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 supported by 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 is FedRAMP High Authorized and meets the NIST 800-63B Authentication Assurance Level 2 (AAL2) and AAL3 when properly configured on supported devices. It 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. It will cover: enabling the FastPass authentication method, configuring and testing policies that require phishing-resistant authentication, and rolling 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 with 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

- An Okta tenant powered by the Okta Identity Engine (OIE). If you wish to try FastPass in a non-production environment, then use a free trial tenant or a preview Okta tenant.
- 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 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 test 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

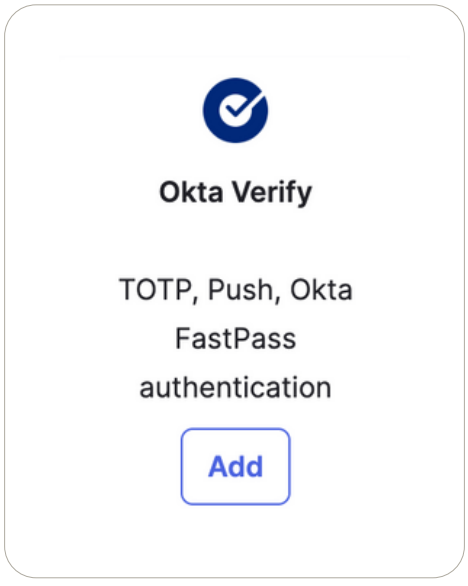
Enable FastPass as an authentication method in your Okta tenant.

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***).



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 this guide when FastPass is deployed to a wider audience.

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

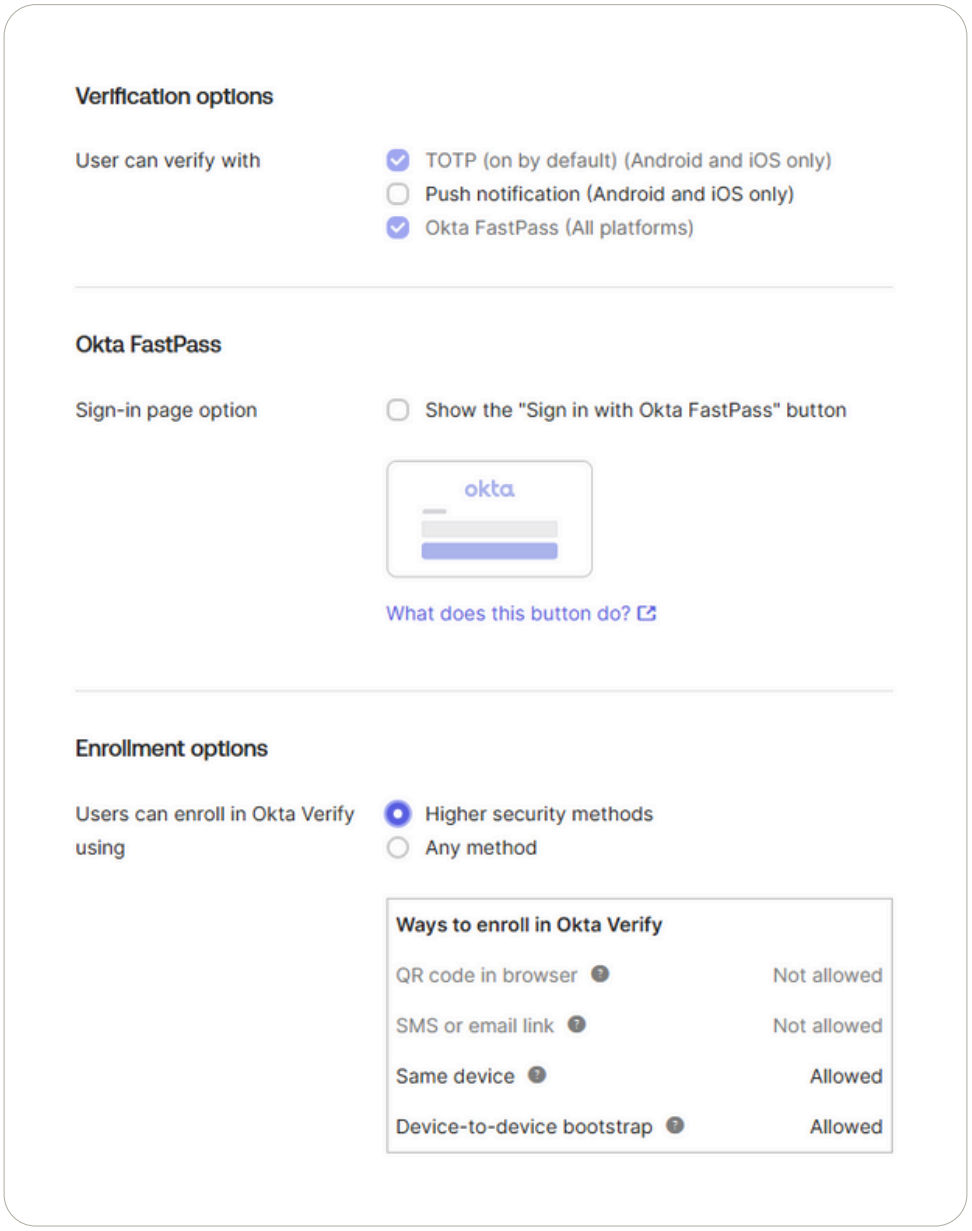
For now, leave the ***Show the "Sign in with Okta FastPass"*** button unchecked.

Under ***Enrollment options***, Okta recommends selecting ***Higher security methods***, so end users are driven to start and complete the Okta Verify enrollment on the same device.

If you see the option for ***Device passcode or biometric user verification***, it may be set to ***Preferred***, ***Required***, *or* ***Required with biometrics only*** – each option will achieve phishing-resistant authentication via FastPass.

- 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.
- 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.
- If you select ***Required with biometrics only***, then during Okta Verify enrollment, users must enable biometrics. If the device doesn't support biometrics, users can't enroll in or authenticate with Okta Verify.

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



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.

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 Okta Verify and authenticate with FastPass.

A. Implement

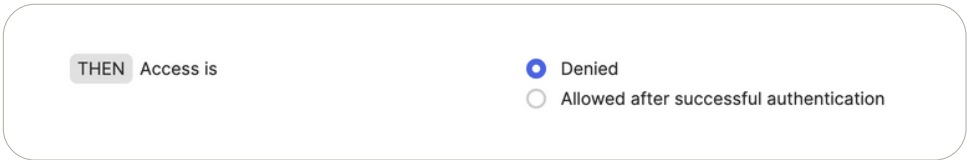
Navigate to ***Security > Authentication Policies > App sign-in*** to edit the authentication policy for your test application.

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.

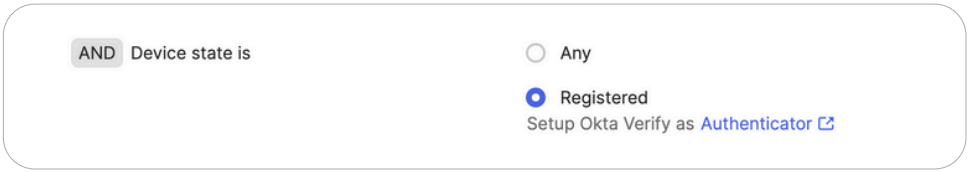
Edit the rules within the policy so that:

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



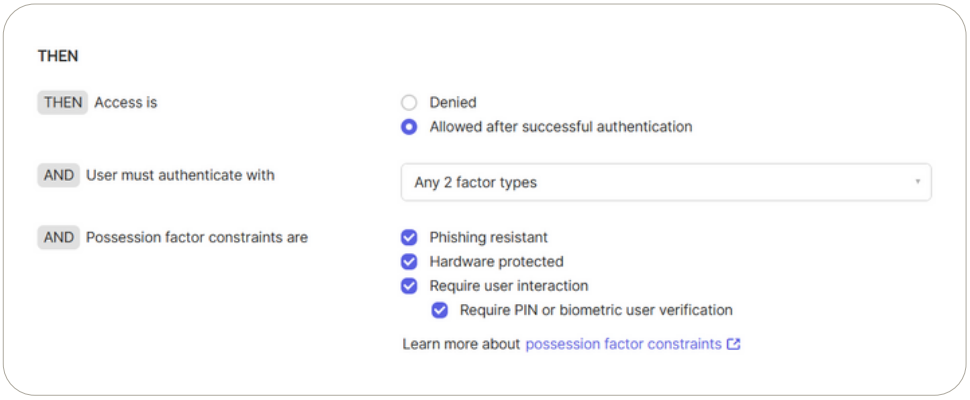
b. For all rules (at least 1) prior to the ***Catch-all*** rule:

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



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

- 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.



- If you wish to further specify the permitted authentication methods, you can do so by creating either an allowlist or disallow list under the ***Authentication methods*** section. Make sure that ***Okta Verify - FastPass*** is listed as one of the authenticators in the box labeled, ***Your org's authenticators that satisfy this requirement:***, and that access is either fully or partially constrained to using FastPass.
- ***Prompt for authentication*** specifies ***Every time user signs in to resource*** (recommended for clarity in testing and also for general security).

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

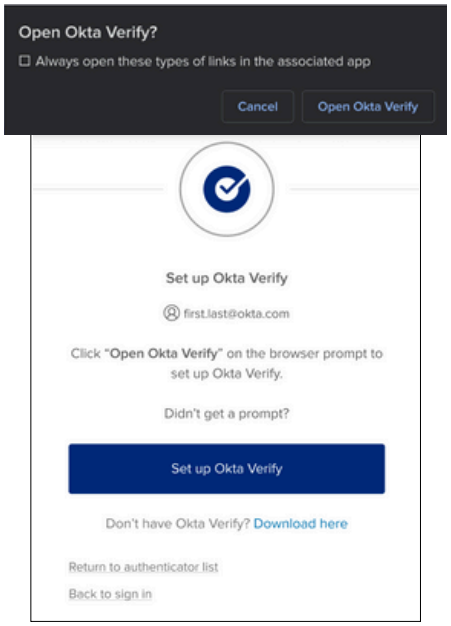
B. Test

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.

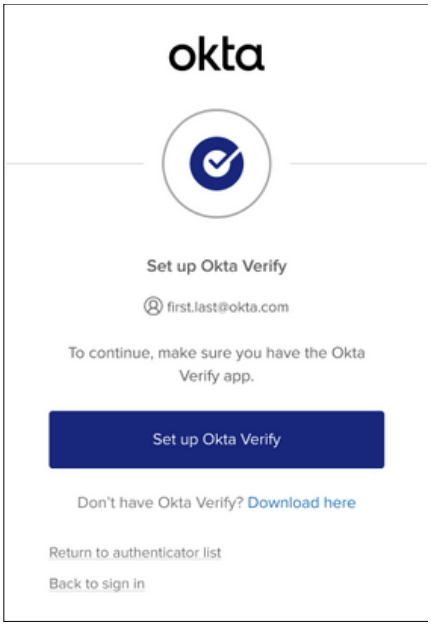
a. Assign yourself to this test application and sign in to the application.

b. You will be prompted to download or open Okta Verify. You must download Okta Verify if you haven't already.

Desktop (macOS)



Mobile (iOS)



Note: These images reflect the Okta sign-in widget version 7.18 and newer that is available with the self-service Early Access feature, Same-Device Enrollment for Okta FastPass.

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, you may be prompted for your organization's sign-in URL. This is the web address you use in your browser to access your organization's apps portal. It looks like example.okta.com or atko.biz.

c. Sign out and sign back in to the test application to use Okta FastPass to authenticate. You can assign other admins to the test application for additional testing.

C. Confirm

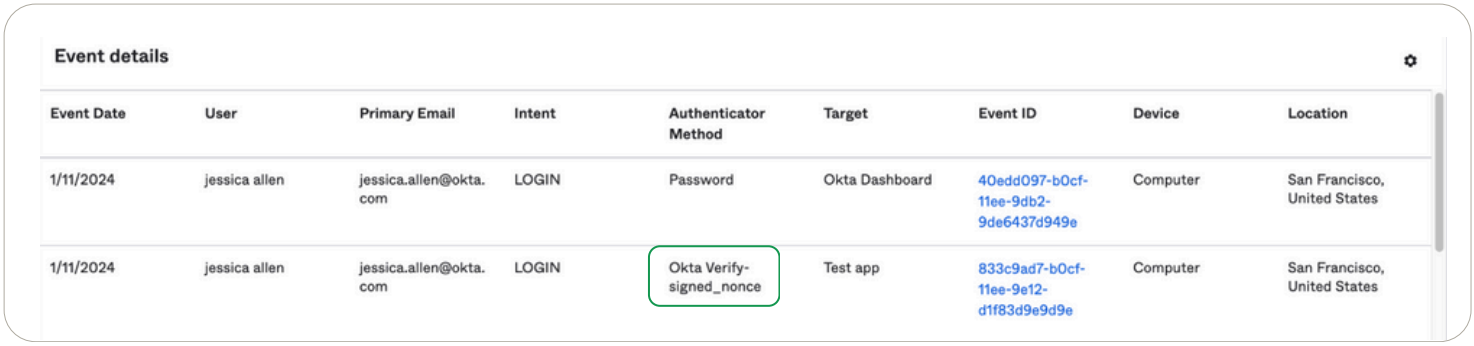
After some time has passed, you can check the MFA Activity report to see trends and how often FastPass is being used. Note that source data for this report is refreshed hourly during the day, so you might not see your recent activity immediately after it occurs.

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 user verification flows? Are there any accessibility challenges?

Step 3

Drive FastPass enrollment across your organization (10 min)

A. Prepare

Select which application(s) you want to protect with FastPass in this first batch of end 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:

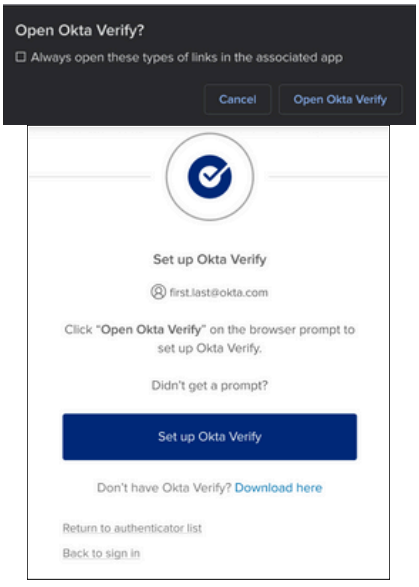
Subject: A new way to sign in called Okta FastPass is coming soon

Hi team,

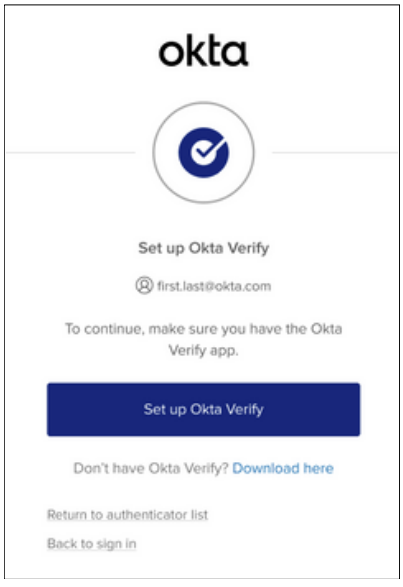
We are rolling out a new, quick, and secure way to sign in to the apps you use at work – Okta FastPass. This week, we will get many of you set up to use Okta FastPass. This is a one-time process where you will be prompted to download Okta Verify and set up Okta FastPass on your device. Complete the download then follow the instructions and verification process to set it up.

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

Desktop (macOS)



Mobile (iOS)



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

B. 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 > App sign-in***.

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.

C. Confirm

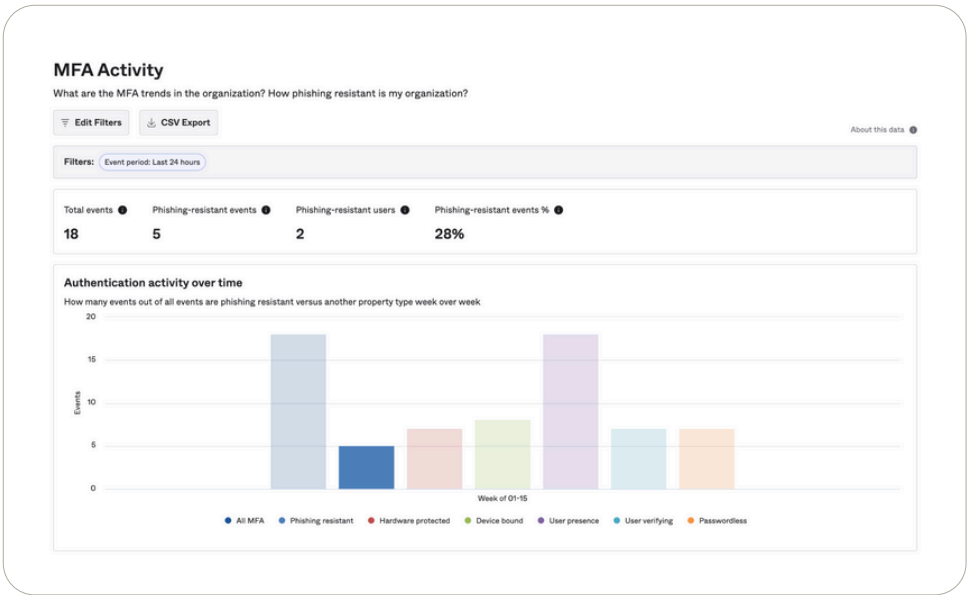
Check the MFA Activity report to see trends and how often FastPass is being used.

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



Step 4

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

A. Prepare

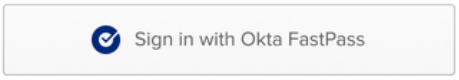
Email users to give them a heads up that they can soon click “Sign in with Okta FastPass” to skip entering their username. Here’s an example email you could send:

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 the next time you sign in. When you do, you can skip entering your username (hooray!) and proceed with signing in.



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.

B. Implement

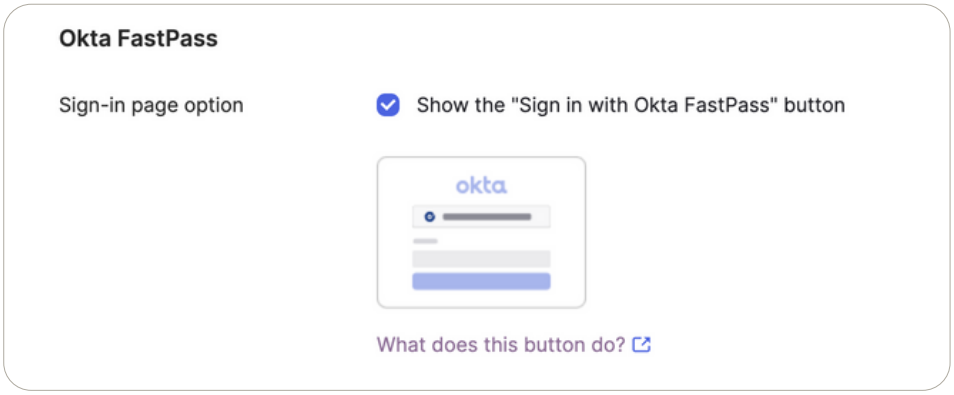
Once many of your users have enrolled in FastPass, it’s appropriate to show the “Sign in with Okta FastPass” button to everyone.

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.



What this button does

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

- Allows a seamless sign-in for users who have already enrolled in FastPass
- 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

C. 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 are protecting your apps with a phishing-resistant authentication policy, and your users can sign in more efficiently with FastPass.

Recommended setups and deviations

The following recommendations and techniques can help you to enable a smoother FastPass rollout and further secure your organization.

Deploy Okta Verify and FastPass without blocking Windows Hello for Business

Many organizations attempt to deploy Okta Verify, FastPass, and Windows Hello for Business (WHfB) simultaneously. WHfB is primarily available on Windows devices, and for organizations with a diverse device fleet, tying these projects together can often slow down the process. Decoupling the WHfB rollout from Okta Verify and FastPass reduces support issues by avoiding the simultaneous setup of interdependent systems. For more detailed information, please refer to this article.

Disable iCloud Private Relay to enable unmanaged iOS phishing resistance

Unmanaged iOS devices can not satisfy a phishing resistance policy requirement when iCloud Private Relay is enabled. If you are supporting unmanaged iOS devices, end users must disable iCloud Private Relay before authenticating. This issue applies only to Safari and native apps using Safari authentication view controllers; Chrome and Firefox are unaffected. For more detailed information, please refer to this article.

Configure Chrome to suppress the Local Network Access prompt

Starting with Chrome version 142, when you sign in with FastPass, Chrome and any Chromium-based browsers will require your permission for the Okta sign-in page to communicate with a secure loopback server on your devices. Okta recommends either notifying your end users that this is a safe and expected prompt or pre-granting that permission for using the Local Network Access enterprise policy for Managed Chrome Profiles. For more detailed information, please refer to this article.

Configure an Okta account management policy

The Okta account management policy defines authentication requirements when users enroll or unenroll authenticators, recover their passwords, and unlock their accounts. Its rule-based framework lets you enforce phishing resistance from onboarding to authentication and recovery. This policy can be used to drive new members of your workforce to enroll in phishing-resistant authenticators on their first day. For more detailed information, please refer to the documentation.

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 may 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 please refer to the section "Run an IT Campaign" in this guide for an overview 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).

Leverage 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 your organization's sign-in 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 the documention to learn more.

Configure an SSO extension on iOS and macOS devices

If you have 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.

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: for Windows users, for macOS users, for Android users, and for iOS users.

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, Inc. is The World's Identity Company™. We secure Identity, so everyone is free to safely use any technology. Our customer and workforce solutions empower businesses and developers to use the power of Identity to drive security, efficiencies, and success — all while protecting their users, employees, and partners. Learn why the world's leading brands trust Okta for authentication, authorization, and more at okta.com.