Okta Identity Engine

Deploying passwordless authentication

Document history

Date	Version	Description
September 20, 2023	1.3	Updated some links and finalized the document for Okta Support.
September 12, 2023	1.2	Branding and links update
February 28, 2023	1.1	Validate and update information
November 15, 2021	1.0	Initial publication

Table of Content

Document history 1

How to use this guide 2

Who the guide is for 2

Why Passwordless? 3

Going Passwordless 3

Introducing Okta Fastpass 4

Okta Fastpass Benefits 4

Strategic considerations when deploying Fastpass 5

Key concepts & definitions 5

Registration 5

Enabling Okta Fastpass 5

User sign-on experience 5

Okta administrator experience 6

What do you need to consider before deploying Fastpass? 6

Prerequisites 7
Enable FastPass using Okta Verify as an authenticator 7
User sign-on experience 7
Okta Verify with Biometrics enabled 8
User Enumeration 9
Create a FastPass group 9
Create a Global Session policy 10
Discovery questions 11
Use cases 11
Simple security with 1-factor authentication 11
Create a bookmark app 12
Add an authentication policy for the app 12
User sign-on experience 12
Alternate sign-on flow 12
FIDO2(WebAuthn) 13
Add the WebAuthn authenticator 14
Create a bookmark app 15
Create an authentication policy 16
User sign-on experience 17
Registered & unmanaged devices with 2-factor authentication 17
Create a bookmark app 17
Create an authentication policy for the app 17
User sign-on experience 18
Other passwordless experiences 18

How to use this guide

The guide is meant to show you the options for creating passwordless sign-on experiences. Each use case is independent, so you can jump right to any use case after going through the prerequisites. For the sake of simplicity, the examples in this guide use bookmark apps.

Who the guide is for

The guide is meant for technical implementers who design, test, and deploy Okta.

The guide is written for an internal audience and should not be shared externally.

Why Passwordless?

Traditional authentication using a username and password has been the foundation of digital identity for over 50 years. But with the ever-growing number of user accounts, there are new issues: the burden on end-users to remember multiple passwords, support costs, and most importantly, the security risks posed by compromised credentials. As a result, the case for eliminating passwords from the authentication experience is getting more compelling every day.

Understanding the need for passwordless authentication starts with understanding the challenges presented by passwords. The core challenges with passwords can be broken down into the following areas:

- **Poor account security** - “80% of hacking-related breaches used either weak or stolen passwords” — Verizon Data Breach Report 2019.
- **Poor user experience** — A survey by the University of Oxford predicted that roughly a third of online purchases are abandoned at checkout because people cannot remember their passwords.
- **Increased costs** - 12.6 minutes per week average time spent entering or resetting passwords, $5m+ cost in productivity, and labor lost per company, according to the 2019 Ponemon Authentication report.

Moving beyond passwords requires some deep thought. Before organizations decide to eliminate passwords, we recommend a gradual approach by looking at threats, technology, user journeys, costs, adoption friction, and implementation.

Going Passwordless

Eliminating passwords and going passwordless can be accomplished using several different technologies.

Fundamentally, passwordless authentication is synonymous with eliminating knowledge-factor authentication methods (all memorized secrets).

In the table below, we provide an example of definitions of assurance levels (classified into three categories: low, medium & high) and requirements for authentication, as well as the “context” of the device.

Note that these assumptions are not a reference model but an example, and they must be adjusted by or with the customer based on their specific security requirements.

Authentication Assurance Level	Low	Medium	High
Factor Type	Possession	Possession + Registered	Possession + Inherence
Passwordless Authenticators & Authentication Methods options	• Email (magic link) • SMS or Phone OTP	• WebAuthn only (the cryptographic key is unique to you) • Okta Verify (no biometric) • Okta Fastpass (without biometrics)	• WebAuthn + Okta Verify Push (no biometrics) • Okta Fastpass (with Biometrics)
Device Context[1] or state	Not managed, Not Registered	Registered, Not Managed	Registered and Managed (optional)

Example only; needs to be adjusted for specific customers' requirements

(1) Refer to the Device Context Deployment Guide for more details

Finally, the user context can be considered for even more sophisticated policies enabling passwordless authentication. Internal users might have different requirements or constraints than contractors or partners. Okta offers flexibility to bring users, networks, and even risk assessment into consideration when designing policies. This is beyond the scope of this Deployment Guide.

Introducing Okta Fastpass

Okta Fastpass is a passwordless authentication method that can satisfy a medium or high assurance level (when combined with biometrics). Okta Fastpass is a new authentication method in Okta Verify.

Okta Fastpass Benefits

End users go through a one-time process with Okta Verify to register their devices in Okta's Universal Directory. Registering your device creates a strong user + device binding that establishes an ongoing session to Okta, enabling a secure passwordless login experience.

Okta Fastpass is available on Windows, Mac OS, iOS/iPadOS, and Android and offers the same user-friendly experience across these platforms.

Key benefits include:

- Secure passwordless user experience, offering a high assurance level (when used with biometrics)
- Always on productivity, regardless of location
- Modern Universal Directory for administrator visibility, not requiring AD or any other LDAP directory

Strategic considerations when deploying Fastpass

Key concepts & definitions

Registration

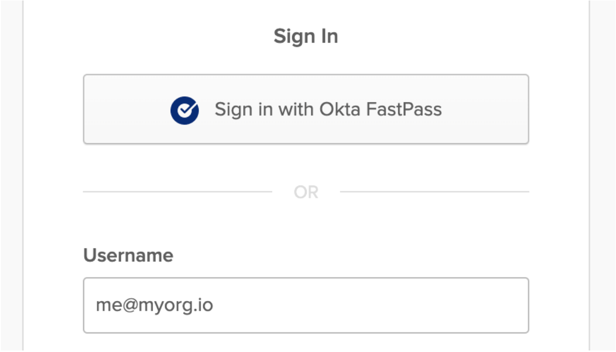
End users go through a registration process with Okta Verify to register their devices in Okta's Universal Directory. Registering your device creates a strong user + device binding, which enables a secure passwordless login experience.

Enabling Okta Fastpass

Fastpass is an optional feature of the Okta Verify authenticator and must be first activated in the authenticator configuration. Next, the organization sign-on policy (OSOP) must be set to 'Password/IDP or any factor allowed by app sign-on policy' (ASOP), delegating authentication at the application level. Finally, the ASOP can be tuned to require the end-user to be prompted and asked for biometrics or not, depending on security requirements.

User sign-on experience

Once activated, a new authentication method, ' Sign in with Okta Fastpass' is made available to the end-user.


Sign In

Sign in with Okta FastPass

OR

Username

me@myorg.io

Depending on the ASOP policy setting, the end-user is prompted by Okta Verify and/or required to provide biometrics.

Okta administrator experience

Registering devices with Okta Verify is also part of Device Context. This new feature gives the administrator visibility on the devices that the end-user has registered and for which Okta Fastpass is available for authentication.

What do you need to consider before deploying Fastpass?

Okta Fastpass is a powerful new authentication method available with Okta Verify. Major considerations:

- App Level Policies aka ASOP (and their relationship with control the access org sign-on policy (OSOP)) are an enabler of passwordless with Okta Fastpass
- Device Context allows for fine control or the context that the user, its devices, and the network he/she is connected to must present in order to be allowed to authenticate with Okta Fastpass

Furthermore, the following considerations must also be taken into account:

- Delegating authentication to ASOP and enabling Fastpass requires carefully crafting ASOP for ALL your applications; default catch-up rules in ASOP might not be enough to protect your apps.
- Although Okta Verify creates a strong binding between users and their devices, it is not a replacement for a device management solution. Limiting Okta Fastpass to managed devices only should be considered for the most sensitive apps.
- As there is 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 authenticate unless other authenticators are available
- For a complete understanding of how to balance end-user experience, assurance level, and risk, it is highly recommended that you read the Authentication Policies and Device Context Deployment guides.

Prerequisites

Before you enable any of the passwordless use cases, you have to enable FastPass using Okta Verify as an authenticator at the org level. You only have to do this once to enable all of the use cases.

Enable FastPass using Okta Verify as an authenticator

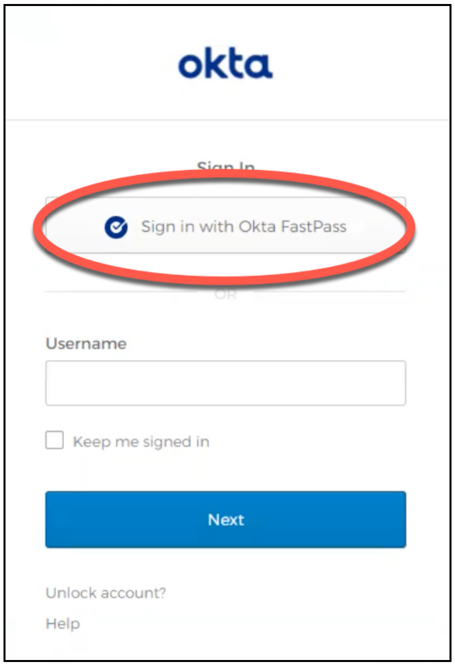
1. Open the admin console for your tenant.
2. Navigate to **Security** > **Authenticators**.
3. In the **Authenticators** section, select **Actions** > **Edit** next to **Okta Verify**.
4. On the **Okta Verify** screen, in the **Verification options** section, select **Okta FastPass (All platforms)**.
5. In the **Okta FastPass** section, select **Show the "Sign in with Okta FastPass" button**.

Selecting **Show the "Sign in with Okta FastPass" button** does three things.

- It walks first-time users through installing Okta Verify and registering a device.
- It allows an alternative if the end user's configuration doesn't permit silent sign-on. For example, mac users without a device management solution like Jamf Pro or a safari SSO browser extension will not be able to sign in silently. Enabling the button allows these users a way to sign in.
- It acts as a backup if Okta Verify doesn't load automatically.

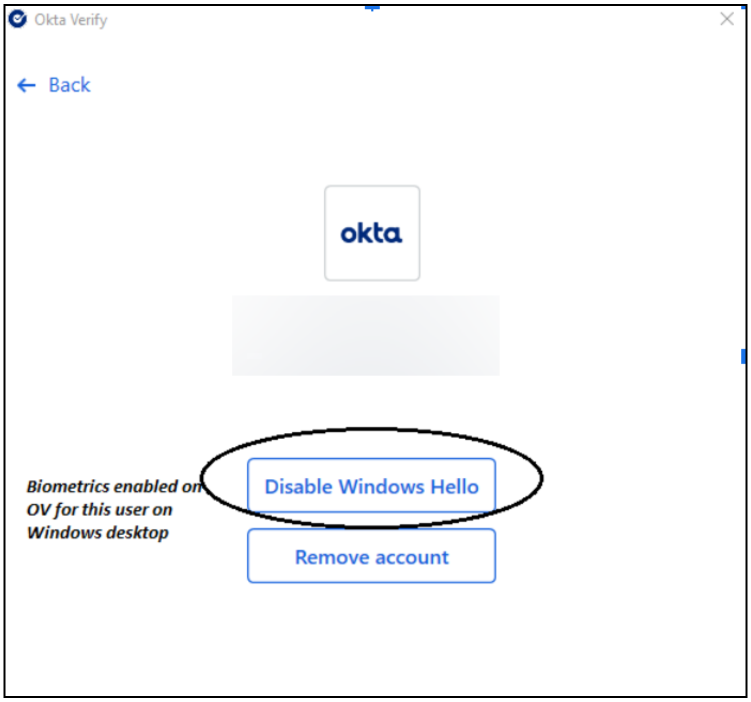
User sign-on experience

Here's what end-users will see if you enable the **Show the "Sign in with Okta FastPass" button**.



Okta Verify with Biometrics enabled

If the end-user has Okta Verify installed on the device with Biometrics enabled for Okta Verify, Okta will prompt the user for Biometrics every time irrespective of the app-level sign-on policy. Using Biometrics means that the user has satisfied a higher level of assurance. It simplifies the login to any other app requiring a higher level of assurance, which the user may attempt to access during their current session.



Biometrics enabled on OV for this user on Windows desktop

User Enumeration

This feature is intended to protect against attackers who try to find user accounts and authenticator enrollments. If this is enabled, any first-time sign-in from an unknown device will show a standard default flow with password/email options if authentication is allowed. Once the user has successfully logged in with password/email options from that device, they will be presented with all the available authenticators for subsequent authentication attempts.

Create a FastPass group

To simplify the examples in the rest of this document, create a group for passwordless sign-on and add a person to it. We're using bookmark apps for demonstration purposes but in your environment, you'd use whatever integration you need for each app.

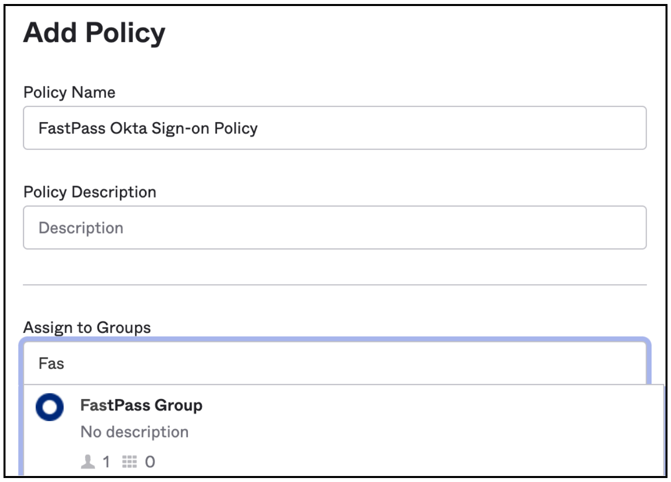
1. In your admin console, navigate to **Directory** > **Groups** and select **Add Group**.
2. In the **Add Group** dialog, enter a **Name**, for example, **FastPass Group 1**, and optionally a **Group Description** and select **Add Group**.
3. Navigate to **Directory** > **People** and select **Add person**.
4. In the **Add Person** dialog, add a **First name**, **Last name**, **Username**, and **Primary email**. Add your own email to the **Secondary email** field.
5. In the **Groups** field, select the FastPass group you created in step 2.
6. In the **Password** field, select **Set by admin**, enter a password, and deselect **User must change password on first login**.

7. Select **Save**. This is the group you'll use to walk through the steps for the first Simple security with 1-factor authentication use case.
8. Optionally create two more groups (**FastPass Group 2** and **FastPass Group 3**) for the other two use cases described in this document: Registered & unmanaged devices with 2-factor authentication and FIDO2(WebAuthn).

Create a Global Session policy

Configuring passwordless authentication requires changing your global session policy by adding a higher priority rule. This change shifts responsibility for defining and enforcing strict authentication requirements to each of your app sign-on policies. Before you remove this global requirement, protect all of your apps with a strong authentication policy.

1. In your admin console, navigate to **Security** > **Global Session Policy** and select **Add policy**.
2. In the **Add Policy** dialog, enter a **Policy Name**. A best practice is to add "Okta Sign-on Policy" to the name so that it's easy to see which policies are Okta sign-on policies when you read the logs.
3. Assign this policy to the group you created in the previous procedure. It will look similar to this:



Add Policy

Policy Name

FastPass Okta Sign-on Policy

Policy Description

Description

Assign to Groups

Fas

FastPass Group

No description

1 0

4. Select **Create Policy and Add Rule**.
5. In the **Add Rule** dialog, enter a **Rule Name**.
6. In the **Multifactor authentication (MFA) is** field, select **Not required**.

Passwordless authentication is incompatible with requiring a secondary factor. Selecting this option removes the requirement for MFA for every app in this Org and will make the global session policy to the authentication policies to determine what authenticators are needed to access the app.

1. Leave all other default values and select **Create Rule**.

Discovery questions

Before you deploy passwordless authentication, you should consider the following questions. The answers to these questions will determine what kind of passwordless experience you should use and impact configuration settings.

1. When is a user allowed this experience based on device context - should it be all devices? Registered devices only? Managed devices only?
2. What requirements does a login event need to meet to allow this flow?
3. What kind of devices are predominant in the environment? Do all of these have native biometric access? Do you want to enforce biometric flows each time?
4. What are your authentication requirements per app? You should understand Okta assurance levels and how they apply to authenticator types.
5. What other factors are allowed in Okta?
6. Does your organization use Active Directory?
7. Do you allow users to bring their own devices?
8. Do you want a different user experience depending on the device platform (for example, ios or Windows)?
9. Do you want users to be logged in silently without any user interaction?
10. Do you want your app policies to apply to users from specific network zones?

Use cases

In this section, we will cover three passwordless use cases. Using the example of assurance level and authentication method to achieve them given in the Going passwordless section above, we will cover two medium and one high assurance level.

Here are the use cases described in this document.

1. **Medium assurance level**: Simple security with 1-factor authentication
2. **Medium assurance level**: FIDO2(WebAuthn)
3. **High assurance level**: Registered & unmanaged devices with 2-factor authentication

Simple security with 1-factor authentication

In this use case, only one factor type is required to authenticate. The main objective is to show Okta Fastpass in action to offer a passwordless experience. If the policy does not require biometrics, this example is classified as having a medium assurance level.

Create a bookmark app

1. In your admin console, navigate to **Applications** > **Applications** and select **Browse App Catalog**.
2. In the **Search** box, type *bookmark app*, and select **Bookmark App** > **Add Integration**.
3. On the **Add Bookmark App** screen, change the Application label to **Bookmark App 1**.
4. Enter a **URL** and select **Done**. Because this app is for demonstration purposes only, you can choose any url you like. In a real environment, you would use the url of the app you're setting up SSO for.
5. Select the **Assignments** tab.
6. Select **Assign** > **Assign to Groups**, and then select **Assign** for **FastPass Group 1**. Don't select the group name unless you want to review the group properties.
7. Select **Done**.

Add an authentication policy for the app

Add an authentication policy allowing one-factor authentication so end-users can sign in without a password. When you add an authentication policy, you should consider who the policy applies to. Which specific users, groups, user types, or users should this policy apply to?

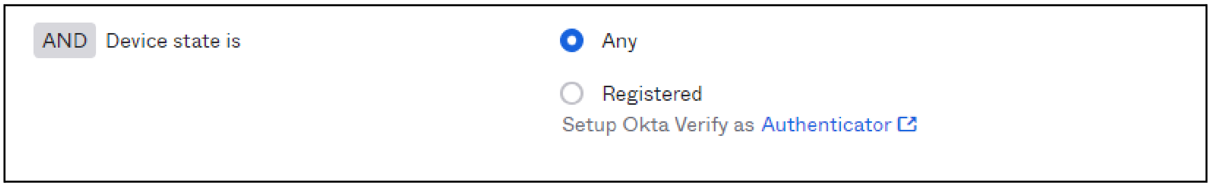
1. In your admin console, navigate to **Security** > **Authentication Policies** and select **One factor access**.
2. Select the **Applications** tab.
3. Select **Add app**.
4. In the **Add app** dialog, add **Bookmark App 1.**
5. Select **Close.**

User sign-on experience

1. In another browser instance or incognito window, navigate to the Okta end-user dashboard for this org. When changing settings, you should always clear the browser before you test the settings.
2. You should be directly signed into the app without any user interaction.

Alternate sign-on flow

If you select **Any** instead of **Registered** in the **Device State** field,



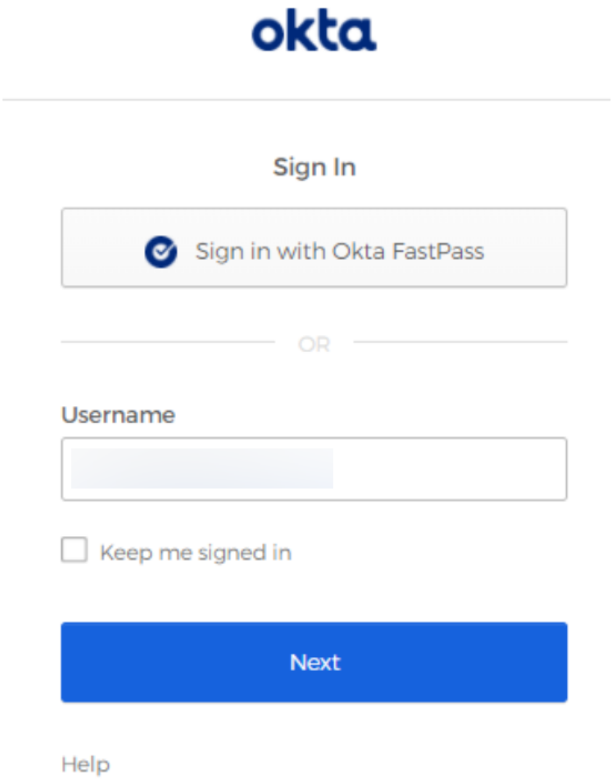
AND Device state is

● Any

○ Registered

Setup Okta Verify as Authenticator

users will always be redirected to the Okta Sign-in Widget (no silent authentication).



FIDO2(WebAuthn)

In this use case, the end-user will be offered a passwordless experience with a WebAuthn authenticator on an unmanaged device. In our example, this is classified as a medium assurance level.

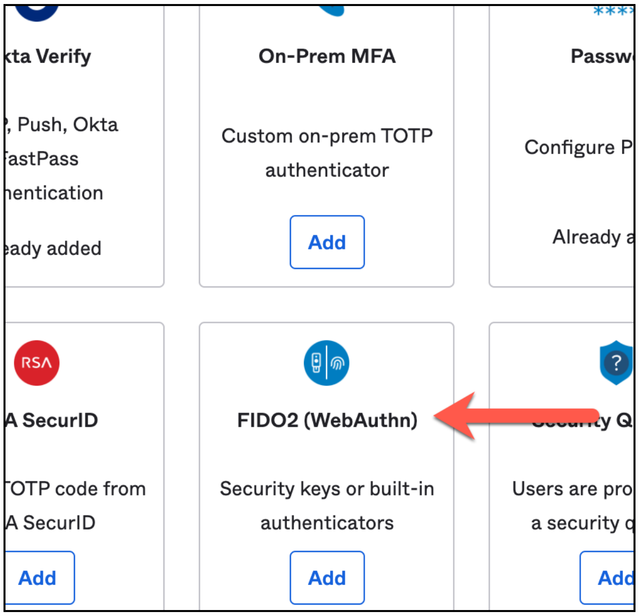
FIDO2 Web Authentication (WebAuthn) is a standard web API incorporated into web browsers and related web platform infrastructures used to securely authenticate users on the web across various sites and devices. For more information about the FIDO2 WebAuthn standard, see FIDO2 Project.

Configure FIDO2 (WebAuthn) as a multifactor authentication (MFA) option. The WebAuthn standard provides users with new methods to authenticate with MFA factors enabled and configured specifically for WebAuthn. Users must provide additional verification when configuring a WebAuthn authenticator when signing in to Okta. Users can enroll in up to 10 instances of the same WebAuthn authenticator. Users set themselves up from the sign-in widget or settings on their end-user dashboard.

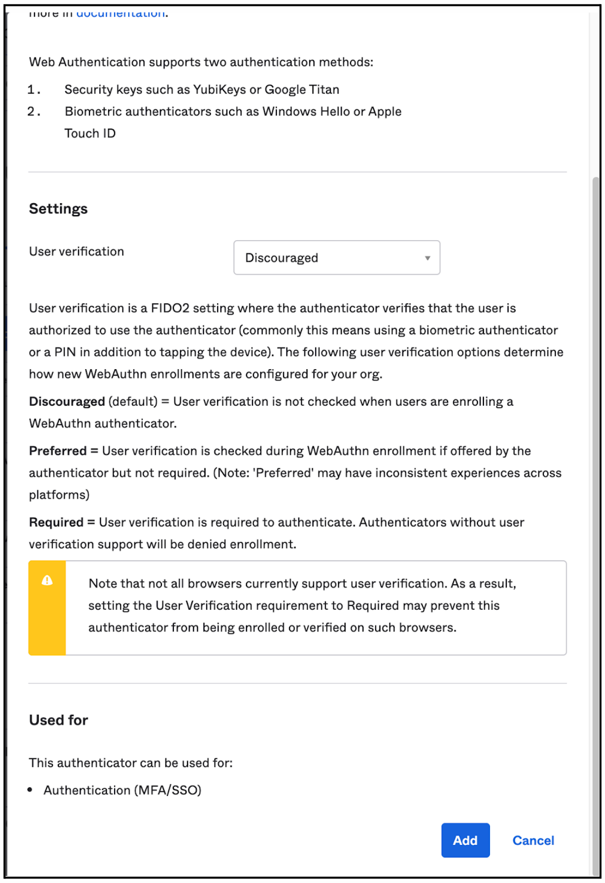
Add the WebAuthn authenticator

Okta’s WebAuthn Biometric authenticator follows the FIDO2 Web Authentication (WebAuthn) standard.

1. In your admin console, go to **Security** > **Authenticators**.
2. On the **Setup** tab, select **Add Authenticator**.
3. In the **Add Authenticator** dialog, select **Add** on the **FIDO2(WebAuthn)** tile.



4. In the **Add FIDO2 (WebAuthn)** dialog, keep default settings and select **Add**.



more in documentation.

Web Authentication supports two authentication methods:

1. Security keys such as YubiKeys or Google Titan
2. Biometric authenticators such as Windows Hello or Apple Touch ID

Settings

User verification: Discouraged

User verification is a FIDO2 setting where the authenticator verifies that the user is authorized to use the authenticator (commonly this means using a biometric authenticator or a PIN in addition to tapping the device). The following user verification options determine how new WebAuthn enrollments are configured for your org.

Discouraged (default) = User verification is not checked when users are enrolling a WebAuthn authenticator.

Preferred = User verification is checked during WebAuthn enrollment if offered by the authenticator but not required. (Note: 'Preferred' may have inconsistent experiences across platforms)

Required = User verification is required to authenticate. Authenticators without user verification support will be denied enrollment.

Note that not all browsers currently support user verification. As a result, setting the User Verification requirement to Required may prevent this authenticator from being enrolled or verified on such browsers.

Used for

This authenticator can be used for:

- Authentication (MFA/SSO)

When you configure your org with **User Verification** set to **Discouraged**, end-users who enroll a WebAuthn factor do not see the WebAuthn enrollment names of the factors they enroll; they are listed generically as **Authenticator**, and no other details about the factor are provided.

Create a bookmark app

1. In your admin console, navigate to **Applications** > **Applications** and select **Browse App Catalog**.
2. In the **Search** box, type *bookmark app*, select **Bookmark App,** and select **Add**.
3. On the **Add Bookmark App** screen, change the Application label to **Bookmark App 2**.
4. Enter a **URL** and select **Done**. Because this app is for demonstration purposes only, you can choose any URL you like. In a real environment, you would use the URL of the app you're setting up SSO for.
5. On the **Assignments** tab, select **Assign** > **Assign to Groups**, and then select **Assign** for **FastPass Group 3**. Don't select the group name unless you want to review the group properties.
6. Select **Done**.

Create an authentication policy

Create an authentication sign-on policy to allow for biometric authentication for end-users.

1. In your admin console, navigate to **Security** > **Authentication policies.**.
2. Select **Add a Policy**.
3. Enter a descriptive name for your new policy.
4. You will see a default sign-on policy with a **Catch-all Rule** that requires passwords.
5. Select **Add Rule**.
6. In the **Add Rule** dialog, add a rule name, for example, **Bookmark App 2 rule**.
7. In the **User's user type** is field, select **Any user type**.
8. In the **User's group membership includes a field**, select **At least one of the following groups**.
9. Start typing the name of the group you created in the prerequisites and then select it, for example, **FastPass Group 2**.
10. In the **User is** field, select **Any user**.
11. In the **Device State** field select **Any**. This turns off the silent polling feature of the Okta Sign-In Widget, which means the Sign-In Widget will display options for the authenticators you have enabled for your users.
12. Use default values for **Device Platform(Any platform)** and the **User's IP**(**Any IP)**. Also, leave the "**The following custom expression is true"** field blank. You can use the Okta Expression Language (EL) to add a custom expression to an app sign-on policy.
13. For the "**User must authenticate with"** field, choose **Possession factor**. Choosing **possession factor** would exclude "Password" as an authenticator in this policy.
14. Leave the default values in the other fields and select **Save**.
15. Select the **Applications** tab.
16. Select **Add app**.
17. Select **Add** next to the **BookMark App 2**.
18. Select **Close**.

User sign-on experience

1. In another browser instance or incognito window, navigate to the Okta end-user dashboard for this org. When changing settings, you should always clear the browser before you test the settings.
2. On the sign-in widget, users will be prompted to authenticate with their **Security Key** or **Biometric Authenticator.**

Registered & unmanaged devices with 2-factor authentication

In this use case, the end-user will be offered a passwordless experience with Okta Fastpass with biometrics on a registered but not managed device. This is classified as a high assurance level.

Create a bookmark app

1. In your admin console, navigate to **Applications** > **Applications** and select **Browse App Catalog**.
2. In the **Search** box, type *bookmark app*, select **Bookmark App,** and select **Add**.
3. On the **Add Bookmark App** screen, change the Application label to **Bookmark App 2**.
4. Enter a **URL** and select **Done**. Because this app is for demonstration purposes only, you can choose any URL you like. In a real environment, you would use the URL of the app you're setting up SSO for.
5. Select the **Assignments** tab.
6. Select **Assign** > **Assign to Groups**, and then select **Assign** for **FastPass Group 3**. Don't select the group name unless you want to review the group properties.
7. Select **Done**.

Create an authentication policy for the app

Create an authentication policy to allow for biometric authentication for end-users. These steps use one of the bookmark applications you created in the prerequisites section.

1. Navigate to **Security** > **Authentication Policies** .
2. Select **Add a policy** .
3. Enter a descriptive name for your new policy.
4. You will see a default sign-on policy with a **Catch-all Rule** that requires passwords.
5. Select **Add Rule.**
6. In the **Add Rule** dialog, add a rule name.
7. In the **User's user type** is field, select **Any user type**.

8. In the **User's group membership includes a field**, select **At least one of the following groups**.
9. Start typing the name of the group you created in the prerequisites and then select it, for example, **FastPass Group 3**.
10. In the **User is** field, select **Any user**.
11. In the **Device State** field, select **Any**. This turns off the silent polling feature of the Okta Sign-In Widget, which means the Sign-In Widget will display options for the authenticators you have enabled for your users.
12. Use default values for **Device Platform(Any platform)** and the **User's IP**(**Any IP)**. Also, leave the "**The following custom expression is true"** field blank. You can use the Okta Expression Language (EL) to add a custom expression to an app sign-on policy.
13. In the **Access** field, select **Allowed after successful authentication**.
14. For the "**User must authenticate with"** field, choose **Possession factor**.
15. In the **Access with Okta FastPass is granted** field, choose **If the user approves a prompt in Okta Verify or provides biometrics**. This way, the user will always see the sign-in screen and must select which authenticator to use.
16. Leave the default values in the other fields and select **Save**.
17. Select the **Applications** tab.
18. Select **Add app**.
19. Select **Add** next to the **BookMark App 2**.
20. Select **Close**.

User sign-on experience

1. In another browser instance or incognito window, navigate to the Okta end-user dashboard for this org. When changing settings, you should always clear the browser before you test the settings.
2. You should see the Sign-in Widget with an option for Okta Verify. If you choose that option, you'll be asked for biometric confirmation.

Other passwordless experiences

You can also provide passwordless sign-in with other Okta features, but they are outside this document's scope.

Enhanced experience using the Okta SSO browser extension	If supported by the app's sign-on policy, you can provide Okta Verify-enrolled users an Okta FastPass experience on Safari browsers only if their device is managed and you've configured Apple

	Extensible Single Sign-On (SSO) in your mobile device management (MDM) solution. The configuration defines extensions for multi-factor user authentication on macOS devices enrolled in an MDM solution.
Email Magic Link	You can create an app sign-on policy to provide passwordless access to apps with an email magic link that your end-users can select to sign in to an application.
Agentless Desktop Single Sign-On	With agentless Desktop Single Sign-on (DSSO), you don't need to deploy IWA agents in your Active Directory domains to implement DSSO functionality. This reduces or eliminates the maintenance overhead and provides high availability as Okta assumes responsibility for Kerberos validation. The same experience can be achieved with Okta Fast Pass silent authentication flow.