BeyondInsight and Password Safe Authentication Guide 21.1

2

Table of Contents

BeyondInsight and Password Safe Authentication Guide	3
Create and Configure Groups in BeyondInsight	4
Create a BeyondInsight Local Group	4
Active Directory and LDAP	7
Create and Edit Directory Credentials	7
Add an Active Directory Group	8
Add an LDAP Directory Group	11
Assign Permissions	14
Assign Group Permissions	14
Assign Features Permissions	14
Assign Smart Groups Permissions	17
Configure Two-Factor Authentication for BeyondInsight and Password Safe RADIUS Server	Using 18
Configure the RADIUS Server	18
Configure RADIUS Two-Factor Authentication Using Duo	19
Configure Alternate Directory Attribute for RADIUS	
Configure SecureAuth with Password Safe using RADIUS	21
Configure Smart Card Authentication	
Configure Two-Factor Authentication Settings for User Accounts	
Configure a Claims-Aware Website in BeyondInsight	
Set Up SAML With a Generic Security Provider	
Configure ADFS with Password Safe Using SAML	
Configure Okta with Password Safe	
Configure Ping Identity with Password Safe	44
Troubleshoot Authentication Issues	47

3

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 users who are managed exclusively by BeyondInsight. You can also add Active Directory users and groups and apply BeyondInsight authentication.

For a user to log in to BeyondInsight using BeyondInsight authentication, the user account must reside in the BeyondInsight database.

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.

Note: By default, an **Administrators** group is created. The permissions assigned to the 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 and LDAP groups into BeyondInsight.

BeyondInsight	Configu	ration d Access → U	lser Management
		GROUPS	
T Filter by			
Create New Group	_		
📽 Create a New Group		Users	Description
Add an Active Directory Group.		0	test
Add an LDAP Group	dmins	0	Users who can create and delete enterprise domain

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.

USER MANAGEMENT @

	GROUPS
T	Piter by
	Туре
	Name
	Description
	Last Synchronization Date

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
•	SIDemo	100 150	
i	Domain Guests	200 250	All domain guests
	Page 1 of 1 P	100 🔻	ltems per page

4

After a group is created, add user accounts to the group. When a user is added to a group, the user is assigned the permissions assigned to the group.

Create a BeyondInsight Local Group

- 1. Select Configuration.
- 2. Under Role Based Access, select User Management.

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

>

5

- 3. Under Groups, click Create New Group.
- 3. Select Create a New Group.

BeyondInsight	Configu	ration Access → U	ser Management
		GROUPS	
Create a New Group		Users	Description
Add an Active Directory Group Add an Active Directory Group	ıp	0	test
Add an LDAP Group	dmins	0	Users who can create and delete enterprise domain

4. Enter a Group Name and Description for the group.

• Under Group Details, select Users.

• From the Show dropdown list, select Users not assigned.

• Filter the list of users displayed in the grid by **Type**,

Username, Name, Email, and Domain, if desired.

- 5. The group is set to **Active (yes)** by default. Click the toggle to set the group to **Active (no)** if you wish to activate it later.
- 6. Click Create Group.

7. Assign users to the group:

CREATE NEW GROUP

Active (yes)

Group Name New Test Group

Description New Test Group



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

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

Use	rs 🕜			
Show Users	not assigned	•	Username name	S T Filter by
Assig	n User 🔶			
7 item	is (6 selected)			
	Username	Name 🔺	Email	Domain
•	a.name4	a.name4	e@mail4.null	n i i i n
	a.name5	a.name5	e@mail5.null	: n
•	a.name6	a.name6	e@mail6.null	: n
•	a.name7	a.name7	e@mail7.null	e n
	a.name8	a.name8	e@mail8.null	: n
	a.name9	a.name9	e@mail9.null	n

1 By default, new groups are not assigned any permissions. You must assign permissions on features and smart groups after creating a new group. For more information on permissions and how to assign them, please see "Assign Group Permissions" on page 14.

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.

©2003-2021 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

Active Directory and LDAP

Create and Edit Directory Credentials

A directory credential is required for querying Active Directory and LDAP, and also for adding Active Directory and LDAP groups and users in BeyondInsight.

- 1. Select Configuration.
- 2. Under Role Based Access, select Directory Credentials.
- 3. Click Create Directory Credential.



- 4. Select the directory type and provide a name for the credential.
- 5. Enter the name of the domain where the directory and user credentials reside.
- 6. Enable the 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.

- Enter the credentials for the account that has permissions to query the directory.
- 8. Enable the **Use Group Resolution** option to use this credential to for resolving groups from the directory.
 - **Note:** Only one credential can be set for group resolution per domain or server.
- 9. Click **Test Credential** to ensure the credential can successfully authenticate with the domain or domain controller before saving the credential.
- 10. Click Save Credential.

New	Directory	Credential
14044	Directory	creacticiat

New Directory cree		
Directory Type		
• Active Directory		
O LDAP		
Credentials		
Title		
Domain		
Use SSL		
Username		
Password		۲
Use Group Res	olution (Optional)	
TEST CREDENTIAL	SAVE CREDENTIAL	DISCARD CHANGES

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

- BeyondTrust
 - 11. To edit a directory credential, select the credential and edit as desired.
 - If you change the **Domain**, **Use SSL** option, or the **Username**, you must change the password.
 - The **Change Password** section expands to display fields to enter and confirm the new password.
 - 12. Click **Test Credential** to ensure the edited credential can successfully authenticate with the domain or domain controller before saving the credential.
 - 13. Click Save Credential.

Add an Active Directory Group

Q Search Directory Credentials		Edit Directory Cred	ential	
Create Dire	ctory Credential 🔂	Title hello		G
Showing all 9 Directory Crede	entials	Domain mydomain.local		C
Group resolution disabled	Û			
gman (Active Directory) Group resolution disabled	童	Use SSL		
Group resolution disabled	Û	theuser		G
Group resolution disabled	Û	CHANGE PASSWORD		
Group resolution enabled	Û	Use Group Reso	olution (Optional)	
hello (Active Directory) Group resolution disabled	ŵ	TEST CREDENTIAL	SAVE CREDENTIAL	DISCARD CHANGES

Active Directory group members can log in to the management console or a specific domain controller and perform tasks based on the

permissions assigned to the group. The group can authenticate against either a domain or domain controller.

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

- 1. Select Configuration.
- 2. Under Role Based Access, select User Management.
- 3. Under Groups, click Create New Group.
- 3. Select Add an Active Directory Group.

BeyondInsight	Onfig Role Bas	uration	ser Management
USER MANAGEMENT 😡			
		GROUPS	
Filter by Greate New Group	1		
📽 Create a New Group		Users	Description
Add an Active Directory Group		0	test
📣 Add an LDAP Group	dmins	0	Users who can create and delete enterprise domain

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.

©2003-2021 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



9

4. Select a credential, or click **Manage Credentials** to add or edit a credential.

	group 🔻
	Manage Credentials
Domain	
local.local	
Filter by Group Name	
*	

- 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.

Note: For performance reasons, a maximum of 250 groups from Active Directory 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.

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



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

ACTIVE DIRECTORY GROUP SEARCH	>
testgroup713	
testgroup512	1
✓ testgroup898	
testgroup831	
testgroup274	
testgroup933	
testgroup652	
testgroup394	•
ADD GROUP CANCEL	

- 9. The group is added and set to **Active** but not provisioned or synchronized with Active Directory. Synchronization with Active Directory to retrieve users begins immediately.
- 10. Once the group has been synced with Active Directory, 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: LOCAL.LOCAL\TESTGROUP898

Has 103 users S Active O Group not provisione	d (last synced on Jan 09, 2020, 3:11 PM)
Group Details	Vsers Ø
Details & Attributes	Show Assigned users Tilter by
Features	Assigned users
Smart Groups	Users not assigned
Users (103)	🗌 Username Name 🔺 Email
API Registrations	testuser1 User1, Test
	🗌 💿 testuser11 User1103, Test
	testuser11 User1193, Test
	Stestuser16 User1635, Test
	User17, Test mmac

10

Note: By default, new groups are not assigned any permissions. You must assign permissions on features and smart groups after creating a new group. For more information on permissions and how to assign them, please see "Assign Group Permissions" on page 14.

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

i

For more information on creating and editing directory credentials, please see "Create and Edit Directory Credentials" on page 7.

Add an LDAP Directory Group

LDAP group members can log in to the management console or a specific domain controller and perform tasks based on the permissions assigned to the group. The group can authenticate against either a domain or domain controller.

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

- 1. Select Configuration.
- 2. Under Role Based Access, select User Management.

3. Under Groups, click Create New Group.

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

BeyondInsight	Configuration Role Based Access 	User Management
USER MANAGEMENT Ø		
	GROUPS	
Tilter by		
Create New Group	_	
Ereate a New Group	lisore	Description
Add an Active Directory Group	0	test
📣 Add an LDAP Group	dmins 0	Users who can create and delete enterprise domain
BeyondInsight	Configuration Role Based Access	User Management
USER MANAGEMENT @		
	GROUPS	
T Filter by		
Create New Group		
E Create a New Group	licore	Description
Add an Active Directory Group	0	test
📣 Add an LDAP Group	dmins 0	Users who can create and delete enterprise domain

4. Select a credential, or click **Manage Credentials** to edit a credential or create a new one.

age Credentials.
FETCH

- 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 wildcard.
- 7. Click Search LDAP.
- 8. Select a group, and then click **Continue to Add Group**.

LDAP GROUP SEARCH	>
SEARCH LDAP	ł
Search Results	1
OracleDBSecurityAdmins Users who can create and delete enterprise domains in this realm, move database	
OracleDBCreators Users who can register databases in this realm, including creating the database	
 OracleNetAdmins Users who can register Network Service Alias in this Oracle Context. 	
OracleDefaultDomain	
OracleContextAdmins Users who can administer all entities in this Oracle Context	•
CONTINUE TO ADD GROUP CANCEL	

12

- 9. Select the Group Membership Attribute and Account Naming Attribute.
- 10. Click Add Group.
- 11. The group is added and set to **Active** but 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.

LDAP GROUP SEARCH	>
Active (yes)	
_{Name} OracleNetAdmins	
Description Users who can register Netwo	ork Service Alias in t
Group Membership attribute uniqueMember	•
Account Naming attribute	•
ADD GROUP CANCEL	
GROUP: LOCAL.LOCAL\TESTGROUP898	st synced on Jan 09, 2020, 3:11 PM)
Group Details	Users O
Details & Attributes	Show Assigned users Tilter by
Features	Assigned users
Smart Groups	Users not assigned
Users (103)	Username Name A Email
API Registrations	User1, Test
	Contestuser11 User1193, Test
	User1635, Test
	User17, Test mmac

13

Note: By default, new groups are not assigned any permissions. You must assign permissions on features and smart groups after creating a new group. For more information on permissions and how to assign them, please see "Assign Group Permissions" on page 14.

For more information on creating and editing directory credentials, please see "Create and Edit Directory Credentials" on page 7.

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

Assign Permissions

Assign Group Permissions

Permissions

Permission	Description
No Access	Users cannot access the selected feature. In most cases, the feature s 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 must be assigned cumulatively. For example, if you want a BeyondInsight administrator to manage configuration compliance scans only, then you must assign **Full Control** for the following features:

- Asset Management
- Benchmark Compliance
- Reports Management
- Scan Job Management
- Scan Management

Assign Features Permissions

- 1. Under Group Details, select Features.
- 2. Filter the list of features displayed in the grid using the **Show** and **Filter by** dropdown lists.
- 3. Select the features you wish to assign permissions to, and then click **Assign Permissions**.
- 4. Select Assign Permissions Read Only, Assign Permissions Full Control, or Disable Permissions.

inow All Features	- T Filter by	View Details
Assign Permissions		+ Assign Permissions Read Only
8 items (1 selected)		+ Assign Permissions Full Contro
Feature Name Change	Permission No access	O Disable Permissions
Feature Name Change Password Safe Domain Management	Permission No access Full Control	Disable Permissions

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.

14 TC: 7/22/2021

15

The following table provides information on the features permissions that 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.
	Note: After you create a group, go to the Analytics & Reporting Configuration page and run the process daily cube job. Data between the management console and the reporting cube must be synchronized.
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.
Audit Manager	Audit Manager on the Configuration page in the management console.
Audit Viewer	Use the Audit Viewer in Analytics & Reporting.
Benchmark Compliance	Configure and run benchmark compliance scans.
Credential Management	Add and change credentials when running scans and deploying policies.
Directory	Grant access to the configuration area where directory credentials are managed. This feature must
Credential Management	be enabled to support access to directory queries as well.
Directory Query Management	Grant access to the configuration area where directory queries are managed. Please note, access to Directory Credential Management must also be granted.
Endpoint Privilege Management	Use the Endpoint Privilege Management module, including asset details and the exclusions section on the Configuration page.
Endpoint Privilege Management for Unix and Linux	Use the Endpoint Privilege Management for Unix and Linux module.
File Integrity Monitoring	Work with File Integrity rules.
License Reporting	View the Licensing folder in Analytics & Reporting (MSP reports, Privilege Management for Windows, Privilege Management for Mac true-up reports, and Assets Scanned report).
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	Read or write managed accounts through the public API.
Password Safe Admin Session	Password Safe web portal admin sessions.
Password Safe Global API Quarantine	Access to the Quarantine APIs.

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

16

Feature	Provides Permissions To:
Password Safe Bulk Password Change	Change more than one password at a time.
Password Safe Domain Management	Check the Read and Write boxes to permit users to manage domains.
Password Safe Role Management	Allow 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.
Patch Management	Use Patch Management module.
Protection Policy Management	Activate the protection policy feature. User groups can deploy policies, and manage protection policies on the Configuration page.
Reports Management	Run scans, create reports, and create report categories.
Scan - Audit Groups	Create, delete, update, and revert audit group settings.
Scan - Job Management	Activate Scan and Start Scan buttons.
	Activate Abort, Resume, Pause, and Delete on the Job Details page.
Scan - Policy Manager	Activate the settings on the Edit Scan Settings view.
Scan - Port Groups	Create, delete, update, and revert port group settings.
Scan - Report Delivery	Allow a user to set report delivery options when running a scan:
	Export Type
	Do not create a report for this vulnerability scan
	Notify when complete
	Email report to
	 Include scan metrics in email (only available for All Audits Scan, PCI Compliance Report, and Vulnerabilities Report)
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.
Session Monitoring	Use the session monitoring features.
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.
User Accounts Management	Add, delete, or change user groups and user accounts.
User Audits	View audit details for management console users on the User Audits page.
Vulnerability Exclusions	Select this option to prevent users from excluding vulnerabilities from the display. You can exclude vulnerabilities from the display to view those that require remediation to satisfy regulatory compliance. In some situations, you might not want all of your users to set an exclusion on a vulnerability.

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

i

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/index.htm.

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.
Benchmark Compliance	Benchmark Management - Full Control.
Connectors	Asset Management and Management Console Access - Full Control.
Organizations	User Accounts Management - Full Control.
Patch Management	Patch Management - Full Control.
Password Safe Connections	Member of the built-in BeyondInsight Administrators group.
Endpoint Privilege Management Module	Management Console Access and Endpoint Privilege Management - Full Control.
Protection Policies	Everyone can access.
Scan Options	Scan Management - Full Control.
SCCM	Patch Management - Full Control.
Services	Member of the built-in BeyondInsight 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.

Assign Smart Groups Permissions

- 1. Under Group Details, select Smart Groups.
- 2. Filter the list of smart groups displayed in the grid using the **Show** and **Filter by** dropdown lists.
- 3. Select the smart groups you wish to assign permissions to, and then click **Assign Permissions**.
- 4. Select Assign Permissions Read Only, Assign Permissions Full Control, or Disable Permissions.



17

Configure Two-Factor Authentication for BeyondInsight and Password Safe Using RADIUS Server

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

After you set up two-factor authentication, users must log in using the two-factor authentication method.

To set up two-factor authentication, you must:

- Configure the RADIUS server.
- Configure the two-factor authentication settings for users.

Configure the RADIUS Server

 Select Configuration > Multi-factor Authentication > Radius two-factor authentication.

MULTI-FACTOR AUTHEN	ITICATION
Radius two-factor authentica Modify Radius multi-factor a	ation ^
Smart Card two-factor author Modify Smart Card multi-fac	tor authentication.
BeyondInsight Cor	figuration
RADIUS Q Search RADIUS allases Create I Showing all 2 RADIUS allases	Create RADIUS Alias You can configure two-factor instance here, then select tw Priority RADIUS Alias
1 qwerty	This field is required.

18

2. Click Create Radius Alias.

- 3. In the Create RADUIS Alias pane, 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.

- 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.
- Initial 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 RADIUS Alias.

Configure RADIUS Two-Factor Authentication Using Duo

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

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

- RADIUS Auto
- RADIUS Challenge
- RADIUS Duo only

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

Follow the steps outlined above in "Configure the RADIUS Server" on page 18, using the following settngs:

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



19

Create RADIUS Alias

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

Configure Two-Factor for a RADIUS Duo-only Configuration

Follow the steps outlined above in "Configure the RADIUS Server" on page 18, using the followng 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.

Alias				
Duo	0			
^{Filter} All domain users	•			
Host 10.101.10.23	0			
Authentication mechanism PAP	•			
Authentication port 1812				
Authentication request timeout				
seconds				
Shared secret	۲			
initial request Forward username and token	•	impt iter RADIUS code:	٥	
Transmit NAS identifiers				

Example: Duo-Only Login Page

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

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

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

Configure Alternate Directory Attribute for RADIUS

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

Note: This setting is optional.

- 1. Select Configuration .
- 2. Under Role Based Access, select Options.
- Under RADIUS Two-Factor Authentication, set the following:
 - Alternate directory attribute: Enter the Active Directory or LDAP attribute that is matched on the RADIUS server to identify the user account. This can be any attribute in Active Directory or LDAP. The default value is extensionName.
 - Enable for new directory accounts: Click the toggle to enable this attribute for new accounts when they are discovered.
- 4. Click Update RADIUS Two-Factor Authentication Options.

20

Configure SecureAuth with Password Safe using RADIUS

Use the following procedures to configure SecureAuth multi-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.

^{©2003-2021} 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: 7/22 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.

 $\overline{}$

 $\mathbf{\Lambda}$

Configure Smart Card Authentication

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. To configure smart card authentication for a user in BeyondInsight and Password Safe, follow the below steps.

1. Select Configuration > Multi-factor Authentication > Smart Card two-factor authentication.

MULTI-FACTOR AUTHENTICATION

Radius two-factor authentication

Modify Radius multi-factor authentication.

Smart Card two-factor authentication

Modify Smart Card multi-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.

SMART CARD AUTHENTICATION

You can configure Smart Card authentication to log in to the system. Your network must already be configured to use Smart Card technology to use this feature.



Enable Smart Cards (Yes)

Allow UPN override on user (No)

UPDATE SMART CARD AUTHENTICATION

*

Note: You must also enable the **Override Smart Card User** setting for the user accounts that use smart cards to authenticate. The User Principal Name is also required. This can be set when creating a new user or editing an existing user.

Multi-Factor Authentication

Override Smart Card User (yes)

User Principal Name

The user principal name is required

TC: 7/22/2021

22

^{©2003-2021} 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.



1/20/2010

Verify the BeyondInsight Server Certificate

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

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

Verify the Web Server Certificate

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

🚡 File Action View Favorites Window Help 🔶 🖄 📰 🗈 🖬 🖬

Sole Root Certificates (Local Compute Personal Certificates Certificates

Personal Certificates Trusted Root Certificatic Enterprise Trust Intermediate Certificatic Trusted Publishers Untrusted Certificates

Third-Party Root Certi

Trusted People Client Authentic Smart Card Trus /eb Ho

used of a Mich Aid

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

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

File	View	Help
Conne	ctions	
0 ,- [.		8
	Start Pag	je
a •	HOMEN	IS01 (HOME\admin.insight)
	👌 Appl	ication Pools
⊿ ··	🧃 Sites	
	🛓 🌏 D	efault Web Site
	⊳ - [aspnet_client
	Þ - f	Clarity
	Þ - f	eEye.RetinaCS.Server
	Þ - f	eEye.RetinaCSClaimsAware
	Þ - f	eEye.RetinaCSSSO
	Þ - f	EventService
	Þ - f	PolicyService
	Þ - f	RetinaCSSC
	Þ	RetinaCSWebgate
	Þ - f	Retinalnsight

eEyeEmsCA eEyeEmsCA HOMEMS01 eEve EMS CA

-HOMECA02-C

ondTrust RevondSAAS MalwareInfo Web4

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. Select Server Certificates.

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



Update Default Web Site Bindings with CA-Issued Certificate

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

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



24



1. Select https, and then click Edit.

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

			Site	Bindings	? X
Туре	Host Name	Port	IP Address	Binding Informa	Add
http		80	*		
https		443	•		<u>E</u> dit
					Remove
					Browse
					-
					Close

Edit Site Bindin	g ? X
Lype: IP address: https V All Unassigned Host name:	P <u>o</u> rt: 4 43
☐ Require Server <u>N</u> ame Indication]
SSL certificate:	
BeyondTrust Web	Select <u>V</u> iew
Not selected HOMEMS01	
BeyondTrust Web	OK Cancel
eEyeEmsServer	

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.
- 3. From the **SSL Certificate** menu, select the **Domain Issued** certificate.
- 4. Click Apply.



25

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

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>/WebConsole/PasswordSafe, where you are prompted to select your certificate and enter your pin. You are logged in using a secure encrypted connection.

Windows Security	/	×
Smart Card Please enter yo	ur authentication PIN.	
	PIN PIN Click here for more information	
	OK Cance	

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. From the left navigation pane in the console, select Configuration.
- 2. Under Role Based Access, select User Management.
- 1. Select the user.
- 2. Click the More Options icon, and then select Edit User Details.
- 3. On the Edit User page, select RADIUS from the Two Factor Authentication list.
- 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.

e@mail4	JSER I.nuii
Username a.name4	1
	Account Quarantined (no)
Multi-F	actor Authentication
	Override Smart Card User (no)
	Disable Forms Login (no)
Two Factor	Authentication
Map Two	o Factor User
Manual	ly Specified
Alterna	te Directory Attribute (extensionName)
Disting	uished Name
User Pr	inciple Name
SAM Ac	count Name
Domair	NUser Name
Map Two Fa	actor User

5. Click Update User.

27

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.

Ŷ	Add Relying Party Trust Wizard
Select Data Source	
Steps	Select an option that this wizard will use to obtain data about this relving party:
Welcome	O lease t data takes if the relation matrix of blacked online or on a lease lease of the
Select Data Source	Use this option to import the percentage data and certificates from a relying party consolitation that nublehas
Configure Multifactor Authentication Now?	tis federation metadata online or on a local network.
 Choose Issuance Authorization Rules 	recercicon metadata accress grost name or UniLJ.
Ready to Add Trust	Example: fs.contoso.com or https://www.contoso.com/app
 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 its federation metadata to a file. Ensure that this file is from a trusted source. This witcard will not validate the source of the file. Federation metadata file location:
	Browse



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	x
You can configure this rule to send a claim group that the user is a member of, and spe	based on a user's Active Directory group me cify the outgoing claim type and value to issu	mbership. Specify the ie.
<u>C</u> laim rule name:		
BILogonGroupMembership1		
Rule template: Send Group Membership as	a Claim	
User's group:		
ADFS\BILogonGroup	Browse	
Outgoing claim type:		
Group	~	
Outgoing name ID format:		
Unspecified	~	
Outgoing claim value:		
AD COLLEGE		

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 shows you how to set up a claims-aware website using the Windows Identity Foundation (WIF) SDK.

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

The selected application's configuration will be mo	dified to trust and accept the claims i	ssued by an existing
STS. Specify the WS-Federation metadata docum	ent location for the existing STS.	
TS WS-Enderation metadata document location -		
15 WS-rederation metadata document location		
ttps://adfsaccount.adatum.com	Browse	Test location

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

Set Up SAML With a Generic Security Provider

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

Configure SAML

To configure SAML, go to the Dashboard or **Menu** and click **Configuration**, then, under **Multi-Factor Authentication**, click **SAML Configuration**.

Identity Provider Settings:

- 1. **Entity ID:** The name of the identity provider (IdP) entry, normally supplied by the provider.
- 2. Single Sign-on Service URL: The SSO URL, from the provider.
- 3. Select SSO URL Protocol Binding type, Redirect or Post.
- 4. Single Logout Service URL: The SLO URL, from the provider.
- 5. Select SLO URL Protocol Binding type, Redirect or Post.
- 6. Under **Encryption and Signing Configuration**, check applicable boxes as required by your service provider.
- 7. Select the **Signature Method** from the dropdown list of methods. The correct method is as required by your IdP.
- 8. Upload the identity provider certificate.

SAML Configu	uration	
Identity Provider	Settings	
Entity ID		±
Single Sign-on Serv	ice URL	
SSO URL Protocol Bindi	ıg	
HTTP Redirect	O HTTP POST	
Single Logout Servi	ce URL	
SLO URL Protocol Bindir	ng	
HTTP Redirect	O HTTP POST	
Encryption and Signing	Configuration	
Sign Authentic	ation Request	Want Logout Request Signed
Sign Logout Re	quest	Override Pending Authentication Request
Sign Logout Re	sponse	Disable Audience Restriction Check
Want SAML Re	sponse Signed	Disable In Response To Check
Want Assertior	n Signed	Disable Inbound Logout
Want Assertior	n Encrypted	Disable Outbound Logout
Want Logout R	esponse Signed	
Signature Method SHA-256		•
Current Identity Provi	der Certificate	
Subject		
lssuer		
Valid from	0001-01-01T0	0:00:00
Valid to	0001-01-01T0	0:00:00
Upload Certificate		
Drop	<i>File to upload (or click)</i>	

^{©2003-2021} 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: 7/22/2021 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.

Θ

BeyondTrust

Service Provider Settings

9. Entity ID: The fully qualified domain, followed by the file name:

https://<serverURL>/eEye.RetinaCSSAML

This is used for the audience restriction.

10. Click SAVE SAML CONFIGURATION.

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

4	Service Provider Settings
	Entity ID
	/eEye.RetinaCSSAML/
	Assertion Consumer Service URL
	/eEye.RetinaCSSAML/SAML/AssertionConsumerService.aspx
	Lownload Certificate
	SAVE SAML CONFIGURATION DISCARD CHANGES

Update Host Name and SAML access URL

Note: This is applicable to on-premises installations only. For PS Cloud or on-premises installations, Access URLs can also be set in the BI configuration.

- 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://<server>/eEye.RetinaCSSAML

- 4. Scroll down to the Host Name field under the Web Site Information section.
- 5. Update it to the fully qualified domain, for example, https://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 Identity Provider (IdP)

Below are some of the values an IdP might need:

- Audience Restriction: https://<server>/eEye.RetinaCSSAML
- SSO Service URL: https://<server>/eEye.RetinaCSSAML/SAML/AssertionConsumerService.aspx
- SLO Service URL: https://<server>/eEye.RetinaCSSAML/SAML/SLOService.aspx
- Service Provider Certificate: (generated when SAML configuration is saved)

Your identity provider needs to provide the following attributes in the assertion:

- Group: (Required) This must match the group created in BeyondInsight or imported from Active Directory. If an Active Directory
 group is used, it must match the BI format Domain\GroupName.
- Name: (Required) This should be the be in the format domain\username or UPN.
- Email: (Optional).
- Surname: (Optional).
- GivenName: (Optional).

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

Configure ADFS with Password Safe Using SAML

Configure ADFS on the Identity Provider Server

- 1. Open the ADFS management console.
- 2. Expand Trust Relationships.
- 3. Right-click Relying Party Trusts.
- 4. Select Add Relying Party Trust.



- 5. Click Start.
- 6. Select Enter data about the relying party manually, and then click Next.

7. Enter a Display name, and then click Next.



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

8. Leave AD FS 2.0 profile selected, and then click Next.

BeyondTrust



- 9. Click **Browse** on the **Configure Certificate** screen to import the service provider (SP) public certificate.
- 10. Navigate to the location of the SP certificate.
- 11. Select the certificate, click Open, and then click Next.



- 12. Select Enable support for the SAML 2.0 WebSSO protocol.
- 13. Enter the **Relying party SAML 2.0 SSO service URL**, and then click **Next**.



33

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

14. Enter the **Relying party trust identifier**, click **Add**, and then click **Next**.

BeyondTrust

Steps	Rebing parties may be identified by one or more unique identifier strings. Specify the identifiers for this
Welcome	relying party trust.
Select Data Source	Relying party trust identifier:
Specify Display Name	https://< <server fqdn="">>/eEye.RetinaCSSAML/ Add</server>
Choose Profile	Example: https://is.contoso.com/adis/services/taust
Configure Certificate	Relying party trust identifiers:
Configure URL	Remove
Configure Identifiers	
 Choose Issuance Authorization Rules 	
Ready to Add Trust	
Finish	

15. Select the preferred method of access, and then click **Next**. The default is **Permit all users**.

Steps	Issuance authorization rules determine whether a user is nemitted to service claims for the reking party
Welcome	Choose one of the following options for the initial behavior of this relying party's issuance authorization
Select Data Source	rues.
Specify Display Name	Permit all users to access this relying party
Choose Pholile	The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may shill deny the user access.
Configure Certificate	
Configure URL	C Deny all users access to this relying party
Configure Identifiers	The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.
 Choose Issuance Authorization Rules 	
Ready to Add Trust	You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Bules in the actions name.
	< Previous Next > Cancel Help
Add Relying Party Trus Ready to Add Trust	
Steps	The tables nature that has been configured. Begins the following retriever and then click Next to add the
Welcome	relying party trust to the AD FS configuration database.
Select Data Source	
Specify Display Name	Monitoring Identifiers Encryption Signature Accepted Claims Organization Endpoints N.
Choose Profile	Specily the monitoring settings for this relying party trust.

This relying party's federation metadata data was last chec

aty was last updated from feder

(Previous Next > Cancel Help

E Monit

< never > This relying :

Ready to Add Trust

Finid

16. Click **Next**, and then click **Close**.

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



- 17. Click Add Rule.
- 18. Select the **Send Group Membership as a Claim** rule template, and then click **Next**.

📬 Add Transform Claim R	ule Wizard 🗙
Select Rule Templat	e
Steps Choose Buile Turne	Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.
Configure Claim Rule	Claim rule template:
	Send Group Membership as a Claim Claim rule template description:
	Using the Send Group Membership as a Claim rule template you can select an Active Directory security group to rend as a claim. Only a single claim will be entitled from this rule, based on the group selected. For example, you can use this use template to carear a rule that will end a group claim will an value of "Admin" if the user is a member of the "Domain Admin" security group. This rule template should only be used for user of the local Active Directory Domain.
	Let me more about this rule template
	Cancel Help

- 19. Enter a name for the claim rule.
- 20. Select the User's group.
- 21. Select the Outgoing claim type.
- 22. Select the Outgoing claim value.
- 23. Click Finish.

Note: The outgoing Group claim must match exactly what is in BeyondInsight.



- 24. Click Add Rule.
- 25. Select the **Send LDAP Attributes as Claims** rule template, and then click **Next**.

Select Rule Templat	e
Steps	Select the template for the claim rule that you want to create from the following list. The description
Choose Rule Type	provides details about each claim rule template.
 Configure Claim Rule 	Claim rule template:
	Send LDAP Atributes as Claims Claim rule template description:
	Ling the Evert LDMP Altibute as Claims rule tanglate you can select altibutes into an LDAP altibutes store such a chocke Directory to end at claims to the relings pays, Margin altibutes may be card as multiple claims from a single rule using the rule type. For example, you can use the rule tanglate to create a rule that will exist at thibute values for some rule rule rule pays. The directory altibutes and then send those values as two different outgrand telephoneNumber Achen Directory attributes and then send those values as two different outgrand telephoneNumber Achen Directory attributes and then send those values as two different outgrand claims. The rule may dive be used to low of all of them send those values as two different outgrand individual group memberships, use the Send Group Membership as a Claim rule template.



- 26. Enter a Claim rule name.
- 27. Select the Attribute store.
- 28. Select User-Principal-Name for the LDAP Attribute.
- 29. Select Name as the Outgoing Claim Type.
- 30. Click Finish.

💱 Add Transform Claim Ri	ule Wizard			
Configure Rule				
Steps Choose Rule Type Configure Claim Rule	You o which issue Claim Name Rule I	an configure this tube to send the to extract LDAP athibutes. Specific the from the tube. rule name: Final send LDAP Athibutes of the store.	e values of L sity how the as Claims	DAP attributes as claims. Select an attribute store from attributes will map to the outgoing claim types that will be
	Activ	ve store: e Directory ing of LDAP attributes to outgoin	g claim type	x
		LDAP Attribute		Outgoing Claim Type
	_	User-Principal-Name	<u> </u>	Name 💌
				_
			(Pre	uinu [Erich] Curvel [Math

- 31. On the Relying Party Trusts page, right-click BT Service Provider, and then select Properties.
- 32. Select the **Signature** tab.
- 33. Click **Add**, and then enter the service provider public certificate.

isplay Name		Enabled	Identifier	
disweb.trejsesearch.net		Yes	https://adfsweb.treyre	:earch.net/eEy
Service Provider		Yes	https://adfsweb.treyre	tearch.net/eEy
81	Service Provider P	roperties		×
	Accepted Claims	Organization	Endpoints Notes	Advanced
	Monitoring	Identifiers	Encryption	Signature
	Specify the signature	e verification certi	ficates for requests from t	his relaind
	party.	e remeaner een		in reging
	Cubicat	Leaver	Effective Date	Euclidia
	Subject	CNmmm to c	11/22/2013 4/2	12/31/5
			011 1172272010 4.E	120111
	1			
	•			
	Add.	View	Remove	
-				
	OK	Cano	el Apply	Help

Configure SAML on the Service Provider Server (UVM)

To configure SAML, go to the Dashboard or **Menu** and click **Configuration**. Under **Multi-Factor Authentication**, click **SAML Configuration**.

Identity Provider Settings:

- 1. **Entity ID**: The name of the identity provider (IdP) entry, normally supplied by the provider.
- 2. Single Sign-on Service URL: The SSO URL, from the provider.
- 3. Select SSO URL Protocol Binding type, Redirect or Post.
- 4. Single Logout Service URL: The SLO URL, from the provider.
- 5. Select SLO URL Protocol Binding type, Redirect or Post.

Encryption and Signing Configuration:

 Depending on IdP configuration, check any of the first 3 settings, Sign Authentication Request, Sign Logout Request, and Sign Logout Response.

7. Check the appropriate service provider (SP) settings.



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	1
Signature Method SHA-256	•

Encryption and Signing Contiguration 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	_

8. Check any required miscellaneous settings.



9. Select the **Signature Method**, from the dropdown list of methods. The correct method is as required by your IdP.

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 SHA-256	•
Current Identity Provider Certificate	
Subject	

0001-01-01T00:00:00

0001-01-01T00:00:00

Drop File to upload (or click)

10. Upload the identity provider certificate.

Service Provider (SP) Settings:

- 11. Entity ID: The fully qualified domain, followed by the file name: https://<serverURL>/eEye.RetinaCSSAML
- 12. Click SAVE SAML CONFIGURATION.
- 13. Once the SAML configuration is saved, a public SP certificate is available to download and upload to the IdP, if required.

Entry ID https://adfsweb.treyresearch.net/eEye.RetinaCSSAML/	8
Assertion Consumer Service URL https://adfsweb.treyresearch.net/eEye.RetinaCSSAML/SAML/AssertionC	ConsumerService.asp
📩 Download Certificate	
Service Provider Settings	
Entity ID https://adfsweb.treyresearch.net/eEye.RetinaCSSAML/	0

https://adfsweb.treyresearch.net/eEye.RetinaCSSAML/SAML/AssertionConsumerService.aspx

📥 Download Certificate

Issuer Valid from

Valid to

Upload Certificate



Configure Okta with Password Safe

- 1. Log in to the Okta admin portal.
- 2. Click Add Application.

3. Click Create New App.

- 4. Select **SAML 2.0** as the sign-in method.
- 5. Click Create.

okta. Deshboerd						Applications 😐
Add and configure an application that can be assigned users IPL Add Application IPL Add Application Active - 2 Inactive - 3	I to your ssign Applications					Applications Help
SAMLOOI SAMLOOI SAMLOOI				Active •	Active Applications These apps are configur assigned to people. Dee removes it time every us Deleting an app deactive its settings. Embed links to your ap Links to a nop from a po location outside of Okta- link.	ed and can be covering an app ents home page, tes it and discerds plications tail or other using it's embed
okta Deshboard Director	y Applications	Security F	Reports Se	mings	My	Applications 😁
HAdd Application					-	Back to Applications
QI		All	ABCDE	FGHIJKLM	NOPORST	JVWXYZ
Can't find an app? Creste New App		Teladoc Okta Verified				Add
Apps you created (2) →	&frankly	&frankly Okta Venified V S	SAML			Add
okta Dashboard Directory	Applications	Security R	leports Sei	tings	16	, Applications
🛱 Add Application					-	Back to Applications
		All	ABCDE	FGHIJKLM	NOPQRST	u v w x y z
Can't find an app? Create New App	O TELADOC	Teladoc Okto Verified				Add
Apps yn create a New Appli	cation Integratio	n			×	Add
INTEGRATION PS Sign on method		O Secure Web A Users credent	Authentication (SV Sals to sign in. Thi	(A) is integration works wit	th most apps.	Add
Supports SAML Supports Provisi		SAML 2.0 Uses the SAM than SWA, if the	II, protocol to log he app supports I	users into the app. Thi L	s is a better option	Add
CATEGORIES				Create	Cancel	Add
Content Management 179 Collaboration 704	15Five	15five Okta Verified VS				Add

39

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

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



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.
- 17. Add attributes, and then click Next.
 - **Group:** 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**.
 - Name: (optional)
 - Email: (optional)
 - Surname: (optional)
 - GivenName: (optional)

Name					
	Name format	(optional)	Value		
Name	Unspecifie	Hd +	user.email		•
Group	Unspecifie	۰ bi	OktaUser		*
Email	Unspecifie	۰ bi	user.email		*
GivenName	Unspecifie	rd +	user.frstName		Ŧ
Surname	Unspecifie	id v	user.lastName		¥
Add Another					
GROUP ATTRIBUTE	STATEMENTS (OPT	IONAL)			
Name	Name format	(optional)	Filter		
	Unspecifie	id v	Starts with		
Add Another					
Preview the SAML	assertion general	ted from	the information abo	ve	
s shows you the XML	that will be used in th	ne assertio	and a second sec		
			n - use it to verify the i	nfo you entered above	P
revious Cr	ancel		n - use is to verify the i	nfo you entered above	o Ni
revious Ca	ancel		forward the applicat	nfo you entered above	° N
revious Cr Help Okta Suppor	ncel t understand how r partner?	you con	figured this applicat an Okta customer addi	Ion Ig an internal app ke to integrate my app	p with Okta
revious C4 Help Okta Suppor Are you a customer or The optional 4	t understand how r partner?	you con i'm a ist Okta Si	figured this applicat an Okta customer addi a software vendor. I'd il	Ion ng an internal app ke to integrate my apj g your app integration	p with Okta
revious Ca Help Okta Suppor Are you a customer or The optional i	t understand how r partner? questions below assi	you con i'm i ist Okta Si This	figured this applicat an Okta customer addi a software vendor. I'd il upport in understandin i is an internal app that	Ion Ig an Internal app ke to Integrate my apj g your app Integration we have created	p with Okta
revious Ca Help Okta Suppor Are you a customer or The optional i App type @ Contact app vendor	t understand how r partner? questions below assi	you con I'm i I'm i It's i	figured this applicat an Okta customer addi a software vendor. I'd li upport in understanding is an internal app that equired to contact the	Ion Ion g an internal app ke to integrate my apj g your app integration we have created vendor to enable SAN	P with Okta
revious C4 Help Okta Suppor Are you a customer of The optional 4 App type Contact app vendor Which app pages did	t understand how r partner? questions below assi	you con in im	Ingured this applicat an Okta customer addi a software vendor. I'd li upport in understandin is an internal app that equired to contact the	Ion Ig an Internal app ke to Integrate my app g your app Integrated we have created vendor to enable SAM	p with Okta
revious C4 Help Okta Suppor Are you a customer o The optional a App type Contact app vendor Which app pages did Enter links, describe	t understand how r partner? questions below assi you consult to config where the pages are	you con Trm t Trm t This It's f gure SAM	figured this applicat an Okta customer addi a software vendor. I'd li upport in understanding it is an internal app that equired to contact the E2 E2	for Ig an internal app ke to integrate my app g your app integration we have created vendor to enable SAN	p with Okta
revious Ca Help Okta Suppor Are you a customer or The optional a App type Contact app vendor Which app pages did Enter links, describe Did you find SAML do	r partner? questions below assi you consult to confir where the pages are cs for this app?	you con I'm i I'm i I'm i I'm i It's i It's i gure SAM 	In clock to very bern figured this applicat an Okta customer addi a software vendor. I'd li upport in understanding is an internal app that equired to contact the L2 L2	ION ION Ig an Internal app ke to Integrate my app gyour app Integration we have created vendor to enable SAN	p with Okta
tevious Ca Help Okta Suppor Are you a customer or The optional i App type Contact app vendor Which app pages did Enter links, describe Did you find SAML do Enter any links here	t understand how r partner? questions below assi you consult to confif where the pages are cs for this app?	you con into the second secon	figured this applicat an Okta customer addli a software vendor. I'd il upport in understanding is an internal app that equired to contact the current to contact the current to contact the current to contact the	Ion Ion Ig an Internal app ke to Integrate my apj g your app Integration we have created vendor to enable SAN ipful	P with Okte
	t understand how r partner? questions below assi you consult to confir where the pages are cs for this app?	you con image: Image:	In duck to very bern figured this applicat an Okta customer addi a software vendor. I'd li upport in understanding is an internal app that equired to contact the L2 L2	Ion Ion internal app ke to integrate my app g your app integration we have created vendor to enable SAN ilpful	p with Okta
revious Col Help Okta Suppor Are you a customer o The optional o App type Contact app vendor Which app pages did Enter links, describe Did you find SAML do Enter any links here Naty tips or additional Ploceholder text	t understand how r partner? questions below assi you consult to confly where the pages are cs for this app? comments?	you con image: frm of the first of the firs	In clock to very bern ingured this applicat an Okta customer addit a software vendor. I'd li upport in understandin is an internal app that equired to contact the equired to contact the L2	ION ION Ig an Internal app ke to Integrate my app g your app Integration we have created vendor to enable SAN Ipful	p with Okta
revious Ca Help Okta Suppor Are you a customer of The optional of App type Contact app vendor Which app pages did Enter links, describe Did you find SAML do Enter any links here Did you find SAML do Enter any links here	ancel t understand how r partner? questions below ossi you consult to confly where the pages are cs for this app? comments?	you con i I'm i I'm i i I'm i st Okta Si i I'hi It's ri gure SAM a, or anyth	Ingured this applicat an Okta customer addi a software vendor. If d ii upport in understanding is an internal app that equired to contact the E?	Ion Ig an internal app ke to integrate my app g your app integrated vendor to enable SAN ipful	p with Okta

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

41



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	s			E
SIGN (ON METHODS	ermines how a	a user signs int	o and manages their credentials for an application. Some sig
onmet	ious require audi	uonai comigu	radon in the Sr	a party application.
• s	AML 2.0			
	Default Relay St	tate		
€	SAML 2.0 IS View Setu	not configure	ed until you cor	mplete the setup instructions.
	Identity Prov	nder metadati	a is available if	this application supports dynamic configuration.
CREDE	NTIALS DETAIL	S		
Applica	tion username fo	rmat	Okta us	sername
Decou	and reveal			
Passwo	ord reveal			ow users to securely see their password (Recommended)
Identity Prov	ider Single Sign-On U	IRL:		
Identity Prov	ider Single Sign-On U	IRL:		
https://dentity.	ider Single Sign-On U	IRL:	dtrustdev 22245 _p	asswcródafe_1/ezki 12345 0000.07p0h7/sso∕saml
https://d	ider Single Sign-On U lev- 22345 .oktaprevie	IRL: w.com/app/beyon	dtrustdev 22845 _p	asswordsafe_1/eski 32343 (qp0,07)gb/h7/sso/sam1
https://dentity Prov	ider Single Sign-On U lev- 12345 .oktaprevie ider Single Logout UR	IRL: w.com/app/beyon RL:	dtrustdev 22845 _p	asseer/hafe_1/res/1234500.01p0/7/soc/set1
https://dentity Prov	ider Single Sign-On U lev- 22385 okteprevie ider Single Logout UF	IRL: w.com/app/beyon RL:	dtrustdev 22845 _p	asserritarfs_1/em/12049000_07p0/7/ass/uml
Identity Prov	ider Single Sign-On U lev- 12585 oktaprevie ider Single Logout UF lev- 12585 oktaprevie	IRL: w.com/app/beyon RL: w.com/app/beyon	ðtrustdev 22845 _p dtrustdev 42846 _p	asserretus (*) / res: 120451000.01;00/17/00/17/00/14/01 asserretus (*) / res: 1204510000.01;00/17/01/14/01
Identity Prov	ider Single Sign-On U lev- 12585 : oktoprevie ider Single Logout UF lev- 12585 : oktoprevie	IRL: w.com/app/beyon RL: w.com/app/beyon	dtrustder 22845 _p dtrustder 49888 _p	asserrbafe_1/msv. 12345 000.07p0*7/sac/aml
Identity Prov https://d Identity Prov https://d	ider Single Sign-On U lev-12585: oktaprevie ider Single Logout UF lev-12585: oktaprevie ider Issuer:	IRL: w.con/app/beyon RL: w.con/app/beyon	dtrustder 22345 _p dtrustder 193345 _p	asseer flasfe, 1 / res. 1234500.01;00:7/10:/140/1401 asseer flasfe, 1 / res. 22345000.01;00:7/16/1401
Identity Prov https://d Identity Prov https://d	ider Single Sign-On U Iev- 12345 Attaprevie Ider Single Logout UR Iev- 12385 , oktaprevie Ider Issuer:	RL: w.con/app/beyon RL: w.con/app/beyon Standa strinen?	ótrustórv 22845 _p ótrustórv 49326 _p	asseer that fr., 1 / res. 1234500.01/p0/7./soc/soc) asseer that fr., 1 / res. 12345000.01/p0/7./soc/soc)
Identity Prov https://d Identity Prov https://w	ider Single Sign-On U lev-122345 oktaprevie Ider Single Logout UF lev-22345 oktaprevie Ider Issuer: w. okta.com/ebk12342	IRL: w.com/app/beyon RL: w.com/app/beyon BoboLetpdn7	dirustór 22845 _p	asseerfulafe,1/res/1 2345 000.07p07/rss/sen] asseerfulafe,1/res/1 2245 0000.07p07/ris/sen]
Identity Prov https://d Identity Prov https://d Identity Prov https://d	ider Single Sign-On U iev-122385 oktaprevie ider Single Logout UF iev-22385, oktaprevie ider Issuer: w. okta. com/eski12342 cote:	IRL: wcom/app/beyon RL: wcom/app/beyon	dirustór 22845 _p	asserfasfr,1/mi-12345000,07(x07/s0/sm)
Joentty Prov Mttps://w Identty Prov Mttps://w Identty Prov Mttps://w X509 Certif X509 Certif X509 Certif X509 Certif X509 Certif X1000cc X100cccc X100ccccc X100ccccc X100cccccc X100ccccc	dee Single Sign-On U re-12383 integres/e re-22383 integres/e	IRL: 		asser the fr, 1/rssi 12345000,00,00,00,00,00,00,00,00,00,00,00,00
beening Prov been		IRL: 		essent/bafe,1/res/12345000.01(p0/7/sio/sel essent/bafe,1/res/12345000.01(p0/7/sio/sel essent/bafe,1/res/12345000.01(p0/7/sio/sel essent/bafe,1/res/12345000.01(p0/7/sio/sel essent/bafe,1/res/12345000.01(p0/7/sio/sel essent/bafe,1/res/12345000.01(p0/7/sio/sel essent/bafe,1/res/12345000.01(p0/7/sio/sel essent/bafe,1/res/12345000.01(p0/7/sio/sel essent/bafe,1/res/12345000.01(p0/7/sio/sel essent/bafe,1/res/12345000.01(p0/7/sio/sel essent/bafe,1/res/12345000.01(p0/7/sio/sel essent/bafe,1/res/123450000.01(p0/7/sio/sel essent/bafe,1/res/12345000.01(p0/7/sel essent/bafe,1/res/12345000.01(p0/7/sel essent/bafe,1/res/12345000.01(p0/7/sel essent/bafe,1/res/123450000.01(p0/7/sel essent/bafe,1/res/12345000000000000000000000000000000000000
Deentity Prov Mttps://w Ideentity Prov Mttps://w Ideentity Prov Mttps://w Ideentity Prov Mttps://w X509 Centif X5	dee Single Sign-On U we-12928; integrevie we-22928; integr	IRL: 		asserrins fr., 1/assi 123450000,07(x07/ass/ass1

Configure SAML in Password Safe

23. Go to the Dashboard or Menu and click Configuration, then, under Multi-Factor Authentication, click SAML Configuration.

- 24. For Entity ID, enter the Okta value Identity Provider Issuer.
- 25. For Single Sign-on Service URL, enter the Okta value Identity Provider Single Sign-On URL.
- 26. If available, set **Single Logout Service URL** to Okta value **Identity Provider Single Logout URL**.
- 27. Click HTTP POST Protocol Binding for SSO and SLO.

28. Under **Encryption and Signing Configuration**, check applicable boxes. A typical configuration is shown; however, depending on your Okta settings, some configuration selections may be different.

29. Upload Okta X.509 certificate.

- 30. Enter the service provider Entity ID.
- 31. Click SAVE SAML CONFIGURATION.
- 32. Once the SAML configuration is saved, a public SP certificate is available to download. It can be uploaded to the IdP if required.

and the second se	Beyond	Insight	Configuration
	6	BeyondTrust	> General > SAML Configuration
	SAML Cor	nfiguration	
		0	
	Identity Pro	vider Settings	
	http://www.o	kta.com/exki2343v3	39bGL0Yp0h7
	Single Sign on Ser https://dev-12	vice URL 2345.oktapreview.co	om/app/beyondtrustdev12345_passwordsafe_1/ 🕲
	SSD URL Protoco	i Binding	
	O HTTP Red	irect 🔘 HTTP PO	ST
	Single Logout Sen https://dev-12	vice URL 2345.oktapreview.co	om/app/beyondtrustdev12345_passwordsafe_1/ 🚱
	SLO URI Protoco	Rinding	
	O HTTP Red	irect 🔘 HTTP PO	ST
ncrypti	ion and Signing Co	infiguration	
Sig	gn Authenticat	ion Request	✓ Want Logout Request Signed
Sig	gn Logout Req	uest	Override Pending Authentication Request
Sig	gn Logout Res;	ponse	Disable Audience Restriction Check
Wa	ant SAML Resp	oonse Signed	Disable In Response To Check
Wa	ant Assertion S	Signed	Disable Inbound Logout
w	ant Assertion 8	Encrypted	Disable Outbound Logout
_ ···			
Wa	ant Logout Res	sponse Signed	
Wa	ant Logout Res re Method	sponse Signed	
Wa Wa SHA-25	ant Logout Res re Method 56	sponse Signed	
Wa Ignatur HA-29	ant Logout Res e Method 56	sponse Signed	•
Watur gnatur HA-29 urrent	ant Logout Re: 19 Method 56 Identity Provider	sponse Signed Certificate E=info@okta.co Francisco, S=Cal	m, CN=dev OU=SSOProvider, O=Okta, L=San Ifornia, C=US
Wa gnatur HA-29 urrent ubject	ant Logout Re: * Method 56 Identity Provider	certificate Ewinfo@okta.co Francisco, S=Cal Ewinfo@okta.co Francisco, S=Cal	m, CN=dev OU=SSOProvider, O=Okta, L=San Ifornia, C=US m. CN#dev OU=SSOProvider, O=Okta, L=San Ifornia, C=US
Wi gnatur HA-29 urrent abject suer alid fro	ant Logout Res te Method 56 Identity Provider	Certificate E=info@okta.co Francisco, S=Cal E=info@okta.co Francisco, S=Cal 2018-10-10T16:	m, CN=dev OU=SSOProvider, O=Okta, L=San Ifornia, C=US OU=SSOProvider, O=Okta, L=San Ifornia, C=US 30:542
Wi gnatur HA-2: uurrent ubject swer alid fro alid to	ant Logout Res ie Method 56 identity Provider	Certificate E=info@okta.co Francisco,S=Cai E=info@okta.co Francisco,S=Cai 2018-10-10T16: 2028-10-10T16:	m. CN=dev OU=SSOProvider, O=Okta, L=San Iifornia, C=US OU=SSOProvider, O=Okta, L=San Iifornia, C=US 30:54Z 31:54Z
Wi (gnatur HA-2: Uurrent ubject alid fro alid to Jpload	ant Logout Res te Method 56 Identity Provider om	Certificate E=info@okta.co Francisco, S=Cal E=info@okta.co Francisco, S=Cal 2018-10-10T16: 2028-10-10T16:	m, CN=dev OU=SSOProvider, O=Okta, L=San lifornia, C=US m, CN=dev OU=SSOProvider, O=Okta, L=San lifornia, C=US 30:542 31:542
Willingnatur Ignatur HHA-21 Lurrent Lubject Isiser Ialid fro Ialid to	ant Logout Re: e Method 56 Identity Provider am d Certificate Drop Fil	Certificate E=info@okta.co Francisco, S=Cal E=info@okta.co Francisco, S=Cal 2018-10-10T16: 2028-10-10T16: 2028-10-10T16:	m, CN=dev OU=SSOProvider, O=Okta, L=San Ifornia, C=US m, CN=dev OU=SSOProvider, O=Okta, L=San Ifornia, C=US 30:542 31:542
Wi Ignatur HA-22 Uurrent ubject suer alid fro alid to	ant Logout Res e Method 56 identity Provider om d Certificate Drop Fil (or	certificate E=info@okta.co Francisco, S=Cal E=info@okta.co Francisco, S=Cal 2018-10-10T16: 2028-10-10T16: 2028-10-10T16:	m, CN=dev OU=SSOProvider, O=Okta, L=San lifornia, C=US m, CN=dev OU=SSOProvider, O=Okta, L=San lifornia, C=US 30:542 31:542
Wi Wi Wirrent Wire	ant Logout Re: e Method 56 Identity Provider om d Certificate Drop Fil (or projee Provide	Certificate E=info@okta.co Francisco.S=Cal E=info@okta.co Francisco.S=Cal 2018-10-10T16: 2028-10-10T16: 2028-10-10T16: e to upload click) er Settings	m. CN=dev OU=SSOProvider, O=Okta, L=San lifornia, C=US m, CN=dev OU=SSOProvider, O=Okta, L=San lifornia, C=US 30:542 31:542
Wi Wi Wirrent Wirrent Wirrent Wirrent Sorr Ser Entre	ant Logout Res te Method 56 Identity Provider orn d Certificate Drop Fil (or rvice Provide	Certificate E=info@okta.co Francisco, S=Cal E=info@okta.co Francisco, S=Cal 2018-10-10T16: 2028-10-10T16: 2028-10-10T16: e to upload r click/ er Settings	m, CN=dev OU=SSOProvider, O=Okta, L=San lifornia, C=US m, CN=dev OU=SSOProvider, O=Okta, L=San lifornia, C=US 30:542 31:542
Wi ignatur HHA-22 Uurrent iubject ssuer /alid fro Jpload Sert Entti http	ant Logout Res e Method 56 Identity Provider am d Certificate Drop Fil (or prvice Provide ps://FQDN/eEj	Certificate E=info@okta.co Francisco, S=Cal E=info@okta.co Francisco, S=Cal 2018-10-10T16: 2028-10-10T16: 2028-10-10T16: e to upload r click) er Settings ye.RetinaCSSAM	m, CN=dev OU=SSOProvider, O=Okta, L=San lifornia, C=US m, CN=dev OU=SSOProvider, O=Okta, L=San lifornia, C=US 30:542 31:542
Wi Wi WithA-2:	ant Logout Res e Method 56 Identity Provider am d Certificate Drop Fil (al rvice Provide hy ID ps://FQDN/eEj ertion Consumer S	Certificate E=info@okta.co Francisco, S=Cal E=info@okta.co Francisco, S=Cal 2018-10-10T16: 2028-10-10T16: 2028-10-10T16: 2028-10-10T16: et o upload r click) er Settings ye.RetinaCSSAM	m, CN=dev OU=SSOProvider, O=Okta, L=San Ifornia, C=US OU=SSOProvider, O=Okta, L=San Ifornia, C=US 30:542 31:542
Wi (gnatur HA-2) (urrent ubject alid fro alid fro alid fro alid to Ser Entry Asso http	ant Logout Res e Method 56 identity Provider am d Certificate Drop Fill (or vrice Provide ps://FQDN/eEj ps://FQDN/eEj	Certificate E=info@okta.co Francisco.S=Cal E=info@okta.co Francisco.S=Cal 2018-10-10T16: 2028-10-10-100-100-100-100-100-100-100-100-	m, CN=dev OU=SSOProvider, O=Okta, L=San Ifornia, C=US 0U=SSOProvider, O=Okta, L=San Ifornia, C=US 30:542 31:542 L L

DISCARD CHANGES

SAVE SAML CONFIGURATION

Configure Ping Identity with Password Safe

- 1. Log in to the Ping Identity admin portal.
- 2. Click the Add Application button, and then select New SAML Application from the menu.



- 3. Fill in Application Name and Description.
- 4. Set Category to Other, and then click Continue to Next Step.

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

https://<ServerURL>/eEye.RetinaCSSAML/saml/Asserti onConsumerService.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.

44

- 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).

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	3
5	GivenName	First Name	As Literal Advanced	3

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

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

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

Configure SAML in Password Safe

- 10. Go to the Dashboard or Menu and click Configuration, then, under Multi-Factor Authentication, click SAML Configuration.
- 11. For Entity ID, enter the Okta value Identity Provider Issuer.
- 12. For Single Sign-on Service URL, enter the Okta value Identity Provider Single Sign-On URL.
- 13. If available, set **Single Logout Service URL** to Okta value **Identity Provider Single Logout URL**.
- 14. Click HTTP POST Protocol Binding for SSO and SLO.



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

46

15. Under **Encryption and Signing Configuration**, check applicable boxes. A typical configuration is shown, however, depending on your Ping settings, some configuration selections may be different.

	ntication Request	Want Logout Request Signed
Sign Logout	: Request	Override Pending Authentication Reques
Sign Logout	Response	Disable Audience Restriction Check
Want SAML	Response Signed	Disable In Response To Check
🛃 Want Asser	tion Signed	Disable Inbound Logout
Want Asser	tion Encrypted	Disable Outbound Logout
SHA-256		•
SHA-256 Current Identity Pr	ovider Certificate E≈info®okta.c	om. CN=dev OU=SSOProvider. O=Okta. La
SHA-256 Current Identity Pr Subject	ovider Certificate E=info@okta.c Francisco, S=C	om, CN=dev OU=SSOProvider, O=Okta, L= alifornia, C=US
SHA-256 Current Identity Pr Subject Issuer	ovider Certificate E≖info@okta.c Francisco, S=C E≈info@okta.c Francisco, S=C	om. CN=dev OU=SSOProvider, O=Okta, Le alfornia, C=US om. CN=dev OU=SSOProvider, O=Okta, Le alfornia, C=US
SHA-256 Current Identity Pr Subject Issuer Valid from	ovider Certificate E=info@okta.c Francisco, S=C E=info@okta.c Francisco, S=C 2018-10-10T16	om. CN=dev OU=SSOProvider. O=Okta, L= allfornia, C=US om. CN=dev-OU=SSOProvider, O=Okta, L= allfornia, C=US s:30:54Z
SHA-256 Current Identity Pr Subject Issuer Valid from Valid to	ovider Certificate E=info@okta.c Francisco.S=C E=info@okta.c Francisco.S=C 2018-10-10T16 2028-10-10T16	om, CN=dev OU=SSOProvider, O=Okta, L= alifornia, C=US om, CN=dev OU=SSOProvider, O=Okta, L= alifornia, C=US 5:30:54Z 5:31:54Z
SHA-256 Current Identity Pr Subject Issuer Valid from Valid to Upload Certifica	ovider Certificate E=info@okta.c Francisco, S=C E=info@okta.c Francisco, S=C 2018-10-10T16 2028-10-10T16 te	OU=SSOProvider, O=Okta, L= alfornia, C=US OU=SSOProvider, O=Okta, L= alfornia, C=US s:30:54Z 5:31:54Z

- 16. Upload Ping X.509 certificate.
- 17. Enter the service provider Entity ID.

BeyondTrust

- 18. Click SAVE SAML CONFIGURATION.
- 19. Once the SAML configuration is saved, a public SP 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

47

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 https://support.microsoft.com/en-us/kb/327825.

Authentication Errors when using SAML 2.0 Web Applications

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

Runtime Error

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

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 Eri	ror
escription: An ap	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 running on
Netallis: To enable t	e details of this specific enor message to be viewable on remote machines, please create a «customEnors» tag within a "web config" configuration file located in the root directory of the current web application. This «customEnors» tag
hould then have its "	noon" attribute set to "Off".
d. which	fig reafiguration file
< web.com	ag contager state>
<pre><configurati <system.<="" pre=""></configurati></pre>	n>
ccus	tomErrors mode="Off"/>
<td>los</td>	los
Inters The current	any page way be seened as the evolution for a market second to a market second to a first backet all advants all the second second second second to a market second
class Web Con	fig configuration file
1 23	>
23	> <system.web></system.web>
23 24 25	> <aystem.veb> <!--</td--></aystem.veb>
1 23 1 24 1 25 1 26	> <system.web> <!--<br-->Set compilation debug="true" to insert debugging</system.web>
1 23 1 24 1 25 1 26 1 27	> <system.web> <!--<br-->Set compilation debug="true" to insert debugging symbols into the compiled page. Because this</system.web>
23 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>
1 23 1 24 1 25 1 26 1 27 1 28 29	> <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 during development.</system.web>
1 23 1 24 1 25 1 26 1 27 1 28 1 29 30	> <pre><-> </pre> <pre></pre> <pre></pre> <pre></pre> <pre></pre> <pre>Set compilation debug="true" to insert debugging symbols into the compiled page. Because this <pre>affects performance, set this value to true only during development></pre></pre>
23 24 25 26 27 28 29 30 31	> <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 during development. > <compilation debug="true" targetframework="4.5"></compilation></system.web>
23 24 25 26 27 28 29 30 31 32	> <pre></pre> <pre><-> </pre> <pre></pre>
1 23 1 24 1 25 1 26 1 27 1 28 1 29 1 30 1 31 33	> <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 during development. > ccompilation debug="true" targetFramework="4.5" /> <authentication mode="Forms"> <authentication mode="Forms"></authentication></authentication></system.web>
23 24 25 26 27 28 29 30 31 32 33 34	<pre>> <system.web> <!-- Set compilation debug="true" to insert debugging</td--></system.web></pre>
23 24 25 26 27 28 30 31 32 33 33 34 35	> <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 during development. > <compilation debug="true" targetframework="4.5"></compilation> <authentication mode="Forms"> <formsme="servicefrovider" loginurl="login.aggx"></formsme="servicefrovider"> <fauthentication></fauthentication></authentication></system.web>
23 24 25 26 27 28 29 30 31 32 33 34 34 35 36	<pre>> <system.web> <> <> <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"></compilation> <authentication mode="forma"> </authentication> </system.web></system.web></pre>
23 24 25 26 27 28 29 30 31 32 33 34 35 36 37	> <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 during development. > <compilation debug="true" targetframework="4.5"></compilation> <authentication mode="Forms"> <forms loginutl="login.mggx" mame="ServiceProvider"></forms> <fauthentication> <authentication> <authentication></authentication></authentication></fauthentication></authentication></system.web>

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 appliance.
- 2. Browse to the SAML website, and then double-click **Default Document**.



48

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

49



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



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