



BeyondTrust

BeyondInsight and Password Safe Authentication Guide 7.0

Table of Contents

BeyondInsight and Password Safe Authentication Guide	3
Create and Configure Groups in BeyondInsight	4
Create a BeyondInsight Local Group	4
Create and Edit Directory Credentials	6
Add an Active Directory Group	7
Add an LDAP Directory Group	10
Assign Group Permissions	13
Assign Features Permissions	13
Assign Smart Groups Permissions	16
Configure Two-Factor Authentication for BeyondInsight and Password Safe Using RADIUS Server	17
Configure the RADIUS Server	17
Configure RADIUS Two-Factor Authentication Using Duo	18
Configure Alternate Directory Attribute for RADIUS	19
SAML Setup With a Generic Security Provider	20
Configure SecureAuth with Password Safe using RADIUS	24
Configure AD FS with Password Safe Using SAML	25
Configure Smart Card Authentication	32
Configure Two-Factor Authentication Settings for User Accounts	36
Configure a Claims-Aware Website in BeyondInsight	38
Configure Okta with Password Safe	41
Configure Ping Identity with Password Safe	46
Troubleshoot Authentication Issues	49

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.

To allow a user to log into BeyondInsight using BeyondInsight authentication, the user account must reside in the BeyondInsight database.

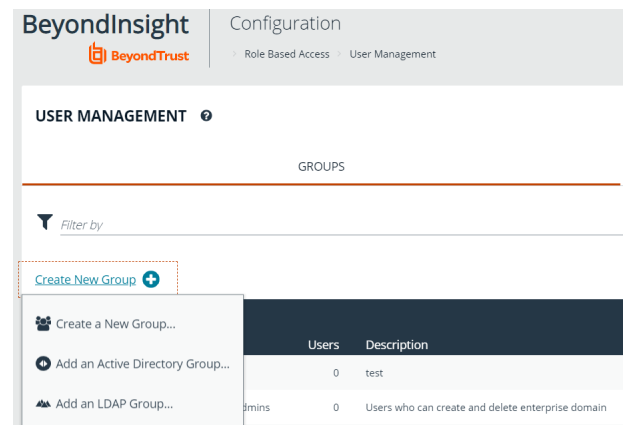
Create and Configure Groups in BeyondInsight

BeyondInsight offers a role-based delegation model so that you can explicitly assign permissions to groups on specific product features based on their role.



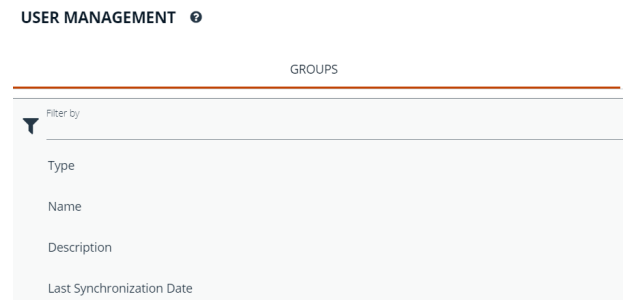
Note: By default, an **Administrators** group is created. The permissions assigned to the group cannot be changed. The user account you created when you configured BeyondInsight is a member of the group.

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

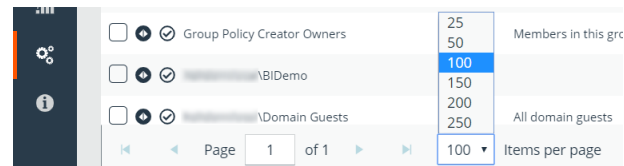


Users	Description
0	test
0	Users who can create and delete enterprise domain

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.




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	Members in this group
25	
50	
100	
150	
200	
250	

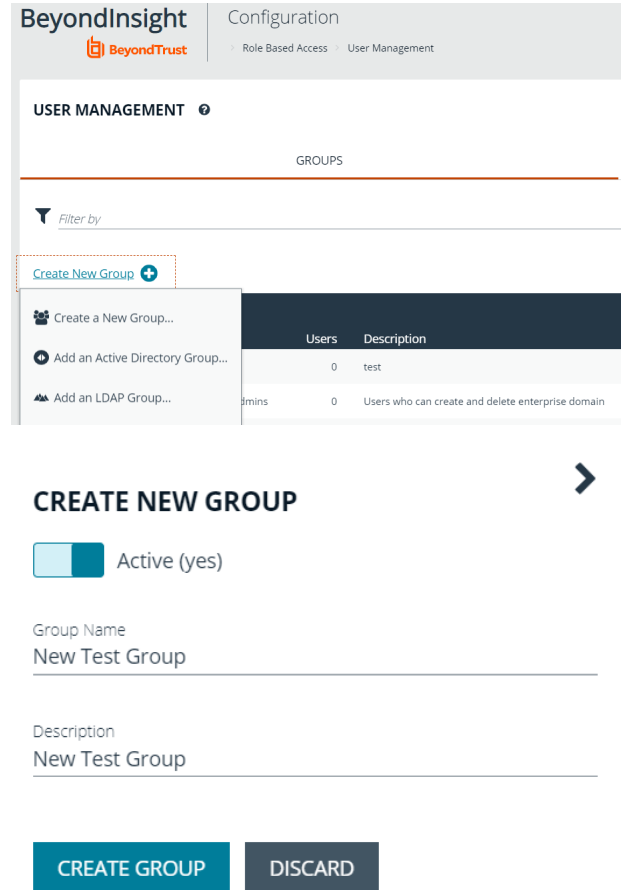
After a group is created, add user accounts to the group. When a user is added to a group, the user is assigned the permissions assigned to the group.

Create a BeyondInsight Local Group

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

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

4. Enter a **Group Name** and **Description** for the group.
5. The group is set to **Active (yes)** by default. Click the toggle to set the group to **Active (no)** if you wish to activate it later.
6. Click **Create Group**.



BeyondInsight Configuration
Role Based Access > User Management

USER MANAGEMENT

GROUPS

Filter by

Create New Group +

Create a New Group...
Add an Active Directory Group...
Add an LDAP Group...

Users	Description
0	test
0	Users who can create and delete enterprise domain

CREATE NEW GROUP

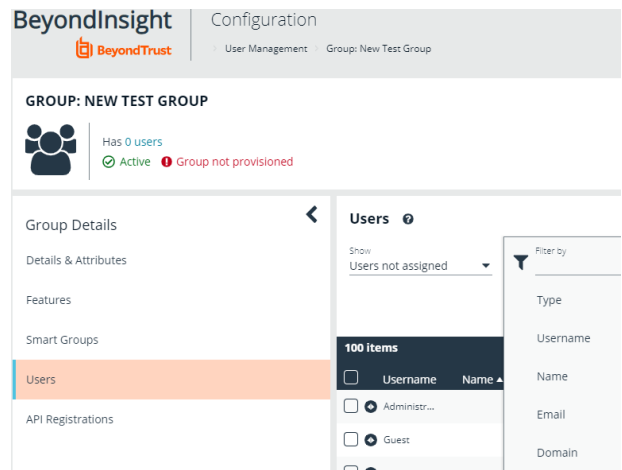
Active (yes)

Group Name
New Test Group

Description
New Test Group

CREATE GROUP DISCARD

7. Assign users to the group:
 - a. Under **Group Details**, select **Users**.
 - b. From the **Show** drop-down list, select **Users not assigned**.
 - c. Filter the list of users displayed in the grid by **Type**, **Username**, **Name**, **Email**, and **Domain**, if desired.



BeyondInsight Configuration
User Management > Group: New Test Group

GROUP: NEW TEST GROUP

Has 0 users
Active Group not provisioned

Group Details
Details & Attributes
Features
Smart Groups
Users
API Registrations

Users

Show
Users not assigned

Filter by
Type
Username
Name
Email
Domain

100 items

Username Name

Administr...
Guest

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

Users ⓘ

Show
Users not assigned ▼

Username
name ✕

Filter by

Assign User +

7 items (6 selected)

<input type="checkbox"/>	Username	Name ▲	Email	Domain
<input checked="" type="checkbox"/>	a.name4	a.name4	e@mail4.null	n
<input checked="" type="checkbox"/>	a.name5	a.name5	e@mail5.null	n
<input checked="" type="checkbox"/>	a.name6	a.name6	e@mail6.null	n
<input checked="" type="checkbox"/>	a.name7	a.name7	e@mail7.null	n
<input checked="" type="checkbox"/>	a.name8	a.name8	e@mail8.null	n
<input checked="" type="checkbox"/>	a.name9	a.name9	e@mail9.null	n

i 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 13.

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**.

DIRECTORY CREDENTIALS <

Search Directory Credentials

Create Directory Credential +

Showing all 9 Directory Credentials

Active Direct...	Group resolution disabled	✕
gman (Active Directory)	Group resolution disabled	✕
Group resolution disabled	Credenti...	✕
Group resolution disabled	al) (Acti...	✕
Group resolution disabled	(Active ...	✕
hello (Active Directory)	Group resolution disabled	✕

Edit Directory Credential Credentials

Type
Active Directory

Domain

☐ Use SSL

Username
administrator

CHANGE PASSWORD

☐ Use Group Resolution (Optional) ⓘ

TEST CREDENTIAL **SAVE CREDENTIAL** **DISCARD CHANGES**

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.

7. 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**.

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**.

New Directory Credential

Directory Type

- ☒ Active Directory
- ☐ LDAP

Credentials

Title

Domain

☐ Use SSL

Username

Password

☐ Use Group Resolution (Optional) ?

TEST CREDENTIAL

SAVE CREDENTIAL

DISCARD CHANGES

DIRECTORY CREDENTIALS

Q Search Directory Credentials

Create Directory Credential +

Showing all 9 Directory Credentials

Group resolution disabled	
gman (Active Directory)	
Group resolution disabled	
Group resolution disabled	
Group resolution disabled	
Group resolution disabled	
Group resolution disabled	
Group resolution disabled	
Group resolution disabled	
hello (Active Directory)	
Group resolution disabled	

Edit Directory Credential Credentials

Title hello

Domain mydomain.local

☐ Use SSL

Username theuser

CHANGE PASSWORD

☐ Use Group Resolution (Optional) ?

TEST CREDENTIAL SAVE CREDENTIAL DISCARD CHANGES

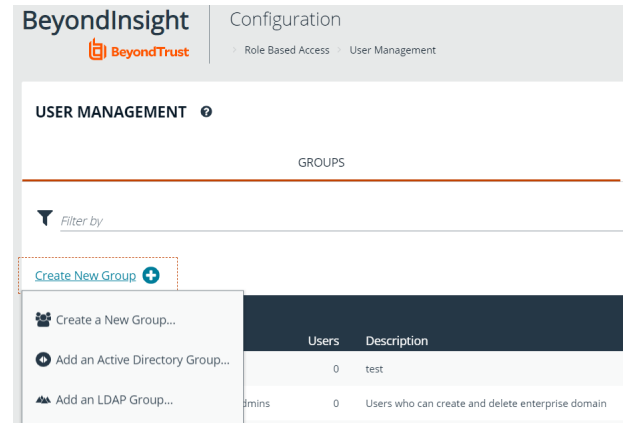
Add an Active Directory Group

Active Directory group members can log into 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 into 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**.



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



For more information on creating and editing directory credentials, please see "[Create and Edit Directory Credentials](#)" on page 6.

ACTIVE DIRECTORY GROUP SEARCH

Credential [Manage Credentials...](#)

Domain

Filter by Group Name
*

SEARCH ACTIVE DIRECTORY **CANCEL**

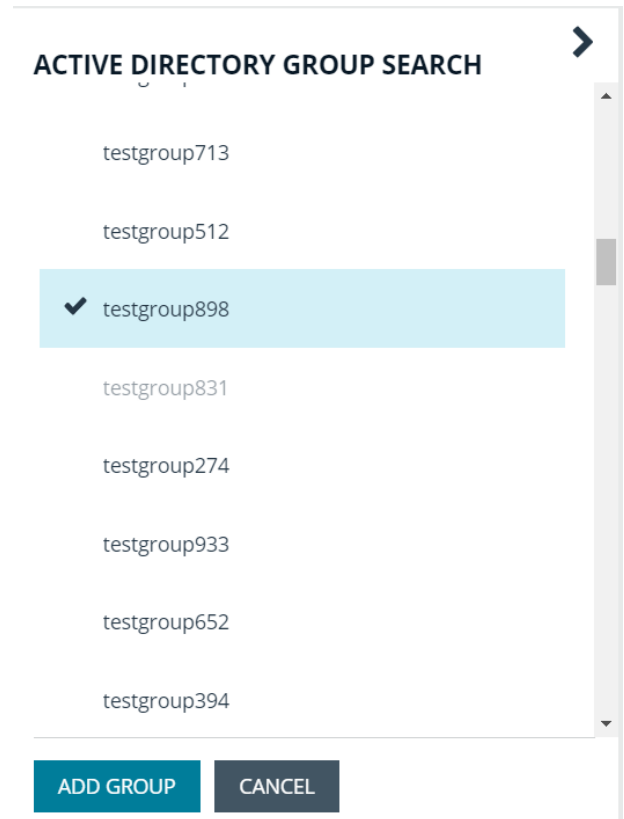
5. If not automatically populated, enter the name of a domain or domain controller.
6. After you enter the domain or domain controller credential information, click **Search Active Directory**. A list of security groups in the selected domain is displayed.



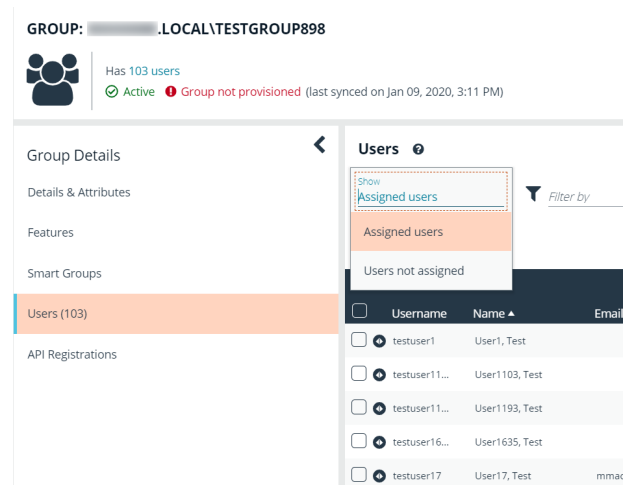
Note: For performance reasons, a maximum of 250 groups from Active Directory is retrieved. The default filter is an asterisk (*), which is a wild card filter that returns all groups. Use the group filter to refine the list.

7. Set a filter on the groups that will 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**.



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.



i 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 13.

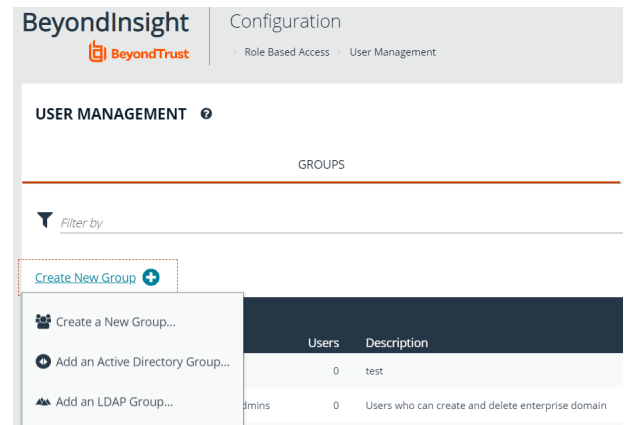
Add an LDAP Directory Group

LDAP group members can log into 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 into the management console at least once to receive email notifications.

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



BeyondInsight Configuration

Role Based Access > User Management

USER MANAGEMENT

GROUPS

Filter by

Create New Group +

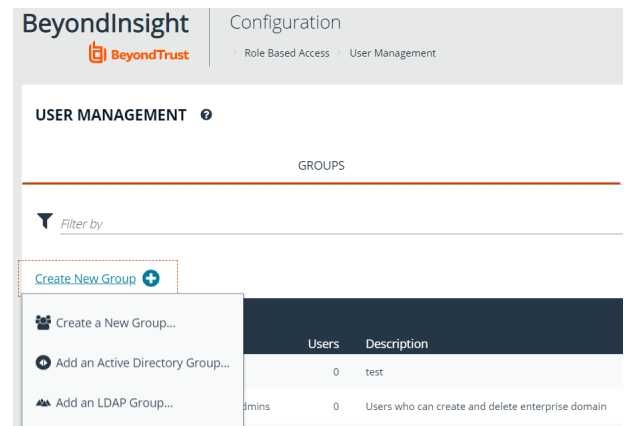
Create a New Group...

Add an Active Directory Group...

Add an LDAP Group...

Users	Description
0	test
0	Users who can create and delete enterprise domain

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

GROUPS

Filter by

Create New Group +

Create a New Group...

Add an Active Directory Group...

Add an LDAP Group...

Users	Description
0	test
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.

i For more information on creating and editing directory credentials, please see "[Create and Edit Directory Credentials](#)" on page 6.

LDAP GROUP SEARCH

Credential
orac1 admin ▼
[Manage Credentials...](#)

Server

Domain / Domain controller ▼ **FETCH**

Filter by Group Name
*

SEARCH LDAP **CANCEL**

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

LDAP GROUP SEARCH

SEARCH LDAP

Search Results

OracleDBSecurityAdmins
Users who can create and delete enterprise domains in this realm, move database

OracleDBCreators
Users who can register databases in this realm, including creating the database

✓ OracleNetAdmins
Users who can register Network Service Alias in this Oracle Context.

OracleDefaultDomain

OracleContextAdmins
Users who can administer all entities in this Oracle Context

CONTINUE TO ADD GROUP

CANCEL

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 Network Service Alias in t


Group Membership attribute
uniqueMember

Account Naming attribute

ADD GROUP

CANCEL

GROUP: .LOCAL\TESTGROUP898



Has 103 users
Active Group not provisioned (last synced on Jan 09, 2020, 3:11 PM)

Group Details
 Details & Attributes
 Features
 Smart Groups
Users (103)
 API Registrations

Users

Show

Assigned users

Assigned users

Users not assigned

Filter by

<input type="checkbox"/>	Username	Name	Email
<input checked="" type="checkbox"/>	testuser1	User1, Test	
<input type="checkbox"/>	testuser11...	User1103, Test	
<input type="checkbox"/>	testuser11...	User1193, Test	
<input type="checkbox"/>	testuser16...	User1635, Test	
<input type="checkbox"/>	testuser17	User17, Test	mimac

i 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](#).

Assign Group Permissions

Permissions

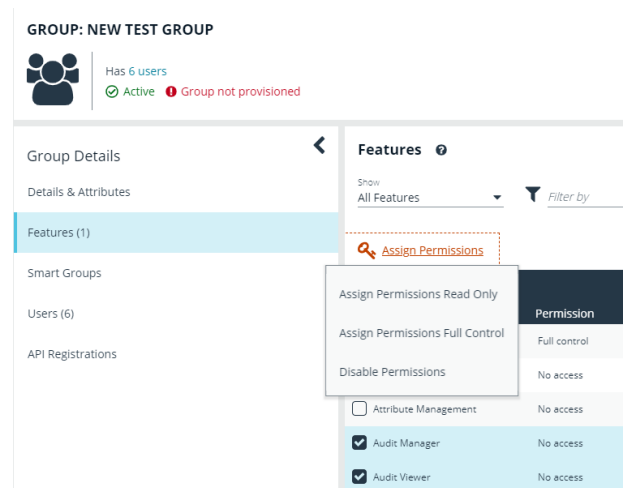
Permission	Description
No Access	Users cannot access the selected feature. In most cases, the feature will not be visible to the users.
Read Only	Users can view selected areas, but cannot change information.
Full Control	Users can view and change information for the selected feature.

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** drop-down 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**.



GROUP: NEW TEST GROUP

Has 6 users
Active Group not provisioned


Group Details
 Details & Attributes
Features (1)
 Smart Groups
 Users (6)
 API Registrations

Features ⓘ
 Show All Features Filter by

Assign Permissions

Assign Permissions Read Only	Permission
Assign Permissions Full Control	Full control
Disable Permissions	No access
<input type="checkbox"/> Attribute Management	No access
<input checked="" type="checkbox"/> Audit Manager	No access
<input checked="" type="checkbox"/> Audit Viewer	No access

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

Feature	Provides Permissions To:
Analytics and Reporting	<p>Log into the console and access Analytics & Reporting to generate and subscribe to reports.</p> <div>  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. </div>
Asset Management	<p>Create smart rules.</p> <p>Edit and delete buttons on the Asset Details window.</p> <p>Create Active Directory queries.</p> <p>Create address groups.</p>
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 Credential Management	Grant access to the configuration area where Directory Credentials are managed. This feature must be enabled to support access to Directory Queries as well.
Directory Query Management	Grant access to the configuration area where Directory Queries are managed. 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.

Feature	Provides Permissions To:
Password Safe Account Management	<p>Read or write managed accounts through the public API.</p> <div>  <p>For more information, please see the <i>Managed Accounts</i> section in the BeyondInsight and Password Safe API Guide at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/index.htm.</p> </div>
Password Safe Admin Session	Password Safe web portal admin sessions.
Password Safe Global API Quarantine	Access to the Quarantine APIs.
Password Safe Bulk Password Change	Change more than one password at a time.
Password Safe 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	<p>Activate Scan and Start Scan buttons.</p> <p>Activate Abort, Resume, Pause, and Delete on the Job Details page.</p>
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	<p>Allow a user to set report delivery options when running a scan:</p> <ul style="list-style-type: none"> 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	<p>Delete, edit, duplicate, and rename reports on the Manage Report Templates page.</p> <p>Activate New Report and New Report Category.</p> <p>Activate the Update button on the Edit Scan Settings view.</p>
Session Monitoring	Use the session monitoring features.

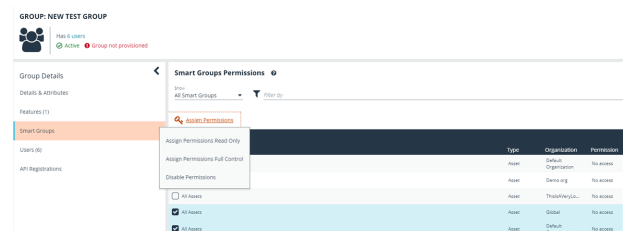
Feature	Provides Permissions To:
Ticket System	View and use the ticket system.
Ticket System Management	Mark a ticket as inactive. The ticket no longer exists when Inactive is selected.
User Accounts Management	Add, delete, or change user groups and user accounts.
User Audits	View audit details for management 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.

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** drop-down 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**.



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

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

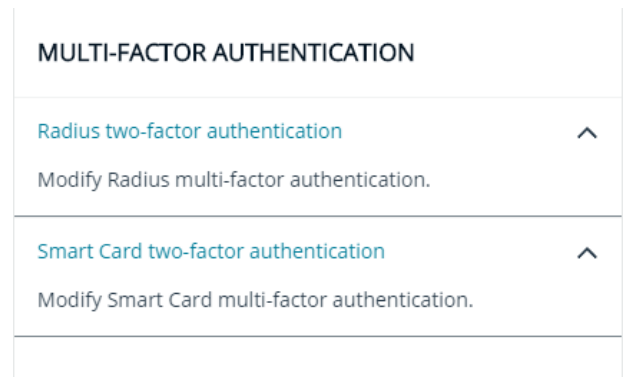
After you set up two-factor authentication, users must log in using the two-factor authentication method.

To set up two-factor authentication, you must:

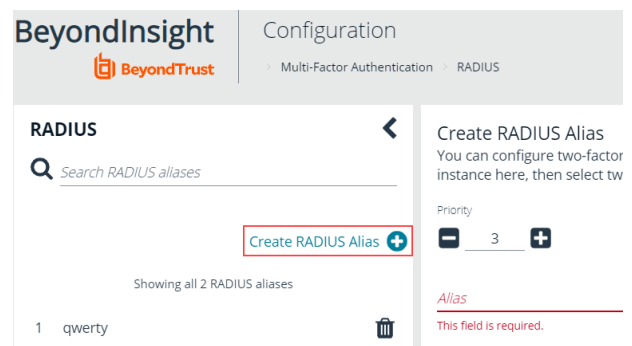
- Configure the RADIUS server.
- Configure the two-factor authentication settings for users.

Configure the RADIUS Server

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



2. Click **Create Radius Alias**.



3. In the **Create RADIUS Alias** pane, set the following:
 - **Alias:** Provide a name used to represent the RADIUS server instance. This will be 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. This should be a domain or comma-separated list of domains, depending on the setting selected for the filter.
 - **Host:** Enter the DNS name or the IP address for your RADIUS server.

- **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 BeyondInsight will 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 into 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 will 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 17](#), using the following settings:

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

Create RADIUS Alias

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

Priority:

Alias:

Filter:

Host:

Authentication mechanism:

Authentication port:

Authentication request timeout: seconds

Shared secret:

Initial request:

☐ Transmit NAS identifiers

[CREATE RADIUS ALIAS](#) [DISCARD CHANGES](#)

Configure Two-Factor for a RADIUS Duo-only Configuration

Follow the steps outlined above in "Configure the RADIUS Server" on page 17, using the following settings:

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

Create RADIUS Alias

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

Priority: 3

Alias: Duo

Filter: All domain users

Host: 10.101.10.23

Authentication mechanism: PAP

Authentication port: 1812

Authentication request timeout: 500 seconds

Shared secret: *****

Initial request: Forward username and token

Prompt: Enter RADIUS code:

☐ Transmit NAS identifiers

[CREATE RADIUS ALIAS](#) [DISCARD CHANGES](#)



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**.
3. Under **RADIUS Two-Factor Authentication**, set the following:
 - **Alternate directory attribute:** Enter the Active Directory or LDAP attribute that will be 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**.

SAML Setup With a Generic Security Provider

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

1 - Copy certificates from Identity Provider (IdP)

1. After the IdP is configured you will receive an idp.cer file, or will need one provided.
2. Copy this cert to the UVM and put it in the folder: C:\Program Files (x86)\eEye Digital Security\Retina CSI\WebSiteSAML\Certificates

2 - Generate or Obtain sp.pfx (Private cert for Service Provider)

You will need a Service Provider Certificate. For this you can generate your own Self Signed Cert, or get one provided from a CA.

Self Signed Certificate

1. Use PowerShell to generate a new certificate:

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



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

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

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

4. Convert the certificate to base 64:

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

Certificate Authority Provided Certificate

Your Certificate will need the following capabilities:

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

Add the certificate to the Local Machine, Personal Store

You will want to add any Intermediate or Root certs to the proper stores if needed.

If you want to use the Service Provider cert from the Certificate Store you will need to grant permissions to IIS to READ the Private Key

1. Open MMC
2. Add the Certificate SnapIn for Local Machine
3. Explore to Personal/Certificates

4. Right Click on your Certificate that was setup for the service provider.
5. Select All Tasks -> Manage Private Keys
6. Add the IIS user: IIS_IUSRS

3 - Modify saml.config

Located: C:\Program Files (x86)\eEye Digital Security\Retina CS\WebSiteSAML\

Update Service Provider Section:

- Name: should be Fully qualified domain followed by eEye.ReintaCSSAML, this is used for the Audience Restriction
- Description: Doesn't matter to much what you put here
- AssertionConsumerServiceUrl: This shouldn't need to me modified.
- If you save the certificate for the SP to the certificate folder use these options
 - LocalCertificateFile: Path to the certificate
 - LocalCertificatePassword: password for the PFX file
- If you want to use the certificate from the cert store remove LocalCertificateFile and LocalCertificatePassword and add:
 - LocalCertificateThumbprint: This would be the Thumbprint of the certificate.

You can remove all but your one IdP entry.

The following IdP fields will need to be updated to your environment settings:

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

The other settings are set to what your Provider requires.

Below are some common configurations for some of the common IdP's

example saml.config (this is configured for ADFS using a self signed service provider certificate)

```
<?xml version="1.0"?>
<SAMLConfiguration xmlns="urn:componentspace:SAML:2.0:configuration">
  <ServiceProvider Name="http://pws.mycompany.com/eEye.RetinaCSSAML"
    Description="Example Service Provider"
    AssertionConsumerServiceUrl="~/SAML/AssertionConsumerService.aspx">
    <LocalCertificates>
      <Certificate
        Thumbprint="7120E0BD353429D18F9829096AB3BC9A80AF33B8" />
      </Certificate>
    </LocalCertificates>
  </ServiceProvider>

  <PartnerIdentityProviders>

    <!-- example -->
    <PartnerIdentityProvider Name="http://localhost/MvcExampleIDP"
      Description="MVC Example Identity Provider"
```

```

        SignAuthnRequest="true"
        WantSAMLResponseSigned="true"
        WantAssertionSigned="false"
        WantAssertionEncrypted="false"
        SingleSignOnServiceUrl="http://localhost/MvcExampleIDP/SAML/SSOService"
        SingleLogoutServiceUrl="http://localhost/MvcExampleIDP/SAML/SLOService">
        <PartnerCertificates>
        <Certificate
            FileName="Certificates\idp.cer" />
        </PartnerCertificates>
    </PartnerIdentityProvider>

</PartnerIdentityProviders>
</SAMLConfiguration>

```

4 - Modify web.config

On a new install of BeyondInsight (6.10 or later) you won't need to change anything. If you are upgrading from a previous version, you may need to make some changes.

In the AppSettings there is a key for disabling SLO if you don't want to use the Single Logout Service. The default value is **False**, you can set it to **True** to disable SLO

```
<add key="disableSLO" value="True" />
```

If it is an Upgrade you may need to comment out the two lines:

```
<add name="TextWriter"/> so they appear as <!--<add name="TextWriter"/>-->
```

5 - Update hostname and SAML access URL

1. Open the BeyondInsight Configuration Tool
2. Scroll Down to SAML Access URL
3. Update it to: **https://<FQDN>/eEye.RetinaCSSAML**
4. Scroll down the **Host Name** field under the **Web Site Information** section
5. Update it to: **<FQDN>** (eg. bidev.shines.test.cloud)
6. Click **Apply**



Note: The Host Name should be the FQDN used to access BI/PWS. If this is a load balanced instance, this should be the same on all servers.

Configure Identity Provider (IdP)

Below are some of the values an IdP may need:

- Audience Restriction: **https://<FQDN>/eEye.RetinaCSSAML**
- SSO Service URL: **https://<FQDN>/eEye.RetinaCSSAML/SAML/AssertionConsumerService.aspx**

- SLO Service URL: [HTTPS://<FQDN>/eEye.RetinaCSSAML/SAML/SLOService.aspx](https://<FQDN>/eEye.RetinaCSSAML/SAML/SLOService.aspx)
- Service Provider Certificate: sp.cer (generated yourself, or obtained from a Certificate Authority)

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 AD. If an AD 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)
- **Given Name:** (optional)

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.

To test the configuration:

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



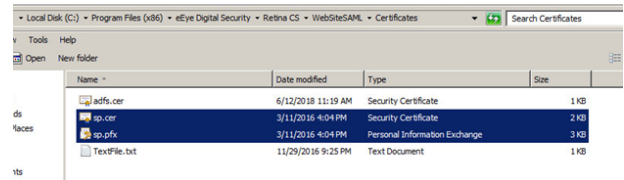
Note: For the push method (4), increase the timeout to **30 seconds**.

Configure AD FS with Password Safe Using SAML

Create and Copy Certificates

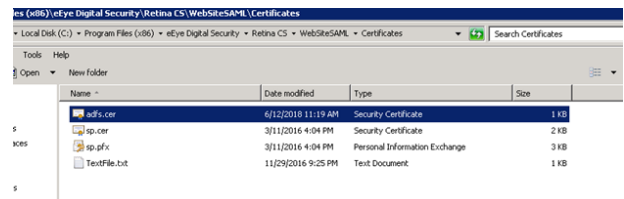
1. Create a personal information exchange (.pfx) certificate and a public certificate for the BeyondInsight service provider. Place them both in the following folder on the UVM:

C:\Program Files (x86)\eEye Digital Security\Retina CS\WebSiteSAML\Certificates



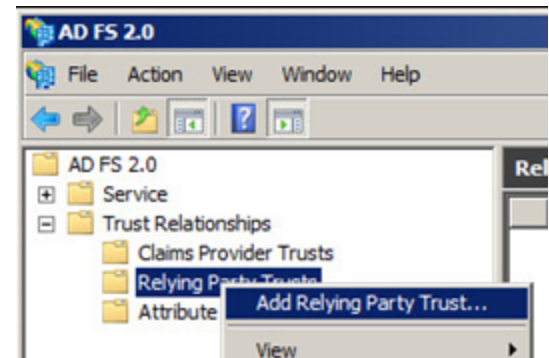
2. Copy the public certificate to the AD FS server.
3. Copy the AD FS certificate to the following folder on the UVM:

C:\Program Files (x86)\eEye Digital Security\Retina CS\WebSiteSAML\Certificates

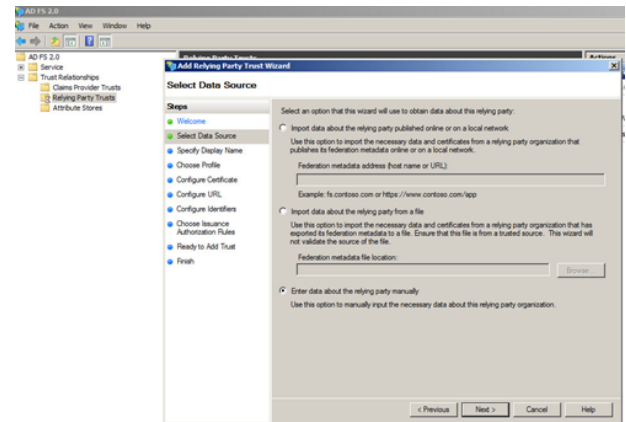


Configure AD FS on the Identity Provider Server

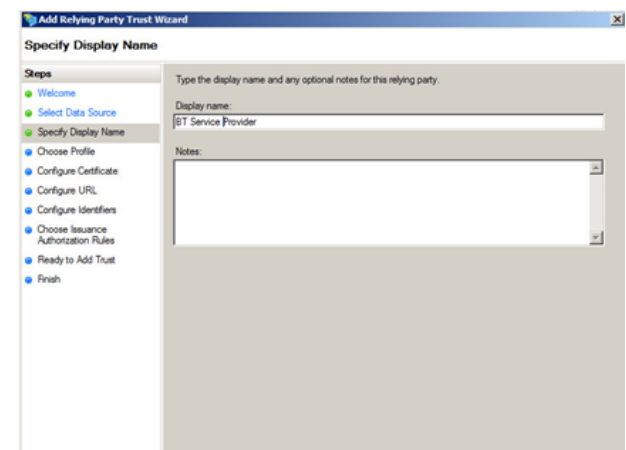
1. Open the AD FS management console.
2. Expand **Trust Relationships**.
3. Right-click **Relying Party Trusts**.
4. Select **Add Relying Party Trust**.



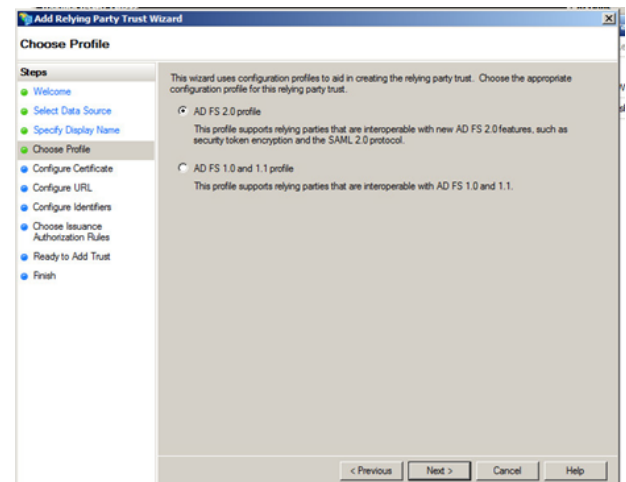
5. Click **Start**.
6. Select **Enter data about the relying party manually**, and then click **Next**.



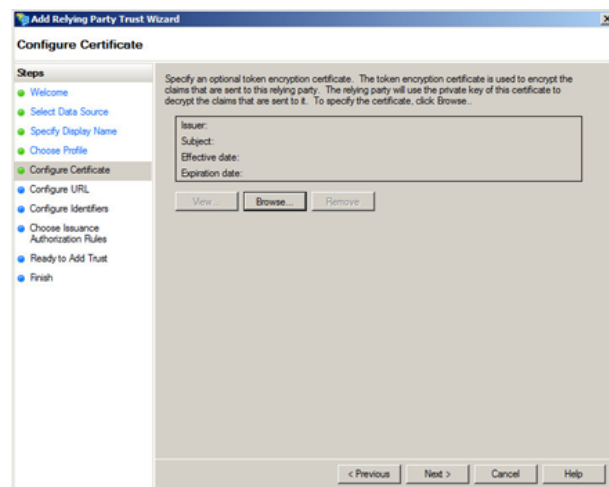
7. Enter a **Display name**, and then click **Next**.



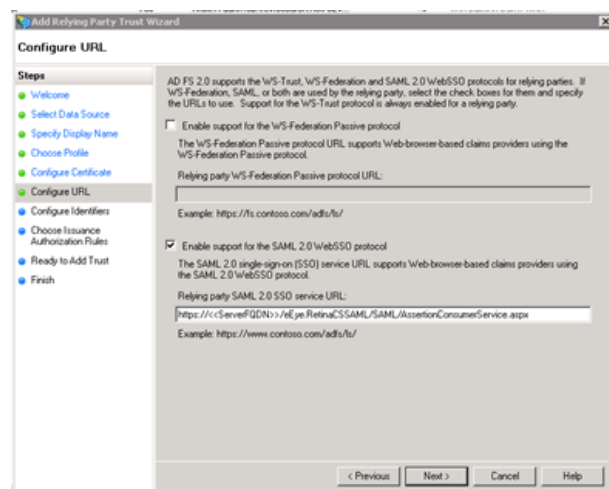
8. Leave **AD FS 2.0 profile** selected, and then click **Next**.



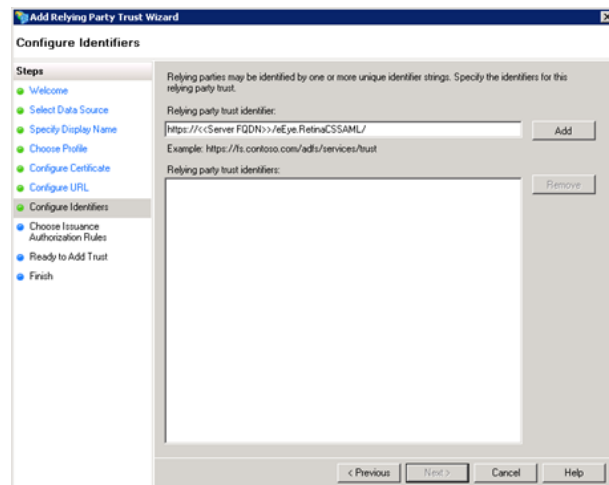
9. Click **Browse** on the **Configure Certificate** screen to import the service provider (SP) public certificate.
10. Navigate to the location of the SP certificate.
11. Select the certificate, click **Open**, and then click **Next**.



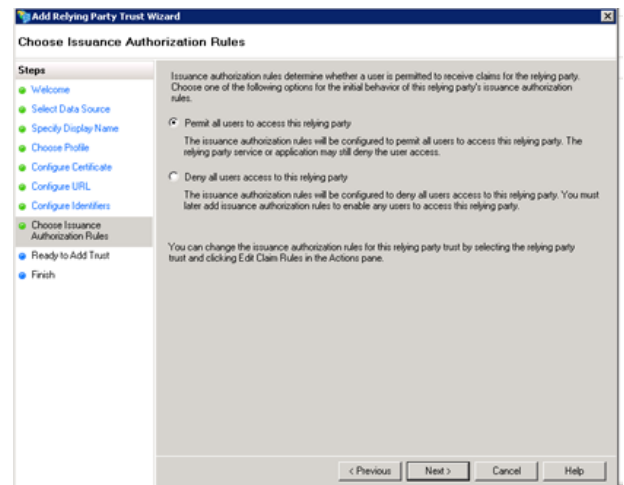
12. Select **Enable support for the SAML 2.0 WebSSO protocol**.
13. Enter the **Relying party SAML 2.0 SSO service URL**, and then click **Next**.



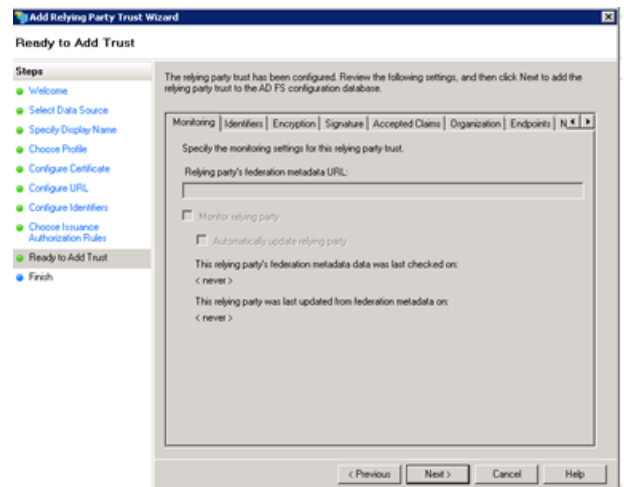
14. Enter the **Relying party trust identifier**, click **Add**, and then click **Next**.



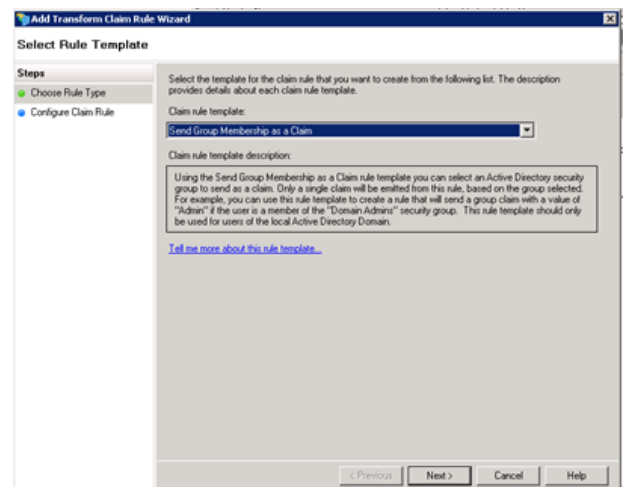
15. Select the preferred method of access, and then click **Next**. The default is **Permit all users**.



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



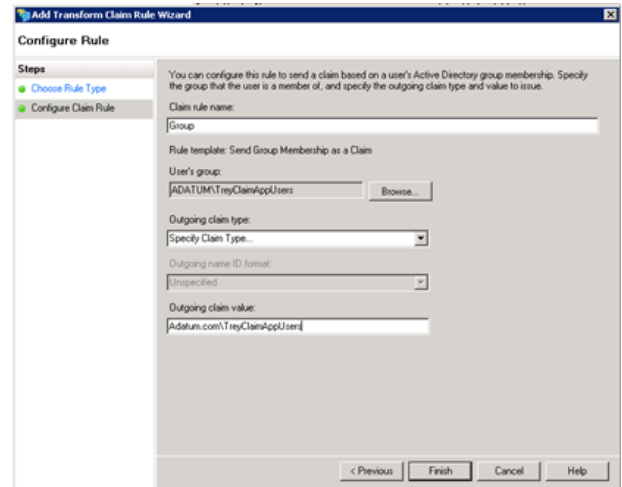
17. Click **Add Rule**.
18. Select the **Send Group Membership as a Claim** rule template, and then click **Next**.



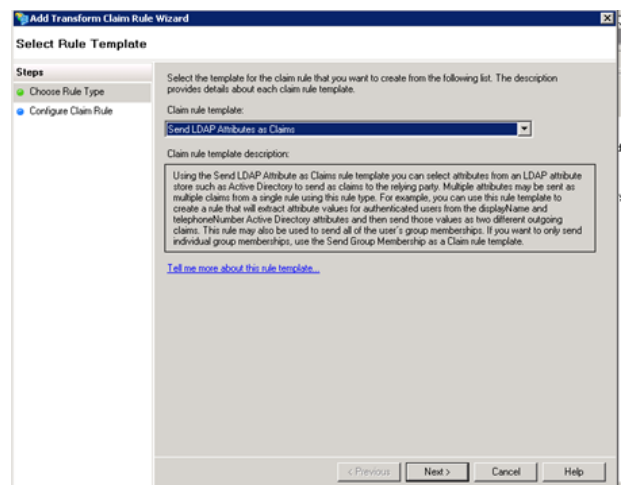
19. Enter a name for the claim rule.
20. Select the **User's group**.
21. Select the **Outgoing claim type**.
22. Select the **Outgoing claim value**.
23. Click **Finish**.



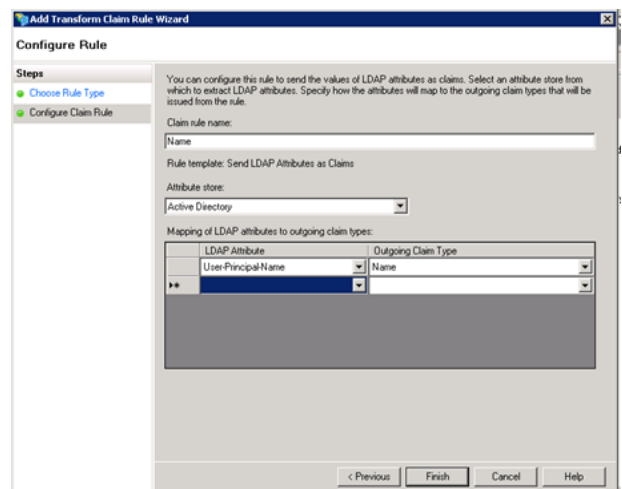
Note: The outgoing Group claim must match exactly what is in BeyondInsight.



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



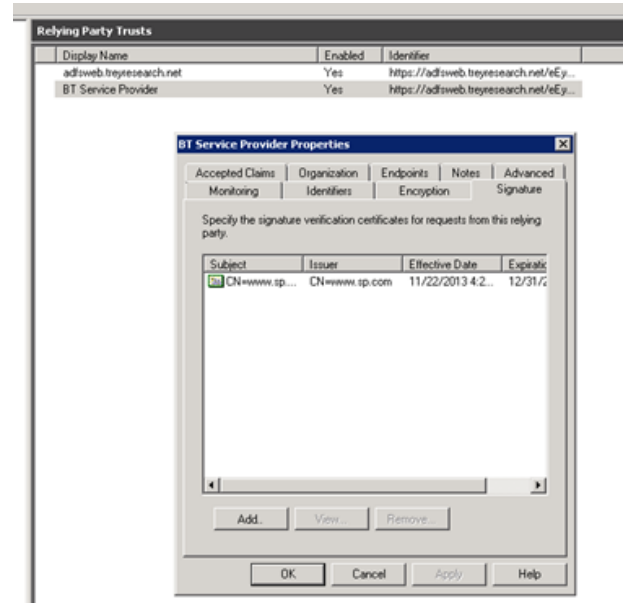
26. Enter a **Claim rule name**.
27. Select the **Attribute store**.
28. Select **User-Principal-Name** for the **LDAP Attribute**.
29. Select **Name** as the **Outgoing Claim Type**.
30. Click **Finish**.



LDAP Attribute	Outgoing Claim Type
User-Principal-Name	Name

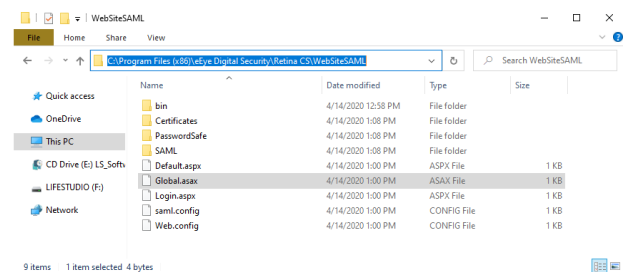
31. On the **Relying Party Trusts** page, right-click **BT Service Provider**, and then select **Properties**.

32. Select the **Signature** tab.
33. Click **Add**, and then enter the service provider public certificate.



Configure SAML on the Service Provider Server (UVM)

1. On the UVM, open the **C:\Program Files (x86)\eEye Digital Security\Retina CS\WebSiteSAML\saml.config** file in a text editor such as **Notepad**.

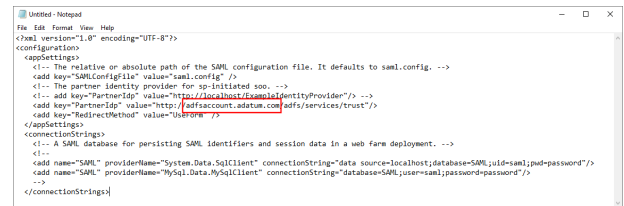


2. Edit the following:

- Service Provider name (URL)
- Local certificate file name and password
- Identity Provider name (URL in 3 locations)
- Identity Provider certificate name



3. Open the **C:\Program Files (x86)\eEye Digital Security\Retina CS\WebSiteSAML\web.config** file in a text editor such as **Notepad**, and then edit the **Identity Provider** server name.



```
Untitled - Notepad
File Edit Format View Help
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <appSettings>
    <!-- The relative or absolute path of the SAML configuration file. It defaults to saml.config. -->
    <add key="SAMLConfigFile" value="saml.config" />
    <!-- The partner identity provider for sp-initiated soos. -->
    <!-- add key="PartnerId" value="http://localhost/ExampleIdentityProvider/" -->
    <add key="PartnerId" value="http://redfraccount.adatum.com/pdfs/service/trust/" />
    <add key="RedirectMethod" value="UserForm" />
  </appSettings>
  <connectionStrings>
    <!-- A SAML database for persisting SAML identifiers and session data in a web farm deployment. -->
    <!--
    <add name="SAML" providerName="System.Data.SqlClient" connectionString="data source=localhost;database=SAML;uid=saml;pwd=password"/>
    <add name="SAML" providerName="MySql.Data.MySqlClient" connectionString="database=SAML;user=saml;password=password"/>
    -->
  </connectionStrings>
</configuration>
```

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**.
2. Click the toggle to **Enable Smart Cards**.
3. Click the toggle to enable the **Allow UPN Override On User** option. This allows a BeyondInsight user with a smart card that has a different Subject Alternative Name to log into BeyondInsight and maps the smart card to the user.
4. Click **Update Smart Card Authentication**.

MULTI-FACTOR AUTHENTICATION

Radius two-factor authentication



Modify Radius multi-factor authentication.

Smart Card two-factor authentication



Modify Smart Card multi-factor 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 will 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)

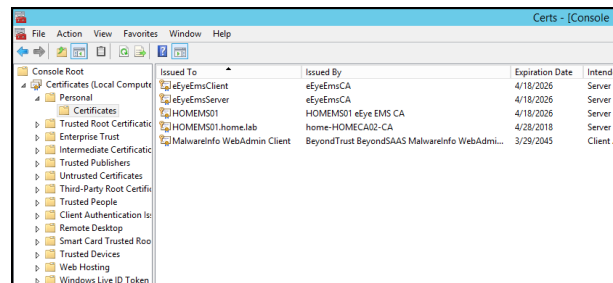
User Principal Name

The user principal name is required

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 will show as **Issued By eEyeEmsCA**.

To authenticate using smart cards, the server where BeyondInsight is running will need a certificate issued and signed by a certificate authority (CA). You will need to verify your BeyondInsight server has the correct certificates issued before continuing.

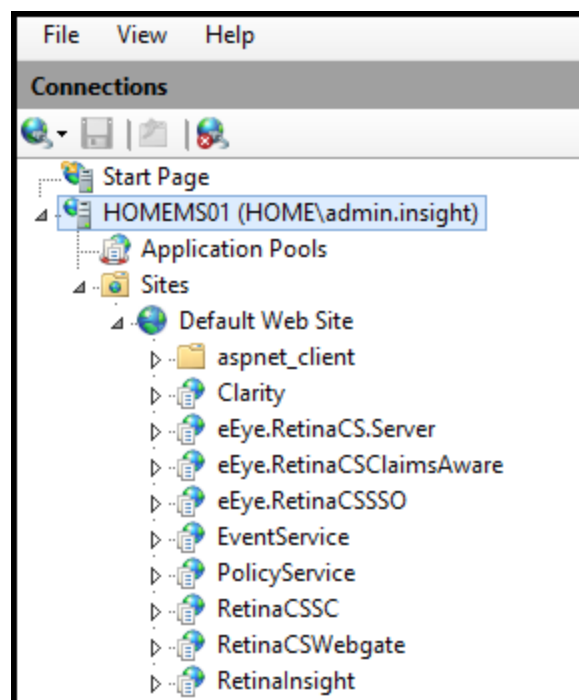


Verify the Web Server Certificate

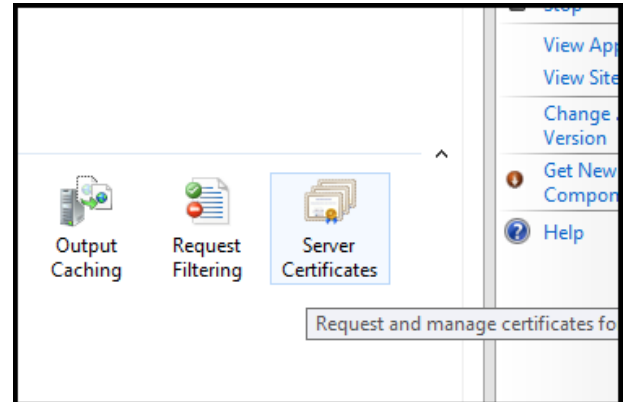
During the BeyondInsight installation, a self-signed web server certificate is created. This certificate must be replaced with a CA-issued certificate.

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

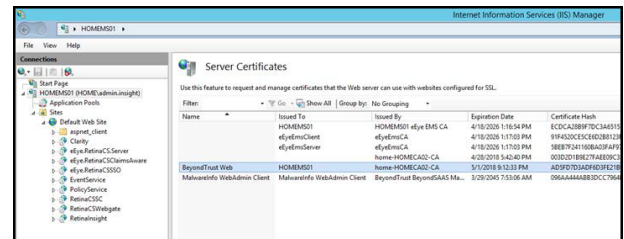
1. Open **IIS**.
2. Select your web server.



3. Select **Server Certificates**.



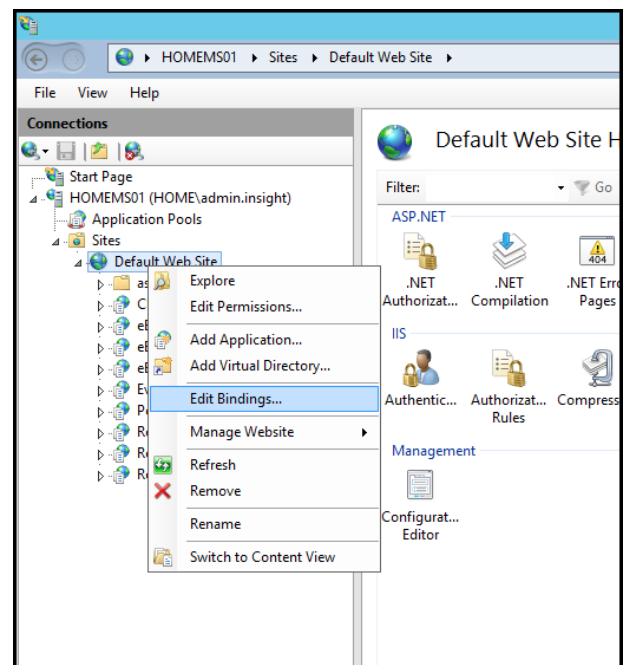
4. Verify you have a CA-issued certificate. If you do not see one listed, you will need to request one from your certificate authority.



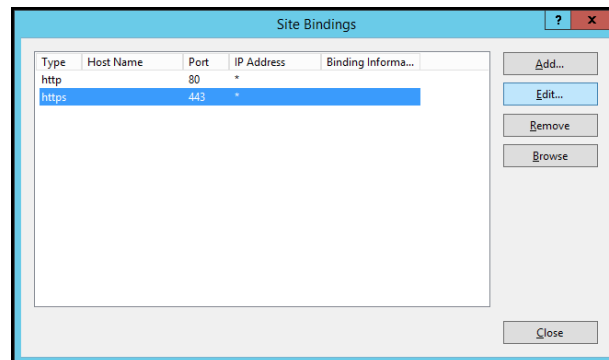
Update Default Web Site Bindings with CA-Issued Certificate

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

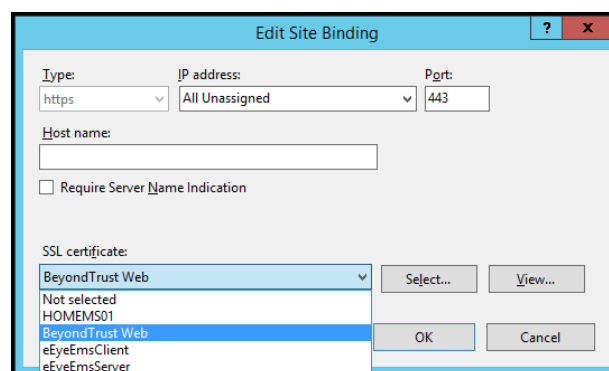
1. Open **IIS**.
2. Expand **Sites**, and then select **Default Web Site**.
3. Right-click **Default Web Site**, and then select **Edit Bindings**.



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



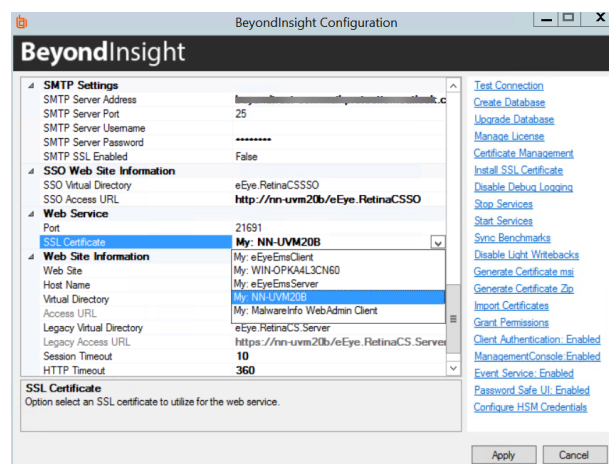
1. Select the issued domain certificate in the **SSL certificate** list, and then click **OK**.



Update SSL Certificate in BeyondInsight Configuration Tool

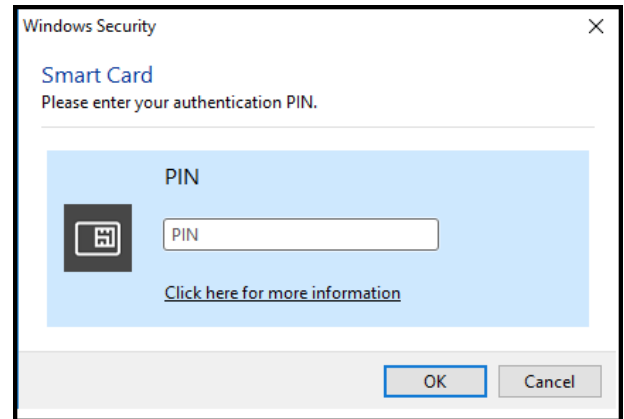
The next step is to change the domain issued certificate in the BeyondInsight Configuration tool.

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



Log into BeyondInsight and Password Safe Using a Smart Card

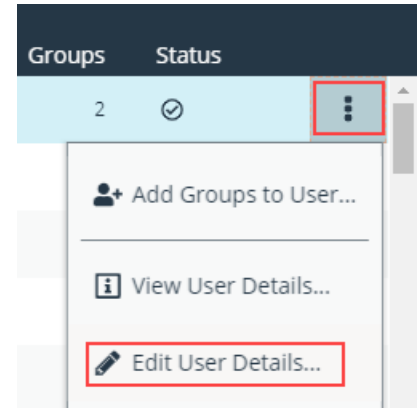
With the correct certificates now applied, you can now open the BeyondInsight console or go to **<https://<servername>/WebConsole/PasswordSafe>**, where you will be prompted to select your certificate and enter your pin. You will be logged in using a secure encrypted connection.



Configure Two-Factor Authentication Settings for User Accounts

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

1. 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.
 4. 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 will enter 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 will enter 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.

EDIT USER

e@mail4.null

Username

a.name4

☐

Account Quarantined (no)

Multi-Factor Authentication

☐

Override Smart Card User (no)

☐

Disable Forms Login (no)

Two Factor Authentication

RADIUS

Map Two Factor User

Manually Specified

Alternate Directory Attribute (extensionName)

Distinguished Name

User Principle Name

SAM Account Name

Domain\User Name

Map Two Factor User

5. Click **Update User**.

Configure a Claims-Aware Website in BeyondInsight

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

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

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

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

Create a BeyondInsight Group

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

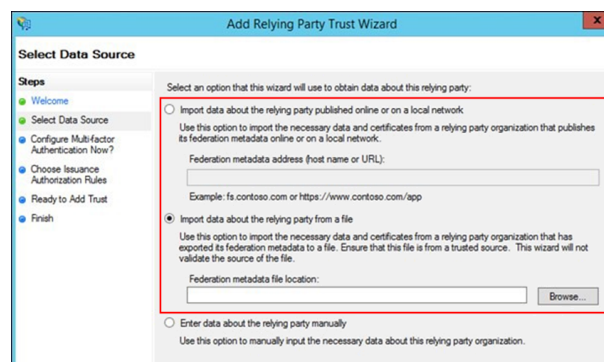
Add Relying Party Trust

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

The metadata is located in the following directory:

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

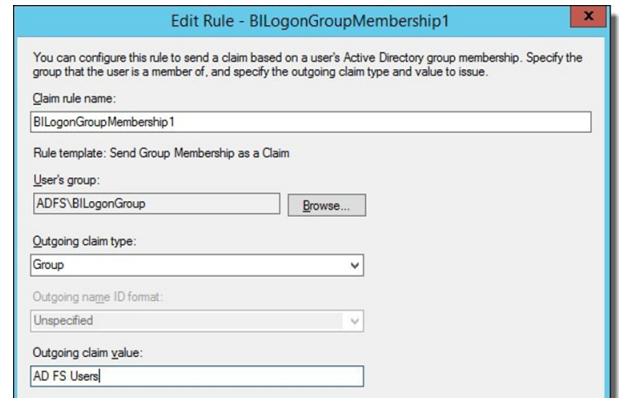
When selecting a **Data Source** in the **Add Relying Party Trust** wizard, select the **FederationMetadata.xml** generated during the install.



Set Up Claim Rules



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



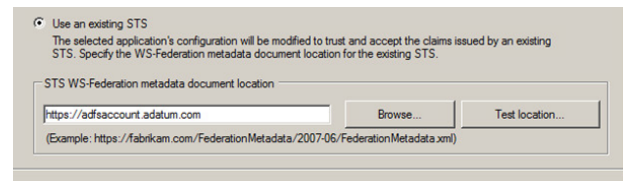
Supported Federation Service Claim Types

Outgoing Claim Type	Outgoing Claim Type	Mapping to BeyondInsight User Detail
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.

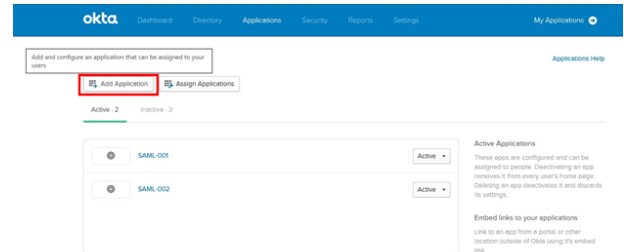
1. Start the **Windows Identity Foundation Federation Utility**.
2. On the **Welcome** page, browse to and select the **web.config** file for **BeyondInsight Claims Aware** site. The application URI should automatically populate.
3. Click **Next**.
4. Select **Using an existing STS**.
5. Enter **Root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



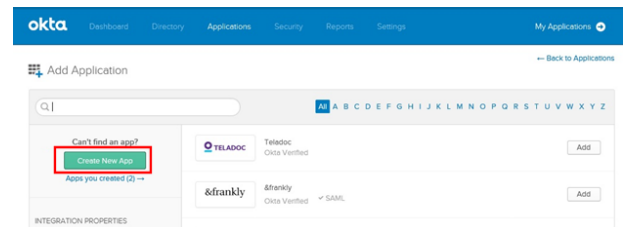
10. Select the appropriate claims, and then click **Next**.
11. Review the settings on the **Summary** page, and then click **Finish**.

Configure Okta with Password Safe

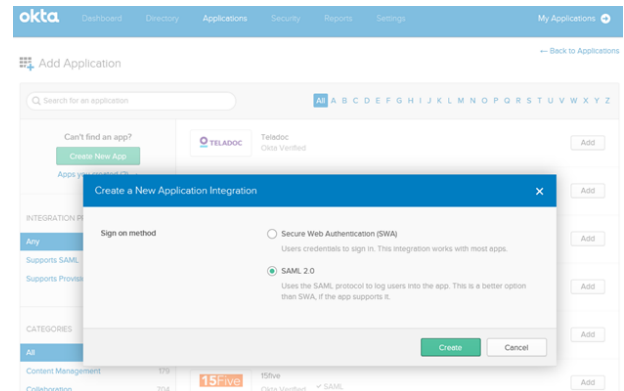
1. Log into the Okta admin portal.
2. Click **Add Application**.



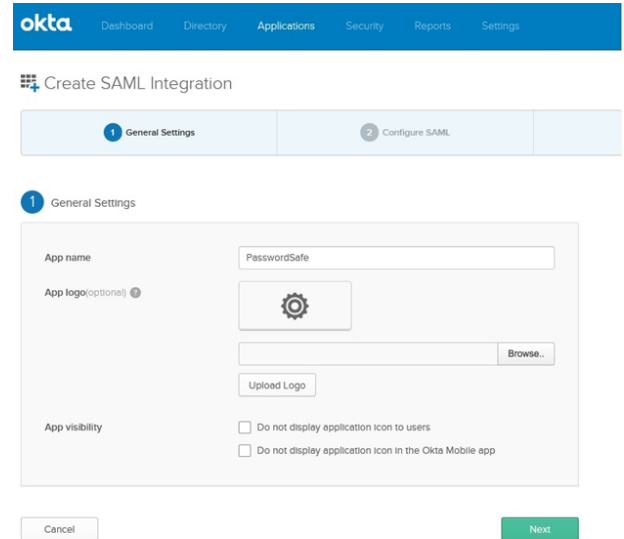
3. Click **Create New App**.



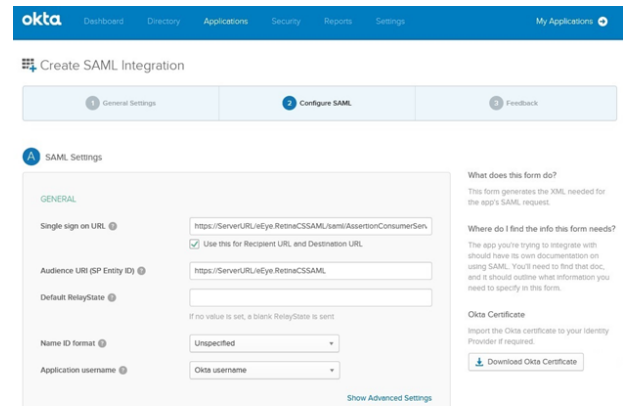
4. Select **SAML 2.0** as the sign in method.
5. Click **Create**.



6. Enter the application name, and then click **Next**.



7. Enter the single sign on URL:
https://ServerURL/eEye.RetinaCSSAML/saml/AssertionConsumerService.aspx
8. Check the **Use this for Recipient and Destination URL** box.
9. Enter the audience URI (SP entity ID):
https://<ServerURL>/eEye.RetinaCSSAML
10. From the **Application username** list, select **Okta username**.



SLO Optional Setting

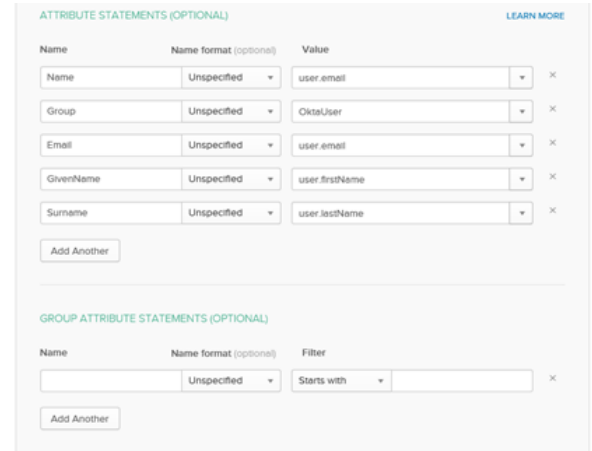
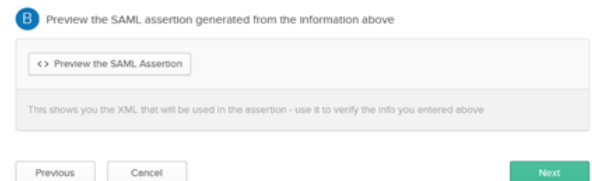
1. Select **Advanced Settings**.
2. Select **Enable Single Logout**.
3. Fill in the **Single Logout URL**:

HTTPS://<FQDN>/eEye.RetinaCSSAML/SAML/SLOService.aspx.

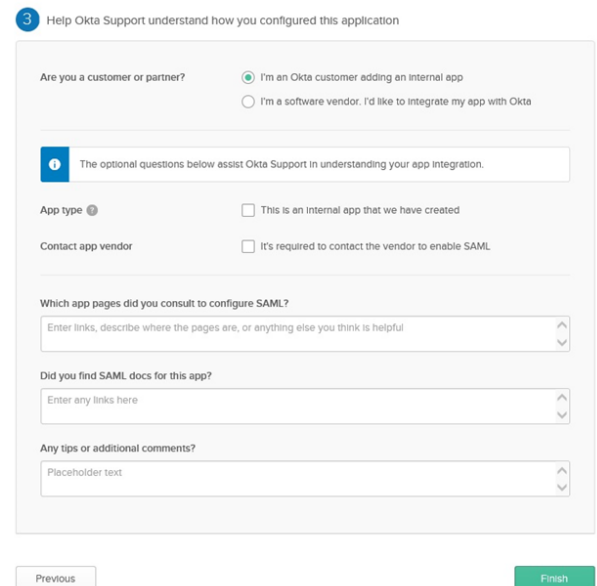
4. Fill in the **SP Issuer**: **HTTPS://<FQDN>/eEye.RetinaCSSAML**.
5. Select the **sp.cer** certificate.
6. Click **Upload Certificate**.

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

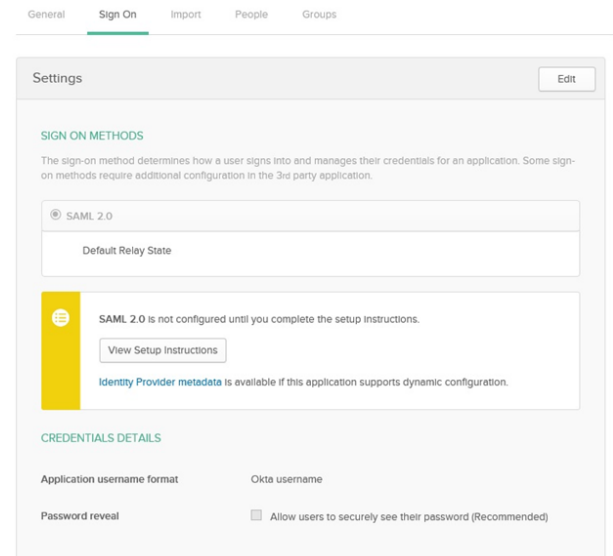
- **Group:** Set as a literal. This must match the group created in BeyondInsight or imported from AD. If an AD group is used, it must match the BI format Domain\GroupName.
- **Name:** (optional)
- **Email:** (optional)
- **Surname:** (optional)
- **Given Name:** (optional)

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

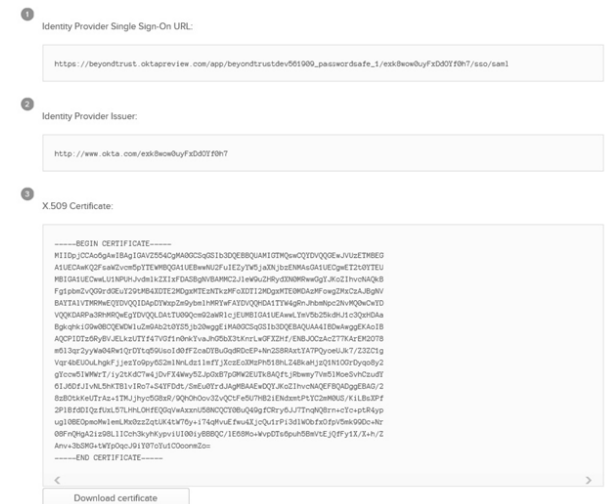


9. Click **View Setup Instructions**.



The screenshot shows the 'Settings' page with tabs for General, Sign On, Import, People, and Groups. The 'Sign On' tab is active. Under 'SIGN ON METHODS', 'SAML 2.0' is selected. A message states: 'SAML 2.0 is not configured until you complete the setup instructions.' with a 'View Setup Instructions' button. Below this, under 'CREDENTIALS DETAILS', there are fields for 'Application username format' and 'Okta username', and a checkbox for 'Password reveal' which is currently unchecked.

10. Copy the **Identity Provider Single Sign-On URL**. Save the value to be used in the next step.
11. Copy the **Identity Provider Issuer**. Save the value to be used in the next step.
12. Click **Download certificate**.



This screenshot shows the configuration details for the Identity Provider. It includes three sections:

- Identity Provider Single Sign-On URL:** A text box containing the URL: `https://beyondtrust-oktapreview.com/app/beyondtrustdev051009_passwordsafe_1/okta/saml`
- Identity Provider Issuer:** A text box containing the URL: `http://www.okta.com/okta/saml`
- X.509 Certificate:** A large text area containing a base64-encoded certificate string starting with '-----BEGIN CERTIFICATE-----' and ending with '-----END CERTIFICATE-----'. Below the text area is a 'Download certificate' button.

13. Save the certificate on the BeyondInsight server in:
C:\Program Files (x86)\Eye Digital Security\Retina CS\WebSiteSAML\Certificates
14. Rename the certificate to **okta.cer**.
15. Create or save a **.pfx** certificate that has a key and password (password must be known) in:
C:\Program Files (x86)\Eye Digital Security\Retina CS\WebSiteSAML\Certificates
16. Open the **saml.config** file:
C:\Program Files (x86)\Eye Digital Security\Retina CS\WebSiteSAML\saml.config
17. In a text editor such as **Notepad**, edit the following:
 - **ServiceProvider Name:** `https://ServerURL/Eye.RetinaCSSAML`
 - **FileName:** `Certificates\CertificateName.pfx`

- **Password:** <password>
- **PartnerIdentityProvider Name:** Identity provider issuer from above step
- **SingleSignOnServiceUrl:** Identity provider single sign-on URL from above step
- **SingleLogoutServiceUrl:** Identity provider single sign-on URL from above step

18. Save the **saml.config** file.

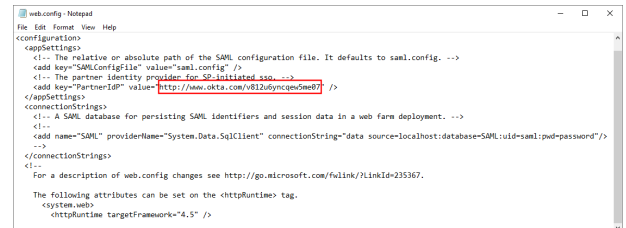
```
<?xml version="1.0"?><SAMLConfiguration xmlns="urn:oasis:names:tc:SAML:2.0:configuration"><ServiceProvider Name="http://localhost:ServiceProvider"><Description>Example Service Provider</Description><AssertionConsumerServiceUrl="http://localhost:ServiceConsumer"></AssertionConsumerServiceUrl><LocalCertificates><Certificate File="certificates/cert.pem" Password="password"/></LocalCertificates></ServiceProvider><PartnerIdentityProviders><!-- example --><PartnerIdentityProvider Name="http://localhost:NvExampleIdentityProvider"><Description>NVC Example Identity Provider</Description><SignOnRequest="true"></SignOnRequest><WantSAMLResponseSigned="true"></WantSAMLResponseSigned><WantAssertionSigned="false"></WantAssertionSigned><SingleSignOnServiceUrl="http://localhost:NvExampleIdentityProvider/SAML/SSOService"></SingleSignOnServiceUrl><SingleLogoutServiceUrl="http://localhost:NvExampleIdentityProvider/SAML/SLOService"></SingleLogoutServiceUrl><PartnerCertificates><Certificate File="certificates/cert.pem" Password="password"/></PartnerCertificates></PartnerIdentityProvider></PartnerIdentityProviders></SAMLConfiguration>
```

19. Open the **web.config** file:

C:\Program Files (x86)\Eye Digital Security\Retina CS\WebSiteSAML\web.config.

20. In a text editor such as **Notepad**, edit the **PartnerIdP** value to the identity provider issuer from above step.

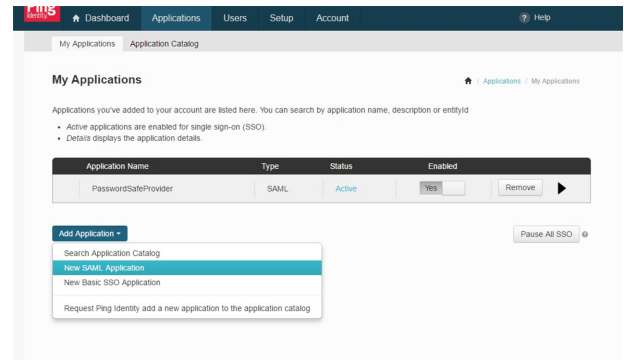
21. Save the **web.config** file.



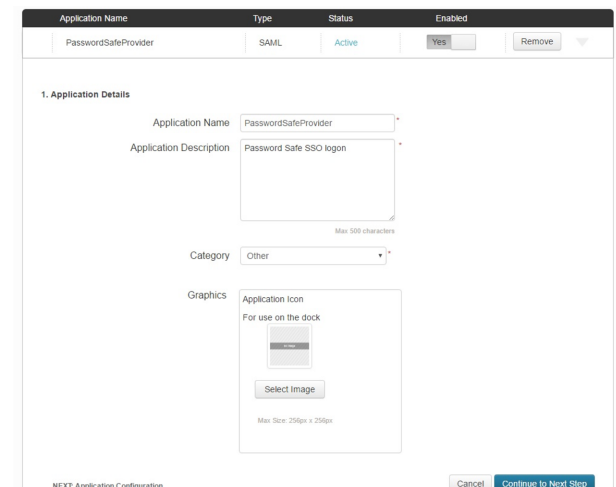
```
web.config - Notepad
File Edit Format View Help
<configuration>
  <appSettings>
    <!-- The relative or absolute path of the SAML configuration file. It defaults to saml.config. -->
    <add key="SAMLConfigFile" value="saml.config" />
    <!-- The Partner Identity provider for SP-initiated sso. -->
    <add key="PartnerIdP" value="http://www.okta.com/v81ubyncqew07" />
  </appSettings>
  <connectionStrings>
    <!-- A SAML database for persisting SAML identifiers and session data in a web farm deployment. -->
    <!--
    <add name="SAML" providerName="System.Data.SqlClient" connectionString="data source=localhost;database=SAML;uid=saml;pwd=password"/>
    -->
  </connectionStrings>
  <!--
  For a description of web.config changes see http://go.microsoft.com/fwlink/?linkid=235367.
  The following attributes can be set on the <httpRuntime> tag.
  <system.web>
    <httpRuntime targetFramework="4.5" />
  </system.web>
</configuration>
```

Configure Ping Identity with Password Safe

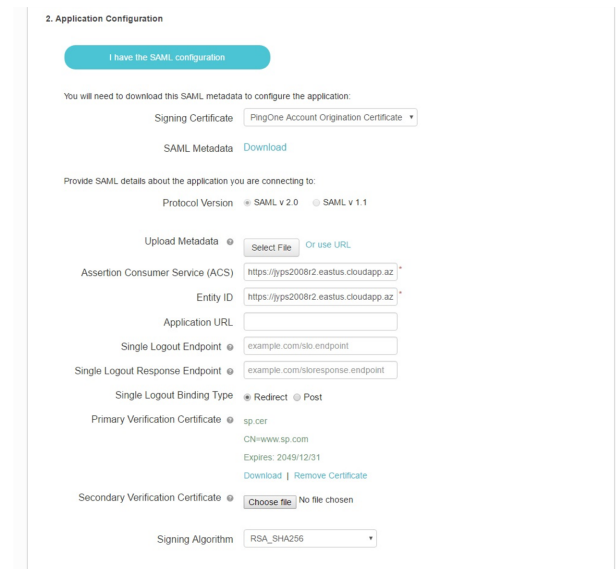
1. Log into the Ping Identity admin portal.
2. Click the **Add Application** button, and then select **New SAML Application** from the menu.



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



5. Set the following:
 - Set **Assertion Consumer Service (ACS)** to **https://<ServerURL>/eEye.RetinaCSSAML/saml/AssertionConsumerService.aspx**
 - Set **Entity ID** to **https://<ServerURL>/eEye.RetinaCSSAML**.
 - Set **Single Logout Binding Type** to **Redirect**.
 - Upload **Primary Verification Certificate** (use **sp.cer** from **\\WebSiteSAML\Certificates**).
 - Click **Continue to Next Step**.



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).

3. SSO Attribute Mapping

Map the necessary application provider (AP) attributes to attributes used by your identity provider (IdP).

Application Attribute	Identity Bridge Attribute or Literal Value	As Literal	Advanced	Required
1 Group	PingID	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2 Name	Email	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3 Email	Email	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4 Surname	Last Name	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5 GivenName	First Name	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

[Add new attribute](#)

NEXT: Review Setup Cancel Back Save & Publish




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 will automatically be brought into 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 into Password Safe. If the attribute is not present or is set to anything other than **Password Safe**, the user will be directed to BeyondInsight.


- Download the **Signing Certificate**.
- Download **SAML Metadata**.
- Click **Finish**.
- Copy **Signing Certificate** to the BeyondInsight server. Save it in the following location:
C:\Program Files (x86)\Eye Digital Security\Retina CSI\WebsiteSAML\Certificates.
- Rename the certificate to **pingone.cer**.
- Copy the private certificate with its key to
C:\Program Files (x86)\Eye Digital Security\Retina CSI\WebsiteSAML\Certificates
- Open **C:\Program Files (x86)\Eye Digital Security\Retina CSI\WebsiteSAML\saml.config**.


4. Review Setup

Test your connection to the application

Icon 

Name  PasswordSafeProvider

Description  Password Safe SSO login

Category  Other

(Optional) Click the link below to invite this SaaS Application's Administrator to register their SaaS Application with PingOne.

Invite SaaS Admin

These parameters may be needed to configure your connection


saasid b5c143a8-bd3e-4427-a53a-5ad833844955


idpid 44537c6b-90bd-4cf1-beed-0b8bebe35063

Protocol Version SAML v 2.0

ACS URL https://yps2008r2.eastus.cloudapp.azure.com/EyeRetinaCSSAML/saml/AssertionConsumerService.aspx

entityid https://yps2008r2.eastus.cloudapp.azure.com/EyeRetinaCSSAML

Initiate Single Sign-On (SSO) URL  https://sso.connect.pingidentity.com/sso/spinit/sso?saasid=b5c143a8-bd3e-4427-a53a-5ad833844955&idpid=44537c6b-90bd-4cf1-beed-0b8bebe35063

Single Sign-On (SSO) Relay State  https://pingone.com/v1.0/b5c143a8-bd3e-4427-a53a-5ad833844955


Signing Certificate [Download](#)

SAML Metadata [Download](#)

Single Logout Endpoint

Single Logout Response Endpoint

Signing Algorithm RSA_SHA256

Force Re-authentication  false

Click the link below to open the Single Sign-On page:
[Single Sign-On](#)

Back Finish

14. In a text editor such as **Notepad**, edit the following:

- Change **ServiceProvider Name** to **https://<ServerURL>/eEye.RetinaCSSAML**
- Change **PartnerIdentityProvider Name** to the **entityID** from the metadata:
https://pingone.com/idp/yourPingIDName
- Change **FileName** to **Certificates\CertificateName.pfx**.
- Change **Password** to **<password>**.
- Change **SingleSignOnServiceUrl**: **SingleSignOnService** to the **Location** from the metadata:

**https://sso.connect.pingidentity.com/sso/idp/SSO.saml
2?idpid=yourPingidpid**

```
<?xml version="1.0"?>
<SAMLConfiguration xmlns="urn:ietf:params:xml:ns:saml:2.0:configuration">
  <ServiceProvider Name="https://localhost:ServiceProvider">
    <Description>Example Service Provider</Description>
    <AssertionConsumerServiceUri>../SAML/AssertionConsumerService.aspx</AssertionConsumerServiceUri>
    <LocalCertificates>
      <Certificate
        FileName="Certificates\CertificateName.pfx"
        Password="password" />
    </LocalCertificates>
  </ServiceProvider>
  <PartnerIdentityProviders>
    <!-- example -->
    <PartnerIdentityProvider Name="https://localhost:MyExampleIdentityProvider">
      <Description>My Example Identity Provider</Description>
      <SignAuthnRequest>true</SignAuthnRequest>
      <WantSamlResponseSigned>true</WantSamlResponseSigned>
      <WantAssertionSigned>false</WantAssertionSigned>
      <WantAssertionEncrypted>false</WantAssertionEncrypted>
      <SingleSignOnServiceUri>https://localhost:MyExampleIdentityProvider/SAML/SSOService</SingleSignOnServiceUri>
      <SingleLogoutServiceUri>https://localhost:MyExampleIdentityProvider/SAML/SLOService</SingleLogoutServiceUri>
      <PartnerCertificates>
        <Certificate
          FileName="Certificates\ldg.crt" />
      </PartnerCertificates>
    </PartnerIdentityProvider>
  </PartnerIdentityProviders>
</SAMLConfiguration>
```

15. Save the **saml.config** file.

16. Open **C:\Program Files (x86)\eEye Digital Security\Retina CS\WebSiteSAML\web.config**.

17. In a text editor such as **Notepad**, change the **PartnerIdP** value to the **entityID** from the metadata:
https://pingone.com/idp/yourPingIDName.

18. Save the **web.config** file.

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <appSettings>
    <!-- The relative or absolute path of the SAML configuration file. It defaults to saml.config. -->
    <add key="samlConfigFile" value="saml.config" />
    <add key="PartnerIdP" value="https://pingone.com/idp/BeyondTrust" />
  </appSettings>
  <system.web>
    <!--
      Set compilation debug="true" to insert debugging
      symbols into the compiled page. Because this
      affects performance, set this value to true only
      during development.
    -->
  </system.web>
</configuration>
```


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 into the BeyondInsight management console, Analytics & Reporting, or Password Safe, although correct credentials were supplied:

- Authentication fails with *The user name 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.



For more information, please see [Problems with Kerberos authentication when a user belongs to many groups](https://support.microsoft.com/en-us/kb/327825) at <https://support.microsoft.com/en-us/kb/327825>.

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.

Authentication Errors when using SAML 2.0 Web Applications

Runtime Error

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

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

This should provide an actual error.

```

Server Error in '/eEye.RetinaCSSAML' Application.

Runtime Error
Description: An application 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 the local server machine.
Details: To enable the details of this specific error message to be viewable on remote machines, please create a 'customErrors' tag within a 'web.config' configuration file located in the root directory of the current web application. This configuration tag should have the following attribute set to 'true'.

<!-- web.config configuration file -->
<configuration>
  <system.web>
    <customErrors mode="Off"/>
  </system.web>
</configuration>

Notes: The current error page you are seeing can be replaced by a custom error page by modifying the 'defaultRedirect' attribute of the application's <customErrors> configuration tag to point to a custom error page URL.

<!-- web.config configuration file -->

```

```

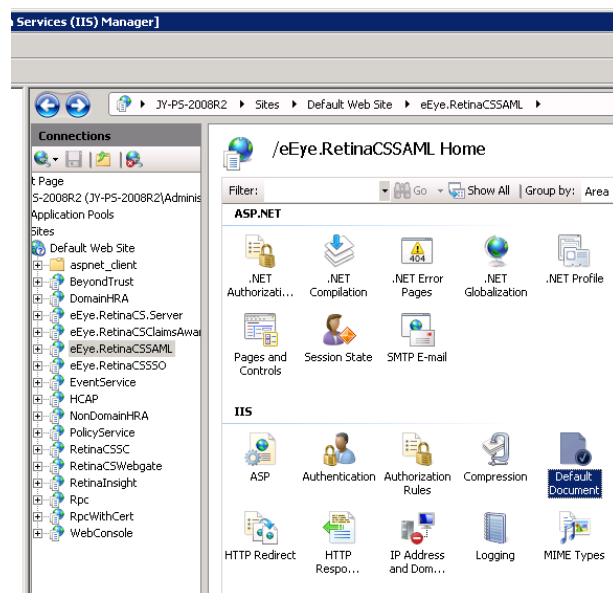
23 -->
24 <system.web>
25 <!--
26     Set compilation debug="true" to insert debugging
27     symbols into the compiled page. Because this
28     affects performance, set this value to true only
29     during development.
30 -->
31 <compilation debug="true" targetFramework="4.5" />
32 <authentication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

```

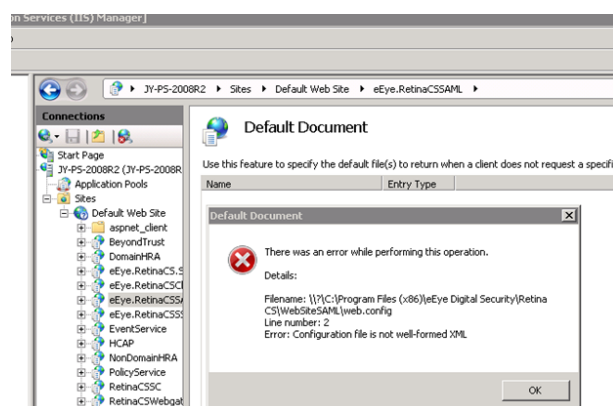
Internal Server Error (500)

Internal Server Error (500) 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**.



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



Extra Debug Logging

1. If it doesn't already exist on the appliance, create the **c:\temp** directory.
2. Add the following app setting key to the **web.config** file: **<add key="enableDebugLogging" value="True" />**.

3. Attempt a new SAML login. If Password Safe code is being hit after the user logs into the SAML 2.0 web application, a debug file is created in the **c:\temp** folder.

```

Web.config
1 <?xml version="1.0" encoding="UTF-8"?>
2 <configuration>
3   <appSettings>
4     <!-- The relative or absolute path of the SAML configuration file. It defaults to saml.config. -->
5     <add key="SAMLConfigFile" value="saml.config" />
6     <!-- The partner identity provider for SP-initiated SSO. -->
7     <add key="PartnerIdP" value="https://localhost/ExampleIdentityProvider/" />
8     <add key="enableDebugLogging" value="True" />
9   </appSettings>
10  <connectionStrings>
11    <!-- A SAML database for persisting SAML identifiers and session data in a web farm deployment. -->
12    <!--

```