INTEGRATIONS
- CrowdStrike Integration
- Intune Integration
- Jamf Integration

DIRECTORY
- Identities
- Groups
- Devices
- Roles

POLICY
- Rules

REPORTING
- Device Query

ACCESS CONTROL
- Applications
  - Generic SCIM
  - Microsoft External Authentication Methods (EAM)
  - Okta
  - OneLogin
  - WS-Fed Integration Guide
- Identity Providers

Version: Secure Access

Okta integration guide overview

This guide is a walkthrough of the stages and steps to integrate Beyond Identity as a phishing-resistant multifactor authentication addition to your Okta organization.

Once the following stages and steps are complete, end users can authenticate to Okta using their device's passkey. This enhances security by eliminating passwords from the login flow while also improving the user experience by removing the need to enter a password.

Stage summary

The integration setup consists of the four stages below. Each stage covers the initial set up for continuing the integration process on each respective platform. Follow the guide in linear order to complete the integration.

STAGE	SUMMARY	OKTA	BEYOND IDENTITY
I	Initial set up	- Set up Beyond Identity group in Okta	- Set up Okta Application in Beyond Identity Console
II	System for Cross-domain Identity Management (SCIM) implementation	- Create SCIM app - Update provisioning for SCIM - Push SCIM users	- Create API token for inbound SCIM
III	Single sign-on configuration	- Create Okta API token - Set up custom attribute for users	- Configure Okta domain
IV	Identity provider setup and enrollment	- Configure new identity provider - Create routing rules	- Assign application to group - Enroll users - Create Okta bookmark

Prerequisites

This information contains the necessary items for integrating Beyond Identity into your Okta organization with phishing-resistant multifactor authentication.

Okta

- Okta account access with Organizational Admin or Super Admin privileges
- Available features of OpenID Connect IdP and routing rules
  - Validate the following with these steps below in your Okta Console to view their availability
    - OpenID Connect IdP: Security → Identity Providers → Add identity provider button → OpenID Connect IdP
    - Routing rules: Security → Identity Providers → Routing rules
  - NOTE: If these features are missing from your organization, contact Okta support for activation.

Beyond Identity requirements

The list below covers the basic Beyond Identity requirements for the integration.

- Secure Access Tenant with Super Admin Role
  - Use an existing account, or sign up here to create a new Beyond Identity account
- Have at least two devices and two Super Admin roles configured*
  - **Recommended, optional*

Steps

Follow the steps in the sections below to complete your integration for Beyond Identity and Okta.

Legend

The sections below use these two color codings to identify the steps for separate platforms.

🔵 Beyond Identity: Beyond Identity platform tasks are highlighted in blue. 🟠 Okta: Okta platform tasks are highlighted in orange.

Stage I

The sections here are for the initial setup between Beyond Identity and Okta. This is for setting up the Okta Application in the Beyond Identity Console and for creating groups in Okta for Beyond Identity. This group is a subset of your users that use Beyond Identity for authentication instead of any current authentication methods.

🔵 Beyond Identity: Set up Okta application in Console

The steps in this section are for going through the initial Beyond Identity configuration. This covers adding the Okta integration application in the Beyond Identity Console.

1. Navigate to your Beyond Identity console.
2. On the left-hand navigation under **Access Control**, click **Applications**.
3. Select the **Browse Applications** tab.
4. Click **Okta** to proceed.
5. Click **Add OIDC**.
6. Under **General** → **Display Name**, input `Okta` into the text field.
7. Keep the app open for values to add to Okta later.

🟠 Okta: Set up Beyond Identity group

This section covers creating a Beyond Identity group in your Okta environment. This is the subset of users to use Beyond Identity phishing-resistant authentication to authenticate into Okta.

1. On your Okta home page, navigate to **Directory** → **Groups** on the left hand side.
2. Click the **Add Group** button.
3. In the **Name** field, input `Beyond Identity`. Description is optional.
4. Click **Save**. This returns you to the **Groups** page.
5. Click the **Beyond Identity** group.
6. Click the **Assign people** button to assign users with the **+** icon to the **Beyond Identity** group.
7. Click **Done** to return to the **Groups** page.

Stage II

The Stage II sections cover the System for Cross-domain Identity Management (SCIM) implementation between Beyond Identity as the inbound platform and Okta as the outbound platform.

SCIM is used to populate users from your Okta directory to the Beyond Identity directory. The SCIM protocol automatically updates any changes in your Okta directory to the Beyond Identity directory.

> NOTE
>
> With the SCIM implementation, this means the Okta directory is the source of truth. Any changes made to your Okta directory are pushed and reflected in the Beyond Identity directory.

🟠 Okta: Create outbound SCIM app

To have Okta act as the outbound SCIM provider, follow the steps below. All the steps in this process happen within the Okta platform.

1. Navigate to **Applications** → **Applications** on the left hand side.
2. Click the **Browse App catalog** button.
3. In the search field, input `SCIM 2.0 Test App (OAuth Bearer Token)` to select the correct app.
4. On the `SCIM 2.0 Test App (OAuth Bearer Token)` page, click **Add integration**.
5. In the Application label field, update the text to `Beyond Identity Outbound SCIM`.
6. For the **General settings· Required** page, the default values are valid. Click **Next**.
7. For the **Sign-On Options· Required** page, the default values are valid as well. Click **Done** at the bottom of the page.

After this section, return to the Beyond Identity Console to copy values for this SCIM configuration.

🔵 Beyond Identity: Create API token for inbound SCIM

This section is for configuring Okta as an inbound SCIM provider for your Beyond Identity directory. Follow the steps below in your Beyond Identity Console.

1. In the Okta app in Beyond Identity you created in Stage I, navigate to the **Bearer tokens** section.
2. Click **Add bearer token**.
3. Input a name for the bearer token such as `Okta SCIM Token`.
4. Select an expiration date for the token. The default value is valid.
5. Copy the value and store in a secure location.
6. Scroll to the **Configure inbound provisioning** section.
7. Copy the **SCIM URL** value, for example `https://api-us.beyondidentity.com/v1/.../scim/v2`.

> NOTE
>
> The Beyond Identity bearer token for the inbound SCIM has an expiration date. To continue with the SCIM implementation, the token must be updated after the initial token expires.
>
> Okta does not support SCIM with `client credentials`. This is a service-to-service authentication protocol that automatically refreshes the tokens.
>
> Adding `Basic Authentication` to our SCIM implementation and not having to update the token after expiration is coming at a later time.

🟠 Okta: Update provisioning for SCIM

After completing the Beyond Identity section for copying the SCIM URL and Bearer token values, this section goes over testing the credentials within Okta to prepare for SCIM. These steps are from your Okta Admin Console.

1. In your **Beyond Identity Outbound SCIM** application you created earlier, navigate to the **Provisioning** tab.
2. Click the **Configure API Integration** button.
3. Check the **Enable API integration** box.
4. From the Beyond Identity: Create API token for inbound SCIM section, copy and input the following values into Okta.
   - **SCIM URL → SCIM 2.0 Base Url**
   - **Bearer token → OAuth Bearer Token**
5. Click **Test API Credentials**.
   - Click **Save** if the test is successful.
   - If the test is not successful, return to the Beyond Identity: Create API token for inbound SCIM section above and repeat the steps.

🟠 Okta: Continue SCIM app setup

When the API credentials are configured, this means Okta can now begin provisioning users from your Okta directory to the Beyond Identity directory. Follow the steps below to finish your SCIM app setup in Okta.

When this step is completed, the **Beyond Identity** group created in Okta: Set up Beyond Identity group is synced to your Beyond Identity directory.

1. On the **SCIM Beyond Identity Application** page, navigate to **Provisioning** → **To App** → **Provisioning to App** section.
2. Click **Edit.**
3. Check the following boxes.
   a. **Create Users**
   b. **Update User Attributes**
   c. **Deactivate users**
4. Click **Save**.
5. Navigate to **Assignments** → Click **Assign** drop down → Select **Assign to Groups**.
6. Select **Assign** for **Beyond Identity** group.
7. Click **Save and Go Back**.
8. Click **Done**.

🟠 Okta: Push SCIM users

With the configuration complete for the inbound and outbound SCIM implementation, the app must push users to Beyond Identity. Begin this process with the steps below.

1. On the **Beyond Identity Outbound SCIM** Application page, navigate to **Push Groups** tab.
2. Click **Push Groups** dropdown.
3. Select **Find groups by name**.
4. Search for **Beyond Identity** group.
   - *NOTE*: The Okta directory cannot have a group with the same name existing in the Beyond Identity directory. Group name collisions result in an error.
5. Click **Save**. This prompts the SCIM process to begin in Okta to push the group to Beyond Identity.

> NOTE
>
> Identities may not appear in the group when pushing the SCIM transfer if users are provisioned before the group in Okta. This may happen because of a provisioning error during the SCIM transfer.
>
> To update users and groups in the correct order, provision users in Okta after provisioning the group for the SCIM transfer. If an identity provisioining error occurs during the SCIM transfer, navigate to the **Identities** section of your Okta dashboard to resolve the error.

Stage III

This section involves setting up a callback hook into your Okta directory to update an attribute on users in your Okta directory. This value communicates that the user has registered a Beyond Identity passkey. This attribute is necessary in Stage IV, Okta: Create routing rules to route your users to use Beyond Identity to authenticate into Okta rather than your existing authentication methods.

🟠 Okta: Create Okta API token

The steps below are for the Okta platform. This section guides you through creating an API token to use within Beyond Identity.

1. On the Okta platform, navigate to **Security** → **API** → click the **Tokens** tab.
2. Click the **Create token** button.
3. Input a name for the token in the first field.
4. On the dropdown field below, select **Any IP**.
5. Click **Create token**.
6. Name the token **Beyond Identity API Token**.
7. API Calls made with this token must originate from **Any IP**. This can be changed later.
8. Copy the token value and store it in a secure location. Click **OK, got it** to continue.

🟠 Okta: Set up custom attribute for users

The section here is for setting up a custom attribute for users in Okta. This value acts as a flag for users signing in to Okta to be directed to the Beyond Identity sign on process.

When the user registers a Beyond Identity passkey, the cloud service sets the `byndidRegistered` value to `true` in the Okta user's profile. This indicates the user has a Beyond Identity passkey. It is used for the routing rule to direct users to use Beyond Identity authentication during login.

1. On the Okta platform, navigate to **Directory** → **Profile editor**.
2. Select the **User (default)** profile under the Okta type.
3. Scroll to the **Attributes** section.
4. Click **+ Add attribute**.
5. For the attribute, select the following and input or select the values in the associated fields.
   a. **Data type** → **Boolean**
   b. **Display name** → `Beyond Identity Registration Status`
   c. **Variable name** → `byndidRegistered`
   d. **User permission** → select **Read only**
6. Click **Save**.

🔵 Beyond Identity: Configure Okta domain and set up API Access

This section guides you through configuring the Okta token created in the previous step to set an attribute in your Okta directory, indicating that the user is registered with Beyond Identity. This attribute is also used in the Okta: Create routing rules section to route users through Beyond Identity for authentication.

1. On the new Okta app in Beyond Identity, navigate to the **Configure registration attribute for users in Okta** section.
2. Input the following information into the respective fields.
   - Okta Domain → the Okta domain URL value from your Okta account
     NOTE: This value must resolve to the full URL and omit the `-admin` suffix, for example `https://dev-48007952.okta.com`.
   - Okta Token → the Okta token from Step 6 of 🟠 Okta: Create Okta API token
3. Click **Save changes** at the top of the page.
4. Scroll down to the **Client Information & Endpoints** section for values to copy to Okta.

> NOTE
>
> Check the identities and groups in the Beyond Identity Console to confirm the SCIM setup and application success. Updates may take time. If the SCIM setup hasn't completed, check your SCIM application configuration.

Stage IV

In this stage of the integration, the Okta platform requires the new identity provider of Beyond Identity to get configured. The sections below also include using routing rules for Beyond Identity to serve as the identity provider when logging into Okta resources.

After Okta has the Beyond Identity identity provider set up, the users and groups in Beyond Identity must be assigned to the new Okta app within the console. This completes the process to use Beyond Identity as the phishing-resistant multi-factor authentication flow for users.

🟠 Okta: Configure new identity provider

This section is for setting up Beyond Identity as a new identity provider in Okta. These steps require values from Beyond Identity to enable the phishing-resistant multifactor authentication flow.

> NOTE
>
> The steps here must be completed before moving on to the Beyond Identity sections for Stage IV.

1. On the Okta platform, navigate to **Security** → **Identity Providers**.
2. Click **+ Add identity provider**.
3. Select **OpenID Connect IdP** and click **Next**.
4. Under the General settings section, input `Beyond Identity` for the name.
5. Under the **Client details** and **Endpoints** sections, input the following values from **Client Information & Endpoints** of your Okta app in Beyond Identity.

NOTE: On your Okta app in Beyond Identity, confirm the `Client ID` and `Client secret` values are from the **Client Information & Endpoints** section. The separate values from the **Configure inbound provisioning** section aren't valid for the Okta identity provider.

- **Client ID** → 🟠 **Client ID**, under Client details
- **Client Secret** → 🟠 **Client Secret**, under Client details
- **Issuer** → 🟠 **Issuer**, under Endpoints
- **JWKS URI** → 🟠 **JWKS endpoint**, under Endpoints
- **Authorization Endpoint** → 🟠 **Authorization endpoint**, under Endpoints
- **Token Endpoint** → 🟠 **Token endpoint**, under Endpoints
- **User Info Endpoint** → 🟠 **Userinfo endpoint**, under Endpoints

6. Under the **Authentication settings optional** section, configure the following fields and values.
   - **Match against** → **Okta Username or Email**
   - **Account link policy** → **Automatic**
   - **If no match is found** → **Redirect to Okta Sign-in page**
7. Keep the default values for remaining sections. Click **Finish** at the bottom of the page.

🟠 Okta: Create routing rules

After having Beyond Identity as an identity provider in Okta, set up routing rules for enrolled Beyond Identity users to go through Beyond Identity for phishing-resistant multifactor authentication.

1. On the Okta platform, navigate to **Security** → **Identity providers** → **Routing rules** tab
2. Click **Add routing rule**.
3. Input `Beyond Identity` as the name for the routing rule.
4. Configure the **AND User matches** option to **User attribute**. Add the following values for the option.
   - `byndidRegistered`, **Equals**, **true**
5. For the **THEN Use this identity provider** option, remove **Okta.**
6. Select **Beyond Identity**.
7. Click **Create rule**.

> ⊗ DANGER
>
> Routing rules in Okta are active immediately after creating the rule. For security purposes, maintain a super administrator account that is isolated from routing rules to prevent lockout.

🔵 Beyond Identity: Assign Application to group

This section of Stage IV is for assigning the Okta application to Beyond Identity. When this is configured, users can begin using the phishing-resistant multifactor authentication process through Okta and Beyond Identity. Complete these steps within the Beyond Identity console.

1. On the Okta app in Beyond Identity, navigate to the **Assignments** tab.
2. Click the **Add assignments** dropdown and select **By Group**.
3. On the **Assign Groups** pop up, select the **Beyond Identity** group.
4. Click **Assign Groups**.
5. At the top of the page, click **Save Changes**.

> NOTE
>
> Users must be assigned the Okta application in Beyond Identity to use the phishing-resistant multifactor authentication flow.

🔵 Beyond Identity: Enroll users

After completing the Okta and Beyond Identity integration for phishing-resistant multifactor authentication, follow the steps in this section to enroll users and their passkeys.

With the passkey, the process for users to log in to their Okta resources uses the Beyond Identity flow without requiring a password. Use the Beyond Identity console to complete the steps below.

Bulk Enrollment

1. On the Beyond Identity console, navigate to **Identities**.
2. Use the **Enrollment status** filter to filter by enrollment status. Enrollment status can be one of the following values:
   - **Unenrolled**: The identity does not have any pending invites or any active passkeys.
   - **Pending**: The identity has one or more pending invites and no active passkeys.
   - **Enrolled**: The identity has one or more active passkeys.
3. After filtering, you can multi-select users that you want to send an enrollment email to.
4. Click the **Add passkey(s)** button above the identities table. A **Send enrollment** modal should appear.
5. Under Identity Verification Method, select **Magic link**.
   a. For the **Send email** option, the email connected to that identity receives a Beyond Identity welcome email for the process to register a passkey.
6. When the user goes through the enrollment process, they will go through an interactive guide with the following 2 steps:
   a. Download the Beyond Identity Platform Authenticator - this is the app that is required for Beyond Identity authentication.
   b. Enroll a passkey on their device.

Single identity enrollment

1. On the Beyond Identity console, navigate to **Identities** → a specific user → **Passkeys** tab.
2. The following options are avaialable for adding a passkey for an identity:
   a. If an identity does not have any active passkeys, click the **Add a passkey** button in the middle.
   b. If an identity has one or more active passkeys, click the **Actions** button → **Add passkey**.
3. Under Identity Verification Method, select **Magic link**.
4. For the Delivery Method option, select **Send email** or **Generate link.**
5. Click the **Send enrollment** button.
   a. For the **Send email** option, the email connected to that identity receives a Beyond Identity welcome email for the process to register a passkey.
   b. For the **Generate link** option, a URL is generated from Beyond Identity. This link is for sharing with the user for them to register a passkey.
6. When the user goes through the enrollment process, they will go through an interactive guide with the following 2 steps:
   a. Download the Beyond Identity Platform Authenticator - this is the app that is required for Beyond Identity authentication.
   b. Enroll a passkey on their device.

🔵 Beyond Identity: Create Okta bookmark

With the sections above completed, this section is for creating a bookmark for Okta within Beyond Identity. This streamlines users within Beyond Identity to access their Okta resources from their login page. Follow the steps below from within the Beyond Identity console.

1. On the Beyond Identity console, navigate to **Applications** → **Browse Applications** → **Bookmark** → Click **Add Bookmark**.
2. Input `Okta` in the **Display Name** field.
3. For the **Login Link** field, input the Okta organization URL, for example `https://beyondidentity.okta.com/`.
4. Optionally, for the **App Tile** option, use the Upload icon file to add an image for the user dashboard.
5. Click **Save Changes** at the top of the screen.
6. Navigate to the **Assignments** tab and add the Beyond Identity group to this bookmark app.

End users: Register passkey

End users receive their link then follow the interactive guide for Beyond Identity.

This enrollment email guides through the following steps.

1. Download the Beyond Identity Platform Authenticator. This is the required application for Beyond Identity authentication.
2. Enroll a passkey on their device.

> TIP
>
> Congratulations! You've completed your Okta and Beyond Identity integration!
>
> Now, when your users login to Okta, they are prompted with Beyond Identity for seamless authentication experience.

Stage summary
Prerequisites
  Okta
  Beyond Identity requirements
Legend
Stage I
  🔵 Beyond Identity: Set up Okta application in Console
  🟠 Okta: Set up Beyond Identity group
Stage II
  🟠 Okta: Create outbound SCIM app
  🔵 Beyond Identity: Create API token for inbound SCIM
  🟠 Okta: Update provisioning for SCIM
  🟠 Okta: Continue SCIM app setup
  🟠 Okta: Push SCIM users
Stage III
  🟠 Okta: Create Okta API token
  🟠 Okta: Set up custom attribute for users
  🔵 Beyond Identity: Configure Okta domain and set up API Access
Stage IV
  🟠 Okta: Configure new identity provider
  🟠 Okta: Create routing rules
  🔵 Beyond Identity: Assign Application to group
  🔵 Beyond Identity: Enroll users
  🔵 Beyond Identity: Create Okta bookmark
End users: Register passkey

See something not documented or want to contribute?
- Submit a content issue
- Suggest an idea for the documentation
- Edit this page

Join our community!
- Slack
- Twitter

© 2025 Beyond Identity | Terms and Conditions