Whitepaper

Step-by-step guide to becoming phishing resistant with Okta FastPass

Contents

Introduction

Traditional authentication using a username and password has been the foundation of digital Identity for over 50 years. With the rise of credential phishing attacks, it's more critical than ever to move beyond passwords and adopt phishing resistant authentication.

Okta FastPass (a verification option in Okta Verify) is a phishing-resistant authenticator that supports any SAML, OIDC, or WS-Fed app in Okta and satisfies a high security assurance level. FastPass detects and prevents the disclosure of sensitive authentication data during a phishing attack.

FastPass phishing resistance is supported on Windows, macOS, iOS, and Android devices and offers the same user-friendly experience across these platforms.

This guide provides technical implementers with steps to safely and gradually protect apps with FastPass. The guide will cover: enabling the FastPass authentication method, configuring policies that require phishing resistant authentication, how to try it out for just yourself and your admin team, and how to roll out FastPass to your users in phases. Users will be required to download Okta Verify and setup FastPass on their device.

Key concepts

FastPass Enrollment and Device Registration

FastPass is an authentication method provided by the Okta Verify app.

The process of downloading Okta Verify on a device and enrolling in FastPass does the following:

- Uniquely binds a set of keys to the device and to the user.
- Registers the device in Okta's Universal Directory.

This establishes a trusted user and device pairing that verifies that the device is recognized by Okta and in possession of an authorized user.

A note on device registration vs. device management

A device is considered "registered" when it is enrolled in Okta Verify; this is different from a device that's considered "managed," which requires the device to be controlled or managed by a mobile device management (MDM) solution or equivalent. When registered with Okta Verify, admins cannot read or access personal information on the device, remotely wipe the device, or track your exact location, which may be possible for a device managed by an MDM.

Prerequisites

Let's start the journey toward enabling phishing-resistant FastPass across your organization. This guide will take you through the steps to try it out for yourself (and other admins) before you roll it out to your users. This way, you will have a safe and measured deployment in a timeframe that works for you.

Prerequisites

1. An Okta tenant powered by the Okta Identity Engine (OIE). If you wish to try it out in a non-production environment, then use a free trial tenant or a preview Okta tenant.
2. An Okta Administrator account to sign in to the tenant.

Test Okta FastPass yourself

Optional MDM details

If your user's devices are managed with an MDM, you can install Okta Verify on those devices automatically. See the chapter "Use MDMs to install Okta Verify on managed devices" in this guide on page 18 to learn more.

Step 1

Add Okta Verify as an authenticator (5 min)

Add Okta Verify as an authenticator option and enable FastPass as a security method that can be used to access applications.

A. **Prepare**
Select a testing application or a very low-traffic application that you want to protect with FastPass so that you can try it out yourself and with other admins first.

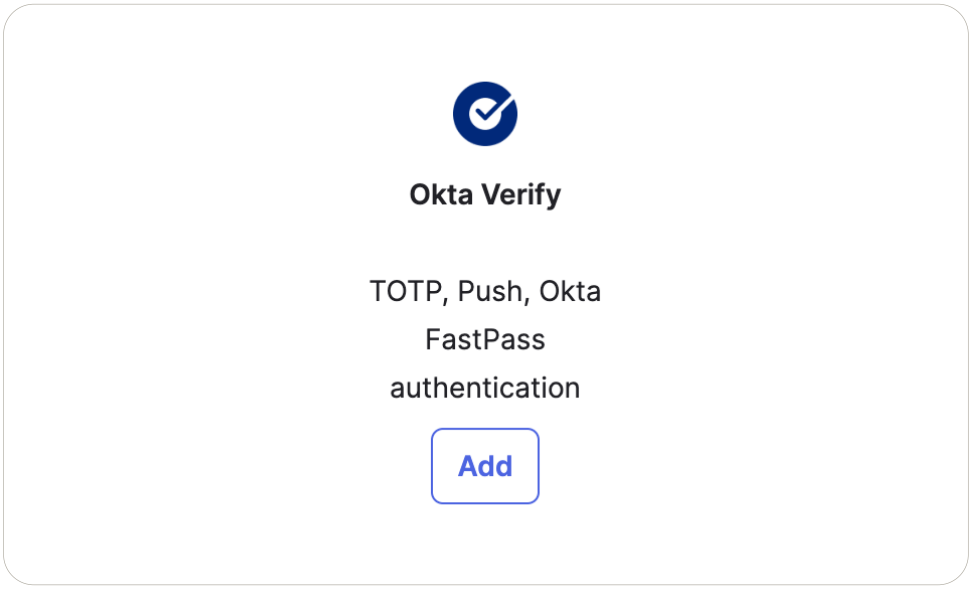
B. **Implement**
Enable FastPass as an authentication method in your Okta tenant.

   a. If needed, sign in to your Okta Admin Console

   b. Navigate to ***Security > Authenticators***

   c. If Okta Verify isn't already enabled, select ***Add Authenticator***

   d. On the Okta Verify tile, select ***Add***. (If Okta Verify was already added because your tenant uses Push or TOTP, then use the ***Actions*** dropdown menu to ***Edit***)


Okta Verify

TOTP, Push, Okta FastPass authentication

Why not show the "Sign in with Okta FastPass" button now?

This display control will affect your entire user base. You cannot control the display on a per-group or per-app basis. Okta recommends that you hold off on showing this button until you have enrolled a significant portion of your users in FastPass.

Even though this option remains unchecked, if a user has FastPass set up, they will be able to use FastPass to authenticate. This screen will be returned to later in the guide when FastPass is deployed to a wider audience.

e. Under ***Enrollment options***, Okta recommends selecting ***Higher security methods***, so end users are driven to start and complete the Okta Verify enrollment with the organization's sign-in URL and on the same device.

   For the ***Verification options*** section, select ***Okta FastPass (All platforms)***.

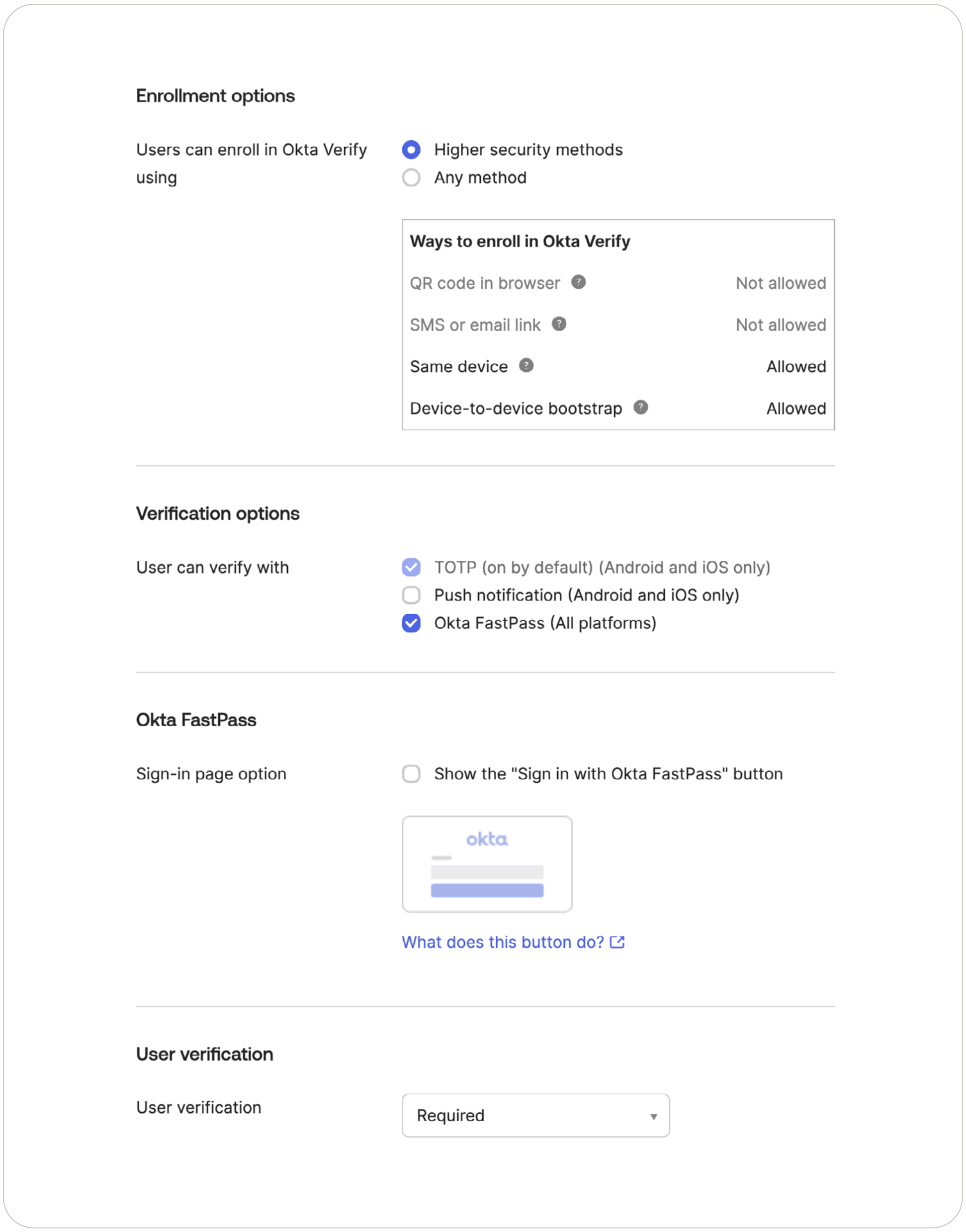
   For now, leave the ***Show the "Sign in with Okta FastPass"*** button unchecked.

   If you see the option for ***User verification***, it may be set to ***Preferred*** or ***Required*** – either option will achieve phishing-resistant authentication via FastPass.

   i. If you select ***Required***, then during Okta Verify enrollment, users must enable biometrics or set up a PIN. Generally, Okta recommends that you select ***Required*** so that users are prepared to verify with another factor alongside FastPass for 2FA.

   ii. If you select ***Preferred***, then during Okta Verify enrollment, users are prompted to set up biometrics or a PIN but are not required to do so at that time in order to finish the enrollment process. The user can choose to finish user verification setup at a later time.

   For more information on how to configure user verification, please refer to the documentation.



Enrollment options

Users can enroll in Okta Verify using
● Higher security methods
○ Any method

Ways to enroll in Okta Verify

QR code in browser	Not allowed
SMS or email link	Not allowed
Same device	Allowed
Device-to-device bootstrap	Allowed

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

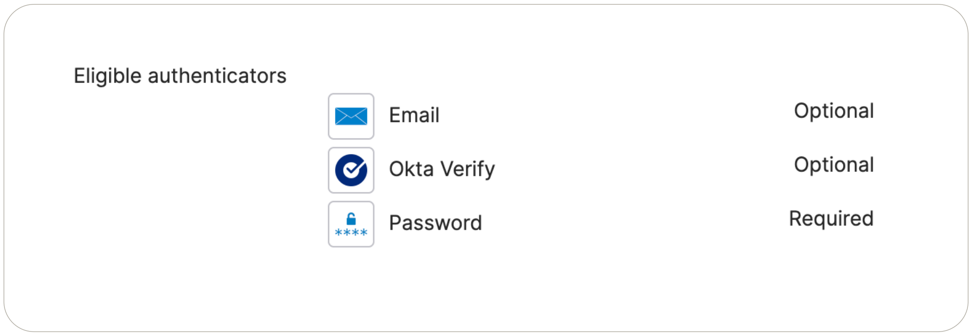
What does this button do?

User verification

User verification: Required

f. Authenticator enrollment policies enable users to enroll into authenticators. This step enables users to start using Okta Verify, which is necessary in order for them to use FastPass.

In the Authenticator Enrollment Policy (***Security > Authenticators > Enrollment*** tab), see that Okta Verify is ***Optional*** or ***Required*** – either option will achieve phishing resistant authentication via FastPass.



Eligible authenticators

Email	Optional
Okta Verify	Optional
Password	Required

i. If Okta Verify is ***Optional***, then you can scope the rollout of Okta Verify to just the users who need access to applications you want to protect with FastPass (see ***Step 2*** in this guide). Users will be prompted to install Okta Verify and enroll FastPass on the device initiating sign in, all in the same workflow. This is Okta's recommended selection for this guide because it streamlines the user setup experience and allows fine-grained targeting of the enrollment.

ii. If Okta Verify is ***Required***, then all users in the group targeted in this policy will be required to download Okta Verify when they next log in. However, the current enrollment flow only provides users with instructions to download Okta Verify on a mobile device, and NOT on a desktop, even if that's where they initiate the sign-in. Requiring Okta Verify downloaded to mobile devices doesn't hurt anyone, and this setting is fine, especially if your organization will use or already uses Okta Verify for TOTP and/or Push. This option may not provide the most controlled deployment path and may complicate how you will need to communicate with different user sets about when and how to enroll in FastPass.

Step 2

Edit the Authentication Policy for your test app (10 min)

Authentication policies define how a user must authenticate to gain access to an app. You will create a policy that requires a registered device and phishing-resistant authentication, which will force the user to download and authenticate with FastPass.

A. **Implement**

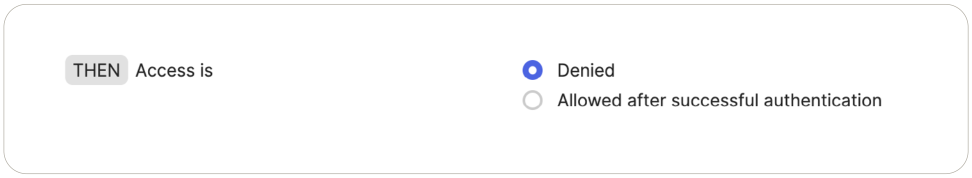
Navigate to ***Security > Authentication Policies*** to edit the Authentication Policy for your test application.

If the policy is shared across multiple applications, you'll want to clone it or make a one-off new policy that only protects the test application.

Name the policy "FastPass" so you remember what it's for.

Edit the rules within the policy so that:

a. The ***Catch-all rule*** specifies ***Access is - Denied***.

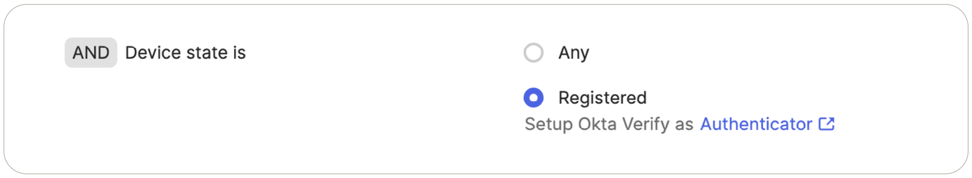


THEN Access is

● Denied
○ Allowed after successful authentication

b. For all rules (at least 1) prior to the ***Catch-all*** rule:

i. Use the condition ***Device state is: Registered***



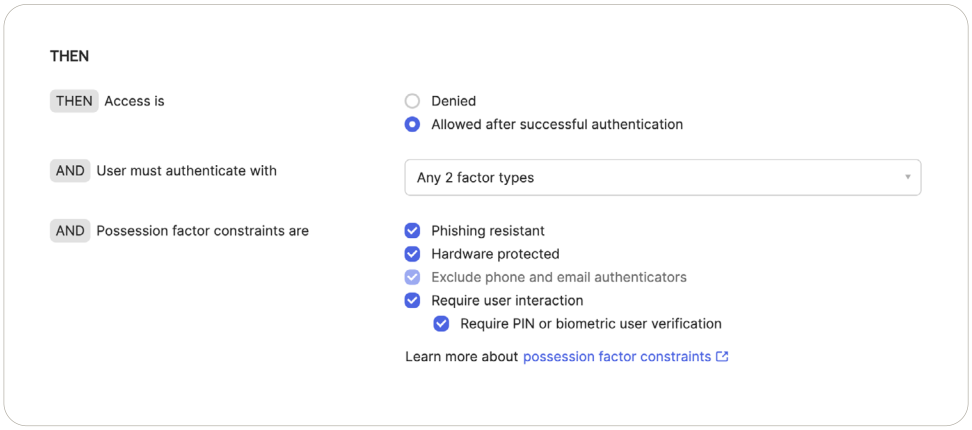
AND Device state is

○ Any
● Registered
Setup Okta Verify as Authenticator

ii. ***User must authenticate with: Any two factor types*** or ***Possession factor***

iii. The ***Possession factor constraints*** are ***phishing resistant*** (required), ***Hardware protected*** (recommended), ***Require user interaction*** (recommended) and ***Require PIN or biometric user verification*** (recommended), which enforces user verification alongside FastPass for 2FA.

Okta Verify should be listed as one of the authenticators in the box labeled: ***Your org's authenticators that satisfy this requirement:***



THEN

THEN Access is
○ Denied
● Allowed after successful authentication

AND User must authenticate with
Any 2 factor types

AND Possession factor constraints are
☑ Phishing resistant
☑ Hardware protected
☑ Exclude phone and email authenticators
☑ Require user interaction
☑ Require PIN or biometric user verification

Learn more about possession factor constraints

iv. ***Re-authentication frequency*** specifies ***Every sign-in attempt*** (recommended for clarity in testing and also for general security).

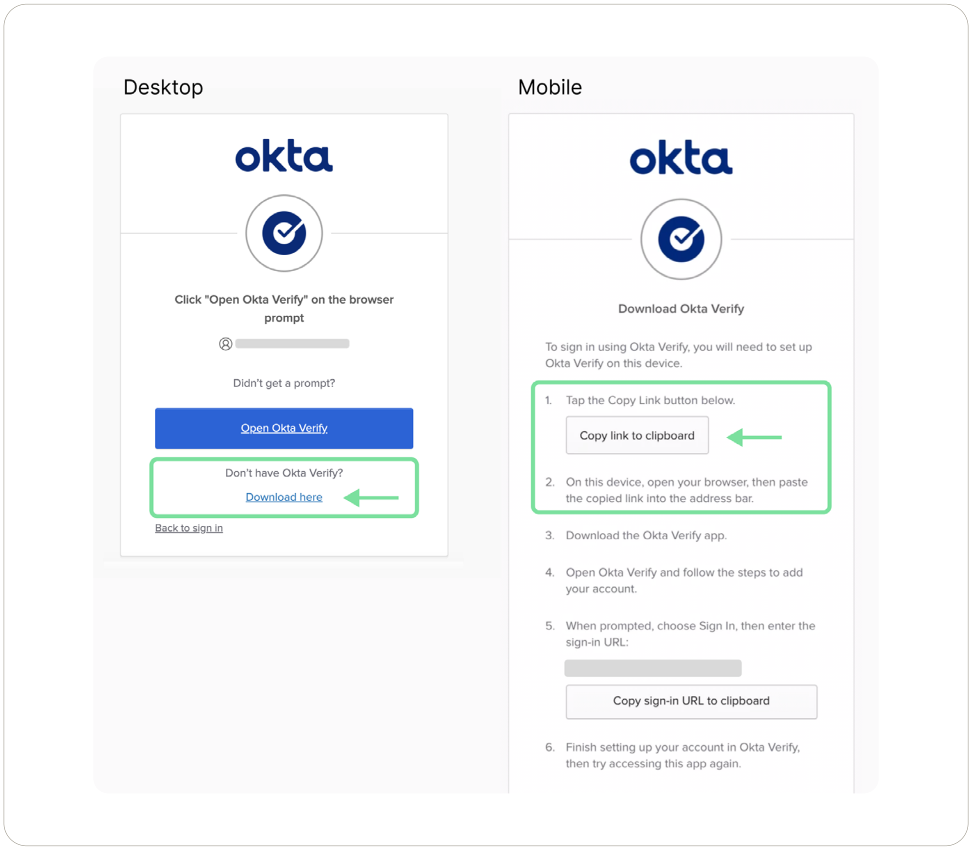
(For more detailed information on all these selections, please refer to the documentation.)

B. Test

When users access any application protected by this policy, they will be prompted to set up FastPass on that device, and must use it to authenticate into the application. Try it yourself.

a. Assign yourself to this test application and sign in to the application.

b. You will be prompted to download or open Okta Verify. You must download Okta Verify if you haven't already downloaded it on your device.



Desktop

okta

Click "Open Okta Verify" on the browser prompt

Didn't get a prompt?

Open Okta Verify

Don't have Okta Verify?

Download here

Back to sign in

Mobile

okta

Download Okta Verify

To sign in using Okta Verify, you will need to set up Okta Verify on this device.

1. Tap the Copy Link button below.

   Copy link to clipboard

2. On this device, open your browser, then paste the copied link into the address bar.
3. Download the Okta Verify app.
4. Open Okta Verify and follow the steps to add your account.
5. When prompted, choose Sign In, then enter the sign-in URL:

   Copy sign-in URL to clipboard

6. Finish setting up your account in Okta Verify, then try accessing this app again.

Complete the download, then open the Okta Verify app and follow the instructions and verification process to create an Okta Verify account and enroll in FastPass.

When you create an Okta Verify account, if you're prompted for ***"Organization's Sign-In URL"***, on desktop, you can copy-paste the URL from your browser address bar where you initiated sign in. On mobile, you can use the "Copy sign-in URL to clipboard" button.

c. Sign out and sign back in to the test application to use Okta FastPass to authenticate.

d. You can assign other admin testers to the test application for more testing before protecting additional applications to roll it out in phases to the larger audience.

C. Confirm

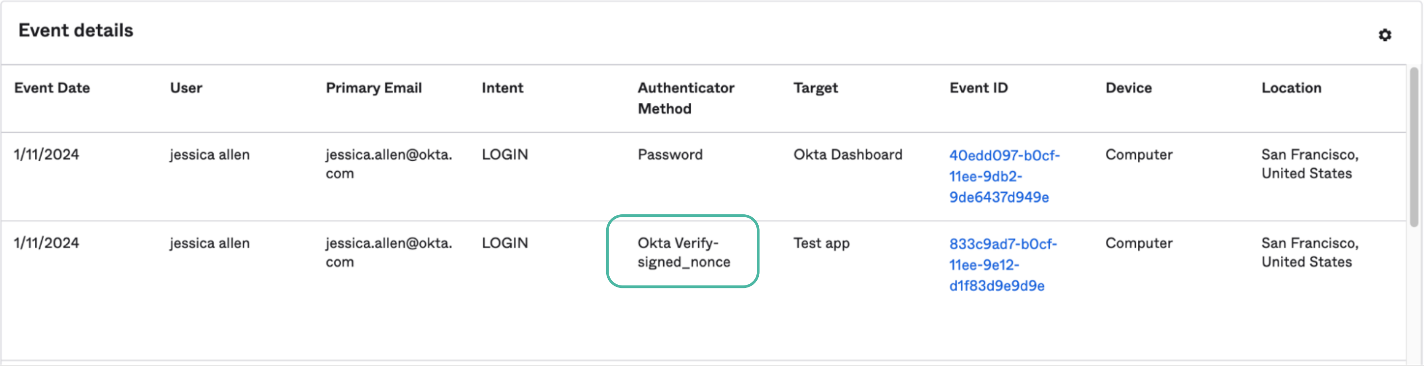
After some time has passed, you can check the MFA Activity report to see trends and see how often FastPass is being used in your org. Note that source data for this report is refreshed hourly during the day, so you might not see your recent activity immediately after it occurs.

a. Navigate to ***Reports > Reports***

b. Click the ***MFA Events*** report

c. Optionally click ***Edit Filters*** to filter the report by duration. The default filter is the last 24 hours

d. In the ***Event details*** table, see that the ***Authentication Method*** "Okta Verify-signed_nonce" was used to sign in to the test application – this means FastPass was used



Event details

Event Date	User	Primary Email	Intent	Authenticator Method	Target	Event ID	Device	Location
1/11/2024	jessica allen	jessica.allen@okta.com	LOGIN	Password	Okta Dashboard	40edd097-b0cf-11ee-9db2-9de6437d949e	Computer	San Francisco, United States
1/11/2024	jessica allen	jessica.allen@okta.com	LOGIN	Okta Verify-signed_nonce	Test app	833c9ad7-b0cf-11ee-9e12-d1f83d9e9d9e	Computer	San Francisco, United States

Deploy Okta FastPass in phases

Before you begin deploying FastPass to a larger portion of your workforce, you should consider the following questions, which may impact how you ultimately configure and deploy FastPass.

- Which applications should require FastPass phishing-resistant authentication?
- Will only managed devices be able to authenticate with FastPass?
- Do you want to enable biometric (i.e., user verification) flows? Are there any accessibility challenges?

Step 3

Drive FastPass enrollment across your organization (10 min)

1. **Prepare**

   Select which application(s) you want to protect with FastPass in this first batch of user enrollment. Give a heads up to the users that are assigned to these application(s) and will be affected by this change. Let them know that they will soon be prompted to download Okta Verify on their devices. Here's an example email you could send.

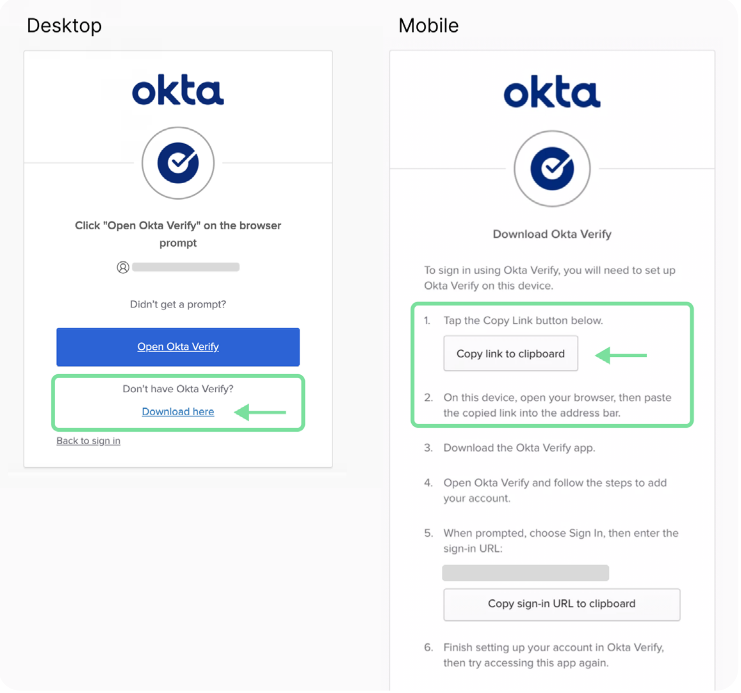
   Subject: A new way to sign in called Okta FastPass is coming soon

   Hi team,

   We are rolling out a new, quick, and secure way to sign in to the apps you use at work – Okta FastPass. You will be required to set up Okta FastPass on all of the devices you use for work.

   This week, we will get many of you set up to use Okta FastPass. This is a one-time process where you will be prompted to download Okta Verify and set up Okta FastPass on your device. Complete the download then follow the instructions and verification process to set it up.

   The prompt to download Okta Verify will look something like this:



Click "Open Okta Verify" on the browser prompt

Didn't get a prompt?

Don't have Okta Verify?

Download Okta Verify

To sign in using Okta Verify, you will need to set up Okta Verify on this device.

1. Tap the Copy Link button below.

   Copy link to clipboard

2. On this device, open your browser, then paste the copied link into the address bar.
3. Download the Okta Verify app.
4. Open Okta Verify and follow the steps to add your account.
5. When prompted, choose Sign In, then enter the sign-in URL:

   Copy sign-in URL to clipboard

6. Finish setting up your account in Okta Verify, then try accessing this app again.

If you are prompted for your org URL, use <<Admin to enter the org URL here>>

Please reach out if you have questions.

Best regards,

Your IT/BT Team

2. **Implement**
   Drive more user enrollment by protecting other applications with the "FastPass" policy. Use this technique to phase your rollout in manageable stages. Wait a day or so between protecting each batch of applications with the "FastPass" policy so that you have time to manage any questions that arise from your users.

   a. Navigate to ***Security*** > ***Authentication Policies***

   b. Select the "FastPass" policy

   c. Navigate to the ***Applications*** tab

   d. Click ***Add app***

   e. Add the application(s) you want to protect with FastPass

      If you're ready to allow every user to enroll in FastPass and for every application to be accessed with FastPass, protect all applications with the FastPass policy.

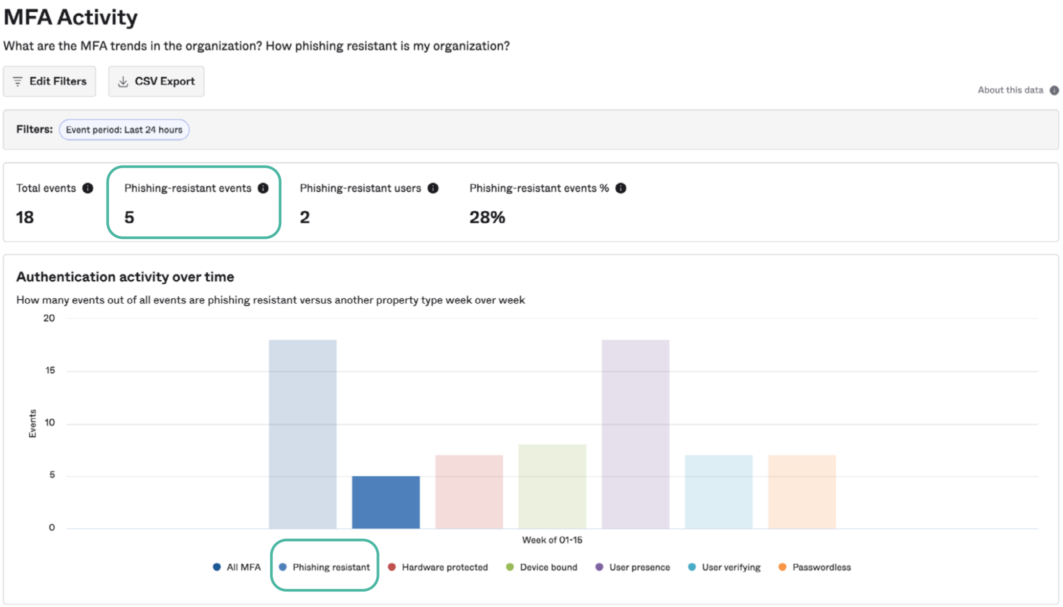
3. **Confirm**
   Check the MFA Activity report to see trends and see how often FastPass is being used in your org.

   d. Navigate to ***Reports*** > ***Reports***

   e. Click the ***MFA Events*** report

   f. Optionally click ***Edit Filters*** to filter the report by duration. The default filter is the last 24 hours

   g. In the chart ***Authentication activity over time***, see that ***Phishing resistant*** authentication events are occurring



MFA Activity

What are the MFA trends in the organization? How phishing resistant is my organization?

Edit Filters CSV Export

About this data

Filters: Event period: Last 24 hours

Total events	Phishing-resistant events	Phishing-resistant users	Phishing-resistant events %
18	5	2	28%

Authentication activity over time

How many events out of all events are phishing resistant versus another property type week over week

Step 4

Show the “Sign in with Okta FastPass” button (5 min)

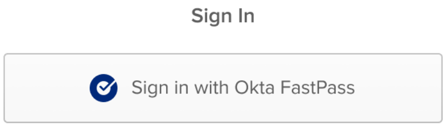
1. **Prepare**
   Email users to give them a heads up that they can soon click “Sign in with Okta FastPass” to skip entering their username. Here’s an example email you could send:

   Subject: Button to sign in with Okta FastPass

   Hi team,

   We are going to include a button on your sign-in screen to “Sign in with Okta FastPass”.

   Click on that button next time you sign in – when you do, you can skip entering your username (hooray!) and proceed with signing in.



Sign In

Sign in with Okta FastPass

   Please reach out if you have questions.

   Best regards,
   Your IT/BT Team

When should I show the "Sign in with Okta FastPass" button?

You can show this button whenever you would like – but be aware that it's an org-wide setting, so every user will see it in the sign-in widget regardless of which application they are accessing.

2. **Implement**

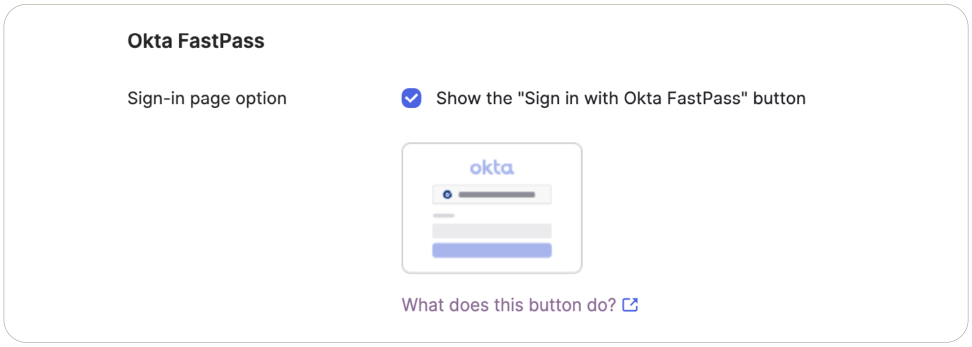
   Once many of your users have enrolled in FastPass, it's appropriate to show the "Sign in with Okta FastPass" button to everyone.

   a. Navigate to ***Security*** > ***Authenticators***

   b. Use the ***Actions*** dropdown to ***Edit*** the authenticator ***Okta Verify***

   c. Select the checkbox to ***Show the "Sign in with Okta FastPass" button***

   d. Now, that button will appear in the Sign-in page for all apps.



Okta FastPass

Sign-in page option ☑ Show the "Sign in with Okta FastPass" button

What does this button do?

What this button does

This button will now appear for all applications and all users within the tenant. Selecting this button does 3 things:

- Allows a seamless sign-in for users who already have enrolled in FastPass
- It walks first-time end users through installing Okta Verify on phones only
- It provides an alternative if the end user's configuration doesn't permit silent sign-on. Enabling the button allows these users a way to sign

3. **Confirm**

   Sign out to sign back in to any application protected by your tenant to see the "Sign in with Okta FastPass button". Click the button to sign in. You will not be prompted for your identifier (email).

Well done! You have protected every app with a phishing resistant authentication policy, and your users can sign in more efficiently with FastPass.

Suggested next steps

Now that you’ve set up FastPass, these techniques can further secure your org

Require phishing-resistant authentication to enroll additional authenticators

You can require users to authenticate using a phishing-resistant authentication method (if they have one enrolled, such as FastPass) before they enroll in additional authenticators.

Note: If a user doesn't have a phishing-resistant authentication method enrolled and this feature is turned on, they will be permitted to enroll in additional authenticators after authenticating with two factors. They will not be blocked because of their lack of a phishing-resistant authentication method.

a. In the Admin Console, go to ***Settings***, and then ***Features***

b. Click the toggle switch for ***Require phishing-resistant authenticator to enroll additional authenticators*** to turn it on

c. Result: Whenever the user adds or edits any authentication method, they will first be required to verify themselves with a phishing-resistant authentication method (i.e., FastPass)

Only allow managed devices to access your most sensitive applications

Although Okta Verify creates a strong binding between users and their devices, it’s not a replacement for a device management solution. Limiting application access to managed devices should be considered for the most sensitive apps. As there’s a strong binding between user and device, should the end user lose access to the device (or the device is suspended or deactivated by the Okta administrator), it will be impossible for the user to sign in.

Use MDMs to install Okta Verify on managed devices

Deploy Okta Verify to managed devices

For devices that are managed, optionally use your device management solution to deploy Okta Verify to devices. When admins deploy Okta Verify to managed devices, admins can use their existing MDM solution to push Okta Verify to install on the end user device, in addition to any MDM app configuration profiles that help configure Okta Verify for end users. However, users will still need to launch Okta Verify on their device to finish setting up an account, enroll in FastPass, and configure biometrics or a PIN for user verification.

The setup process will be automatically initiated when they sign in to an app protected by the "FastPass" policy in this guide. But you might want to encourage users to do this set-up independently, and if that's the case we recommend an IT campaign. Please refer to the section "Run an IT Campaign" for guidance on how to ensure users are fully enrolled in FastPass even though they haven't been required to sign in with FastPass yet.

Methods to deploy Okta Verify differ by platform. Please refer to the Okta documentation for admins for Android, iOS, macOS and Windows in order to deploy Okta Verify to test user(s) device(s).

Managed app configurations

With managed app configurations, you can streamline the end-user process to create an account in Okta Verify. You can do things such as configure the sign-in or org URL to automatically show up on the user's enrollment page, which makes it easier for the user to complete the enrollment process. For macOS and Windows, these configurations can also help you to prompt end users to enroll in Okta Verify if they haven't already. We highly recommend any configurations that can help your end users more easily set up Okta Verify and FastPass. Please refer to these documents to learn more.

Configure an SSO extension on iOS and macOS devices

If you've managed macOS and iOS devices, you must create an SSO extension profile. The SSO extension forwards requests from a browser or app to Okta Verify. Therefore, the browser or app doesn't prompt users to open Okta Verify. ***For macOS, the SSO extension also introduces phishing resistance properties to the authentication flow***. We highly recommend that you configure this extension to enable the most secure experience. Please refer to these documents for macOS and iOS to configure the SSO extension. If you are testing with a macOS or iOS device, please make sure these SSO extension profiles are properly configured and pushed to those devices prior to testing.

Enable phishing-resistant authentication for Universal Windows Platform applications

For Universal Windows Platform apps and Microsoft 365 apps, you must run a script to ensure phishing-resistant authentication on managed devices. To complete this task, please follow these steps.

Run an IT Campaign

We suggest an IT campaign to provide the necessary instructions to end users. Okta provides end-user documentation that you can share with your users as part of the campaign for FastPass adoption and sample email templates that you can find in the Launch Kit for Okta Admins.

For Windows and macOS devices, you will need to provide your end users with your organization's sign-in URL, which for new employees is often made available in a Welcome/Activation email that IT sends out. You can also choose to deploy managed app configurations through your MDM to pre-populate the sign-in URL in the enrollment flow for your users.

If you have chosen to deploy Okta Verify to all managed devices, end users will already have Okta Verify installed on their devices. To finish the setup process, you can share these end-user documents with your workforce to enable them to set up Okta Verify accounts on their Windows and macOS computers.

For Android and iOS devices, with the authentication enrollment policy configured to ***Required*** for Okta Verify, end users will be pushed to set up Okta Verify on their phones when they next try to access an application. The process for end users to set up an Okta Verify account and start using FastPass is intuitive from the UI and should be similar to the steps provided earlier in this guide. If you want to share additional documentation to end users on how to enable biometrics in Okta Verify on mobile phones, you can share these end-user documents for Android and iOS.

Enroll subsequent devices in Okta Verify

Okta is making it easier and safer to enroll subsequent devices, managed or unmanaged, in Okta Verify with an intuitive enrollment process that reduces the risk of phishing attempts. For any user who wants to extend their existing Okta Verify account to additional laptops and phones, they can do so securely by syncing the devices using Bluetooth and scanning a QR code or entering a code manually.

Please share these documents with your users to enable them to securely enroll additional devices: Android, iOS, macOS, and Windows.

Conclusion

We hope that your users enjoy a more seamless and phishing-resistant sign-in experience with FastPass!

If you need additional support, contact support@okta.com.

We would love to learn more about how this guide worked for you so we can improve it in the future. If you would like to share feedback, please provide feedback on this Okta FastPass guide.

About Okta
Okta is the World's Identity Company. As the leading independent Identity partner, we free everyone to safely use any technology—anywhere, on any device or app. The most trusted brands trust Okta to enable secure access, authentication, and automation. With flexibility and neutrality at the core of our Okta Workforce Identity and Customer Identity Clouds, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customizable solutions and more than 7,000 pre-built integrations. We're building a world where Identity belongs to you. Learn more at okta.com.