



BeyondTrust

**Remote Support
Security Provider Integration: SAML
Single Sign-On**

Table of Contents

Use SAML for Single Sign-On Authentication	3
Create and Configure a SAML Security Provider for Representatives and Public Portals	4
SAML For Representatives Settings	4
SAML For Public Portals Settings	7
Log in Using SAML Single Sign-On	10
Log in to the Representative Console Using SAML Credentials	10
Log in to the /login Interface using SAML Credentials	11
Log in to the Public Portal Using SAML Credentials	11
Log in to BeyondTrust from the Identity Provider Side	12
Log in Directly to the Web Rep Console Using SAML	13
Manage SAML Security Providers	14
Disable	14
View Log	14

Use SAML for Single Sign-On Authentication

Integration of your B Series Appliance with external identity providers enables you to efficiently manage user access to BeyondTrust accounts by authenticating users against external directory stores.

This guide helps you configure the B Series Appliance to communicate with an identity provider using SAML 2.0 for the purpose of user authentication and group lookup.

Should you need any assistance, please log into the [Customer Portal](https://beyondtrustcorp.service-now.com/csm) at <https://beyondtrustcorp.service-now.com/csm> to chat with Support.



For more information about using SAML with specific providers, please see the following:

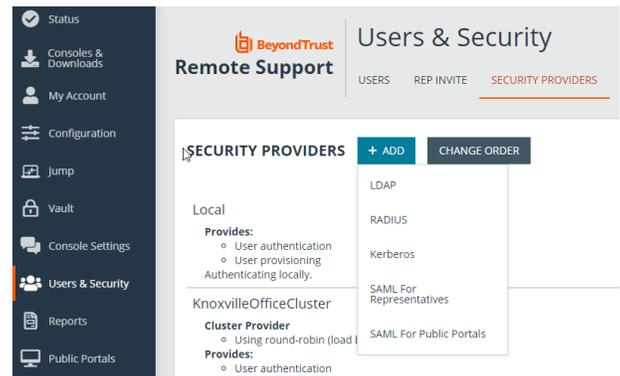
- [Configure SAML 2.0 for Remote Support Using Beyond Identity](https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/bid-saml/index.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/bid-saml/index.htm>
- [Configure SAML 2.0 for Remote Support Using Azure AD](https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/azure-saml/index.htm) at <https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/azure-saml/index.htm>

Create and Configure a SAML Security Provider for Representatives and Public Portals

Go to `/login > Users & Security > Security Providers`.

From the **+ ADD** dropdown, select the type of server you want to configure.

Note: You can configure only one SAML provider for public portals. Multiple SAML providers can be configured for representatives, but a representative who is defined in more than one provider can only be mapped to the first provider.



SAML For Representatives Settings

Name

Enter a unique name to help identify your provider.

Enabled

If checked, your BeyondTrust Appliance B Series can search this security provider when a user attempts to log in to the representative console or `/login`. If unchecked, this provider will not be searched.

Associated Email Domains

This setting only applies if you have more than one active SAML provider and is ignored otherwise.

Add any email domains that should be associated with this SAML provider, one per line. When authenticating, users are asked to enter their email. The domain of their email is matched against this list, and they are redirected to the appropriate identity provider for authentication.

If multiple SAML providers are configured and the user's email does not match any of the associated domain on any provider, then they are not allowed to authenticate.

Identity Provider Settings

Metadata

The metadata file contains all the information needed for the initial setup of your SAML provider and must be downloaded from your identity provider. Save the XML file, and then click **Upload Identity Provider Metadata** to select and upload the selected file.

Entity ID

Unique identifier for the identity provider you are using.

Server Certificate

This certificate will be used to verify the signature of the assertion sent from the identity provider.



Note: The fields for **Entity ID**, **Single Sign-On Service URL**, and **Certificate** are automatically populated from the identity provider's metadata file. If you cannot get a metadata file from your provider, this information can be entered manually. For metadata files with multiple identity providers, enter the **Entity ID** of the desired Identity Provider in the field below before uploading the metadata.

Single Sign-On Service URL

When you want to log in to BeyondTrust using SAML, this is the URL where you are automatically redirected so you can log in.

SSO URL Protocol Binding

Determines whether a user posts or is redirected to the sign on URL. This should be left defaulted to redirect unless otherwise required by the identity provider.

If request signing is enabled (under Service Provider settings), protocol binding is limited to redirect only.

Service Provider Settings

Download Service Provider Metadata

Download the BeyondTrust metadata, which must then be uploaded to your identity provider.

Entity ID

This is your BeyondTrust URL. It uniquely identifies the service provider.

Private Key

If necessary, you can decrypt messages sent by the identity provider, if they support and require encryption. Click **Choose File** to upload the private key necessary to decrypt the messages sent from the identity provider.

Signed AuthnRequest

Check to enable request signing. If enabled, SSO URL protocol binding is limited to redirect only. The SSO URL protocol binding field is updated automatically, if necessary.

A private key and signing certificate is required for request signing.

User Attribute Settings

SAML attributes are used to provision users within BeyondTrust. The default values match BeyondTrust-certified applications with various identity providers. If you are creating your own SAML connector, you may need to modify the attributes to match what is being sent by your identity provider. If your identity provider requires case-insensitivity for the NameID attribute, select **Use case-insensitive comparison for NameIDs**.

Authorization Settings

Lookup Groups Using This Provider

Enabling this feature allows faster provisioning by automatically looking up groups for this user, using **Group Lookup Attribute Name** and **Delimiter**. We recommend enabling this feature. If not used, SAML users must be manually assigned to group policies after their first successful authentication.

Group Lookup Attribute Name

Enter the name of the SAML attribute that contains the names of groups to which users should belong. If the attribute value contains multiple group names, then specify the **Delimiter** used to separate their names.

If left blank, SAML users must be manually assigned to group policies after their first successful authentication.

Group Lookup Delimiter

If the **Delimiter** is left blank, then the attribute value may contain multiple XML nodes with each one containing a different name.

Available Groups

This is an optional list of SAML groups always available to be manually assigned to group policies. If left blank, a given SAML group is made available only after the first successful authentication of a user member of such group. Please enter one group name per line.

Default Group Policy

Each user who authenticates against an external server must be a member of at least one group policy in order to authenticate to your B Series Appliance, logging into either the /login interface or the representative console. You can select a default group policy to apply to all users allowed to authenticate against the configured server.

If a default policy is defined, any allowed user who authenticates against this server might have access at the level of this default policy. Therefore, we recommend you set the default to a policy with minimum privileges to prevent users from gaining permissions you do not wish them to have.



Note: *If a user is in a default group policy and is then specifically added to another group policy, the settings for the specific policy always take precedence over the settings for the default, even if the specific policy is a lower priority than the default, and even if the default policy's settings are set to disallow override.*

SAML For Public Portals Settings

Name

The name for your SAML provider is auto-generated and cannot be edited at this time.

Enabled

If checked, your BeyondTrust Appliance B Series can search this security provider when a user attempts to log in to the public portal. If unchecked, this provider is not searched.

Identity Provider Settings

Metadata

The metadata file contains all the information needed for the initial setup of your SAML provider and must be downloaded from your identity provider. Save the XML file, and then click **Upload Identity Provider Metadata** to select and upload the selected file.

Entity ID

Unique identifier for the identity provider you are using.

Server Certificate

This certificate will be used to verify the signature of the assertion sent from the identity provider.



Note: The fields for **Entity ID**, **Single Sign-On Service URL**, and **Certificate** are automatically populated from the identity provider's metadata file. If you cannot get a metadata file from your provider, this information can be entered manually. For metadata files with multiple identity providers, enter the **Entity ID** of the desired Identity Provider in the field below before uploading the metadata.

Single Sign-On Service URL

When you want to log in to BeyondTrust using SAML, this is the URL where you are automatically redirected so you can log in.

SSO URL Protocol Binding

Determines whether a user posts or is redirected to the sign on URL. This should be left defaulted to redirect unless otherwise required by the identity provider.

If request signing is enabled (under Service Provider settings), protocol binding is limited to redirect only.

Service Provider Settings

Download Service Provider Metadata

Download the BeyondTrust metadata, which must then be uploaded to your identity provider.

Entity ID

This is your BeyondTrust URL. It uniquely identifies the service provider.

Private Key

If necessary, you can decrypt messages sent by the identity provider, if they support and require encryption. Click **Choose File** to upload the private key necessary to decrypt the messages sent from the identity provider.

Signed AuthnRequest

Check to enable request signing. If enabled, SSO URL protocol binding is limited to redirect only. The SSO URL protocol binding field is updated automatically, if necessary.

A private key and signing certificate is required for request signing.

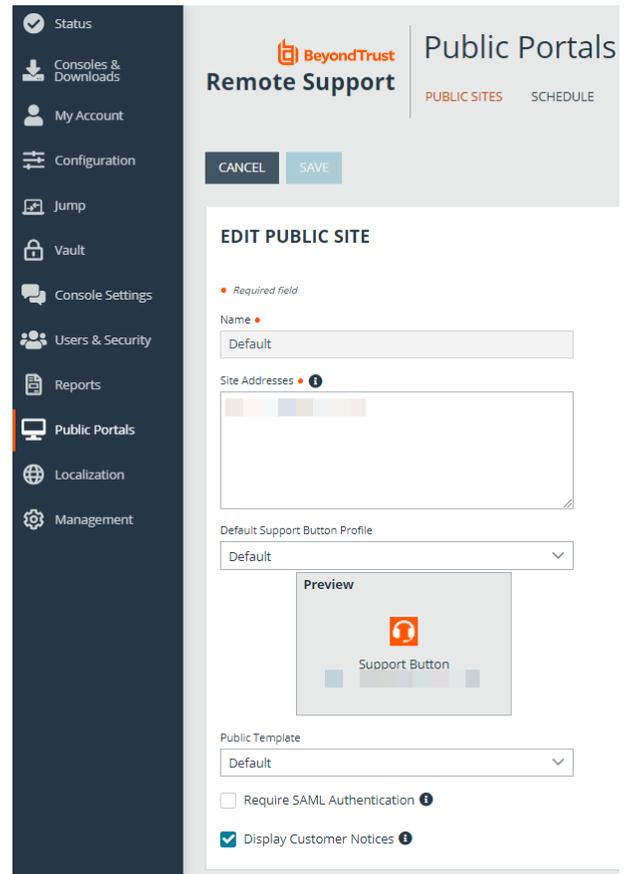
User Attribute Settings

SAML attributes are used to provision users within BeyondTrust. The default values match BeyondTrust-certified applications with various identity providers. If you are creating your own SAML connector, you may need to modify the attributes to match what is being sent by your identity provider. The SAML attributes can also be associated with customer sessions by adding custom fields with matching code names on the **Custom Fields** page in **/login**.

Enable SAML Authentication on a Public Site

Once **SAML for Public Portals** settings have been configured, you can enable SAML authentication on a public site in **/login** as follows:

1. Go to **Public Portals > Public Sites**.
2. Click **Edit** next to the desired public site.
3. Select **Require SAML Authentication**.
4. Click **Save**.



The screenshot shows the 'EDIT PUBLIC SITE' configuration page. On the left is a dark sidebar with navigation items: Status, Consoles & Downloads, My Account, Configuration, Jump, Vault, Console Settings, Users & Security, Reports, Public Portals (highlighted), Localization, and Management. The main content area has a header with the BeyondTrust logo, 'Remote Support', and 'Public Portals' with sub-links for 'PUBLIC SITES' and 'SCHEDULE'. Below the header are 'CANCEL' and 'SAVE' buttons. The form fields include: 'Name' (required field, value: Default), 'Site Addresses' (a list of colored address boxes), 'Default Support Button Profile' (dropdown menu, value: Default), a 'Preview' window showing a 'Support Button' with the BeyondTrust logo, 'Public Template' (dropdown menu, value: Default), and two checkboxes: 'Require SAML Authentication' (unchecked) and 'Display Customer Notices' (checked).

Log in Using SAML Single Sign-On

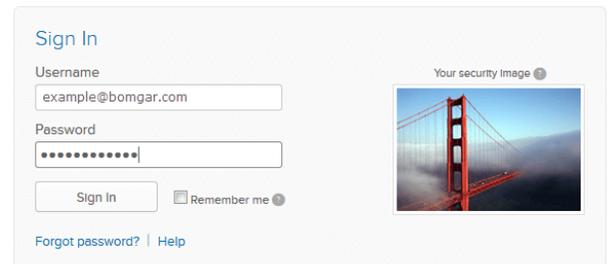
Representatives can utilize SAML single sign-on to gain access to the representative console or **/login** interface. Customers can utilize SAML single sign-on to gain access to the public support portal. Alternatively, a login can be initiated from the identity provider's side.

Log in to the Representative Console Using SAML Credentials

1. Select **SAML Credentials** from the dropdown menu.



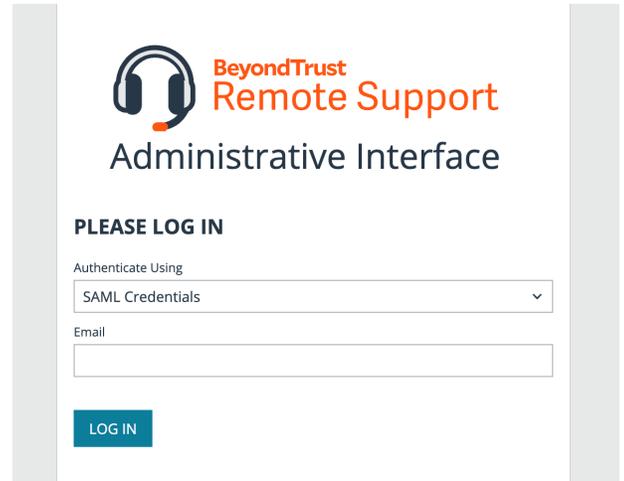
2. If you have not yet logged into your identity provider, you will be redirected using the default browser.



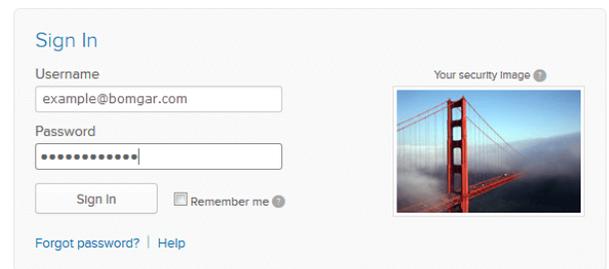
- i** Representatives can access the mobile representative console using SAML for mobile. For more information, please see:
- [Log in to the Representative Console for iOS at www.beyondtrust.com/docs/remote-support/getting-started/rep-console/ios/howtouseherepconsole.htm](http://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/ios/howtouseherepconsole.htm)
 - [Log in to the Representative Console for Android at www.beyondtrust.com/docs/remote-support/getting-started/rep-console/android/howtouseherepconsole.htm](http://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/android/howtouseherepconsole.htm)

Log in to the /login Interface using SAML Credentials

1. From the /login interface, select **Use SAML Authentication**.



2. If you have not yet logged in to your identity provider, you will be redirected to their site to enter your credentials.



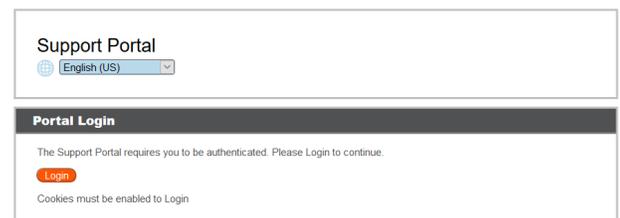
3. Click **Sign In**. You are taken to the /login interface.



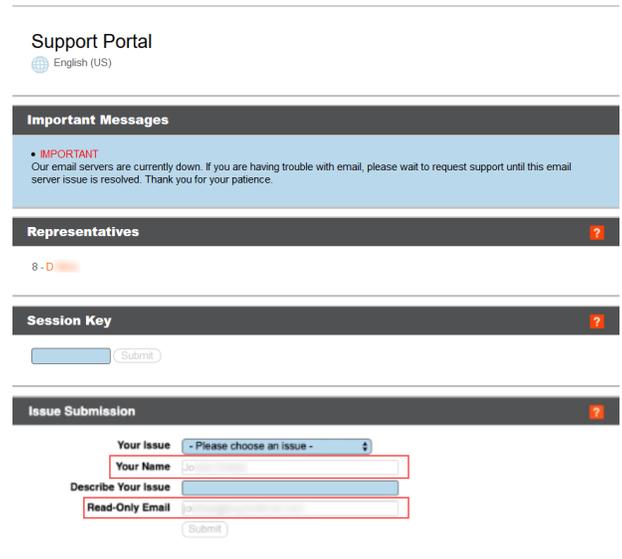
Note: If you are already logged into your identity provider when you click **Use SAML Authentication**, you are taken directly to the /login interface.

Log in to the Public Portal Using SAML Credentials

A customer can access the public support portal using the URL provided by a representative. If SAML authentication is configured and enabled for the public site, the customer is presented with the **Portal Login** window. The customer must click **Login** and then provide credentials to authenticate with the identity provider.



The customer is then taken to the support portal page where they can submit their request for support. The customer's name and any custom fields that are configured, such as email, are automatically populated and are not editable.



The screenshot shows the 'Support Portal' interface. At the top, it says 'Support Portal' with a globe icon and 'English (US)'. Below this is an 'Important Messages' section with a blue background and a red 'IMPORTANT' header. The message states: 'Our email servers are currently down. If you are having trouble with email, please wait to request support until this email server issue is resolved. Thank you for your patience.' Below that is a 'Representatives' section with a red question mark icon and a small red box containing '8 - D'. The 'Session Key' section has a 'Submit' button. The 'Issue Submission' section contains a dropdown menu for 'Your Issue', and three input fields for 'Your Name', 'Describe Your Issue', and 'Read-Only Email', each with a 'Submit' button below them.

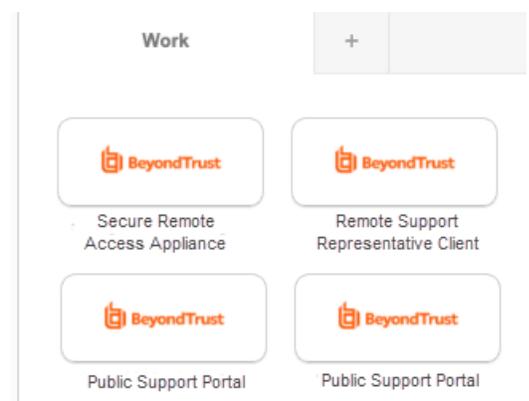
 **Tip:** A green check mark is displayed next to the customer's name in the representative console chat window to indicate the user is public portal authenticated.



The screenshot shows a chat window interface. At the top, there is a user profile card for 'Jo' with a green checkmark icon next to the name. Below the profile is a large text input field. At the bottom of the input field, there are 'Messages' and 'Send' buttons. Below the input field are three tabs: 'Everyone', 'Representatives', and 'Notes'. At the very bottom, there is a 'Session Info' section with a plus sign icon.

Log in to BeyondTrust from the Identity Provider Side

Depending on your identity provider, you can opt to log in to your BeyondTrust representative console, public portal, or **/login** interface from the provider's web site. In this example, the provider has icons for BeyondTrust applications. Simply log in to your provider's site, and then click on the application you want to use.



The screenshot shows an identity provider application selection screen. At the top, there is a 'Work' section with a plus sign icon. Below this are four application cards, each with the BeyondTrust logo and a title: 'Secure Remote Access Appliance', 'Remote Support Representative Client', 'Public Support Portal', and 'Public Support Portal'.

Log in Directly to the Web Rep Console Using SAML

It is possible to configure an application or tile in a SAML identity provider (IdP), (like the tiles used to log into Okta and similar applications) that takes you directly to the web rep console rather than to /login.

To configure this, you must:

- Set up application in the IdP as you would for /login
- Change the **RelayState** parameter to the word *console* (lowercase, no /, etc.)

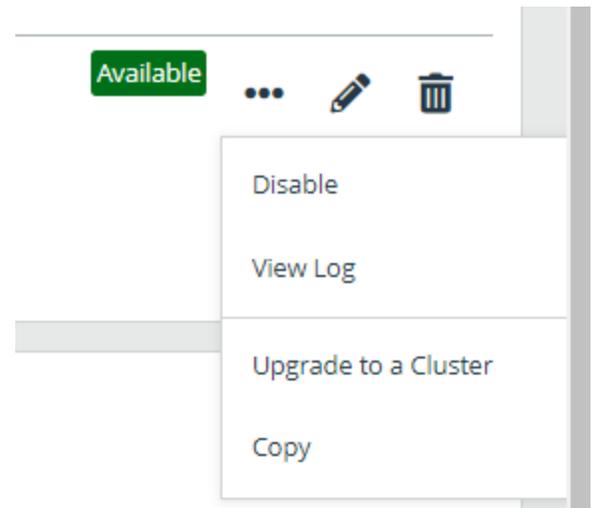
There are two parts to the SAML configuration: the IdP and service provider (SP). In this instance you are the SP, and the SAML service is the IdP (OneLogin, Okta, and similar). Currently, you can export metadata from the SAML security provider on /login (in the Service Provider section), which you can then import into the IdP to help configure the SAML side. If, as part of this configuration, you set the **RelayState** parameter to **console**, then any login initiated from the IdP (for example, clicking the tile in Okta) sends you to the web rep console rather than to /login.

Manage SAML Security Providers

The list of security providers has several icons at the right end of row. Click the pencil icon to edit the provider. Click the trash can icon to delete the provider. Click the ellipsis for actions available for that providers. Actions available depend on the provider type and setting, but usually include **Disable** and **View Log**.

Disable

Disable this security provider connection. This is useful for scheduled maintenance, when you want a server to be offline but not deleted.



View Log

View the status history or any errors for a security provider connection.