



# BeyondTrust

## **Identity Security Insights Connectors Guide 24.04**

## Table of Contents

---

<b>Identity Security Insights Connector Administration</b> .....	<b>4</b>
Available Connectors .....	4
Get Started with Insights Connectors .....	5
Manage Existing Connectors .....	5
View Available Connectors .....	7
Connect Identity Security Insights to Amazon Web Services .....	8
Add an AWS Connector .....	8
Connect Identity Security Insights to Microsoft Azure .....	9
Run the Microsoft Azure Connector Installation Script .....	9
Create the Microsoft Azure Connector .....	10
Connect Identity Security Insights to GitHub .....	11
Configure a New GitHub App .....	11
Add a GitHub Connector .....	12
Connect Identity Security Insights to Google Cloud Platform .....	13
Manually Configure a Google Cloud Platform Connector .....	13
Create a GCP Connector with Google Cloud Shell .....	15
Connect Identity Security Insights to Microsoft Active Directory .....	18
Prerequisites .....	18
Create the Microsoft Active Directory Connector .....	18
Information Collection .....	19
Connect Identity Security Insights to Okta .....	21
Create an Okta App Integration .....	21
Add an Okta Connector .....	22
Connect Identity Security Insights to PingOne .....	23
Create a PingOne Application .....	23
Add a PingOne Connector .....	23
Connect Identity Security Insights to BeyondTrust Endpoint Privilege Management Cloud .....	25
Create a Endpoint Privilege Management Cloud API Account .....	25
Add an Endpoint Privilege Management Cloud Connector .....	25
Connect Identity Security Insights to BeyondTrust Privileged Remote Access Cloud .....	26
Create a Privileged Remote Access API Account .....	26

---

Add a Privileged Remote Access Connector .....	26
Connect Identity Security Insights to BeyondTrust Password Safe .....	28
Configure Password Safe .....	28
Add a Password Safe Cloud Connector .....	30
Add a Password Safe On-Premise Connector .....	31
Connect Identity Security Insights to BeyondTrust Remote Support Cloud .....	32
Create a Remote Support API Account .....	32
Add a Remote Support Cloud Connector .....	32

# Identity Security Insights Connector Administration

Identity Security Insights connectors allow you to integrate third- and first-party identity and account information with your BeyondTrust Insights console. The Insights platform uses this data to build identity analytics, detect identity security threats, and make security recommendations.

Once configured, Identity Security Insights automatically schedules and pulls data from your enabled connectors, and updates the console's dashboards and reports with new or changed recommendations and detections.

## Available Connectors

When logged in to your Insights console, a list of currently available connectors can be found by selecting your desired tenant from the home screen, clicking **View Connectors**, and selecting **Available**.

- Amazon Web Services
- Github
- Google Cloud Platform
- Microsoft Azure
- Microsoft Active Directory
- Okta
- Password Safe On-Prem and Cloud
- PingOne
- Privilege Management Cloud
- Privileged Remote Access Cloud
- Remote Support Cloud



## Get Started with Insights Connectors

Identity Security Insights connectors represent integrations with both first- and third-party software. The connectors dashboard allows you to add new connectors, manage or remove existing connectors, and view each connector's status and current connectivity.

After logging in, the connectors dashboard is available by selecting your desired tenant from the home screen, and clicking **View Connectors** in the tenant console.



**Note:** For organizations that wish to restrict access to Insights by IP address, the following public IP addresses must be allowed:

- 54.163.153.193
- 54.225.135.48
- 50.16.236.14

## Manage Existing Connectors

From the connectors dashboard, existing connectors can be managed from the **Configured** tab. The list of existing connectors provides additional information regarding connection status and connectivity, as well as high-level information like connector type, name, and activity.

## Connection Options

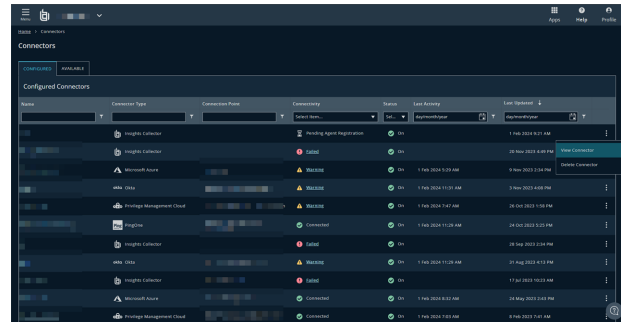
Clicking on the ellipsis beside any connector provides a list of management options.

- **View Connector** displays the connector's detailed information.
- **Turn Off Connector** pauses any scans and new recommendations. Connectors which have been turned off can be turned on again from the same menu.



**Note:** The Microsoft Active Directory connector cannot be turned off from this menu.

- **Delete Connector** removes the connector entirely. Deleted connectors must be added again from the **Available Connectors** tab.



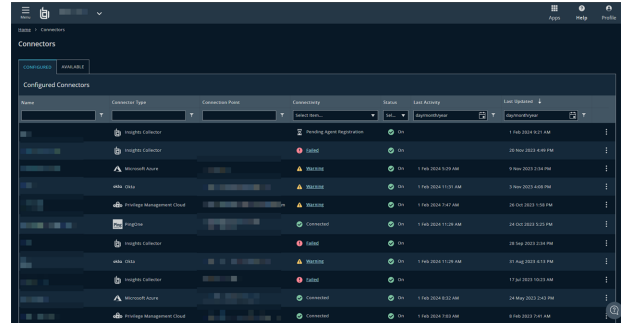
Connector Name	Connection Point	Connectivity	Status	Last Activity	Last Update
Insights Connector	...	Connected	On	7 Feb 2024 9:27 AM	7 Feb 2024 9:27 AM
Insights Connector	...	Disconnected	Off	28 Nov 2023 6:49 PM	28 Nov 2023 6:49 PM
Microsoft Azure	...	Connected	On	7 Feb 2024 3:29 AM	7 Feb 2024 3:29 AM
Web Sites	...	Connected	On	7 Feb 2024 11:20 AM	7 Feb 2024 11:20 AM
Privilege Management Cloud	...	Connected	On	7 Feb 2024 7:47 AM	16 Oct 2023 1:08 PM
Programs	...	Connected	On	7 Feb 2024 11:28 AM	24 Oct 2023 1:03 PM
Insights Connector	...	Disconnected	Off	28 Nov 2023 2:04 PM	28 Nov 2023 2:04 PM
Web Sites	...	Connected	On	7 Feb 2024 11:28 AM	27 Feb 2024 4:12 AM
Insights Connector	...	Disconnected	Off	17 Feb 2023 10:23 AM	17 Feb 2023 10:23 AM
Microsoft Azure	...	Connected	On	7 Feb 2024 8:22 AM	16 May 2023 2:03 PM
Privilege Management Cloud	...	Connected	On	7 Feb 2024 1:03 AM	18 Feb 2023 7:05 AM

## Connectivity and Status

Connectors with a **Status** set to **On** actively scan and provide recommendations for the source service. Connectors with a status of **Off** have been paused, and do not scan the service or provide new recommendations until manually turned on.

**Connectivity** displays whether or not the connector is appropriately configured.

- **Connected:** The connector is appropriately configured, and is able to scan and provide recommendations for the source service.
- **Warning:** The connector is ingesting data, but some connector requests are failing. Additional information is kept in the connector's activity history page.
- **Failed:** The connector is unable to scan or communicate with the source service. Click **Failed** to go to the connector's activity history page.
- **Connector Off:** The connector has been paused from scanning and providing recommendations.
- **Pending Agent Registration:** In the case of Microsoft Active Directory, the connector is waiting to be registered with the installer.

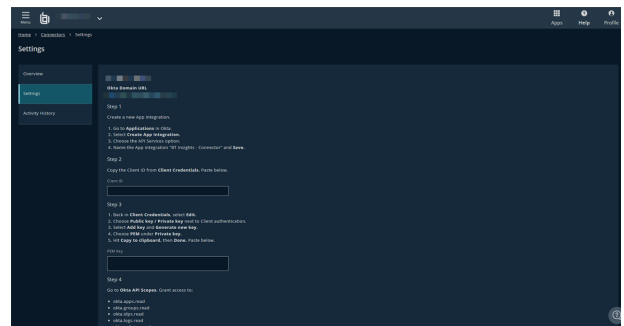


## Connection Details

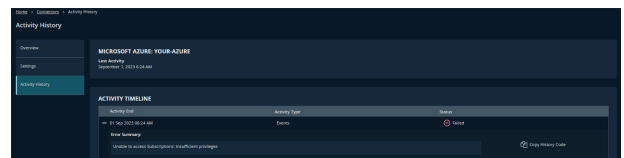
Clicking **View Connector** from the **Configured** connectors list displays detailed information for the selected connector.

The connection **Overview** displays high-level information about the selected connector. From this window, the connection name can be edited, and the connector can be turned off, on, or deleted.

**Settings** allows you to review the connection information for your selected connector. Depending on the connector type, you can update configuration requirements such as the connector's domain, API keys, usernames, authentication rules, and other credentials.



**Activity History** displays a list of the date and time of any updates or changes made to the connector. For connectors with a connectivity status of **failing** or **warning**, expand the **Activity Timeline** entry to view a summary of the error to aid in troubleshooting.



## Switch Between BeyondTrust Applications

When Identity Security Insights is connected to a BeyondTrust application, the **Apps** icon appears in the upper right of the navigation bar. The apps menu allows you to switch between connected BeyondTrust applications, and will appear in the same place in the connected application itself. The menu is automatically removed if all BeyondTrust applications are removed from Identity Security Insights, or if the connection has not been active in 60 days.

To switch between applications, click on **Apps** in the navigation bar, and click on the desired application. Re-entering credentials may be necessary depending on the login configuration of the connected application.

## View Available Connectors

New connectors can be added from the **Available** tab.

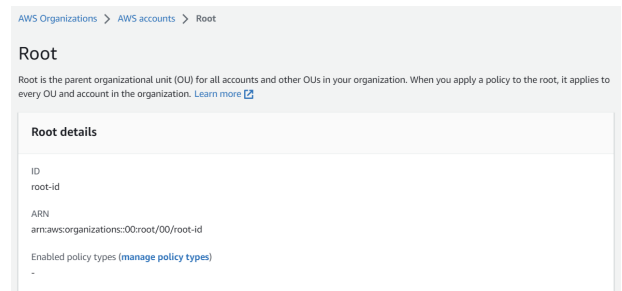
Clicking **Add** beside any connector type begins the process of adding a new connector of that type. You can add multiple connectors of the same type to a single tenant.


# Connect Identity Security Insights to Amazon Web Services

## Add an AWS Connector

1. Within the Insights **Tenant** dashboard, navigate to **Menu > Connectors > Available** and click **Create Connector** beside **AWS**.
2. In the connection panel, enter a human-readable name for your AWS connector.
3. Use the provided AWS Organizations link to log in to your AWS account. This link directs you to the **AWS Organizations > AWS accounts** page.

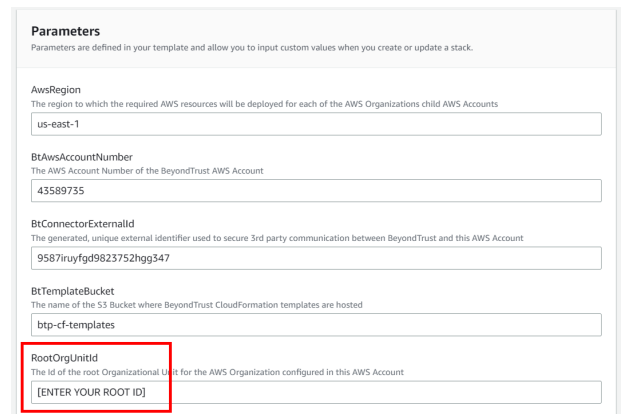
Under the **Root details** section, copy the **ID**. You use this ID in the next step.



 **Note:** To use the template provided by the AWS connector, a credit card must be associated with your AWS account.

A **CloudFormation** template link is provided in the Insights connection panel. This template creates an IAM role and policy for Insights to use when accessing your AWS resources. To create a new stack from this template, follow the steps below:

1. Click the **CloudFormation** link to prepopulate the Create Stack wizard with the required parameters, including the URL of the Insights CloudFormation template.
2. In the new **CloudFormation** window, paste the ID you obtained in Step 2 into the **RootOrgUnitId** field in the **Parameters** section.
3. Confirm the **BtConnectorExternalId** field in the **Parameters** section is the same as External ID shown in the Insights Connection panel.
4. Under **Capabilities**, select *[I acknowledge that AWS CloudFormation might create IAM resources]*.
5. Click **Create Stack**. It can take several minutes to finish building your new stack.
6. Once your stack has been created, navigate to the **Outputs** tab in AWS CloudFormation.
  - Copy the **ARN** value provided in the **Outputs** tab, and paste it into the **ARN** field within the Identity Security Insights connection panel.
7. Click **Create Connector**.



Navigate to the **Configured Connectors** panel (**Menu > Connectors > Configured**) to confirm that connector creation was successful and review any connector settings.



# Connect Identity Security Insights to Microsoft Azure

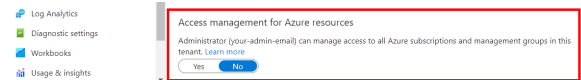
## Run the Microsoft Azure Connector Installation Script

1. Within the Insights **Tenant** dashboard, navigate to **Menu > Connectors > Available** and click **Create Connector** beside **Microsoft Azure**.



**Note:** To use the script provided by the Microsoft Azure connector, a credit card must be associated with your Azure instance.

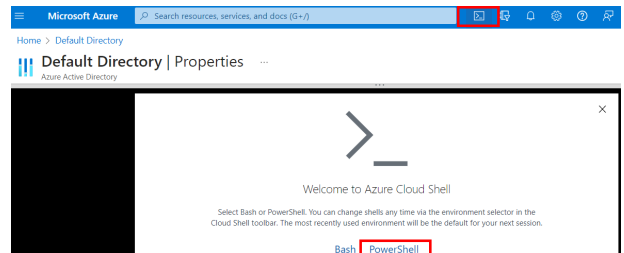
2. The Azure connector provides a script to retrieve the tenant ID, directory name, client ID, and client secret. To run the script:
  - Log in to Microsoft Azure as a user with Global Administrator privileges.
  - Within Microsoft Entra ID, navigate to **Properties**, and toggle **Access management for Azure resources** to **Yes**. This can be switched back after running the script.



3. The provided script can be run either locally, or within the Azure Cloud Shell from your Azure Dashboard. Select an option from the dropdown menu, and follow the instructions below for your chosen installation method.

### Install via Cloud Shell

1. From the Azure portal, launch **Cloud Shell**.
2. Select **PowerShell** from the shell environment dropdown.
3. Paste and run the resulting script into the shell environment. Once complete, the tenant ID, directory name, client ID, and client secret are displayed for use in the following step.



### Install via Local Shell

1. Ensure you have installed Azure PowerShell on Windows. For more information, see the [Azure PowerShell documentation](https://learn.microsoft.com/en-us/powershell/azure/install-azps-windows) at <https://learn.microsoft.com/en-us/powershell/azure/install-azps-windows>.
2. Once installed, open PowerShell and log in to Azure by running the command **Connect -AzAccount**. Enter your login credentials in the following window.
3. Ensure you are connected to the correct Azure tenant and directory, and run the following commands:
  - a. **Get-AzTenant** to see all the directories you have access to.
  - b. **Set-AzContext -Tenant "TenantID"**, where TenantID is the ID of the directory where the script will be installed.
  - c. **Get-AzContext** to verify your selection.
4. Run the resulting script to retrieve the Tenant ID, Directory Name, Client ID, and Client Secret. The Client Secret will only be shown temporarily.



**Note:** The Microsoft Azure connector can also be configured manually. To configure your connector without running the provided script, the tenant ID, directory name, client ID, and client secret must be provided from your Azure instance.

Log in to the Azure portal and retrieve the following:

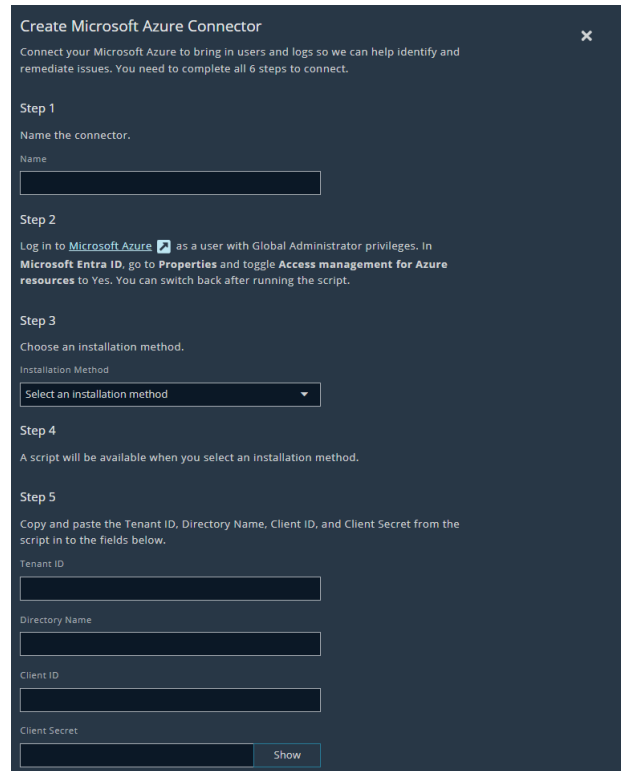


- **Tenant ID and Directory Name:** Navigate to **Microsoft Entra ID > Manage > Properties**.
- **Client ID and Client Secret:** Navigate to **Microsoft Entra ID > App Registrations**, and then select the application associated with Insights. Click **Certificates & secrets** to retrieve the client ID and create a new client secret.

## Create the Microsoft Azure Connector

1. In the Identity Security Insights **Connectors** dashboard, provide the following information to connect to Azure:
  - **Name:** A human-readable name for your Microsoft Azure connector.
  - **Tenant ID:** The tenant ID output by the Cloud Shell script.
  - **Directory ID:** The directory ID output by the Cloud Shell script.
  - **Client ID:** The client ID output by the Cloud Shell script.
  - **Client Secret:** The client secret output by the Cloud Shell script.
2. Click **Create Connector**.

Navigate to the **Configured Connectors** panel (**Menu > Connectors > Configured**) to confirm that connector creation was successful and review any connector settings.



**Create Microsoft Azure Connector**

Connect your Microsoft Azure to bring in users and logs so we can help identify and remediate issues. You need to complete all 6 steps to connect.

**Step 1**  
Name the connector.  
Name

**Step 2**  
Log in to [Microsoft Azure](#) as a user with Global Administrator privileges. In [Microsoft Entra ID](#), go to [Properties](#) and toggle [Access management for Azure resources](#) to Yes. You can switch back after running the script.

**Step 3**  
Choose an installation method.  
Installation Method  
Select an installation method

**Step 4**  
A script will be available when you select an installation method.

**Step 5**  
Copy and paste the Tenant ID, Directory Name, Client ID, and Client Secret from the script in to the fields below.

Tenant ID

Directory Name

Client ID

Client Secret

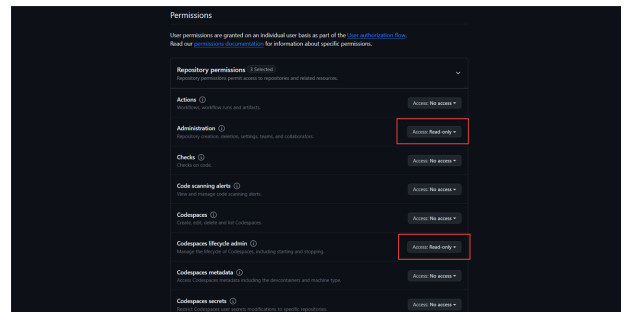
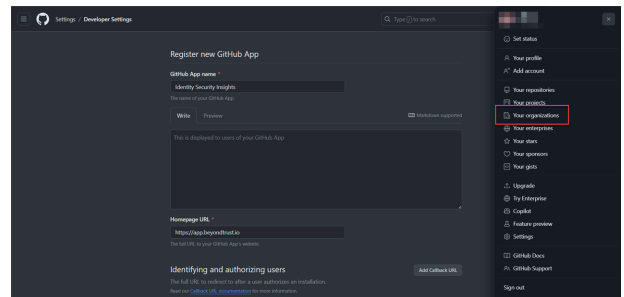
# Connect Identity Security Insights to GitHub

## Configure a New GitHub App



**Note:** A GitHub organization owner is required to install a new GitHub App.

1. Log in to GitHub as an organization owner.
2. In the upper-right corner, select your profile photo, and click **Your organizations**.
3. To the right of the organization where the Insights app will be installed, click **Settings**.
4. In the left sidebar, click **Developer settings**, and select **GitHub Apps**.
5. Click **New GitHub App**.
6. Provide the following information to create your new app:
  - **GitHub App name:** A unique name for your new application.
  - **Homepage URL:** `https://app.beyondtrust.io`
7. Under **Webhook**, uncheck **Active**.
8. Under **Repository permissions**, set the following resources to **Read only**:
  - Administration
  - Codespaces lifecycle admin
  - Metadata
  - Webhooks
9. Under **Organization permissions**, set the following resources to **Read only**:
  - Administration
  - Blocking users
  - Custom organization roles
  - Custom repository roles
  - Events
  - Members
  - Webhooks
10. Under **Where can this GitHub App be installed?**, select **Only on this account**.
11. Click **Create GitHub App**.
  - GitHub generates a new **App ID**. Save this for use when creating your Insights GitHub connector.
12. Under **Private Keys**, click **Generate a private key**.
  - A PEM file downloads to your local system. Save the contents of this file for use when creating your Insights GitHub connector.



13. In the left-hand menu, navigate to the **Settings** page, and click **Install App**.
14. Click **Install**. Review your settings and permissions, then click **Install** again.
15. Copy the **URL string** from your web browser's address bar. Save this for use when creating your Insights GitHub connector.

## Add a GitHub Connector

1. Within the Insights **Tenant** dashboard, navigate to **Menu > Connectors > Available** and click **Create Connector** beside **GitHub**.
2. In the connection panel, enter a human-readable name for your GitHub connector.
3. Provide the following information from your GitHub app:
  - **App ID:** The app ID generated in step 11.
  - **PEM Key:** The contents of the PEM file downloaded in step 12.
  - **Installed GitHub App URL:** The URL string saved in step 15.
4. Click **Create Connector**.

Navigate to the **Configured Connectors** panel (**Menu > Connectors > Configured**) to confirm that connector creation was successful and review any connector settings.



**Create Github Connector** ✕

Connect your GitHub Organization to bring in event logs and users so we can identify and help remediate issues. You need to complete all 5 steps to connect.

**Before You Start**

An Organization owner is required to install the GitHub App.

**Step 1**

Install and configure the GitHub App using the [setup guide](#).

**Step 2**

Name the connector.

Name

**Step 3**

Provide the GitHub App ID.

App ID

**Step 4**

Copy the full private key for the GitHub app. Paste below.

PEM Key

**Step 5**

Enter the GitHub URL below that contains your organization name and app installation ID.

Installed GitHub App URL

Example: <https://github.com/organizations/Sample-Org-Name/settings/installations/123456789>

**Create Connector** **Discard**

# Connect Identity Security Insights to Google Cloud Platform

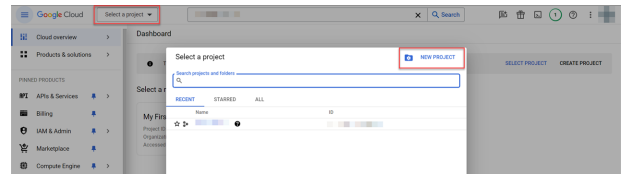
Identity Security Insights requires a service account to access information in your Google Cloud Platform organization. A service account can be created manually, via the Google Cloud Console, or via a script for Google Cloud Shell provided by Identity Security Insights.

## Manually Configure a Google Cloud Platform Connector

### Configure Google Cloud Platform

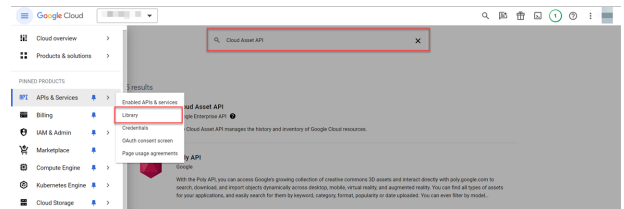
#### Create a New Project

1. Within the Google Cloud Console, click the project selector in the top navigation bar, and select your organization.
2. In the project window, click **New Project**.
3. Enter a human-readable name for your project.
4. Click **Create**.



#### Enable Required Services

1. From your new project's navigation menu, go to **APIs & Services > Library**.
2. Search for and enable the following APIs:
  - **Cloud Asset API**
  - **Cloud Logging API**
  - **Cloud Resource Manager API**



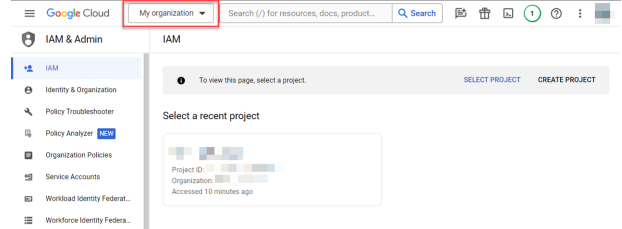
**Note:** Ensure all projects within your organization have the same APIs enabled.

#### Create a Service Account

1. From the navigation menu, go to **IAM & Admin > Service Accounts**.
2. Click **Create Service Account**.
  - Enter a human-readable display name for your new service account.
  - Enter a unique service account ID.
3. The Google Cloud console will generate an email address for this service account. This email address will be required in the next step.
4. When finished, click **Done**.

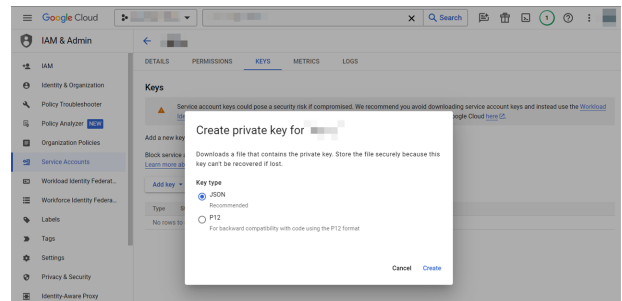
## Assign Service Account Roles

1. In the top navigation toolbar, click the project selector, and select your organization.
2. Navigate to **IAM & Admin > IAM**, and click **Grant Access**.
3. In the **New principals** field, enter the service account email generated by Google Cloud.
4. Under **Assign roles**, select the following roles:
  - Cloud Asset Viewer
  - Security Reviewer
5. When finished, click **Save**.



## Generate a Key for the Service Account

1. In the top navigation toolbar, click the project selector, and select your new project.
2. From the navigation menu, go to **IAM & Admin > Service Accounts**, and select the created service account.
3. Click the **Keys** tab.
4. Click **Add Key > Create new key**.
  - Select **JSON** as the key type.
  - Click **Create**.
5. A new key will be automatically downloaded to your local system. *Ensure you keep the downloaded JSON key in a secure location.*



## Create the Google Cloud Platform Connector

1. Within the Insights **Tenant** dashboard, navigate to **Menu > Connectors > Available** and click **Create Connector** beside **Google Cloud Platform**.
2. In the connection panel, enter a human-readable name for your GCP Connector.
3. Select **Manual Configuration** from the installation method drop-down menu.
4. Provide the following information about your service account:
  - **Organization ID:** Your organization ID can be found in the Google Cloud Console by selecting your organization from the drop-down menu, and navigating to **IAM & Admin > Settings**.
  - **Service Account Key:** The JSON key created for your service account.
5. Click **Create Connector**.

Navigate to the **Configured Connectors** panel (**Menu > Connectors > Configured**) to confirm that connector creation was successful and review any connector settings.

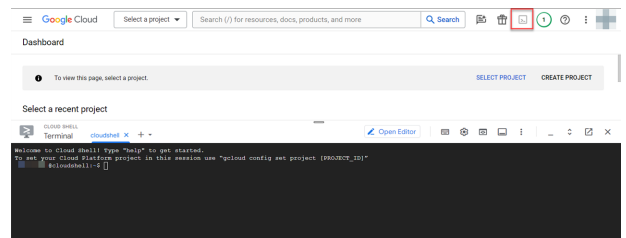
## Create a GCP Connector with Google Cloud Shell

### Create the Google Cloud Platform Connector

1. Within the Insights **Tenant** dashboard, navigate to **Menu > Connectors > Available** and click **Create Connector** beside **Google Cloud Platform**.
2. In the connection panel, enter a human-readable name for your GCP Connector.
3. Select **Google Cloud Shell** from the installation method drop-down menu.

### Configure Google Cloud Platform

1. In a new window, sign into Google Cloud Platform Console.
2. Click **Activate Cloud Shell** in the upper-right navigation menu to open the command line interface.



**Note:** If you are prompted to authorize an action after running a command, authorize it. The command may need to be re-run after authorization.

### Retrieve the Organization ID

1. Run the following command to retrieve your organization ID:

```
gcloud organizations list
```

2. Paste your organization ID in the **Organization ID** field in Identity Security Insights.

### Create a New Project

1. Run the following command to create a new project, replacing **<Project\_ID>** with a unique ID of your choosing:

```
gcloud projects create <Project_ID>
```

### Set the Current Project

1. Run the following command to set your current project, replacing **<Project\_ID>** with the ID you created:

```
gcloud config set project <Project_ID>
```

## Enable Required Services

1. Run the following command to enable necessary Google Cloud services:

```
project_ids=$(gcloud projects list --format json | jq -r '[][.projectId]')
for project_id in $project_ids; do
  gcloud services enable cloudresourcemanager.googleapis.com --project "$project_id"
  gcloud services enable cloudasset.googleapis.com --project "$project_id"
  gcloud services enable logging.googleapis.com --project "$project_id"
done
```

This command enables the following APIs for all projects:

- Cloud Asset API
- Cloud Logging API
- Cloud Resource Manager API

## Create a Service Account

1. Run the following command to create a new service account, replacing `<Service_account_ID>` with a unique ID:

```
gcloud iam service-accounts create <Service_account_ID>
```

## Assign Service Account Roles

1. Run the following command to assign necessary roles to your new service account, replacing `<Organizations_ID>`, `<Service_account_ID>`, and `<Project_ID>` with the values set in earlier steps:

```
gcloud organizations add-iam-policy-binding <Organizations_ID> --role
'roles/iam.securityReviewer' --member serviceAccount:<Service_account_ID>@<Project_
ID>.iam.gserviceaccount.com
gcloud organizations add-iam-policy-binding <Organizations ID> --role 'roles/cloudasset.viewer' -
-member serviceAccount:<Service_account_ID>@<Project_ID>.iam.gserviceaccount.com
```

## Generate a Key for the Service Account

1. Run the following command to generate a new key, replacing `<Service_account_ID>` and `<Project_ID>` with the values set in earlier steps:

```
gcloud organizations add-iam-policy-binding <Organizations_ID> --role
'roles/iam.securityReviewer' --member serviceAccount:<Service_account_ID>@<Project_
ID>.iam.gserviceaccount.com
gcloud organizations add-iam-policy-binding <Organizations ID> --role 'roles/cloudasset.viewer' -
-member serviceAccount:<Service_account_ID>@<Project_ID>.iam.gserviceaccount.com
```

2. Copy the full JSON output, and paste it in **Service Account Key** field in Identity Security Insights.



When finished, click **Create Connector**.

Navigate to the **Configured Connectors** panel (**Menu > Connectors > Configured**) to confirm that connector creation was successful and review any connector settings.

# Connect Identity Security Insights to Microsoft Active Directory

## Prerequisites

The Microsoft Active Directory connector must be installed and configured on a member server in your Active Directory. The installer is provided for your tenant after you have completed the initial configuration.

Ensure the following requirements are met prior to installation:

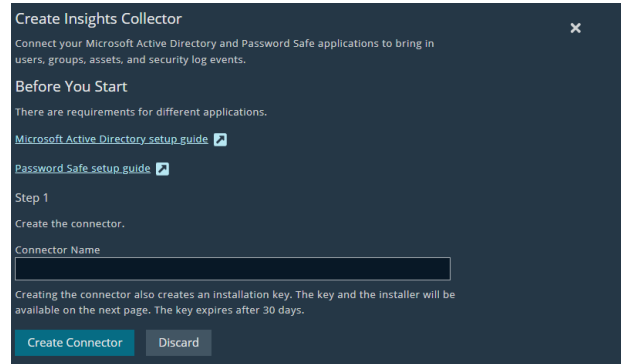
- **Member Server:** The installer must be run on a Windows Server joined to the domain you would like Identity Security Insights to access.
- **Service Account:** A provisioned on-premises service account for the Active Directory connector to use. This service account requires the following permissions:
  - Domain User Group
  - Event Log Reader Group
  - Read access to the 'Deleted Objects' OU
- **Connectivity:** The member server must be able to:
  - Connect to Active Directory using SSL and TCP 636.
    - If SSL/636 are not available, the installer can optionally be configured to use TCP 389.
  - Connect outbound to Identity Security Insights via the following URLs:
    - Authentication: *https://login.beyondtrust.io*
    - Events: *https://ingest.beyondtrust.io*
- The following firewall rules on the Domain Controller should allow for communication from the member server to facilitate event log collection:
  - COM+ Network Access (DCOM-In)
  - Remote Event Log Management (NP-In)
  - Remote Event Log Management (RPC)
  - Remote Event Log Management (RPC-EPMAP)
  - Windows Management Instrumentation (ASync-In)
  - Windows Management Instrumentation (DCOM-In)
  - Windows Management Instrumentation (WMI-In)

## Create the Microsoft Active Directory Connector

1. Within the Insights **Tenant** dashboard, navigate to **Menu > Connectors > Available** and click **Create Connector** beside **Insights Collector**.

2. In the **Connection** panel, enter a human-readable name for your Microsoft AD connector, and click **Create Connector** to continue.
3. **Download and run the installer** provided on the following page.
4. Enter the installation key generated by Insights when prompted by the installer. *Do not close the connector before you have entered these credentials.*
5. Once your credentials have been provided to the installer, click **Close Key**.

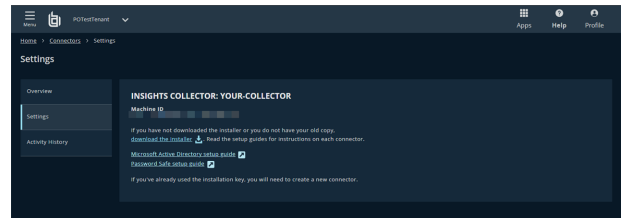
Navigate to the **Configured Connectors** panel (**Menu > Connectors > Configured**) to confirm that connector creation was successful and review any connector settings.



## Update or Reinstall the Active Directory Connector

The Identity Security Insights Active Directory connector updates automatically when a new version becomes available, without any need for manual installation.

To redownload the Active Directory installer, navigate to **Menu > Connectors > Configured**, and click on the ellipsis to the right of your Active Directory connector. Click **View Connector**, and navigate to **Settings**.



The Active Directory settings page allows you to download the installer created during your initial connector setup. If you've already used the installation key provided during setup, you will need to create a new connector.

## Information Collection

To report to the Identity Security Insights console, the installed Microsoft Active Directory connector collects a variety of information as part of its operation.



**Note:** *The Microsoft Active Directory connector collects information from Active Directory, and sends this information Insights for analysis. Some security solutions may detect this as an attack pattern after the connector is installed.*

Security alerts you may see include:

- *Suspicious LDAP search*
- *A service account is authenticating over Kerberos*
- *A device is sending data externally*

From the domain controller event log, which is polled every 10 minutes, Insights collects or accesses the following:

- The Windows event log (read by the connected domain controller)
- EventIDs from the security log: 4768, 4771, 4770, 4776, 4777
- The last collection date for each pull (to collect new events)

From the AD inventory, which is polled every 30 minutes, Insights collects or accesses the following:

- Active Directory object metadata
- Important Access Control Lists (ACLs)
- Objects:
  - user
  - groups
  - computer
  - containers
  - organizational units (OUs)
  - domain
  - group policy objects (GPOs)
  - Active Directory Certificate Services

From the Active Directory Certificate Services, which is polled every 60 minutes, Insights collects the following:

- LDAP object properties for certificate authority, certificate templates, and enrollment services from the configuration container
- Security events from the enrollment service machines: 4886, 4887, 5145
  - Events 4886 and 4887 are only logged if "Issue and manage certificate requests" is enabled on the Audit tab of the CA's properties in Certificate Services MMC snap-in
- The agent security Access Control Lists (ACLs) from the enrollment service machines via the registry
- The enrollment agent restrictions from the enrollment service machines via the registry

# Connect Identity Security Insights to Okta

## Create an Okta App Integration



**Note:** Ensure you are logged in to your Okta account as an administrator.

### Create a New App Integration

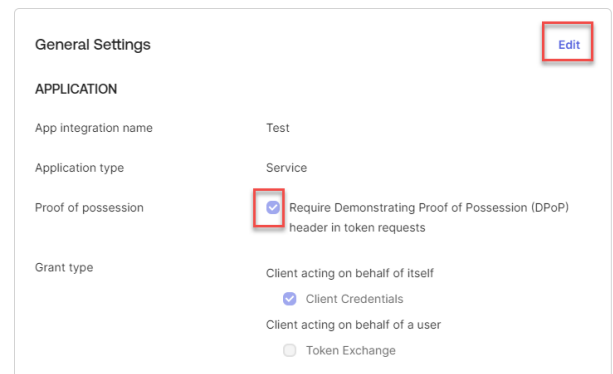
1. Within the Okta console, navigate to **Applications**, and click **Create App Integration**.
2. Click **API Services**, enter the name *BT Insights - Connector*, and click **Save**.
  - Okta provides a **Client ID** under **Client Credentials**. Save your Client ID for use in Insights.
3. Navigate to **Client Credentials** and click **Edit**.
4. Select **Public key / Private key** next to **Client authentication**.
5. Select **Add key**, then **Generate new key**.
6. Select **PEM** under **Private key**.



**Note:** Only one key can be active at a time.

7. Click **Copy to clipboard**, save your key for use in the next step, and click **Done** when finished.
8. Navigate to **Okta API Scopes**, and grant access to the following:
  - **okta.apiTokens.read**
  - **okta.apps.read**
  - **okta.groups.read**
  - **okta.idps.read**
  - **okta.logs.read**
  - **okta.policies.read**
  - **okta.roles.read**
  - **okta.users.read**

9. Navigate to **General Settings** and click **Edit**.
10. Uncheck **Require Demonstration of Proof-of-Possession (DPoP) header in token requests**.
11. When finished, click **Save**.



General Settings		Edit
<b>APPLICATION</b>		
App integration name	Test	
Application type	Service	
Proof of possession	<input checked="" type="checkbox"/> Require Demonstrating Proof of Possession (DPoP) header in token requests	
Grant type	<input type="checkbox"/> Client acting on behalf of itself <input checked="" type="checkbox"/> Client Credentials <input type="checkbox"/> Client acting on behalf of a user <input type="checkbox"/> Token Exchange	

### Create a New Role and Resource Set

1. Within the Okta console, navigate to **Security**, and select **Administrators**.
2. Select **Roles > Create new role**, and provide the role a name of *Identity Security Insights*.

3. Under Identity and Access Management, select the following options:
  - **View roles, resources, and admin assignments**
4. Click **Save role**.
5. Navigate to **Resources**, and select **Create new resource set**.
6. Provide the resource set a name of *Identity Security Insights*.
7. Click **Add resource set**.
8. In the search field, choose **Identity and Access Management**, and select the following:
  - **All Identity and Access Management resources**
9. Click **Save resource set**.

## Add the Administrator Role to Insights

1. Navigate to **Applications**, and select your new *BT Insights - Connector* app.
2. Go to **Admin Roles > Edit Assignments**.
3. Select the new Identity Security Insights role and Identity Security Insights Resource set.
4. Click **Add assignment**.
5. Select the **Read-only Administrator** role.
6. Click **Save changes**.

## Add an Okta Connector

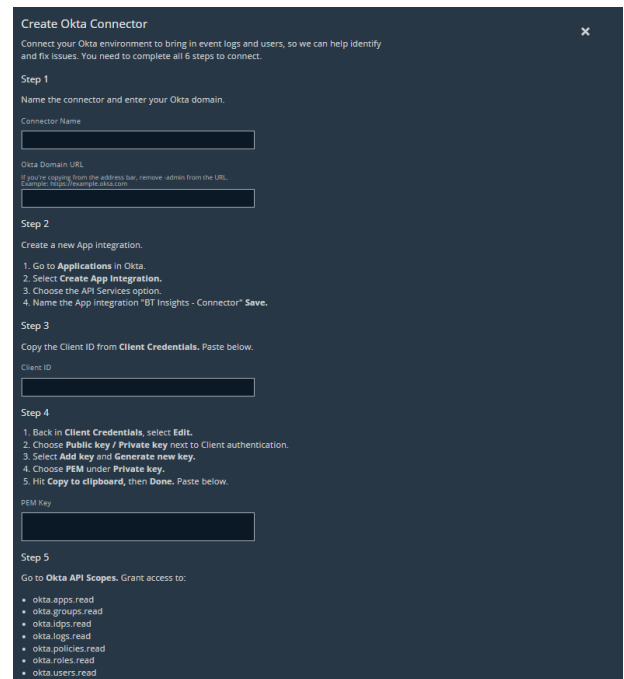
1. Within the Insights **Tenant** dashboard, navigate to **Menu > Connectors > Available** and click **Create Connector** beside **Okta**.
2. Provide the following information to connect to Okta:

- **Configuration Name:** A human-readable name for your Okta connector.
- **Domain:** Your full Okta domain, e.g., *subdomain.okta.com*.  
If copying your domain from the address bar, remove the - admin ending (e.g., *subdomain-admin.okta.com*).

- **Client ID:** Paste the Client ID provided in your Okta configuration above.
- **PEM Key:** Paste the PEM key generated in your Okta configuration above.

3. Click **CREATE CONNECTOR**.

Navigate to the **Configured Connectors** panel (**Menu > Connectors > Configured**) to confirm that connector creation was successful and review any connector settings.



**Create Okta Connector**

Connect your Okta environment to bring in event logs and users, so we can help identify and fix issues. You need to complete all 6 steps to connect.

**Step 1**

Name the connector and enter your Okta domain.

Connector Name

Okta Domain URL  
If you're copying from the address bar, remove -admin from the URL. Example: https://example.okta.com

**Step 2**

Create a new App Integration.

1. Go to **Applications** in Okta.
2. Select **Create App Integration**.
3. Choose the **API Services** option.
4. Name the App integration "BT Insights - Connector". **Save**.

**Step 3**

Copy the Client ID from **Client Credentials**. Paste below.

Client ID

**Step 4**

1. Back in **Client Credentials**, select **Edit**.
2. Choose **Public key / Private key** next to Client authentication.
3. Select **Add key and Generate new key**.
4. Choose **PEM** under Private key.
5. Hit **Copy to clipboard**, then **Done**. Paste below.

PEM Key

**Step 5**

Go to **Okta API Scopes**. Grant access to:

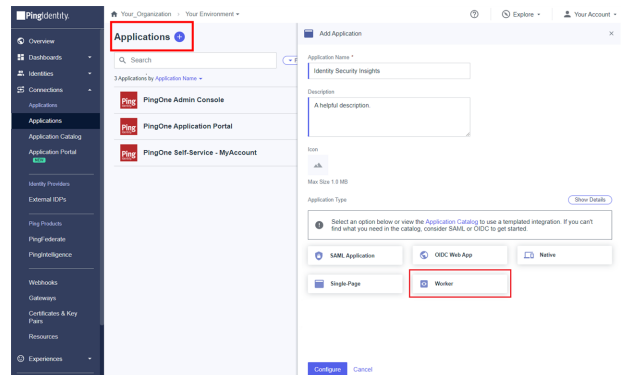
- okta:apps:read
- okta:groups:read
- okta:idps:read
- okta:logs:read
- okta:policies:read
- okta:roles:read
- okta:users:read


# Connect Identity Security Insights to PingOne

## Create a PingOne Application

Ensure you are logged into PingOne as a user with administration privileges.

1. Within your PingOne dashboard, navigate to **Connections > Applications**.
2. Click the **Add Application** button, and:
  - Provide a human-readable name for the new application.
  - Select **Worker** for the application type
  - Click **Configure** to create your application.
3. In your new application, navigate to **Roles** and click **Grant Roles**.
  - Select **Remove All**.
  - Click **Save**.
4. Click **Grant Roles**, and use the search field to find **Read Only**.
  - Select **Select All**.
  - Click **Save**.



 **Note:** Verify *Read Only* roles are the only roles granted to the application.

5. Toggle the Application to **On**.
6. Navigate to **Configuration** for this application and expand **General**.
7. The **Client ID**, **Client Secret**, and **Environment ID** are required in the next section.

## Add a PingOne Connector

1. Within the Insights **Tenant** dashboard, navigate to **Menu > Connectors > Available** and click **Create Connector** beside **PingOne**.

2. Provide the following information to connect to PingOne:
  - **Name:** A human-readable name for your Ping connector.
  - **Client ID:** Paste the **Client ID** provided in **Step 7** of your Ping configuration above.
  - **Client Secret:** Paste the **Client Secret** provided in **Step 7** of your Ping configuration above.
  - **Environment ID:** Paste the **Environment ID** provided in **Step 7** of your Ping configuration above.
3. Click **CREATE CONNECTOR**.

Navigate to the **Configured Connectors** panel (**Menu > Connectors > Configured**) to confirm that connector creation was successful and review any connector settings.

### Create PingOne Connector

Connect your Ping Identity environment to bring in event logs and users so we can identify and help remediate issues. You need to complete all 2 steps to connect.

**Step 1**  
Name the connector.

Name

**Step 2**  
Log in to [Ping Identity](#) as a user with Administrator privileges.


1. Go to **Connections > Applications** and select the **Add Application** button. Provide a name for the Application, select **Worker** for Application type and select **Save**.
2. Navigate to the **Roles** and click **Grant Roles**. Next, select **Remove All** and **Save**.
3. Now that all permissions have been removed, select **Grant Roles**. Use the search field and enter **Read Only**. Select **Select All** and **Save**. Verify Read Only roles are the only ones listed.
4. Toggle the Application to **On**.
5. Navigate to **Configuration** for this Application and expand **General**. Copy the **Client ID**, **Client Secret**, and **Environment ID** into the corresponding fields below.

Client ID

Client Secret

Environment ID

**Create Connector** **Discard**





# Connect Identity Security Insights to BeyondTrust Endpoint Privilege Management Cloud

## Create a Endpoint Privilege Management Cloud API Account

1. Within your Endpoint Privilege Management administration dashboard, navigate to **Configuration > API Settings** and click **Create an API Account**.
2. When prompted, enter a human-readable name and description for referencing your token.
3. Privilege Management Cloud generates a new **Client ID** and **Client Secret**. *Copy your Client ID and Client Secret prior to exiting this page.*

### CREATE AN API ACCOUNT

Name <sup>?</sup>

Description <sup>?</sup>

Client ID <sup>?</sup>

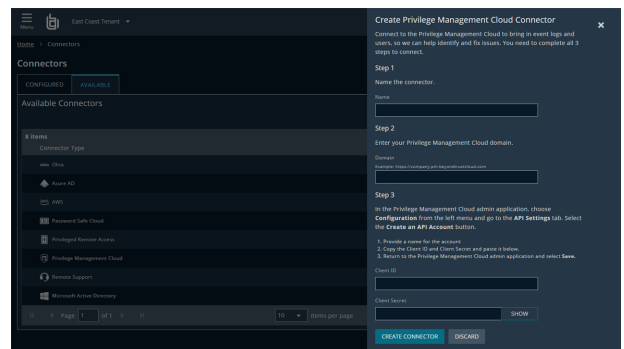
Client Secret <sup>?</sup>

You are responsible for storing the Client Secret in a secure location. This is the only time you will be able to view the Client Secret in plain text.

[SAVE API ACCOUNT](#) [CANCEL](#)

## Add an Endpoint Privilege Management Cloud Connector

1. Within the Insights **Tenant** dashboard, navigate to **Menu > Connectors > Available** and click **Create Connector** beside **Privilege Management Cloud**.
2. Provide the following information to connect to PM Cloud:
  - **Name:** A human-readable name for your PM Cloud connector.
  - **Domain:** Your full PM Cloud domain, e.g., *https://company.pm.beyondtrustcloud.com*.
  - **Client ID:** Paste the **Client ID** provided in **Step 3** of your PM Cloud configuration above.
  - **Client Secret:** Paste the **Client Secret** provided in **Step 3** of your PM Cloud configuration above.
3. Click **CREATE CONNECTOR**.

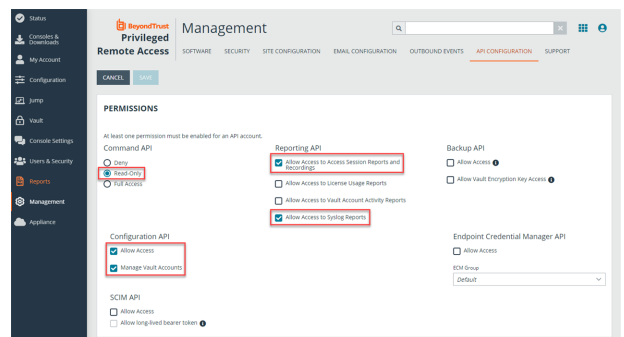


Navigate to the **Configured Connectors** panel (**Menu > Connectors > Configured**) to confirm that connector creation was successful and review any connector settings.

# Connect Identity Security Insights to BeyondTrust Privileged Remote Access Cloud

## Create a Privileged Remote Access API Account

1. Within your Privileged Remote Access administration dashboard, navigate to **Management** and click **API Configuration**.
2. Under **API CONFIGURATION**, ensure **Enable XML API** is checked.
3. Click **Add** beside **API Accounts** and configure the following:
  - Provide a human-readable name, and any descriptive comments for referencing your account.
  - Under **Permissions**, ensure the following options are selected:
    - **Command API:** Read only
    - **Configuration API:** Allow Access, Manage Vault Accounts
    - **Reporting API:** Allow Access to Access Session Reports and Recordings, Allow Access to Syslog Reports
4. Privileged Remote Access generates a new client ID and client secret. *Copy your client ID and client secret prior to saving your information and exiting this page.*
5. Click **Save**.



## Add a Privileged Remote Access Connector

1. Within the Insights **Tenant** dashboard, navigate to **Menu > Connectors > Available** and click **Create Connector** beside **Privileged Remote Access Cloud**.

2. Provide the following information to connect to PRA:
  - **Name:** A human-readable name for your PRA connector.
  - **Subdomain:** Your PRA subdomain, e.g., *subdomain.beyondtrustcloud.com*.
  - **Client ID:** Paste the **Client ID** provided in **Step 3** of your PRA configuration above.
  - **Client Secret:** Paste the **Client Secret** provided in **Step 3** of your PRA configuration above.
3. Click **CREATE CONNECTOR**.

Navigate to the **Configured Connectors** panel (**Menu > Connectors > Configured**) to confirm that connector creation was successful and review any connector settings.

### Create Privileged Remote Access Connector ✕

Connect your Privileged Remote Access environment to bring in event logs and users, so we can help identify and fix issues. You need to complete all 3 steps to connect.

**Step 1**

Name the connector.

Name

**Step 2**

Enter your Privileged Remote Access domain.

Domain

Example: <https://company.beyondtrustcloud.com>

**Step 3**

Provide your Client ID and Client Secret and set the required permissions.

In the Privileged Remote Access admin application, choose **Management** from the lefthand menu and then go to the **API Configuration** tab.

1. Under the **API Configuration** section, make sure **Enable XML API** is selected.
2. Under the **API Accounts** section, select the **Add** button.
  - 2.1. Under **Permissions**, choose the following options for each API:
    - **Command:** Read Only
    - **Reporting:** Allow Access to Access Session Reports and Recordings, Allow Access to Syslog Reports
    - **Configuration API:** Allow Access and Manage Vault Accounts
  - 2.2. Under **Network Restrictions** enter the following IP addresses:
    - 50.16.236.14
    - 54.163.153.193
    - 54.225.135.48
  - 2.3. Copy the **Client ID** and **Client Secret** and paste it below.
  - 2.4. Return to the Privileged Remote Access admin application and select **Save**.

# Connect Identity Security Insights to BeyondTrust Password Safe

## Configure Password Safe

Identity Security Insights is capable of connecting to both cloud and on-premises instances of Password Safe. To access account and identity information for either application, Identity Security Insights first requires a group and user in Password Safe, provisioned with appropriate roles.

### Create a New API Registration

1. In the BeyondInsight console, navigate to **Configuration > General > API Registrations**.
2. Click **Create API Registration**.
3. Select **API Key Policy** from the dropdown.
4. From the registration's **Details** pane:

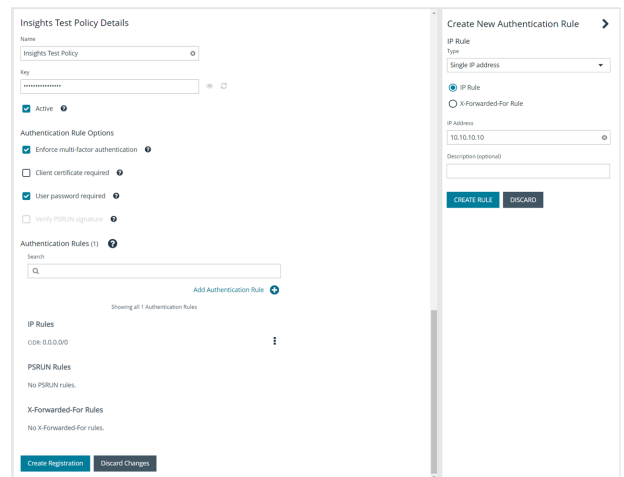
- Enter a name for the new registration.
- Select the your desired rule options and optionally, check the the **User password required** box to add a password for the connector.

5. Add three Authentication Rules, one for each IP address required for Insights:

- Under **Authentication Rules**, click **Add Authentication Rule**.
- From the **Type** dropdown menu, select **Single IP Address**.

- For instances of **Password Safe Cloud**, the following IP addresses must be added:
  - **50.16.236.14**
  - **54.163.153.193**
  - **54.225.135.48**
- For **on-premise** instances of Password Safe, authorize the IP address of the server where the Insights Connector will be installed.
- Click **Create Rule**, and repeat this process for any remaining IP addresses.

6. In the registration page, ensure the **Active** box is checked.
7. Click **Create Registration**.



### Create a New User



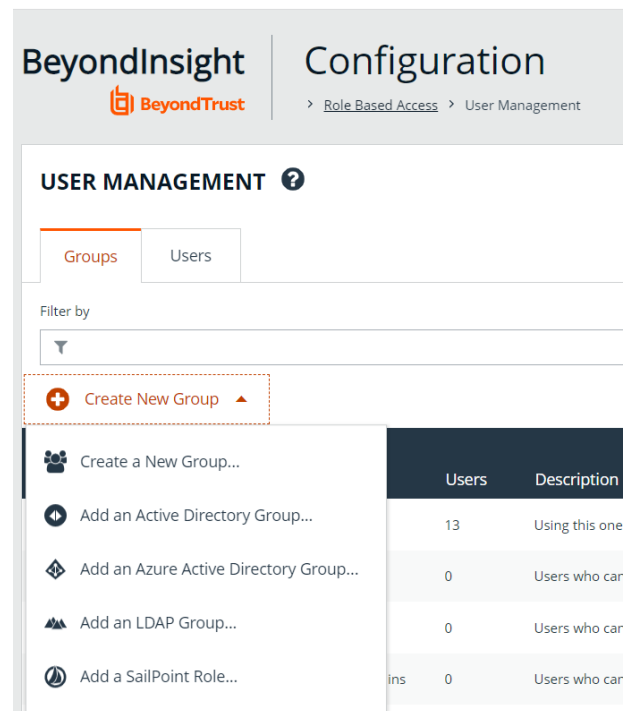
**Note:** This user allows Identity Security Insights to access Password Safe. We recommend creating a new user for this purpose. To use an existing account, please see "[Create and Configure a New Group](#)" on page 29.

1. Navigate to **Configuration > Role Based Access > User Management**.
2. Click **Users**, and then click **Create New User** above the grid.

3. Select **Create a New User** and provide the following information:
  - Complete the **Identification** section. These fields are required.
  - Optionally, enter the user's contact information.
  - Select an **Activation Date** and an **Expiration Date** for the user account.
  - Check **User Active** to activate the user account.
  - Set **Two-Factor Authentication** to **None**.
4. Click **Create User**.

## Create and Configure a New Group

1. Navigate to **Configuration > Role Based Access > User Management**.
2. From the **Groups** tab, click **Create New Group** above the grid.
3. Select **Create a New Group** and enter a name and description.
  - a. Click **Create Group** to save your information.
4. Assign the user created for Identity Security Insights to the group:
  - Under **Group Details**, select **Users**.
  - From the **Show** dropdown list, select **Users not assigned**. This displays a list of all users not currently assigned to a group.
  - Filter the list of users displayed in the grid by **Type**, **Username**, **Name**, **Email**, or **Domain** to assist in finding the new Insights user.
  - Select the user you wish to add to the group, and then click **Assign User** above the grid.
5. Configure API access for the group:
  - Under **Group Details**, select **API Registrations**.
  - Check the box next to the API registration created for Identity Security Insights.
6. Assign features permissions to the group:
  - Under **Group Details**, select **Features**.
  - From the **Show** dropdown menu, select **All Features**.
  - Select the following features:
    - **Analytics and Reporting**
    - **Asset Management**
    - **Password Safe Account Management**
    - **Password Safe Role Management**
    - **Password Safe System Management**
    - **Ticket System**
    - **User Accounts Management**



- Click **Assign Permissions** above the grid and select **Assign Permissions Read Only**.
  - Click **User Audits**, and select **Assign Permissions Full Control**.
7. Assign Smart Groups permissions and roles to the group:
- Under **Group Details**, select **Smart Groups**.
  - From the **Show** dropdown menu, select **All Smart Groups**.
  - Select the **All Assets** Smart Group.
  - Click **Assign Permissions** above the grid, and select **Assign Permissions Read Only**.
  - Click the vertical ellipsis button for the **All Assets** Smart Group.
  - Select **Edit Password Safe Roles**.
  - Check the **Auditor** box.
  - Click **Save Roles**.

## Add a Password Safe Cloud Connector

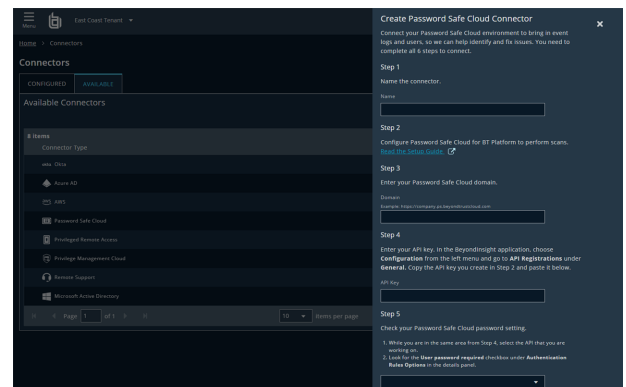


**Note:** The following steps are for Password Safe Cloud applications. Instructions for on-premises applications are provided at the end of this guide.

1. Within the Insights **Tenant** dashboard, navigate to **Menu > Connectors > Available** and click **Create Connector** beside **Password Safe Cloud**.
2. Provide the following information to connect to Password Safe Cloud:

- **Name:** A human-readable name for your Password Safe Cloud connector.
- **Domain:** Your Password Safe Cloud domain, e.g., `https://company.ps.beyondtrustcloud.com`.
- **API Key:** The API Key generated from **Create New API Registration**.
- **Username:** Provide the username added to the Password Safe group made for Identity Security Insights.
- **Password:** A password is required if the **User Password required** box is checked in your API Registration.

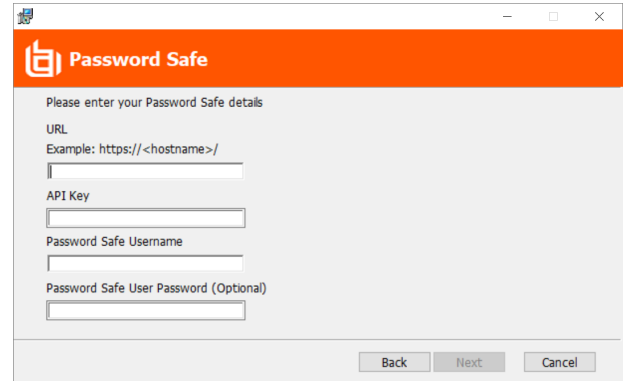
3. Click **CREATE CONNECTOR**.



Navigate to the **Configured Connectors** panel (**Menu > Connectors > Configured**) to confirm that connector creation was successful and review any connector settings.

## Add a Password Safe On-Premise Connector

1. Within the Insights **Tenant** dashboard, navigate to **Menu > Connectors > Available** and click **Create Connector** beside **Insights Collector**.
2. In the **Connection** panel, enter a human-readable name for your new connector, and click **Create Connector** to continue.
3. **Download and run the installer** provided on the following page. Ensure the collector is installed on any server on which the Password Safe application is located.
4. Enter the installation key generated by Insights when prompted by the installer. *Do not close the connector before you have entered these credentials.*
5. Provide the following information when required:
  - **URL:** Your Password Safe URL, e.g., *https://<hostname>/*.
  - **API Key:** The API Key generated from **Create New API Registration**.
  - **Username:** Provide the username added to the Password Safe group made for Identity Security Insights.
  - **Password:** A password is required if the **User Password required** box is checked in your API Registration.
6. Once your credentials have been provided to the installer, click **Close Key**.

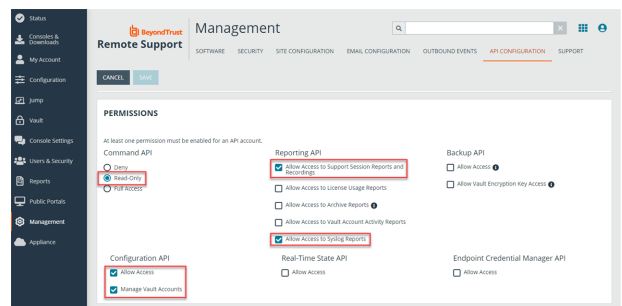


Navigate to the **Configured Connectors** panel (**Menu > Connectors > Configured**) to confirm that connector creation was successful and review any connector settings.

# Connect Identity Security Insights to BeyondTrust Remote Support Cloud

## Create a Remote Support API Account

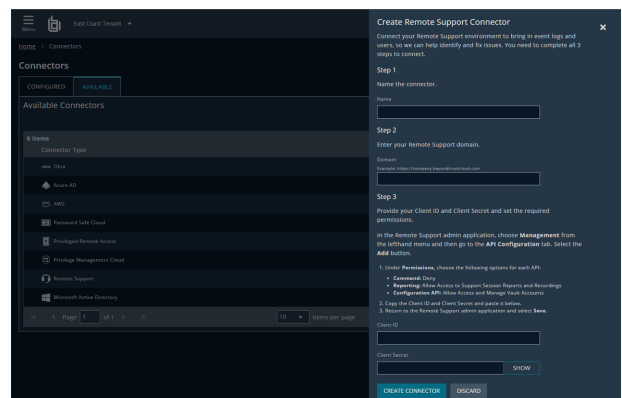
1. Within your Remote Support administration dashboard, navigate to **Management** and click **API Configuration**.
2. Under **API CONFIGURATION**, ensure **Enable XML API** is checked.
3. Click **Add** beside **API Accounts** and configure the following:
  - Provide a human-readable name and any descriptive comments for referencing your account.
  - Under **Permissions**, ensure the following options are selected:
    - **Command API:** Read only
    - **Configuration API:** Allow Access, Manage Vault Accounts
    - **Reporting API:** Allow Access to Access Session Reports and Recordings, Allow Access to Syslog Reports



4. Remote Support will generate a new client ID and client secret. *Copy the client ID and client secret prior to saving the information and exiting this page.*
5. Click **Save**.

## Add a Remote Support Cloud Connector

1. Within the Insights **Tenant** dashboard, navigate to **Menu > Connectors > Available** and click **Create Connector** beside **Remote Support Cloud**.
2. Provide the following information to connect to Remote Support:
  - **Name:** A human-readable name for your Remote Support connector.
  - **Remote Support Domain:** Your Remote Support domain, e.g., *subdomain.beyondtrustcloud.com*.
  - **Client ID:** Paste the **Client ID** provided in **Step 3** of your Remote Support configuration, above.
  - **Client Secret:** Paste the **Client Secret** provided in **Step 3** of your Remote Support configuration, above.



3. Click **CREATE CONNECTOR**.

Navigate to the **Configured Connectors** panel (**Menu > Connectors > Configured**) to confirm that connector creation was successful and review any connector settings.