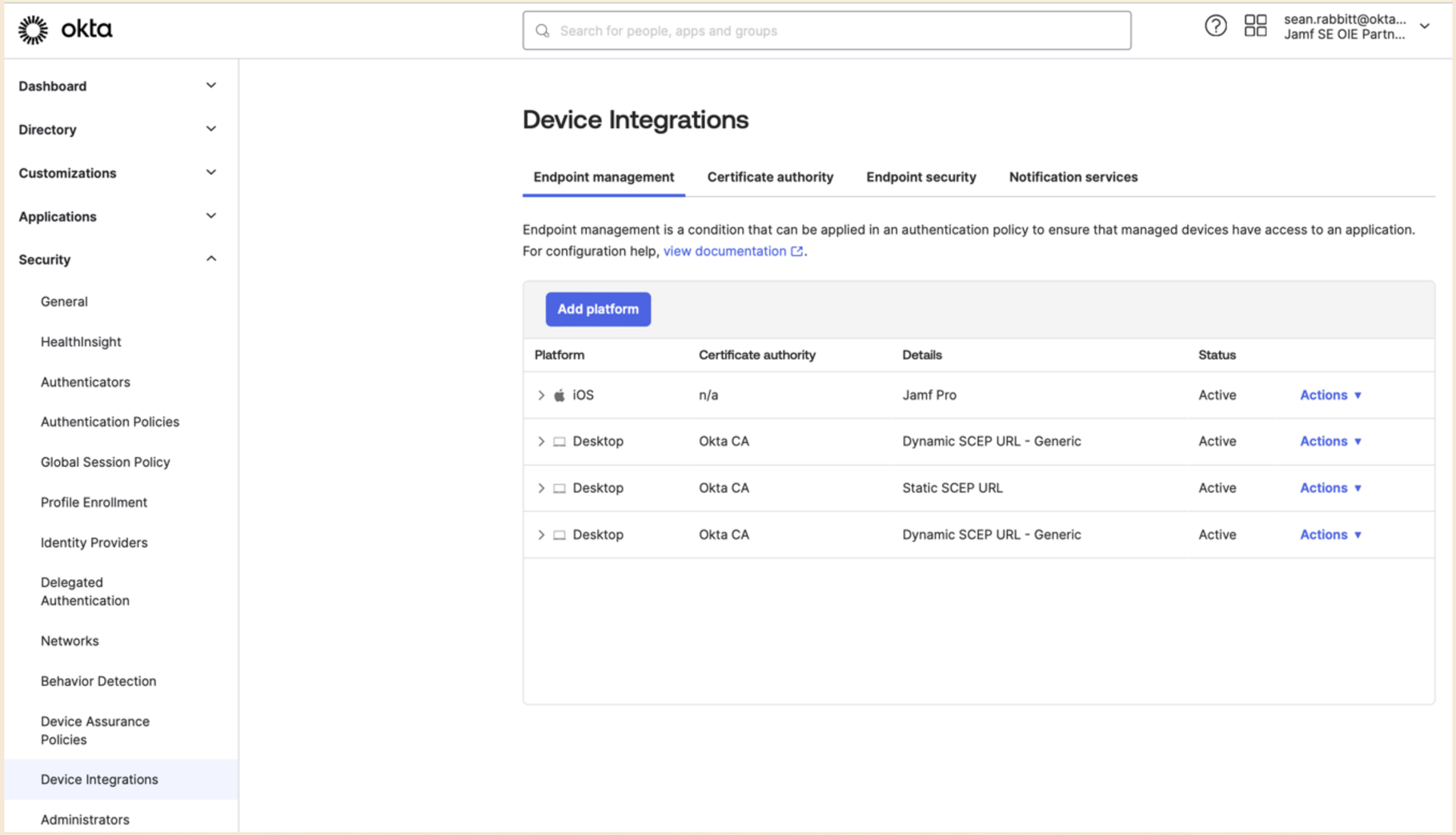




https://jamf.it/oktaCA

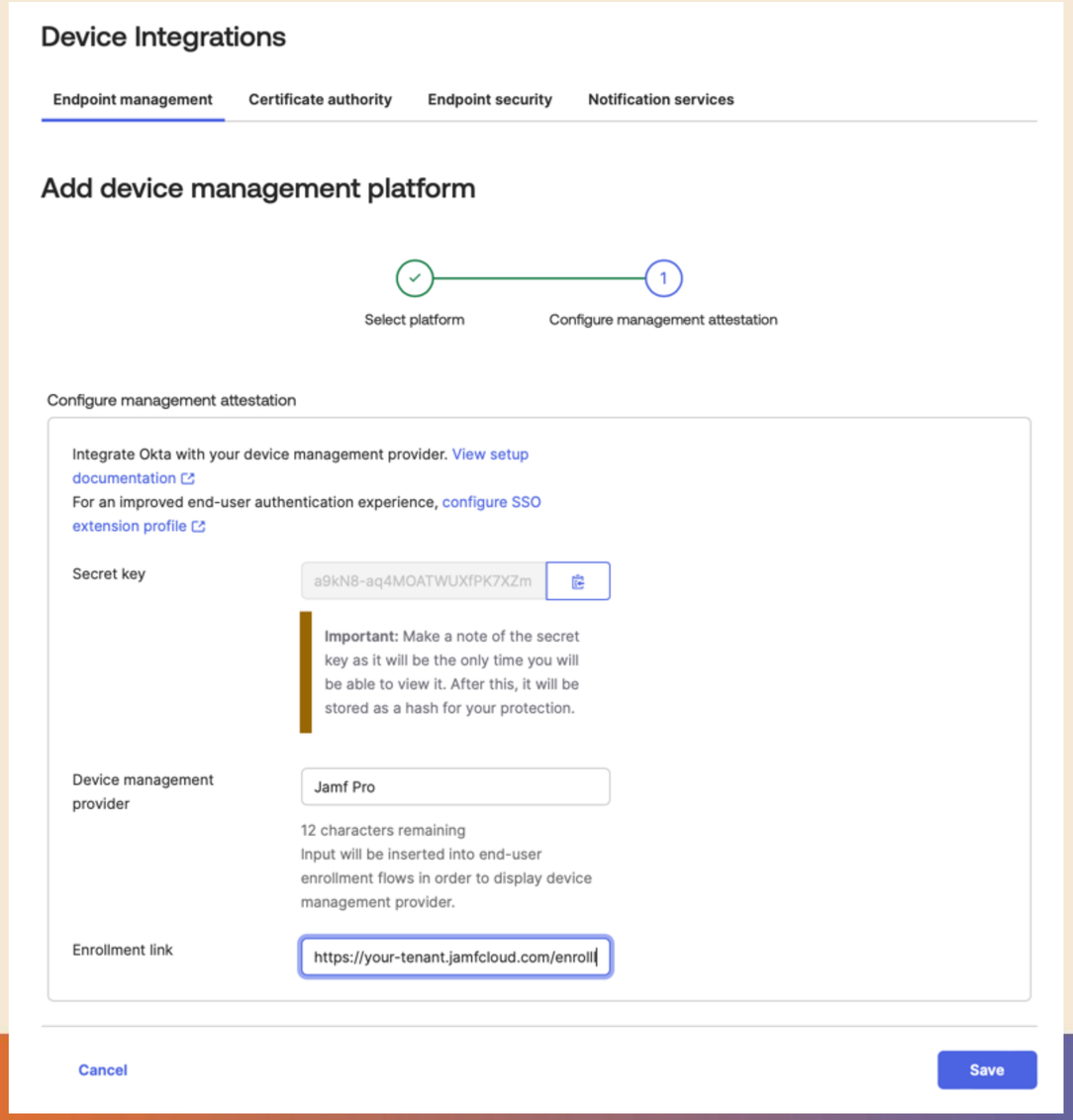
Configuring Okta Device Trust

managementHint for iOS / iPadOS



Configuring Okta Device Trust

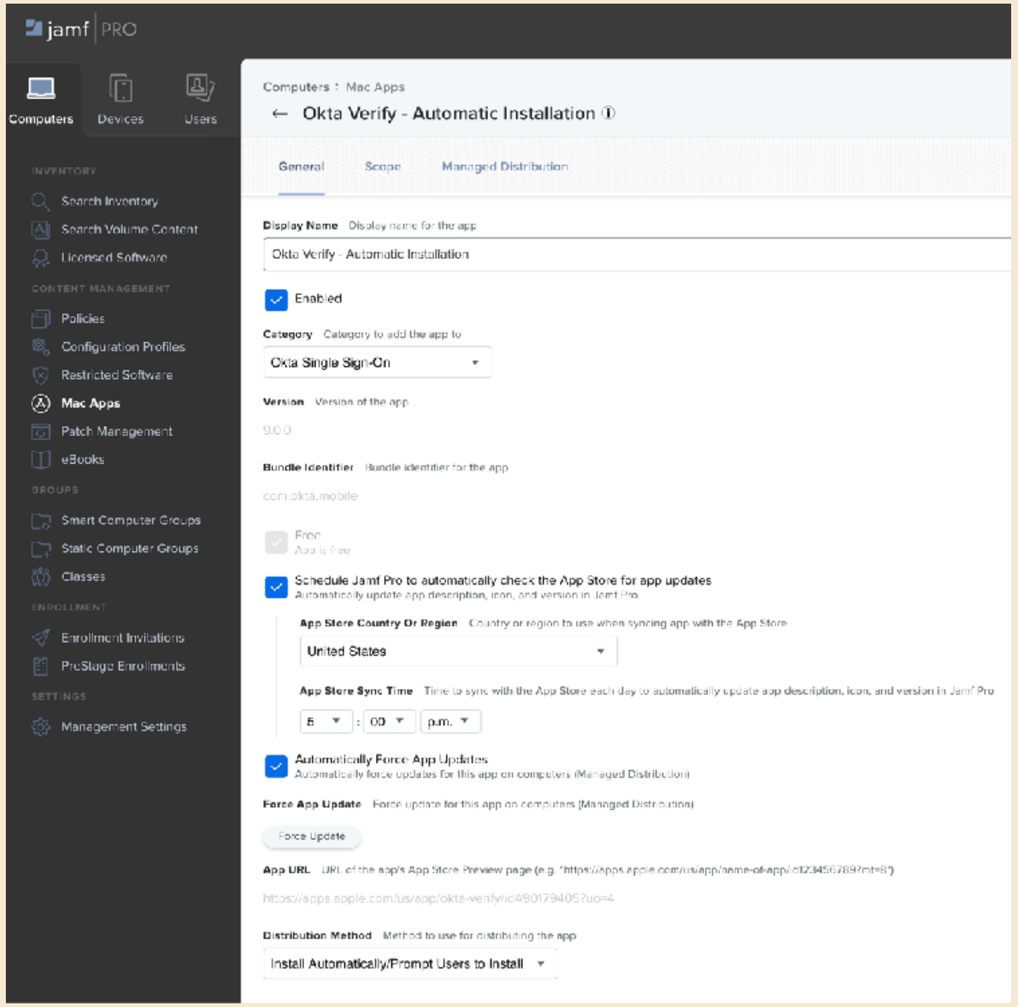
managementHint for iOS / iPadOS

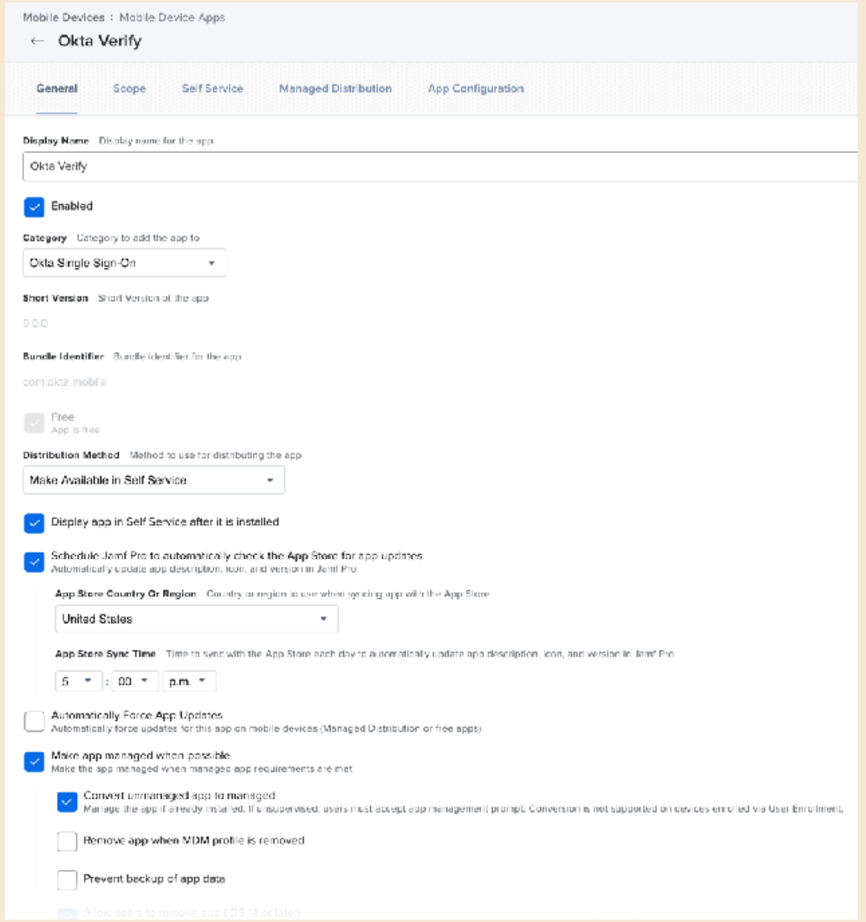


https://jamf.it/oktaiOS

Configuring Okta Device Trust

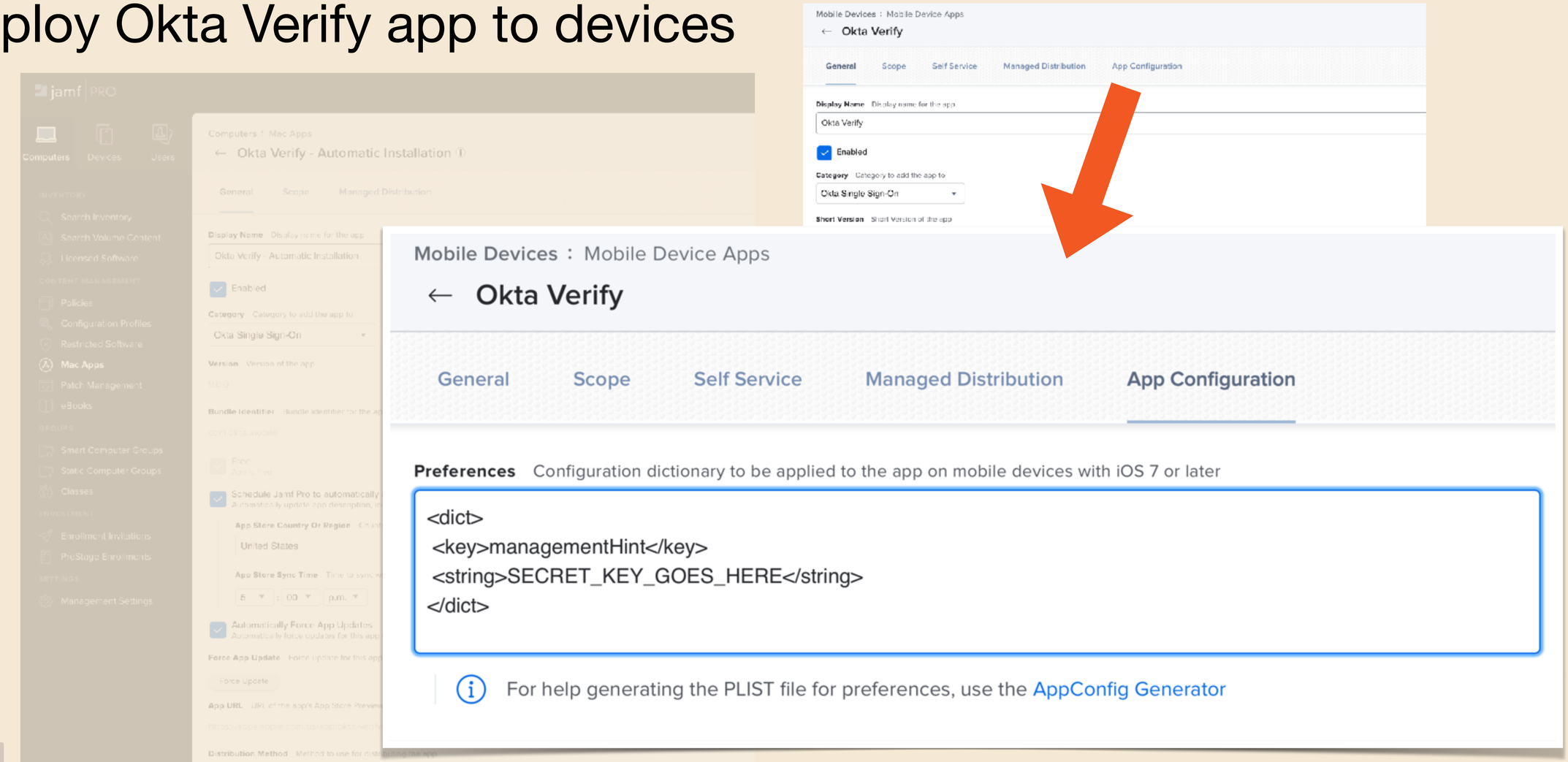
Deploy Okta Verify app to devices





Configuring Okta Device Trust

Deploy Okta Verify app to devices



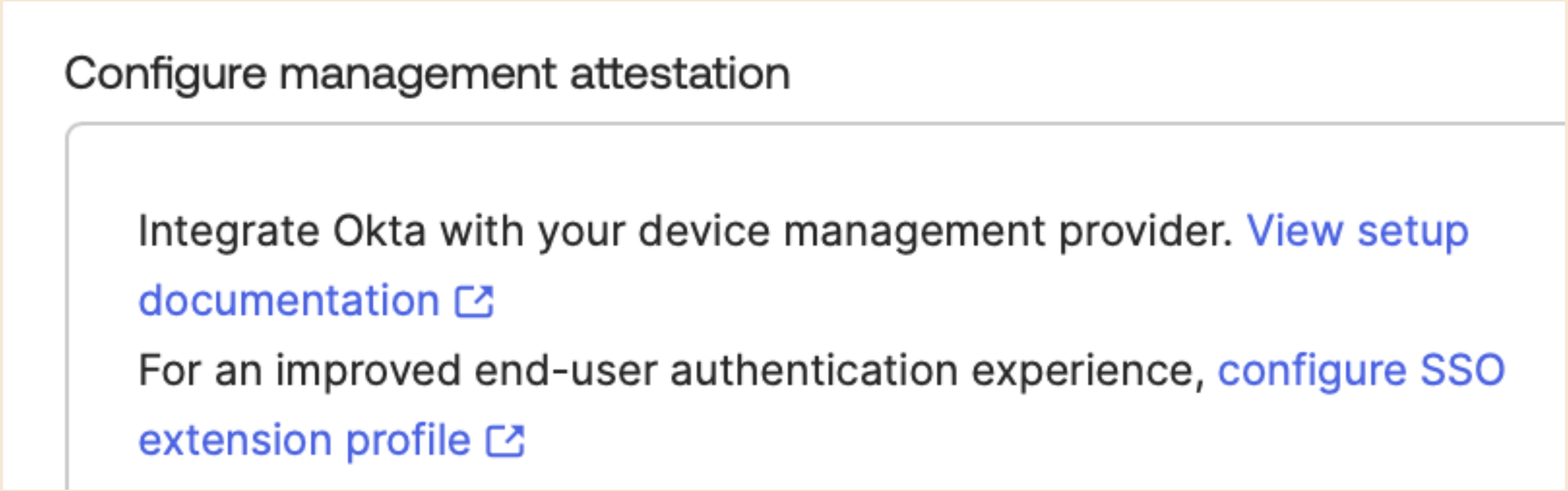
Configuring Okta Device Trust

AppConfig Value - iOS / iPadOS only

```
<dict>
  <key>managementHint</key>
  <string>SECRET_KEY_GOES_HERE</string>
</dict>
```

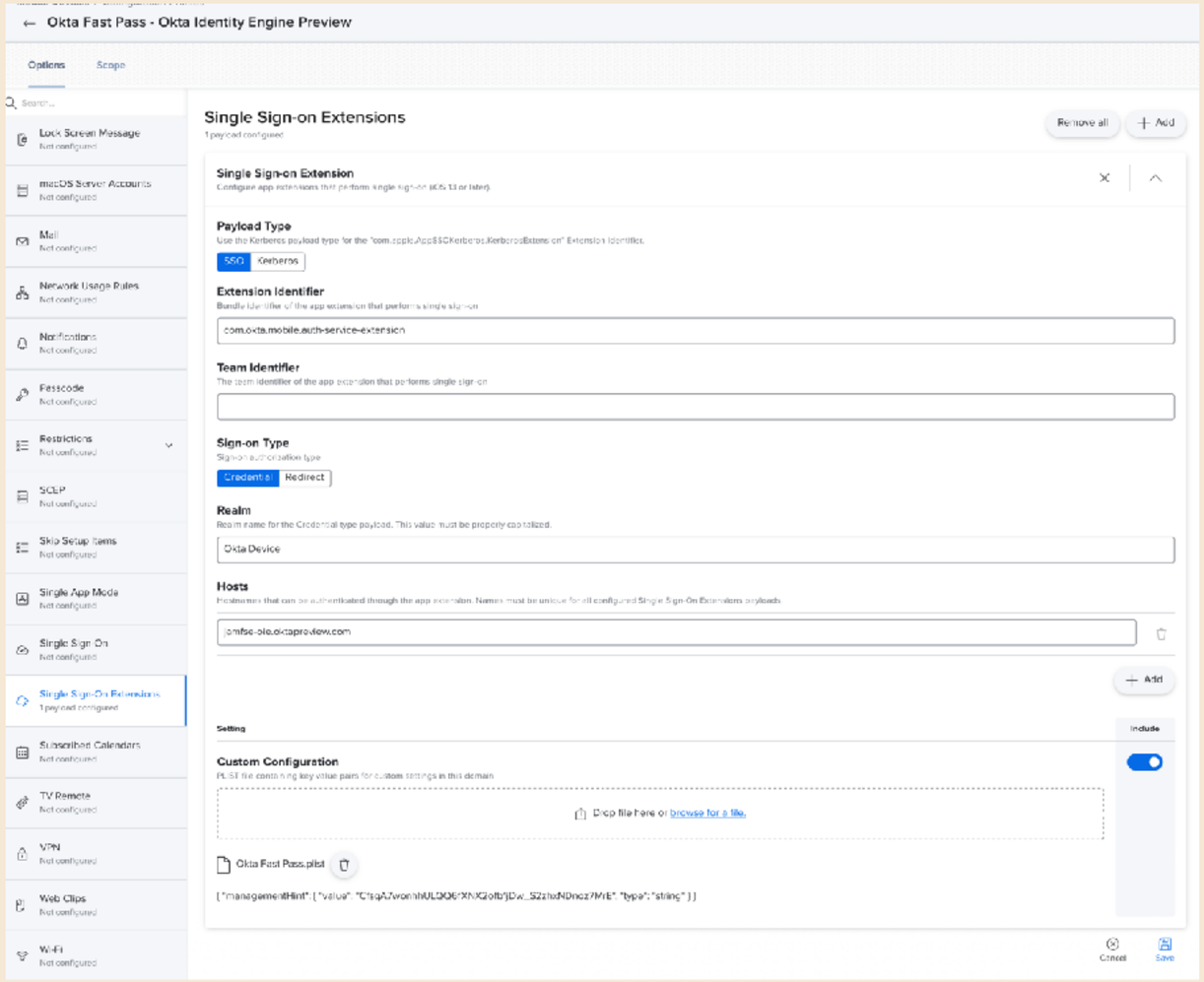
Configuring Okta Device Trust

BONUS GAME: Single Sign On Extension



Configuring Okta Device Trust

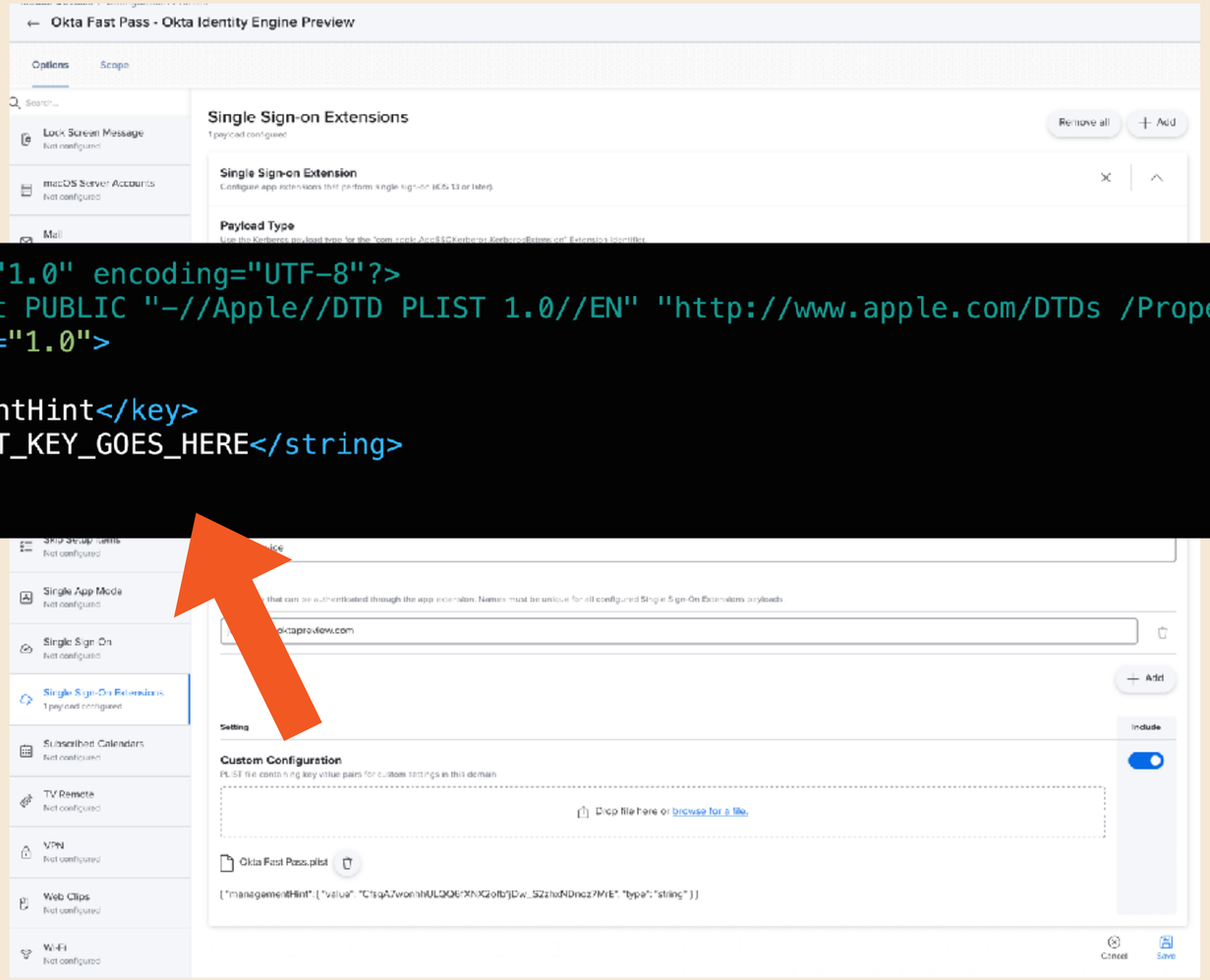
BONUS GAME: Single Sign On Extension



https://jamf.it/oktaSSOe

Configuring Okta Device Trust

BONUS GAME: Single Sign On Extension

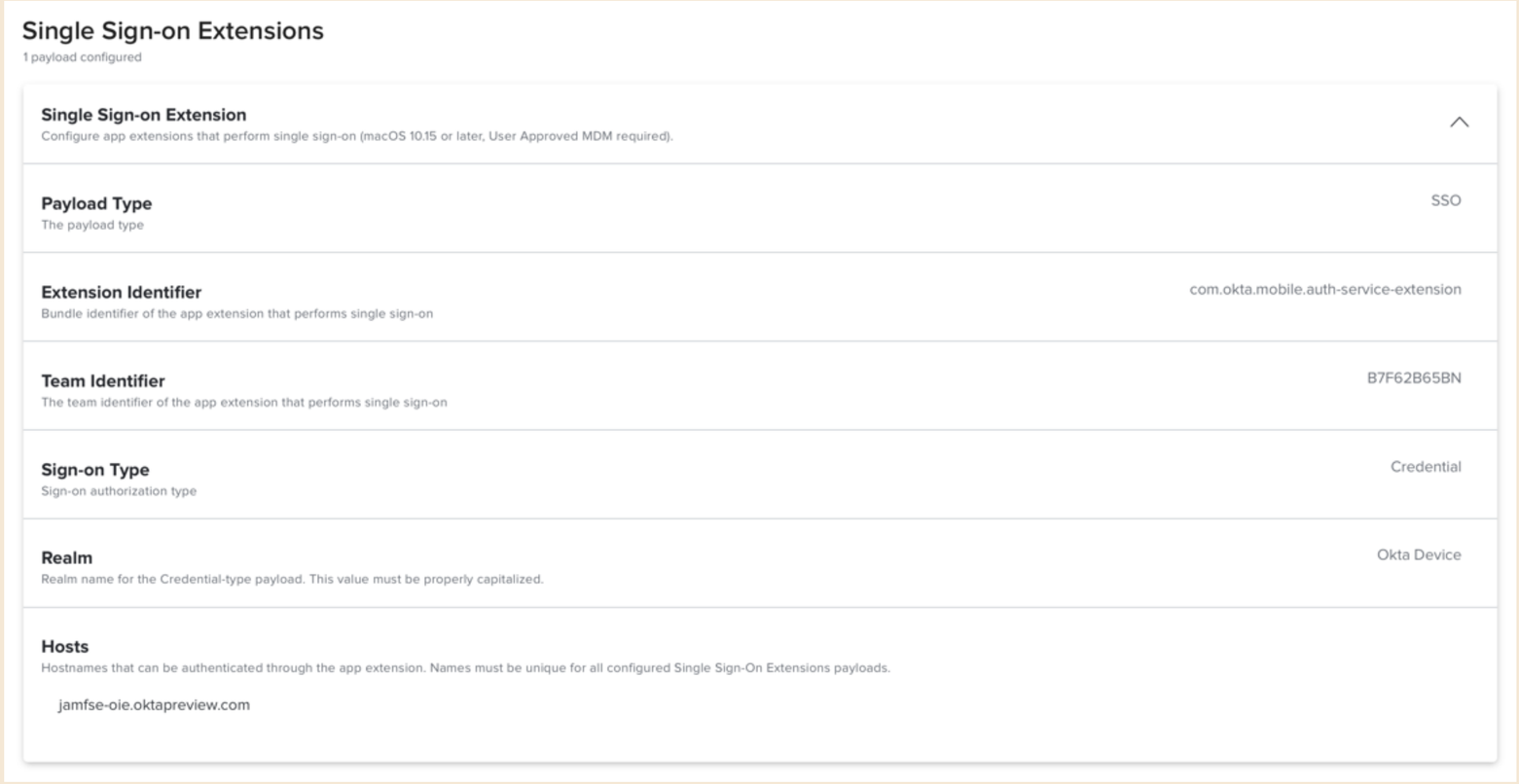



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs /PropertyList-1.0.dtd ">
<plist version="1.0">
<dict>
 <key>managementHint</key>
 <string>SECRET_KEY_GOES_HERE</string>
</dict>
</plist>
```

https://jamf.it/oktaSSOe

Configuring Okta Device Trust

BONUS GAME: Single Sign On Extension



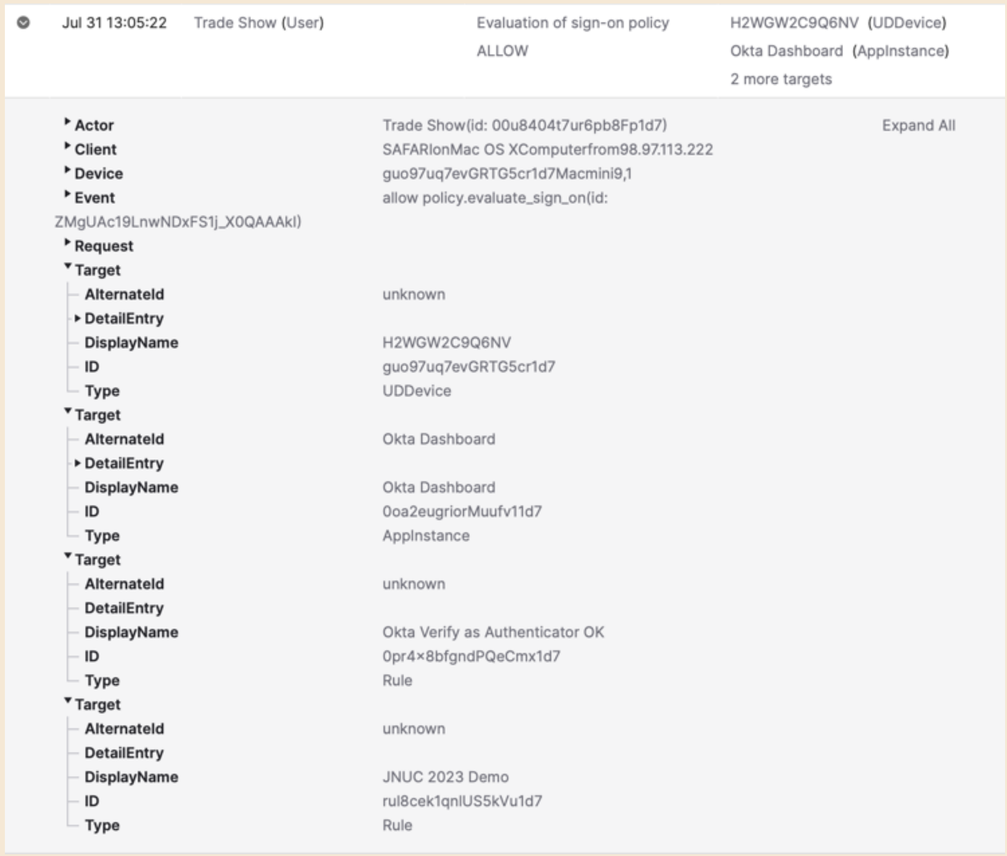
https://jamf.it/oktaSSOe


Finder
File
Edit
View
Go
Window
Help
Mon Jul 31 1:04 PM
JUL
31
tv


Finder
File
Edit
View
Go
Window
Help
Mon Jul 31 1:04 PM
JUL
31
tv

Configuring Okta Device Trust

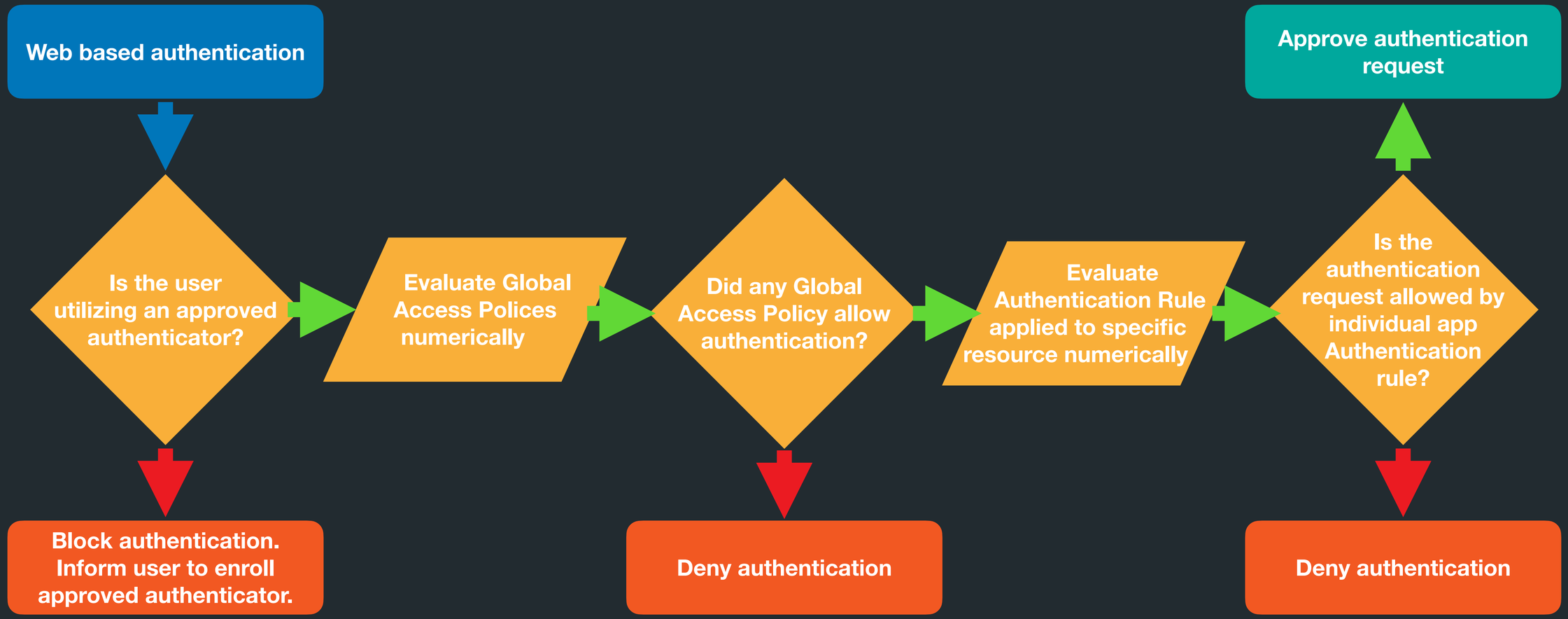
Determining which rules applied

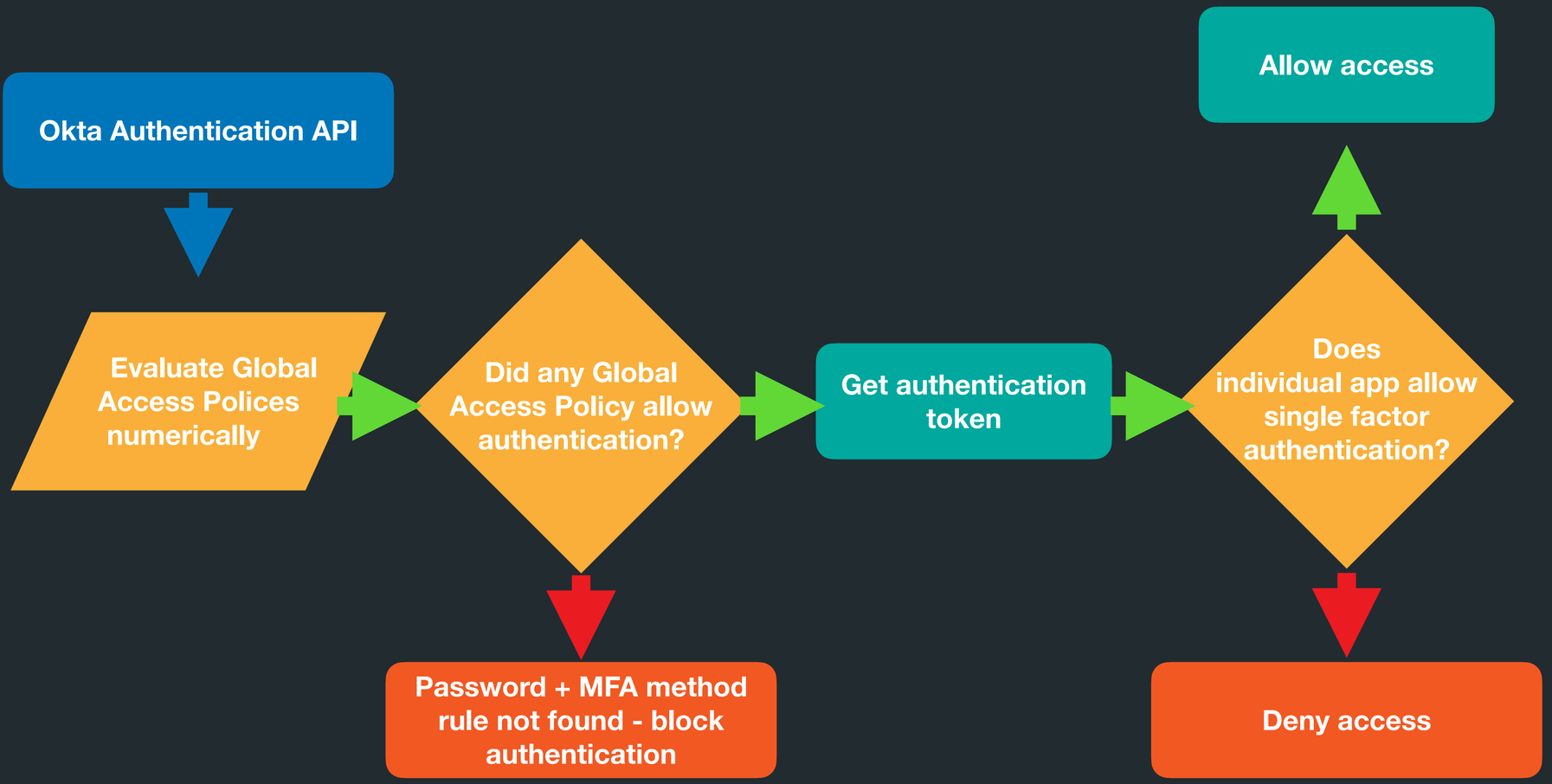


How does Okta Device Trust affect Jamf Connect

Jamf Connect and OIE

	Rules Applied
Jamf Connect with Okta Authentication API (The “usual” way)	Global Session Policy ONLY
Jamf Connect with Okta as an OIDC Application	Global Session Policy Authentication Policy





Jamf Connect and OIE

	Gotchas
Jamf Connect with Okta Authentication API (The “usual” way)	OIDC apps for Admin rights, Access rights, Secondary account creation rights require OIDC app - watch your Authentication rules!
Jamf Connect with Okta as an OIDC Application	Can’t restrict creating “second” account on device short of disabling login window

Jamf Connect and OIE

	Benefits
Jamf Connect with Okta Authentication API (The “usual” way)	Enforcement of the “Restrict Second Account” creation
Jamf Connect with Okta as an OIDC Application	More granular control over authentication rules Okta login shown as a webview

Jamf and Okta Device Trust

okta

- What is Okta Device Trust
- The Okta at Okta experience
- Jamf Pro setup and deployment
- End user experience
- How does this affect Jamf Connect

2023 JNUC

okta

Thank you for listening!

2023 JNUC