



# BeyondTrust

**Privileged Remote Access  
Security Provider Integration: SAML  
Single Sign-On**

## Table of Contents

---

<b>Use SAML for Single Sign-On Authentication</b> .....	<b>3</b>
<b>Create and Configure the SAML Security Provider</b> .....	<b>4</b>
Add Security Provider .....	4
Identity Provider Settings .....	5
Service Provider Settings .....	5
User Attribute Settings (Visible Only if This Provider is Used for User Provisioning) .....	6
Authorization Settings (Visible Only if This Provider is Used for User Provisioning) .....	6
<b>Log in to Privileged Remote Access Using SAML Single Sign-On</b> .....	<b>8</b>
Log into the Access Console Using SAML Credentials .....	8
Log into the /login Interface using SAML Credentials .....	9
<b>Manage Security Providers: SAML Servers and Others</b> .....	<b>10</b>
View Log .....	10
Disable Connection .....	10

## 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:*

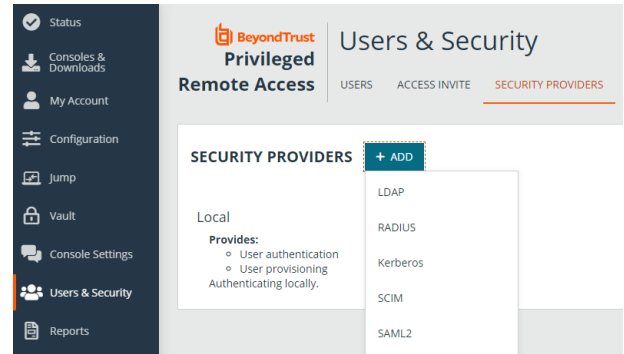
- [Configure SAML 2.0 for Privileged Remote Access using Beyond Identity at https://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/security-providers/bid-saml/index.htm](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/security-providers/bid-saml/index.htm)
- [Configure SAML 2.0 for Privileged Remote Access using Azure AD App at https://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/security-providers/azure-saml/index.htm](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/security-providers/azure-saml/index.htm)

## Create and Configure the SAML Security Provider

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

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

 **Note:** Multiple SAML providers can be configured, but a user who is defined in more than one provider can only be mapped to the first provider.



## Add Security Provider

### Name


Enter a unique name to identify the provider.

### Enabled

If checked, your B Series Appliance searches this security provider when a user attempts to log in. If unchecked, this provider is not searched.

### User Provision

By default, user provisioning occurs on this provider. If you have a SCIM provider set up, you can choose to provision users through that provider instead.

 **Note:** This setting cannot be modified after this security provider is first saved.

## 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

### Identity Provider 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 **Choose File** to select and upload the selected file.



*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.*

### Entity ID

This is the unique identifier for the identity provider you are using.

### Single Sign-On Service URL

This is the URL where you are automatically redirected to log in to BeyondTrust Privileged Remote Access using SAML.

### SSO URL Protocol Binding

This determines whether an HTTP POST occurs or whether the user is redirected to the sign-on URL. Choose HTTP redirect if not specified by the provider.

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

### Server Certificate

This certificate is used to verify the signature of the assertion sent from the identity provider. Click **+UPLOAD** to open a file browse window, navigate to the certificate, and click Open.

## Service Provider Settings

### Service Provider Metadata

Download the BeyondTrust metadata, which you then need to upload to your identity provider.

### Entity ID

This is your BeyondTrust URL. It uniquely identifies your site to the identity 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 (Visible Only if This Provider is Used for User Provisioning)

### User SAML Attributes

These 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.

## Authorization Settings (Visible Only if This Provider is Used for User Provisioning)

### 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 access 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.*

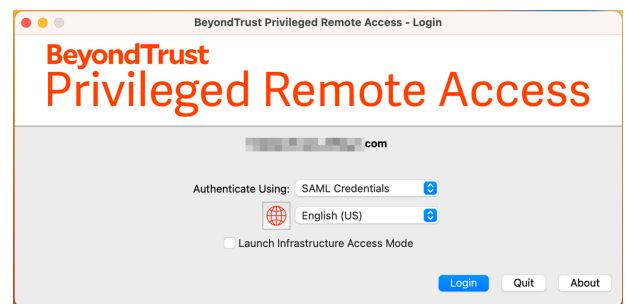
# Log in to Privileged Remote Access Using SAML Single Sign-On

SAML single sign-on works for the access console or the administrative /login interface.

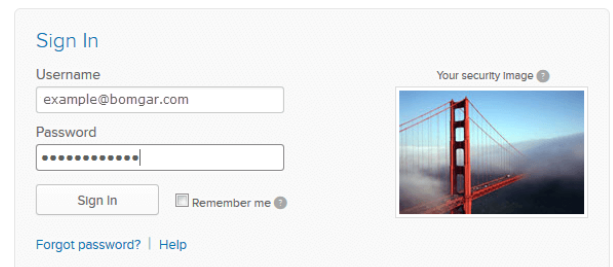
Depending on your identity provider, users can also log in to the BeyondTrust access console or /login interface from the provider's web site or application.

## Log into the Access Console Using SAML Credentials

To log into the BeyondTrust access console, select **SAML Credentials** from the dropdown menu.



If you have not yet logged into your identity provider, you are redirected using the default browser. After logging into the identity provider, the web browser redirects you to access console.

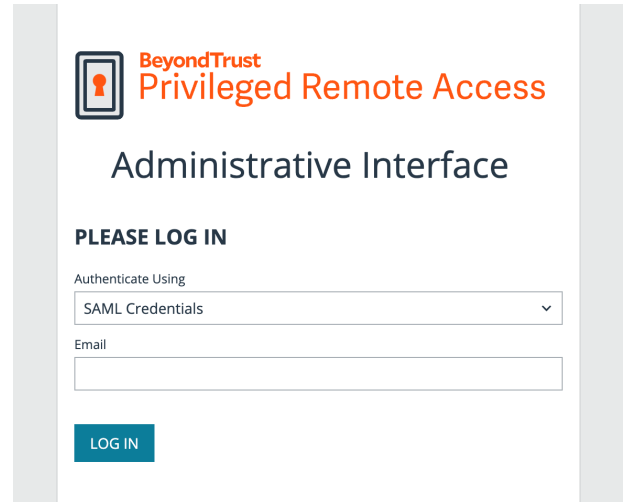


**Note:** Users can access the mobile access console using SAML for mobile. To learn more, please see [Log into the Access Console at www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/apple-ios/access-console.htm](http://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/apple-ios/access-console.htm) and [Log into the Access Console for Android at www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/android/access-console.htm](http://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/android/access-console.htm).



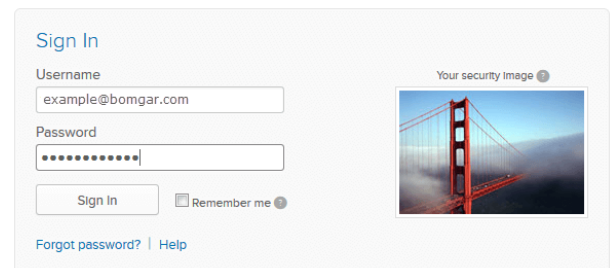
## Log into the /login Interface using SAML Credentials

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



The screenshot shows the login interface for BeyondTrust Privileged Remote Access. At the top left is the BeyondTrust logo. To its right, the text reads "BeyondTrust Privileged Remote Access" in orange and "Administrative Interface" in dark grey. Below this, the heading "PLEASE LOG IN" is displayed in bold. Underneath is a form with a dropdown menu labeled "Authenticate Using" set to "SAML Credentials". Below the dropdown is an "Email" input field. At the bottom of the form is a blue "LOG IN" button.

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



The screenshot shows a generic "Sign In" page. It has a title "Sign In" in blue. Below the title are two input fields: "Username" with the value "example@bomgar.com" and "Password" with masked characters. To the right of the password field is a "Remember me" checkbox. Below the input fields is a "Sign In" button. At the bottom left, there are links for "Forgot password?" and "Help". On the right side, there is a section titled "Your security image" with a small image of the Golden Gate Bridge.

When you click **Sign In** you are taken to the /login interface.



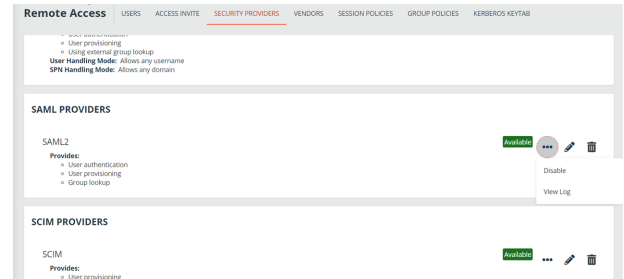
**Note:** If you are already logged into your identity provider, then when you click **Use SAML Authentication** to log in, you are taken directly to the /login interface.

## Manage Security Providers: SAML Servers and Others

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 provider.

### View Log

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



### Disable Connection

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