BeyondTrust

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

TC:2/8/2019

Table of Contents

SAML for Single Sign-On Authentication

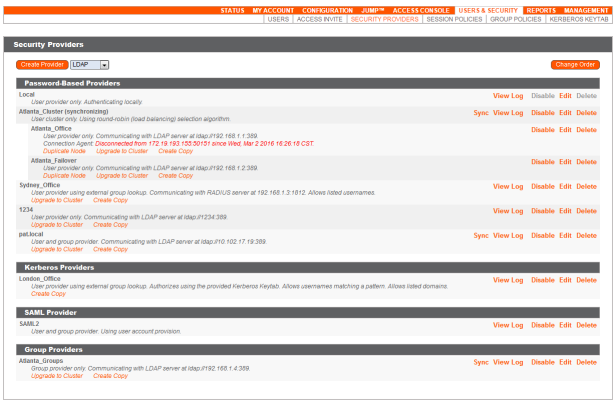
Integration of your BeyondTrust Appliance with external identity providers enables administrators to efficiently manage user access to BeyondTrust accounts by authenticating users against external directory stores. This guide is designed to help you configure the BeyondTrust Appliance to communicate with an identity provider using SAML 2.0 for the purpose of user authentication and group lookup.

Should you need any assistance, please contact BeyondTrust Technical Support at help.bomgar.com.

Create and Configure the SAML Security Provider

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

From the dropdown, select the type of server you want to configure. Then click the **Create Provider** button.



> ***Note:*** *You can configure only one SAML provider.*

General Settings

Name

This unique name helps to identify your provider. The name for your SAML provider is auto-generated and cannot be edited at this time.

Enabled

If checked, your BeyondTrust Appliance can search this security provider when a user attempts to log in. If unchecked, this provider will not be 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.*

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 **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

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

Protocol Binding

This determines whether an HTTP POST occurs or whether the user is redirected to the sign-on URL. This should be left as redirect unless otherwise required by the identity provider.

Certificate

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

Service Provider Settings

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.

User Provision Settings *(Visible Only if This Provider is Used for User Provisioning)*

User Attribute

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)*

Group Lookups

This is the SAML attribute that contains the names of groups to which users should belong. The default name for the BeyondTrust applications is "Groups".

> ***Note:*** *If the attribute value contains multiple group names, you need to specify the delimiter used to separate their names. If the delimiter is left blank, then the attribute value may contain multiple XML nodes with each one containing a different name.*

Available Groups

Allows a predefined list of groups to be associated with the security provider. This list can then be used to associate a group with the appropriate group policy.

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 BeyondTrust 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.

Note that if a default policy is defined, then any allowed user who authenticates against this server will potentially have access at the level of this default policy. Therefore, it is recommended that you set the default to a policy with minimum privileges to prevent users from gaining permissions that you do not wish them to have.

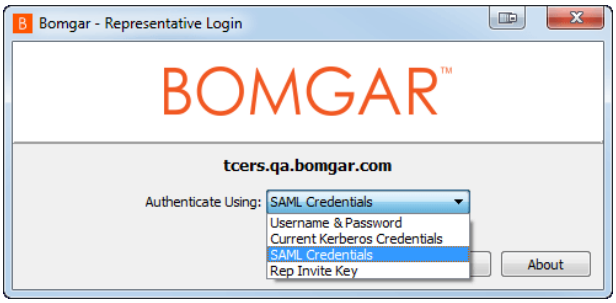
> ***Note:*** *If a user is in a default group policy and is then specifically added to another group policy, the settings for the specific policy will always take precedence over the settings for the default, even if the specific policy is a lower priority than the default, and even if the default policy's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

Log in Using SAML Single Sign-On

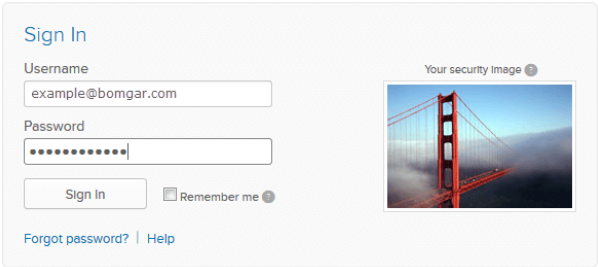
Users can utilize SAML single sign-on to gain access to the access console or /login interface. Alternatively, a login can be initiated from the identity provider's side.

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 will be redirected using the default browser.



Once authenticated, a BeyondTrust access console script is downloaded to gain access to the access console.

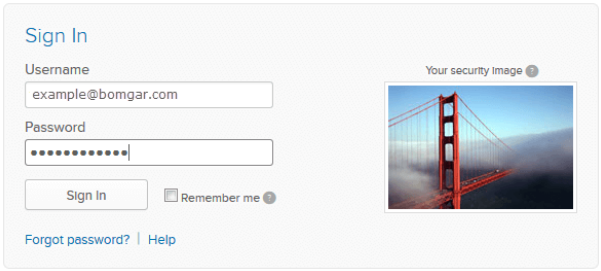
Note: *The BRCS file that is downloaded is configured by default to open the access console. Most browsers can be configured to do this automatically, which will keep the user from having to execute the script with each login.*

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 and Log into the Access Console for Android at 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**.

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

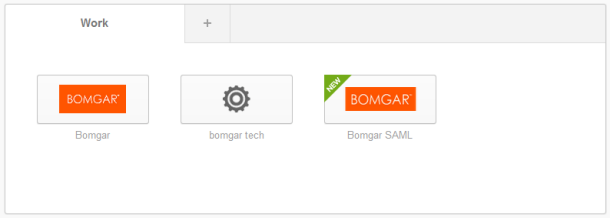


When you click **Sign In** you are taken to the /login interface.

> ***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.*

Log into BeyondTrust from the Identity Provider Side

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



Manage Security Providers: SAML Servers and Others

View Log

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

Disable

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