BeyondInsight and Password Safe 23.3 Authentication Guide

2

Table of Contents

BeyondInsight and Password Safe Authentication Guide	5
Create and Configure Groups in BeyondInsight	6
Create a BeyondInsight Local Group	7
Create and Edit Directory Credentials	9
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
Map Directory Credentials to a Domain	17
Add an Active Directory Group	18
Propagate Domain Changes to Group Members	21
Add an Azure Active Directory Group	
Add an LDAP Group	25
Assign Permissions to Groups in BeyondInsight	29
Assign Features Permissions	30
Assign Smart Groups Permissions	34
Configure RADIUS Two-Factor Authentication for BeyondInsight and Password Safe	e35
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
Configure SecureAuth with Password Safe using RADIUS	41
Test the Configuration	41
Configure TOTP Two-Factor Authentication for BeyondInsight and Password Safe $\ .$	42
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

Configure Smart Card Authentication for BeyondInsight and Password Safe	46
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
Configure a Claims-Aware Website in BeyondInsight	55
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
Set Up SAML With a Generic Security Provider in BeyondInsight	60
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
Configure SAML 2.0 for Password Safe using Azure AD App	71
Install and Configure	71
Configure Password Safe to use the SAML Azure AD App	75
Configure AD FS Authentication Using SAML for BeyondInsight and Password Sat	fe78
Configure AD FS on the Identity Provider Server	78
Configure SAML on the Service Provider Server (U-Series Appliance)	85
Configure Okta SAML Authentication for BeyondInsight and Password Safe	88
Configure SAML Application in Okta	89
Configure SAML Identity Provider in BeyondInsight	92
Disable Forms Login	94
Configure Ping Identity SAML Authentication for BeyondInsight and Password Saf	e97
Configure SAML Application in Ping Identity	98
Configure SAML Identity Provider in BeyondInsight	100

4

Disable Forms Login	101
Configure Password Safe and Ping Identity for PingOne	
Create a SAML Identity Provider in Password Safe	
Troubleshoot Authentication Issues	
Active Directory User Cannot Authenticate with BeyondInsight or Password Safe \dots	
Authentication Errors when using SAML 2.0 Web Applications	

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

5

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.

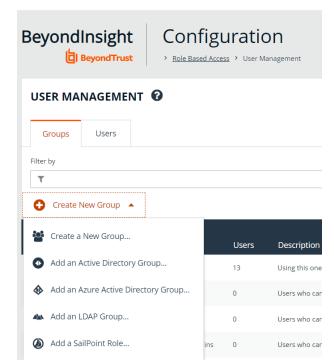
SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

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.



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.

°°	Group Policy Creator Owners	25 50	Members in this gro
	BIDemo	100 150	
Û	Domain Guests	200 250	All domain guests
	Page 1 of 1 > >	100 🔻	Items per page

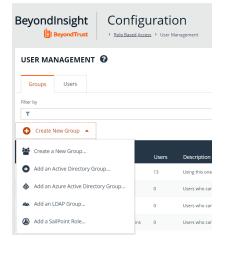
6

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

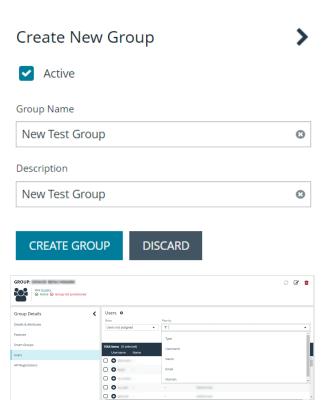
Create a BeyondInsight Local Group

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.



7

Under Group Details, select Users.

7. Assign users to the group:

- 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.

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

8

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 <u>"Assign Permissions to</u> 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.

For more information on creating and editing directory credentials, please see <u>"Create and Edit Directory Credentials" on page</u> <u>9</u>.

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 <u>"Register and Configure an Application</u> 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.

- 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	
O LDAP	
O Azure Active Directory	
Credentials	
Title	
Domain	
Use SSL	
Username	
Password	
Password	
	SHOW
Confirm Password	
	SHOW
Use Group Resolution (Optional)	0
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.

- 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	
0	
Credentials	
Title	
LDAP Server	
Port	
3 89	
Use SSL	
Password	
Bind DN	
Password	
	SHOW
Confirm Password	
	SHOW
Use Group Resolution (Optional)	0
	•
TEST CREDENTIAL	
CREATE CREDENTIAL DISCARD	

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

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.

Navy Dive stars Cus de stiel	
New Directory Credential	
Directory Type	
O Active Directory	
O LDAP	
Azure Active Directory	
Credentials	
Title	
Client ID	
Tenant ID	
Client Secret	SHOW
Use Group Resolution (Optional)	ค
	-
TEST CREDENTIAL	
CREATE CREDENTIAL DISCARD	

Edit a Directory Credential

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

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



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.

- 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	
Active Directory	0
Domain	
	8
Use SSL	
Username	
administrator	0
CHANGE PASSWORD	
Use Group Resolution (Optional) 🛛 🕄	
TEST CREDENTIAL	
UPDATE CREDENTIAL DISCARD CHANGES	

13

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 <u>"Configure Azure Active Directory SAML</u> with BeyondInsight SAML" on page 66.

Register and Configure an Application in Azure Active Directory

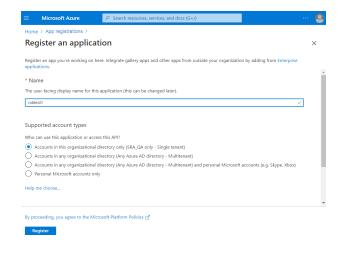
Before you can create Azure Active Directory (AD) credentials and add Azure AD groups and users into BeyondInsight, you must first register and configure an application in the Azure AD tenant where the user accounts reside. The below steps walk through creating a registered application in Azure AD, creating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

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

Create a Registered Application in Azure AD

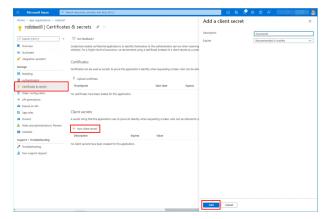
Sign into Azure and connect to the Azure AD tenant where the credentials you wish to add into BeyondInsight reside. Then follow these steps:

- 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.



6. 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.

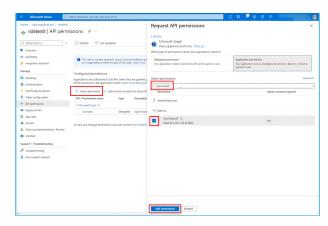
P Search (Otrl+/) «	💙 Got feedback?						
Overview Guidstart	Credentials enable confidential applic scheme). For a higher level of assuran				at a web addressable location (u	sing an HTTPS	
 Integration assistant 	Certificates						
Aanage	Certificates						
Branding	Certificates can be used as secrets to	prove the approaction's loans	ty when hequesting a token. And	can be renemed to a	s public keys.		
Authentication	Upload certificate						
Certificates & secrets	Thumbprint		Start date	Expires	Certificate ID		
Token configuration	No certificates have been added for t	his application.					
API permissions							
Expose an API							
App roles	Client secrets						
Owners	A secret string that the application up	ies to prove its identity when	requesting a token. Also can be i	referred to as applica	tion password.		
Roles and administrators Preview	+ New client secret						
Manifest	Description	Expires	Value	Coor to d	ipboard et ID		
apport + Troubleshooting	mysecret	4/8/2022	UNV7Q~v65~n718mTime			administration (D) (D)	
Troubleshooting			Gilling-yes-to balland	annon y	5		

Assign API Permissions to the Registered Application

- 1. Select the newly created app from the list of App Registrations
- 2. Select API Permissions from the left menu.

BeyondTrust

- 3. Click + Add a permission.
- 4. Click Microsoft Graph.
- 5. Click Application Permissions.
- 6. Search for User.Read.All and check the box in the search results.



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

Home > App registrations > robtext1 	issions #	Request API permissions	
P Search (Ch1+/) «	O Refresh 🛛 🗢 Got feedback?	Microsoft Graph https://graph.microsoft.com/ Docs cf	
Overview Ouloketart Integration assistant	The "Admin concert required" column shows the default value or in organizations where this app will be used. Common:	What type of permissions does your application require? Delegated permissions Your application needs to access the API as the signed-in user.	Application permissions Your application runs as a background service or deemon without a signedie user
Manage Exanding S Authentication	Configured permissions Applications are authorized to call APIs when they are granted p all the permissions the application needs. Learn more about per	Select permissions	equid
Certificates & secrets Token configuration	+ Add a permission V Grant admin consent for DepondT	Permission	Admin consent required
 API permissions 	API / Permissions name Type Description VMercooft Graph (1)	V Group (1)	
Expose an API	UserRead Delegated Sign in and	Group Read All ③ Read #I groups	Wes
 Apprixes Apprixes Refer and administrators Preview Lander Lander Vacidationage Productionage Reverseport request 	To view and manage permissions and sair convert, by Ortegen		
		Add permissions Discard	

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

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

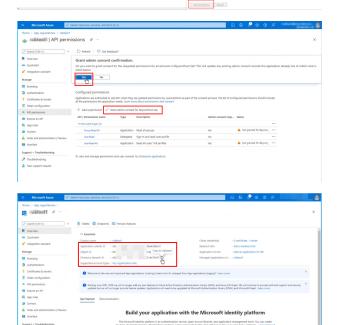
- 11. Click **Grant Admin Consent for <directory name>** to give consent to the app to have those permissions you just added.
- 12. Click Yes to confirm.

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.

For more information on directory credentials, please see "Create and Edit Directory Credentials" on page 9.

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

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



0 The Tab

Type

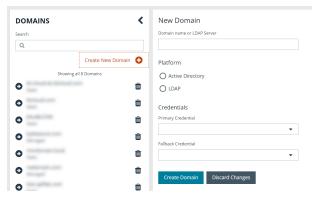
Map Directory Credentials to a Domain

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.

Ť

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.

BeyondInsight	Configurat	tion						6
USER AUDITS						Login Details		>
Create Date filter	Filter by					User Name		
Last 30 days	* T				*		refax version: 93.0	
				2 ± 0	• 0	Mapped Credential PE Mapped Credential Id 18		
Eb4 items (1 selected)						Mapped Creberout 19		
						Description Mapped Credential AC		
✓ 0m21.2021.551.PM	Lope	Lapo	10.00		0	Refern	totoreoury	
Oct 21, 2921, 5:37 PM	Logout	Lapor			0	Vapped Credential Domain/Server	_	
Ow 21, 2021, 5-22 PM	Legin.	Lago			0	Mapped Credential Fil		
0m21.2021.5-20 PM	A66	Domain Management			0	Mapped Credential 10 19 Massard Credential		
0x:21.2021.5/11 PM	644	Configure			0	Description Mapped Credential Ac		
Oct 21, 2021, 5:11 PM	641	Contigura			0	Refere	toeprectory	
Oct 21, 2021, 5-11 PM	fet.	Configure			0	Mapped Credential Domain/Server		
Ger 21, 2021, 5/11 PM	Les.	Configure			0	Authenticate 18 Oxdential M		
0m21.2021.5/11 PM	644	Containe			0	Authenticate Credential DeerSame		
Oct 21, 2021, 5:11 PM	10	Configure			0	Automate		
On 21, 2021, 511 PM	10	Configure			0	Gredential Description		
					0	Authenticate AC Credential Plantare	tiveDirectory	
0er.21,2921,511 PM	bit.	Configure				Automation type Ad	tive Directory	
Oct 21, 2021, 5:11 PM	6de	Configure			0	Consin/Name		
Oct 21, 2021, 5:11 PM	641	Contigure			0	SAM Account Name		
Oct 21, 2021, 511 PM	Edit.	Configure			0			

Add an Active Directory Group

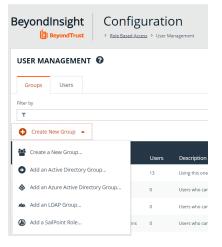
Active Directory (AD) group members can log in to the management console and perform tasks based on the permissions assigned to the group. The group can authenticate against either a domain or domain controller. Upon logging into BeyondInsight, users can select a domain from the **Log in to** list on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



3. Select Add an Active Directory Group.



19

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.

	• • • • • • • • • • • • • • • • • • •
	Create New Credentia
Domain	
	(
Filter by Group Name	
*	(

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.

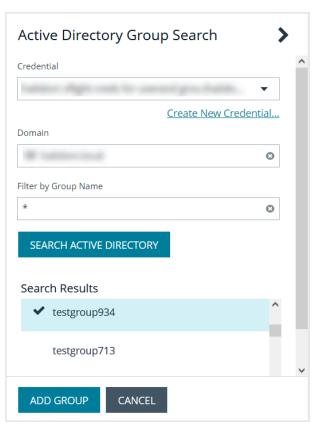
7. Set a filter on the groups to refine the list, and then click Search Active Directory.

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

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

8. Select a group, and then click Add Group.



- 9. The group is added and set to **Active** but not provisioned or synchronized with AD. Synchronization with AD to retrieve users begins immediately.
- 10. 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.

Group Details	<	Users 🛛					
Details & Attributes		Show Assigned users	The T				
Features (38)						0	
Smart Groups (35)		7 items (0 selected)					
Users (7)		Username Nam		mail	Domain		
API Registrations							
					10000-000		
		••			1000-114		
		••	-		10000-000		
		H 4 Page 1	of 1 🕨 📕	25	▼ items per page Sh	wing Items	1-7 o

20

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 <u>"Assign Permissions to Groups in BeyondInsight" on page 29</u>.

For more information on creating and editing directory credentials, please see <u>"Create and Edit Directory Credentials" on page</u> 9.

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

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	
<u>View Group details</u>	
Active	
Name	
Description 	
Credential	
where they not be served	-
	Create New Credential
Domain / Domain controller	
Any domain controller	✓ Fetch
A This change will replace existi	ng user settings.
Propagate this change to all g	group members
Sync Schedule 🛛 😧	
Sync Schedule Options	

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

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.

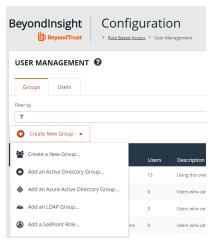
Tip: The **Log** *in* **to** list is only displayed on the **Login** page when there are either AD or LDAP user groups created in the BeyondInsight console. The **Log** *in* **to** list is displayed by default, but may be disabled / enabled by an admin user by toggling the **Show list of domains/LDAP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



3. Select Add an Azure Active Directory Group.

22 TC: 3/7/2024



4. 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.

5. 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

Θ

23

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.

*

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

9	 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 Add Group.	<section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header>

8. 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.

 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

BeyondTrust

filters.

GROUP: Has 2 users Active (last synced of		2 @ f
Group Details Details & Attributes Postures (1)	✓ Users ● Bow Rate by Antiped users • T	
Smart Groups (1)	2 Nerms (0 selectios) Usernamie Name Email	Oomein
Users (2) API Registrations		all an and an
	H 4 Page 1 of 1 b H Z5	items per page Showing Items 1-2 of

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 <u>"Assign Permissions to</u> 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 <u>"Configure Azure Active Directory SAML</u> with BeyondInsight SAML" on page 66.

For more information on creating and editing directory credentials, please see <u>"Create and Edit Directory Credentials" on page</u> <u>9</u>.

Add an LDAP Group

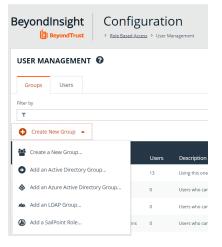
LDAP group members can log in to the management console and perform tasks based on the permissions assigned to the group. The group can authenticate against either a domain or domain controller. Upon logging in to BeyondInsight, users can select a domain or LDAP server from the **Log in to** list on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



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**.

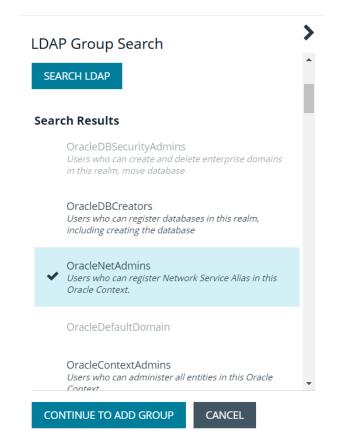
	C 4810			•
			Create New	Credentia
Serv	er			
Dom	ain / Domain contro	oller		
			•	FETCH
Filter	by Group Name			
*				
S	EARCH LDAP	CANCEL		

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**.



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

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

 Active 	
_{Name} OracleNetAdmir	15
Description Users who can r	egister Network Service Alias in
Group Membership a	attribute
uniqueMember	•
Account Naming attri	ibute
uid	•
Base Distinguished N	lame

- 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: Has 12 users Active O Group not p	wovkioned (last synced on Aug 24, 2021, 8:21 PM)	æ	8 🕯
Group Details	✔ Users ●		
Details & Attributes	Show Fiberby Assigned users • T		
Features	Assigned users • T		• 0
Smart Groups	12 Items (0 selected)		
Users (12)	Username Name Email	I Domain	
API Registrations		-101-10 1.0114	
		Contraction Contraction	
	-	Children 1.01.01	
	44	10.0	
	H 4 Page 1 of 1 H	25 • items per page Showing Iter	ms 1-12 of 17

28

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 <u>"Assign Permissions to</u> Groups in BeyondInsight" on page 29.

For more information on creating and editing directory credentials, please see <u>"Create and Edit Directory Credentials" on page 9</u>.

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

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 Analytics & Reporting 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 Asset Details 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.
	Note: Access to Directory Credential Management 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 File Integrity rules.
License Reporting	View the Licensing folder in Analytics & Reporting (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 Managed Accounts page and through the public API: Bulk delete accounts Add accounts to a Quick Group Remove accounts from a Quick Group Add, edit, and delete accounts
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 Configuration > Privileged Access Management Agents page.
Password Safe Configuration Management	Grant a user administrator permissions to the Configuration > Privileged Access Management page.
Password Safe Domain Management	Check the Read and Write boxes to permit users to manage domains.
Password Safe Policy Management	Grant a user administrator permissions to the Configuration > Privileged Access Management Policies page.
Password Safe Role Management	Allows a user to manage roles, provided they have the following permissions: Password Safe Role Management and User Account Management .
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 Scan and Start Scan buttons.
	Activate Abort, Resume, Pause, and Delete on the Job Details page.

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

Feature	Provides Permissions To:		
Scan - Report Delivery	Allow a user to set report delivery options when running a scan:		
	Export Type		
	Notify when complete		
	Email report to		
	Include scan metrics in email (only available for All Audits Scan)		
Scan Management	Delete, edit, duplicate, and rename reports on the Manage Report Templates page.		
	Activate New Report and New Report Category.		
	Activate the Update button on the Edit Scan Settings 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.		
	Note: 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 <u>Use Smart Rules to Organize Assets</u> in the <u>BeyondInsight User Guide</u> .		
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.		
	Note: 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 <u>Use Smart Rules to Organize Assets</u> in the <u>BeyondInsight User Guide</u> .		
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.		
	Note: 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 <u>Use Smart Rules to Organize Assets</u> in the <u>BeyondInsight User Guide</u> .		
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.		
	Note: 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 <u>Use Smart Rules to Organize Assets</u> in the <u>BeyondInsight User Guide</u> .		
Ticket System	View and use the ticket system.		
Ticket System Management	Mark a ticket as inactive. The ticket no longer exists when Inactive is selected.		

33

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 User Audits 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 Backup and Restore options of the U-Series Appliance.
U-Series Appliance High Availability	Provides access to manage the High Availability 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.

1 For more information, please see the Managed Accounts section in the <u>BeyondInsight and Password Safe API Guide</u> 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 User Account Management feature can edit only their user record.
Workgroups	User Accounts Management - Full Control.

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

34

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.

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

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 commaseparated 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.

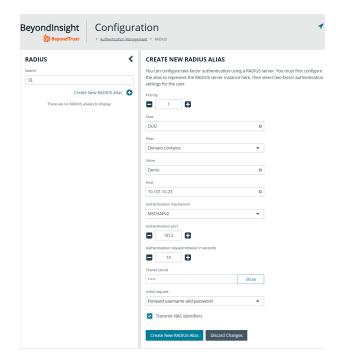
BeyondInsight and Password Safe can work with the following Duo configurations:

- 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 <u>"Configure the RADIUS Server" on page</u> <u>35</u>, using the following settings:

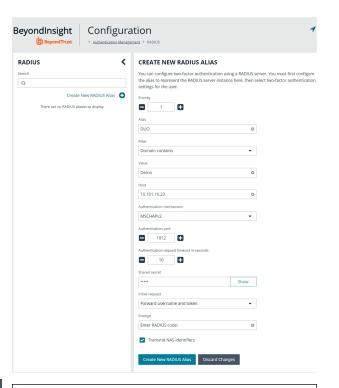
- For Alias, enter Duo.
- · For Authentication Mechanism, select PAP.
- For Initial Request, select Forward User Name and Password.



Configure Two-Factor for a RADIUS Duo-only Configuration

Follow the steps outlined above in <u>"Configure the RADIUS Server" on page</u> <u>35</u>, 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):

37

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.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 3/7/2024 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

- 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.
- 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.

^{©2003-2024} BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 3/7/2 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.



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

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	
Ш О	
Expiration Date	
** ••	
✓ User Active	
Account Locked	
Account Quarantined	
Authentication Options 🛛 😮	
Override Smart Card User Princip	al Name
Disable Forms Login	
Two-Factor Authentication	
RADIUS	•
Map Two-Factor User	
As Logged In	•

39

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

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.

	BeyondInsight Configur	
•	RADIUS <	CONFIGURE AUTHENTICATION You can configure two-factor authentication using a RADIUS server. You may edit settings for the alias representing the RADIUS server instance here.
2	Create New RADIUS Alias 📀 Showing al 2 RADIUS aliases 1 DUO 🗥 💌 🛅	Poorly 2 3 All Fundamental
	2 DUO2 🔺 🔻 🛅	l DUD2 0 Rear Al uners •

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

Configure 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.

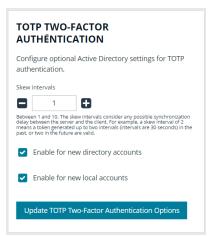
Note: For the push method (4), increase the timeout to 30 seconds.

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**.

BeyondTrust

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

Identification	
First Name	
Last Name	
Email	
Username	
Username	
New Password	
	Show
Confirm New Password	Show
Contact Information	
Contact Information ^{Work Phone}	
Home Phone	
Mobile Phone	
User Status	
Activation Date	
₩ ©	
Expiration Date	
Ш ©	
Vser Active	
Account Locked	
Account Quarantined	
Authentication Options 🛛 😮	
Override Smart Card User Princip	al Name
Disable Forms Login	
Two-Factor Authentication	•

43

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

BeyondTrust

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.



f) 🕥 (in) 🔠

CANCEL

ght © 1999-2022 BevondTrust Corporation. All Rights F

glish (United States)

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
- $\ \ 2. \ \ {\rm Find} \ {\rm the} \ {\rm user} \ {\rm and} \ {\rm click} \ {\rm the} \ {\rm vertical} \ {\rm ellipsis} \ {\rm for} \ {\rm the} \ {\rm user}.$
- 3. Select Edit User Details.
- 4. Scroll to the bottom of the user's details, and under Two-Factor Authentication, click Remove Device.

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

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



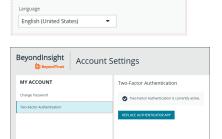
Steps for Users

- 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.

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

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



-

Account Settings

Preferences

BeyondTrust Brand Colors

P

Log Out

46

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**.

Identification First Name	
First Name	
	¢
Last Name	
	¢
Email	
	¢
Username	
	6
Change Password	
Contact Information	
Work Phone	
Home Phone	
Mobile Phone	
Mobile Phone User Status Activation Date	
User Status	
User Status Activation Date	
User Status Activation Date Expiration Date	
User Status Activation Date Expiration Date User Active Account Locked	
User Status Activation Date Expiration Date User Active Account Locked Account Quarantined	
User Status Activation Date Expiration Date User Active Account Locked Account Quarantined Authentication Options	
User Status Activation Date	
User Status Activation Date Activation Date Expiration Date User Active Account Locked Account Quarantined Authentication Options Verride Smart Card User Principal Name User Principal Name	

47

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

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 3/7/2024 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

48

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.

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

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 3/7/2024 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

BeyondTrust

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.

dentification irst Name ast Name mail Jsername	ew User Details			
Irst Name				
ast Name ast Name				
ast Name ast Name a	rst Name			0
mail Isername Change Password Contact Information Vork Phone Nome Phone Mobile Phone Jser Status Acount Phone Image Contact Information Vork Phone Image Contact Information				0
mail Sername Sername Change Password Contact Information Vork Phone Nome Phone Nome Phone Surf Status cutivation Date Ser Status Cutivation Cutiva	ast Name			
Isername Isername Change Password Contact Information Work Phone Mobile Phone Joser Status Abolie Phone User Status Cutivation Date Commend Comme				0
Isername	nail			
Change Password Contact Information Work Phone Mobile Phone Jser Status cutivation Date				Θ
Change Password Contact Information Work Phone Mome Phone Mobile Phone User Status Activation Date	sername			
Contact Information Work Phone Home Phone Abile Phone Mobile Phone Jser Status activation Date xpiration Date xpiration Date xpiration Date account Locked Account Locked Account Quarantined Account Quarantined Account Corride Smart Card User Principal Name Disable Forms Login wo-Factor Authentication				Θ
Vork Phone Kome Phone Abile Phone Abile Phone Jser Status cutivation Date Cutivation	Change Password			
Nome Phone Aobile Phone Jser Status uctivation Date vpiration Date vpiration Date vpiration Date value value Account Locked Account Quarantined Account Quarantined	ontact Informati	on		
Aobile Phone Jser Status Activation Date Activation Date User Active Account Locked Account Quarantined Account Quarantined Account Quarantined Account Quarantined Account Quarantined Account Coptions Disable Forms Login Wo-Factor Authentication	ork Phone			
Aobile Phone Jser Status Activation Date Activation Date User Active Account Locked Account Quarantined Account Quarantined Account Quarantined Account Quarantined Account Quarantined Account Coptions Disable Forms Login Wo-Factor Authentication				
Jser Status ctivation Date m xpiration Date m viser Active Account Locked Account Quarantined Account Control C	ome Phone			
Jser Status ctivation Date m xpiration Date m viser Active Account Locked Account Quarantined Account Control C				
Activation Date	obile Phone			
Activation Date				
Activation Date	ser Status			
 xpiration Date Image: Spiration Date User Active Account Locked Account Quarantined Account Quarantined Account Quarantined Override Smart Card User Principal Name Override Forms Login Wo-Factor Authentication 				
 User Active Account Locked Account Quarantined Account Quarantined Override Smart Card User Principal Name Disable Forms Login wo-Factor Authentication 	m	٢		
 User Active Account Locked Account Quarantined Account Quarantined Account Quarantined Override Smart Card User Principal Name Disable Forms Login wo-Factor Authentication 	piration Date			
Account Locked Account Quarantined Authentication Options Override Smart Card User Principal Name Disable Forms Login wo-Factor Authentication	m	O		
Account Locked Account Quarantined Authentication Options Override Smart Card User Principal Name Disable Forms Login wo-Factor Authentication	Lloor Activo			
Account Quarantined Authentication Options Override Smart Card User Principal Name Disable Forms Login wo-Factor Authentication	Oser Active			
Authentication Options ? Override Smart Card User Principal Name ✓ Disable Forms Login wo-Factor Authentication	Account Locked	b		
 Override Smart Card User Principal Name Disable Forms Login wo-Factor Authentication 	Account Quara	ntined		
Disable Forms Login wo-Factor Authentication	uthentication Op	otions 💡		
wo-Factor Authentication	Override Smart	t Card User Prind	ipal Name	
	Disable Forms I	Login		
None 🔻	vo-Factor Authenticati	ion		
	None			•

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

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

BeyondTrust

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:

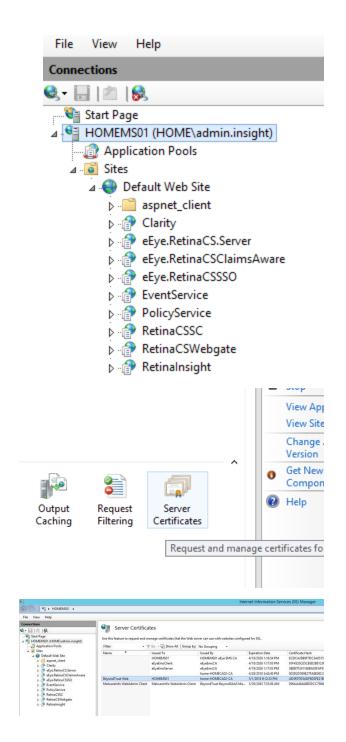
	ssued To	Issued By	Expiration Date	Intende
	eEyeEmsClient	eEyeEmsCA	4/18/2026	Server A
	🖥 eEyeEmsServer	eEyeEmsCA	4/18/2026	Server A
Certificates	HOMEMS01	HOMEMS01 eEye EMS CA	4/18/2026	Server A
👂 🛄 Trusted Root Certificatic 💡	HOMEMS01.home.lab	home-HOMECA02-CA	4/28/2018	Server A
👂 🛄 Enterprise Trust 🛛 🦉	MalwareInfo WebAdmin Client	BeyondTrust BeyondSAAS MalwareInfo WebAdmi	3/29/2045	Client A
Intermediate Certificatic				
Trusted Publishers				
Untrusted Certificates				
Third-Party Root Certific				
Trusted People				
Client Authentication Is:				
Remote Desktop				
Smart Card Trusted Roo				
Trusted Devices				
Web Hosting				
Windows Live ID Token				

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



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

3. Select Server Certificates.



Update Default Web Site Bindings with CA-Issued Certificate

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

request one from your certificate authority.

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

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

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

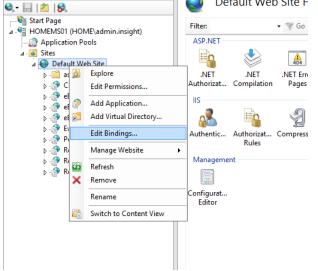
Default Web Site H

?

- 1. Open IIS.
- 2. Expand Sites, and then select Default Web Site.

BeyondTrust

3. Right-click Default Web Site, and then select Edit Bindings.



Site Bindi

♦ HOMEMS01 Sites Default Web Site

C) (

> File View Help

eEyeEmsClient eEyeEmsServer

Connections

4. Select https, and then click Edit.

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

Type Host Na		Binding Informa	<u>A</u> dd
http https	80 * 443 *		<u>E</u> dit
			Remove
			Browse
			Close
	Edit S	Site Binding	? >
<u>T</u> ype:	<u>I</u> P address:	Port:	
https	 All Unassigned 	✓ 443	
<u>H</u> ost name:			
📃 Require Ser	ver <u>N</u> ame Indication		
SSL certi <u>f</u> icates			
BeyondTrust \	Veb	✓ Select	<u>V</u> iew
Not selected			
HOMEMS01			

ОК

Cancel

52

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

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 3/7/2024 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Update SSL Certificate in BeyondInsight Configuration Tool

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

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

4	SMTP Settings	A	Test Connection
	SMTP Server Address	the second se	Create Database
	SMTP Server Port	25	Upgrade Database
	SMTP Server Usemame		
	SMTP Server Password		Manage License
	SMTP SSL Enabled	False	Certificate Management
4	SSO Web Site Information		Install SSL Certificate
	SSO Virtual Directory	eEye.RetinaCSSSO	Disable Debug Logging
	SSO Access URL	http://nn-uvm20b/eEye.RetinaCSSO	Stop Services
4	Web Service		
	Port	21691	Start Services
	SSL Certificate	My: NN-UVM20B	Sync Benchmarks
4	Web Site Information	My: eEyeEmsClient	Disable Light Writebacks
	Web Site	My: WIN-OPKA4L3CN60	Generate Certificate msi
	Host Name	My: eEyeEmsServer	Generate Certificate Zip
	Virtual Directory	My: NN-UVM20B	Import Certificates
	Access URL	My: MalwareInfo WebAdmin Client	
	Legacy Virtual Directory	eEye.RetinaCS.Server	Grant Permissions
	Legacy Access URL	https://nn-uvm20b/eEye.RetinaCS.Server	Client Authentication: Enabled
	Session Timeout	10	ManagementConsole:Enabled
	HTTP Timeout	360 🗠	Event Service: Enabled
ss	L Certificate		Password Safe UI: Enabled
On	tion select an SSL certificate to utilize fo	r the web service	Configure HSM Credentials

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.

Windows Security	у	×
Smart Card Please enter yo) our authentication PIN.	
8	PIN PIN Click here for more information	
	OK Cancel	

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.

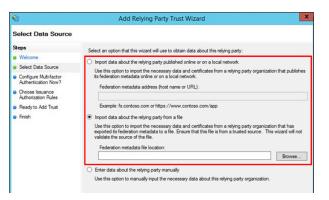
Add Relying Party Trust

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.



^{©2003-2024} Beyond Trust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. Beyond Trust is not a chartered bank or trust company, or TC: 3/ depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

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.

Edit Rule	- BILogonGroupMembership1	×
	aim based on a user's Active Directory group member specify the outgoing claim type and value to issue.	rship. Specify the
<u>Claim rule name:</u>		
BILogonGroupMembership1		
Rule template: Send Group Membership	as a Claim	
ADFS\BILogonGroup	Browse	
Outgoing claim type:		
Group	~	
Outgoing name ID format:		
Unspecified	×	
Outgoing claim <u>v</u> alue:		

Supported Federation Service Claim Types

Outgoing Claim Type	Outgoing Claim Type	Mapping to BeyondInsight User Detail
http://schemas.xmlsoap.org/claims/Group	Required	Group membership
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Required	User name
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	Optional	Surname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	Optional	First name
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	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.

STS. Specify the WS-Federation metadata docume	dified to trust and accept the claims ant location for the existing STS.	issued by an existing
TS WS-Federation metadata document location		
15 WS-rederation metadata document location		
ttps://adfsaccount.adatum.com	Browse	Test location
Example: https://fabrikam.com/FederationMetadata	a/2007-06/Federation Metadata xml)	

57

- 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.

BeyondTrust

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.

ast Name mail sername	
rst Name ast Name ast Nam	
ast Name ast Name ast Name anal sername change Password ontact Information fork Phone come Phone come Phone come Phone come Phone	
ast Name ast Name ast	Θ
mail sername change Password contact Information fork Phone boble Phone boble Phone boble Phone boble Phone boble Phone boble Phone boble Phone boble Phone boble Phone boble Phone boble Phone boble Phone bobl	0
mail sername sername Change Password ontact Information fork Phone come Phone	
sername Change Password ontact Information fork Phone ome Phone boble Phone boble Phone boble Phone boble Phone boble Phone boble Phone boble Phone boble Phone boble Phone boble Phone boble Phone boble Phone bob	Θ
sername Change Password Change Password Contact Information Fork Phone Come Phone Come Phone Come Phone Come Phone Come Phone Come Phone Come Phone Come Phone Come Phone Come Phone	
Change Password Ontact Information fork Phone ome Phone boble Phone boble Phone ctivation Date composition Date co	0
Change Password ontact Information fork Phone ome Phone bible Phone bible Phone ctivation Date civiation Date i User Active Account Locked Account Quarantined uthentication Options	
iontact Information fork Phone ome Phone ioblie Phone ioblie Phone ioblie Phone ioblie Status ctivation Date m ioblie Phone ioblie Status User Status ioblie Phone	0
Index Phone ome Phone Ible Phone <td></td>	
ome Phone Iobile Phone Iser Status ctivation Date im User Active Account Locked Account Quarantined uthentication Options	
Iobile Phone Iser Status ctivation Date	
Iobile Phone Iser Status ctivation Date	
Iser Status ctivation Date	
Iser Status ctivation Date	
ctivation Date	
ctivation Date	
ctivation Date	
xpiration Date Image: Constraint of the second se	
 User Active Account Locked Account Quarantined uthentication Options ? 	
User Active Account Locked Account Quarantined uthentication Options	
Account Locked Account Quarantined uthentication Options	
Account Quarantined	
Account Quarantined	
uthentication Options 🛛 🚷	
	7
Disable Forms Login	
wo-Factor Authentication	
None	•

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.

BeyondTrust

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

59

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:

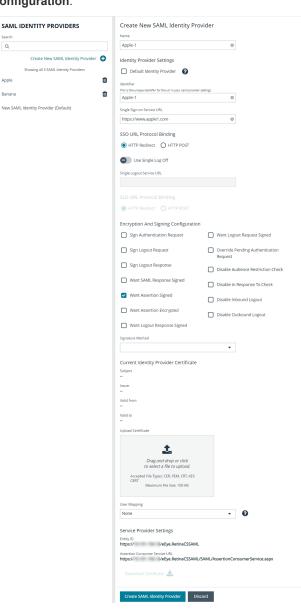
1. Navigate to Configuration > Authentication Management > SAML Configuration.

Q

Apple

Banana

- 2. From the SAML Identity Providers pane, click Create New SAML **Identity Provider.**
- 3. 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: 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.



- 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.

^{©2003-2024} BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 3/7/20 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

63

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 <u>"Configure Azure Active Directory</u> 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

 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).

- 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:

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

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.
- AssertionComsumerServiceUrl: 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:

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

65

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/exk1dg5hgz3LbpBIj5d7/sso/saml
   SingleLogoutServiceBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
   SingleLogoutServiceUrl=https://dev-25872691.okta.com/app/dev-25872691 bi212
1/exk1dg5hqz3LbpBIj5d7/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/

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

- 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

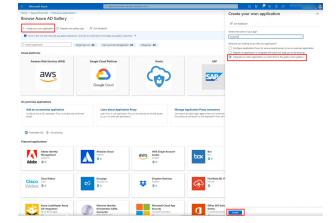
You can integrate Azure Active Directory (Azure AD) SAML with BeyondInsight SAML so that when BeyondInsight receives claims from Azure AD, it can enumerate groups for the user directly from Azure AD using the Group ID value in the claim. This allows an Azure AD user to log in to BeyondInsight using SAML 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.

Microsoft Azure		P Search resources, services, an	nd docs (G+/)		
Home > BeyondTrust QA > Enter	orise applications				
BeyondTrust QA - Azure Active D		S ····	D and feedbacks		
Overview	0				
0 Overview	Iny out the new Enterprise Application of the second se	pps search preview! Oick to enable the pre	rien>		
K Diagnose and solve problems			use your Azure AD tenant as their Identity Provider. Learn		
danage				1 more.	
All applications	Application type Enterprise Applications	Applications status Any V	Application visibility Apply Apply	Reset	
Application proxy					
D User settings	,D First 50 shown, to search all of your applications, enter a display name or the application ID.				
	Name		Homepage URL	Object ID	
Security	_ · · · · 💼 A		http://az		
Conditional Access	O 0				
Consert and permissions	o 9				
Activity	o <i>m</i>				
Sign-in logs	0 0				
🗴 Usage & insights	NO D				
Audit logs	🔿 10				
Provisioning logs	100 FC				
Access reviews					
Admin consent requests					
Troubleshooting + Support					
Virtual assistant (Preview)					

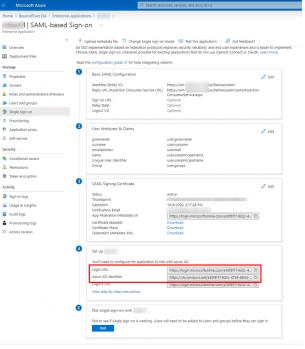
- 2. Click + Create your own application.
- 3. Provide a name.
- Select the Integrate any other application you don't find in the gallery (Non-gallery) option.
- 5. Click Create.



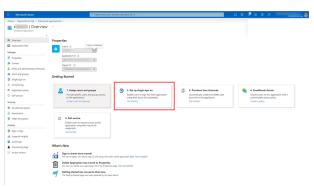
6. In the BeyondInsight console, create a new SAML identity provider. To complete the SAML IdP config in BeyondInsight, use the following information from the enterprise application you just created:

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

- BeyondTrust
 - 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.



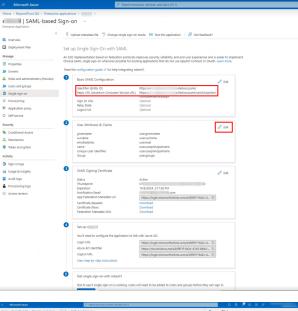
- 7. In Azure, open the **Properties** for the newly created enterprise application.
- 8. From the Getting Started section, click Set up single sign-on.



©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 3 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

BeyondTrust

- 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, the user must log out of BeyondInsight and log back in, to see their name and email in their user profile.

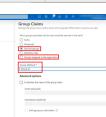
For more information on configuring a SAML IdP in BeyondInsight, please see "Configure SAML in the BeyondInsight Console" on page 60.

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.



BeyondTrust

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.

ast Name mail sername	
rst Name sst Name sst Name sst Name sat Name sername sername change Password change	
ast Name ast Name ast Name anal sername change Password ontact Information fork Phone come Phone come Phone come Phone come Phone	
ast Name ast Name ast	Θ
mail sername change Password contact Information fork Phone boble Phone boble Phone boble Phone boble Phone boble Phone boble Phone boble Phone boble Phone boble Phone boble Phone boble Phone boble Phone bobl	0
mail sername sername Change Password ontact Information fork Phone come Phone	
sername Change Password ontact Information fork Phone ome Phone boble Phone boble Phone boble Phone boble Phone boble Phone boble Phone boble Phon	Θ
sername Change Password Change Password Contact Information Fork Phone Come Phone Come Phone Come Phone Come Phone Come Phone Come Phone Come Phone Come Phone Come Phone Come Phone	
Change Password Ontact Information fork Phone ome Phone boble Phone boble Phone ctivation Date composition Date co	0
Change Password ontact Information fork Phone ome Phone bible Phone bible Phone ctivation Date civiation Date i User Active Account Locked Account Quarantined uthentication Options	
iontact Information fork Phone ome Phone ioblie Phone ioblie Phone ioblie Phone ioblie Status ctivation Date m ioblie Phone ioblie Status User Status ioblie Phone	0
Index Phone ome Phone Ible Phone <td></td>	
ome Phone Iobile Phone Iser Status ctivation Date im User Active Account Locked Account Quarantined uthentication Options	
Iobile Phone Iser Status ctivation Date	
Iobile Phone Iser Status ctivation Date	
Iser Status ctivation Date	
Iser Status ctivation Date	
ctivation Date	
ctivation Date	
ctivation Date	
xpiration Date Image: Constraint of the second se	
 User Active Account Locked Account Quarantined uthentication Options ? 	
User Active Account Locked Account Quarantined uthentication Options	
Account Locked Account Quarantined uthentication Options	
Account Quarantined	
Account Quarantined	
uthentication Options 🛛 🔞	
	7
Disable Forms Login	
wo-Factor Authentication	
None	•

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.

BeyondTrust

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

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

Configure 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

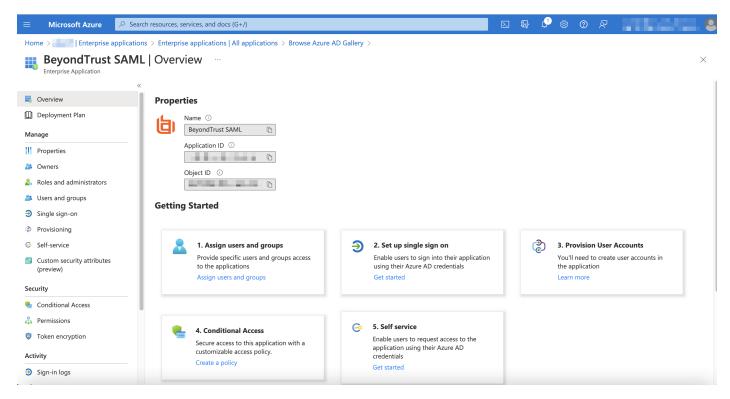
Follow the steps below to install and configure this app.

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

■ Microsoft Azure	え 🖓 ① 🖗 🛛 🖓	
Home > Enterprise applications > Enterprise applications All applications > Browse Azure AD Gallery	BeyondTrust SAML	×
+ Create your own application	blish an application you have Publisher O Provisioning (O vvisioning is not
Showing 6 of 6 results		eyondtrust.com/
BeyondTrust SAML BeyondTrust 多 Beatrust 様式会社 多 Beatrust 様式会社	PostBeyr Read our step-by-step BeyondTrust SAML integra PostBeyonc This application allows Azure AD Users to be provauthenticated into BeyondTrust Remote Support, Access, and Password Safe.	visioned and
OneTrust Privacy Management Software OneTrust Vyond Wyond 3		
	Create	

- 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.

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



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

	✓ Search resources, services, and docs (G+/)	国家 🖓 🔅 ⑦ 戸 admin@2nlp6t.cnmicro 🙎
Home > 2nlp6t Enterprise application	Basic SAML Configuration ×	
BeyondTrust SAML - Enterprise Application	Privileged Remote Access SAML-based Sign-on	⊟ Save A Got feedback?
👪 Overview	≪ ↑ Upload metadata file 🏷 Change single sign-on mode 🔋 Test this application	R ² Gc Identifier (Entity ID) * ⊙
Deployment Plan	Set up Single Sign-On with SAML	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.
🗙 Diagnose and solve problems	An SSO implementation based on federation protocols improves security, reliability, and end us	
Manage	implement. Choose SAML single sign-on whenever possible for existing applications that do no more.	t use C
Properties	Read the configuration quide 🕫 for help integrating BeyondTrust SAML - Privileged Remote A	
A Owners		Patterns: https://remote1.acme.com, https://pra1.acme.com, https://rs1.acme.com/public_portal,
& Roles and administrators	Basic SAML Configuration	https://ps1.acme.com/eEye.RetinaCSSAML
Users and groups	Identifier (Entity ID) https://pra1.acme.com Reply URL (Assertion Consumer Service URL) https://pra1.acme.com/saml/sso	Reply URL (Assertion Consumer Service URL) * ()
Single sign-on	Sign on URL https://pra1.acme.com/saml	The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion
Provisioning	Relay State (Optional) Optional Logout Url (Optional) Optional	Consumer Service" (ACS) in SAML.
Self-service		Index Default
Custom security attributes	2 Attributes & Claims	https://pra1.acme.com/saml/sso 🗸 🗸 🛈 📋
Security	Username user.userprincipalname	Add reply URL Patterns: https://remote1.acme.com/saml/sso, https://pra1.acme.com/saml/sso, https://rs1.acme.com/process,
Conditional Access	Email user.mail	https://ps1.acme.com/eEye.RetinaCSSAML/SAML/AssertionConsumerService.aspx
Permissions	LastName user.surname FirstName user.givenname	
Token encryption	Unique User Identifier user.userprincipalname Group user.groups	Sign on URL (Optional)
Activity	and an	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.
 Sign-in logs 	3 SAML Certificates	https://pra1.acme.com/saml
Usage & insights		
Audit loas	Token signing certificate Status Active	Relay State (Optional) ①
Provisioning logs	Thumbprint 2E0327F4A9A7BB2E358328E0A073EA Expiration 8/23/2026, 7:30:44 AM	The Relay State instructs the application where to reunect users after authentication is completed, and the value is typically a
Access reviews	Notification Email admin@2nlp6t.onmicrosoft.com	URL or URL path that takes users to a specific location within the application.
	App Federation Metadata Url https://login.microsoftonline.com/b Certificate (Base64) Download	23838c Enter a relay state
Troubleshooting + Support	Certificate (Raw) Download	
New support request	Federation Metadata XML Download	Logout Url (Optional)
	Verification certificates (optional)	This URL is used to send the SAML logout response back to the application.
	Required No Active 0	Enter a logout url

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

		Þ.	Ŗ	ø	© %	ন্দ	admin@2nlp6t.onmicro
Home > 2nlp6t Enterprise application	s > Enterprise applications All applications > BeyondTrust SAML - Privileged Remote Access SAML-based Sign-on > SAML-based Sign-on > Attributes & C	Claims >					
Manage claim							×
🖶 Save 🗙 Discard changes 🔗	Got feedback?						
Name	nameidentifier						
Namespace	http://schemas.xmlsoap.org/ws/2005/05/identity/claims						
∧ Choose name identifier format							
Name identifier format *	Persistent					\sim]
Source *	Attribute O Transformation O Directory schema extension (Preview)						
Source attribute *	user.userprincipalname					~	·
Claim conditions							
$ \smallsetminus $ Advanced SAML claims options							

8. 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

	Search resources, services, and docs (G+/)	ы 🗗 🖓 🔅 ⊘ 🖓 admin@2nlp6t.onmicro 🧶
Home > 2nlp6t Enterprise applications > Enterprise application	s All applications > BeyondTrust SAML - Privileged Remote Access SAML-based Sign-on > SAML-based Sign-o	Group Claims ×
Attributes & Claims		Manage the group claims used by Azure AD to populate SAML tokens issued to your app
+ Add new claim + Add a group claim == Columns 🕅	Got feedback?	Which groups associated with the user should be returned in the claim? None All groups
Required claim		All groups Security groups
	Type Value	O Directory roles
Unique User Identifier (Name ID)	SAML user.userprincipalname [***	Groups assigned to the application
Additional claims		Source attribute * Group ID V
Claim name	Type Value	
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	SAML user.groups [Application ***	Emit group name for cloud-only groups ①
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/Email	SAML user.mail ***	 Advanced options
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.sumame ***	Filter groups
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/Username	SAML user.userprincipalname ***	Attribute to match
 Advanced settings 		Match with Match with String Customize the name of the group claim Mame (required) Groups Mamespace (optional) Emit groups as role claims O Anpely regex replace to groups claim content Expose claim in JWT tokens in addition to SAML tokens

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 <u>Configure group claims for applications by using</u> <u>Azure Active Directory</u> at <u>https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-fed-group-claims</u>.

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

75

Configure Password Safe to use the SAML Azure AD App

Once the app has been configured, fllow 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.

	BeyondInsight Configura	ation ment > SAML Configuration
* 	SAML IDENTITY PROVIDERS	Create New SAML Identity Provider
Ŧ	Search	Name
	Q	Azure AD 🕹
٢	Create New SAML Identity Provider 🕒	Identity Provider Settings
Ģ	Showing all 3 SAML Identity Providers	Default Identity Provider
ŝ	Apple III Banana III	Identifier This is the unique identifer for the url in your saml provider settings
12		https://sts.windows.net
	New SAML Identity Provider (Default)	Single Sign-on Service URL
Ve		https://login.microsoftonline.com
4		SSO URL Protocol Binding
9		O HTTP Redirect I HTTP POST
0		Use Single Log Off
สป์		Single Logout Service URL
ಂ		https://login.microsoftonline.
0		SLO URL Protocol Binding
		O HTTP Redirect

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

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

Encryption And Signing Configuration	
Sign Authentication Request	□ Want Logout Request Signed
Sign Logout Request	Override Pending Authentication Request
Sign Logout Response	Disable Audience Restriction Check
✔ Want SAML Response Signed	Disable In Response To Check
✔ Want Assertion Signed	Disable Inbound Logout
Want Assertion Encrypted	Disable Outbound Logout
Want Logout Response Signed	
Signature Method	
SHA256	•

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

Current Identity Provider Certificate

Subject
Issuer
Valid from
0001-01-01T00:00:00
Valid to
0001-01-01T00:00:00
Upload Certificate
Drag and drap or click
Drag and drop or click to select a file to upload.
to select a me to apload.
Accepted File Types: CER, PEM, CRT, KEY,
CERT Maximum File Size: 100 KB
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		•	0
Service Provider Settings			
Entity ID https://	CSSAML		
Assertion Consumer Service URL	COSMINE		
https://	CSSAML/SAML/Assertio	onCons	umerService.aspx
Download Certificate 📩			

Discard

77

Create SAML Identity Provider

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

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.

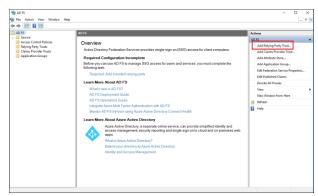
Configure AD FS on the Identity Provider Server

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.



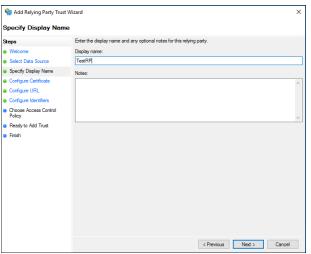
4. On the **Welcome** screen, select **Claims aware**, and then click **Start**.

翰 Add Relying Party Trust \	Nizard	×
Welcome		
Steps Welcome Select Data Source Choose Access Control Policy Ready to Add Trust Finish	Webcome to the Add Pelying Party Trust Wizard Stams-wave applications consume claims in glocations are web-based and use Vindows how your or extranet access. Learnings Image: Construct access. Learnings	
	< Previous Start Canor	si i

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

Add Relying Party Trust	Wizard X
eps Welcome Select Data Source Specify Display Name Configure Certificate Configure URL Configure Identifiers	Select an option that this wizard will use to obtain data about this relying party: Import data about the relying party published online or on a local network Use this option to import the necessary data and certificates from a relying party organization that publishes ts federation metadata address (host name or URL): Federation metadata address (host name or URL): Example: fs contose com or https://www.contose.com/app
Choose Access Control Policy Ready to Add Trust Finish	Import data about the relying party from a file Use this option to import the necessary data and certificates from a relying party organization that has exported at 54 elevation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. Federation metadata file location: Browse
	There data about the relying party manually Use this option to manually input the necessary data about this relying party organization.
	< Previous Next > Cancel

6. 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**.



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

79

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

BeyondTrust

	Wizard
Configure Certificate	
Steps Velcome Select Data Source Specify Duplay Name Corfigure URL Corfigure Ventione Corfigure Ventione Corfigure Ventione Corfigure Ventione Corfigure Ventione Choose Access Control Policy Ready to Add Trust Finish	Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claim that are sert to the refining party. The refining party will use the private key of this certificate to decrypt the Subject: Breater date: Deriven date: View. Browe. Personal

8. 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**.

Add Relying Party Trust	Wizard X
onfigure URL	
sps Welcome Select Data Source Specify Display, Name Configure Certificate Configure URL Configure Mentifiers Choose Access Control Policy Ready to Add Trust Finish	AD FS supports the WS-Truit, WS-Federation and SAML 2.0 WebSSD protocols for relying parties. # WS-Federation, SAML or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Indexta protocol a Web shows and bed for a relying party. The WS-Federation Passive protocol URL supports Web browser-based claims providers using the WS-Federation Passive protocol URL supports Web browser-based claims providers using the WS-Federation Passive protocol URLs. Relying party WS-Federation Passive protocol URL: Example: https://fs.cortoso.com/adfs/fs/ Enable support for the SAML 2.0 WebSSD protocol The SAML 2.0 Single-sign on (SSO) service URL supports Web browser-based claims providers using the SAML 2.0 Single-sign on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 Single-sign on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 Single-sign on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 Single-sign on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 Single-sign on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 Single-sign on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 Single-sign on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 Single-sign on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 Single-sign on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 Single-sign on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 Single-sign on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 Single-sign on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 Single-sign on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 Single-sign on (SSO) service URL suppo
	< Previous Next > Cancel
Add Relying Party Trust	Wizard X
onfigure Identifiers	
ps	Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying
	, the second s

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

翰 Add Relying Party Trust	Wizard	×
Configure Identifiers		
leps	Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for th	is relvina
Welcome	party trust.	
Select Data Source	Relying party trust identifier:	
Specify Display Name	https://< <serverfqdn>>/eEyeDigtalRetinaCSSAML/</serverfqdn>	Add
Configure Certificate	Example: https://fs.contoso.com/adfs/services/trust	
Configure URL	Relying party trust identifiers:	
Configure Identifiers	F	Remove
Choose Access Control Policy		
Ready to Add Trust		
Finish		
	< Previous Next > 0	Cancel

80

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

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

翰 Add Relying Party Trust	Wizard	×
Choose Access Contr	ol Policy	
Steps	Choose an access control policy:	
Welcome	Name	Description ^
Select Data Source	Permit everyone	Grant access to everyone.
Specify Display Name	Permit everyone and require MFA	Grant access to everyone and requir
Configure Certificate	Permit everyone and require MFA for specific group	Grant access to everyone and requir
Configure URL	Permit everyone and require MFA from extranet access	Grant access to the intranet users an
	Permit everyone and require MFA from unauthenticated devices	Grant access to everyone and requir
Configure Identifiers	Pemit everyone and require MFA, allow automatic device registr Pemit everyone for intranet access	Grant access to everyone and requir Grant access to the intranet users
 Choose Access Control Policy 	Permit everyone for intranet access	Grant access to the intranet users.
Ready to Add Trust		,
● Finish	Policy Permit users and require multifactor authentication	
	 I do not want to configure access control policies at this time. No application. 	user will be permitted access for this
	< Pres	vious Next > Cancel

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

🔋 Add Relying Party Trust	Wizard D
eady to Add Trust	
eps Welcome Select Data Source	The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.
Specify Display Name Configure Certificate Configure URL	Specify the monitoring settings for this relying party trust. Relying party's federation metadata URL:
Configure Identifiers Choose Access Control Policy	Monitor relying party Automatically update relying party
Ready to Add Trust Freish	This relying party's federation metadata data was last checked on: < never > This relying party was last updated from federation metadata on: < never >
	< < Previous Next > Cancel

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

Finish			
Steps	The relying party trust was successfully added.		
Welcome	Configure claims issuance policy for this application		
Select Data Source	Conligure claims issuance policy for this application		
Specify Display Name			
Configure Certificate			
Configure URL			
Configure Identifiers			
 Choose Access Control Policy 			
Ready to Add Trust			
Finish			

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

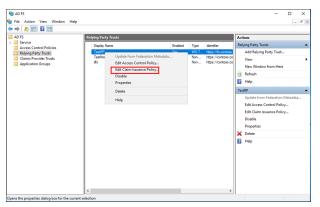
Send LDAP Attributes as Claims

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.
- 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.

Edit Claim Issuance Policy for TestRP	×
Issuance Transform Rules	
The following transform rules specify the claims that will be sent to the relying part	ty.
Order Rule Name Issued Claims	
	1
	₽
Add Rule Edit Rule Remove Rule	
OK Cancel	Apply

82

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

6. 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);

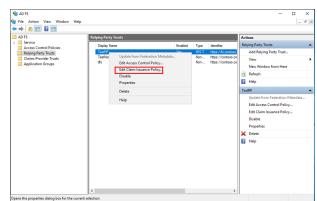
翰 Add Transform Claim	Rule Wizard	×
Configure Rule		
Configure Rule Steps © Choose Rule Type © Configure Claim Rule	<pre>You can corfigure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language. Dam rule name: The template: Send Claims Using a Custom Rule Cystom rule: [cl[Type === "http://sobemas.nicrosoft.com/va/2008/06/identity/claims/windowsaccount name", lassure == "AD AUTORDIT"] > issure(store = "Active Directory", types = ("SecurityIdentifier"), guery = ";objectSid;[0]", param = c.Value);</pre>	~
	< Previous Finish Cancel	

7. 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:

- 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**.



^{©2003-2024} Beyond Trust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. Beyond Trust is not a chartered bank or trust company, or TC: 3/7 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

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

BeyondTrust

	Edit Claim Issuance	Policy for TestRP	×
Order Rule Name Issued Claims Image: Control of the control o	Issuance Transform R	ules	
Add Rule Edit Rule Remove Rule Add Rule Edit Rule Remove Rule K Cancel Apply Add Transform Claim Rule Wizard Select Rule Template for the claim rule that you want to create from the following lat. The description provides details about each claim rule template. Select Rule Template Select Rule Template Select Rule Template Select Rule Template Cam rule template description: Using the Send LDAP Attributes as Claims rule template you can select attributes time rule attributes from an LDAP attribute attribute and claim rule template Configure Claim Rule Cam rule template description: Using the Send LDAP Attributes as Claims rule template you can select attributes time rule attributes from an LDAP attribute attribute and rule template Configure Claim Rule Cam rule template description: Cam rule template descriptio	The following transf	orm rules specify the claims that will be sent to the relying party.	
OK Cancel Apply			\$
Select Rule Template Select Teu Select the template for the claim to the tamplate for the claim to the template for the claim to the template. O choose Rule Type O choose Rule Type Caim Net template. Caim Net template. Caim Net template. Caim Net template description: Caim Net template description: Caim Net template description: Caim Net template attributes as Claims note template spoul can select attributes may be end to an an unit template description: Caim Net template description: Caim	Add Rule		Apply
Steps Select the template for the claim rule trentplate. © Choose Rule Type details about each claim rule template. © Configure Cham Rule Claim rule template. © Configure Cham Rule Claim rule template. © Configure Cham Rule Claim rule template. © Claim rule template. Claim rule template. © Claim rule template description: Using the Sand LOAP Attribute as Claims rule template structures and rule startise structures and rule rule startise structures and rules rule startise structures and rules rule	-	Wizard	×
	-	details alout each claim rule template. Claim rule template: Send LDAP Attributes as Claims Claim due template description: Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP store such as Active Directory to send as claims to the relying party. Multiple attribute may be an use that will ender attribute values for authorizations for an environment.	attribute sent as e to create oneNumber

84

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

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

- 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.

figure Rule					
			of LDAP attributes as claims. Select an attribute store from which		
ose Rule Type	to extr from ti	ract LDAP attributes. Specify how the attrit he rule.	ibutes will map to the outgoing claim types that will be issued		
figure Claim Rule	Claim	rule name:			
	Test	Email Claim Rule			
	Bulet	emplate: Send I DAP Attributes as Claims			
	Activ	e Directory	~		
	Mapping of LDAP attributes to outgoing claim types: LDAP Attributes (Select or type to add more) Outgoing Claim Type (Select or type to add more) User-Principal-Name Name User-Principal-Name Name ID				
			Outgoing Claim Type (Select or type to add more)		
	>	User-Principal-Name	✓ Name		
		User-Principal-Name	✓ Name ID		
		Token-Groups as SIDs	✓ Group		
	•		×		

- 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**.

۹ C

- 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.

0

Want Logout Request Signed

Override Pending Authentication

86

Create New SAML Identity Provider

us identifier for the orl in your sa

https://adfsweb.treyresearch.net/eEye.RetinaCSSAML 0

AD FS Provider

Identity Provider Settings Default Identity Provider

Single Sign-on Service URL

SSO URL Protocol Binding

Use Single Log Off

Single Logout Service URL

HTTP Redirect O HTTP POST

HTTP Redirect O HTTP PO:

Sign Authentication Request

Sign Logout Request

Encryption And Signing 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).
- 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: 0
 - 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
 - ⁸ 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.
- 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. .
- Click Create SAML Identity Provider.

Sign Logout Response Disable Audience Restriction Check Want SAML Response Sign Disable In Response To Check Want Assertion Signed Disable Inbound Logout Want Assertion Encrypted Disable Outbound Logout Want Logout Response Signed SHA256 -Current Identity Provider Certificate Subject Valid from Valid to 1 Drag and drop or click to select a file to unloar ed File Types: CER, PEM, CRT, KEY Maximum File Size: 100 KB Active Directory റ Service Provider Settings Entity ID https:// r Service URI https://l i.com/eEye tificate 👤 Create SAML Identity Provider Discard

87

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

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

88

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.

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

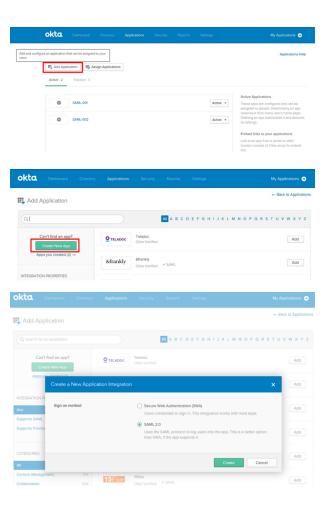
Configure SAML Application in Okta

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.



89

5. Click Create.

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

- 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

<text>

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

okta Deshboerd (Directory Applications	Security Reports	Settings	My Applications 🔿
Create SAML Integ	ration			
General Setting	25	2 Configure SAML		3 Feedback
SAML Settings				
GENERAL				What does this form do? This form generates the XML needed for the app's SAML request.
Single sign on URL	https://ServerURL/	eEye.RetinaCSSAML/saml/Ass	ertionConsumerSen	Where do I find the info this form needs
	Use this for Rec	plent URL and Destination UR	L,	The app you're trying to integrate with should have its own documentation on
Audience URI (SP Entity ID)	https://ServerURL/	eEye.RetinaCSSAML		 and the source is own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.
Default RelayState 🔘				
	If no value is set, a b	olank RelayState is sent		Okta Certificate Import the Okta certificate to your identity
Name ID format 🚱	Unspecified	*		Provider if required.
Application username	Okta username	*		1 Download Okta Certificate
		Shr	w Advanced Setting	N6

90

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.

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



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 STATEMEN	TS	
Name	Name Format	Value
Name	Unspecified	String.substringBefore(user.lo gin, "@")
Email	Unspecified	user.email
GivenName	Unspecified	user.firstName
Surname	Unspecified	user.lastName
GROUP ATTRIBUTE STA	TEMENTS	
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	
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 c	onigure SAML?	
Enter links, describe where the page	s are, or anything else you think is helpful	0
	s are, or anything else you think is helpful	0
	s are, or anything else you think is helpful	
Did you find SAML docs for this app? Enter any links here	s are, or anything else you think is helpful	
Did you find SAML docs for this app?	s are, or anything else you think is helpful	

Previous

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



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.

Setting	5							Ed
SIGN O	N METHODS							
The sig	n-on method dete 10ds require addi					entials for ar	n application. Sor	ne sigi
● s#	AML 2.0							
	Default Relay St	tate						
₽	CANE 2.0 In		d until you con	coloto the co				
		p Instructions	u unui you con	ipiete trie se	up instructio	ons.		
			is available if	this applicati	on supports	dynamic con	figuration.	
CREDE	NTIALS DETAIL	S						
Applica	tion username fo	rmat	Okta us	ername				
Passwo	rd reveal		Allo	w users to s	ecurely see t	heir passwoi	rd (Recommende	d)
					,,			
dentity Provi	ider Single Sign-On U	IRL:						
https://d	ev- 22845 1.oktaprevie	w.com/app/beyond	trustóev 22345 _pa	esswordsafe_1/e	rk 1 12345 1950.01	p0h7/sso/saml		
dentity Provi	ider Single Logout UF	RL:						
https://d	ev- 22345 .oktaprevie	w.com/app/beyond	trustdev 99885 0_pa	sswordsafe_1/e	rk:1 2345 3963201	pOh7/slo/saml		
dentity Provi	ider Issuer:							
http://ww	w.okta.com/exki 1234	\$9950L0Tp0h7						
(.509 Certifi	cate:							
HIIDpDCCA ALUECAWKQ MBIGALUEC DWLUZMGAU BhACVWAKE BAOMBEDrd KOZIPWCNA HCIOOHSy R2AODINA CjeIWXD/R alI/TgJQK IKTIAOKQW IXOGAG23	N CERTIFICATE	1110E8/ww1.2F012E3yT = AR898/WBAMCR10 = AR898/WBAMCR10 S3.JuakEXF JAU89/WB 18 to 32.020/yF8486 220141181 JAN8940 19 y4427244 6954.10 y44272446954.10 y44272446954.10 y44272446954.10 y442720.725510 = A6962040102 = A696204000 = A696204000 = A6962040000 = A6962040000 = A6962040000 = A6962040000 = A6962040000 = A69620400000 = A696200000000000000000000000000000000000	VE) JADNU JO DEDMA SGAT 1 050000 JO DEDMA SGAT J 050000 JO DEDMA SGAT VENDONAL SGORP VI2 VENDONAL SGORP VI2 VENDONAL SGAT VENDONAL SGAT SGAT VENDONAL SGAT SGAT VENDONAL SGAT VENDONAL SGAT V	UECpet2140TEU picpt:020060CQb (Cb);0E,04AGA1U (112728x0TAL8gW NINNTQ4MRw6gTL (24000,TL);04000,TL);04000,0200 (24000,TL);04000,TL);04000,TEU (24000,TL);04000,TEU (24000,TL);04000,TEU (24000,TL);04000,TEU (24000,TL);0400,TEU (24000,TEU (24000,TEU (24000,TEU (24000,TEU (24000,TEU (24000,TEU (24000,TEU (24000,TEU (24000,TEU);0500,TEU (24000,TEU (2				

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.
 - 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.

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

Okta SAML Identity Provider	0
Identity Provider Settings	
Default Identity Provider	
Identifier This is the unique identifier for the url in your saml provider se	ttings
https://www.okta.com/exki2343v39bGL0Yp	0h7 🕲
Single Sign-on Service URL	
https://dev-12345.oktapreview.com/app/be	yondtrustdev ©
SSO URL Protocol Binding	
HTTP Redirect O HTTP POST	
 Use Single Log Off 	
Single Logout Service URL	
HTTP Redirect O HTTP POST	
Encryption And Signing Configuration	
Sign Authentication Request	Want Logout Request Signed
Sign Logout Request	Override Pending Authentication Request
Sign Logout Response	Disable Audience Restriction Che
✓ Want SAML Response Signed	Disable In Response To Check
Want Assertion Signed	Disable Inbound Logout
Want Assertion Encrypted	Disable Outbound Logout
Want Logout Response Signed	
Signature Method	•
Current Identity Provider Certificate Subject	
-	
lssuer	
Valid from	
 Valid to	
-	
Upload Certificate	
•	
1	
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	· 0
	U
Service Provider Settings	
Entity ID https:// beyondtrustcloud.cor	n/eEye.RetinaCSSAML
Assertion Consumer Service URL	
https://l beyondtrustcloud.com/eEye.RetinaCSSA	ML/SAML/AssertionConsumerService.as
Download Certificate 📩	



94

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.

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

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	
<u>View User Details</u>	
Identification	
First Name	
	0
Last Name	
Toolso .	Θ
Email	
production program for all costs	٥
Username	
product, reporter	٥
Change Password	
Contact Information	
Work Phone	
Home Phone	
Mobile Phone	
User Status	
Activation Date	
☆ ◇	
Expiration Date	
** •	
User Active	
oser Adive	
Account Locked	
Account Quarantined	
Authentication Options 🛛 😮	
Override Smart Card User Principal Name	
 Disable Forms Login 	
Two-Factor Authentication	
None	•

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.

BeyondTrust

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

96

Update Forms Login Options

97

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.

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

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.

♠ Dashboard Applications Us	ers Setup	Account		? Help
My Applications Application Catalog				
ly Applications			# /	Applications / My Applications
plications you've added to your account are liste	d here. You can sear	th by application name	description or entitled	
Active applications are enabled for single sign-			, accompany of charging	
Details displays the application details.				
Application Name	Туре	Status	Enabled	
PasswordSafeProvider	SAML	Active	Yes	Remove
Add Application -				Pause All SSO
Search Application Catalog				
New SAML Application				
New Basic SSO Application				
Request Ping Identity add a new application to t	he application catalog	9		
		_		
Application Name	Туре	Status	Enabled	
PasswordSafeProvider	SAML	Active	Yes	Remove
plication Details	PasswordSafePr	ovider		
Application Name	PasswordSafePr]•	
	PasswordSafePr Password Safe S		•	
Application Name			•	
Application Name].	
Application Name			· ·	
Application Name		SSO logon		
Application Name Application Description	Password Safe S	SSO logon Max 500 charact		
Application Name Application Description	Password Safe S	SSO logon Max 500 charact		
Application Name Application Description Category	Password Safe S Other	SSO logon Max 500 charact		
Application Name Application Description Category	Password Safe S Other Application Icon For use on the de	SSO logon Max 500 charact v		
Application Name Application Description Category	Password Safe S Other Application Icon	SSO logon Max 500 charact v		
Application Name Application Description Category	Password Safe S Other Application Icon For use on the de	SSO logon Max 500 charact v		
Application Name Application Description Category	Password Safe S Other Application Icon For use on the de	Max 500 charact		
Application Name Application Description Category	Password Safe S Other Other Application Icon For use on the de Select Imag	Max 500 charact		
Application Name Application Description Category	Other Other Other	Max 500 charact		

98

3. Fill in Application Name and Description.

4. Set Category to Other, and then click Continue to Next Step.

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

- 5. Set the following:
 - Set Assertion Consumer Service (ACS) to:

https://<ServerURL>/eEye.RetinaCSSAML/saml/Assertion ConsumerService.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).

I have the SAML configuration	
You will need to download this SAML metadat	a to configure the application:
Signing Certificate	PingOne Account Origination Certificate
SAML Metadata	Download
Provide SAML details about the application yo	u are connecting to:
Protocol Version	SAML v 2.0 SAML v 1.1
Upload Metadata	Select File Or use URL
Assertion Consumer Service (ACS)	https://jyps2008r2.eastus.cloudapp.az *
Entity ID	https://jyps2008r2.eastus.cloudapp.az *
Application URL	
Single Logout Endpoint @	example.com/slo.endpoint
Single Logout Response Endpoint @	example.com/sloresponse.endpoint
Single Logout Binding Type	Redirect Post
Primary Verification Certificate	sp.cer
	CN=www.sp.com
	Expires: 2049/12/31
	Download Remove Certificate
Secondary Verification Certificate	Choose file No file chosen
Signing Algorithm	RSA_SHA256
Force Reauthontication e	

1	Group	PingID	As Literal Advanced	
2	Name	Email	As Literal Advanced	
3	Email	Email	As Literal Advanced	
4	Surname	Last Name	As Literal Advanced	
5	GivenName	First Name	As Literal Advanced	

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.

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

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. .

Ping Identity	ø
Identity Provider Settings	
Default Identity Provider	
Identifier	
This is the unique identifier for the url in your saml provider s	
https://pingone.com/idp/beyondtrust	٥
Single Sign-on Service URL https://sso.connect.pingidentity.com/sso/ii	In/see sam127 @
SSO URL Protocol Binding	
HTTP Redirect O HTTP POST	
Use Single Log Off	
Single Logout Service URL	
https://sso.connect.pingidentity.com/sso/S	LO.saml2 O
SLO URL Protocol Binding	
HTTP Redirect O HTTP POST	
Encountion And Signing Configuration	
Encryption And Signing Configuration Sign Authentication Request	Want Logout Request Signed
Sign Logout Request	 Override Pending Authentication Request
Sign Logout Response	Disable Audience Restriction Check
Want SAML Response Signed	
 Want Assertion Signed 	Disable In Response To Check
	Disable Inbound Logout
Want Assertion Encrypted	Disable Outbound Logout
Want Logout Response Signed	
Signature Method	
SHA256	•
Current Identity Provider Certificate	
Subject	
ssuer	
/alid to	
Upload Certificate	
1	
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	· 0
Consise Dravidor Cottings	
Service Provider Settings Entity ID	
https:// /eEye.RetinaCSSAML	1
https:// /eEye.RetinaCSSAML	/SAML/AssertionConsumerService.aspx



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.

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

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.

Identification First Name	Identification First Name	Edit User	
Last Name Last Name Last Nam	First Name	<u>View User Details</u>	
Last Name	a Second Contact Information Change Password Contact Information Work Phone Home Phone Second Contact Information Work Phone Second Contact Information Work Phone Second Contact Information Contact Information Work Phone Second Contact Information Contact Informati Contact Inform	Identification	
Last Name Last Name Last Name Last Name Last Name Change Password Change Password Change Password Contact Information Work Phone Home Phone Mobile Phone Expiration Date Contact Status Activation Date Contact Information Expiration Date Contact Information Contact I	Last Name Last Name Change Password C	First Name	
Email Email Username Change Password Contact Information Work Phone Home Phone Home Phone User Status Activation Date	Email Username Change Password Contact Information Work Phone Home Phone Mobile Phone User Status Activation Date Expiration Date Change Active Actount Locked Account Locked Account Locked Account Quarantined Authentication Options Coverride Smart Card User Principal Name Two-Factor Authentication None		Θ
Email Email Username Username Change Password Contact Information Work Phone Home Phone Mobile Phone User Status Activation Date Expiration Date O User Active User Active Account Locked Account Locked Account Quarantined Authentication Options Disable Forms Login Two-Factor Authentication	Email Username Change Password Contact Information Work Phone Home Phone Mobile Phone User Status Activation Date Expiration Date Currie Count Locked Account Locked Account Locked Currie Smart Card User Principal Name Currie Smart Card User Principal Name Disable Forms Login Two-Factor Authentication None	Last Name	
Username Username Change Password Contact Information Work Phone Home Phone User Status Activation Date Expiration Date Contact Locked Account Locked Account Locked Contact Locked Contact Locked Contact Card User Principal Name Con	Username Username Change Password Contact Information Work Phone Home Phone User Status Activation Date Expiration Date Calculate Contact Information Expiration Date Calculate Contact Information Contact In	Testin .	٥
User Active Account Locked Account Locked Account Locked Account Quarantined Authentication Options Disable Forms Login Two-Factor Authentication	User Active Count Cocked Cou	Email	
Change Password Contact Information Work Phone Home Phone Mobile Phone User Status Activation Date Expiration Date Current Correct Authentication Options Current Card User Principal Name Current Car	Change Password Contact Information Work Phone Home Phone User Status Activation Date Expiration Date Contact Locked Actount Locked Account Quarantined Authentication Options Disable Forms Login Two-Factor Authentication None		٥
Change Password Contact Information Work Phone Home Phone User Status Activation Date Expiration Date Colored	Change Password Contact Information Work Phone Home Phone User Status Activation Date Capitation Date Capitati	Username	
Contact Information Work Phone Home Phone Mobile Phone User Status Activation Date Curriation Date Account Locked Account Locked Account Quarantined Authentication Options Disable Forms Login Two-Factor Authentication	Contact Information Work Phone Home Phone Mobile Phone Mobile Phone Expiration Date Expiration Date e Expiration Date e User Active Account Locked Account Quarantined Authentication Options ? Account Quarantined Authentication Options ? Disable Forms Login Two-Factor Authentication 		٥
Work Phone Home Phone Home Phone User Status Activation Date Expiration Date User Active Account Locked Account Locked Account Quarantined Authentication Options ? Override Smart Card User Principal Name	Work Phone Home Phone Home Phone User Status Activation Date Expiration Date Currie Count Locked Account Locked Account Quarantined Authentication Options Disable Forms Login Two-Factor Authentication None	Change Password	
Home Phone Mobile Phone User Status Activation Date Expiration Date User Active Account Locked Account Locked Account Quarantined Authentication Options ? Override Smart Card User Principal Name Disable Forms Login Two-Factor Authentication	Home Phone Mobile Phone User Status Activation Date Expiration Date C C C C C C C C C C C C C C C C C C C	Contact Information	
Mobile Phone User Status Activation Date Expiration Date Curricology of the second s	Mobile Phone User Status Activation Date Expiration Date C User Active Account Locked Account Quarantined Authentication Options Disable Forms Login Two-Factor Authentication None	Work Phone	
Mobile Phone User Status Activation Date Expiration Date Curricology of the second s	Mobile Phone User Status Activation Date Expiration Date C User Active Account Locked Account Quarantined Authentication Options Disable Forms Login Two-Factor Authentication None		
User Status Activation Date Activation Date Expiration Date User Active Account Locked Account Quarantined Authentication Options ? Override Smart Card User Principal Name Disable Forms Login Two-Factor Authentication	User Status Activation Date	Home Phone	
User Status Activation Date Activation Date Expiration Date User Active Account Locked Account Quarantined Authentication Options ? Override Smart Card User Principal Name Disable Forms Login Two-Factor Authentication	User Status Activation Date		
Activation Date	Activation Date Expiration Date Expiration Date	Mobile Phone	
Activation Date	Activation Date Expiration Date Expiration Date		
 Expiration Date Expiration Date Work Active Account Locked Account Quarantined Account Quarantined Authentication Options ? Override Smart Card User Principal Name Disable Forms Login Two-Factor Authentication 	 Expiration Date Expiration Date W User Active Account Locked Account Quarantined Authentication Options ? Override Smart Card User Principal Name Override Smart Card User Principal Name Tisable Forms Login Two-Factor Authentication None 	User Status	
Expiration Date Expiration Date User Active Account Locked Account Quarantined Authentication Options Override Smart Card User Principal Name Disable Forms Login Two-Factor Authentication	Expiration Date Expiration Date User Active Account Locked Account Quarantined Authentication Options Override Smart Card User Principal Name Disable Forms Login Two-Factor Authentication None		
 User Active Account Locked Account Quarantined Authentication Options ? Override Smart Card User Principal Name Disable Forms Login Two-Factor Authentication 	 User Active Account Locked Account Quarantined Authentication Options ? Override Smart Card User Principal Name Disable Forms Login Two-Factor Authentication None	₩ ©	
 User Active Account Locked Account Quarantined Authentication Options ? Override Smart Card User Principal Name Disable Forms Login Two-Factor Authentication 	 User Active Account Locked Account Quarantined Authentication Options ? Override Smart Card User Principal Name Disable Forms Login Two-Factor Authentication None 	Expiration Date	
Account Locked Account Quarantined Authentication Options Override Smart Card User Principal Name Disable Forms Login Two-Factor Authentication	Account Locked Account Quarantined Authentication Options Override Smart Card User Principal Name Disable Forms Login Two-Factor Authentication None	₩ 8	
Account Quarantined Authentication Options Override Smart Card User Principal Name Disable Forms Login Two-Factor Authentication	Account Quarantined Authentication Options Override Smart Card User Principal Name Disable Forms Login Two-Factor Authentication None	User Active	
Authentication Options ? Override Smart Card User Principal Name Disable Forms Login Two-Factor Authentication	Authentication Options Override Smart Card User Principal Name O Disable Forms Login Two-Factor Authentication None	Account Locked	
Override Smart Card User Principal Name Disable Forms Login Two-Factor Authentication	Override Smart Card User Principal Name Disable Forms Login Two-Factor Authentication None	Account Quarantined	
Disable Forms Login Two-Factor Authentication	Disable Forms Login Two-Factor Authentication None	Authentication Options 🛛 😯	٦
Two-Factor Authentication	Two-Factor Authentication	Override Smart Card User Principal Name	
	None 👻	✓ Disable Forms Login	
None 🔻		Two-Factor Authentication	
	Update User Discard	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.

BeyondTrust

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

103

Update Forms Login Options

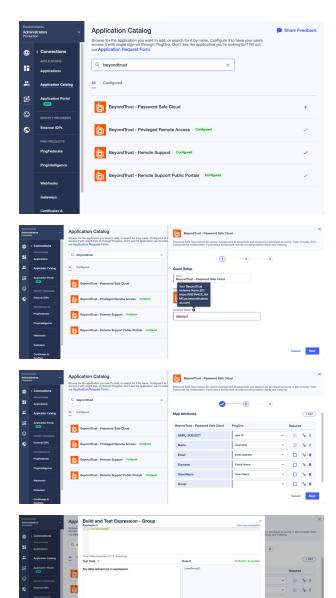
Configure Password Safe and Ping Identity for PingOne

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:

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

- 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**.



104

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

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 3/7/2024 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Test Dare

6. 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.

7. Click Save. The Connection Details page is displayed.

- 8. 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.
- 9. Click Download Signing Certificate. You will import the certificate in Password Safe.

Create a SAML Identity Provider in Password Safe

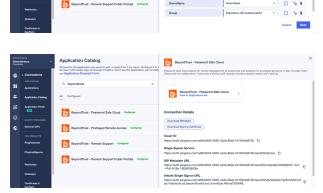
 On the SAML configuration page for PingOne, copy the Identifier (Issuer ID) and Single Sign-On Service URL values from the previous procedure.

Edit PingOne		
Name PingOne	Θ	
Identity Provider Settings		
Default Identity Provider 🔞		
^{dentifier} https://auth.pingone.com/ad94d554-5650-4e3a-80a2-24164fab972b	0	0
single Sign-on Service URL https://auth.pingone.com/ad94d554-5650-4e3a-80a2-24164fab972b/saml20/id	ip/: ©	
550 URL Protocol Binding		
HTTP Redirect HTTP POST		
Disable Single Log Off (disabled)		
Single Logout Service URL https://auth.pingone.com/ad94d554-5650-4e3a-80a2-24164fab972b/saml20/id	ip/ ©	

105

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

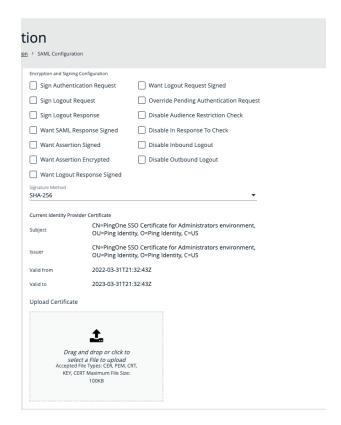
©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 3/7/2024 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.



SAML_SUB Name Email



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



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.

107

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 <u>Problems with Kerberos authentication when a user belongs to many groups</u> at <u>https://docs.microsoft.com/en-US/troubleshoot/windows-server/windows-security/kerberos-authentication-problems-if-user-</u> 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.

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

Runtime Error

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

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

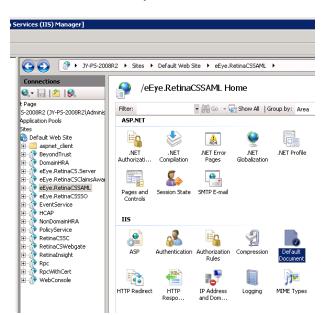
This provides an actual error.

Runtime En	
Description: An at	plication error occurred on the server. The current custom error settings for this application prevent the details of the application error from being viewed remotely (for security reasons). It could, however, be viewed by browsers numming
local server machine.	
Details: To enable t should then have its "	he details of this specific error message to be viewable on remote machines, please create a <customerrors- "off".<="" "web="" <customerrors-="" a="" application.="" config"="" configuration="" current="" directory="" file="" in="" located="" methin="" mething="" of="" root="" set="" tag="" td="" the="" this="" to="" web="" within=""></customerrors->
cl., which	fig Configuration File>
<configurati <system.< td=""><td></td></system.<></configurati 	
<cus <td>toaliroors mode="off"/></td></cus 	toaliroors mode="off"/>
<td></td>	
Notes: The current of	mor page you are seeing can be replaced by a custom error page by modifying the "defaultifiederct" attribute of the applications -contiguration tag to point to a custom error page URL.
<1 web.con	fig Configuration File>
23	>
1 23	> <system.web></system.web>
24	<system.web></system.web>
24 25	<system.web> <!--</td--></system.web>
24 25 26	<system.web> <!--<br-->Set compilation debug="true" to insert debugging</system.web>
24 25 26 27	<system.web> <!-- Set compilation debug="true" to insert debugging symbols into the compiled page. Because this</td--></system.web>
24 25 26 27 28	<system.web> <!--<br-->Set compilation debug="true" to insert debugging symbols into the compiled page. Because this affects performance, set this value to true only</system.web>
24 25 26 27 28 29	<system.web> <!--<br-->Set compilation debug="true" to insert debugging symbola into the compiled page. Because this affects performance, set this value to true only during development.</system.web>
24 25 26 27 28 29 30	<pre><system.web></system.web></pre>
24 25 26 27 28 29 30 31	<pre><system.web> <!--=- Set compilation debug="true" to insert debugging symbola into the compiled page. Because this affects performance, set this value to true only during development--> compilation debug="true" targetFramework="4.5" /></system.web></pre>
24 25 26 27 28 29 30 31 32	<pre><system.veb></system.veb></pre>
24 25 26 27 28 29 30 31 32 33	<pre><system.web> <!-- Set compilation debug="true" to insert debugging symbols into the compiled page. Because this affects performance, set this value to true only during development <compilation debug="true" targetFramework="4.5" /--> <authentication mode="forms"> </authentication> </system.web></pre>
24 25 26 27 28 29 30 31 32 33 33 34	<pre><system.veb></system.veb></pre>
24 25 26 27 28 29 30 31 31 32 33 34 35	<pre><system.web></system.web></pre>

Internal Server Error (500)

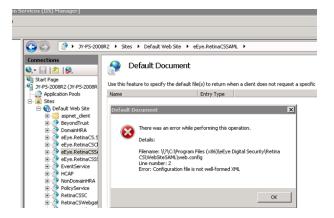
An Internal Server Error (500) message usually indicates that the web.config file is not formatted correctly.

- 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.

BeyondTrust



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