# BeyondTrust

# Identity Security Insights Identity Providers 24.04

2

# **Table of Contents**

Configure Identity Providers for Identity Security Insights	3
Configure Microsoft Entra ID as an Identity Provider	4
Create a New Application in Microsoft Entra ID	4
Add a New Identity Provider in Identity Security Insights	4
Provide Your Microsoft Azure Credentials	5
Update Your Azure Single Sign-On URL	5
Invite Organization Users	6
Configure Okta as an Identity Provider	7
Create a New Application in Okta	7
Add a New Identity Provider in Identity Security Insights	7
Provide Your Okta Credentials	8
Update Your Okta Single Sign-On URL	8
Invite Organization Users	9
Configure PingOne as an Identity Provider1	0
Create a New Application in PingOne1	0
Add a New Identity Provider in Identity Security Insights	0
Provide Your PingOne Credentials1	1
Update Your PingOne Configuration1	1
Invite Organization Users	2

<sup>©2003-2024</sup> BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 4/2/2024 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

3

# **Configure Identity Providers for Identity Security Insights**

Identity Security Insights supports connecting to your third-party single sign-on applications. Configuring an identity provider allows members of your organization secure and authorized access to the Insights platform, enabling you to centrally manage accounts, passwords, and identity verification in a manner familiar to both your users and security team.

Insights currently supports the following identity providers using SAML:

- Microsoft Entra ID
- Okta
- PingOne

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 4/2/2024 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

## **Configure Microsoft Entra ID as an Identity Provider**

Companies using Microsoft Azure to manage identity verification can integrate with Identity Security Insights to provide authorized access to their users. This guide describes how to create a new application in Microsoft Azure and register the application credentials in Insights.

**Note:** You must have your Microsoft Azure dashboard and Identity Security Insights open simultaneously to complete setup. Ensure you are logged in as an administrator in both Microsoft Azure and Insights prior to beginning.

#### **Create a New Application in Microsoft Entra ID**

To begin adding Microsoft Azure as an identity provider, you must create a new application for Identity Security Insights within Microsoft Azure.

- 1. Open your Microsoft Entra ID console, and ensure you are logged in as an administrator.
- 2. Search for and select Enterprise applications.
- 3. Select New application, then Create your own application.
- In the Create your own application panel, provide a humanreadable name (e.g., *Identity Security Insights*), select Integrate any other application you don't find in the gallery (Nongallery), and click Create.
- You are redirected to the management page for your new application. From this page, select Set up single sign-on, and configure the following:
  - Under Select a single sign-on method, choose SAML.
  - Basic SAML Configuration: Select SAML 2.0.
  - Identifier (Entity ID): The URL of your Insights app (e.g., example.io).
  - **Reply URL**: A temporary placeholder URL to complete the app creation (e.g., *https://placeholderazure.com*). This value will be edited with a URL generated by the Insights application in a later step.
- 6. Click Save.

#### Add a New Identity Provider in Identity Security Insights

To register an identity provider for use with Insights, it must be created within the Insights console.

Within your Insights Organization dashboard, add a new identity provider using the following steps:

1. Navigate to Menu > Identity & Authentication Providers and click Add New Identity Provider.



Create your own application



# BeyondTrust

- 2. Provide the following information in the **Add New Authentication Provider** panel:
  - **Provider Name**: The name of your SSO service, or a human-readable name for reference (e.g., *Microsoft Azure*).
  - Binding Type: Select Post from the dropdown.
  - **Domain Name**: Your organization's email domain (e.g., *example.com*).
  - Service Provider Entity ID: The URL of your Insights app (e.g., example.io).

ET Product Cwiners 👻	ADD NEW AUTHENTICATION PROVIDER
SAML Providers	Authentication Provider
Identity & Authentication Providers	
	Binding Type Post
	Service Provider Entity Id

Note: Ensure that the Service Provider Entity ID matches the Identifier (Entity ID) configured in your Azure application.

#### **Provide Your Microsoft Azure Credentials**

Once your Microsoft Azure application is created, Microsoft Azure generates several values required by Insights to complete setup.

**Note:** To provide these credentials to Insights, you must have both the Microsoft Azure and Insights dashboards open simultaneously.

- 1. Within the Azure dashboard, open your app configuration from Step 2, if it is not already open (search for **Enterprise applications**, and click your new Insights app).
- 2. Click Single sign-on for your new Insights app.
- 3. Under SAML Certificates, click Download beside Federation Metadata XML.
- Open the XML file and provide the following values to the Identity Security Insights Add New Authentication Provider panel (opened in Step 1):
  - Copy the entityID from the top line of the document, and paste the value into the Insights Identity Provider Entity ID field.
  - Copy the encoded certificate between the
     <X509Certificate> tags of the document, and paste the certificate into the Insights tab labeled Certificate 1.
  - Close the XML document.
- 5. In your Azure app configuration, under **Set up** for your application, copy the **Login URL**. Within the Insights **Add New Authentication Provider** panel, paste the **Login URL value** into the field labeled **Identity Provider Sign-On URL**.
- 6. Within the Insights Add New Authentication Provider panel, click Save Settings.

#### **Update Your Azure Single Sign-On URL**

The Insights application now generates a unique single sign-on URL to use with Microsoft Azure. To provide this URL to Microsoft Azure, follow the below steps:

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 4/2/2024 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.



# BeyondTrust

1. Within the **Identity & Authentication Providers** dashboard in Identity Security Insights, click **Actions** to the right of your newly configured identity provider and select **Edit**.

Copy the SAML Single Sign-On URL.

2. In your Azure app configuration (in Azure, search for **Enterprise applications**, and click your new Insights app), select **Edit** under **Basic SAML Configuration**.

**Reply URL**: Remove your placeholder single sign-on URL value, and **paste** the value generated by the Insights console.

3. Click Save.

#### Invite Organization Users

ime > Enterprise applications   All app	plications > Identity Security Insights >	Basic SAML Configuration
lentity Security Insigh	its   SAML-based Sign-on	
Overview A	🕴 Upload metadata file 🍏 Change single sign-on mode 💷	
Deployment Plan	Resic SAMI, Configuration	ADD JD#TS1HF
age	Identifier (Entity ID) AD	Reply URL (Assertion Consumer Service URL) * The reply URL is where the application espects to receive the authentication takes. This is also referred to as the Watertion
voperties	Sign on URL Optional Optional	Consumer Service" (ACS) in SAML
Dwners	Logout Url (Optional) Optional	Index Default
Roles and administrators		https://your-mply-unicom

Once your identity provider has been configured in Identity Security Insights, your users can be invited through the User Management console.

For more information, please see the User Management guide at <u>https://www.beyondtrust.com/docs/identity-security-</u> insights/getting-started/admin/users.htm.

depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

## **Configure Okta as an Identity Provider**

Companies using Okta to manage identity verification can integrate with Identity Security Insights to provide authorized access to their users. This guide describes how to create a new application in Okta and register the application credentials in Insights.

**Note:** You must have your Okta dashboard and Identity Security Insights open simultaneously to complete setup. Ensure you are logged in as an administrator in both Okta and Insights prior to beginning.

#### **Create a New Application in Okta**

To begin adding Okta as an identity provider, you must create a new application for Identity Security Insights within Okta.

- 1. Open your Okta tenant dashboard and ensure you are logged in as an administrator.
- 2. Navigate to Applications > Applications and click Create App Integration.
- 3. Select SAML 2.0 and click Next.
- 4. Enter a human-readable app name, such as Identity Security Insights, and then click Next.
- 5. In the Configure SAML step, provide the following information:
  - Single sign-on URL: A temporary placeholder URL to complete the app creation, e.g., *https://placeholder-okta.com*. This value will be edited with a URL generated by the Insights application in a later step.
  - Audience URI: The URL of your Insights app (e.g., example.io).
  - Name ID Format: Select EmailAddress.
  - Application Username: Select Okta username.
- 6. Click Next when complete.
- Select your customer type on the Feedback screen, and then click Finish.

1 General Settings	2 Configure SAML	3 Feedback
A SAML Settings		What does this form do?
General		This form generates the XML needed for the app's SAML request.
Single sign-on URL 🕘	http://placeholderokta.com	
	Use this for Recipient URL and Destination URL	venere do i find the info this form needs?
Audience URI (SP Entity ID) 🛛	beyondtrust.io	The app you're trying to integrate wit should have its own documentation o
Default RelayState		doc, and it should outline what
	If no value is set, a blank RelayState is sent	information you need to specify in thi form.
Name ID format 🚳	EmailAddress *	
Application username		

#### Add a New Identity Provider in Identity Security Insights

To register an identity provider for use with Insights, it must be created within the Insights console.

Within your Insights Organization dashboard, add a new identity provider using the following steps:

- 1. Navigate to Menu > Identity & Authentication Providers and click Add New Identity Provider.
- Provide the following information in the Add New Authentication Provider panel:
  - **Provider Name**: The name of your SSO service, or a human-readable name for reference (e.g., *Okta*).
  - **Binding Type**: Select **Post** from the dropdown.
  - **Domain Name**: Your organization's email domain (e.g., *example.com*).
  - Service Provider Entity ID: The URL of your Insights app (e.g., example.io).



Note: Ensure that the Service Provider Entity ID matches the Audience URI configured in your Okta application.

#### **Provide Your Okta Credentials**

Once your Okta application is created, Okta generates several values required by Insights to complete setup.

Note: To provide these credentials to Insights, you must have both the Okta and Insights dashboards open simultaneously.

- 1. Within your Okta dashboard, navigate to Applications > Applications and select your new Insights app from the list.
- 2. In the Sign On tab, click View SAML setup instructions on the right side.
- 3. Okta displays a list of items required to finish configuration. The following items must be copied from the Okta dashboard and pasted into the Identity Security Insights **Add New Authentication Provider** panel (opened in Step 1):
  - Paste the Okta Identity Provider Single Sign-On URL into the Insights Identity Provider Sign-On URL field.
  - Paste the Okta Identity Provider Issuer value into the Insights Identity Provider Entity ID field.
  - Within Okta, copy the certificate encoding between the text BEGIN CERTIFICATE and END CERTIFICATE, and paste the certificate into the Insights tab labeled Certificate 1.
- Within the Insights Add New Authentication Provider panel, click Save Settings.

#### Update Your Okta Single Sign-On URL

The Insights application now generates a unique single sign-on URL to use with Okta. To provide this URL to Okta, follow the below steps:

- Expression: Constraints of the constraints of th
- 1. Within the **Identity & Authentication Providers** screen in the Insights dashboard, click **Actions** to the right of your newly configured identity provider and select **Edit**.

Copy the SAML Single Sign-On URL.

- In your Okta dashboard, navigate to Applications > Applications and select your newly configured Insights app.
  - Under General > SAML Settings, click Edit.
  - In the General Settings tab, click Next.
  - In the Configure SAML tab, remove your placeholder single sign-on URL value, and paste the value generated by the Insights console.
- 3. Click **Next**, and then click **Finish** to save your changes.



SALES: www.beyondtrust.com/contac	SUPPORT: www.beyondtrust.com/support	DOCUMENTATION: www.beyondtrust.com/docs
-----------------------------------	--------------------------------------	---

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 4/2/2024 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.



9

### **Invite Organization Users**

Once your identity provider has been configured in Identity Security Insights, your users can be invited through the User Management console.

For more information, please see the <u>User Management guide</u> at <u>https://www.beyondtrust.com/docs/identity-security-</u> insights/getting-started/admin/users.htm.

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

## Configure PingOne as an Identity Provider

Companies using PingOne to manage identity verification can integrate with Identity Security Insights to provide authorized access to their users. This guide describes how to create a new application in PingOne and register the application credentials in Insights.

**Note:** You must have your PingOne dashboard and Identity Security Insights open simultaneously to complete setup. Ensure you are logged in as an administrator in both PingOne and Insights prior to beginning.

#### Create a New Application in PingOne

To begin adding PingOne as an identity provider, you must create a new application for Identity Security Insights within PingOne.

- 1. Open your PingOne console and ensure you are logged in as an administrator.
- 2. Select the environment you would like to configure Insights for, and then navigate to **Connections > Applications**.
- 3. Click the plus sign beside **Applications** to create a new application.
- In the Add Application panel, provide a human-readable name (e.g., *Identity Security Insights*), a useful description, and click Configure.
- In the following SAML Configuration page, under Provide Application Metadata, select Manually Enter and provide the following information:
  - ACS URLs: A temporary placeholder URL to complete the app creation (e.g., *https://my-ping-placeholder.com*). This value will be edited with a URL generated by the Insights application in a later step.
  - Entity ID: A unique identifier for your IDP (e.g., ping).



6. Click Save.

#### Add a New Identity Provider in Identity Security Insights

To register an identity provider for use with Insights, it must be created within the Insights console.

Within your Insights Organization dashboard, add a new identity provider using the following steps:

- 1. Navigate to Menu > Identity & Authentication Providers and click Add New Identity Provider.
- Provide the following information in the Add New Authentication Provider panel:
  - Provider Name: The name of your SSO service, or a human-readable name for reference (e.g., *PingOne*).
  - Binding Type: Select Post from the dropdown.
  - **Domain Name**: Your organization's email domain (e.g., *example.com*).
  - Service Provider Entity ID: The unique Entity ID assigned in the previous step.



Note: Ensure that the Service Provider Entity ID matches the Entity ID configured in your Ping application.

#### **Provide Your PingOne Credentials**

Once your PingOne application is created, PingOne generates several values required by Insights to complete setup.

**Note:** To provide these credentials to Insights, you must have both the PingOne and Insights dashboards open simultaneously.

- Within the PingOne dashboard, open your app configuration from Step 2 if it is not already open (navigate to Connections > Application and click your new Insights app), and then click the Overview tab.
- 2. Copy the Single Signon Service URL. Within the Insights Add New Authentication Provider panel, paste the Single Signon Service URL value into the field labeled Identity Provider Sign-On URL.
- 3. Copy the **Issuer ID**. Within the Insights **Add New Authentication Provider** panel, paste the **Issuer ID value** into the field labeled **Identity Provider Entity ID**.
- 4. Click **Download Signing Certificate** and open the certificate file in a program such as Notepad++.
- Copy the text between -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- and paste the value into the field labeled Certificate 1.
- 6. Within the Insights Add New Authentication Provider panel, click Save Settings.

#### Update Your PingOne Configuration

#### Update the ACS URL

The Insights application now generates a unique single sign-on URL to use with PingOne. To provide this URL to PingOne, follow the below steps:

- Within the Identity & Authentication Providers dashboard in Identity Security Insights, click Actions to the right of your newly configured identity provider and select Edit.
- 2. Copy the SAML Single Sign-On URL.
- In your PingOne application (in PingOne, navigate to Connections > Application and click your new Insights app), select Configuration.
- 4. Click the pencil in the top right of the configuration menu and edit the following values:
  - ACS URL: Remove the placeholder value, and paste the SAML Single Sign-On URL generated by the Insights console.
- 5. Click Save.

	Overview	Configuration	Attribute Mappings	Policies	Access		
Configuration details for a	SAML applic	ation.					)
Connection Details	6						
Download Metadata							
Download Signing Cert	ificate						
Issuer ID your-issuer-id 📋							
Single Logout Service your-single-logout-serv	vice 🗖						
Single Signon Service your-single-signon-ser	vice 🗖						
IDP Metadata URL vour-IDP-metadata-url	n						
Initiate Single Sign-On U your-single-sign-on-url	JRL						
SAML Settings							

#### **Update Mapped Attributes**

1. Click on Attribute Mappings.

**Invite Organization Users** 

- 2. Click the pencil in the top right of the configuration menu and edit the following values:
  - saml\_subject: Ensure this is set to Username.
  - userName: Ensure this is set to Username.
- 3. Click Save.

Ove	rview Configuration	Attribute Mappings	Policies	Access	
These mappings associate Ping	One user attributes to S	AML or OIDC attributes i	in the applic	ation. See Mapping	attributes.
If this Application is map the Identity Pro	accessible by users ovider ID attribute so	from more than one I the Application can d	External Id listinguish	P, it is recommen users by their IdF	ided that you
Identity Security Insights		PingOne			
saml_subject		User ID			Required

Once your identity provider has been configured in Identity Security Insights, your users can be invited through the User Management console.

For more information, please see the <u>User Management guide</u> at <u>https://www.beyondtrust.com/docs/identity-security-</u> insights/getting-started/admin/users.htm.

depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or