



AUSTIN, TX

# Jamf and Okta Device Trust

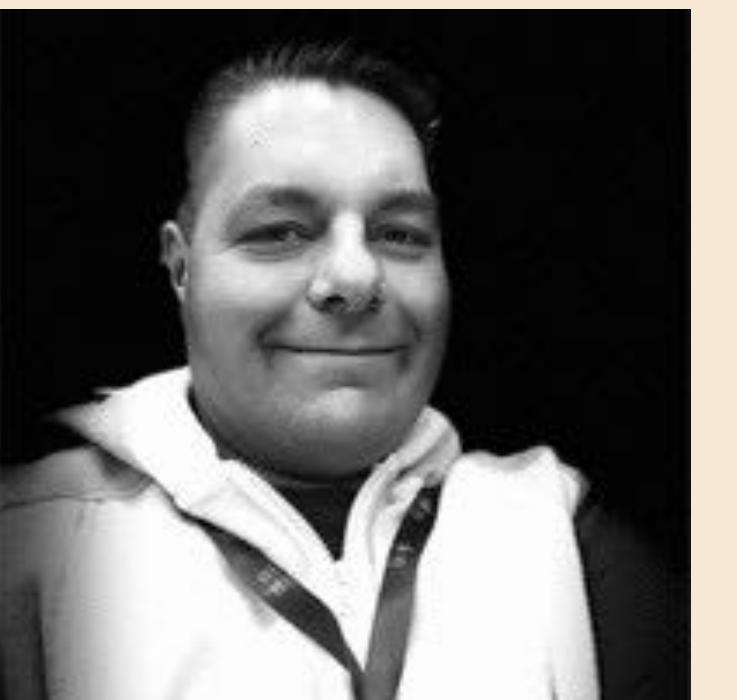
okta

okta



# Jon Lehtinen

Okta



# Sean Rabbitt

Jamf





# Jamf and Okta Device Trust

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



okta

# Okta on Okta (at Okta)



okta

# Okta on Okta (at Okta)

Enable the Business



okta

# Okta on Okta (at Okta)

Enable the Business



Evolve the Product



okta

# Okta on Okta (at Okta)

Enable the Business



Evolve the Product

Showcase the Platform



The Okta logo, consisting of the word "okta" in a lowercase, sans-serif font.

# What is Okta Device Trust



# 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



# What is Okta Device Trust

## What Okta Knows

- Basic Device Inventory information
- Trust established by MDM

The screenshot shows the Okta Device Trust interface for an iPad. At the top, there are buttons for 'Suspend' and 'Deactivate'. Below that, it says 'Active' and 'Enrolled By: Okta Verify'. The main sections include:

- Device users:**

| User        | Enrollment date | Management status | Lock screen                     |
|-------------|-----------------|-------------------|---------------------------------|
| Sean Rabbit | 8/31/2022       | Managed           | Password with TouchID or FaceID |
- Device security signals:**

|   |                 |
|---|-----------------|
| OS version<br>osVersion                 | 15.8.1          |
| Secure Enclave<br>secureHardwarePresent | Supported       |
| Disk encryption<br>diskEncryptionType   | Fully encrypted |
| Jailbreak<br>jailbreak                  | Not jailbroken  |
- Device identifiers:**

|                               |            |
|-------------------------------|------------|
| Display name<br>displayName   | iPad       |
| Platform<br>platform          | iOS device |
| Manufacturer<br>manufacturer  | APPLE      |
| Model<br>model                | iPad13,4   |
| Serial number<br>serialNumber | -          |
| Imei                          | -          |



# 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

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



# 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 | <a href="#">Actions ▾</a> |
| Okta Verify        | Possession<br>Possession + Knowledge <sup>1</sup><br>Possession + Biometric <sup>1</sup> | Device bound<br>Hardware protected<br>Phishing resistant (Okta FastPass) <sup>2</sup> | Authentication<br>Recovery (Push only) | Active | <a href="#">Actions ▾</a> |
| Password           | Knowledge  |   | Authentication                         | Active | <a href="#">Actions ▾</a> |
| FIDO2 (WebAuthn)   | Possession<br>Possession + Knowledge <sup>1</sup><br>Possession + Biometric <sup>1</sup> | Device bound<br>Hardware protected<br>Phishing resistant <sup>2</sup>                 | Authentication                         | Active | <a href="#">Actions ▾</a> |



# Authenticators

## 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

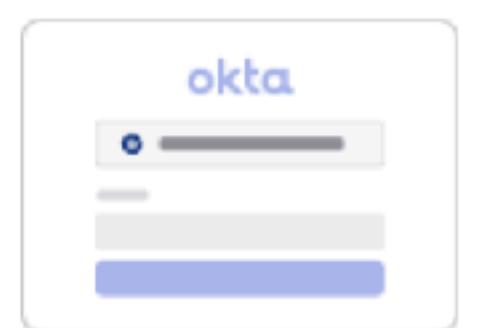
User can verify with

- 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? ↗](#)

okta



# Global Session Policy

okta

**Global Session Policy**

Use this policy to set the user session length so that users can switch between apps with ease. You may also apply blocking rules to your entire org, or require an org-wide Password or 2FA. For flexibility and control, use [Authentication Policies](#) to define authentication requirements for specific applications.

**Add policy**

|                           |                          |                                 |                      |        |
|---------------------------|--------------------------|---------------------------------|----------------------|--------|
| 1 Allow Okta Verify       | <b>Allow Okta Verify</b> | Active ▾                        | Edit                 | Delete |
| 2 Tradeshow Demo Accounts | Description              | Okta Verify as an authenticator |                      |        |
| 3 Default Policy          | Assigned to groups       | All JamfS                       | Mark's Test Accounts |        |

**Add rule**

| Priority | Rule name                       | Access  | Status   | Actions          |
|----------|---------------------------------|---------|----------|------------------|
| 1        | Okta Verify as Authenticator OK | Allowed | Active ▾ | Info Edit Delete |
| 2        | Password backup                 | Allowed | Active ▾ | Info Edit Delete |



# Global Session Policy

okta

## Edit Rule

Rule name

Exclude users

---

**Policy settings**

IF User's IP is  Manage configuration for [Networks](#)

AND Identity provider is

AND Authenticates via

AND Behavior is

AND Risk is

THEN Access is

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

## 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.

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



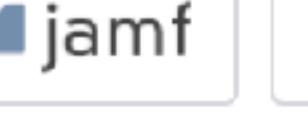
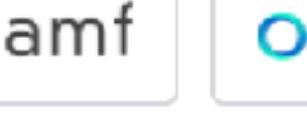
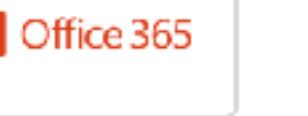
# Authentication policies

okta

**Authentication policies**

Define how a user must authenticate to gain access to an app

[Add a policy](#)

| Policy name   | Applies to   |
|---|--|
| <a href="#">Any two factors</a>   | 0 Apps <a href="#">View</a>  |
| <a href="#">Default Policy</a><br><small>Default</small>  | 6 Apps <a href="#">View all</a><br>   |
| <a href="#">Managed Device Access or Private Access</a><br><small>If device is registered and managed, allow simpler access. Otherwise, require MFA</small> | 3 Apps <a href="#">View all</a><br>   |
| <a href="#">Microsoft Office 365</a><br><small>Application-specific policy</small>  | 1 App <a href="#">View</a><br>  |



[← Back to all Authentication Policies](#)

## Managed Device Access or Private Access

If device is registered and managed, allow simpler access. Otherwise, require MFA

Rules (6) Applications (3)

Actions ▾

Help

Add rule

| Priority | Rule                 | Status  | Actions           |
|----------|----------------------|---------|-------------------|
| 1        | work.email only rule | ENABLED | <a href="#">A</a> |

**IF** Group: Mark's Test Accounts **THEN** Access: Allowed with possession factor  
Device: Registered, Managed

Your org's authenticators that satisfy this requirement:  
1 factor type  
Okta Verify<sup>3</sup>

<sup>3</sup> Phishing resistance may vary based on combinations of apps, browser, operating system, and more. [Learn more](#).

If Okta FastPass is used:  
The user must approve a prompt in Okta Verify or provide biometrics

|   |   |         |                           |
|---|---|---------|---------------------------|
| 4 | Private Access  | ENABLED | <a href="#">Actions ▾</a> |
|   | <b>IF</b> Zone: In zone: Jamf Trust Private Access Cloud Internet Gateway IP Addresses <b>THEN</b> Access: Allowed with possession factor<br>Your org's authenticators that satisfy this requirement:<br>1 factor type<br>Google Authenticator or Okta Verify or FIDO2 (WebAuthn) |         |                           |

If Okta FastPass is used:  
The user must approve a prompt in Okta Verify or provide biometrics

Re-authentication frequency is: Never re-authenticate if the session is active

|   |  |         |                           |
|---|--|---------|---------------------------|
| 5 | Registered and Managed Device  | ENABLED | <a href="#">Actions ▾</a> |
|   | <b>IF</b> Device: Registered, Managed <b>THEN</b> Access: Allowed with possession factor<br>Platform: iOS, MacOS |         |                           |

Your org's authenticators that satisfy this requirement:  
1 factor type  
Okta Verify

If Okta FastPass is used:  
The user must approve a prompt in Okta Verify or provide biometrics



# Authentication policies and device trust

**Edit Rule**

If all of the conditions are true, the authentication settings below will apply. Otherwise, Okta will evaluate the next rule.

Rule name: Registered and Managed Device

**IF**

- IF** User's user type is: Any user type
- AND** User's group membership includes: Any group
- AND** User is: Any user
- AND** Device state is:
  - Any
  - Registered  
Setup Okta Verify as [Authenticator](#)
  - Not managed
  - Managed  
[Go to Device Management](#)
- AND** Device management is:
  - No policy
  - One of the following platforms:
    - iOS ×
    - macOS ×
- AND** Device assurance policy is: No policy
- AND** Device platform is: One of the following platforms:
  - iOS ×
  - macOS ×

**Device state is:**

- Registered

**Device management is:**

- Managed

**Device platform is:**

- iOS (includes iPadOS)
- macOS





# okta

## Registered:

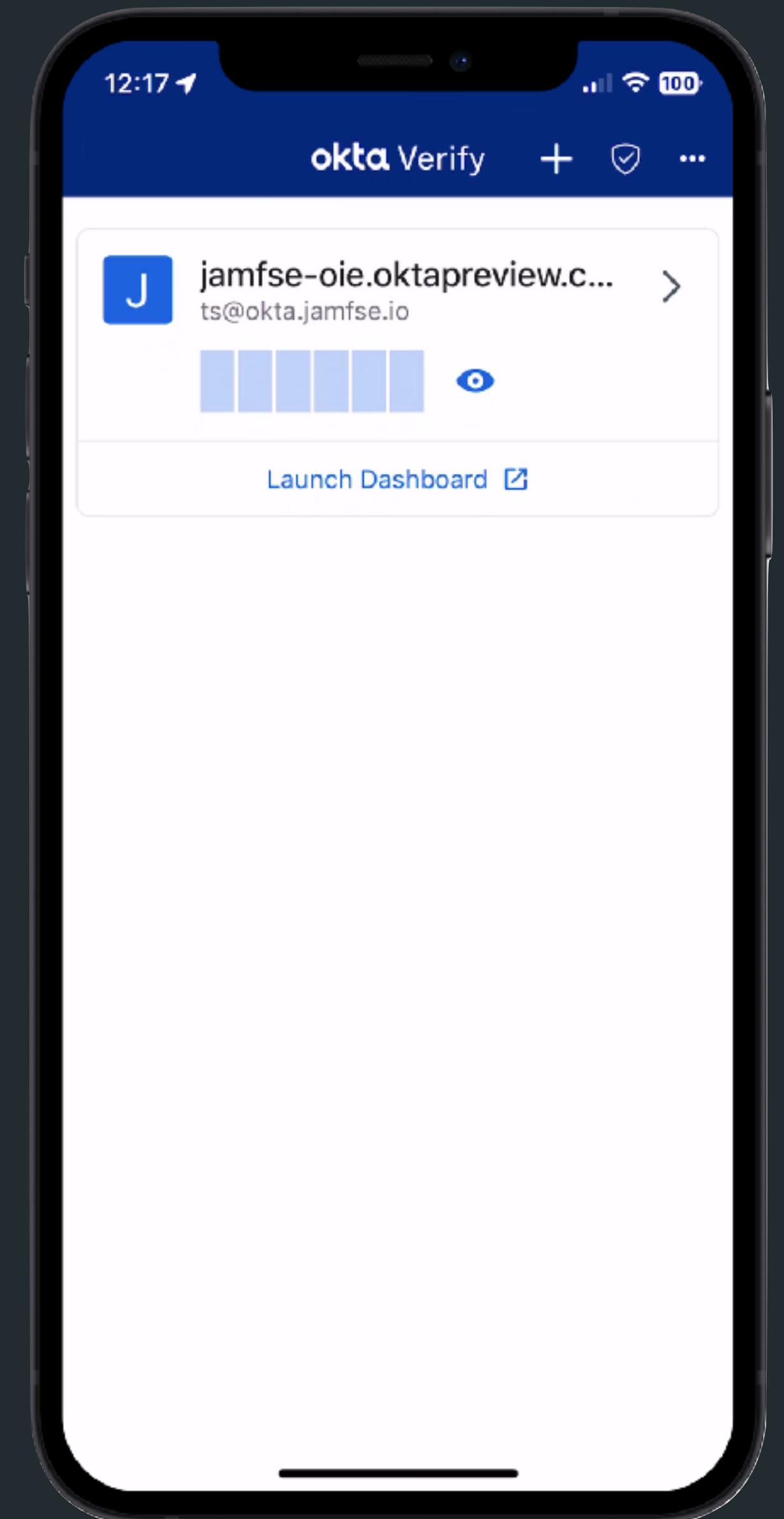
- Okta Verify installed
- User has logged in once
- macOS: Separate keychain created in ~/Library/Keychains



# okta

## Managed:

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



okta

# Okta Device Trust

@

okta



# Okta Device Trust & Authentication Policies

okta

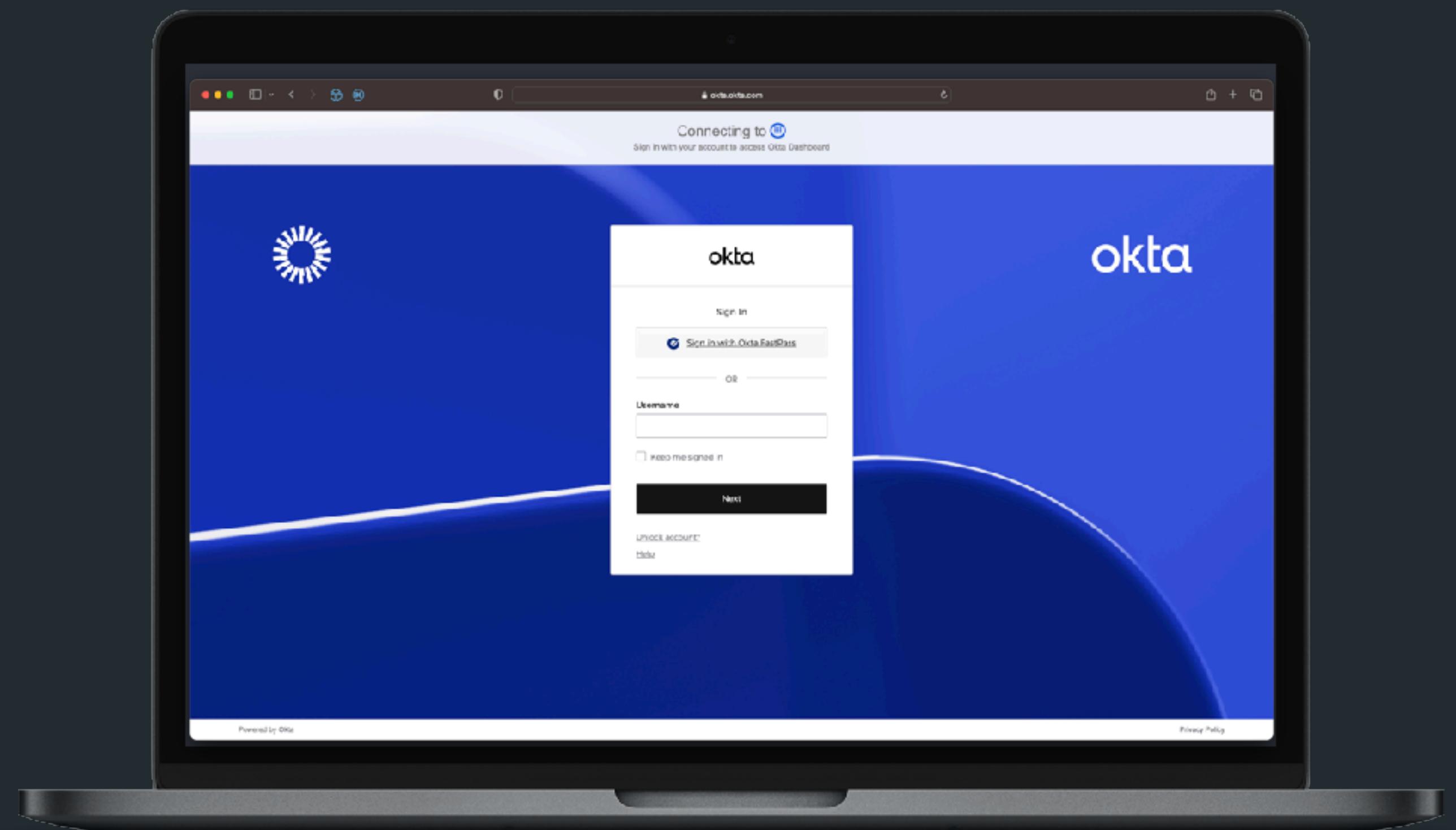
Unmanaged

Low

Medium

Medium Productivity

High



# 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:



# 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

The Okta logo, consisting of the word "okta" in a lowercase, sans-serif font.

## 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**



# 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

The Okta logo, consisting of the word "okta" in a lowercase, sans-serif font.

## 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 WebAuthn**

**Session duration:  
12-hour re-challenge**



# 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 WebAuthn**

## Session duration:

**12-hour re-challenge**

**(Managed)**

**Requires re-auth at each sign-on**



# Okta Device Trust in Action at Okta- High Assurance Policy

The Okta logo, consisting of the word "okta" in a lowercase, sans-serif font.

## 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)**

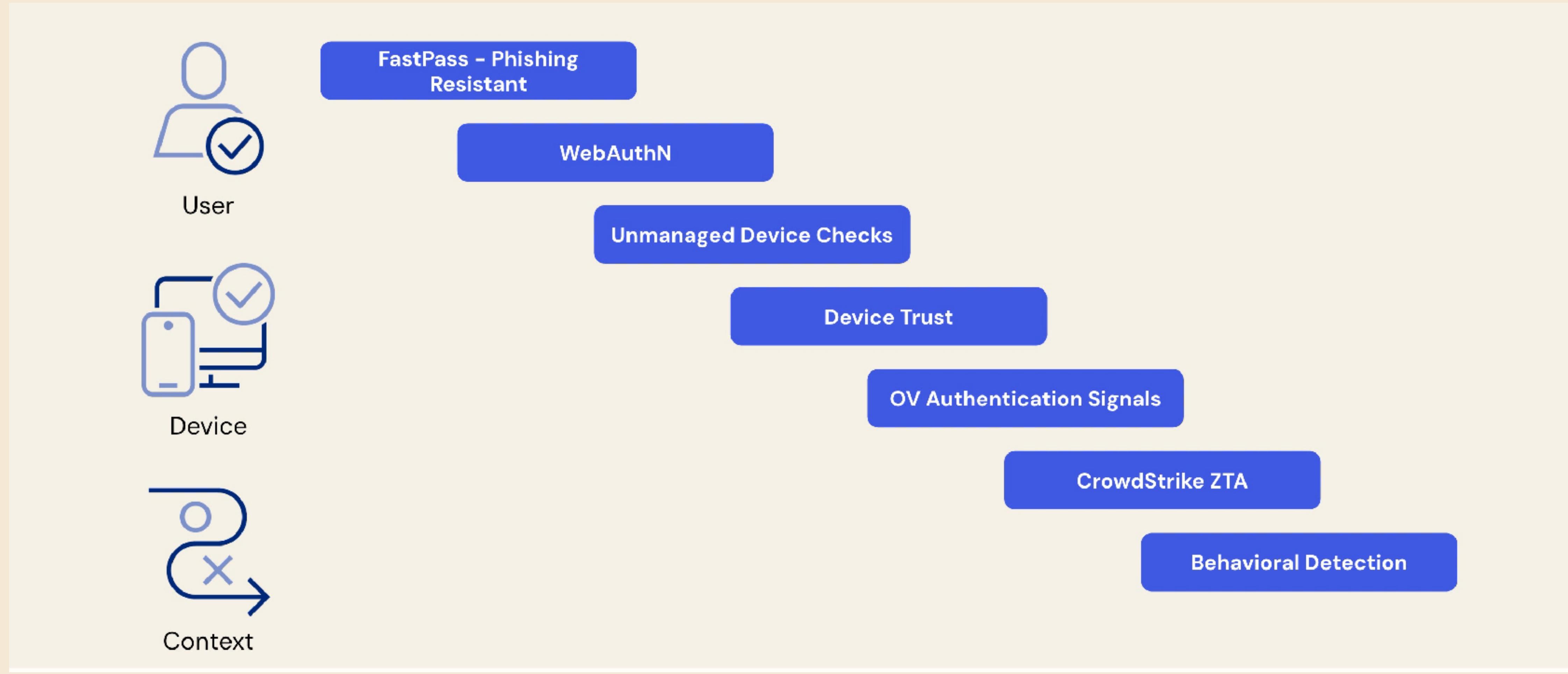
**Password with FastPass (PR  
+ biometric) or WebAuthN  
(Plus pin/biometric)**

**Session duration:**

**Requires re-auth at each  
sign-on**



# Defense in depth Zero Trust Architecture



The Okta logo, consisting of the word "okta" in a lowercase, sans-serif font.

# Configuring Okta Device Trust with Jamf Pro





# Requirements

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



# Configuring Okta Device Trust

## SCEP server in Okta

The screenshot shows the Okta Device Integrations page. The left sidebar has a collapsed navigation tree under Security, with 'Device Integrations' highlighted. The main content area is titled 'Device Integrations' and contains tabs for 'Endpoint management' (selected), 'Certificate authority', 'Endpoint security', and 'Notification services'. A note below the tabs states: 'Endpoint management is a condition that can be applied in an authentication policy to ensure that managed devices have access to an application. For configuration help, [view documentation](#)'.

| Platform  | Certificate authority | Details                    | Status | Actions                 |
|-----------|-----------------------|----------------------------|--------|-------------------------|
| > iOS     | n/a                   | Jamf Pro                   | Active | <a href="#">Actions</a> |
| > Desktop | Okta CA               | Dynamic SCEP URL - Generic | Active | <a href="#">Actions</a> |
| > Desktop | Okta CA               | Static SCEP URL            | Active | <a href="#">Actions</a> |
| > Desktop | Okta CA               | Dynamic SCEP URL - Generic | Active | <a href="#">Actions</a> |

# Configuring Okta Device Trust

## SCEP server in Okta

Device Integrations

Endpoint management   Certificate authority   Endpoint security   Notification services

Add device management platform

1 Select platform   Configure management attestation

Configure management attestation

Integrate Okta with your device management provider. [View setup documentation](#) For an improved end-user authentication experience on macOS, configure SSO extension profile

Certificate authority  Use Okta as certificate authority  Use my own certificate authority [Go to certificate authority](#)

SCEP URL challenge type  Static SCEP URL  Dynamic SCEP URL  Generic  Microsoft Intune (delegated SCEP)

SCEP URL  [Edit](#)  
The base URL for the SCEP server

Challenge URL  [Edit](#)  
URL of the page to use to retrieve the SCEP challenge

Username  [Edit](#)

Password  [Edit](#)  
Please make a note of the password as it will be the only time you will be able to view it.

[Cancel](#) [Save](#)



<https://jamf.it/oktaCA>



# Configuring Okta Device Trust SCEP Payload in Jamf Pro

Computers : Configuration Profiles  
← Okta Device Trust

Options Scope

SCEP

URL The base URL for the SCEP server  
`https://jamfse-oie.oktapreview.com/pki/9C8BDBE64F1D582DD2AC0251E016B08B2374B88F/scep/ac47dutjWQWG60M1d7`

Name The name of the instance: CA IDENT  
`JamfSE-OIE`

Redistribute Profile  
Redistribute the profile automatically when its SCEP issued certificate is the specified number of days from expiring. Configuring this option adds "\$PROFILE\_IDENTIFIER" to the Subject field

5 Days

Subject Representation of a X.500 name (e.g. "O=CompanyName, CN=Name")  
`CN=$PROFILE_IDENTIFIER`

Subject Alternative Name Type The type of a subject alternative name  
None

Challenge Type Type of challenge password to use  
Dynamic-Microsoft CA

URL To SCEP Admin URL of the page to use to retrieve the SCEP challenge  
`https://jamfse-oie.oktapreview.com/api/v1/certificateAuthorities/9C8BDBE64F1D582DD2AC0251E016B08B2374B88F/registrationAuthorities/ac47dutjWQWG`

Username Username in the down-level logon name format required to log in to the SCEP Admin page  
`okta-WQSGVA`

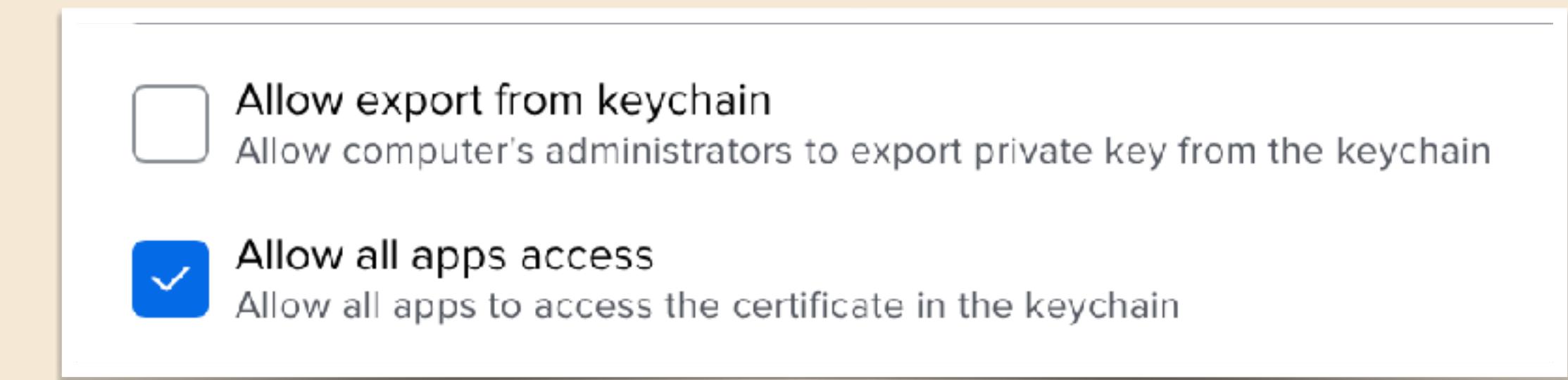
Password Password to use to log in to the SCEP Admin page  
.....

Verify Password  
.....

Retries Number of times to retry after PENDING response  
5

Retry Delay Number of seconds to wait before each retry  
180 Seconds

Cancel Save



<https://jamf.it/oktaCA>

# Configuring Okta Device Trust managementHint for iOS / iPadOS

The screenshot shows the Okta Device Integrations page. The left sidebar has a collapsed navigation menu with sections like Dashboard, Directory, Customizations, Applications, and Security (expanded). Under Security, there are sub-options: General, HealthInsight, Authenticators, Authentication Policies, Global Session Policy, Profile Enrollment, Identity Providers, Delegated Authentication, Networks, Behavior Detection, Device Assurance Policies, Device Integrations (selected), and Administrators. The main content area is titled "Device Integrations" and has tabs for Endpoint management, Certificate authority, Endpoint security, and Notification services. The "Endpoint management" tab is selected. A sub-section explains that endpoint management is a condition applied in authentication policies to ensure managed devices have access. It includes a link to documentation. Below this is a table titled "Add platform" with columns: Platform, Certificate authority, Details, and Status. The table lists four entries:

| Platform  | Certificate authority | Details                    | Status | Actions                   |
|-----------|-----------------------|----------------------------|--------|---------------------------|
| > iOS     | n/a                   | Jamf Pro                   | Active | <a href="#">Actions ▾</a> |
| > Desktop | Okta CA               | Dynamic SCEP URL - Generic | Active | <a href="#">Actions ▾</a> |
| > Desktop | Okta CA               | Static SCEP URL            | Active | <a href="#">Actions ▾</a> |
| > Desktop | Okta CA               | Dynamic SCEP URL - Generic | Active | <a href="#">Actions ▾</a> |

# Configuring Okta Device Trust managementHint for iOS / iPadOS

Device Integrations

Endpoint management   Certificate authority   Endpoint security   Notification services

Add device management platform

Select platform   Configure management attestation

Configure management attestation

Integrate Okta with your device management provider. [View setup documentation](#) For an improved end-user authentication experience, [configure SSO extension profile](#)

Secret key: a9kN8-aq4MOATWUXfPK7XZm [Copy](#)

Important: Make a note of the secret key as it will be the only time you will be able to view it. After this, it will be stored as a hash for your protection.

Device management provider: Jamf Pro  
12 characters remaining  
Input will be inserted into end-user enrollment flows in order to display device management provider.

Enrollment link: <https://your-tenant.jamfcloud.com/enroll>

Cancel   Save



<https://jamf.it/oktaiOS>

# Configuring Okta Device Trust

## Deploy Okta Verify app to devices

The screenshot shows the Jamf Pro interface for managing Mac Apps. The left sidebar includes sections for Computers, Inventory, Content Management (Policies, Configuration Profiles, Restricted Software, Mac Apps), Groups, Enrollment (Enrollment Invitations, PreStage Enrollments), and Settings (Management Settings). The main panel displays the 'Okta Verify - Automatic Installation' configuration under 'Managed Distribution'. Key settings include:

- Display Name:** Okta Verify - Automatic Installation
- Enabled:** Checked
- Category:** Okta Single Sign-On
- Version:** 9.0.0
- Bundle Identifier:** com.okta.mobile
- Free:** Checked
- Schedule Jamf Pro to automatically check the App Store for app updates:** Checked
- App Store Country Or Region:** United States
- App Store Sync Time:** 6:00 p.m.
- Automatically Force App Updates:** Checked
- Force App Update:** Force Update
- App URL:** https://apps.apple.com/us/app/okta-verify/id490179405?uo=4
- Distribution Method:** Install Automatically/Prompt Users to Install

The screenshot shows the Okta Verify configuration page in the Jamf Pro interface. The top navigation bar includes 'Mobile Devices : Mobile Device Apps' and a back arrow labeled '← Okta Verify'. The tabs at the top are General, Scope, Self Service, Managed Distribution, and App Configuration. The General tab is selected. Key settings include:

- Display Name:** Okta Verify
- Enabled:** Checked
- Category:** Okta Single Sign-On
- Short Version:** 9.0.0
- Bundle Identifier:** com.okta.mobile
- Free:** Checked
- Distribution Method:** Make Available in Self Service
- Display app in Self Service after it is installed:** Checked
- Schedule Jamf Pro to automatically check the App Store for app updates:** Checked
- App Store Country Or Region:** United States
- App Store Sync Time:** 6:00 p.m.
- Automatically Force App Updates:** Unchecked
- Make app managed when possible:** Checked
- Convert unmanaged app to managed:** Checked
- Remove app when MDM profile is removed:** Unchecked
- Prevent backup of app data:** Unchecked
- Allow users to remove app (iOS 14 or later):** Unchecked

# Configuring Okta Device Trust

## Deploy Okta Verify app to devices

The screenshot shows two overlapping Jamf Pro application windows. The top window is titled "Mobile Devices : Mobile Device Apps" and "Okta Verify". It has tabs for General, Scope, Self Service, Managed Distribution, and App Configuration. The General tab is selected, showing fields for Display Name (Okta Verify), Enabled (checked), Category (Okta Single Sign-On), and Short Version. A large red arrow points from the bottom window to the App Configuration tab. The bottom window is also titled "Mobile Devices : Mobile Device Apps" and "Okta Verify". It has tabs for General, Scope, Self Service, Managed Distribution, and App Configuration. The App Configuration tab is selected, showing a section titled "Preferences" with the subtext "Configuration dictionary to be applied to the app on mobile devices with iOS 7 or later". Inside this section is a blue-bordered code block containing the following PLIST code:

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

Below the code block is a note: "For help generating the PLIST file for preferences, use the [AppConfig Generator](#)".

# 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

### Configure management attestation

Integrate Okta with your device management provider. [View setup documentation ↗](#)

For an improved end-user authentication experience, [configure SSO extension profile ↗](#)



# Configuring Okta Device Trust

## BONUS GAME: Single Sign On Extension

← Okta Fast Pass - Okta Identity Engine Preview

Options Scope

Search...  
Lock Screen Message  
Not configured

iMacOS Server Accounts  
Not configured

Mail  
Not configured

Network Usage Rules  
Not configured

Notifications  
Not configured

Passcode  
Not configured

Restrictions  
Not configured

SCPL  
Not configured

Skip Setup Items  
Not configured

Single App Mode  
Not configured

Single Sign On  
Not configured

Single Sign-On Extensions  
1 payload configured

Single Sign-on Extension  
Configure app extensions that perform single sign-on (iOS 13 or later).

Payload Type  
Use the Kerberos payload type for the "com.apple.AppSSOKerberosExtension" Extension Identifier.

SSO: Kerberos

Extension Identifier  
Bundle identifier of the app extension that performs single sign-on  
com.okta.mobile.auth-service-extension

Team Identifier  
The team identifier of the app extension that performs single sign-on

Sign-on Type  
Sign-on authorization type

Credentials [ Redirect ]

Realm  
Realm name for the Credential type payload. This value must be properly capitalized.  
Okta Device

Hosts  
Hostnames that can be authenticated through the app extension. Names must be unique for all configured Single Sign-On Extensions payloads.

jamfse-ple.oktapreview.com

Add

Setting

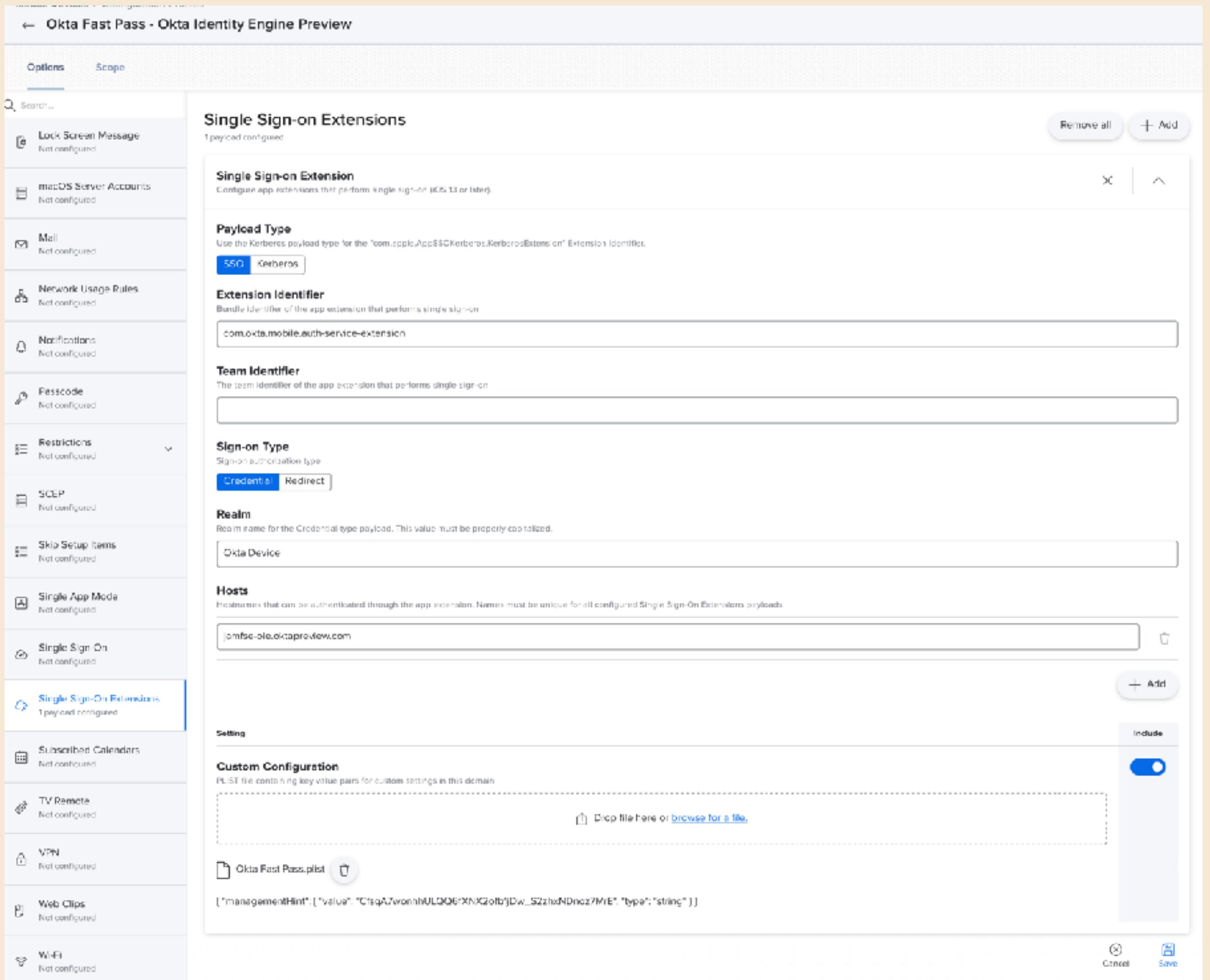
Custom Configuration  
PLIST file containing key value pairs for custom settings in this domain

Drop file here or [browse for a file](#)

Okta Fast Pass.plist

["managementHint": {"value": "CfsgAJwomhHULQG6/XNKGofbJDw\_52zhxDNoz7M/E", "type": "string"}]

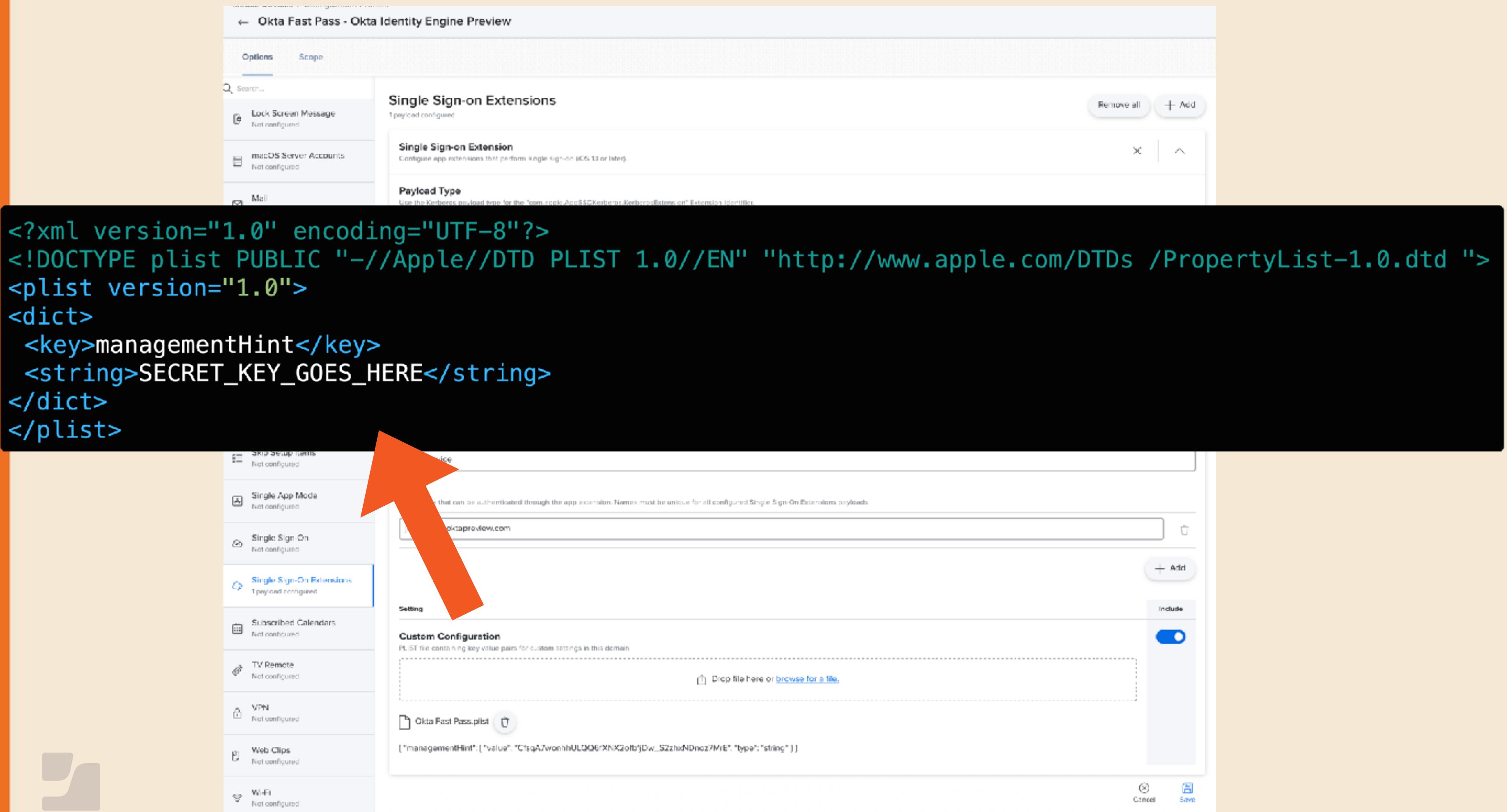
Cancel Save



<https://jamf.it/oktaSSOe>

# Configuring Okta Device Trust

## BONUS GAME: Single Sign On Extension



The screenshot shows the Okta Identity Engine Preview interface. In the main pane, under "Single Sign-on Extensions", there is one payload configured. Below it, a "Payload Type" section provides instructions for using the Kirby's payload type. A large black box covers the configuration details of the extension. At the bottom, a modal dialog is open, titled "Okta Fast Pass - Okta Identity Engine Preview". It shows a file upload interface with a ".plist" file selected, labeled "Okta Fast Pass.plist". A red arrow points from the configuration interface up towards this dialog.

```
<?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>

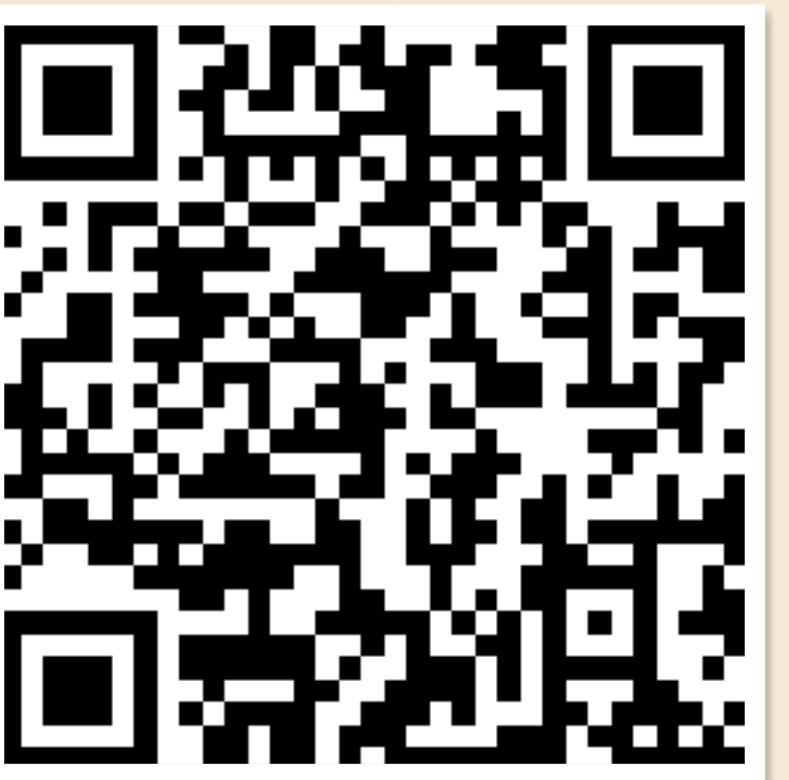
# Configuring Okta Device Trust

## BONUS GAME: Single Sign On Extension

**Single Sign-on Extensions**  
1 payload configured

**Single Sign-on Extension**  
Configure app extensions that perform single sign-on (macOS 10.15 or later, User Approved MDM required).

|  |  |
|--|--|
| <b>Payload Type</b><br>The payload type  | SSO                                    |
| <b>Extension Identifier</b><br>Bundle identifier of the app extension that performs single sign-on   | com.okta.mobile.auth-service-extension |
| <b>Team Identifier</b><br>The team identifier of the app extension that performs single sign-on  | B7F62B65BN                             |
| <b>Sign-on Type</b><br>Sign-on authorization type  | Credential                             |
| <b>Realm</b><br>Realm name for the Credential-type payload. This value must be properly capitalized.   | Okta Device                            |
| <b>Hosts</b><br>Hostnames that can be authenticated through the app extension. Names must be unique for all configured Single Sign-On Extensions payloads. | jamfse-oie.oktapreview.com             |



<https://jamf.it/oktaSSOe>







# Configuring Okta Device Trust

## Determining which rules applied

|   |                   |                              |                              |
|---|-------------------|------------------------------|------------------------------|
| ⌚ Jul 31 13:05:22   | Trade Show (User) | Evaluation of sign-on policy | H2WGW2C9Q6NV (UDDevice)      |
|   |                   | ALLOW                        | Okta Dashboard (AppInstance) |
|   |                   |                              | 2 more targets               |
| <a href="#">Expand All</a>  |                   |                              |                              |
| <ul style="list-style-type: none"><li>▶ Actor Trade Show(id: 00u8404t7ur6pb8Fp1d7)</li><li>▶ Client SAFARlOnMac OS XComputerfrom98.97.113.222</li><li>▶ Device guo97uq7evGRTG5cr1d7Macmini9,1</li><li>▶ Event allow policy.evaluate_sign_on(id: ZMgUAc19LnwNDxFs1j_X0QAAkI)</li><li>▶ Request</li><li>▼ Target<ul style="list-style-type: none"><li>AlternatId unknown</li><li>DetailEntry H2WGW2C9Q6NV</li><li>DisplayName guo97uq7evGRTG5cr1d7</li><li>ID UDDevice</li><li>Type</li></ul></li><li>▼ Target<ul style="list-style-type: none"><li>AlternatId Okta Dashboard</li><li>DetailEntry Okta Dashboard</li><li>DisplayName Ooa2eugriorMuufv11d7</li><li>ID AppInstance</li><li>Type</li></ul></li><li>▼ Target<ul style="list-style-type: none"><li>AlternatId unknown</li><li>DetailEntry Okta Verify as Authenticator OK</li><li>DisplayName 0pr4x8bfndPQeCmx1d7</li><li>ID Rule</li><li>Type</li></ul></li><li>▼ Target<ul style="list-style-type: none"><li>AlternatId unknown</li><li>DetailEntry JNUC 2023 Demo</li><li>DisplayName rui8cek1qnIUS5kVu1d7</li><li>ID Rule</li><li>Type</li></ul></li></ul> |                   |                              |                              |



# **How does Okta Device Trust affect Jamf Connect**



# Jamf Connect and OIE

**Jamf Connect with Okta Authentication API  
(The “usual” way)**

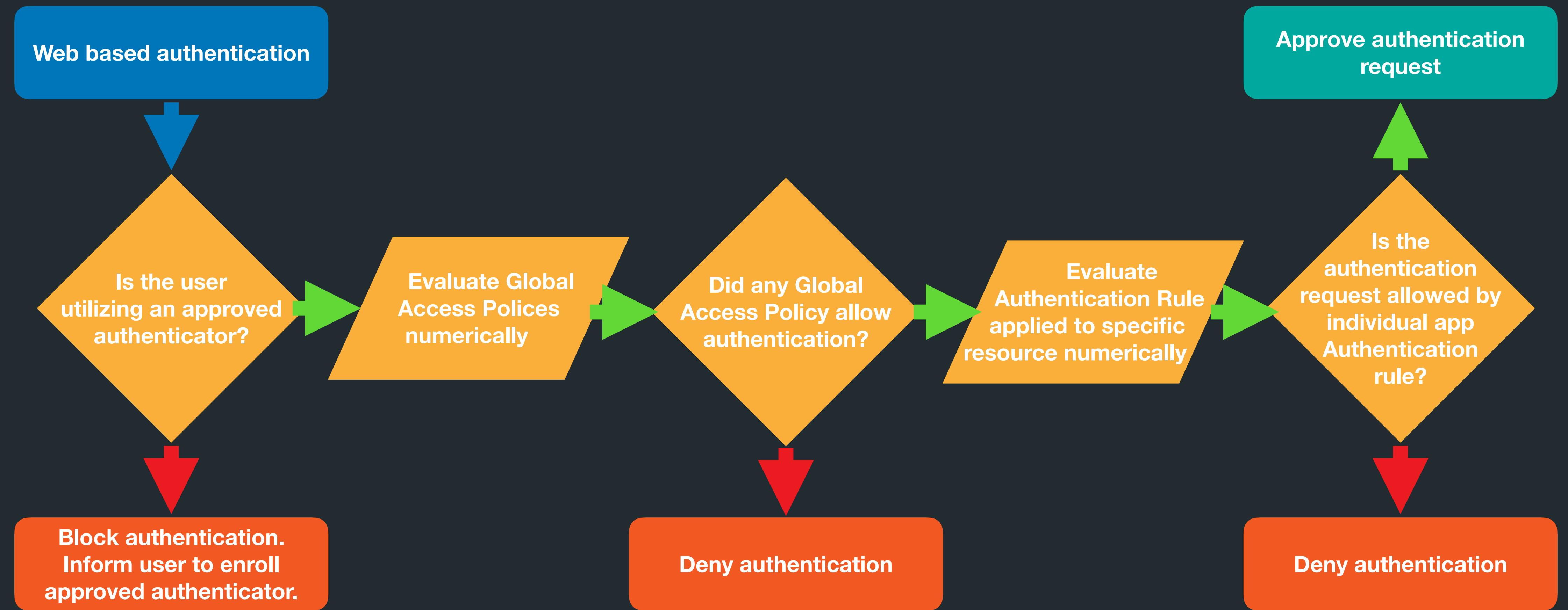
**Jamf Connect with Okta as an OIDC Application**

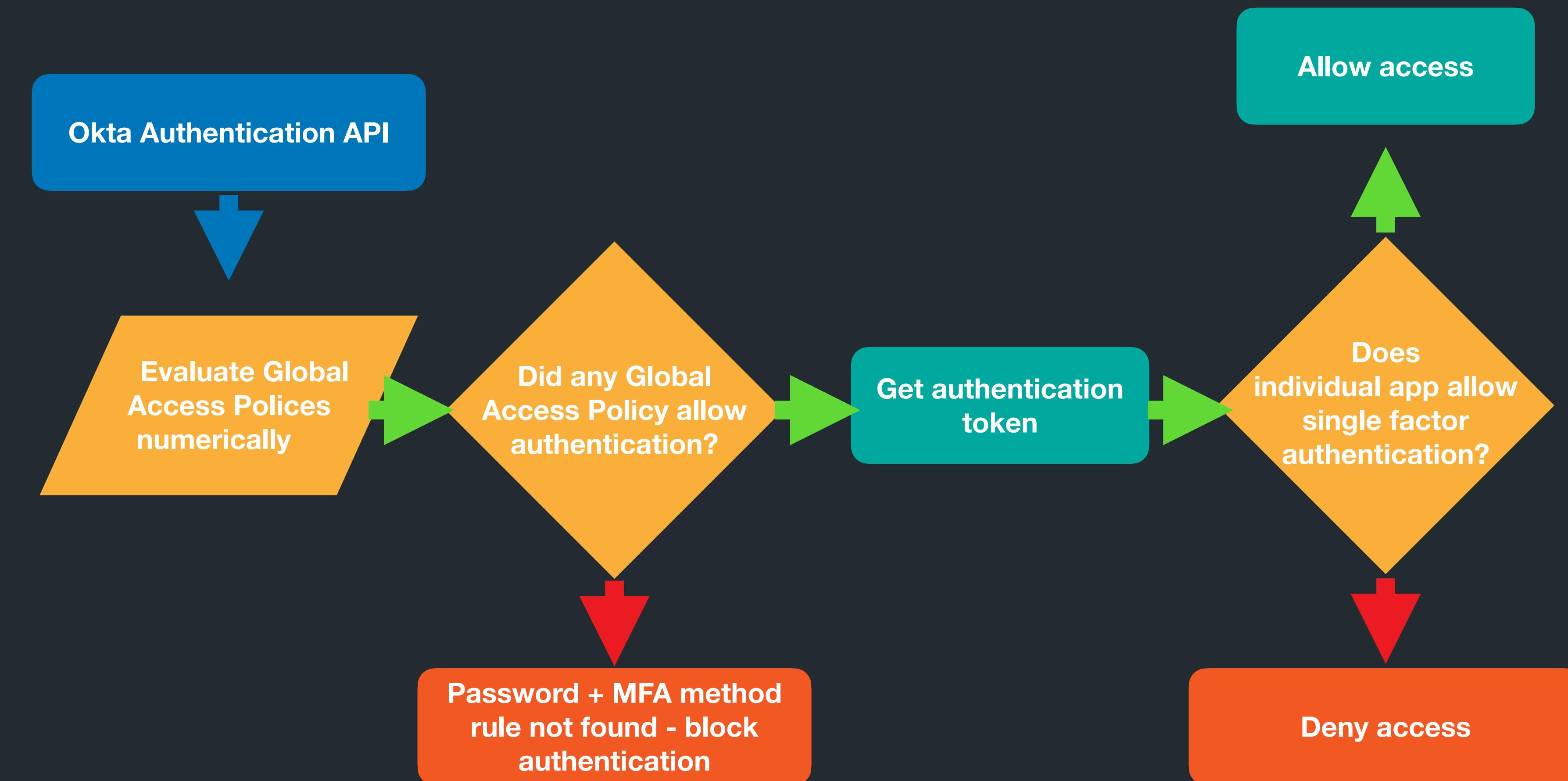
**Rules Applied**

Global Session Policy ONLY

Global Session Policy  
Authentication Policy







# Jamf Connect and OIE

**Jamf Connect with Okta Authentication API  
(The “usual” way)**

**Jamf Connect with Okta as an OIDC Application**

## Gotchas

OIDC apps for Admin rights, Access rights, Secondary account creation rights require OIDC app - watch your Authentication rules!

Can't restrict creating “second” account on device short of disabling login window



# Jamf Connect and OIE

**Jamf Connect with Okta Authentication API  
(The “usual” way)**

**Jamf Connect with Okta as an OIDC Application**

## Benefits

Enforcement of the “Restrict Second Account” creation

More granular control over authentication rules  
Okta login shown as a webview





# Jamf and Okta Device Trust

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



The Okta logo, consisting of the word "okta" in a lowercase, sans-serif font.

Thank you for  
listening!

