



# BeyondTrust

## **BeyondInsight and Password Safe 23.3 Authentication Guide**

# Table of Contents

---

<b>BeyondInsight and Password Safe Authentication Guide</b> .....	<b>5</b>
<b>Create and Configure Groups in BeyondInsight</b> .....	<b>6</b>
Create a BeyondInsight Local Group .....	7
<b>Create and Edit Directory Credentials</b> .....	<b>9</b>
Create an Active Directory Credential .....	10
Create an LDAP Credential .....	11
Create an Entra ID Credential .....	12
Edit a Directory Credential .....	12
Register and Configure an Application in Azure Active Directory .....	13
Create a Registered Application in Azure AD .....	14
<b>Map Directory Credentials to a Domain</b> .....	<b>17</b>
<b>Add an Active Directory Group</b> .....	<b>18</b>
Propagate Domain Changes to Group Members .....	21
<b>Add an Azure Active Directory Group</b> .....	<b>22</b>
<b>Add an LDAP Group</b> .....	<b>25</b>
<b>Assign Permissions to Groups in BeyondInsight</b> .....	<b>29</b>
Assign Features Permissions .....	30
Assign Smart Groups Permissions .....	34
<b>Configure RADIUS Two-Factor Authentication for BeyondInsight and Password Safe</b> ..	<b>35</b>
Configure the RADIUS Server .....	35
Configure RADIUS Two-Factor Authentication Using Duo .....	36
Configure Alternate Directory Attribute for RADIUS .....	37
Apply RADIUS Two-Factor Authentication to User Accounts .....	38
Using Multiple RADIUS Servers .....	40
<b>Configure SecureAuth with Password Safe using RADIUS</b> .....	<b>41</b>
Test the Configuration .....	41
<b>Configure TOTP Two-Factor Authentication for BeyondInsight and Password Safe</b> .....	<b>42</b>
Configure TOTP Two-Factor Authentication Settings .....	42
Set TOTP Two-Factor Authentication on User Accounts .....	42
Register an Authenticator Application Device .....	44
Unregister an Authenticator Application Device .....	44

---

<b>Configure Smart Card Authentication for BeyondInsight and Password Safe</b> .....	<b>46</b>
Enable Smart Card Two-Factor Authentication in BeyondInsight .....	46
Enable Override Smart Card User Principal Name on User Accounts .....	47
Disable Forms Login .....	48
Configure Two-Factor Authentication Settings for User Accounts .....	53
<b>Configure a Claims-Aware Website in BeyondInsight</b> .....	<b>55</b>
Create a BeyondInsight Group .....	55
Add Relying Party Trust .....	55
Set Up Claim Rules .....	56
Supported Federation Service Claim Types .....	56
Claims-Aware SAML .....	56
Disable Forms Login .....	57
<b>Set Up SAML With a Generic Security Provider in BeyondInsight</b> .....	<b>60</b>
Configure SAML in the BeyondInsight Console .....	60
Configure Identity Provider (IdP) .....	61
Multiple Identity Providers .....	63
Configure SAML Using the saml.config File .....	63
Update Host Name and SAML access URL .....	65
Configure Azure Active Directory SAML with BeyondInsight SAML .....	66
Disable Forms Login .....	68
<b>Configure SAML 2.0 for Password Safe using Azure AD App</b> .....	<b>71</b>
Install and Configure .....	71
<b>Configure Password Safe to use the SAML Azure AD App</b> .....	<b>75</b>
<b>Configure AD FS Authentication Using SAML for BeyondInsight and Password Safe</b> ...	<b>78</b>
Configure AD FS on the Identity Provider Server .....	78
Configure SAML on the Service Provider Server (U-Series Appliance) .....	85
<b>Configure Okta SAML Authentication for BeyondInsight and Password Safe</b> .....	<b>88</b>
Configure SAML Application in Okta .....	89
Configure SAML Identity Provider in BeyondInsight .....	92
Disable Forms Login .....	94
<b>Configure Ping Identity SAML Authentication for BeyondInsight and Password Safe</b> ...	<b>97</b>
Configure SAML Application in Ping Identity .....	98
Configure SAML Identity Provider in BeyondInsight .....	100

---

Disable Forms Login .....	101
<b>Configure Password Safe and Ping Identity for PingOne .....</b>	<b>104</b>
Create a SAML Identity Provider in Password Safe .....	105
<b>Troubleshoot Authentication Issues .....</b>	<b>107</b>
Active Directory User Cannot Authenticate with BeyondInsight or Password Safe .....	107
Authentication Errors when using SAML 2.0 Web Applications .....	107

# BeyondInsight and Password Safe Authentication Guide

BeyondInsight and Password Safe support BeyondInsight user account authentication, as well as multi-factor authentication, smart card authentication, and third-party authentication for web tools supporting the SAML 2.0 standard. Various authentication methods, such as smart card authentication, two-factor authentication using a RADIUS server, Ping Identity, Okta, and Active Directory Federation Services (AD FS) are detailed in this guide.

BeyondInsight provides authentication for user accounts found in the BeyondInsight database. You can create BeyondInsight local accounts and groups, and you can add Active Directory, Azure Active Directory, and LDAP users and groups into BeyondInsight. You can apply BeyondInsight authentication to any of these accounts, using the procedures outlined in this guide.

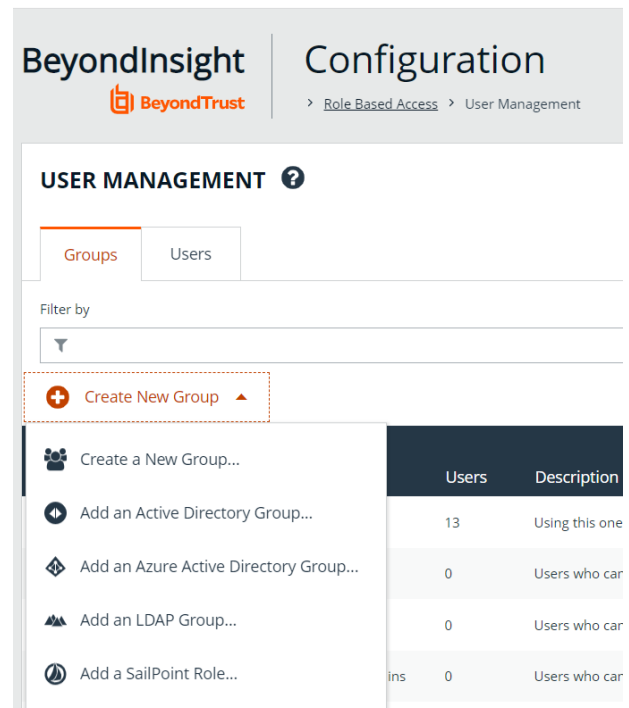
## Create and Configure Groups in BeyondInsight

BeyondInsight offers a role-based delegation model so that you can explicitly assign permissions to groups on specific product features based on their role. Users are provisioned based on the permissions of their assigned groups. A user must always belong to at least one group in BeyondInsight that has permissions assigned to be able to log in to BeyondInsight and Password Safe.



**Note:** By default, an **Administrators** group is created. The permissions assigned to the **Administrators** group cannot be changed. The user account you created when you configured BeyondInsight is a member of the group.

You can create BeyondInsight local groups, as well as add Active Directory, Azure Active Directory, and LDAP groups into BeyondInsight.



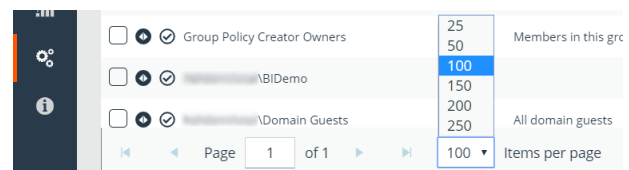
The screenshot shows the 'Configuration' page for 'BeyondInsight' under 'User Management'. It features a 'Groups' tab and a 'Filter by' dropdown. A 'Create New Group' button is highlighted with a red dashed box, and its dropdown menu is open, showing options like 'Create a New Group...', 'Add an Active Directory Group...', 'Add an Azure Active Directory Group...', 'Add an LDAP Group...', and 'Add a SailPoint Role...'. Below the menu is a table with columns 'Users' and 'Description'.

	Users	Description
Create a New Group...		
Add an Active Directory Group...	13	Using this one
Add an Azure Active Directory Group...	0	Users who car
Add an LDAP Group...	0	Users who car
Add a SailPoint Role...	0	Users who car

You can filter the groups displayed in the grid by type of group, name of the group, group description, and the date the group was last synchronized.



**Tip:** By default, the first 100 groups are displayed per page. You can change this by selecting a different number from the *Items per page* dropdown at the bottom of the grid.



The screenshot shows a table of groups with a dropdown menu for 'Items per page' set to 100. The table has columns for checkboxes, group names, and user counts.

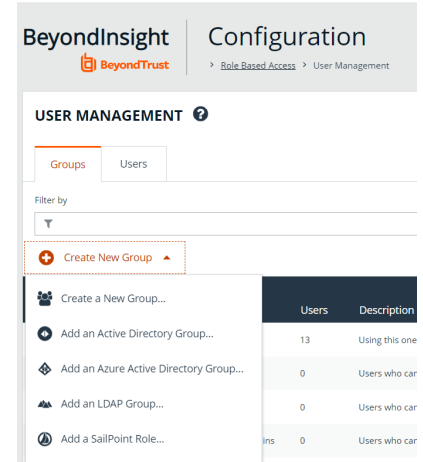
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Group Policy Creator Owners	25 50	Members in this grc
<input type="checkbox"/>	<input checked="" type="checkbox"/>	... \BI Demo	100	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	... \Domain Guests	150 200 250	All domain guests

Page 1 of 1 | 100 Items per page

## Create a BeyondInsight Local Group

To create a local group in BeyondInsight, follow the below steps:

1. Navigate to **Configuration > Role Based Access > User Management**.
2. From the **Groups** tab, click **Create New Group**.



3. Select **Create a New Group**.
4. Enter a **Group Name** and **Description** for the group.
5. The group is set to **Active** by default. Check the box to deactivate it, if you prefer to activate it later.
6. Click **Create Group**.

### Create New Group

Active

Group Name

New Test Group

Description

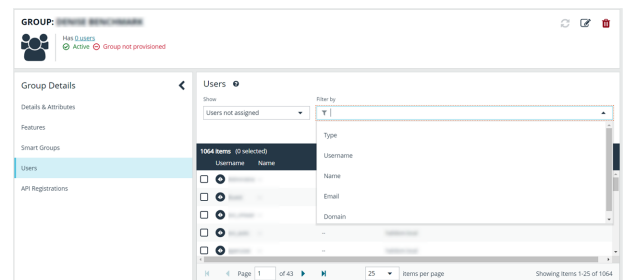
New Test Group

CREATE GROUP

DISCARD

7. Assign users to the group:

- Under **Group Details**, select **Users**.
- From the **Show** dropdown list, select **Users not assigned**.
- Filter the list of users displayed in the grid by **Type**, **Username**, **Name**, **Email**, and **Domain**, if desired.



- Select the users you wish to add to the group, and then click **Assign User** above the grid.



**Note:** By default, new groups are not assigned any permissions. You must assign permissions on features and smart groups after creating a new group. For more information on permissions and how to assign them, please see "[Assign Permissions to Groups in BeyondInsight](#)" on page 29.



**Note:** When a local user logs in to BeyondInsight for the first time using SAML authentication, BeyondInsight provisions their account by mapping it to the groups assigned to their account.

For releases prior to 21.3, and for upgrades to the 21.3 release, if the user account's group membership has changed (in the SAML claims provided) upon subsequent logins, BeyondInsight does not deprovision the user by removing them from the groups that were initially mapped to their account. Instead, BeyondInsight maps the user to any newly assigned groups, in addition to the groups their account is already mapped to.

You can configure BeyondInsight to synchronize group membership each time a local user logs in using SAML, as follows:

1. Navigate to **Configuration > Authentication Management > Authentication Options**.
2. Under **SAML Logon for Local Users**, toggle the **Enable Group Resync** option to enable it.

For new installs of release 21.3 and later releases, this option is enabled by default.

Adding Active Directory, Azure Active Directory, and LDAP groups into BeyondInsight is documented in subsequent chapters. Before you can add directory groups into BeyondInsight you must first create credentials that have permissions to query the directories.

**i** For more information on creating and editing directory credentials, please see "[Create and Edit Directory Credentials](#)" on page 9.



## Create and Edit Directory Credentials

A directory credential is required for querying Active Directory (AD), Azure AD, and LDAP. It is also required for adding AD, Azure AD, and LDAP groups and users in BeyondInsight. Follow the steps below for creating each type of directory credential.



**Note:** Before you can create an Azure AD credential, you must first register and configure permissions for an application in the Azure AD tenant where the user credentials reside. For more information, please see "[Register and Configure an Application in Azure Active Directory](#)" on page 13.

To create a directory credential in BeyondInsight:

1. Navigate to **Configuration > Role Based Access > Directory Credentials**.
2. Click **Create New Directory Credential**.
3. Follow the steps in the applicable section below, based on the type of directory you are creating.

## Create an Active Directory Credential

1. Select **Active Directory** for the **Directory Type**.
2. Provide a name for the credential.
3. Enter the name of the domain where the directory and user credentials reside.
4. Enable the **Use SSL** option to use a secure connection when accessing the directory.



**Note:** If **Use SSL** is enabled, **SSL authentication** must also be enabled in the *BeyondInsight* configuration tool.

4. Enter the credentials for the account that has permissions to query the directory.
5. Enable the **Use Group Resolution** option to use this credential for resolving groups from the directory.



**Note:** Only one credential can be set for group resolution per domain or server.

6. Click **Test Credential** to ensure the credential can successfully authenticate with the domain or domain controller before saving the credential.
7. Click **CreateCredential**.

### New Directory Credential ➤

#### Directory Type

- Active Directory  
 LDAP  
 Azure Active Directory

#### Credentials

Title

Domain

Use SSL

Username

#### Password

Password

 SHOW

Confirm Password

 SHOW

Use Group Resolution (Optional) ?

TEST CREDENTIAL

CREATE CREDENTIAL

DISCARD

## Create an LDAP Credential

1. Select **LDAP** for the **Directory Type**.
2. Provide a name for the credential.
3. Enter the name of the LDAP server where the directory and user credentials reside.
4. Enable the **Use SSL** option to use a secure connection when accessing the directory.



**Note:** If **Use SSL** is enabled, **SSL authentication** must also be enabled in the *BeyondInsight* configuration tool.

5. Enter the credentials for the account that has permissions to query the directory.
6. Enable the **Use Group Resolution** option to use this credential for resolving groups from the directory.



**Note:** Only one credential can be set for group resolution per LDAP server.

7. Click **Test Credential** to ensure the credential can successfully authenticate with the domain or domain controller before saving the credential.
8. Click **Create Credential**.

### New Directory Credential ➤

**Directory Type**

Active Directory  
 LDAP  
 Azure Active Directory

**Credentials**

Title

LDAP Server

Port  - +

Use SSL

**Password**

Bind DN

Password  SHOW

Confirm Password  SHOW

Use Group Resolution (Optional) ?

TEST CREDENTIAL

CREATE CREDENTIAL
DISCARD

## Create an Entra ID Credential

1. Select **Entra ID** for the **Directory Type**.
2. Provide a name for the credential.
3. Paste the **Client ID**, **Tenant ID**, and **Client Secret** that you copied when registering the application in your Azure AD tenant.
4. Enable the **Use Group Resolution** option to use this credential for resolving groups from the directory.



**Note:** Only one credential is supported per Azure AD tenant.

5. Click **Test Credential** to ensure the credential can successfully authenticate with the domain or domain controller before saving the credential.
6. Click **Save Credential**.

### New Directory Credential ➤

Directory Type

Active Directory

LDAP

Azure Active Directory

Credentials

Title

Client ID

Tenant ID

Client Secret

Use Group Resolution (Optional) ?

## Edit a Directory Credential

1. From the **Directory Credentials** grid, click the vertical ellipsis for the credential, and then select **Edit**.

2. Make the changes required.



**Note:** For AD or LDAP credentials, if you change the **Domain** or **LDAP Server**, enable or disable the **Use SSL** option, or update the **Username** or **Bind DN**, you must change the password. Click **Change Password** to display fields to enter and confirm the new password.

3. Click **Test Credential** to ensure the edited credential can successfully authenticate with the domain or domain controller before saving the credential.
4. Click **Save Credential**.

### Edit Directory Credential ➤

**Credentials**

Title

Domain

Use SSL

Username

CHANGE PASSWORD

Use Group Resolution (Optional) ?

TEST CREDENTIAL
UPDATE CREDENTIAL
DISCARD CHANGES



**Note:** To use Azure AD credentials for logging into BeyondInsight, the accounts must use SAML authentication.



For more information on configuring Azure AD SAML with BeyondInsight, please see "[Configure Azure Active Directory SAML with BeyondInsight SAML](#)" on page 66.

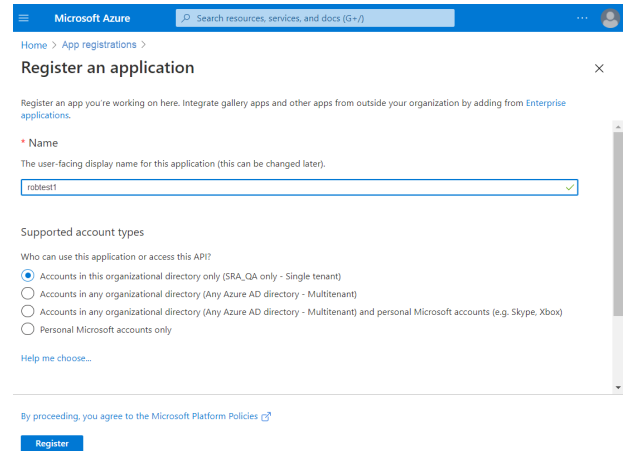
## Register and Configure an Application in Azure Active Directory

Before you can create Azure Active Directory (AD) credentials and add Azure AD groups and users into BeyondInsight, you must first register and configure an application in the Azure AD tenant where the user accounts reside. The below steps walk through creating a registered application in Azure AD, creating a client secret for the registered app, and configuring API permissions for the registered app.

## Create a Registered Application in Azure AD

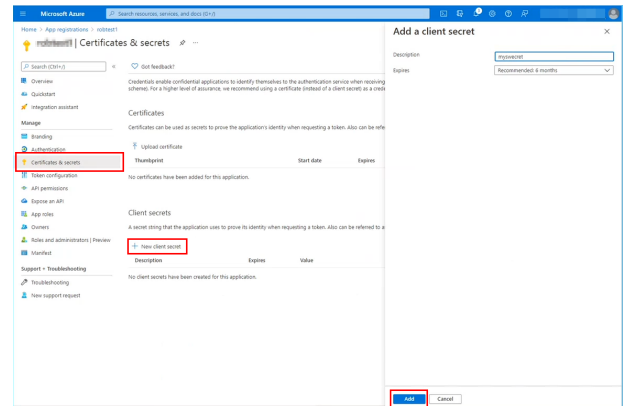
Sign into Azure and connect to the Azure AD tenant where the credentials you wish to add into BeyondInsight reside. Then follow these steps:

1. On the left menu, select **App registrations**.
2. Click **+ New Registration**.
3. Under **Name**, enter a unique application name.
4. Under **Supported account types**, select **Accounts in this organizational directory only**.
5. Click **Register**.



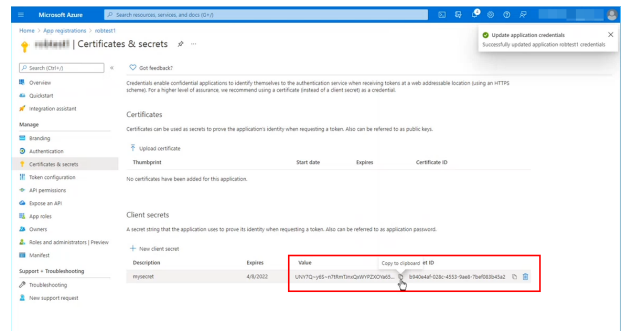
## Create a Client Secret for the Registered App

1. Select the newly created app from the list of **App Registrations** (if not already visible).
2. Select **Certificates & secrets** from the left menu.
3. Click **+ New Client Secret**.
4. Provide a **Description** and appropriate **Expiry**. If you select 1 or 2 years, the directory credential must be refreshed in BeyondInsight with a new client secret on the anniversary of its creation.
5. Click **Add**.



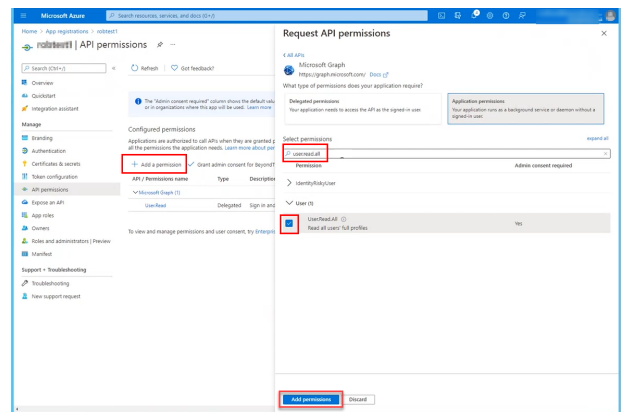
- Copy the client secret and store it in a safe place. It is required when creating directory credentials for Azure AD in BeyondInsight.

**Note:** This is the only time this client secret value is displayed.

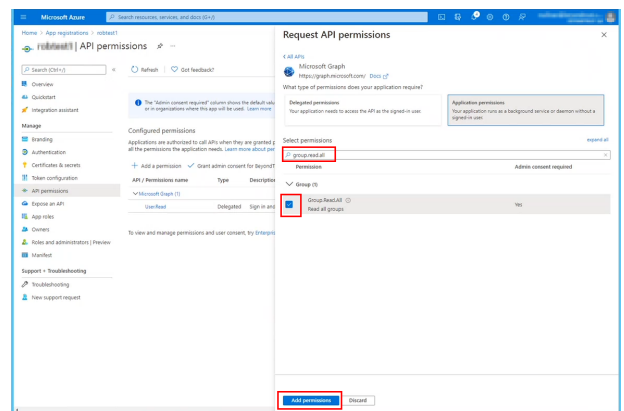


## Assign API Permissions to the Registered Application

- Select the newly created app from the list of **App Registrations**
- Select **API Permissions** from the left menu.
- Click **+ Add a permission.**
- Click **Microsoft Graph.**
- Click **Application Permissions.**
- Search for **User.Read.All** and check the box in the search results.

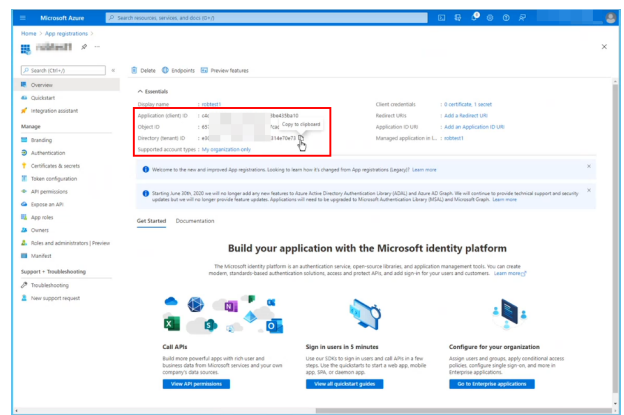
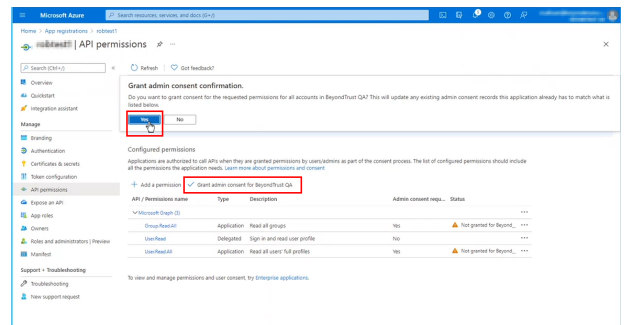
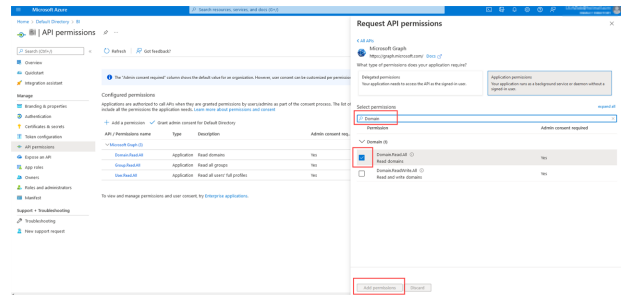


- Search for **Group.Read.All** and check the box in the search results.
- Click **Add permissions.**



9. Search for **Domain.Read.All** and check the box in the search results.
10. Click **Add permissions**.
11. Click **Grant Admin Consent for <directory name>** to give consent to the app to have those permissions you just added.
12. Click **Yes** to confirm.

Now that your registered app is created, has a client secret, and has API permissions assigned, select **Overview** from the left menu and copy the **Application (client) ID** and the **Directory (tenant) ID**. Store these in a safe place as these are required when creating directory credentials for Azure AD in BeyondInsight.



**i** For more information on directory credentials, please see ["Create and Edit Directory Credentials"](#) on page 9.



## Map Directory Credentials to a Domain

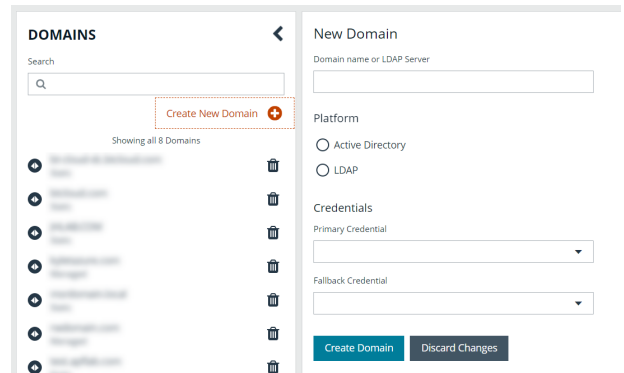
Domain management allows you to map a default primary directory credential and an optional fallback credential as preferred binding credentials used for account resolution against domains in your environment when logging in to BeyondInsight.



**Note:** If credentials are not mapped, or both mapped credentials fail, BeyondInsight attempts login following the legacy process of not using mapped credentials.

Follow these steps to add or edit primary and secondary credentials for a domain:

1. Navigate to **Configuration > Role Based Access > Domain Management**.
2. Click **Create New Domain** to create a new one.
3. Provide the name of the domain or LDAP server.
4. Select the type of platform.
5. Select a **Primary Credential** from the dropdown.
6. Select a **Fallback Credential** from the dropdown.
7. Click **Create Domain**.

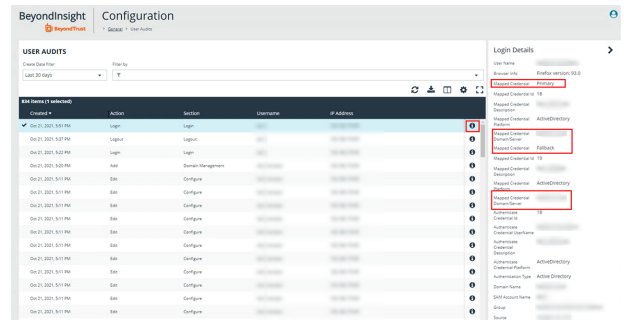


8. To edit credentials for an existing domain, select the domain from the left pane, make your edits, and then click **Save Domain**.



**Tip:** Primary and fallback credentials can include Password Safe managed accounts.

When domain management is configured for a domain and user selects the domain when logging into BeyondInsight, the specified primary and fallback credentials are used to resolve their account. The credentials used for authentication are shown in the **Login Details** for the specific login activity on the **Configuration > General > User Audits** page.



## Add an Active Directory Group

Active Directory (AD) group members can log in to the management console and perform tasks based on the permissions assigned to the group. The group can authenticate against either a domain or domain controller. Upon logging into BeyondInsight, users can select a domain from the **Log in to** list on the **Login** page.



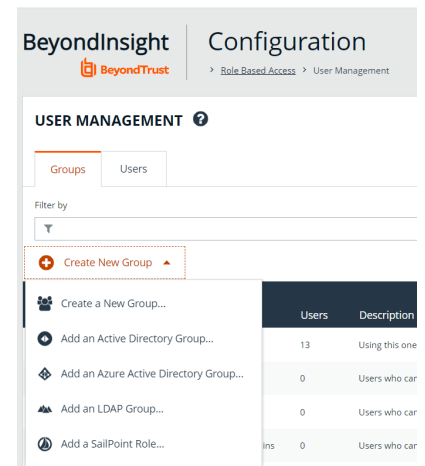
**Tip:** The **Log in to** list is only displayed on the **Login** page when there are either AD or LDAP user groups created in the BeyondInsight console. The **Log in to** list is displayed by default, but may be disabled / enabled by an admin user by toggling the **Show list of domains/LDAP servers on login page** setting from **Configuration > System > Site Options** page.



**Note:** AD users must log in to the management console at least once to receive email notifications.

Create an Active Directory Group in BeyondInsight, as follows:

1. Navigate to **Configuration > Role Based Access > User Management**.
2. From the **Groups** tab, click **Create New Group**.



	Users	Description
Create a New Group...		
Add an Active Directory Group...	13	Using this one
Add an Azure Active Directory Group...	0	Users who car
Add an LDAP Group...	0	Users who car
Add a SailPoint Role...	ins 0	Users who car

3. Select **Add an Active Directory Group**.

4. Select a credential from the list.



**Note:** If you require a new credential, click **Create New Credential** to create one. The new credential is added to the list of available credentials.

5. If the **Domain** field is not automatically populated, enter the name of a domain or domain controller.
6. After you enter the domain or domain controller credential information, click **Search Active Directory**. A list of security groups in the selected domain is displayed.

### Active Directory Group Search

Credential

[Create New Credential...](#)

Domain

Filter by Group Name

SEARCH ACTIVE DIRECTORY

CANCEL



**Note:** The default filter is an asterisk (\*), which is a wild card filter that returns all groups. For performance reasons, a maximum of 250 groups from Active Directory is retrieved.

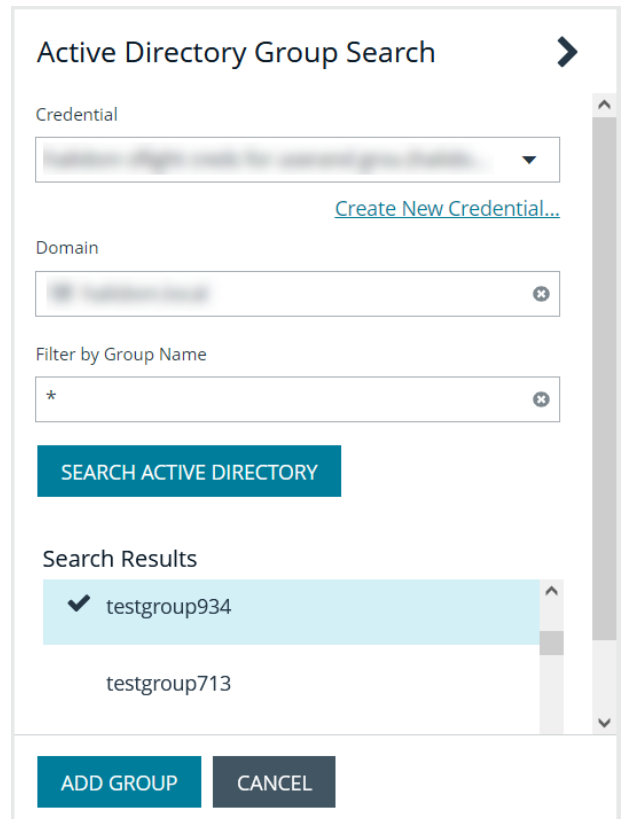
7. Set a filter on the groups to refine the list, and then click **Search Active Directory**.



**Example:** Sample filters:

- **a\*** returns all group names that start with "a"
- **\*d** returns all group names that end with "d"
- **\*sql\*** returns all groups that contain "sql" in the name

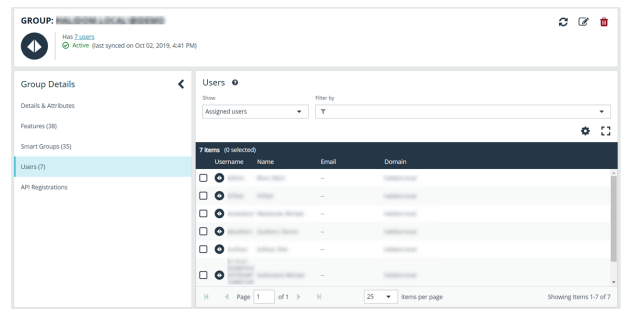
- Select a group, and then click **Add Group**.



- The group is added and set to **Active** but not provisioned or synchronized with AD. Synchronization with AD to retrieve users begins immediately.
- Once the group has been synced with AD, you can view the users assigned to the group by selecting **Users** from the **Group Details** pane.



**Tip:** Use the filters above the grid to narrow down the list of users displayed in the grid by **Type**, **Username**, **Name**, **Email**, or **Domain**, or to show users not assigned to the group.



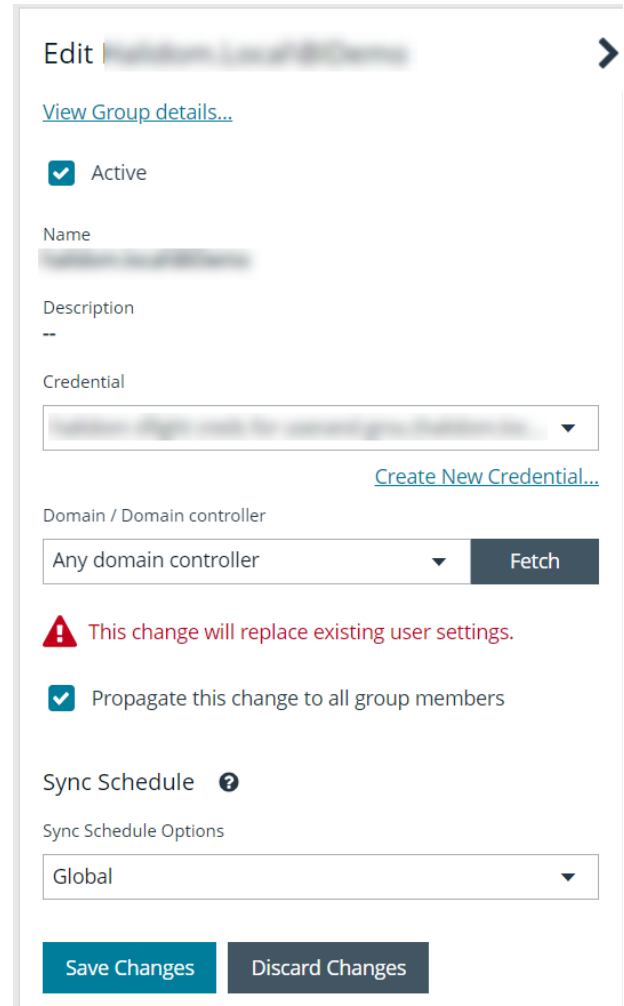

**Note:** By default, new groups are not assigned any permissions. You must assign permissions on features and Smart Groups after creating a new group. For more information on permissions and how to assign them, please see ["Assign Permissions to Groups in BeyondInsight"](#) on page 29.

**i** For more information on creating and editing directory credentials, please see ["Create and Edit Directory Credentials"](#) on page 9.

## Propagate Domain Changes to Group Members

Domain changes can be propagated to all users in a group by enabling the **Propagate this change to all group members** option for the group. By default, this is set to OFF. When enabled, changes to the preferred domain controller at the group level are applied to all group members.

When creating a new group, we advise turning this setting on by editing the new group details. This ensures that all users in the new group get a preferred domain controller from the initial setup of the group.



Edit [Redacted Group Name] >

[View Group details...](#)

Active


Name  
[Redacted]

Description  
--


Credential  
[Redacted] ▼

[Create New Credential...](#)

Domain / Domain controller  
Any domain controller ▼ Fetch

 This change will replace existing user settings.

Propagate this change to all group members

Sync Schedule 

Sync Schedule Options  
Global ▼

Save Changes Discard Changes

## Add an Azure Active Directory Group

Azure Active Directory (AD) group members can log in to the management console using SAML authentication and perform tasks based on the permissions assigned to the group. Upon logging into BeyondInsight, users can select a domain from the **Log in to** list on the **Login** page.



**Tip:** The **Log in to** list is only displayed on the **Login** page when there are either AD or LDAP user groups created in the BeyondInsight console. The **Log in to** list is displayed by default, but may be disabled / enabled by an admin user by toggling the **Show list of domains/LDAP servers on login page** setting from **Configuration > System > Site Options** page.

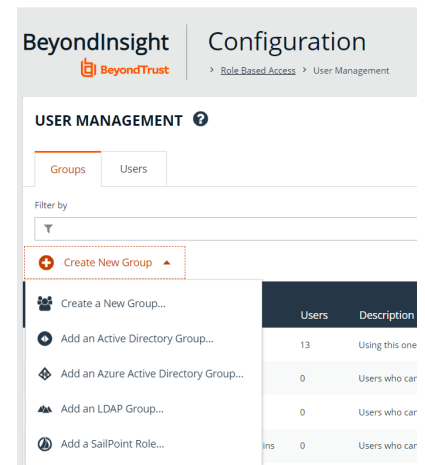


**Note:** AD users must log in to the management console at least once to receive email notifications.

Direct Connect does not support using SAML as an authentication method. Therefore, Direct Connect is not available with Azure AD accounts.

Create an Azure Active Directory Group in BeyondInsight, as follows:

1. Navigate to **Configuration > Role Based Access > User Management**.
2. From the **Groups** tab, click **Create New Group**.



	Users	Description
Create a New Group...		
Add an Active Directory Group...	13	Using this one
Add an Azure Active Directory Group...	0	Users who car
Add an LDAP Group...	0	Users who car
Add a SailPoint Role...	ins 0	Users who car

3. Select **Add an Azure Active Directory Group**.

- Select a credential from the list.



**Note:** If you require a new credential, click **Create a New Credential** to create a new credential. The new credential is added to the list of available credentials.

- Click **Search Azure Active Directory**. A list of security groups displays.

## Azure Active Directory Group Search



Credential

[Create New Credential...](#)

Filter by Group Name

SEARCH AZURE ACTIVE DIRECTORY

CANCEL



**Note:** For performance reasons, a maximum of 250 groups from Azure AD is retrieved. The default filter is an asterisk (\*), which is a wildcard filter that returns all groups. Use the group filter to refine the list.

- Set a filter on the groups that are to be retrieved, and then click **Search Azure Active Directory**.



**Example:** Sample filters:

- **a\*** returns all group names that start with a.
- **\*d** returns all group names that end with d.
- **\*sql\*** returns all groups that contain sql in the name.

- Select a group, and then click **Add Group**.

### Search Results

Functional Accounts

Group used to store Functional Accounts for QA testing



PS\_QA

PasswordSafe QA

Managed Accounts

Password Safe Managed Accounts

Msamigrp

First test group

Automation

For Automation users

Admin

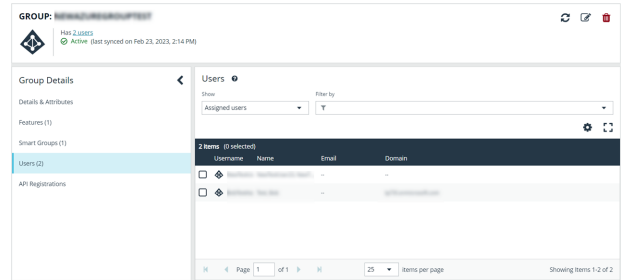
Group of administrators


ADD GROUP


CANCEL


- The group is added and set to **Active** but not provisioned or synchronized with Azure AD. Synchronization with Azure AD to retrieve users begins immediately.

9. Once the group has been synced with Azure AD, you can view the users assigned to the group, as well as unassigned users, by selecting **Users** from the **Group Details** section and then using the filters.



 **Note:** By default, new groups are not assigned any permissions. You must assign permissions on features and Smart Groups after creating a new group. For more information on permissions and how to assign them, please see ["Assign Permissions to Groups in BeyondInsight" on page 29.](#)

 **Note:** To use Azure Active Directory credentials for logging into BeyondInsight, the accounts must use SAML authentication. For more information on configuring Azure AD SAML with BeyondInsight, please see ["Configure Azure Active Directory SAML with BeyondInsight SAML" on page 66.](#)

 For more information on creating and editing directory credentials, please see ["Create and Edit Directory Credentials" on page 9.](#)



## Add an LDAP Group

LDAP group members can log in to the management console and perform tasks based on the permissions assigned to the group. The group can authenticate against either a domain or domain controller. Upon logging in to BeyondInsight, users can select a domain or LDAP server from the **Log in to** list on the **Login** page.



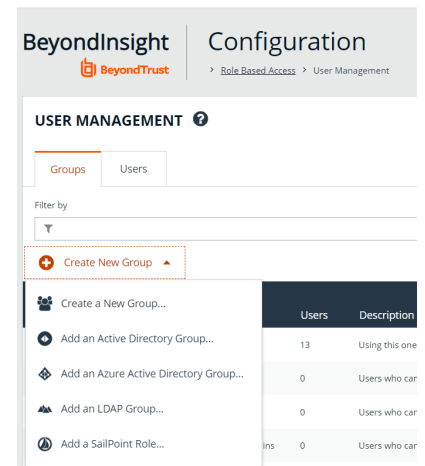
**Tip:** The **Log in to** list is only displayed on the **Login** page when there are either AD or LDAP user groups created in the BeyondInsight console. The **Log in to** list is displayed by default, but may be disabled / enabled by an admin user by toggling the **Show list of domains/LDAP servers on login page** setting from **Configuration > System > Site Options** page.



**Note:** LDAP users must log in to the management console at least once to receive email notifications.

Create an LDAP Group in BeyondInsight, as follows:

1. Navigate to **Configuration > Role Based Access > User Management**.
2. From the **Groups** tab, click **Create New Group**.



The screenshot shows the BeyondInsight Configuration page, specifically the User Management section. The 'Groups' tab is selected. A 'Create New Group' button is highlighted with a red dashed box. A dropdown menu is open, showing options to create a new group, including 'Add an LDAP Group...'. Below the dropdown is a table with columns 'Users' and 'Description'.

	Users	Description
Create a New Group...		
Add an Active Directory Group...	13	Using this one
Add an Azure Active Directory Group...	0	Users who car
Add an LDAP Group...	0	Users who car
Add a SailPoint Role...	ins 0	Users who car

3. Select **Add an LDAP Group** from the list.

4. Select a credential from the list.



**Note:** If you require a new credential, click **Create a New Credential** to create a new one. The new credential is added to the list of available credentials.

5. Click **Fetch** to load the list of Domain Controllers, and then select one.
6. To filter the group search, enter keywords in the group filter or use a wild card, and then click **Search LDAP**.

### LDAP Group Search ➤

Credential

[Create New Credential...](#)

Server

Domain / Domain controller  
 **FETCH**

Filter by Group Name

**SEARCH LDAP** **CANCEL**



**Example:** Sample filters:

- **a\*** returns all group names that start with a.
- **\*d** returns all group names that end with d.
- **\*sql\*** returns all groups that contain sql in the name.

7. Select a group, and then click **Continue to Add Group**.

### LDAP Group Search

SEARCH LDAP

#### Search Results

- OracleDBSecurityAdmins  
*Users who can create and delete enterprise domains in this realm, move database*
- OracleDBCreators  
*Users who can register databases in this realm, including creating the database*
- OracleNetAdmins  
*Users who can register Network Service Alias in this Oracle Context.*
- OracleDefaultDomain
- OracleContextAdmins  
*Users who can administer all entities in this Oracle Context*

CONTINUE TO ADD GROUP    CANCEL

8. Select the **Group Membership Attribute** and **Account Naming Attribute**.
9. Enter a **Base Distinguished Name**, if not automatically populated.
10. Click **Add Group**.

## LDAP Group Search

 Active

Name  
OracleNetAdmins

Description  
Users who can register Network Service Alias in t

Group Membership attribute

uniqueMember

Account Naming attribute

uid

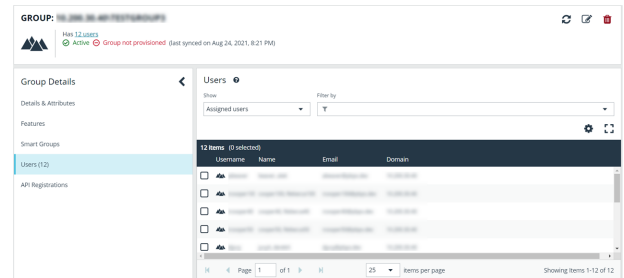
Base Distinguished Name

dc=,dc=

ADD GROUP

CANCEL

11. The group is added and set to **Active** but is not provisioned or synchronized with LDAP. Synchronization with LDAP to retrieve users begins immediately.
12. Once the group has been synced with LDAP, you can view the users assigned to the group, as well as unassigned users, by selecting **Users** from the **Group Details** section, and then using the filters.



GROUP: OracleNetAdmins  
 New 12 users  
 Active Group not provisioned (last synced on Aug 24, 2021, 8:21 PM)

Group Details

Users

Assigned users

Username	Name	Email	Domain
...	...	...	...
...	...	...	...
...	...	...	...
...	...	...	...
...	...	...	...
...	...	...	...
...	...	...	...
...	...	...	...
...	...	...	...
...	...	...	...
...	...	...	...

Showing items 1-12 of 12

**Note:** By default, new groups are not assigned any permissions. You must assign permissions on features and smart groups after creating a new group. For more information on permissions and how to assign them, please see ["Assign Permissions to Groups in BeyondInsight"](#) on page 29.

**i** For more information on creating and editing directory credentials, please see ["Create and Edit Directory Credentials"](#) on page 9.

## Assign Permissions to Groups in BeyondInsight

The following permissions may be assigned to user groups in BeyondInsight for each feature and Smart Group.

Permission	Description
No Access	Users cannot access the selected feature or Smart Group. In most cases, the feature is not visible to the users.
Read Only	Users can view selected areas, but cannot change information.
Full Control	Users can view and change information for the selected feature.

Permissions for a BeyondInsight user must be assigned cumulatively and at the group level. You must assign permissions on features and Smart Groups after creating a new group in order for users in that group to be able to access features in the product. For example, if you want a BeyondInsight administrator to manage discovery scans only, then you must assign full control for the following features:

- **Management Console Access**
- **Asset Management**
- **Reports Management**
- **Scan – Job Management**
- **Scan Management**



**Note:** In addition to the group permissions noted, for the group to be provisioned, there must be at least one enabled Smart Group for the group. This sets the scope for the features.


## Assign Features Permissions






**Note:** The features listed are based upon your BeyondInsight license. Only features relevant to your licensed installation are listed.

1. Navigate to **Configuration > Role Based Access > User Management > Users**.
2. Click the vertical ellipsis button for the group, and then select **View Group Details**.
3. Under **Group Details**, click **Features**.
4. Filter the list of features displayed in the grid using the **Show** and **Filter by** dropdown lists.
5. Select the features you wish to assign permissions to, and then click **Assign Permissions** above the grid.
6. Select **Assign Permissions Read Only**, **Assign Permissions Full Control**, or **Disable Permissions**.

The following table provides information on the features permissions you can assign to your groups.

Feature	Provides Permissions To:
Analytics & Reporting	Log in to the console and access <b>Analytics &amp; Reporting</b> to generate and subscribe to reports.
Appliance (U-Series) Access	Grant access to manage the U-Series Appliance as a BeyondInsight user.
Asset Management	Create Smart Rules. Edit and delete buttons on the <b>Asset Details</b> window. Create Active Directory queries. Create address groups.
Attribute Management	Add, rename, and delete attributes when managing user groups.
Credential Management	Add and change credentials when running scans and deploying policies.
Directory Credential Management	Grant access to the configuration area where directory credentials are managed. This feature must be enabled to support access to directory queries as well.
Directory Query Management	Grant access to the configuration area where directory queries are managed.
	 <b>Note:</b> Access to <i>Directory Credential Management</i> must also be granted.
Domain Management	Grants the user permission to configure mappings of bind credentials to domains for account resolution.
Endpoint Privilege Management	Grant access to the Endpoint Privilege Management features, excluding Policy Editor and Reporting.
Endpoint Privilege Management Policy Editor	Grant access to the Endpoint Privilege Management Policy Editor feature.
Endpoint Privilege Management Reporting	Grant access to the Endpoint Privilege Management Reporting feature.
Endpoint Privilege Management for Unix & Linux	Grant access to the Endpoint Privilege Management for Unix & Linux features.
File Integrity Monitoring	Work with <b>File Integrity</b> rules.
License Reporting	View the <b>Licensing</b> folder in <b>Analytics &amp; Reporting</b> (MSP reports, Endpoint Privilege Management for Windows, Endpoint Privilege Management for Mac true-up reports, and Assets Scanned report).

Feature	Provides Permissions To:
Management Console Access	Access the BeyondInsight management console.
Manual Range Entry	Allow the user to manually enter ranges for scans and deployments rather than being restricted to smart groups. The specified ranges must be within the selected smart group.
Option Management	Change the application options settings (for example, account lockout and account password settings).
Options - Connectors	Access the configuration area where connectors are managed.
Options - Scan Options	Access the configuration area where scan options are managed.
Password Safe Account Management	Grant read or write permissions to the following features on the <b>Managed Accounts</b> page and through the public API: <ul style="list-style-type: none"> <li>• Bulk delete accounts</li> <li>• Add accounts to a Quick Group</li> <li>• Remove accounts from a Quick Group</li> <li>• Add, edit, and delete accounts</li> </ul>
Password Safe Admin Session	Password Safe web portal admin sessions.
Password Safe Admin Session Reviewer	Grant a user admin session reviewer permissions only.
Password Safe Global API Quarantine	Access to the Quarantine APIs.
Password Safe Bulk Password Change	Change more than one password at a time.
Password Safe Agent Management	Grant a user administrator permissions to the <b>Configuration &gt; Privileged Access Management Agents</b> page.
Password Safe Configuration Management	Grant a user administrator permissions to the <b>Configuration &gt; Privileged Access Management</b> page.
Password Safe Domain Management	Check the <b>Read</b> and <b>Write</b> boxes to permit users to manage domains.
Password Safe Policy Management	Grant a user administrator permissions to the <b>Configuration &gt; Privileged Access Management Policies</b> page.
Password Safe Role Management	Allows a user to manage roles, provided they have the following permissions: <b>Password Safe Role Management</b> and <b>User Account Management</b> .
Password Safe System Management	Read and write managed systems through the public API.
Password Safe Ticket System Management	This feature is not presently used.
Reports Management	Run scans, create reports, and create report categories.
Scan - Job Management	Activate <b>Scan</b> and <b>Start Scan</b> buttons.  Activate <b>Abort</b> , <b>Resume</b> , <b>Pause</b> , and <b>Delete</b> on the <b>Job Details</b> page.

Feature	Provides Permissions To:
Scan - Report Delivery	Allow a user to set report delivery options when running a scan: <ul style="list-style-type: none"> <li>• Export Type</li> <li>• Notify when complete</li> <li>• Email report to</li> <li>• Include scan metrics in email (only available for All Audits Scan)</li> </ul>
Scan Management	Delete, edit, duplicate, and rename reports on the <b>Manage Report Templates</b> page. Activate <b>New Report</b> and <b>New Report Category</b> . Activate the <b>Update</b> button on the <b>Edit Scan Settings</b> view.
Secrets Safe	Provides access to Secrets Safe for all members of the selected group.
Session Monitoring	Use the session monitoring features.
Smart Rule Management – Asset	Grants permission to view, create, and edit asset Smart Rules; editing is limited to Smart Rules that are enabled for groups the user is a member of. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <b>Note:</b> Newly created Smart Rules created by a non-administrator are automatically enabled with full permissions for all groups where the user is a member. For more information, see <a href="#">Use Smart Rules to Organize Assets</a> in the <a href="#">BeyondInsight User Guide</a>.                     </div>
Smart Rule Management – Managed Account	Grants permission to view, create, and edit managed account Smart Rules; editing is limited to smart rules that are enabled for groups the user is a member of. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <b>Note:</b> Newly created Smart Rules created by a non-administrator are automatically enabled with full permissions for all groups where the user is a member. For more information, see <a href="#">Use Smart Rules to Organize Assets</a> in the <a href="#">BeyondInsight User Guide</a>.                     </div>
Smart Rule Management – Managed System	Grants permission to view, create, and edit managed system Smart Rules; editing is limited to smart rules that are enabled for groups the user is a member of. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <b>Note:</b> Newly created Smart Rules created by a non-administrator are automatically enabled with full permissions for all groups where the user is a member. For more information, see <a href="#">Use Smart Rules to Organize Assets</a> in the <a href="#">BeyondInsight User Guide</a>.                     </div>
Smart Rule Management – Policy User	Grants permission to view, create, and edit policy user Smart Rules; editing is limited to smart rules that are enabled for groups the user is a member of. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <b>Note:</b> Newly created Smart Rules created by a non-administrator are automatically enabled with full permissions for all groups where the user is a member. For more information, see <a href="#">Use Smart Rules to Organize Assets</a> in the <a href="#">BeyondInsight User Guide</a>.                     </div>
Ticket System	View and use the ticket system.
Ticket System Management	Mark a ticket as inactive. The ticket no longer exists when <b>Inactive</b> is selected.



Feature	Provides Permissions To:
User Accounts Management	Add, delete, or change user groups and user accounts.  A minimum of read access to Directory Credential Management must also be granted to enable creation of AD and LDAP Groups.
User Audits	View audit details for management console users on the <b>User Audits</b> page.
U-Series Appliance Administrator	Provides access to manage all aspects of the U-Series Appliance.
U-Series Appliance Backups	Provides access to manage the <b>Backup and Restore</b> options of the U-Series Appliance.
U-Series Appliance High Availability	Provides access to manage the <b>High Availability</b> features of the U-Series Appliance.
U-Series Appliance Login	Provides access to manage the U-Series Appliance as a BeyondInsight user.
U-Series Appliance Manage RDP	Provides access to manage Remote Desktop Protocol to the U-Series Appliance.
U-Series Appliance Patching	Provides access to manage updates to the U-Series Appliance.



For more information, please see the *Managed Accounts* section in the *BeyondInsight and Password Safe API Guide* at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/api/password-safe/managed-accounts.htm>.

## Features Permissions Required for Configuration Options

Configuration Option	Feature and Permission
Active Directory Queries	Asset Management - Full Control.
Address Groups	Asset Management - Full Control.
Attributes	Asset Management - Full Control.
Connectors	Asset Management and Management Console Access - Full Control.
Password Safe Connections	Member of the Built-In Administrators group.
Endpoint Privilege Management Module	Management Console Access and Endpoint Privilege Management - Full Control.
Scan Options	Scan Management - Full Control.
Services	Member of the Built-In Administrators group.
User Audits	User Audits - Full Control.
User Management	Everyone can access.  Users without the Full Control permission to <b>User Account Management</b> feature can edit only their user record.
Workgroups	User Accounts Management - Full Control.

## Assign Smart Groups Permissions

1. Navigate to **Configuration > Role Based Access > User Management > Users**.
2. Click the vertical ellipsis button for the group, and then select **View Group Details**.
3. Under **Group Details**, select **Smart Groups**.
4. Filter the list of Smart Groups displayed in the grid using the **Show** and **Filter by** dropdown lists.
5. Select the Smart Groups you wish to assign permissions to, and then click **Assign Permissions** above the grid.
6. Select **Assign Permissions Read Only**, **Assign Permissions Full Control**, or **Disable Permissions**.

# Configure RADIUS Two-Factor Authentication for BeyondInsight and Password Safe

You can configure two-factor authentication using a RADIUS server to log in to the BeyondInsight management console, Analytics & Reporting, and Password Safe.

In BeyondInsight, you must first configure the alias to represent the RADIUS server instance, and then select two-factor authentication settings for the user.

After you set up RADIUS two-factor authentication, users must log in to BeyondInsight or Password Safe using the configured two-factor authentication method.

## Configure the RADIUS Server

To configure the RADIUS server instance for two-factor authentication in BeyondInsight, follow the below steps.

1. Navigate to **Configuration > Authentication Management > Radius two-factor authentication**.
2. Click **Create New RADIUS Alias**.
3. Set the following:
  - **Alias:** Provide a name used to represent the RADIUS server instance. This is displayed in the RADIUS server grid and must be unique.
  - **Filter:** Select a filter that will be used to determine if this RADIUS server instance should be used. If you select one of the domain filters, you must enter a **Value**.
  - **Value:** If one of the domain filters is selected, enter a value that will identify the domain. Enter a domain or comma-separated list of domains, depending on the setting selected for the filter.
  - **Host:** Enter the DNS name or the IP address for your RADIUS server.
  - **Resource Zone:** Select a Resource Zone to send RADIUS requests through. Traffic proxies through the Resource Broker and on to the on-prem RADIUS server.
  - **Authentication Mechanism:** Select **PAP**, or **MSCHAPv2** if applicable. MSCHAPv2 is supported only if the Duo proxy is configured to use a RADIUS client.
  - **Authentication Port:** Enter the listening port that is configured on your RADIUS server to receive authentication requests. The default port is **1812**.
  - **Authentication Request Timeout:** Enter the time in seconds that you want BeyondInsight to wait for a response from the RADIUS server before the request times out. The default value is ten seconds.
  - **Shared Secret:** Enter the shared secret that is configured on your RADIUS server.
  - **Initial Request:** Provide the value passed to the RADIUS server on the first authentication request. Select from the following: **Forward User Name** (default), **Forward User Name and Password**, **Forward User Name and Token**.
  - **Prompt:** Provide the first message that displays to the user when they log in to the application. This setting is available only when **Forward User Name and Token** is selected as the initial request value.
  - **Transmit NAS Identifiers:** Enable this option if it is applicable to your environment. When this option is enabled, NAS identifiers are transmitted to permit access. In some cases, a RADIUS server does not permit access if NAS identifiers are not transmitted. BeyondInsight transmits its NAS IP Address and its NAS Identifier.
4. Click **Create New RADIUS Alias**.



**Note:** If a Resource Zone is selected, traffic is routed over a Resource Broker. If no Resource Zone is selected, traffic is routed directly from the cloud.

## Configure RADIUS Two-Factor Authentication Using Duo

This section is a high-level overview on the configuration required for BeyondInsight and Password Safe to work with a RADIUS infrastructure using Duo.

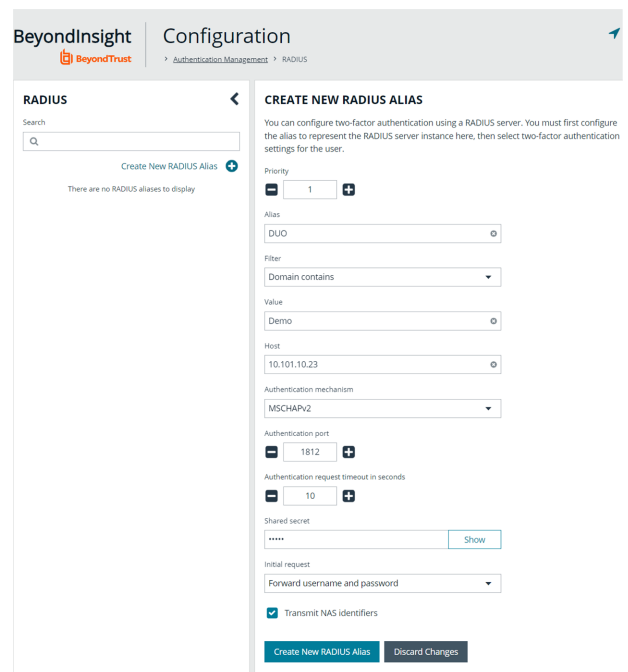
BeyondInsight and Password Safe can work with the following Duo configurations:

- RADIUS Auto
- RADIUS Challenge
- RADIUS Duo only

## Configure Two-Factor for RADIUS Auto and RADIUS Challenge Configurations Using Duo

Follow the steps outlined above in "[Configure the RADIUS Server](#)" on page 35, using the following settings:

- For **Alias**, enter **Duo**.
- For **Authentication Mechanism**, select **PAP**.
- For **Initial Request**, select **Forward User Name and Password**.



**BeyondInsight Configuration**

Authentication Management > RADIUS

**RADIUS**

Search

Create New RADIUS Alias +

There are no RADIUS aliases to display

**CREATE NEW RADIUS ALIAS**

You can configure two-factor authentication using a RADIUS server. You must first configure the alias to represent the RADIUS server instance here, then select two-factor authentication settings for the user.

Priority: 1 +

Alias: DUO

Filter: Domain contains

Value: Demo

Host: 10.101.10.23

Authentication mechanism: MSCHAP2

Authentication port: 1812 +

Authentication request timeout in seconds: 10 +

Shared secret: [masked] Show

Initial request: Forward username and password

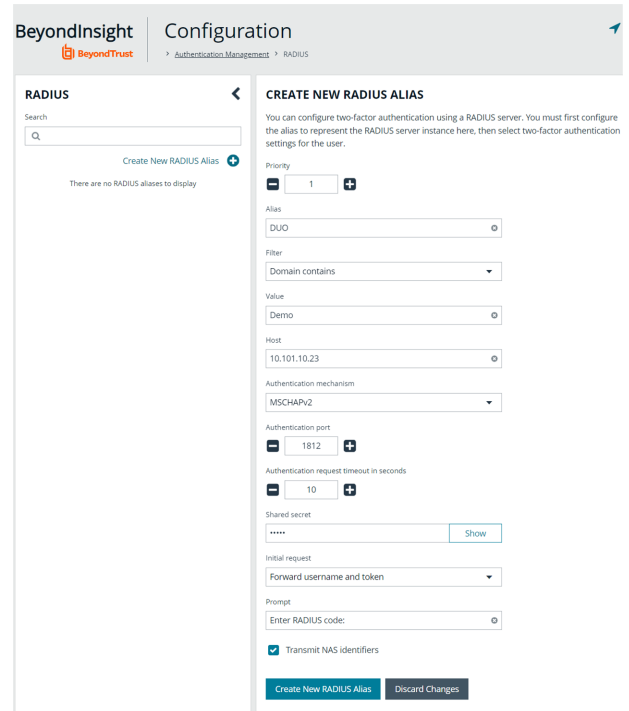
Transmitt NAS identifiers

Create New RADIUS Alias Discard Changes

## Configure Two-Factor for a RADIUS Duo-only Configuration

Follow the steps outlined above in "[Configure the RADIUS Server](#)" on page 35, using the following settings:

- For **Alias**, enter **Duo**.
- For **Authentication Mechanism**, select **PAP**.
- For **Initial Request**, select **Forward User Name and Token**.
- For **Initial Prompt**, enter a message to display on the BeyondInsight login page to provide guidance to users on the information to enter. In this case, the user must enter the RADIUS code.




### Example: Duo-Only Login Page

After RADIUS two-factor authentication is configured, the login page for the end user varies, depending on the configured settings.

The screenshot shows a login page configured for Duo-only authentication. The user can enter a passcode to log in or select a device to send a code to. The user then enters the code on the login page.

Duo two-factor login for user1. Enter a passcode or select one of the following options: 1. Duo Push to XXX-XXX-6313 2. Phone call to XXX-XXX-6313 3. SMS passcodes to XXX-XXX-6313 (next code starts with: 2) Passcode or option (1-3):

## Configure Alternate Directory Attribute for RADIUS

To configure an alternate directory attribute for Active Directory and LDAP users for RADIUS authentication, follow the below steps.



**Note:** This setting is optional.

1. In BeyondInsight, navigate to **Configuration > Authentication Management > Authentication Options**.
2. Under **RADIUS Two-Factor Authentication**, set the following:
  - **Alternate directory attribute:** Enter the Active Directory or LDAP attribute that is matched on the RADIUS server to identify the user account. This can be any attribute in Active Directory or LDAP. The default value is **extensionName**.

- **Enable for new directory accounts:** Click the toggle to enable this attribute for new accounts when they are discovered.
3. Click **Update RADIUS Two-Factor Authentication Options**.

## Apply RADIUS Two-Factor Authentication to User Accounts

The type of two-factor authentication can be set on a user account when a new user is created or when editing an existing user account. You can enable RADIUS two-factor authentication for all new users from **Authentication Options > RADIUS Two-Factor Authentication** settings, as indicated in the above section.

1. In BeyondInsight, navigate to **Configuration > Role Based Access > User Management > Users**.
2. To create a new user, click **Create New User**. To edit an existing user, click the vertical ellipsis for the account and select **Edit User Details**.

- At the bottom of the user account settings, select **RADIUS** from the **Two Factor Authentication** list.

### Create New User ➤

**Identification**

First Name

Last Name

Email

Username

New Password  Show

Confirm New Password  Show

**Contact Information**

Work Phone

Home Phone

Mobile Phone

**User Status**

Activation Date

Expiration Date

User Active

Account Locked

Account Quarantined

**Authentication Options** ?

Override Smart Card User Principal Name

Disable Forms Login

**Two-Factor Authentication**

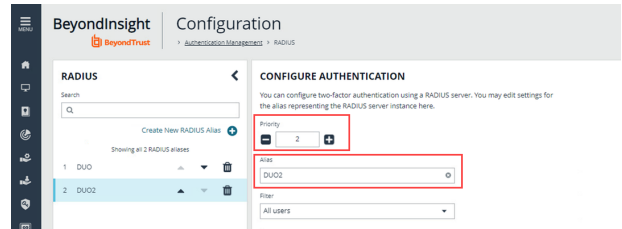
Map Two-Factor User

Create User Discard

## Using Multiple RADIUS Servers

If a customer has multiple RADIUS servers, they are processed from the lowest priority to highest. The DUO server is first. If BeyondInsight connects to that server, no other servers are checked.

If BeyondInsight cannot connect to the first server (DUO), then a connection is attempted with the next server (DUO2) in the list (the next highest priority number). Each server is checked until a connection is made or all servers available have been tried.





## Configure SecureAuth with Password Safe using RADIUS

Use the following procedures to configure SecureAuth two-factor authentication with Password Safe and RADIUS.

1. Install the SecureAuth app on a mobile device and click the bar code to scan.
2. In the BeyondInsight Console, perform the following:
  - Configure RADIUS, ensuring **UDP port 1812** is open for the SecureAuth instance.
  - Create a group with role access for managed accounts.
  - Create a user. The user must also be a user in the SecureAuth system.
  - Enable two-factor authentication for the user. Map the user to the account name in SecureAuth.

## Test the Configuration

1. Log in to the Password Safe web portal using the user account that you created.
2. Enter **1** to receive the passcode in a text message.
3. Retrieve the passcode from your mobile device.
4. Enter the passcode on the Password Safe web portal login page, and then click **Login**.
5. Test other login methods.



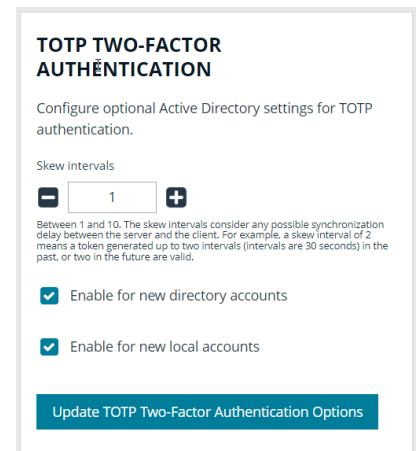
**Note:** For the push method (4), increase the timeout to **30 seconds**.

# Configure TOTP Two-Factor Authentication for BeyondInsight and Password Safe

BeyondTrust supports two-factor authentication options using a time-based one-time password (TOTP). TOTP integrates with two-factor authentication apps. The end user must install one of these apps, such as Google Authenticator or Microsoft Authenticator, to register their device. As part of the configuration process, the user must register this two-factor app with BeyondTrust. The below sections detail how to configure TOTP two-factor authentication settings, apply TOTP authentication to user accounts in BeyondInsight, and how to register their authenticator app device with BeyondTrust.

## Configure TOTP Two-Factor Authentication Settings

1. In BeyondInsight, navigate to **Configuration > Authentication Management > Authentication Options**.
2. Under **TOTP Two-Factor Authentication**, set the following:
  - **Skew Intervals:** Considers how many prior tokens are valid and accepted. You can increase this value from the default if a lag is anticipated in the synchronization between the server and client.
  - **Enable for new directory accounts**
  - **Enable for new local accounts**
3. Click **Update TOTP Two-Factor Authentication Options**.



## Set TOTP Two-Factor Authentication on User Accounts

The type of two-factor authentication can be set on a user account when a new user is created or when editing an existing user account. You can enable TOTP two-factor authentication for all new users from **Authentication Options > TOTP Two-Factor Authentication** settings, as indicated in the above section.

1. In BeyondInsight, navigate to **Configuration > Role Based Access > User Management > Users**.
2. To create a new user, click **Create New User**. To edit an existing user, click the vertical ellipsis for the account and select **Edit User Details**.

3. At the bottom of the user account settings, select **TOTP** from the **Two-Factor Authentication** list.

### Create New User ➤

**Identification**

First Name

Last Name

Email

Username

New Password  Show

Confirm New Password  Show

**Contact Information**

Work Phone

Home Phone

Mobile Phone

**User Status**

Activation Date

Expiration Date

User Active

Account Locked

Account Quarantined

**Authentication Options** ?

Override Smart Card User Principal Name

Disable Forms Login

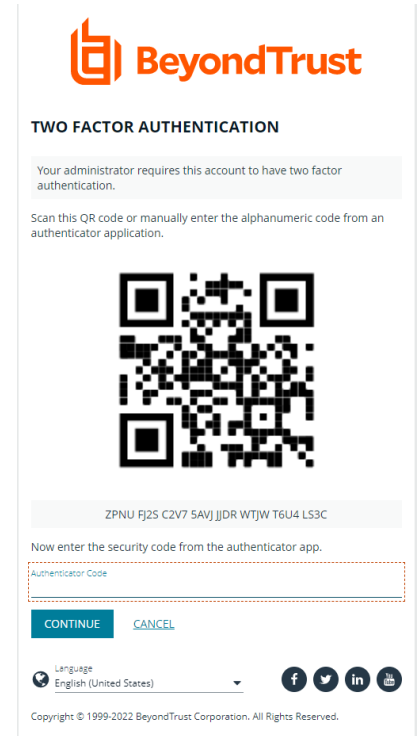
Two-Factor Authentication

Create User Discard

## Register an Authenticator Application Device

The first time a new user logs in, they must register their device with an authenticator app, as follows.

1. Download an authenticator app.
2. Scan the QR code or manually enter the alphanumeric code into the authenticator app. Once the code is detected, the app generates a 6-digit authenticator code.
3. Enter the code into the **Authenticator Code** field, and then click **Continue**. This activates the user's device.
4. Click **Continue**, and then enter login credentials.
5. Enter 6-digit code again.
6. Click **Submit**.



**Note:** The authenticator app generates a new code roughly every 30 seconds.

## Unregister an Authenticator Application Device

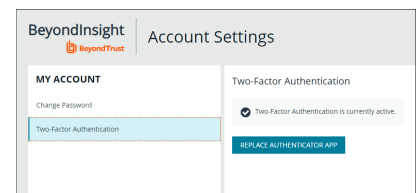
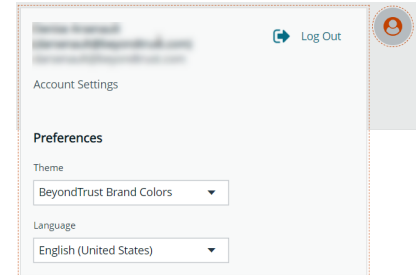
Administrators can unregister a device by removing it from a user account. Users can remove a device from their own account only.

### Steps for Administrators

1. Navigate to **Configuration > Role Based Access > User Management > User**
2. Find the user and click the vertical ellipsis for the user.
3. Select **Edit User Details**.
4. Scroll to the bottom of the user's details, and under **Two-Factor Authentication**, click **Remove Device**.

## Steps for Users

1. Click the **Profile and preferences** icon in the top right corner of the BeyondInsight console.
2. Click **Account Settings**.
3. Select **Two-Factor Authentication**.
4. Click **Replace Authenticator App**.
5. To register the app again, click **Reconfigure Authenticator App**.



**Note:** Users may not enable both RADIUS and TOTP. Only one two-factor authentication type may be selected.

# Configure Smart Card Authentication for BeyondInsight and Password Safe

Smart cards can be used for authentication when logging into BeyondInsight and Password Safe. Your network must already be configured to use smart card technology to use this feature.

This section is written with the understanding that you have a working knowledge of PKI, certificate-based authentication, and IIS.

In BeyondInsight, you must first enable smart card two-factor authentication configuration settings, and then enable the **Override Smart Card User Principal Name** authentication option for the user accounts, as detailed below.

## Enable Smart Card Two-Factor Authentication in BeyondInsight

1. Navigate to **Configuration > Authentication Management > Smart Card two-factor authentication**.
2. Click the toggle to **Enable Smart Cards**.
3. Click the toggle to enable the **Allow UPN Override On User** option. This enables a BeyondInsight user with a smart card that has a different Subject Alternative Name to log into BeyondInsight and maps the smart card to the user.
4. Click **Update Smart Card Authentication**.

## Enable Override Smart Card User Principal Name on User Accounts

You must enable the **Override Smart Card User Principal Name** setting for the user accounts that use smart cards to authenticate and provide the **User Principal Name**. This authentication option allows a BeyondInsight user with a smart card that has a different Subject Alternative Name to log into BeyondInsight, and maps the smart card to the user. When creating a new user or editing an existing one, set this option under **Authentication Options**.

### Edit User ➤

[View User Details...](#)

**Identification**

First Name

Last Name

Email

Username

[Change Password](#)

**Contact Information**

Work Phone

Home Phone

Mobile Phone

**User Status**

Activation Date

Expiration Date

User Active

Account Locked

Account Quarantined

**Authentication Options ?**

**Override Smart Card User Principal Name**

User Principal Name

Disable Forms Login

Two-Factor Authentication

[Update User](#) [Discard](#)

## Disable Forms Login

In environments where SAML, smart card, or claims-aware is configured, we recommend enabling the **Disable Forms Login** authentication option to disallow users from using the standard login form in BeyondInsight.

To disable forms login for existing users, enable this option directly on a user account as follows:

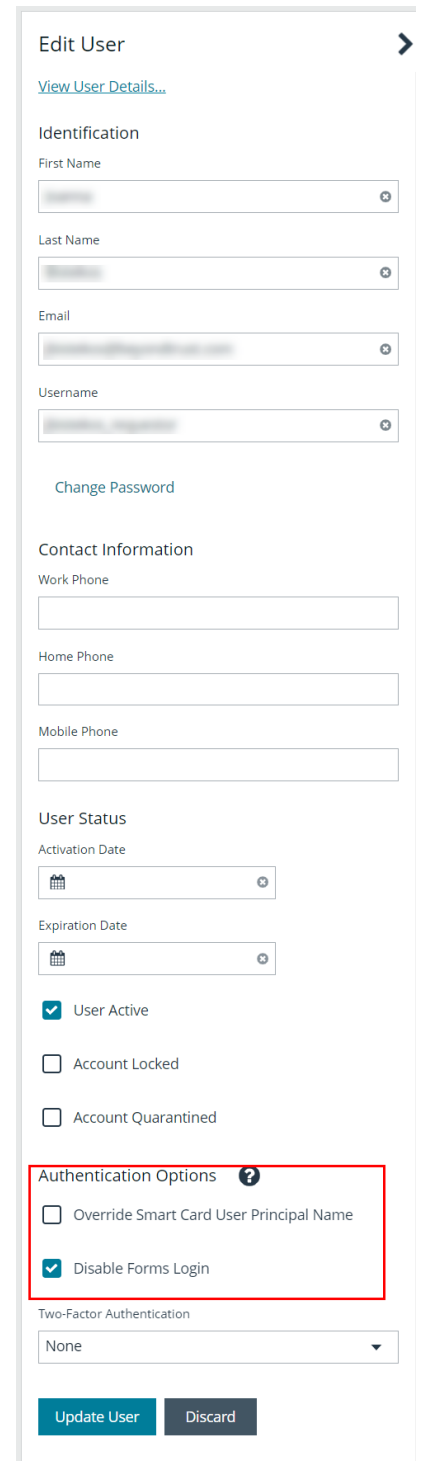
1. Click the vertical ellipsis for the user account, and then click **Edit User Details**.



2. Under **Authentication Options**, check **Disable Forms Login** to enable the option.



**Note:** Please contact BeyondTrust Support for assistance if you need to bulk-apply this setting to existing accounts.



**Edit User** ➤

[View User Details...](#)

**Identification**

First Name

Last Name

Email

Username

[Change Password](#)

**Contact Information**

Work Phone

Home Phone

Mobile Phone

**User Status**

Activation Date

Expiration Date

User Active

Account Locked

Account Quarantined

**Authentication Options** ?

Override Smart Card User Principal Name

Disable Forms Login

**Two-Factor Authentication**

None ▼

[Update User](#) [Discard](#)

To disable forms login globally for newly created directory accounts:

1. Navigate to **Configuration > Authentication Management > Authentication Options**.

- Under **Forms Login Options**, check the **Disable Forms Login for new directory accounts** option to enable it.

#### FORMS LOGIN OPTIONS

Disable Forms Login should only be used in environments where SAML, Smart Card or Claims-aware is configured. Turning this option on will disallow users from using the standard login form in BeyondInsight.

Disable Forms Login for new directory accounts

[Update Forms Login Options](#)

## Verify the BeyondInsight Server Certificate

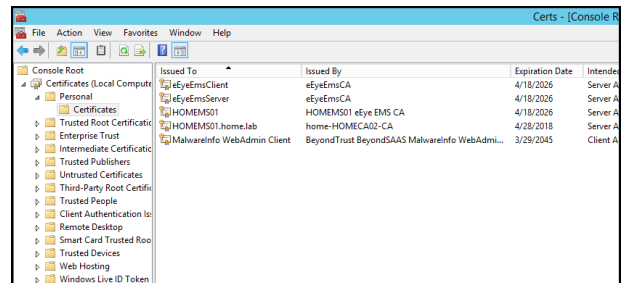
During the BeyondInsight installation, self-signed certificates are created for client and server authentication. These certificates are placed in your **Personal > Certificates** store and show as **Issued By eEyeEmsCA**.

To authenticate using smart cards, the server where BeyondInsight is running also requires a certificate issued and signed by a certificate authority (CA). Verify that your BeyondInsight server has the correct certificates issued before continuing.

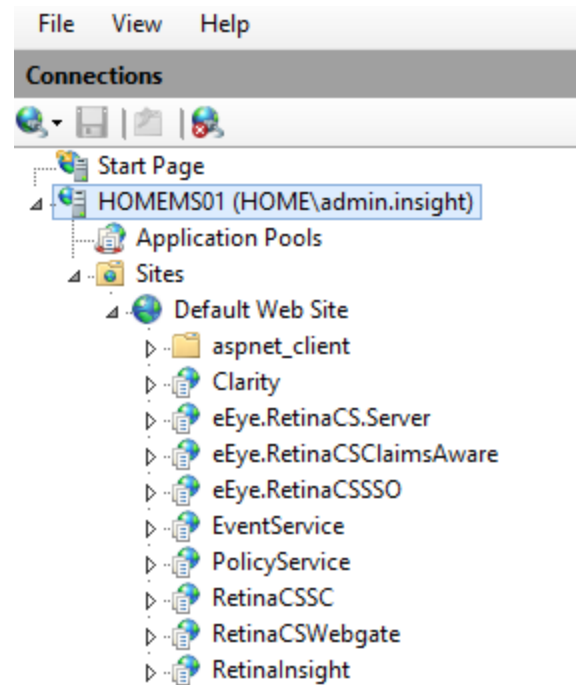
## Verify the Web Server Certificate

During the BeyondInsight installation, a self-signed web server certificate is created. This certificate must be replaced with a CA-issued certificate.

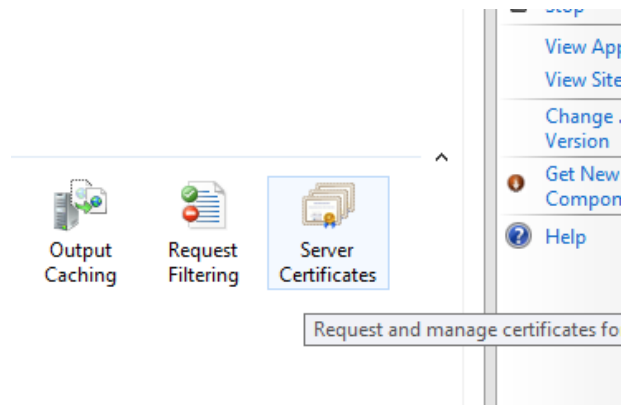
To verify you have a CA-signed certificate issued to the web server:



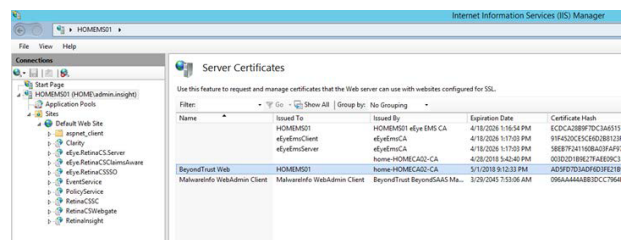
1. Open IIS.
2. Select your web server.



3. Select **Server Certificates**.



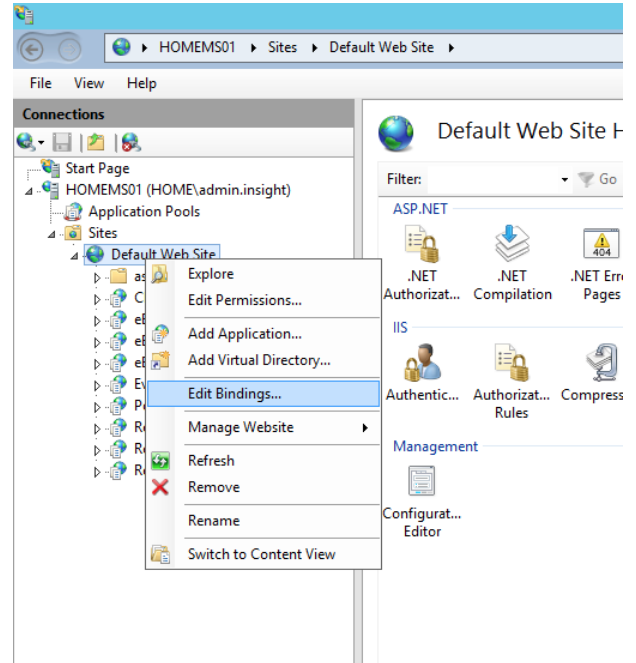
4. Verify you have a CA-issued certificate. If you do not see one listed, request one from your certificate authority.



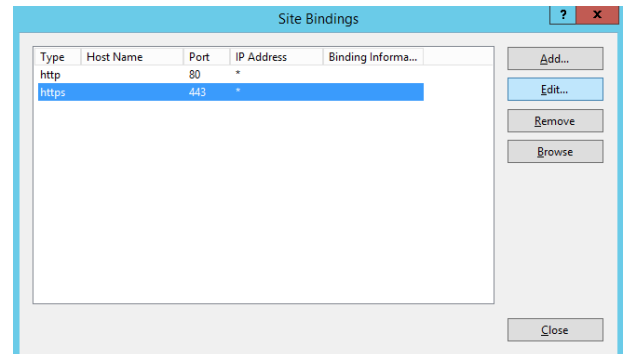
## Update Default Web Site Bindings with CA-Issued Certificate

Once you have a CA-issued certificate in place, you must edit the bindings of the **Default Web Site**, replacing the self-signed certificate.

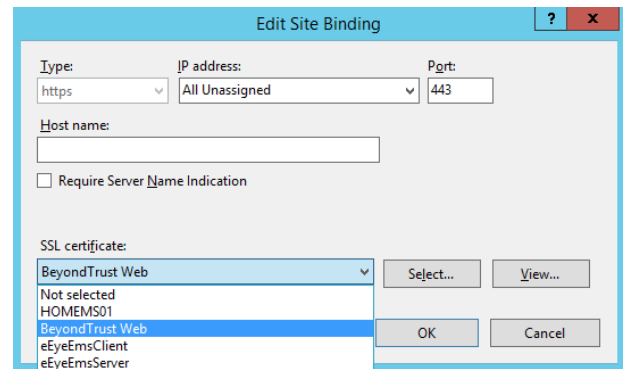
1. Open **IIS**.
2. Expand **Sites**, and then select **Default Web Site**.
3. Right-click **Default Web Site**, and then select **Edit Bindings**.



4. Select **https**, and then click **Edit**.



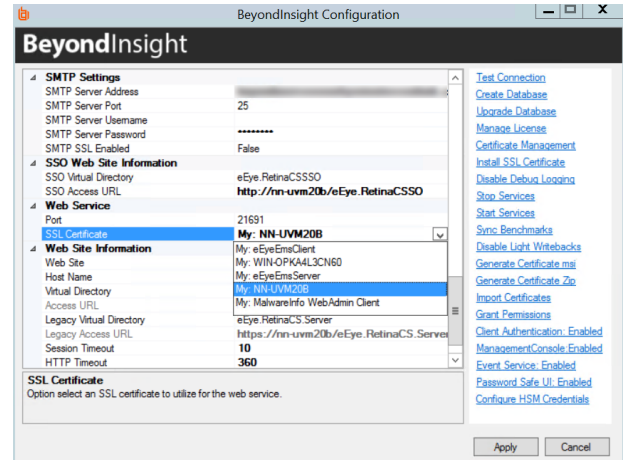
5. Select the issued domain certificate in the **SSL certificate** list, and then click **OK**.



## Update SSL Certificate in BeyondInsight Configuration Tool

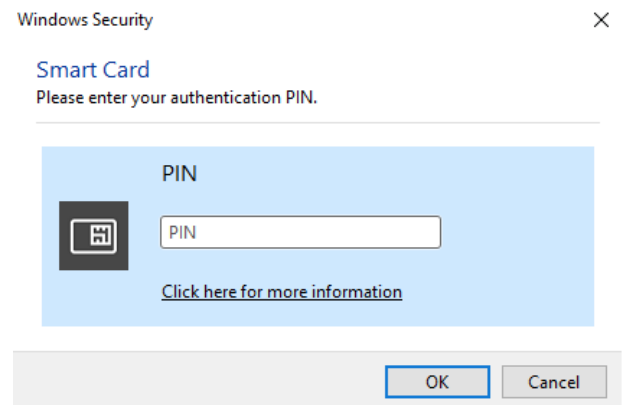
The next step is to change the domain issued certificate in the BeyondInsight Configuration tool.

1. Open the BeyondInsight Configuration tool. The default path is: **C:\Program Files (x86)\eEye Digital Security\Retina CS\REMEMConfig.exe.**
2. Scroll to **Web Service.**
3. From the **SSL Certificate** menu, select the **Domain Issued** certificate.
4. Click **Apply.**



## Log In to BeyondInsight and Password Safe Using a Smart Card

With the correct certificates now applied, you can now open the BeyondInsight Console or go to **https://<servername>/RetinaCSSC**, where you are prompted to select your certificate and enter your pin. You are logged in using a secure encrypted connection.



## Configure Two-Factor Authentication Settings for User Accounts

Two-factor authentication can be configured for Local, Active Directory, and LDAP user accounts as follows:

1. Navigate to **Configuration > Role Based Access > User Management > Users.**
1. Click the vertical ellipsis for the user account, and then select **Edit User Details.**
2. On the **Edit User** page, select **RADIUS** from the **Two Factor Authentication** list.
3. From the **Map Two Factor User** list, select one of the options listed. The user type selected maps to a user on the RADIUS server. The options displayed in the list change depending on the user logging in.

- **Local BeyondInsight Users options:**
  - **As Logged in:** Use the BeyondInsight user account login.
  - **Manually Specified:** Enter the username the user enters when logging in.
- **Active Directory and LDAP Users options:**
  - **SAM Account Name:** This is the default value.
  - **Manually Specified:** This is the username the user enters when logging in.
  - **Alternate Directory Attribute:** This is the Active Directory or LDAP attribute that you set above when configuring the RADIUS server.
  - **Distinguished Name:** This is a combination of common name and domain component.
  - **User Principal Name:** This is a combination of user account name (prefix) and DNS domain name (suffix), joined using the @ symbol.



**Note:** The information for Active Directory and LDAP user settings is retrieved from the corresponding setting in the directory for the user account logging in.

4. Click **Update User**.

## Configure a Claims-Aware Website in BeyondInsight

You can configure a claims-aware website to bypass the current BeyondInsight login page and authenticate against any configured Federated Service that uses SAML to issue claims.

The claims-aware website is configured to redirect to a defined Federation Service through the **web.config**. Upon receiving the required set of claims, the user is redirected to the existing BeyondInsight website. At that point, it is determined if the user has the appropriate group membership to log in, given the claims associated with them.

If users attempting to access BeyondInsight have group claims matching a group defined in BeyondInsight, and the group has the **Full Control** permission to the **Management Console Access** feature, the user bypasses the BeyondInsight login screen. If the user is new to BeyondInsight, they are created in the system using the same claims information. The user is also added to all groups they are not already a member of that match in BeyondInsight, and as defined in the group claim information.

If the user is not a member of at least one group defined in BeyondInsight or that group does not have the **Full Control** permission to the **Management Console Access** feature, they are redirected to the BeyondInsight login page.

## Create a BeyondInsight Group

Create a BeyondInsight group and ensure the group is assigned the **Full Control** permission to the **Management Console Access** feature.

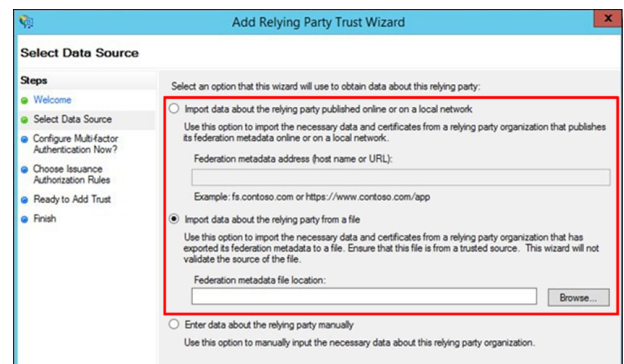
## Add Relying Party Trust

After BeyondInsight is installed, metadata is created for the claims-aware website. Use the metadata to configure the relying party trust on the Federation Services instance.

The metadata is located in the following directory:

<Install path>\eEye Digital Security\Retina CS\WebSiteClaimsAware\FederationMetadata\2007-06\

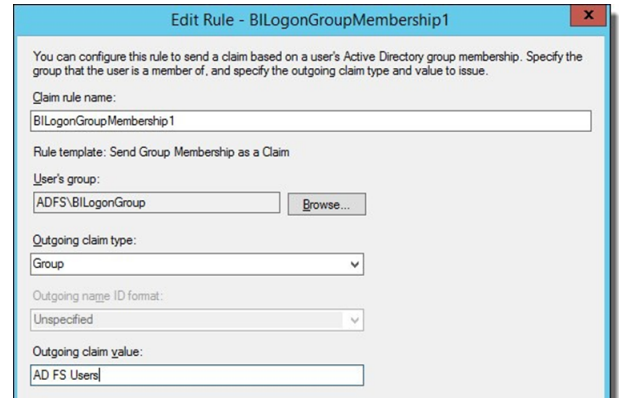
When selecting a **Data Source** in the **Add Relying Party Trust Wizard**, select the **FederationMetadata.xml** generated during the install.



## Set Up Claim Rules



**Note:** Claims rules can be defined in a number of different ways. The example provided is simply one way of pushing claims to BeyondInsight. As long as the claims rules are configured to include at least one claim of outgoing type **Group** (with **Group** claim matching exactly what is in BeyondInsight) and a single outgoing claim of type **Name**, then BeyondInsight has enough information to potentially grant access to the site to the user.



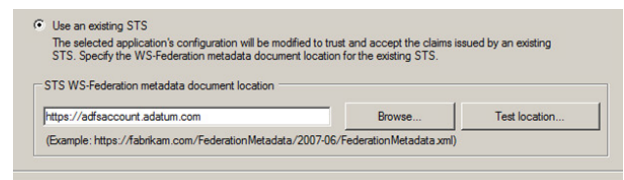
## Supported Federation Service Claim Types

Outgoing Claim Type	Outgoing Claim Type	Mapping to BeyondInsight User Detail
<a href="http://schemas.xmlsoap.org/claims/Group">http://schemas.xmlsoap.org/claims/Group</a>	Required	Group membership
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name</a>	Required	User name
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname</a>	Optional	Surname
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname</a>	Optional	First name
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress</a>	Optional	Email address

## Claims-Aware SAML

The following procedure demonstrates how to set up a claims-aware website using the Windows Identity Foundation (WIF) SDK.

1. Start the **Windows Identity Foundation Federation Utility**.
2. On the **Welcome** page, browse to and select the **web.config** file for **BeyondInsight Claims Aware** site. The application URI automatically populates.
3. Click **Next**.
4. Select **Using an existing STS**.
5. Enter **Root URL of Claims Issuer or STS**.
6. Select **Test location**. **FederationMetadata.xml** is downloaded.
7. Click **Next**.
8. Select a STS signing certificate option, and then click **Next**.
9. Select an encryption option, and then click **Next**.





10. Select the appropriate claims, and then click **Next**.
11. Review the settings on the **Summary** page, and then click **Finish**.

## Disable Forms Login

In environments where SAML, smart card, or claims-aware is configured, we recommend enabling the **Disable Forms Login** authentication option to disallow users from using the standard login form in BeyondInsight.

To disable forms login for existing users, enable this option directly on a user account as follows:

1. Click the vertical ellipsis for the user account, and then click **Edit User Details**.

2. Under **Authentication Options**, check **Disable Forms Login** to enable the option.



**Note:** Please contact BeyondTrust Support for assistance if you need to bulk-apply this setting to existing accounts.

### Edit User

[View User Details...](#)

**Identification**

First Name

Last Name

Email

Username

[Change Password](#)

**Contact Information**

Work Phone

Home Phone

Mobile Phone

**User Status**

Activation Date

Expiration Date

User Active

Account Locked

Account Quarantined

**Authentication Options** ?

Override Smart Card User Principal Name

Disable Forms Login

Two-Factor Authentication

[Update User](#) [Discard](#)

To disable forms login globally for newly created directory accounts:

1. Navigate to **Configuration > Authentication Management > Authentication Options**.

2. Under **Forms Login Options**, check the **Disable Forms Login for new directory accounts** option to enable it.

#### FORMS LOGIN OPTIONS

Disable Forms Login should only be used in environments where SAML, Smart Card or Claims-aware is configured. Turning this option on will disallow users from using the standard login form in BeyondInsight.

Disable Forms Login for new directory accounts

[Update Forms Login Options](#)

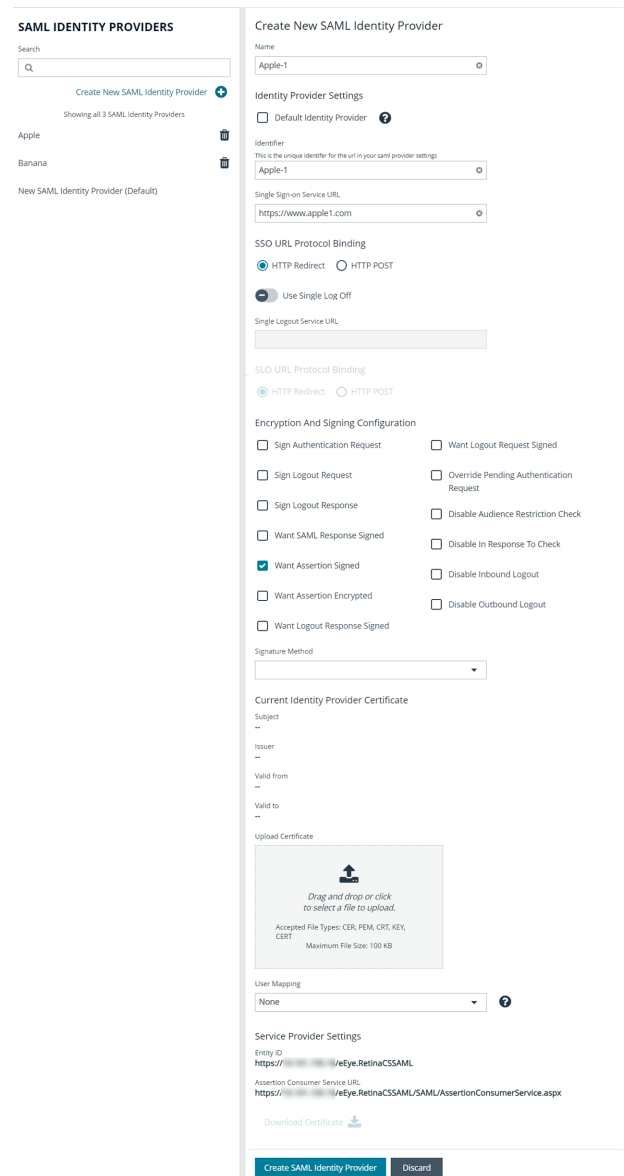
# Set Up SAML With a Generic Security Provider in BeyondInsight

The following steps show how to set up BeyondInsight with a generic security provider.

## Configure SAML in the BeyondInsight Console

To configure SAML in the BeyondInsight console, take follow the steps:

1. Navigate to **Configuration > Authentication Management > SAML Configuration**.
2. From the **SAML Identity Providers** pane, click **Create New SAML Identity Provider**.
3. Provide a name for the new SAML identity provider (IdP).
4. Complete the **Identity Provider Settings** as follows:
  - Check the **Default Identity Provider** option if you have more than one IdP for the same service provider (SP), and would like this IdP to be used as default for SP initiated logins. This is useful in the case where a user accesses the SAML site access URL without providing an IdP. Also, when a user clicks the **Use SAML Authentication** link from the BeyondInsight login page, they are redirected to the default IdP's site for authentication.
  - **Identifier:** Enter the name of the identity provider entry, normally supplied by the provider.
  - **Single Sign-on Service URL:** Provide the SSO URL, from the provider.
  - **SSO URL Protocol Binding:** Select either **HTTP Redirect** or **HTTP Post** as the type.
  - **Single Logout Service URL:** Enter the SLO URL, from the provider.
  - **SLO URL Protocol Binding:** Select either **HTTP Redirect** or **HTTP Post** as the type.
  - **Encryption and Signing Configuration:** Check applicable boxes to enable options, as required by your service provider.
  - **Signature Method:** Select the method, as is required by your IdP, from the dropdown.
  - **Current Identity Provider Certificate:** Upload the identity provider certificate.
  - **User Mapping:** Select the type of user account from the dropdown. This indicates how user claims from the SAML provider are mapped in the BeyondInsight User database.
    - **None:** This is the legacy type of mapping, which is not based on type of user.



The screenshot shows the 'SAML IDENTITY PROVIDERS' section on the left with a search bar and a list of providers including 'Apple', 'Banana', and 'New SAML Identity Provider (Default)'. The main area is titled 'Create New SAML Identity Provider' and contains the following configuration options:

- Name:** Apple-1
- Identity Provider Settings:**
  - Default Identity Provider
- Identifier:** Apple-1
- Single Sign-on Service URL:** https://www.apple1.com
- SSO URL Protocol Binding:**  HTTP Redirect  HTTP POST
- Use Single Log Off
- Single Logout Service URL:** (empty field)
- SLO URL Protocol Binding:**  HTTP Redirect  HTTP POST
- Encryption And Signing Configuration:**
  - Sign Authentication Request
  - Sign Logout Request
  - Sign Logout Response
  - Want SAML Response Signed
  - Want Assertion Signed
  - Want Assertion Encrypted
  - Want Logout Response Signed
  - Want Logout Request Signed
  - Override Pending Authentication Request
  - Disable Audience Restriction Check
  - Disable In Response To Check
  - Disable Inbound Logout
  - Disable Outbound Logout
- Signature Method:** (dropdown menu)
- Current Identity Provider Certificate:**
  - Subject: --
  - Issuer: --
  - Valid from: --
  - Valid to: --
  - Upload Certificate: Drag and drop or click to select a file to upload. Accepted File Types: CER, PEM, CRT, KEY, CERT. Maximum File Size: 100 KB.
- User Mapping:** None
- Service Provider Settings:**
  - Entity ID: https://.../eEye.RetinaCSSAML
  - Assertion Consumer Service URL: https://.../eEye.RetinaCSSAML/SAML/AssertionConsumerService.aspx
  - Download Certificate: (download icon)

Buttons at the bottom: **Create SAML Identity Provider** and **Discard**.

- **Local:** Select this option for local user account claims. BeyondInsight maps the user and group name.
  - **Azure Active Directory:** Select this option for Azure Active Directory user account claims. When selected, BeyondInsight maps the **ObjectID** attribute to the **AppUser** and **UserGroup** attributes for the user.
  - **Active Directory:** Select this option for Active Directory user account claims. If the claims are configured to pass the SID of the user and group, BeyondInsight maps the SID for the user and group, which is preferred over mapping domain name and group name attributes.
5. Click **Save SAML Identity Provider**.
  6. The following **Service Provider Settings** are auto-generated by BeyondInsight:
    - **Entity ID:** This is the fully qualified domain name, followed by the file name: **https://<serverURL>/eEye.RetinaCSSAML/**. This is used for audience restriction.
    - **Assertion Consumer Service URL:** The HTTPS endpoint on the service provider where the identity provider redirects to with its authentication response. .
  7. Click **Save SAML Configuration**.

Once the SAML configuration is saved, a public service provider certificate is available to download. It can be uploaded to the IdP, if required.

## Configure Identity Provider (IdP)

Below are some of the values an IdP may need:

- Audience Restriction: **https://<FQDN>/eEye.RetinaCSSAML/**
- SSO Service URL: **https://<FQDN>/eEye.RetinaCSSAML/SAML/AssertionConsumerService.aspx**
- SLO Service URL: **https://<FQDN>/eEye.RetinaCSSAML/SAML/SLOService.aspx**
- Service Provider Certificate: Generated when SAML configuration is saved.

Your IdP must provide the following attributes in the assertion:

- **None:**
  - **Group:** This must match the group created in BeyondInsight or imported from Active Directory / LDAP. If an Active Directory group is used, it must match the BI format of Domain\GroupName.
  - **Name:** UPN, domain\username, username or EmailAddress formats are acceptable.
  - **EmailAddress**
  - **Surname**
  - **GivenName**
- **Local:**
  - **Group:** This is the BeyondInsight groups the user must belong to and must be sent as the GroupName for each group.
  - **Name:** This is sent as the BeyondInsight username.
  - **EmailAddress**
  - **Surname**
  - **GivenName**

- **Active Directory:**
  - **SecurityIdentifier:** The user's SID.
  - **Group:** This is the BeyondInsight groups the user must belong to and must sent as the SID for each group.
  - **Name:** This is sent as UPN.
  - **EmailAddress**
  - **Surname**
  - **GivenName**
- **Azure Active Directory:**
  - **ObjectID:** The user's ObjectID. Azure includes this with the assertion by default.
  - **Group:** This is the BeyondInsight groups the user must belong to and must be sent as the ObjectID for each group.
  - **Name:** This is sent as UPN.
  - **EmailAddress**
  - **Surname**
  - **GivenName**




**Note:** *EmailAddress, Surname, and GivenName are optional. All other attributes are required. Assertion requirements change based on the SAML mapping you choose when configuring SAML.*

## Multiple Identity Providers

If you have added multiple IdPs to your SAML configuration, users can log in to BeyondInsight / Password Safe using the following two methods:

- IdP initiated login: the user logs in to the IdP first and launches BeyondInsight / Password Safe from there.
- SP initiated login: the user accesses the SP initiated URL to log in. During SP initiated logins the user is able to specify which IdP they want to log in with; otherwise BeyondInsight / Password Safe uses the default IdP.
  - Default SAML Site Access URL: **https://<BeyondInsightURL>/eEye.RetinaCSSAML/login.aspx**
  - Specific SAML Site Access URL: **https://<BeyondInsightURL>/eEye.RetinaCSSAML/login.aspx?partnerIdP=<IdP EntityID>**

 For more information on configuring an Azure Active Directory SAML Provider, please see "[Configure Azure Active Directory SAML with BeyondInsight SAML](#)" on page 66.

## Configure SAML Using the saml.config File

In the case where you have multiple service providers, you can configure SAML manually as outlined below.

### Copy Certificates from IdP

1. Copy the **idp.cer** file you received from the IdP to the following folder on the UVM: **C:\Program Files (x86)\eEye Digital Security\Retina CS\WebSiteSAML\Certificates**.

### Generate or Obtain a Private Service Provider Certificate (sp.pfx file)

Generate your own Self Signed Certificate as follows:

1. Use PowerShell to generate a new certificate:

```
New-SelfSignedCertificate -Subject "BI SAML SP" -CertStoreLocation cert:\LocalMachine\My -
Provider "Microsoft Enhanced RSA and AES Cryptographic Provider" -HashAlgorithm SHA256 -
KeyLength 2048 -NotAfter 1/1/2050
```



**Note:** This command requires PowerShell 5.0 or later (Windows 10 or Server 2016).

2. Make note of the Thumbprint for later use, for example: **7120E0BD353429D18F9829096AB3BC9A80AF33B8**.
3. Export the public key for your certificate:

```
Export-Certificate -Cert cert:\LocalMachine\My\7120E0BD353429D18F9829096AB3BC9A80AF33B8 -
FilePath c:\certs\sp.der
```

4. Convert the certificate to base 64:

```
Certutil.exe -encode c:\certs\sp.der c:\certs\sp.cer
```

Use a certificate obtained from a Certificate Authority as follows:

Your Certificate must have the following capabilities:

- Enhanced Key Usage: Client Authentication, Server Authentication
- Key Usage: Digital Signature, Key Encipherment

Add the certificate to the Local Machine, **Personal Store** and add any Intermediate or Root certs to the proper stores if needed.

If you want to use the service provider cert from the **Certificate Store** you must grant permissions to IIS to READ the Private Key:

1. Open MMC.
2. Add the Certificate SnapIn for Local Machine.
3. Explore to **Personal/Certificates**.
4. Right-click on your Certificate that was setup for the service provider.
5. Select **All Tasks > Manage Private Keys**.
6. Add the IIS user: **IIS\_IUSRS**.

## Modify **saml.config** File

The file is located here: **C:\Program Files (x86)\eEye Digital Security\Retina CS\WebSiteSAML**.

Update the **Service Provider** section as follows:

- **Name**: Should be fully qualified domain followed by **eEye.ReintaCSSAML**. This is used for the Audience Restriction.
- **Description**: Add a description.
- **AssertionConsumerServiceUrl**: This shouldn't need to be modified.
- If you save the certificate for the SP to the certificate folder use these options:
  - **LocalCertificateFile**: Path to the certificate
  - **LocalCertificatePassword**: Password for the PFX file
- If you want to use the certificate from the cert store remove **LocalCertificateFile** and **LocalCertificatePassword** and add:
  - **LocalCertificateThumbprint**: Thumbprint of the certificate

You can remove all but your one IdP entry.

The following IdP fields must be updated to your environment settings:

- **Name**: The name of the Provider entry, normally provided by the Provider
- **SingleSignOnServiceUrl**: URL for SSO from IdP
- **SingleLogoutServiceUrl**: URL for SLO from IdP
- **PartnerCertificateFile**: Location to the public cert for the IdP

The other settings are set to what your Provider requires.

Below are some common configurations for some of the common IdPs:



## Example saml.config (this is configured for OKTA using a self signed service provider certificate)

```
<?xml version="1.0" encoding="utf-8"?>
<SAMLConfiguration xmlns="urn:componentspace:SAML:2.0:configuration">
  <ServiceProvider
    Name=https://pws.mydomain.com/eEye.RetinaCSSAML/
    Description="Example Service Provider"
    AssertionConsumerServiceUrl="~/SAML/AssertionConsumerService.aspx">
    <LocalCertificates>
      <Certificate
        Thumbprint="05552BAF3B8BC9675C94EDB885D4B821F3DC15DE" />
    </LocalCertificates>
  </ServiceProvider>
  <PartnerIdentityProviders>
    <PartnerIdentityProvider
      Name=http://www.okta.com/exkldg5hqz3LbpBIj5d7
      Description="ADFS"
      SignAuthnRequest="false"
      SignLogoutRequest="false"
      WantSAMLResponseSigned="false"
      WantAssertionSigned="false"
      WantAssertionEncrypted="false"
      WantLogoutResponseSigned="false"
      SingleSignOnServiceBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      SingleSignOnServiceUrl=https://dev-25872691.okta.com/app/dev-25872691_bi212_1/exkldg5hqz3LbpBIj5d7/sso/saml
      SingleLogoutServiceBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      SingleLogoutServiceUrl=https://dev-25872691.okta.com/app/dev-25872691_bi212_1/exkldg5hqz3LbpBIj5d7/slo/saml>
      <PartnerCertificates>
        <Certificate
          FileName="Certificates\okta.cer" />
      </PartnerCertificates>
    </PartnerIdentityProvider>
  </PartnerIdentityProviders>
</SAMLConfiguration>
```

## Update Host Name and SAML access URL



**Note:** The below steps are applicable for on-premises installations only. Access URLs can also be set from the configuration area in the BeyondInsight console for both PS Cloud and on-premises installations by navigating to **Configuration > Authentication Management > Single sign on site access urls**.

1. Open the BeyondInsight Configuration Tool.
2. Scroll Down to **SAML Access URL**.
3. Update it to the fully qualified domain, followed by the file name:

**https://<FQDN>/eEye.RetinaCSSAML/**

4. Scroll down to the **Host Name** field under the **Web Site Information** section.
5. Update it to the fully qualified domain, for example, **bidev.shines.test.cloud**.
6. Click **Apply**.



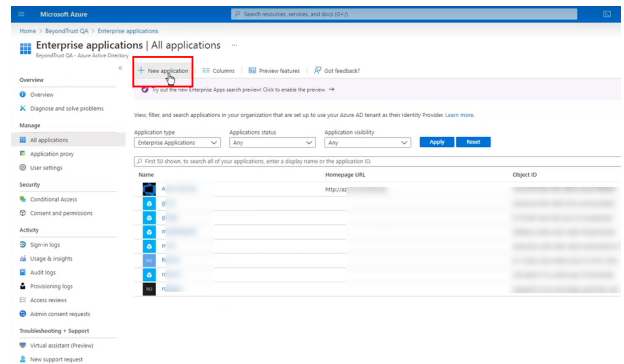
**Note:** The host name is the fully qualified domain name used to access BI/PS. If this is a load-balanced instance, the host name is the same on all servers.

## Configure Azure Active Directory SAML with BeyondInsight SAML

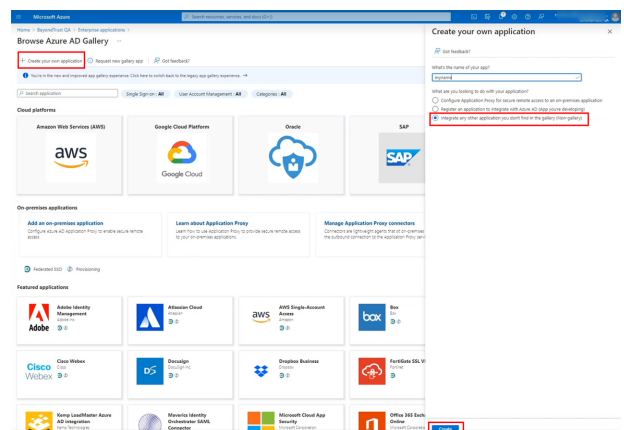
You can integrate Azure Active Directory (Azure AD) SAML with BeyondInsight SAML so that when BeyondInsight receives claims from Azure AD, it can enumerate groups for the user directly from Azure AD using the Group ID value in the claim. This allows an Azure AD user to log in to BeyondInsight using SAML authentication when the user account does not yet exist in the BeyondInsight User database. BeyondInsight adds the user to its database automatically upon successful Azure AD group enumeration and authentication into BeyondInsight.

To configure the integration between Azure AD SAML and BeyondInsight SAML, log in to your Azure AD tenant and follow the instructions below to add a new enterprise application to host the SAML configuration for BeyondInsight:

1. In Azure, navigate to **Enterprise Applications**, and then click + **New Application**.

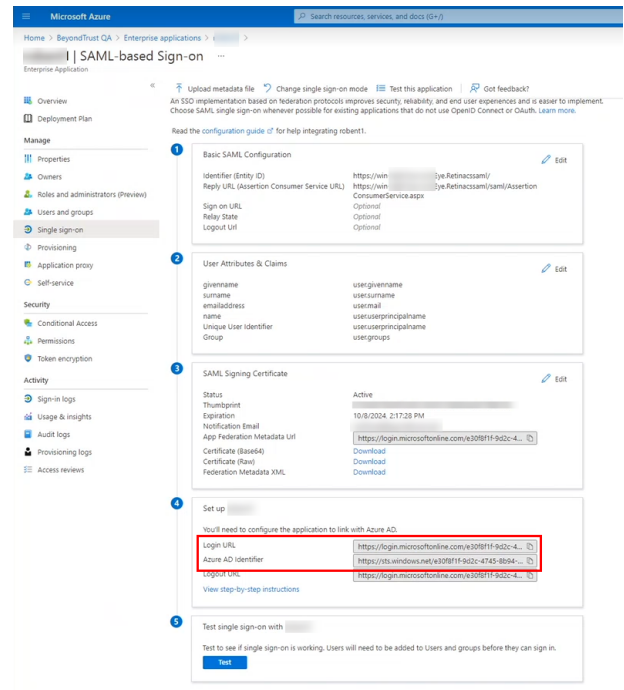


2. Click + **Create your own application**.
3. Provide a name.
4. Select the **Integrate any other application you don't find in the gallery (Non-gallery)** option.
5. Click **Create**.

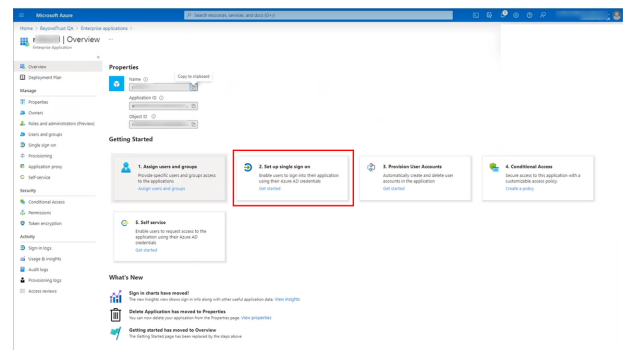


6. In the BeyondInsight console, create a new SAML identity provider. To complete the SAML IdP config in BeyondInsight, use the following information from the enterprise application you just created:

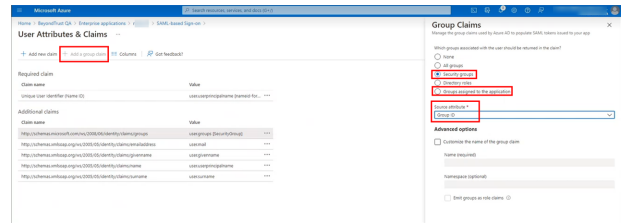
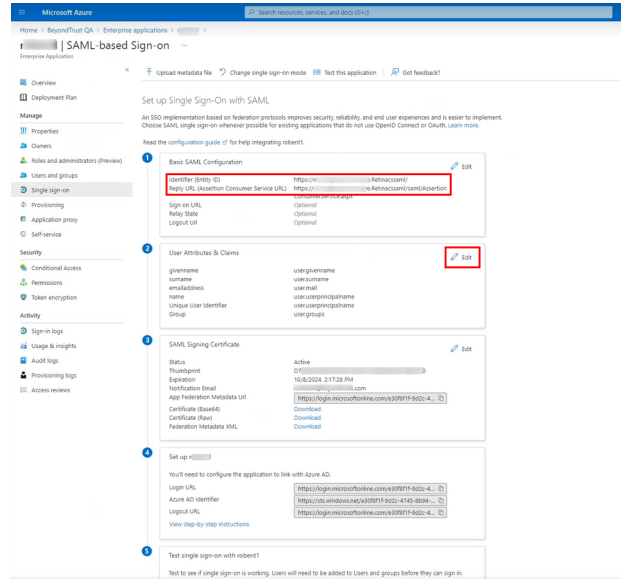
- In Azure, go to the **SAML-based Sign-on** configuration page for the application.
- In the **Set up <application name>** section, copy the **Login URL** and the **Azure AD Identifier** and save them.
- Paste them into the **Identifier, Single Sign-on Service URL, and Single Logout Service URL** fields in the BeyondInsight SAML IdP configuration.



7. In Azure, open the **Properties** for the newly created enterprise application.
8. From the **Getting Started** section, click **Set up single sign-on**.



9. In the **Basic SAML Configuration** section, provide the **Identifier (Entity ID)** and **Reply URL (Assertion Consumer Service URL)** obtained from the SAML IdP you just created in BeyondInsight.
10. In the **User Attributes & Claims** section, click **Edit** to add the group claim.
11. Click **+ Add a group claim**.
12. In the **Group Claims** section:
  - Select which groups associated with the user to return in the claim: either **Groups assigned to the application** or **Security Groups**.
  - Select **Group ID** from the **Source attribute**.



**Note:** If user accounts are configured in Okta, ensure **GivenName**, **Surname**, and **Email** attributes are set for user accounts in Okta. When these attributes are not set, the user's name and email do not display in the user's profile for the logged in user in BeyondInsight. If these attributes are set after the user has logged into BeyondInsight and log back in, to see their name and email in their user profile.

**i** For more information on configuring a SAML IdP in BeyondInsight, please see "[Configure SAML in the BeyondInsight Console](#)" on page 60.

## Disable Forms Login

In environments where SAML, smart card, or claims-aware is configured, we recommend enabling the **Disable Forms Login** authentication option to disallow users from using the standard login form in BeyondInsight.

To disable forms login for existing users, enable this option directly on a user account as follows:

1. Click the vertical ellipsis for the user account, and then click **Edit User Details**.

2. Under **Authentication Options**, check **Disable Forms Login** to enable the option.



**Note:** Please contact BeyondTrust Support for assistance if you need to bulk-apply this setting to existing accounts.

### Edit User

[View User Details...](#)

#### Identification

First Name

Last Name

Email

Username

[Change Password](#)

#### Contact Information

Work Phone

Home Phone

Mobile Phone

#### User Status

Activation Date

Expiration Date

User Active

Account Locked

Account Quarantined

#### Authentication Options

Override Smart Card User Principal Name

Disable Forms Login

Two-Factor Authentication

[Update User](#) [Discard](#)

To disable forms login globally for newly created directory accounts:

1. Navigate to **Configuration > Authentication Management > Authentication Options**.

2. Under **Forms Login Options**, check the **Disable Forms Login for new directory accounts** option to enable it.

**FORMS LOGIN OPTIONS**

Disable Forms Login should only be used in environments where SAML, Smart Card or Claims-aware is configured. Turning this option on will disallow users from using the standard login form in BeyondInsight.

Disable Forms Login for new directory accounts

[Update Forms Login Options](#)

# Configure SAML 2.0 for Password Safe using Azure AD App

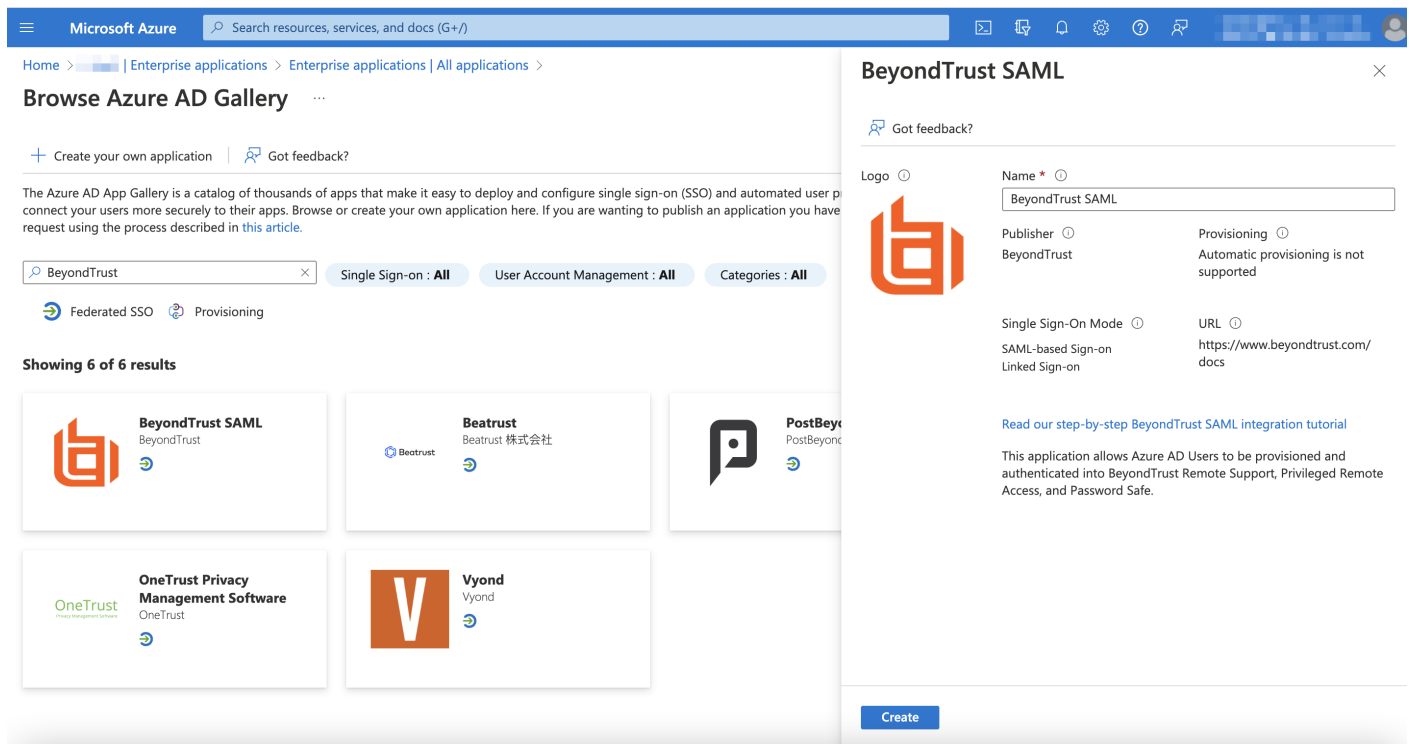
Azure Active Directory (Azure AD), part of Microsoft Entra, is an enterprise identity service that provides single sign-on, multifactor authentication, and conditional access to guard against a wide range of cybersecurity attacks.

A BeyondTrust app, available in Azure AD App Gallery, provides Single Sign-On and provisioning via SAML. This app supports Remote Support and public portals, Privileged Remote Access, Password Safe, and Password Safe Cloud.


## Install and Configure

Follow the steps below to install and configure this app.

1. Locate the BeyondTrust SAML app in Microsoft Azure AD Gallery.

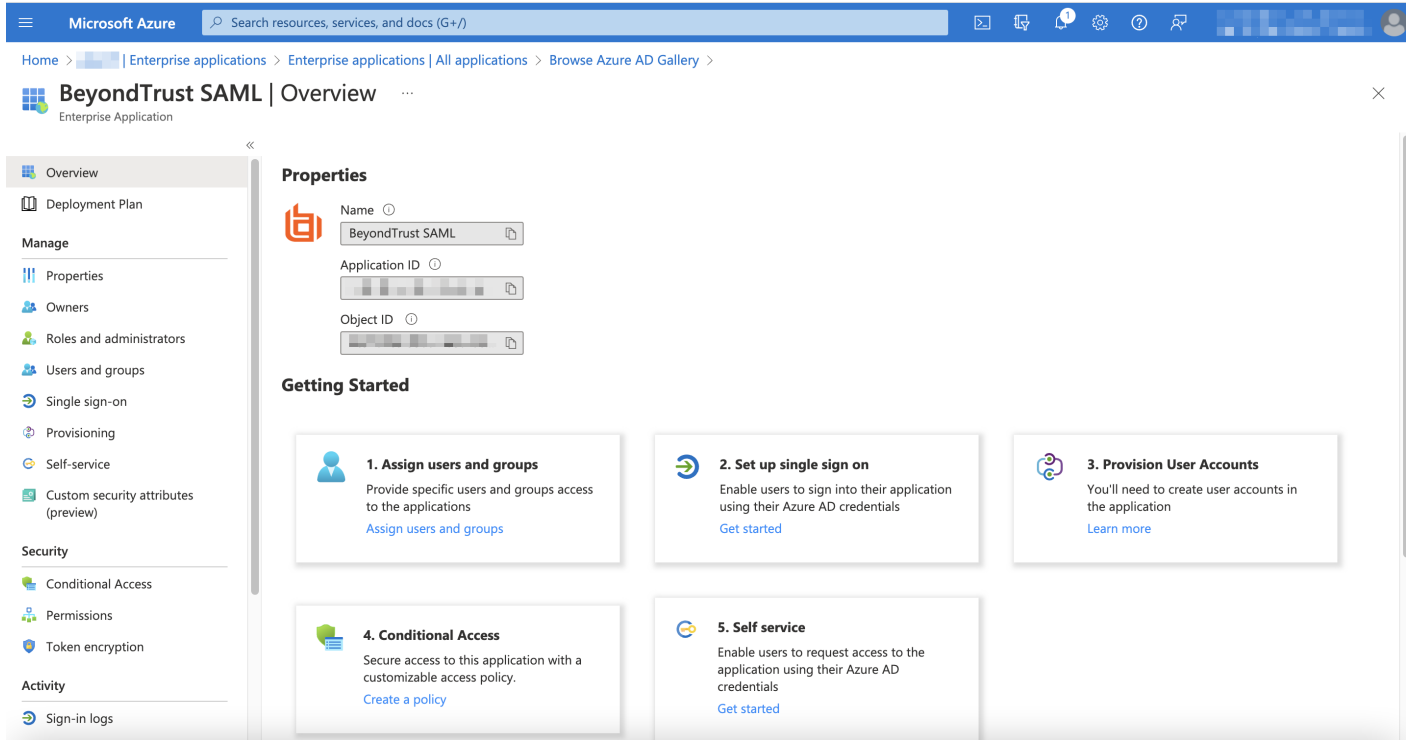


2. Change the name to your preferred descriptive name, for example, BeyondTrust SAML – Password Safe. Some screenshots below use BeyondTrust Privileged Remote Access for examples, however the process is the same for Password Safe.

 **Note:** While a single instance of the app can service multiple BeyondTrust products simultaneously, we recommend creating a separate app instance for Password Safe, if you are using that product.

3. Click **Create**.

- Information about the BeyondTrust SAML app displays when creation is completed.
- Click **Set up single sign on** under **Getting Started**.



Microsoft Azure Search resources, services, and docs (G+)

Home > Enterprise applications > Enterprise applications | All applications > Browse Azure AD Gallery >

## BeyondTrust SAML | Overview

Enterprise Application

- Overview
- Deployment Plan
- Manage
  - Properties
  - Owners
  - Roles and administrators
  - Users and groups
  - Single sign-on
  - Provisioning
  - Self-service
  - Custom security attributes (preview)
- Security
  - Conditional Access
  - Permissions
  - Token encryption
- Activity
  - Sign-in logs

### Properties

Name: BeyondTrust SAML

Application ID: [Redacted]

Object ID: [Redacted]

### Getting Started

- 1. Assign users and groups**  
Provide specific users and groups access to the applications  
[Assign users and groups](#)
- 2. Set up single sign on**  
Enable users to sign into their application using their Azure AD credentials  
[Get started](#)
- 3. Provision User Accounts**  
You'll need to create user accounts in the application  
[Learn more](#)
- 4. Conditional Access**  
Secure access to this application with a customizable access policy.  
[Create a policy](#)
- 5. Self service**  
Enable users to request access to the application using their Azure AD credentials  
[Get started](#)



- Configure Basic SAML Configuration to match your Password Safe instance. The Entity IDs are specific to the instances for each product.

**Basic SAML Configuration**

Identifier (Entity ID) \*   
The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default  
https://pra1.acme.com

Reply URL (Assertion Consumer Service URL) \*   
The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Index Default  
https://pra1.acme.com/saml/sso

Sign on URL (Optional)   
Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

Relay State (Optional)   
The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

Logout URL (Optional)   
This URL is used to send the SAML logout response back to the application.

**Attributes & Claims**

Username	user.userprincipalname
Email	user.mail
LastName	user.surname
FirstName	user.givenname
Unique User Identifier	user.userprincipalname
Group	user.groups

**SAML Certificates**

<b>Token signing certificate</b>	Active
Status	2E0327F4A9A78B2E358328E0A073EAD0978
Thumbprint	8/23/2026, 7:30:44 AM
Expiration	admin@2nlp6t.onmicrosoft.com
Notification Email	https://login.microsoftonline.com/b23838c...
App Federation Metadata Url	Download
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

**Verification certificates (optional)**

Required	No
Active	0

- Change the Unique Identifier (Name ID) to the Persistent format.

**Manage claim**

Name: nameidentifier

Namespace: http://schemas.xmlsoap.org/ws/2005/05/identity/claims

Choose name identifier format

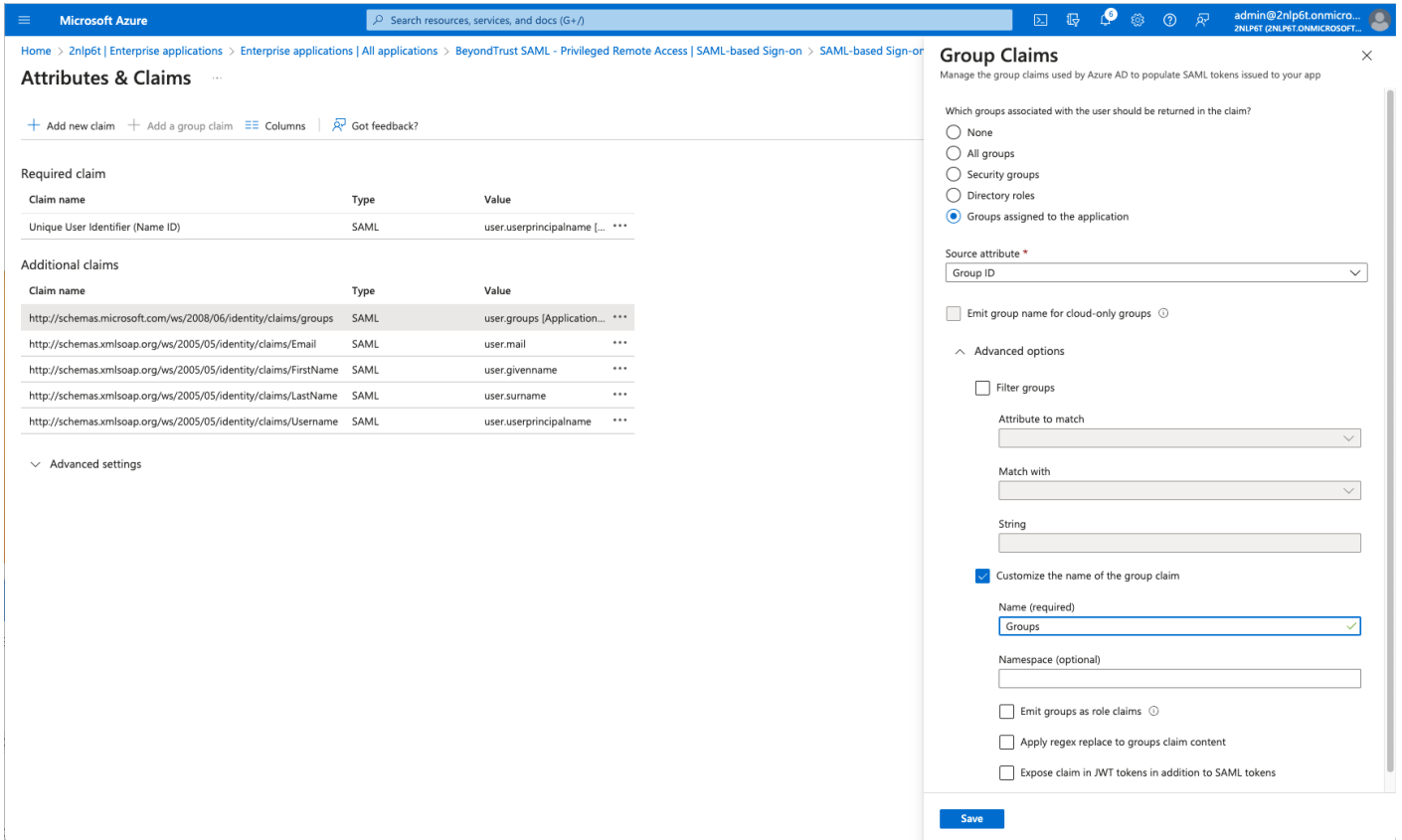
Name identifier format \*   
Persistent

Source \*   
Attribute

Source attribute \*   
user.userprincipalname

- Configure **Attributes & Claims** sources and values as shown in the table below, then add a group claim as show in the image below:

Source	Value
Username	user.principalname
FirstName	user.givenname
LastName	user.surname
Email	user.email
Group Claim	Group ID



**Attributes & Claims**

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.principalname [...]

Additional claims

Claim name	Type	Value
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	SAML	user.groups (Application...)
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/Email	SAML	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/FirstName	SAML	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/LastName	SAML	user.surname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/Username	SAML	user.principalname

**Group Claims**

Which groups associated with the user should be returned in the claim?

None  
 All groups  
 Security groups  
 Directory roles  
 Groups assigned to the application

Source attribute \*

Group ID

Emit group name for cloud-only groups

Advanced options

Filter groups

Attribute to match

Match with

String

Customize the name of the group claim


Name (required)

Groups

Namespace (optional)

Emit groups as role claims  
 Apply regex replace to groups claim content  
 Expose claim in JWT tokens in addition to SAML tokens

Save

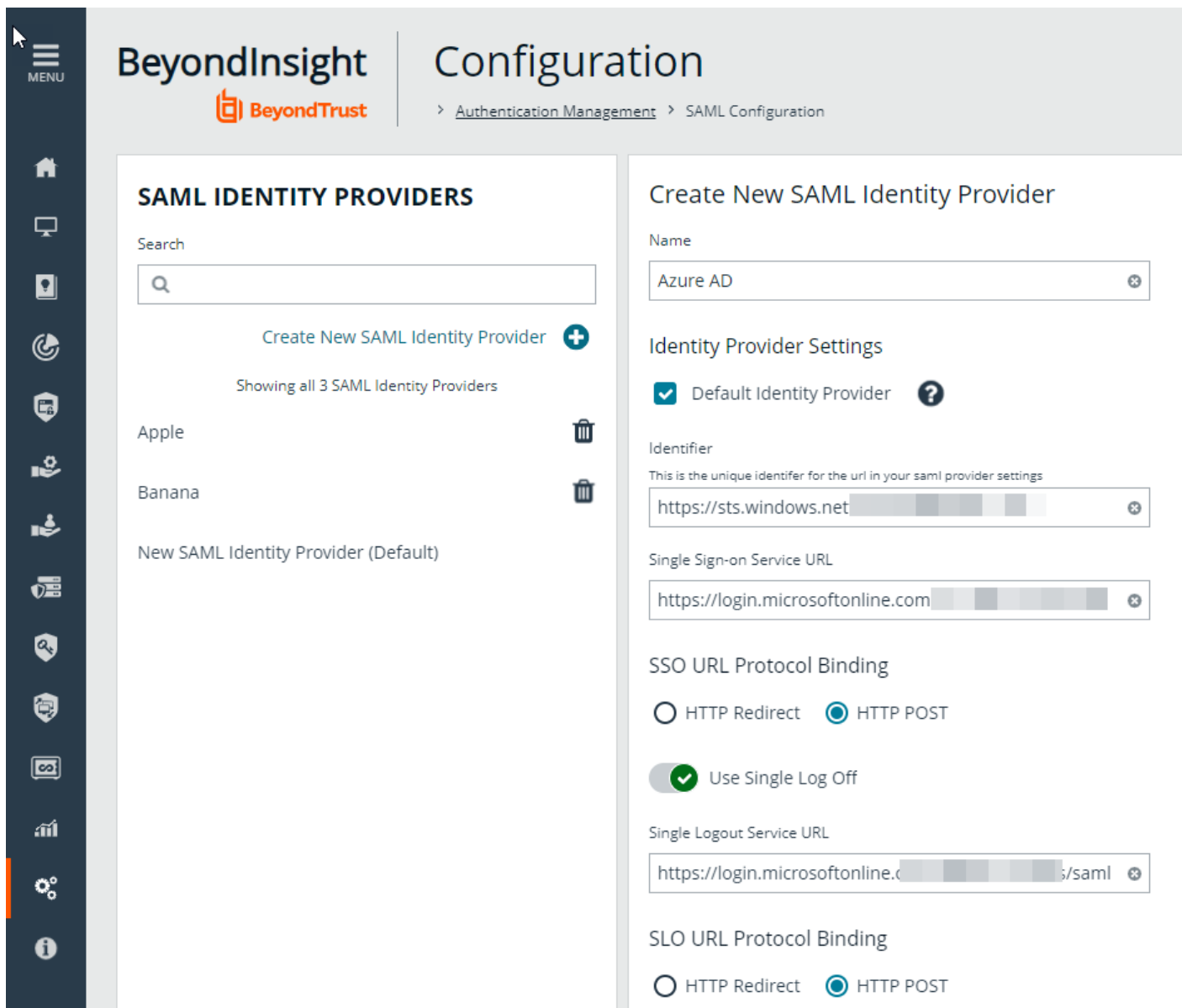
 **Note:** The group claim must be configured to use only groups assigned to the application, to prevent errors that may occur if a user belongs to more than 150 AD groups. For more information, please see [Configure group claims for applications by using Azure Active Directory](https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-fed-group-claims) at <https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-fed-group-claims>.

- Click **Edit** on the SAML certificates section.
- For **Signing Option**, select **Sign SAML response and assertion**.
- Download the Federation Metadata XML.

## Configure Password Safe to use the SAML Azure AD App

Once the app has been configured, follow these steps to add the provider to Password Safe:

1. Log in to Password Safe.
2. Navigate to **Configuration > Authentication Management > SAML Configuration**.
3. Click **Create New SAML Identity Provider**.
4. Paste the **Identifier** and **Sign-On URL** from the Azure AD app.



The screenshot shows the BeyondTrust Configuration interface. The left sidebar contains a menu with icons for Home, Settings, and other system functions. The main content area is titled "Configuration" and includes a breadcrumb trail: "Authentication Management > SAML Configuration".

The "SAML IDENTITY PROVIDERS" section on the left lists three providers: "Apple", "Banana", and "New SAML Identity Provider (Default)". A "Create New SAML Identity Provider" button is visible. The "New SAML Identity Provider (Default)" is selected, and its configuration details are shown on the right.

The "Create New SAML Identity Provider" configuration form includes the following fields and options:

- Name:** Azure AD
- Identity Provider Settings:**  Default Identity Provider
- Identifier:** https://sts.windows.net [redacted]
- Single Sign-on Service URL:** https://login.microsoftonline.com [redacted]
- SSO URL Protocol Binding:**  HTTP Redirect,  HTTP POST
- Use Single Log Off:**
- Single Logout Service URL:** https://login.microsoftonline.com [redacted]/saml
- SLO URL Protocol Binding:**  HTTP Redirect,  HTTP POST

5. Ensure **Want SAML Response Signed** and **Want Assertion Signed** match the Azure AD App selections.
6. Select the **Signature Method**.

7. Upload the certificate, using the certificate downloaded from the Azure AD App.

## Encryption And Signing Configuration

- |   |  |
|---|--|
| <input type="checkbox"/> Sign Authentication Request          | <input type="checkbox"/> Want Logout Request Signed              |
| <input type="checkbox"/> Sign Logout Request                  | <input type="checkbox"/> Override Pending Authentication Request |
| <input type="checkbox"/> Sign Logout Response                 | <input type="checkbox"/> Disable Audience Restriction Check      |
| <input checked="" type="checkbox"/> Want SAML Response Signed | <input type="checkbox"/> Disable In Response To Check            |
| <input checked="" type="checkbox"/> Want Assertion Signed     | <input type="checkbox"/> Disable Inbound Logout                  |
| <input type="checkbox"/> Want Assertion Encrypted             | <input type="checkbox"/> Disable Outbound Logout                 |
| <input type="checkbox"/> Want Logout Response Signed          |  |

Signature Method

SHA256

## Current Identity Provider Certificate

Subject

--

Issuer

--

Valid from

0001-01-01T00:00:00

Valid to

0001-01-01T00:00:00

## Upload Certificate




*Drag and drop or click  
to select a file to upload.*

Accepted File Types: CER, PEM, CRT, KEY,  
CERT

Maximum File Size: 100 KB

8. Select Azure Active Directory for **User Mapping**.
9. Click **Create SAML Identity Provider**.  
(missing or bad snippet)


User Mapping

Azure Active Directory 

Service Provider Settings

Entity ID  
[https://\[redacted\]](https://[redacted]) CSSAML

Assertion Consumer Service URL  
[https://\[redacted\]](https://[redacted]) CSSAML/SAML/AssertionConsumerService.aspx

[Download Certificate](#) 

---

[Create SAML Identity Provider](#) [Discard](#)

# Configure AD FS Authentication Using SAML for BeyondInsight and Password Safe

Active Directory Federation Services (AD FS) is Microsoft's claim based single sign-on (SSO) solution. It allows users access to integrated applications and systems using their Active Directory (AD) credentials. AD FS uses trust relationships to allow AD to issue authentication claims for transferring user identities to the requesting application. The instructions below provide detailed steps on how to configure the trust relationship in the AD FS management console and how to configure the SAML identity provider and service provider in BeyondInsight.

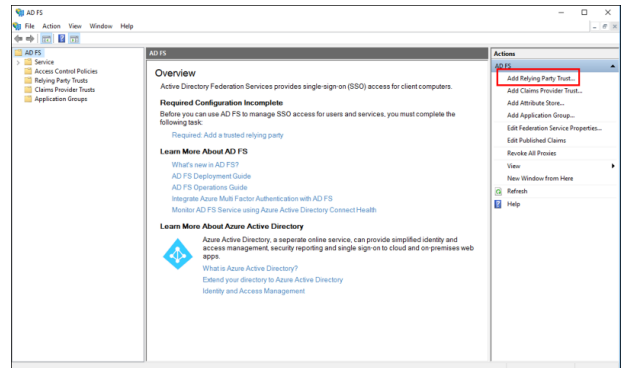
## Configure AD FS on the Identity Provider Server

Configuring AD FS on the identity provider server involves creating a relying party trust in AD FS for the BeyondInsight SAML service URL, creating a rule to send the AD group membership as a claim to the relying party, and creating a rule that selects attributes from an LDAP attribute store, such as Active Directory, to send as claims to the relying party. The sections below provide detailed steps to configure each of these in AD FS.

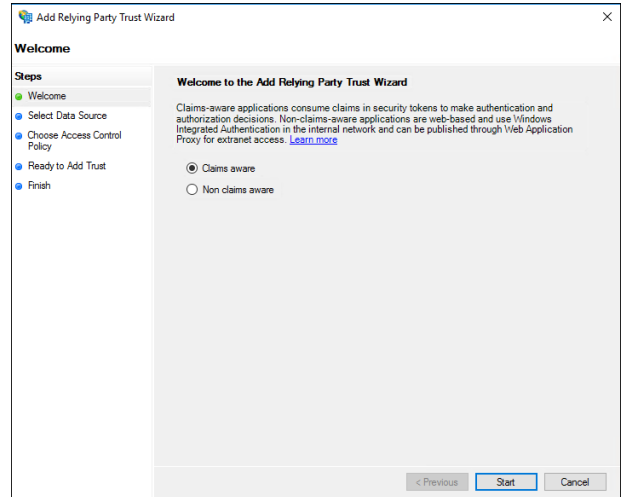
### Add a Relying Party Trust in AD FS Management

To add a relying party trust manually in AD FS on your identity provider server, follow the below steps:

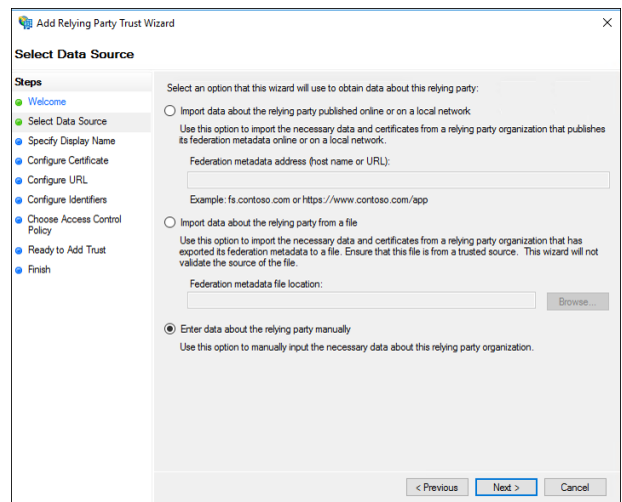
1. Log in to the identify provider server as an administrator and open Server Manager.
2. In Server Manager, click **Tools**, and then select **AD FS Management**.
3. From the **Actions** pane, click **Add Relying Party Trust**.



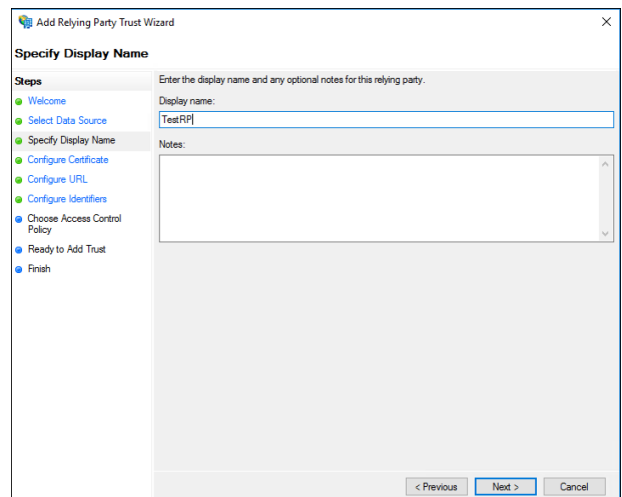
- On the **Welcome** screen, select **Claims aware**, and then click **Start**.



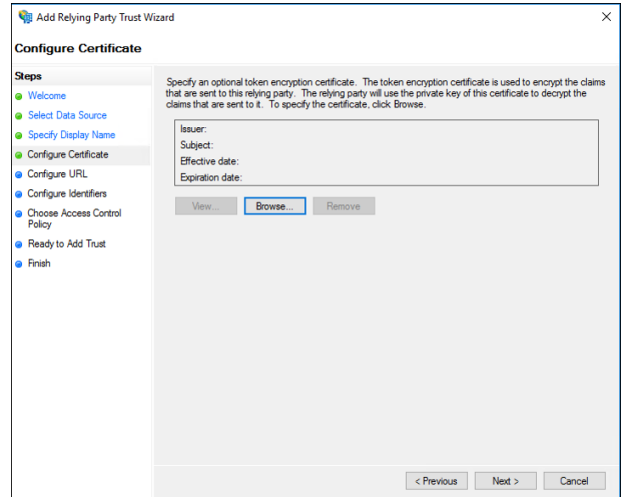
- On the **Select Data Source** screen, select **Enter data about the relying party manually**, and then click **Next**.



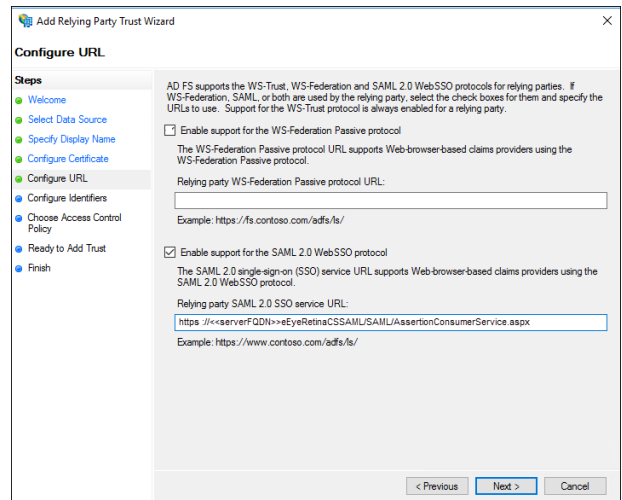
- On the **Specify Display Name** screen, enter a name in the **Display name** field. Below that, under **Notes**, provide a description for this relying party trust, and then click **Next**.



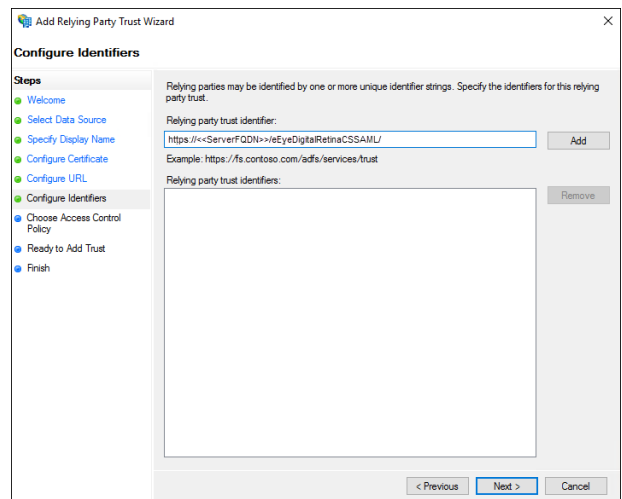
- On the **Configure Certificate** screen, click **Browse** to locate and import the service provider public certificate file, and then click **Next**.



- On the **Configure URL** screen, check **Enable support for the SAML 2.0 WebSSO protocol**, enter the **Relying party SAML 2.0 SSO service URL**, and then click **Next**.

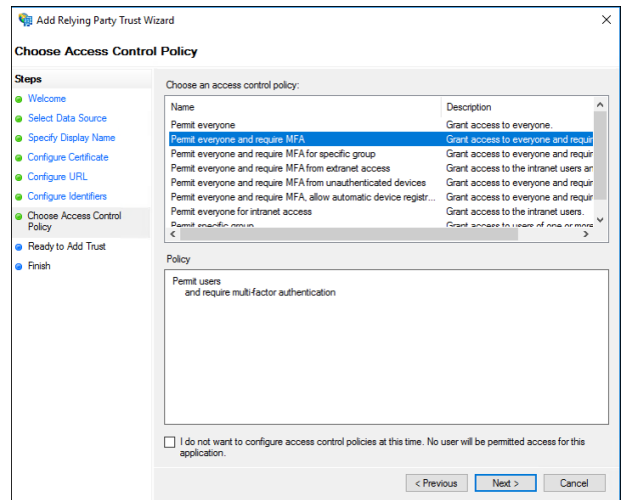


- On the **Configure Identifiers** screen, enter the **Relying party trust identifier**, click **Add**, and then click **Next**.

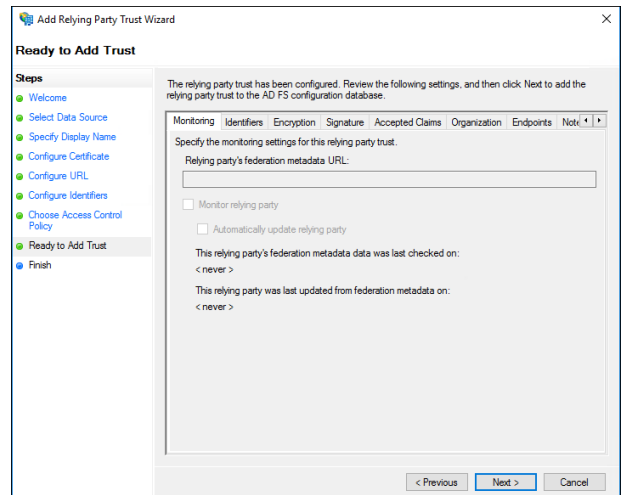




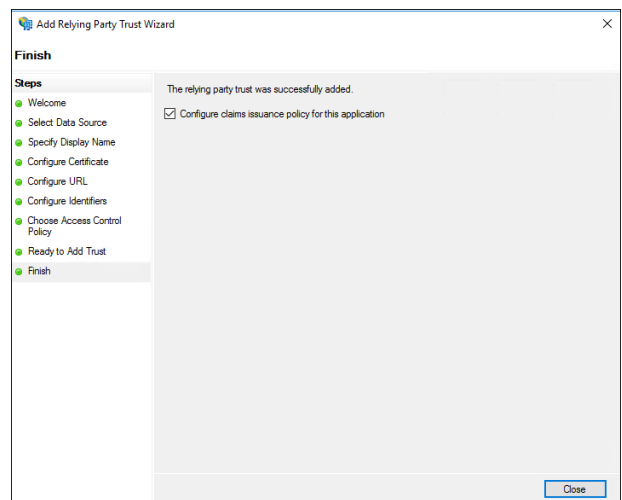
- On the **Choose Access Control Policy** screen, select a policy, and then click **Next**.



- On the **Ready to Add Trust** screen, review the settings, and then click **Next** to save your relying party trust information.



- On the **Finish** screen, click **Close**. The **Edit Claim Rules** dialog box displays.



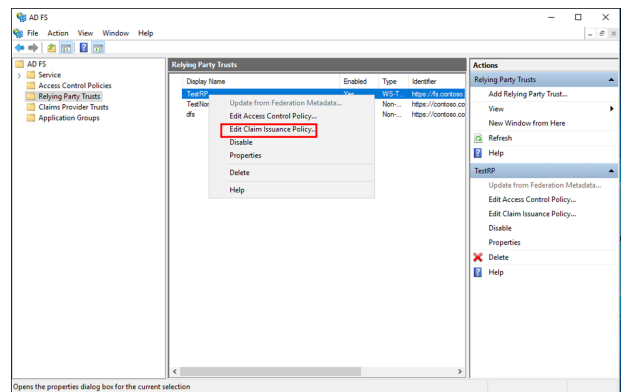
## Send LDAP Attributes as Claims

Using the **Send Claims as a Custom Rule** template in AD FS, you can create a rule to add the SID attribute to claims. Using the **Send LDAP Attributes as Claims** template allows you to select attributes from an LDAP attribute store, such as Active Directory, to send as claims to the relying party. Configuring these rules allows you to send all of the SIDs for groups as part of the claim, as well as other attributes, such as **User-Principle Name**. The steps for configuring each of these rule types is outlined in the sections below.

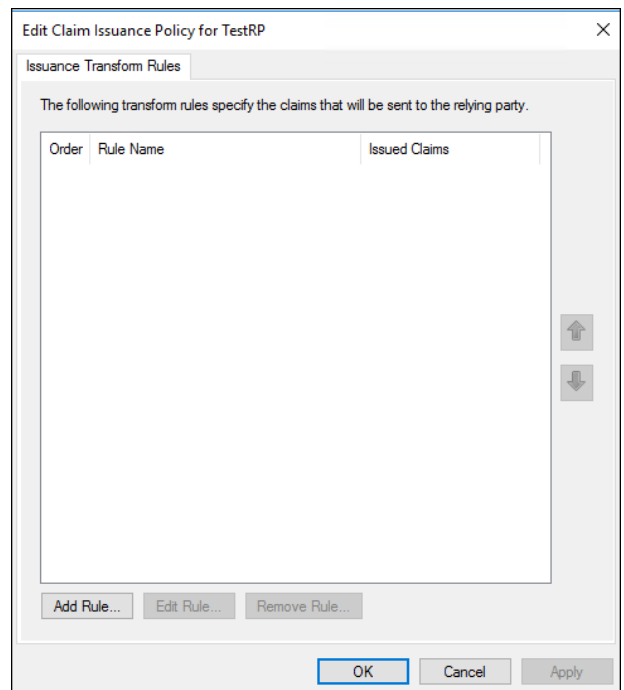
### Create Rule to Add SID Attribute

To create a custom rule to add the SID attribute to claims, follow these steps:

1. In Server Manager, click **Tools**, and then select **AD FS Management**.
2. In the AD FS navigation tree on the left, click **Relying Party Trusts**.
3. Right-click the selected trust, and then click **Edit Claim Issuance Policy**.



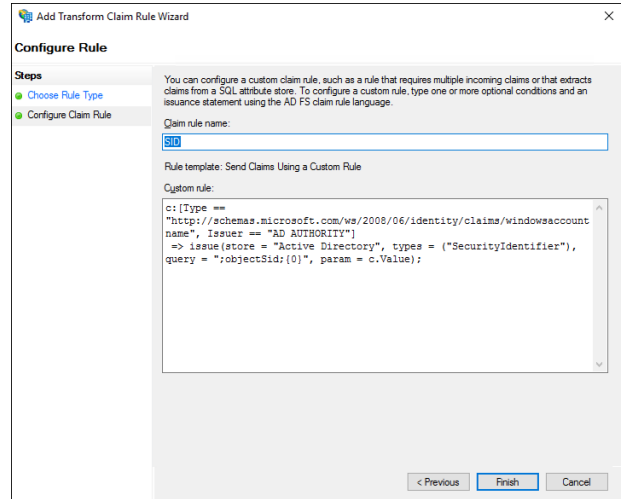
4. In the **Edit Claim Issuance Policy** dialog box, under **Issuance Transform Rules** click **Add Rule** to start the **Add Transform Claim Rule** wizard.



5. On the **Select Rule Template** screen, select **Send Claims as a Custom Rule** from the **Claim rule template** list, and then click **Next**.

- On the **Configure Rule** screen, type the display name for this rule and type the following for the **Custom rule**:

```
c:[Type==
http://schemas.microsoft.com/ws/2008/06/identity/
claims/windowsaccountname, Issuer == "AD AUTHORITY"]
=> issue(store = "Active Directory", types =
("SecurityIdentifier"), query = ";objectSid;{0}";
param = c.Value);
```

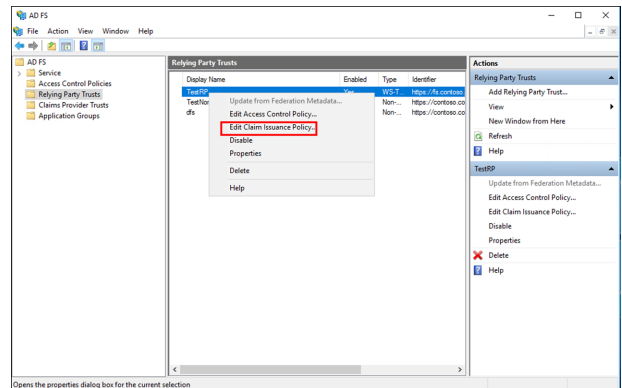


- Click **Finish**, and then click **OK** in the **Edit Claim Issuance Policy** dialog to close it and save the rule.

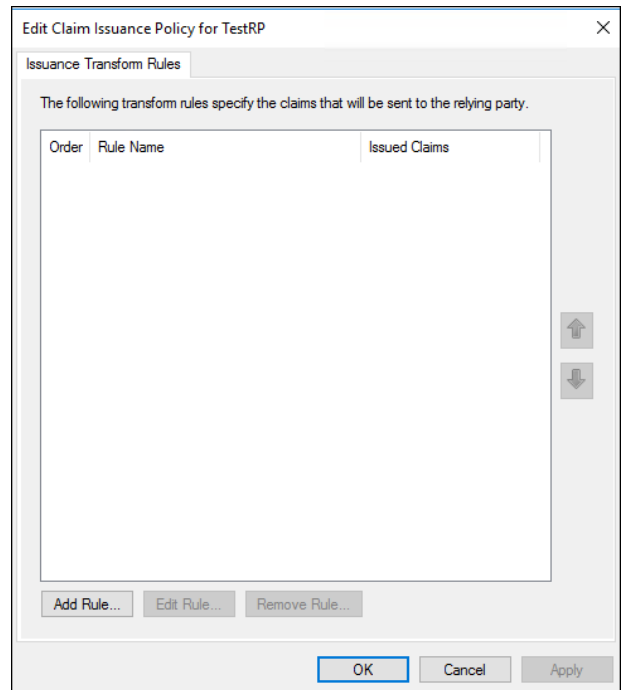
## Create Rule to Send LDAP Attributes Claims

To create a rule to send attributes from Active Directory as claims, follow these steps:

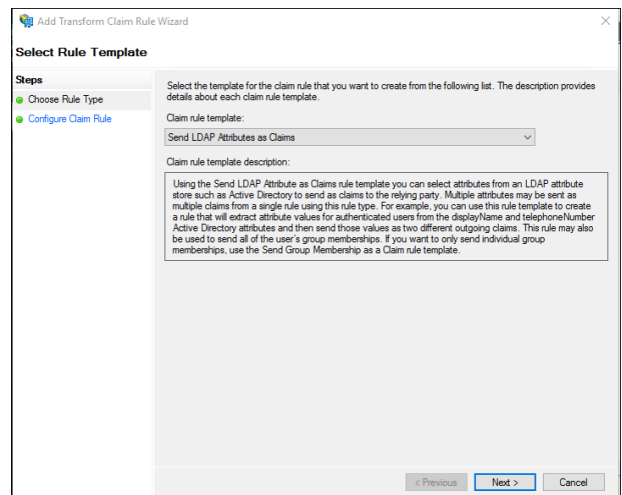
- In Server Manager, click **Tools**, and then select **AD FS Management**.
- In the AD FS navigation tree on the left, click **Relying Party Trusts**.
- Right-click the selected trust, and then click **Edit Claim Issuance Policy**.



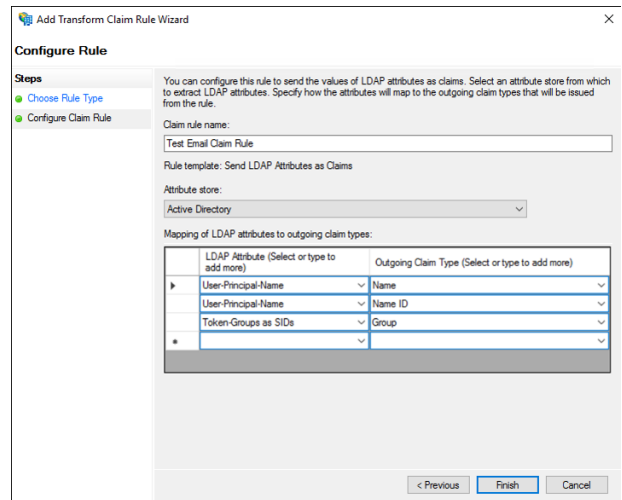
- In the **Edit Claim Issuance Policy** dialog box, under **Issuance Transform Rules** click **Add Rule** to start the **Add Transform Claim Rule** wizard.



- On the **Select Rule Template** screen, select **Send LDAP Attributes as Claims** from the **Claim rule template** list, and then click **Next**.



6. On the **Configure Rule** screen:
  - In the **Claim rule name** box, type the display name for this rule
  - For **Attribute Store**, select **Active Directory** from the list.
  - Select **User-Principal-Name** for the **LDAP Attribute** and **Name** as the **Outgoing Claim Type**.
  - Select **User-Principal-Name** for the **LDAP Attribute** and **Name ID** as the **Outgoing Claim Type**.
  - Select **Token-Groups as SIDs** for the **LDAP Attribute** and **Group** as the **Outgoing Claim Type**
  - Click **Finish**.



7. Click **OK** in the **Edit Claim Issuance Policy** dialog to close it and save the rule.
8. On the **Relying Party Trusts** page, right-click the relying party trust you had added for BeyondInsight, and then select **Properties**.
9. Click the **Signature** tab.
10. Click **Add**, and then enter the service provider public certificate.

## Configure SAML on the Service Provider Server (U-Series Appliance)

As an administrator, log in to BeyondInsight on the U-Series Appliance and follow the below instructions to configure SAML:

1. Navigate to **Configuration > Authentication Management > SAML Configuration**.

- From the **SAML Identity Providers** pane, click **Create New SAML Identity Provider**.
- Provide a name for the new SAML identity provider (IdP).
- Complete the **Identity Provider Settings** as follows:

- Check the **Default Identity Provider** option if you have more than one IdP for the same service provider (SP), and would like this IdP to be used as default for SP initiated logins. This is useful in the case where a user accesses the SAML site access URL without providing an IdP. Also, when a user clicks the **Use SAML Authentication** link from the BeyondInsight login page, they are redirected to the default IdP's site for authentication.
- Identifier:** Enter the name of the identity provider entry, normally supplied by the provider.
- Single Sign-on Service URL:** Provide the SSO URL, from the provider.
- SSO URL Protocol Binding:** Select either **HTTP Redirect** or **HTTP Post** as the type.
- Single Logout Service URL:** Enter the SLO URL, from the provider.
- SLO URL Protocol Binding:** Select either **HTTP Redirect** or **HTTP Post** as the type.
- Encryption and Signing Configuration:**

- Depending on IdP configuration, check any of the first three settings:

- **Sign Authentication Request**
- **Sign Logout Request**
- **Sign Logout Response**

- Check the appropriate service provider signing settings:

- **Want SAML Response Signed**
- **Want Assertion Signed**
- **Want Assertion Encrypted**
- **Want Logout Response Signed**
- **Want Logout Request Signed**

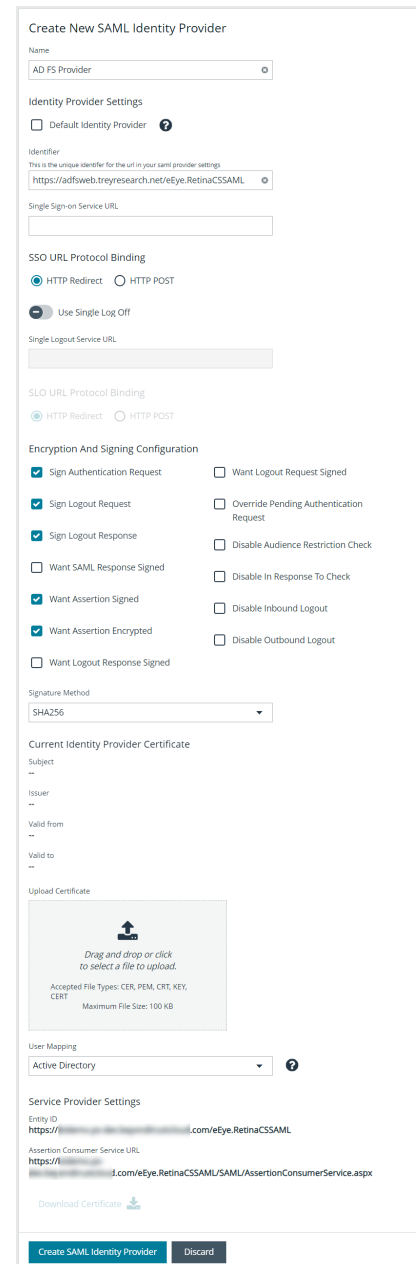
- Check any of the remaining miscellaneous settings as required.

- Signature Method:** Select the method, as is required by your IdP, from the dropdown.
- Current Identity Provider Certificate:** Upload the identity provider certificate.
- User Mapping:** Select **Active Directory** from the dropdown. This indicates how user claims from the SAML provider are mapped in the BeyondInsight User database.

- The following **Service Provider Settings** are auto-generated by BeyondInsight:

- Entity ID:** This is the fully qualified domain name, followed by the file name: **https://<serverURL>/eEye.RetinaCSSAML/**. This is used for audience restriction.
- Assertion Consumer Service URL:** The HTTPS endpoint on the service provider where the identity provider redirects to with its authentication response. .

- Click **Create SAML Identity Provider**.



Once the SAML configuration is saved, a public service provider certificate is available to download. It can be uploaded to the IdP, if required.

# Configure Okta SAML Authentication for BeyondInsight and Password Safe

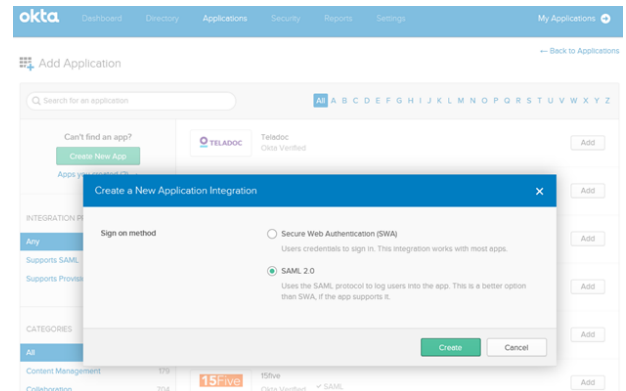
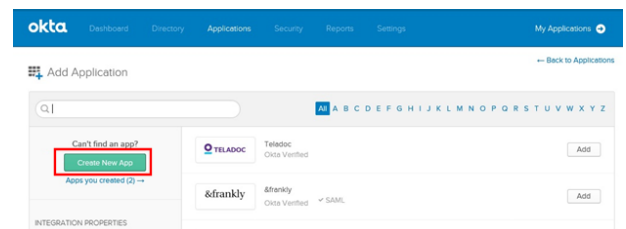
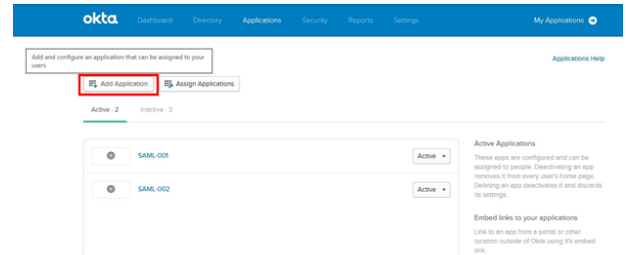
Configuring BeyondInsight and Password Safe to use Okta SAML authentication involves configuring the SAML application with BeyondInsight SAML information in the Okta admin portal and then configuring the SAML identity provider settings for Okta in the BeyondInsight console. The configuration for each of these is detailed the below sections.



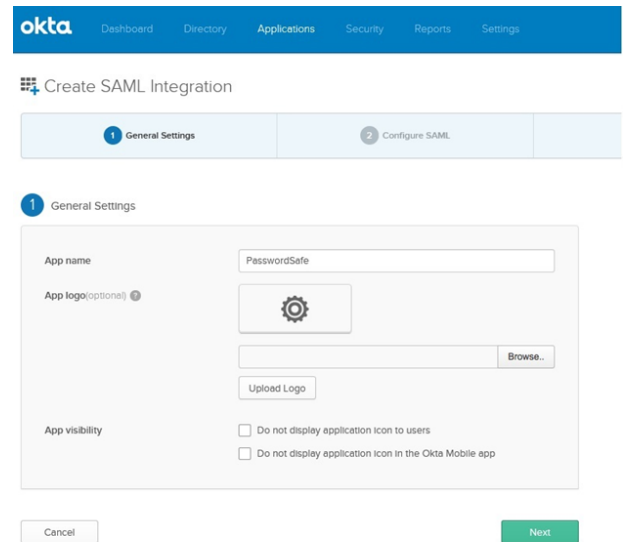
## Configure SAML Application in Okta

To configure a new SAML application for BeyondInsight and Password Safe in Okta, follow the below steps.

1. Log in to the Okta admin portal.
2. Click **Add Application**.
3. Click **Create New App**.
4. Select **SAML 2.0** as the sign-in method.
5. Click **Create**.

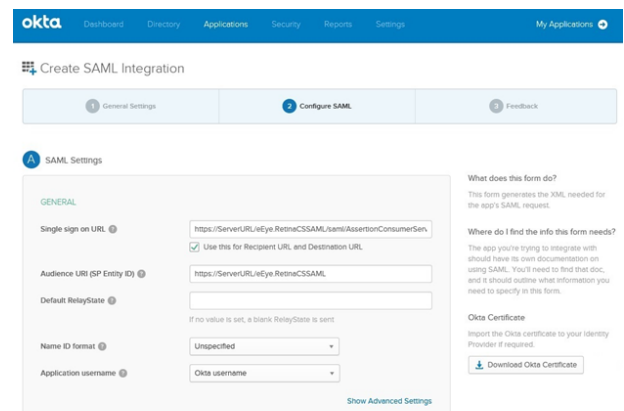


6. Enter the application name, and then click **Next**.
7. Enter the single sign on URL:  
*https://ServerURL/eEye.RetinaCSSAML/saml/AssertionConsumerService.aspx*
8. Check the **Use this for Recipient and Destination URL** box.
9. Enter the audience URI (SP entity ID):  
*https://<ServerURL>/eEye.RetinaCSSAML*



The screenshot shows the 'Create SAML Integration' wizard in Okta. The 'General Settings' step is active. The 'App name' field contains 'PasswordSafe'. The 'App logo' field has a gear icon and a 'Browse...' button. Below it is an 'Upload Logo' button. Under 'App visibility', there are two checkboxes: 'Do not display application icon to users' and 'Do not display application icon in the Okta Mobile app', both of which are currently unchecked. 'Cancel' and 'Next' buttons are at the bottom.

10. From the **Application username** list, select **Okta username**.



The screenshot shows the 'Configure SAML' step of the 'Create SAML Integration' wizard. The 'GENERAL' section contains the following fields: 'Single sign on URL' with the value 'https://ServerURL/eEye.RetinaCSSAML/saml/AssertionConsumerService.aspx'; 'Audience URI (SP Entity ID)' with the value 'https://ServerURL/eEye.RetinaCSSAML'; 'Default RelayState' (empty); 'Name ID format' set to 'Unspecified'; and 'Application username' set to 'Okta username'. A checkbox 'Use this for Recipient URL and Destination URL' is checked. A 'Show Advanced Settings' link is at the bottom right. On the right side, there is a 'What does this form do?' section, a 'Where do I find the info this form needs?' section, and an 'Okta Certificate' section with a 'Download Okta Certificate' button.

## SLO Optional Setting

11. Click **Show Advanced Settings**.
12. Select **Enable Single Logout**.
13. Fill in the **Single Logout URL**:  
*HTTPS://<FQDN>/eEye.RetinaCSSAML/SAML/SLOService.aspx*
14. Fill in the **SP Issuer**: *HTTPS://<FQDN>/eEye.RetinaCSSAML/*
15. Select the **SP Public Certificate.cer** certificate.
16. Click **Upload Certificate**.

## Configure Attributes

17. Add attributes, and then click **Next**.

- **Name:** (required)
- **Email:** (optional)
- **GivenName:** (optional)
- **Surname:** (optional)
- **Group:** (required) - Set as a literal. This must match the group created in BeyondInsight or imported from AD. If an AD group is used, it must match the BI format **Domain\GroupName**.

18. Select appropriate settings for Okta support, and then click **Finish**.

ATTRIBUTE STATEMENTS		
Name	Name Format	Value
Name	Unspecified	String.substringBefore(user.Login, "@")
Email	Unspecified	user.email
GivenName	Unspecified	user.firstName
Surname	Unspecified	user.lastName
GROUP ATTRIBUTE STATEMENTS		
Name	Name Format	Filter
Group	Unspecified	Matches regex: *

3 Help Okta Support understand how you configured this application

Are you a customer or partner?  I'm an Okta customer adding an internal app  I'm a software vendor. I'd like to integrate my app with Okta

**1** The optional questions below assist Okta Support in understanding your app integration.

App type  This is an internal app that we have created

Contact app vendor  It's required to contact the vendor to enable SAML

Which app pages did you consult to configure SAML?

Did you find SAML docs for this app?

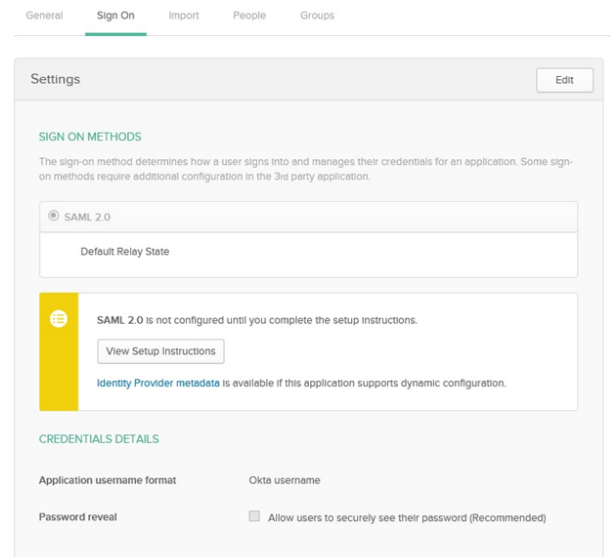
Any tips or additional comments?

Previous

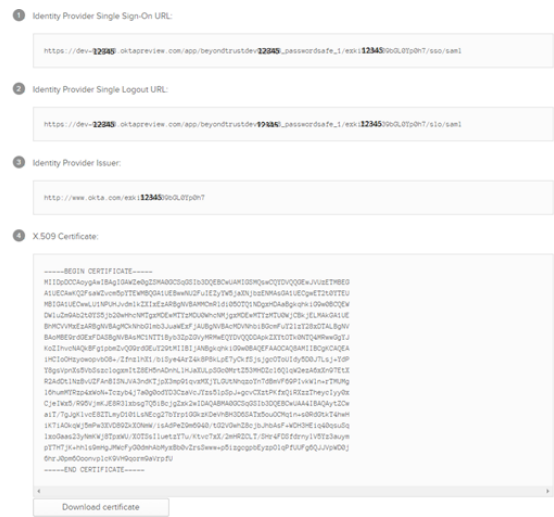
Finish

## Find IdP Information

19. Click **View Setup Instructions**.



20. Copy the **Identity Provider Single Sign-On URL**. Save the value to be used in the next step.
21. Copy the **Identity Provider Issuer**. Save the value to be used in the next step.
22. Click **Download certificate**.

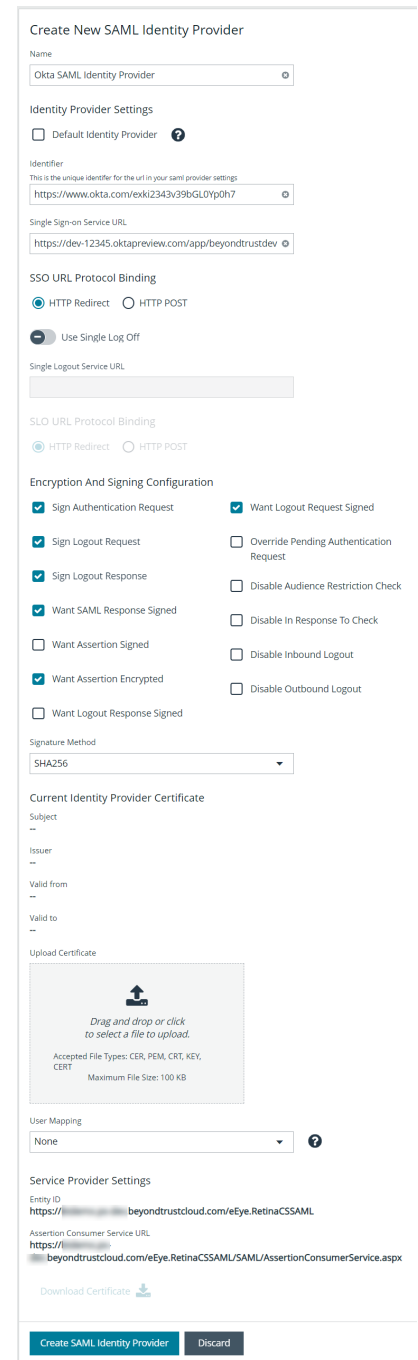


## Configure SAML Identity Provider in BeyondInsight

To configure a new SAML identity provider for Okta in BeyondInsight, follow the below steps.

1. Navigate to **Configuration > Authentication Management > SAML Configuration**.
2. From the **SAML Identity Providers** pane, click **Create New SAML Identity Provider**.

3. Provide a name for the new SAML identity provider (IdP).
4. Complete the **Identity Provider Settings** as follows:
  - Check the **Default Identity Provider** option if you have more than one IdP for the same service provider (SP), and would like this IdP to be used as default for SP initiated logins. This is useful in the case where a user accesses the SAML site access URL without providing an IdP. Also, when a user clicks the **Use SAML Authentication** link from the BeyondInsight login page, they are redirected to the default IdP's site for authentication.
  - **Identifier:** Enter the Okta value **Identity Provider Issuer**.
  - **Single Sign-on Service URL:** Enter the Okta value **Identity Provider Single Sign-On URL**.
  - **SSO URL Protocol Binding:** Select **HTTP Post** as the type.
  - **Single Logout Service URL:** Enter the Okta value **Identity Provider Single Logout URL**.
  - **SLO URL Protocol Binding:** Select **HTTP Post** as the type.
  - **Encryption and Signing Configuration:** Check applicable boxes to enable options, based on your Okta settings. A typical configuration is shown; however, depending on your Okta settings, some configuration selections may be different.
  - **Signature Method:** Select the method, as is required by Okta.
  - **Current Identity Provider Certificate:** Upload the Okta X.509 certificate.
    - **None:** This is the legacy type of mapping, which is not based on type of user.
    - **Local:** Select this option for local user account claims. BeyondInsight maps the user and group name.
    - **Azure Active Directory:** Select this option for Azure Active Directory user account claims. When selected, BeyondInsight maps the **ObjectID** attribute to the **AppUser** and **UserGroup** attributes for the user.
    - **Active Directory:** Select this option for Active Directory user account claims. If the claims are configured to pass the SID of the user and group, BeyondInsight maps the SID for the user and group, which is preferred over mapping domain name and group name attributes.
5. The following **Service Provider Settings** are auto-generated by BeyondInsight:
  - **Entity ID:** This is the fully qualified domain name, followed by the file name: **https://<serverURL>/eEye.RetinaCSSAML/**. This is used for audience restriction.
  - **Assertion Consumer Service URL:** The HTTPS endpoint on the service provider where the identity provider redirects to with its authentication response. .
6. Click **Create SAML Identity Provider**.



**Create New SAML Identity Provider**

Name  
Okta SAML Identity Provider

Identity Provider Settings  
 Default Identity Provider

Identifier  
This is the unique identifier for the url in your saml provider settings  
https://www.okta.com/exki2343v39bGLOyp0h7

Single Sign-on Service URL  
https://dev-12345.oktapreview.com/app/beyondtrustdev

SSO URL Protocol Binding  
 HTTP Redirect  HTTP POST  
 Use Single Log Off

Single Logout Service URL

SLO URL Protocol Binding  
 HTTP Redirect  HTTP POST

Encryption And Signing Configuration

<input checked="" type="checkbox"/> Sign Authentication Request	<input checked="" type="checkbox"/> Want Logout Request Signed
<input checked="" type="checkbox"/> Sign Logout Request	<input type="checkbox"/> Override Pending Authentication Request
<input checked="" type="checkbox"/> Sign Logout Response	<input type="checkbox"/> Disable Audience Restriction Check
<input checked="" type="checkbox"/> Want SAML Response Signed	<input type="checkbox"/> Disable In Response To Check
<input type="checkbox"/> Want Assertion Signed	<input type="checkbox"/> Disable Inbound Logout
<input checked="" type="checkbox"/> Want Assertion Encrypted	<input type="checkbox"/> Disable Outbound Logout
<input type="checkbox"/> Want Logout Response Signed	

Signature Method  
SHA256

Current Identity Provider Certificate

Subject  
--

Issuer  
--

Valid from  
--

Valid to  
--

Upload Certificate

Drag and drop or click to select a file to upload.  
Accepted File Types: CER, PEM, CRT, KEY, CERT  
Maximum File Size: 100 KB

User Mapping  
None

Service Provider Settings

Entity ID  
https://beyondtrustcloud.com/eEye.RetinaCSSAML

Assertion Consumer Service URL  
https://beyondtrustcloud.com/eEye.RetinaCSSAML/SAML/AssertionConsumerService.aspx

Download Certificate

Create SAML Identity Provider Discard

Once the SAML configuration is saved, a public SP certificate is available to download. It can be uploaded to the IdP if required.

## Disable Forms Login

In environments where SAML, smart card, or claims-aware is configured, we recommend enabling the **Disable Forms Login** authentication option to disallow users from using the standard login form in BeyondInsight.

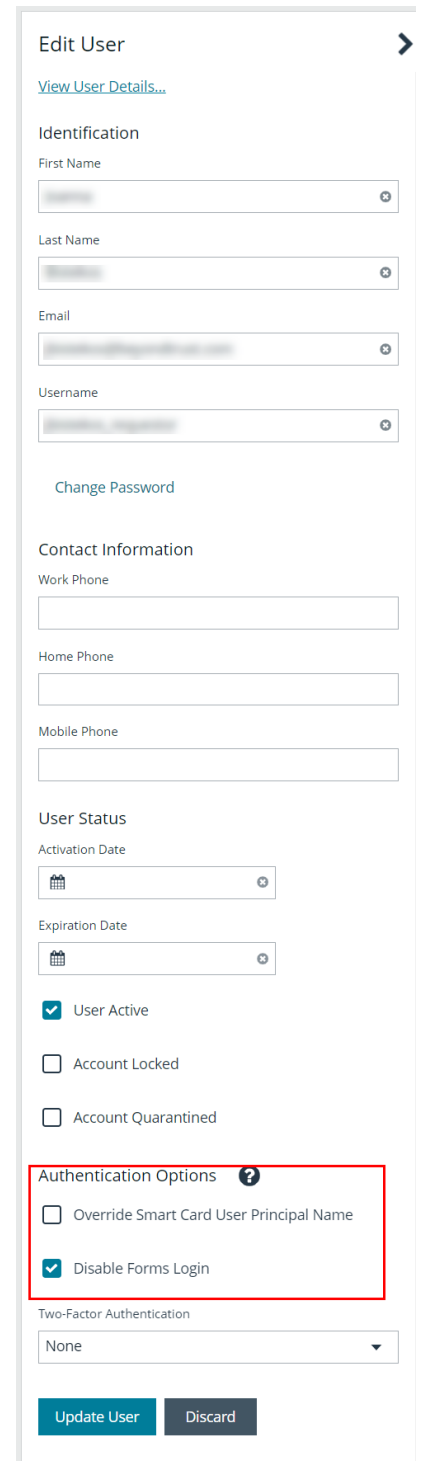
To disable forms login for existing users, enable this option directly on a user account as follows:

1. Click the vertical ellipsis for the user account, and then click **Edit User Details**.

- Under **Authentication Options**, check **Disable Forms Login** to enable the option.



**Note:** Please contact BeyondTrust Support for assistance if you need to bulk-apply this setting to existing accounts.



**Edit User** ➤

[View User Details...](#)

**Identification**

First Name

Last Name

Email

Username

[Change Password](#)

**Contact Information**

Work Phone

Home Phone

Mobile Phone

**User Status**

Activation Date

Expiration Date

User Active

Account Locked

Account Quarantined

**Authentication Options** ?

Override Smart Card User Principal Name

Disable Forms Login

Two-Factor Authentication

[Update User](#) [Discard](#)

To disable forms login globally for newly created directory accounts:

- Navigate to **Configuration > Authentication Management > Authentication Options**.

2. Under **Forms Login Options**, check the **Disable Forms Login for new directory accounts** option to enable it.

**FORMS LOGIN OPTIONS**

Disable Forms Login should only be used in environments where SAML, Smart Card or Claims-aware is configured. Turning this option on will disallow users from using the standard login form in BeyondInsight.

Disable Forms Login for new directory accounts

[Update Forms Login Options](#)



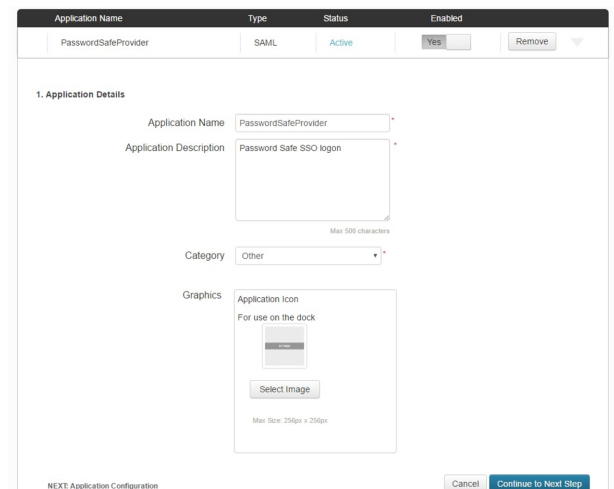
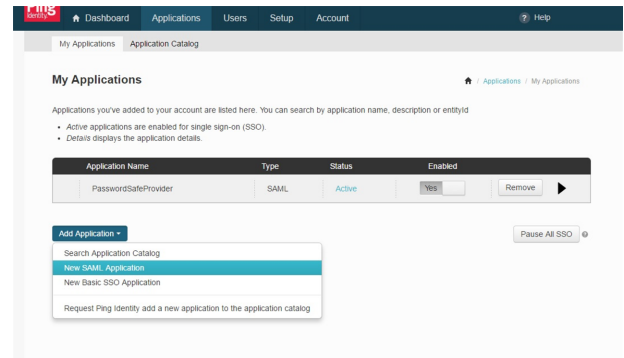
# Configure Ping Identity SAML Authentication for BeyondInsight and Password Safe

Configuring BeyondInsight and Password Safe to use Ping Identity SAML authentication involves configuring the SAML application with BeyondInsight SAML information in the Ping Identity admin portal and then configuring the SAML identity provider settings for Ping Identity in the BeyondInsight console. The configuration for each of these is detailed the below sections.

## Configure SAML Application in Ping Identity


To configure a new SAML application for BeyondInsight and Password Safe in Ping Identity, follow the below steps.

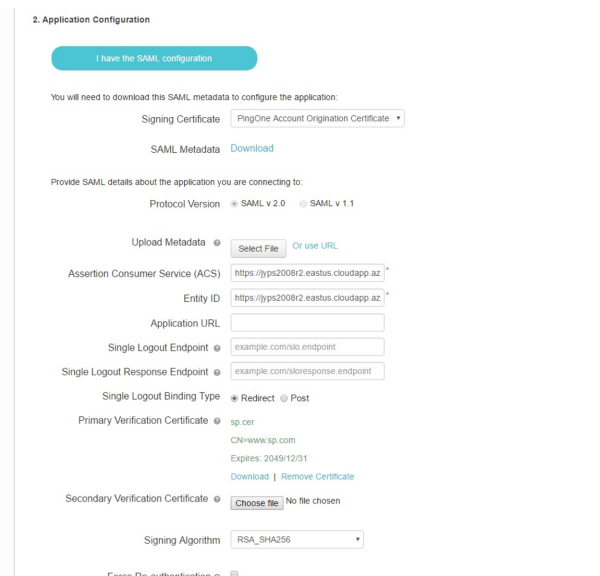
1. Log in to the Ping Identity admin portal.
2. Click the **Add Application** button, and then select **New SAML Application** from the menu.
3. Fill in **Application Name** and **Description**.
4. Set **Category** to **Other**, and then click **Continue to Next Step**.



5. Set the following:

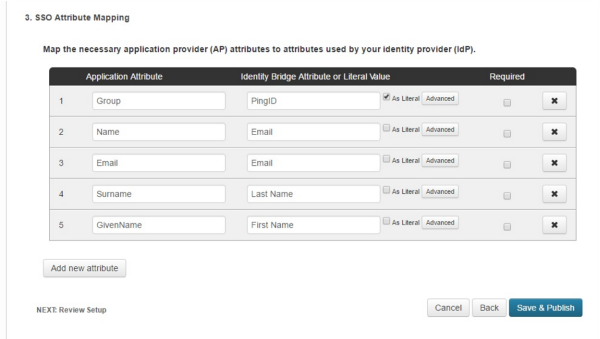
- Set **Assertion Consumer Service (ACS)** to:  
*https://<ServerURL>/eEye.RetinaCSSAML/saml/AssertionConsumerService.aspx*
- Set **Entity ID** to:  
*https://<ServerURL>/eEye.RetinaCSSAML/*
- Set **Single Logout Binding Type** to **Redirect**.
- Upload **Primary Verification Certificate** (use **SP Public Certificate.cer** from **\\WebSiteSAML\Certificates**). The certificate is automatically generated when the BI SAML configuration is saved.
- Click **Continue to Next Step**.


 **Note:** After setting up SAML configuration in the BeyondInsight console, you must download the certificate from the configured SAML identity provider in BeyondInsight. The steps are detailed in the next section.



6. Add the following attributes, and then click **Save & Publish**:

- **Group:** Check the **As Literal** box. This must match the group created in BeyondInsight.
- **Name** (required).
- **Email** (optional).
- **Surname** (optional).
- **GivenName** (optional).



 **Note:** The following is applicable **only to BI version 6.3.1**. It is not required for 6.4.4 or later releases. In 6.4.4 and later releases, the user is automatically logged in to Password Safe, and can then navigate to BeyondInsight, if they have the proper permissions.

To create an application that goes to Password Safe when IdP-initiated login is used, add a new attribute called **Website**. When the value of **Website** is set to **Password Safe**, the user is logged in to Password Safe. If the attribute is not present or is set to anything other than **Password Safe**, the user will be directed to BeyondInsight.

7. Download the **Signing Certificate**.
8. Download **SAML Metadata**.
9. Click **Finish**.

## Configure SAML Identity Provider in BeyondInsight

To configure a new SAML for Ping Identity in BeyondInsight, follow the below steps.

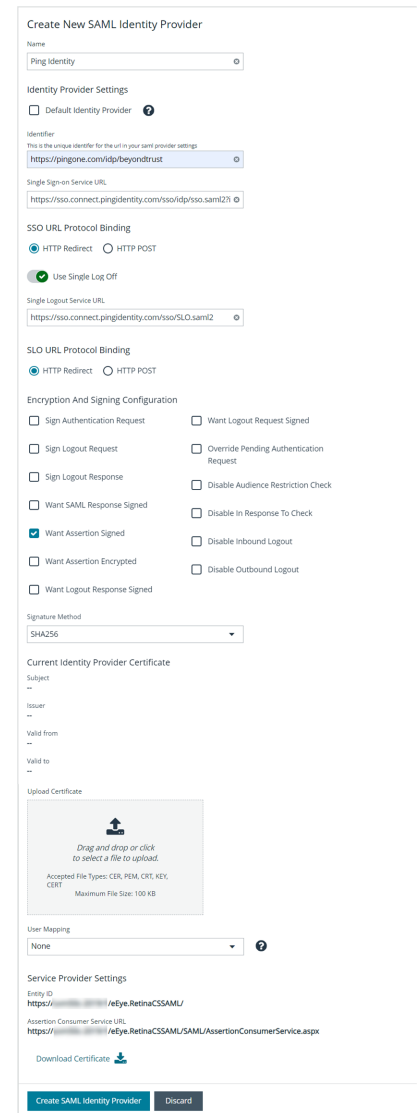
1. Navigate to **Configuration > Authentication Management > SAML Configuration**.
2. From the **SAML Identity Providers** pane, click **Create New SAML Identity Provider**.
3. Provide a name for the new SAML identity provider (IdP).
4. Complete the **Identity Provider Settings** as follows:

- Check the **Default Identity Provider** option if you have more than one IdP for the same service provider (SP), and would like this IdP to be used as default for SP initiated logins. This is useful in the case where a user accesses the SAML site access URL without providing an IdP. Also, when a user clicks the **Use SAML Authentication** link from the BeyondInsight login page, they are redirected to the default IdP's site for authentication.
- **Identifier:** Enter the Ping Identity value **Identity Provider Issuer**.
- **Single Sign-on Service URL:** Enter the Ping Identity value **Identity Provider Single Sign-On URL**.
- **SSO URL Protocol Binding:** Select **HTTP Post** as the type.
- **Single Logout Service URL:** Enter the Ping Identity value **Identity Provider Single Logout URL**.
- **SLO URL Protocol Binding:** Select **HTTP Post** as the type.
- **Encryption and Signing Configuration:** Check applicable boxes to enable options, based on your Ping Identity settings. A typical configuration is shown; however, depending on your Ping Identity settings, some configuration selections may be different.
- **Signature Method:** Select the method, as is required by Ping Identity.
- **Current Identity Provider Certificate:** Upload the Ping X.509 certificate.
- **User Mapping:** Select the type of user account from the dropdown. This indicates how user claims from the SAML provider are mapped in the BeyondInsight User database.

- **None:** This is the legacy type of mapping, which is not based on type of user.
- **Local:** Select this option for local user account claims. BeyondInsight maps the user and group name.
- **Azure Active Directory:** Select this option for Azure Active Directory user account claims. When selected, BeyondInsight maps the **ObjectID** attribute to the **AppUser** and **UserGroup** attributes for the user.
- **Active Directory:** Select this option for Active Directory user account claims. If the claims are configured to pass the SID of the user and group, BeyondInsight maps the SID for the user and group, which is preferred over mapping domain name and group name attributes.

5. The following **Service Provider Settings** are auto-generated by BeyondInsight:

- **Entity ID:** This is the fully qualified domain name, followed by the file name: **https://<serverURL>/eEye.RetinaCSSAML/**. This is used for audience restriction.
- **Assertion Consumer Service URL:** The HTTPS endpoint on the service provider where the identity provider redirects to with its authentication response. .



6. Click **Create SAML Identity Provider**.

## Disable Forms Login

In environments where SAML, smart card, or claims-aware is configured, we recommend enabling the **Disable Forms Login** authentication option to disallow users from using the standard login form in BeyondInsight.

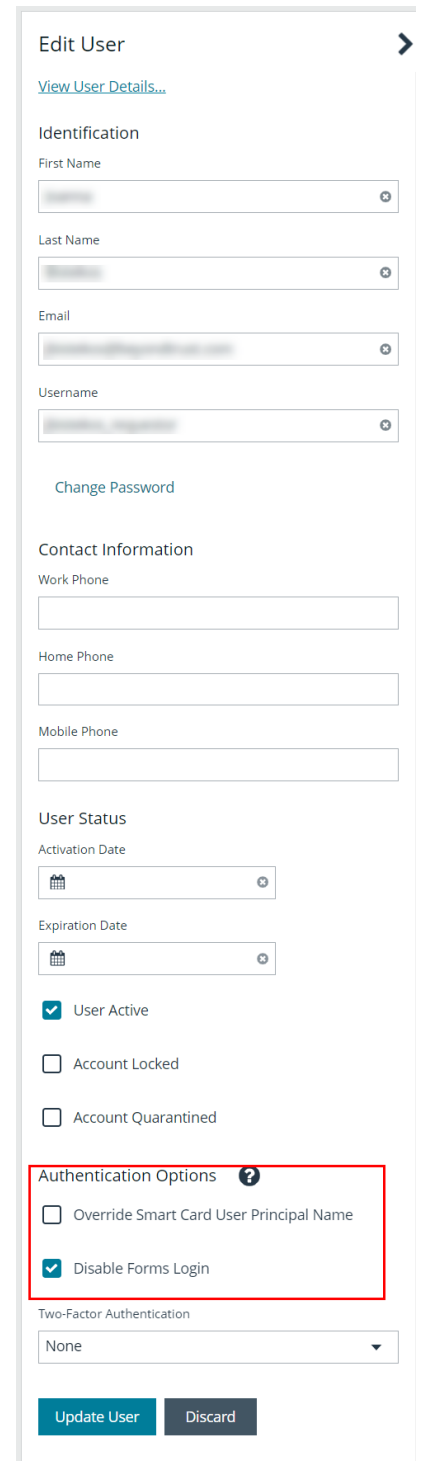
To disable forms login for existing users, enable this option directly on a user account as follows:

1. Click the vertical ellipsis for the user account, and then click **Edit User Details**.

2. Under **Authentication Options**, check **Disable Forms Login** to enable the option.



**Note:** Please contact BeyondTrust Support for assistance if you need to bulk-apply this setting to existing accounts.



**Edit User** ➤

[View User Details...](#)

**Identification**

First Name

Last Name

Email

Username

[Change Password](#)

**Contact Information**

Work Phone

Home Phone

Mobile Phone

**User Status**

Activation Date

Expiration Date

User Active

Account Locked

Account Quarantined

**Authentication Options** ?

Override Smart Card User Principal Name

Disable Forms Login

**Two-Factor Authentication**

None ▼

[Update User](#) [Discard](#)

To disable forms login globally for newly created directory accounts:

1. Navigate to **Configuration > Authentication Management > Authentication Options**.

2. Under **Forms Login Options**, check the **Disable Forms Login for new directory accounts** option to enable it.

**FORMS LOGIN OPTIONS**

Disable Forms Login should only be used in environments where SAML, Smart Card or Claims-aware is configured. Turning this option on will disallow users from using the standard login form in BeyondInsight.

Disable Forms Login for new directory accounts

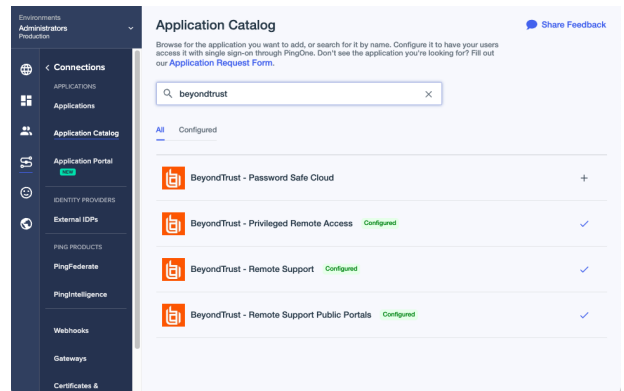
[Update Forms Login Options](#)

# Configure Password Safe and Ping Identity for PingOne

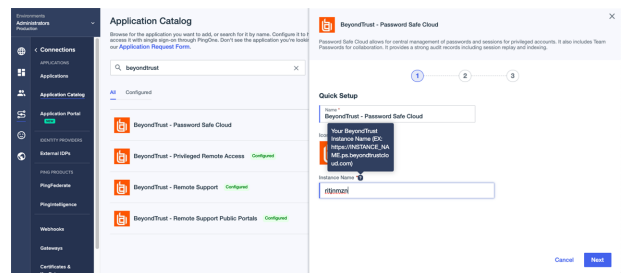
Using the PingOne Application Catalog, leverage the Password Safe app to configure the integration between Password Safe or Password Safe Cloud and PingOne.

To configure the Password Safe App from the PingOne Application Catalog:

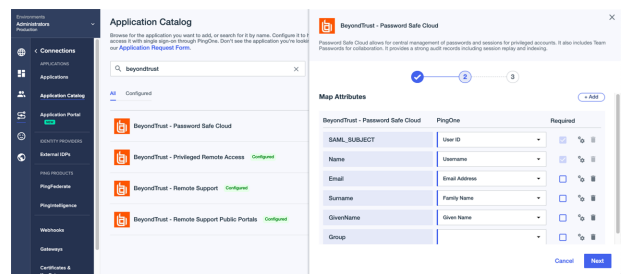
1. Access the Application Catalog for your Ping Identity environment, and search for BeyondTrust.



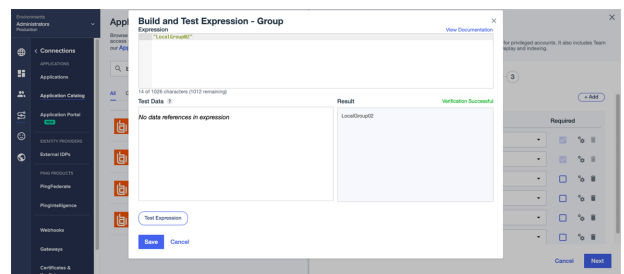
2. Click the + sign next to **BeyondTrust – Password Safe Cloud** application.
3. In the **Instance Name** box, enter the unique part of your instance URL, and then click **Next**.



4. On the **Map Attributes** page, add a group. The **Group** attribute is mandatory and corresponds to the group that will be included in the SAML Assertion for users. In this guide, we configure a static value that is the same for all users accessing Password Safe using this application. Optionally, you can map this attribute to a Ping user attribute.



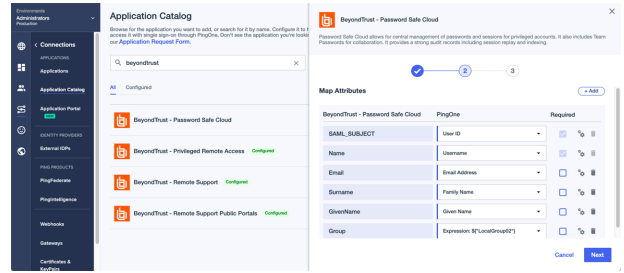
5. Click the **gear** icon to open the Expression Builder for the **Group** attribute. Add a Password Safe group name within double-quotes, and then click **Save**.



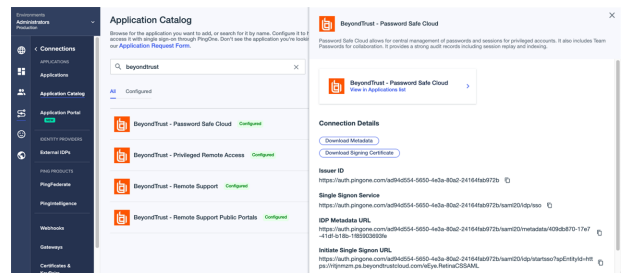


- The **Map Attributes** page will look similar to the screen capture shown. Click **Next**.

You can use access control groups in PingOne to allow access to the app. In this scenario, access is open to all users.



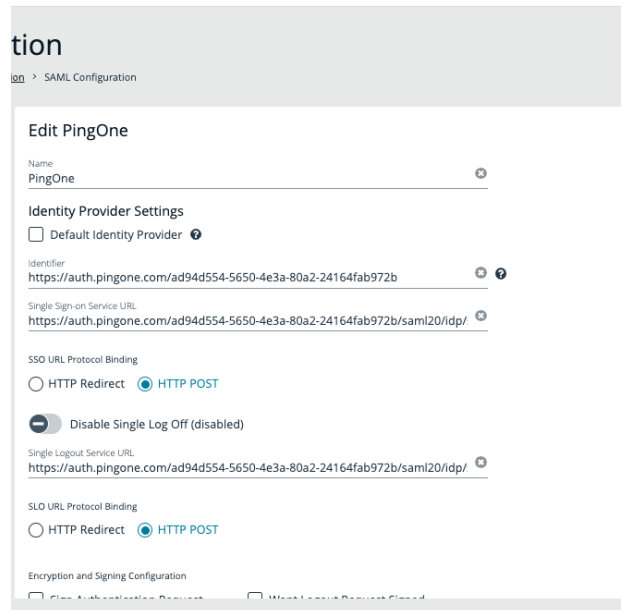
- Click **Save**. The **Connection Details** page is displayed.



- To configure the SAML identity provider in Password Safe, you need: **Issuer ID**, **Single Signon Service URLs**, and the certificate. On the **Connection Details** page, copy the **Issuer ID** and **Single Signon Service URLs** to use later.
- Click **Download Signing Certificate**. You will import the certificate in Password Safe.

## Create a SAML Identity Provider in Password Safe

- On the **SAML configuration** page for PingOne, copy the **Identifier** (Issuer ID) and **Single Sign-On Service URL** values from the previous procedure.



2. Import the certificate downloaded from PingOne in the previous procedure.

**Authentication**

Home > SAML Configuration

Encryption and Signing Configuration


<input type="checkbox"/> Sign Authentication Request	<input type="checkbox"/> Want Logout Request Signed
<input type="checkbox"/> Sign Logout Request	<input type="checkbox"/> Override Pending Authentication Request
<input type="checkbox"/> Sign Logout Response	<input type="checkbox"/> Disable Audience Restriction Check
<input type="checkbox"/> Want SAML Response Signed	<input type="checkbox"/> Disable In Response To Check
<input type="checkbox"/> Want Assertion Signed	<input type="checkbox"/> Disable Inbound Logout
<input type="checkbox"/> Want Assertion Encrypted	<input type="checkbox"/> Disable Outbound Logout
<input type="checkbox"/> Want Logout Response Signed	

Signature Method  
SHA-256

Current Identity Provider Certificate

Subject	CN=PingOne SSO Certificate for Administrators environment, OU=Ping Identity, O=Ping Identity, C=US
Issuer	CN=PingOne SSO Certificate for Administrators environment, OU=Ping Identity, O=Ping Identity, C=US
Valid from	2022-03-31T21:32:43Z
Valid to	2023-03-31T21:32:43Z

Upload Certificate



*Drag and drop or click to select a File to upload*  
Accepted File Types: CER, PEM, CRT, KEY, CERT Maximum File Size: 100KB

3. Save the SAML configuration settings.

PingOne users can now log on to Password Safe using single sign-on.

If an account does not already exist in Password Safe, then the SAML assertion sent by PingOne creates the account. The account is added to the group configured on the **Attribute Mapping** page.

## Troubleshoot Authentication Issues

### Active Directory User Cannot Authenticate with BeyondInsight or Password Safe

If an Active Directory user is a member of more than 120 Active Directory groups, the user may encounter the following error when attempting to log in to the BeyondInsight management console, Analytics & Reporting, or Password Safe, although correct credentials were supplied:

- Authentication fails with *The username or password is incorrect. Please try again.*
- An error is logged in the **frontend.txt** file associated with that login attempt, that includes *A local error occurred.*

The user cannot authenticate because the Kerberos token that is generated during authentication attempts has a fixed maximum size. To correct this issue, you can increase the maximum size in the registry.

1. Start the registry editor on the BeyondInsight server.
2. Locate and click the following registry subkey:

**HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters**



**Note:** If the **Parameters** key does not exist, create it now.

3. From the **Edit** menu, select **New**, and then select **DWORD Value**, or **DWORD (32-bit) Value**.
4. Type **MaxPacketSize**, and then press **Enter**.
5. Double-click **MaxPacketSize**, type **1** in the **Value** box, select **Decimal**, and then click **OK**.
6. From the **Edit** menu, select **New**, and then click **DWORD Value**, or **DWORD (32-bit) Value**.
7. Type **MaxTokenSize**, and then press **Enter**.
8. Double-click **MaxTokenSize**, type **65535** in the **Value** box, select **Decimal**, and then click **OK**.
9. Close the registry editor, and then restart the BeyondInsight server.



For more information, please see [Problems with Kerberos authentication when a user belongs to many groups](https://docs.microsoft.com/en-US/troubleshoot/windows-server/windows-security/kerberos-authentication-problems-if-user-belongs-to-groups) at <https://docs.microsoft.com/en-US/troubleshoot/windows-server/windows-security/kerberos-authentication-problems-if-user-belongs-to-groups>.

### Authentication Errors when using SAML 2.0 Web Applications



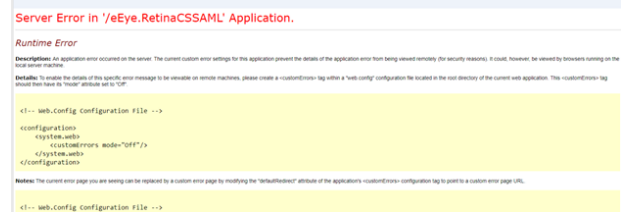
**Note:** Both **Runtime Error** and **Internal Server Error** are for on-premises Password Safe deployments only. If an error shown below occurs using Password Safe Cloud, please contact BeyondTrust Technical Support.

## Runtime Error

If you receive a Runtime Error, add the following to the **web.config** file:

**Set mode to Off < customErrors mode="Off" />**

This provides an actual error.



```

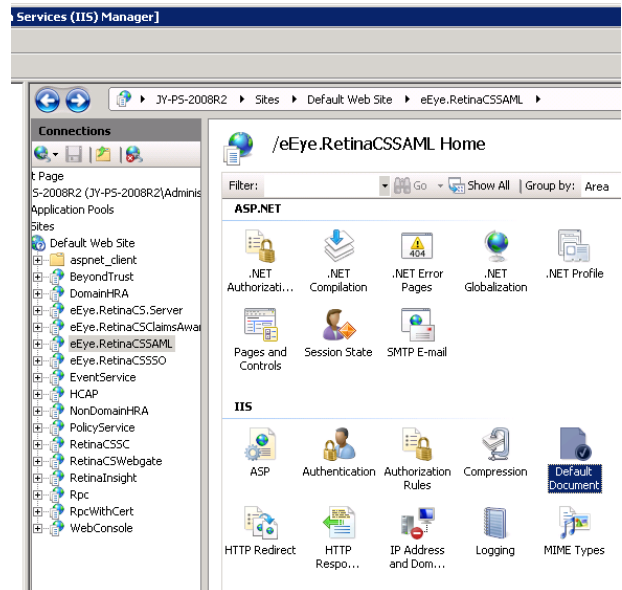
23 <!-->
24 <system.web>
25 <!--
26     Set compilation debug="true" to insert debugging
27     symbols into the compiled page. Because this
28     affects performance, set this value to true only
29     during development.
30 <!-->
31 <compilation debug="true" targetFramework="4.5" />
32 <authentication mode="Forms">
33   <forms name="ServiceProvider" loginUrl="login.aspx" />
34 </authentication>
35 <authorization>
36   <deny users="?" />
37 </authorization>
38 <customErrors mode="Off" />

```

## Internal Server Error (500)

An *Internal Server Error (500)* message usually indicates that the **web.config** file is not formatted correctly.

1. Open IIS on the U-Series Appliance.
2. Browse to the SAML website, and then double-click **Default Document**.



3. If there is a formatting error in the **web.config** file, an error displays, indicating the line number for the error.

