

In this lab, you will unlock the combined power of Okta Verify and FastPass. You will enable an experience where passwordless authentication becomes an integral part of an employee’s workday, boosting employee productivity without the common password pitfalls. Not only will you discover an enhanced security posture resistant to phishing threats, but you’ll also appreciate the inherent protection it offers, sometimes even against our own human errors.

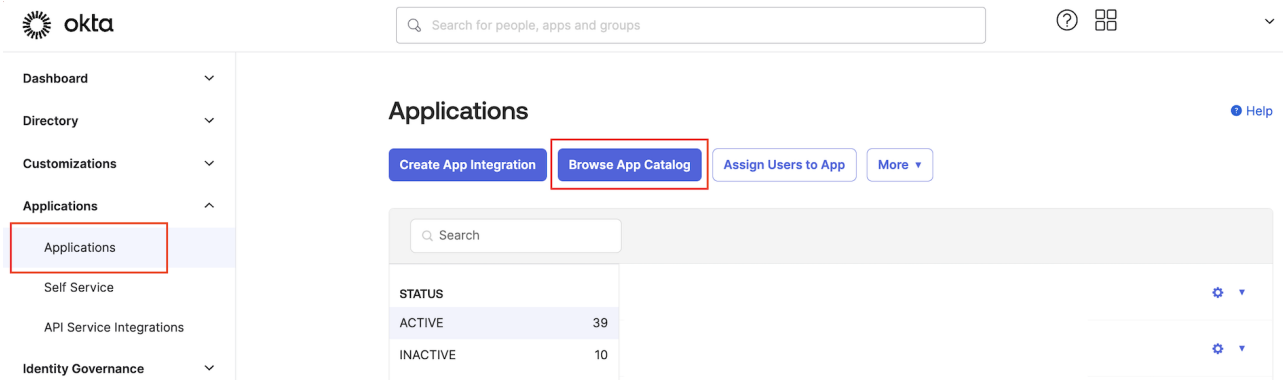
Prerequisites

Create a Bookmark app

We are going to create a "fake" application that will be used for demonstrate security policies.

The application is a simple bookmark, but it's useful for try and test the policies without the need of a real application.

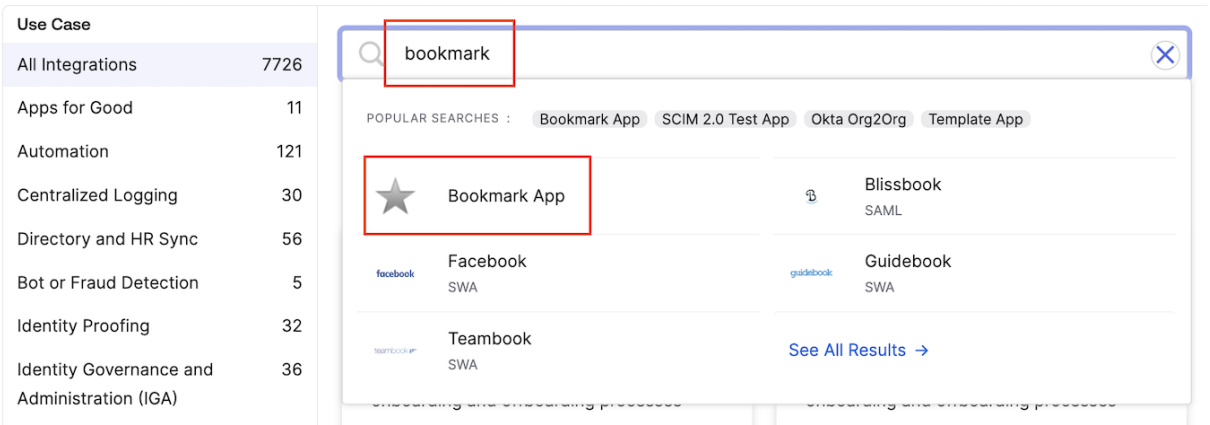
- 1. Go on **Applications** and click on **Browse App Catalog**



- 2. Type **bookmark** in the search bar and click on **Bookmark App**

Browse App Integration Catalog

Create New App



- 3. Click on **Add Integration**

Last updated: October 21, 2021

[Add Integration](#)

Bookmark App

4. Compile the form with the following data:


Application label	Marketo
URL	https://www.okta.com/products/adaptive-multi-factor-authentication/

And click **Done**

General settings- Required


Application label	<input type="text" value="Marketo"/>
	This label displays under the app on your home page
URL	<input type="text" value="https://www.okta.com/products/adaptive-multi-factor-a"/>
	The URL of the sign-in page for this app
Request Integration	<input type="checkbox"/>
	Would you like Okta to add an integration for this app?
Application Visibility	<input type="checkbox"/> Do not display application icon to users
Cancel	Done

5. Click on **Assign** and then on **Assign to Groups**



An Adobe Company

Active ▾

View Logs

General

Sign On

Assignments

Assign ▾

Convert assignments ▾

Assign to People


Assign to Groups

File		Type
People		
Groups		011
		011
		011


6. Click on **Assign** on the right of *Everyone*

Assign Marketo to Groups


Search...

EMEA
oktaice.local/Employees/EMEA

Assign

Engineering
oktaice.local/Employees/Engineering

Assign

Everyone
All users in your organization

Assign

Note: it's not a best practice to assign applications to Everyone. Instead is better to use Okta or Active Directory groups.

7. Click **Done**

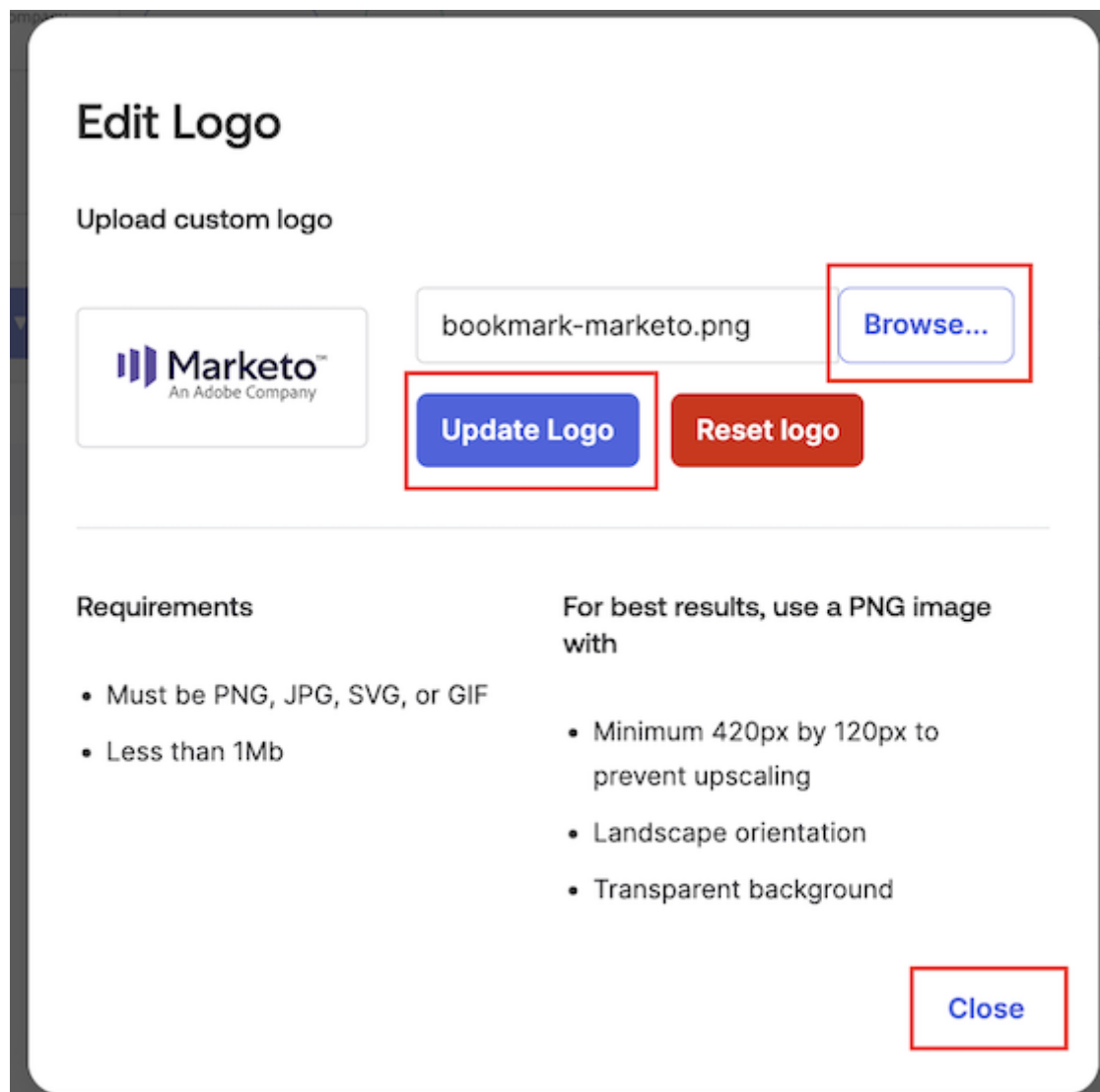
8. (optional) Click on the star icon for upload the app logo



8.1. Save the following image:



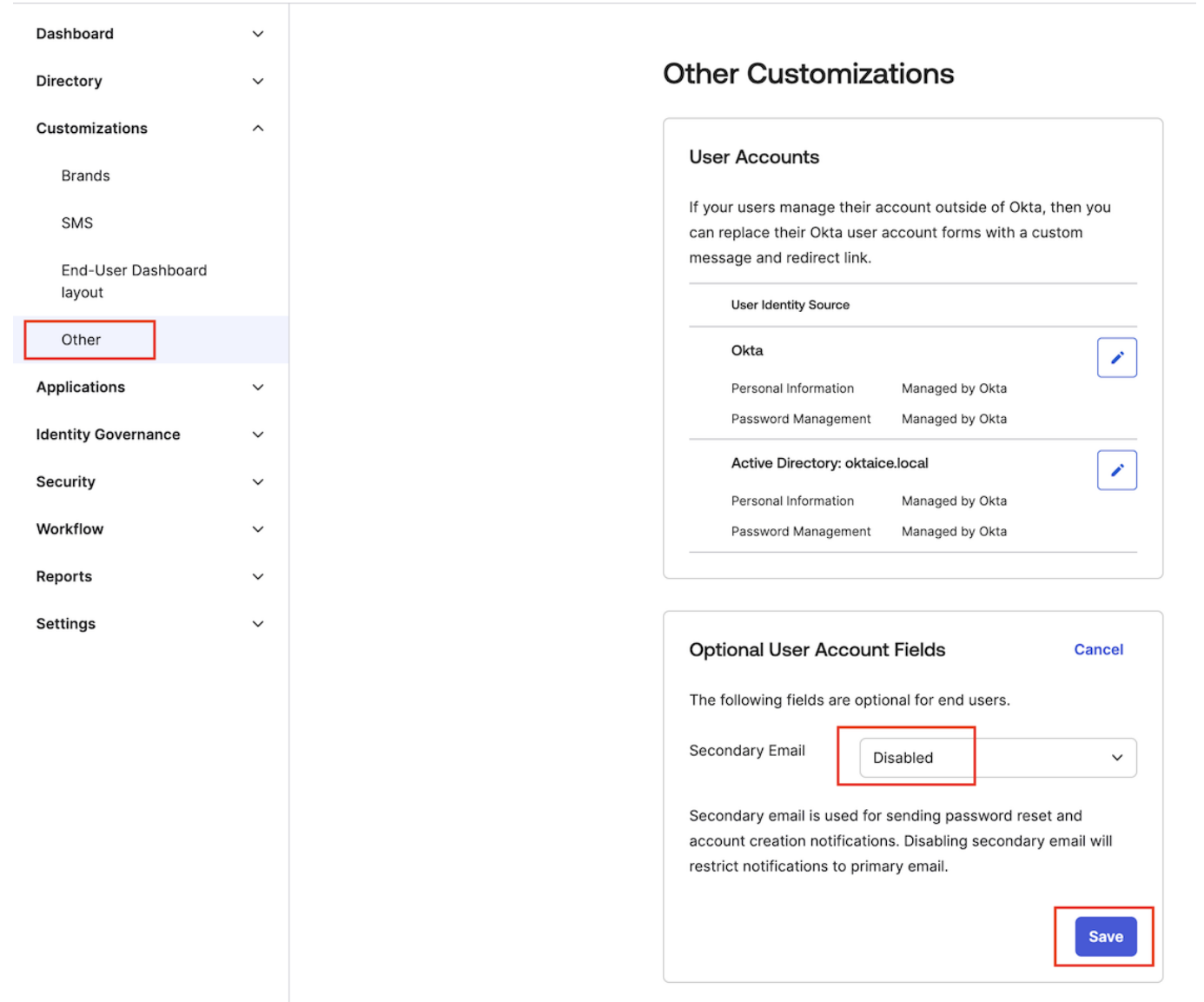
8.2. **Browse** for the saved image, click on **Update Logo** and then **Close**



Disable secondary email

On **Customization / Other** edit the **Optional User Account Fields**.

Set the **Secondary Email** to **Disabled**



Setup Okta FastPass on the Virtual Desktop

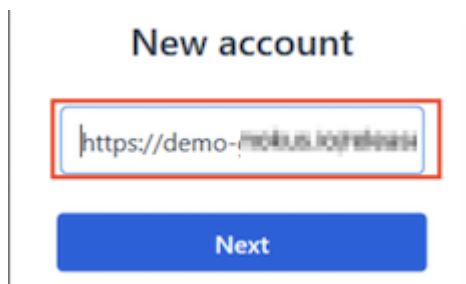
Install Okta Verify on your Virtual Desktop

1. In the **Virtual Desktop**, download the **Okta Verify** setup:
https://{{idp.name}}.okta.com/api/v1/artifacts/WINDOWS_OKTA_VERIFY/download?releaseChannel=GA
2. Run the executable
3. In the Okta Verify installation window, select **I agree to the License terms and conditions**, and then click **Install**. Wait for confirmation saying that Okta Verify was successfully installed.
4. Click **Finish**.
5. Close the **Download** window.

Add New Employee Account to Okta Verify

1. In the **Virtual Desktop**, open the **Okta Verify** application.

2. On **Welcome to Okta Verify**, click **Get started**.
3. Click **Next**.
4. For **New Account**, enter `https://{{idp.name}}.okta.com`



5. Click **Next**. This will open your Okta tenant's sign-in page.
6. Sign in with the username and password of an existing user (e.g. `emily.boone@oktaice.com`).

Note: Password for all Active Directory users is `Tra!nme4321`

7. Close the Okta Verify window, and then close the browser.

Configure Security Policies and FastPass

Enable Okta Verify for FastPass Authentication

1. Return to your **Okta Admin Console** browser session.
2. In the Admin Console, select **Security > Authenticators**.
3. For **Okta Verify**, click **Actions**, and then select **Edit**.
4. For **Okta FastPass** select **Show the "Sign in with Okta FastPass" button**.

Okta FastPass

Sign-in page option

☒ Show the "Sign in with Okta FastPass" button



What does this button do? [↗](#)

5. Scroll down and click **Save**.

Add a rule to the Default Policy

1. In the Admin Console, select **Security > Authentication Policies**.

- 2. Select the **Any two factors** authentication policy.
- 3. Click **Add Rule**.
- 4. Set the **Rule name** to **Okta FastPass**
- 5. Set the following **IF** conditions for the rule:

IF	Value
User's type is	<i>Any user type</i>
User's group membership includes	At least one of the following groups:
Enter groups to include:	HR and Management
Device state is:	Registered

Add Rule

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

Rule name

Okta FastPass

IF

IF

User's user type is

Any user type

AND

User's group membership includes

At least one of the following groups:

And none of the following groups:

Enter groups to exclude...

[Go to Groups](#)

AND

User is

Any user

AND

Device state is

Any

Registered

Setup Okta Verify as Authenticator

Not managed

AND

Device management is

TODO CHANGE IMAGE

- 6. Set the following **THEN** access and authentication settings for the rule:

THEN
User must authenticate with: Possession factor

7 / 25

THEN

If Okta FastPass is used

The user is not required to approve a prompt in Okta Verify or provide biometrics

THEN

THEN

Access is

☐ Denied

☒ Allowed after successful authentication

AND

User must authenticate with

Possession factor

AND

Possession factor constraints are

☐ Phishing resistant

☐ Hardware protected

☒ Exclude phone and email authenticators

AND

If Okta FastPass is used

☐ The user must approve a prompt in Okta Verify or provide biometrics

☒ The user is not required to approve a prompt in Okta Verify or provide biometrics

7. Click **Save**.

8. Verify that the **Okta FastPass** rule is up to **Priority 1** in the list of rules for the policy.

Priority	Rule	Status	Actions
1	Okta FastPass	ENABLED	Actions ▾

9. Click on **Actions** in the top-right corner and then **Edit name and description**

10. Change the name to **Standard Security Apps** and the description to **Default Passwordless access**

Experience an Employee Passwordless Login

1. Return to your **Virtual Desktop**.
2. In the Virtual Desktop, launch a Chrome browser using the **Chrome** shortcut on the desktop.
3. Open your Okta tenant: `https://{{idp.name}}.okta.com`
4. You will automatically be authenticated to your End-User Dashboard. No prompts, no typing, pure magic!
5. Sign out of Okta.
6. At the Okta login, click **Sign in with Okta FastPass**. Again, you will be signed in to the End-User Dashboard, no password required.

Set Up Device Assurance

Add a Device Assurance Policy

With device assurance policies you can check security-related device attributes as part of your authentication policies.

1. Return to your **Okta Admin Console** browser session.
2. In the Admin Console, select **Security > Device Assurance Policies**.
3. Click **Add a policy**.
4. Set **Policy name** to **Windows 11**
5. For **Platform**, select **Windows**.
6. For **Minimum Windows version**, select **Windows 11 (22H2)**.
7. For **Lock Screen**, deselect **Windows Hello must be enabled**.
8. Click **Save**.

Add device assurance policy

Policy name

Windows 11

Platform

☐ Android

☐ ChromeOS

☐ iOS

☐ macOS

☒ Windows

Device attribute provider(s)

☒ Okta Verify

☐ Chrome Device Trust

Windows

Minimum Windows version

☒ Use a preset version

Windows 11 (21H2)

☐ Customize

Major

Minor

Build

Rev

Current minimum Windows: Windows 11 (21H2)

Lock screen

☐ Windows Hello must be enabled

Disk encryption

☐ Device disk must be encrypted

Trusted Platform Module

☐ Device uses a Trusted Platform Module

Save

Cancel

Add an "High Security Apps Policy" to include Device Assurance Policy

- 1. In the Admin Console, select **Security > Authentication policies**.
- 2. Click **Add a policy**
- 3. Insert the following information:

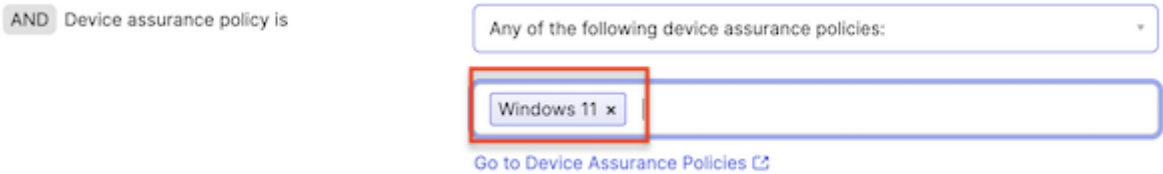
Name	High Security Apps
------	--------------------

Description Policy for High Security Apps with Device Assurance

- 4. Click **Add Rule**.
- 5. Set the **Rule name** to **Windows 11 or higher**
- 6. Set the following **IF** conditions for the rule:

IF	Value
User's type is	<i>Any user type</i>
User's group membership includes	At least one of the following groups:
Enter groups to include:	HR and Management
Device state is:	Registered
Device assurance policy is	Any of the following device assurance policies:

and then select **Windows 11**



- 7. Set the following **THEN** access and authentication settings for the rule:

THEN	
User must authenticate with:	Possession factor
If Okta FastPass is used	The user is not required to approve a prompt in Okta Verify or provide biometrics

THEN

THEN

Access is

☐ Denied

☒ Allowed after successful authentication

AND

User must authenticate with

Possession factor

AND

Possession factor constraints are

☐ Phishing resistant

☐ Hardware protected

☒ Exclude phone and email authenticators

AND

If Okta FastPass is used

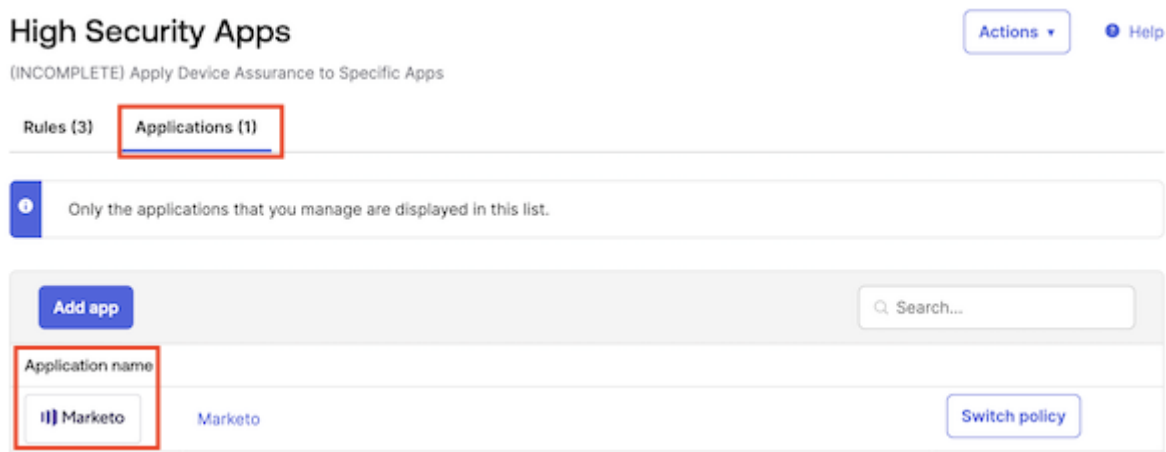
☐ The user must approve a prompt in Okta Verify or provide biometrics

☒ The user is not required to approve a prompt in Okta Verify or provide biometrics

8. Click **Save**.
9. For the **Catch-all Rule** Rule, click **Actions**, and then select **Edit**.
10. On the **THEN** section set **Access is : Denied**
11. Click save

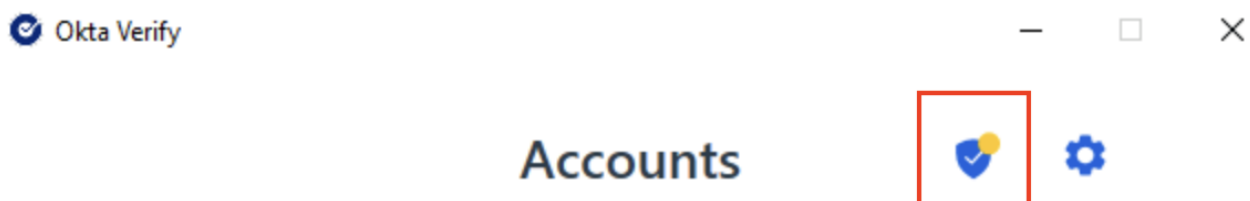
Add Marketo to the High Security Apps Policy

1. In the **High Security Apps** policy, select the **Applications** tab.
2. Click **Add app**.
3. Locate **Marketo** in the list of apps, and then click **Add**.
4. Click **Close**.

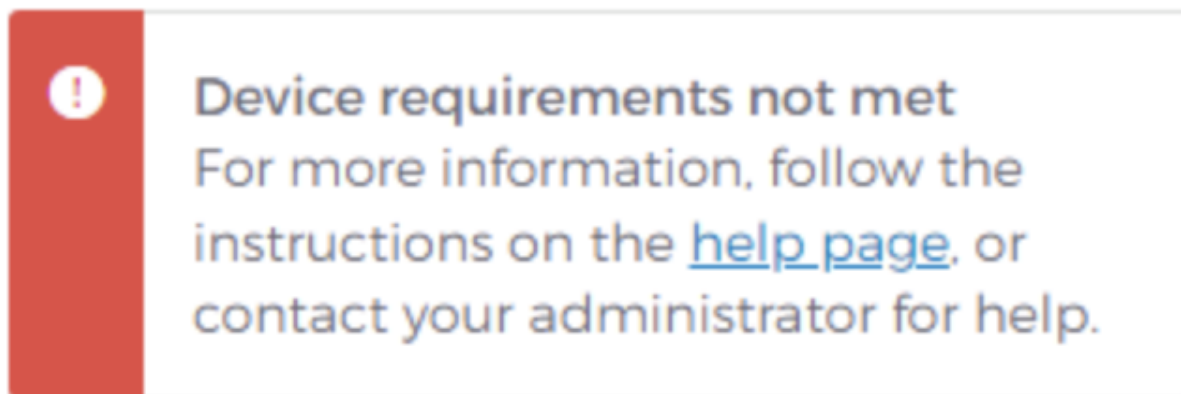


Test the Device Assurance Policy

1. Return to your **Virtual Desktop**.
2. In your Virtual Desktop, open the **Okta Verify** app.
3. On the **Accounts** page, click the device health icon to verify that your OS version is version 10.



4. In your Virtual Desktop, sign into your Okta tenant as **emily.boone@oktaice.com**.
5. Select the **Marketo** app. You will be denied access because your device does not meet the device assurance policy.



Switch the Authentication Policy for Marketo

1. Return to your **Okta Admin Console** browser session.
2. In the Admin Console, select **Security > Authentication Policies**.
3. Select **High Security Apps > Applications** tab.
4. For the **Marketo** app, click **Switch Policy**.
5. Select the **Standard Security Apps** policy, and then click **Save**.

Change an Authentication Policy

Use this policy for Marketo

Standard Security Apps

[View all authentication policies](#)

6. Return to your Virtual Desktop and verify that your new employee can now access the **Marketo** app.

Note: With the exception of Office 365, the apps in this lab are Bookmark apps. Bookmark apps are used to direct users to a specific web page. Real app integrations do exist in the Okta Integration Network for all of the apps shown in this lab.

Enable Okta ThreatInsight

Okta ThreatInsight aggregates data about sign-in activity across the Okta customer base to analyze and detect potentially malicious IP addresses and to prevent credential-based attacks such as: password spraying, credential stuffing, and brute-force cryptographic attacks. Because ThreatInsight collects information about the origin of sign-in activity directed at Okta organizations and Okta endpoints, it provides a security baseline for all Okta customers.

To enable Okta ThreatInsight, proceed with the following steps:

1. Return to your **Okta Admin Console** browser session.

2. In the Admin Console, select **Security > General**.
3. Scroll down to Okta ThreatInsight settings and click **Edit**.
4. Select **Log and enforce security based on threat level**. This setting will make Okta automatically deny access to sign-in requests that come from potentially malicious IP addresses that ThreatInsight detects.
5. Click **Save**.

Contextual Access & Device Management (optional)

If you have time please feel free to add network and behavior detection rules to your tenant.

Networks & Zones

1. Navigate to **Security -> Networks**.
2. There are two default Zones already configured. *BlockedIpZone* and *LegacyIpZone*.

Networks

[Help](#)

Add zone ▾		
Name	Zone type	Details
BlockedIpZone	IP block list	
LegacyIpZone	IP	

3. We are going to add a trusted IP Zone containing our computer address. To do this click **Add Zone -> IP Zone** as shown below.

Networks

[Help](#)

Add zone ▾		
+ IP Zone Create ranges of gateway IPs and proxy IPs	Zone type	Details
	IP block list	
+ Dynamic Zone Conditions for IP Type and location	IP	

4. Name the new zone Trusted Enterprise Network or similar and click on the address next to **Add your current IP address**. This will add your computer's address to a trusted list and we can later use this in Authentication Policies.

Add IP Zone

Zone name

☐ **Block access from IPs matching conditions listed in this zone**
WARNING: Selecting this option will prevent matching IPs from accessing Okta.

Gateway IPs ?
Add your current IP address Max 150

Trusted proxy IPs ?
ZScaler proxy addresses can be found [here](#) Max 150

Dynamic Zones and Behaviors use the configured proxies to identify where requests originated.

ThreatInsight automatically allows access from the configured proxies for your org.

Save **Cancel**

5. Next we can add a Dynamic Zone to block access from Tor proxies. To do this click **Add Zone -> Dynamic Zone**. Check *Block access from IPs matching conditions listed in this zone* and from the **IP type** drop down select *Tor anonymizer proxy* as shown below.

Add Dynamic Zone

Zone name

☒ **Block access from IPs matching conditions listed in this zone**
WARNING: Selecting this option will prevent matching IPs from accessing Okta.

IP type

Locations

ISP ASNs ?

Save **Cancel**

6. Your *Networks* list should now look similar to the following.

Networks

Help

Add zone

Name	Zone type	Details	
Block Tor	Dynamic Block list	IP typeTor anonymizer proxy	Active
BlockedIpZone	IP block list		
LegacyIpZone	IP		
Trusted Enterprise Network	IP	Gateway IPs	Active

Note

- Adaptive SSO or Adaptive MFA licenses are required to leverage Dynamic Zones
- At a later stage if you would like to see what is added to Okta Logs when an IP is blocked you can add your computer IP to the BlockedIpZone by clicking on the pencil icon at the end of the line and then clicking on your current IP address as shown below. Please ensure you remember to remove this setting afterwards if you wish to test other policies in more detail.

Edit IP Zone

Zone name

BlockedIpZone

☒ Block access from IPs matching conditions listed in this zone

WARNING: Selecting this option will prevent matching IPs from accessing Okta.

Gateway IPs ⓘ

Add your current IP addressMax 1000

Save

Cancel

Behavior Detection (Information only)

1. Navigate to **Security -> Behaviour Detection**.

Behavior Detection

[Help](#)

Add behavior ▾					
Name	Behavior type	Details			
New City	Location	Location granularity	City	Active ▾	✎ ✕
		Evaluate against past	20 authentications		
New Country	Location	Location granularity	Country	Active ▾	✎ ✕
		Evaluate against past	10 authentications		
New Device	Device	Evaluate against past	20 authentications	Active ▾	✎ ✕
New Geo-Location	Location	Location granularity	Latitude - Longitude	Active ▾	✎ ✕
		Evaluate against past	20 authentications		
		Radius from location	20 kilometers		
New IP	IP	Evaluate against past	50 authentications	Active ▾	✎ ✕
New State	Location	Location granularity	State or Region	Active ▾	✎ ✕
		Evaluate against past	15 authentications		
Velocity	Velocity	Velocity	805 Km/h	Active ▾	✎ ✕

2. Here you can see and adjust a wide range of behaviors. These can be later used in authentication policies either leveraging the Risk level Okta assigns or specifically by evaluating specific behaviors in a custom expression. See the (Okta Expression language documentation) [<https://developer.okta.com/docs/reference/okta-expression-language-in-identity-engine/>] for more details.

Note

Location data is provided by a third-party geolocation service. Okta updates the geolocation IP data on a weekly basis.

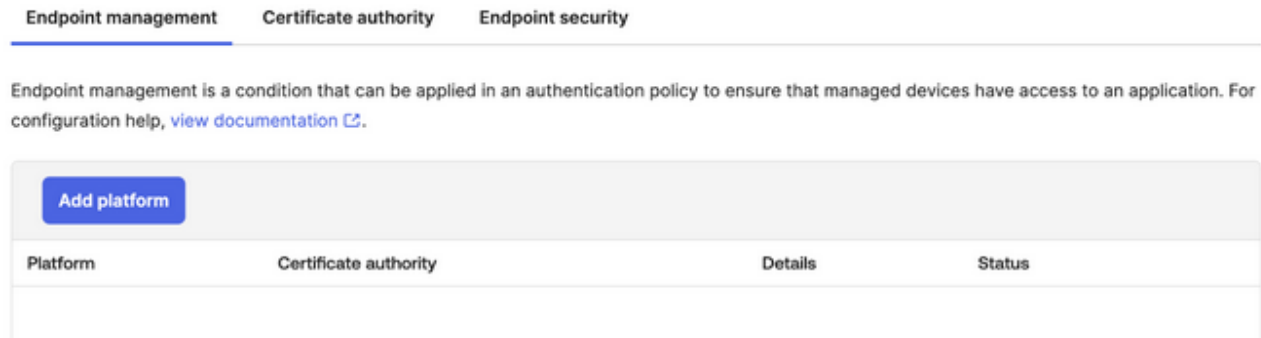
Device Integrations (Information only)

Device Integrations are used to link Okta with endpoint management systems such as Intune, JAMF etc. We will not be leveraging these device integrations during this workshop.

1. Navigate to **Security -> Device Integrations**. Here you will see three tabs.
2. The first and second tabs *Endpoint Management & Certificate Authority* allows you to add a device management platform, such as JAMF or Intune, and the associated trusted certificate chain. You can find more details on specific configuration in the (documentation)[<https://help.okta.com/oie/en->

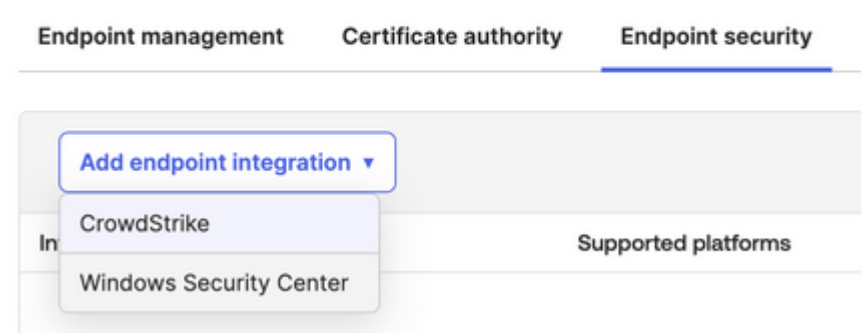
us/Content/Topics/identity-engine/devices/managed-main.htm].

Device Integrations



3. The third tab Endpoint Security allows you to integrate with CrowdStrike or Windows Security Center to leverage signals directly from the endpoints during authentication policy evaluation.

Device Integrations



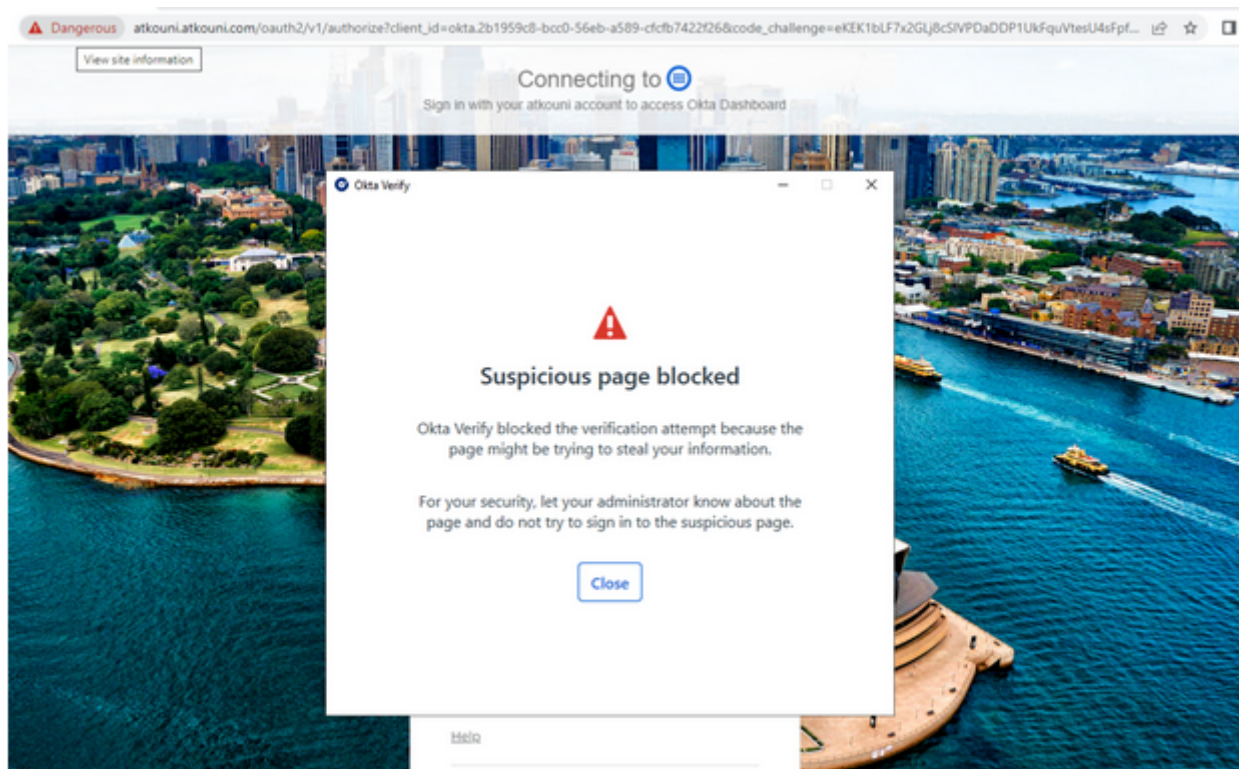
Detecting & Responding to Phishing Attacks (optional)

In this section, we will look at how you can enable Okta Fastpass to detect and respond to real-time phishing attacks caused by AiTM services like EvilGinX. **This guide will not cover setting up of EvilGinX.**

In the previous lab section, you’ve already learned how to enable Okta Fastpass as an Authenticator for your end-users.

The next section will focus and discuss on how you can leverage Fastpass to detect and respond to Phishing attacks targeted by threat actors to your end users.

One benefit of using Okta Fastpass is that by default it already inherits phishing resistant qualities meaning it is able to automatically detect if the site is a phishing site or legitimate site. If it is a phishing site, automatically, it will provide an end-user friendly message to your end users.



The only prerequisite to have this feature/capability enabled is to make sure your end-users are running the latest version of Okta Fastpass and have their Okta account enrolled with it. From an administrator level, the only task you need to do is to create a rule within your Authentication Policy that leverages Fastpass as the authenticator of choice. Always remember that phishing sites will always try to farm your end-user's password by imitating your identity provider's authentication/login page/screen/service. The goal is to not allow your end-users to not use a password or non-phishing resistant authenticators as part of the authentication process such that nothing is shared or stored to your attacker's service.

Create a Phishing proof Authentication Policy rule

1. Navigate to any one of your Authentication policies and create a new rule.

A screenshot of the Okta Admin console showing an Authentication Policy rule configuration. The policy is named 'Okta WIC2 Workshop' and is 'ENABLED'. The rule is configured with the following conditions and actions:

- IF** Device: Registered, Not managed
- THEN** Access: Allowed with possession factor

The rule requires 'Your org's authenticators that satisfy this requirement: 1 factor type', specifically 'Okta Verify or FIDO2 (WebAuthn)'. Additional requirements include: 'If Okta FastPass is used: The user must approve a prompt in Okta Verify or provide biometrics' and 'Re-authentication frequency is: Never re-authenticate if the session is active'. An 'Actions' button is visible in the top right corner.

2. If we inspect the rule closely, this is what should be defined from a policy decision point perspective:

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

Rule name

Okta WIC2 Workshop

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

☐ Managed

Setup Okta Verify as [Authenticator](#)

[Go to Device Management](#)

AND

Device management is

☒ Not managed

☐ Managed

[Go to Device Management](#)

AND

Device assurance policy is

No policy

AND

Device platform is

Any platform

AND

User's IP is

Any IP

AND

Risk is

Any

AND

The following custom expression is true

This is an optional advanced setting. If the expression is formatted incorrectly or conflicts with conditions set above, the rule may not match any users.
[Expression language reference](#)

3. From a policy enforcement point perspective, this is what should be defined:

THEN

THEN Access is

☐ Denied

☒ Allowed after successful authentication

AND User must authenticate with

Possession factor

AND Possession factor constraints are

☐ Phishing resistant

☐ Hardware protected

☒ Exclude phone and email authenticators

AND If Okta FastPass is used

☒ The user must approve a prompt in Okta Verify or provide biometrics

☐ The user is not required to approve a prompt in Okta Verify or provide biometrics

Your org's authenticators that satisfy this requirement:

1 factor type

Okta Verify or FIDO2 (WebAuthn)

Re-authentication frequency

AND Re-authentication frequency is

☐ Every sign-in attempt

☐ Never re-authenticate if the session is active

☒ Re-authenticate after:

2 Hours

Save **Cancel**

4. Click **Save** and make sure the rule is ranked as one of the highest ranking of your authentication policy.

During this lab we will not setup an **EvilGinX** instance for demonstrate the phishing resistance.

You can watch this video for a demo: [Detect, Prevent and Protect Phishing Attempts through Phishing Resistant Authenticators by Okta](#)

Or you can try at home to run an EvilGinX proxy and emulate an attacker!

Adding Observability and Workflows (Information only)

Okta logs every transaction and processed event within the platform. All of these logs are kept and accessible via Okta's System Log. Okta also provides extensibility points within the platform through Hooks. One type of hook that we can leverage here is [Event Hooks](#). You can define multiple Event Hooks within the Okta platform. Navigate to **Workflow -> Event Hooks**.

Event Hooks

[Help](#)

Event hooks send event data from Okta to an external endpoint when a selected event occurs

Create Event Hook

Event Hook Name	Status	Verification *	Actions
Phishing Event Hook Notification	Active	VERIFIED	Actions ▾

You can do the following instructions at your own time or pace. You can create Event Hooks that will meet your requirements and specifications. The example Event Hooks workflow we will define below will intercept and Phishing Attacks declined by Okta Fastpass.

1. Click Create Event Hook

Create event hook

Help

1

2

3

4

Create hook

Apply filters to events

Preview

Activate hook

Add hook details

Endpoint URL

Event Hook name

Description

Optional - Describe what this event hook is used for

Customize request

Enhance security

Optional

Authentication field

The name of the authentication header

Authentication secret

The value of the authentication header

Custom headers

Optional

Custom header fields

Field Name

Value

+ Add Field

Select Events

Select all events that apply

2. Supply an Endpoint URL, Event Hook Name and description.

Edit

Endpoint URL

https://atkouni.workflows.okta.com/api/flo/704ff142814a97a4f97ebb3ca7ad3ae3/invoke

This is a workflows API URL. No verification is required.

Event Hook name

Phishing Event Hook Notification

Description

Optional - Describe what this event hook is used for

3. Let's leave the Customise Request as default.

4. Let's select a specific event.

Select Events

Select all events that apply

Authentication of user via MFA. x

Save Cancel

5. Click Next and let's apply a filter.

USER AUTH EVENTS

Authentication of user via MFA. (user.authentication.auth_via_mfa)

☐ Apply filter

Save Cancel

6. Click the Use Okta Expression Language (advanced)

USER AUTH EVENTS

Authentication of user via MFA. (user.authentication.auth_via_mfa)

☒ Apply filter

Field	Operator	Value
eventType	contains	Enter value

+ Add Another

Use Okta Expression Language (advanced)

Save Cancel

7. Use the following filter `event.outcome.reason eq "FastPass declined phishing attempt"`. Click **Save**.

USER AUTH EVENTS

Authentication of user via MFA. (user.authentication.auth_via_mfa)

☒ Apply filter

Expression language

event.outcome.reason eq "FastPass declined phishing attempt"

Sample Expressions

Switch to simple UI

Save Cancel

8. Make sure you also verify the Event hook you created by following the instructions here.

Conclusion

In this lab, we've journeyed beyond traditional barriers, tapping into the wonders of Okta Verify and FastPass. Goodbye, cumbersome passwords and hello, sleek passwordless wonders! Together, we've fortified our defenses against those sneaky phishers and, yes, even our own little mishaps. Here's raising a toast to a future of ease, enhanced security, and fewer facepalms!