Privileged Remote Access BlokSec Integration Guide

TC:3/4/2024

Table of Contents

Integrate BlokSec and BeyondTrust Privileged Remote Access ... 3

Prerequisites ... 3

Create Privileged Remote Access Application in the BlokSec Administration Console ... 3

Configure the SAML Identity Provider in BeyondTrust ... 8

Test the Configuration ... 10

Integrate BlokSec and BeyondTrust Privileged Remote Access

Traditional remote access methods such as RDP, VPN, and legacy remote desktop tools lack granular access management controls. These processes enable easy exploits via stolen credentials and session hijacking. Extending remote access to your vendors makes matters even worse.

BeyondTrust Privileged Remote Access enables organizations to apply least privilege and audit controls to all remote access from employees, vendors, and service desks. BlokSec provides users the ability to securely connect without the hassle of passwords or MFA.

Integrating Privileged Remote Access with BlokSec requires configuring a BlokSec instance and configuring a SAML authentication provider in Privileged Remote Access.

To learn more about BlokSec, please see the BlockSec website at https://bloksec.com/.

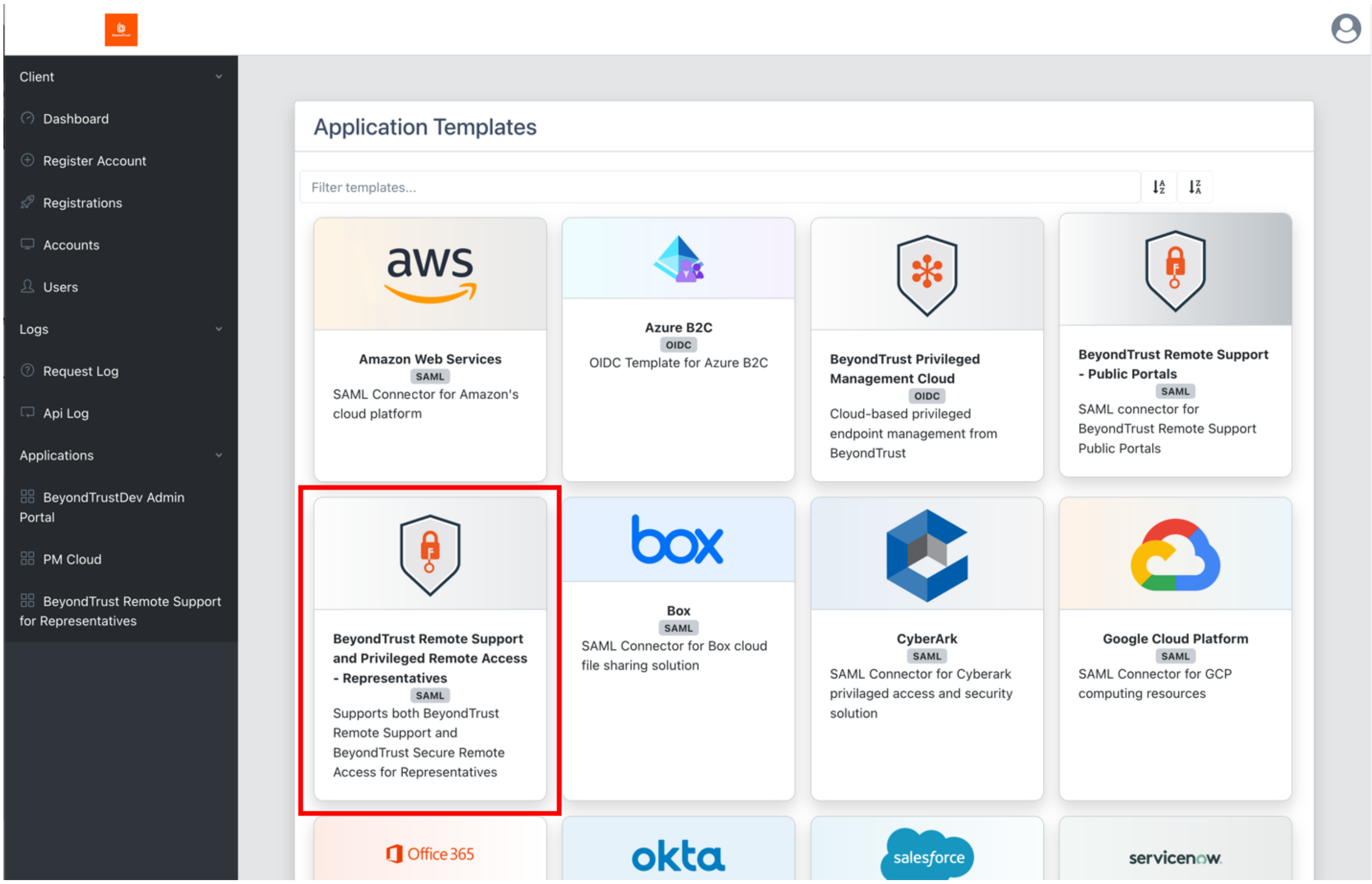
Prerequisites

- Installed BeyondTrust Privileged Remote Access instance
- Installed BlokSec instance
- BlokSec test users with mobile app installed

Create Privileged Remote Access Application in the BlokSec Administration Console

Log in to Bloksec and follow the steps below:

1. From the dashboard, click **+ Add Application**.
2. Select **Create from Template**.
3. Select the **BeyondTrust Remote Support and Privileged Remote Access for Representatives** template.



Application Templates

Amazon Web Services
SAML
SAML Connector for Amazon's cloud platform

Azure B2C
OIDC
OIDC Template for Azure B2C

BeyondTrust Privileged Management Cloud
OIDC
Cloud-based privileged endpoint management from BeyondTrust

BeyondTrust Remote Support - Public Portals
SAML
SAML connector for BeyondTrust Remote Support Public Portals

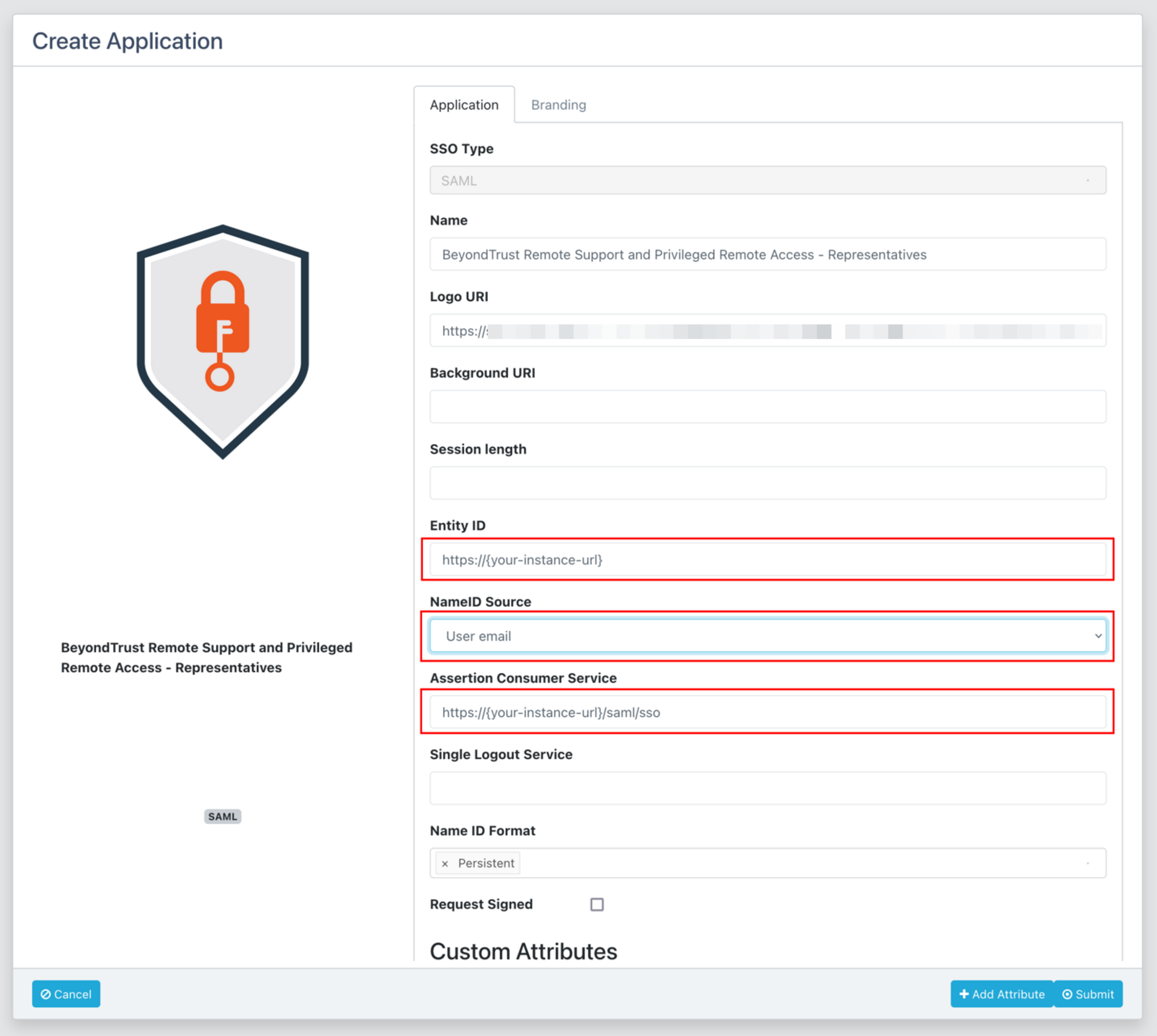
BeyondTrust Remote Support and Privileged Remote Access - Representatives
SAML
Supports both BeyondTrust Remote Support and BeyondTrust Secure Remote Access for Representatives

Box
SAML
SAML Connector for Box cloud file sharing solution

CyberArk
SAML
SAML Connector for Cyberark privilaged access and security solution

Google Cloud Platform
SAML
SAML Connector for GCP computing resources

4. On the **Create Application** screen:
   - Replace **{your-instance-url}** in the **Entity ID** and **Assertion Consumer Service** URLs with the URL of your BeyondTrust site (for example, **eval######.beyondtrustcloud.com** or your customer URL).
   - Set the **NameID Source** to **User email**.



Create Application

BeyondTrust Remote Support and Privileged Remote Access - Representatives

SSO Type: SAML

Name: BeyondTrust Remote Support and Privileged Remote Access - Representatives

Logo URI: https://[redacted]

Background URI:

Session length:

Entity ID: https://{your-instance-url}

NameID Source: User email

Assertion Consumer Service: https://{your-instance-url}/saml/sso

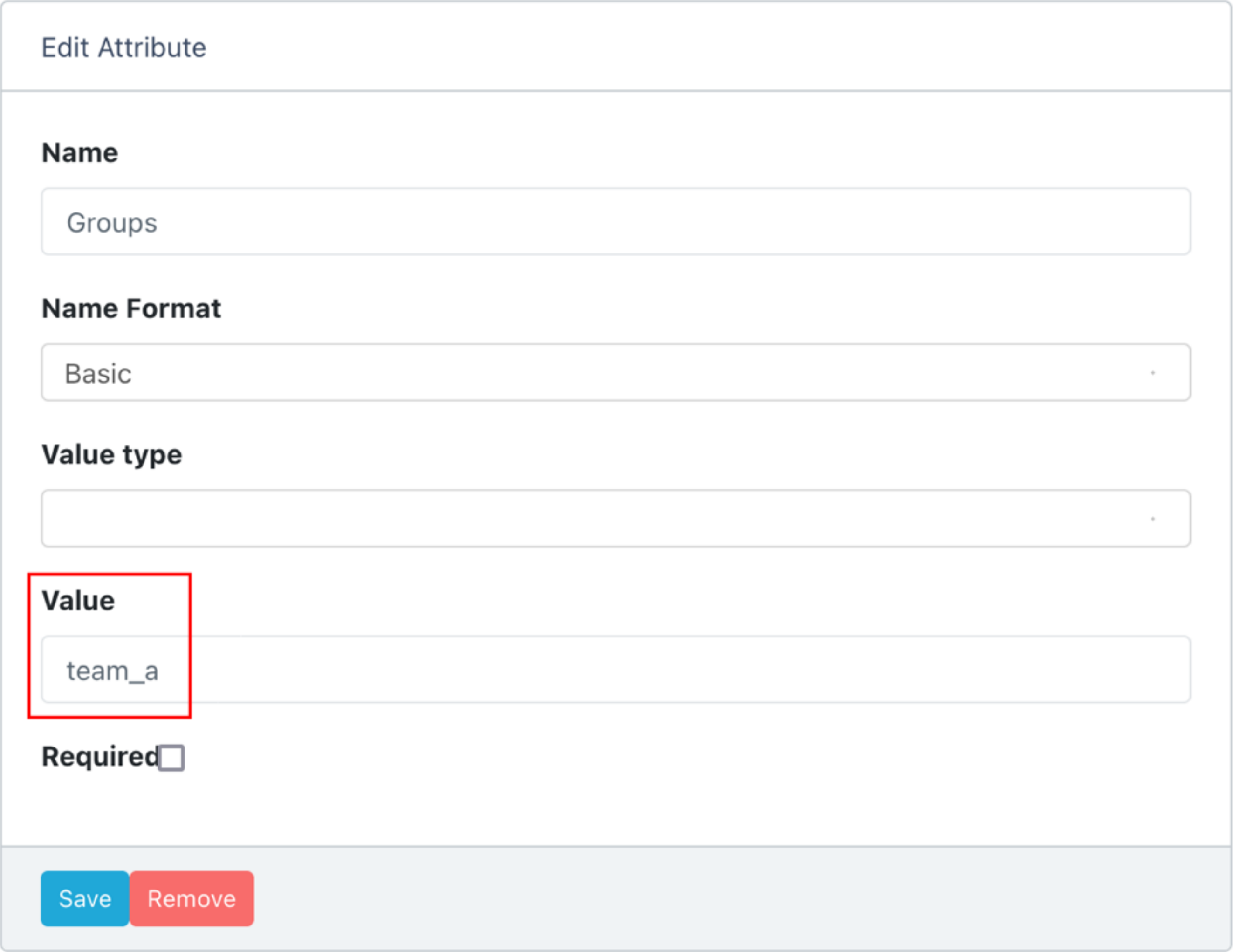
Single Logout Service:

Name ID Format: × Persistent

Request Signed □

Custom Attributes

5. Edit the **Groups** attribute and set the **Value** to the group name, which is passed with the SAML assertion.



Edit Attribute

Name: Groups

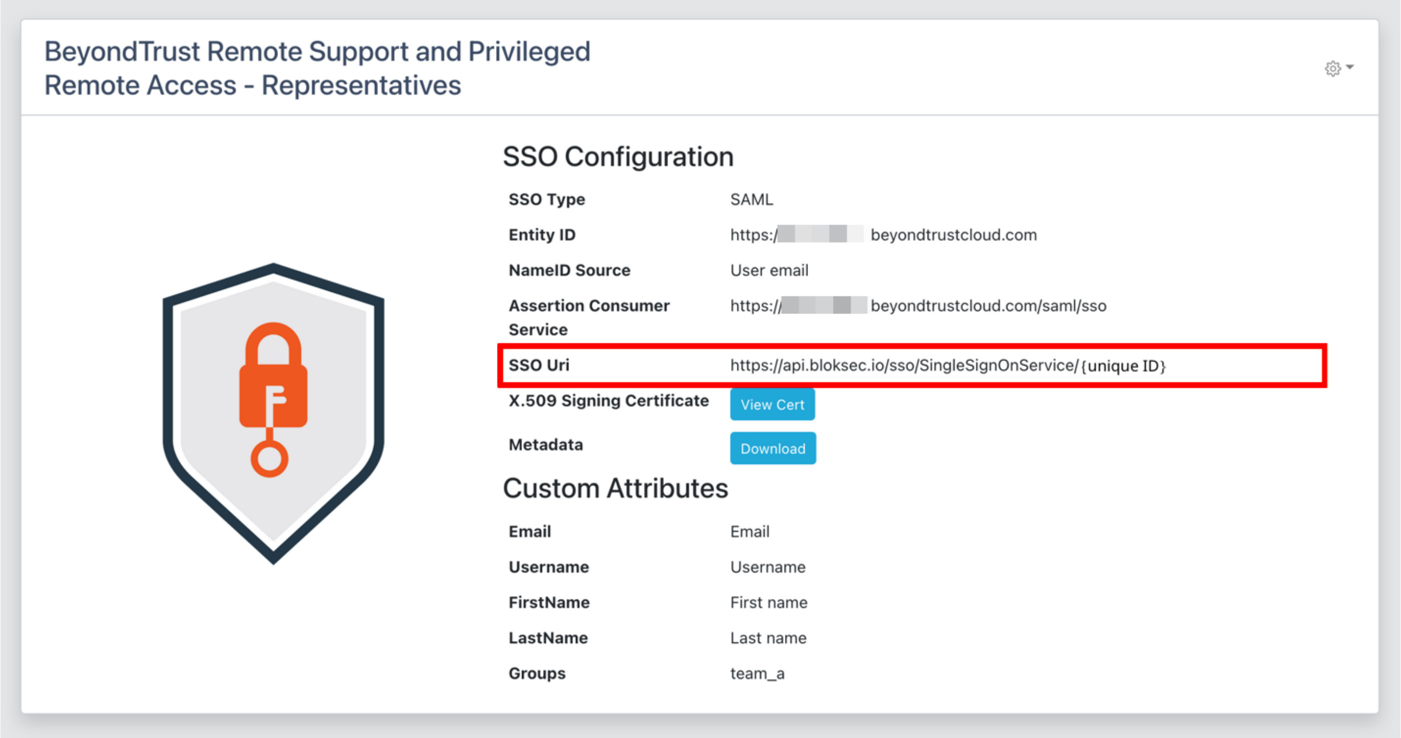
Name Format: Basic

Value type:

Value: team_a

Required □

6. Submit the new application, and then make note of the **SSO Uri**, and view and save the **X.509 Signing Certificate** in a new file, for example, **signing_cert.pem**.



BeyondTrust Remote Support and Privileged Remote Access - Representatives

SSO Configuration

SSO Type	SAML
Entity ID	https:/[redacted] beyondtrustcloud.com
NameID Source	User email
Assertion Consumer Service	https://[redacted] beyondtrustcloud.com/saml/sso
SSO Uri	https://api.bloksec.io/sso/SingleSignOnService/{unique ID}
X.509 Signing Certificate	View Cert
Metadata	Download

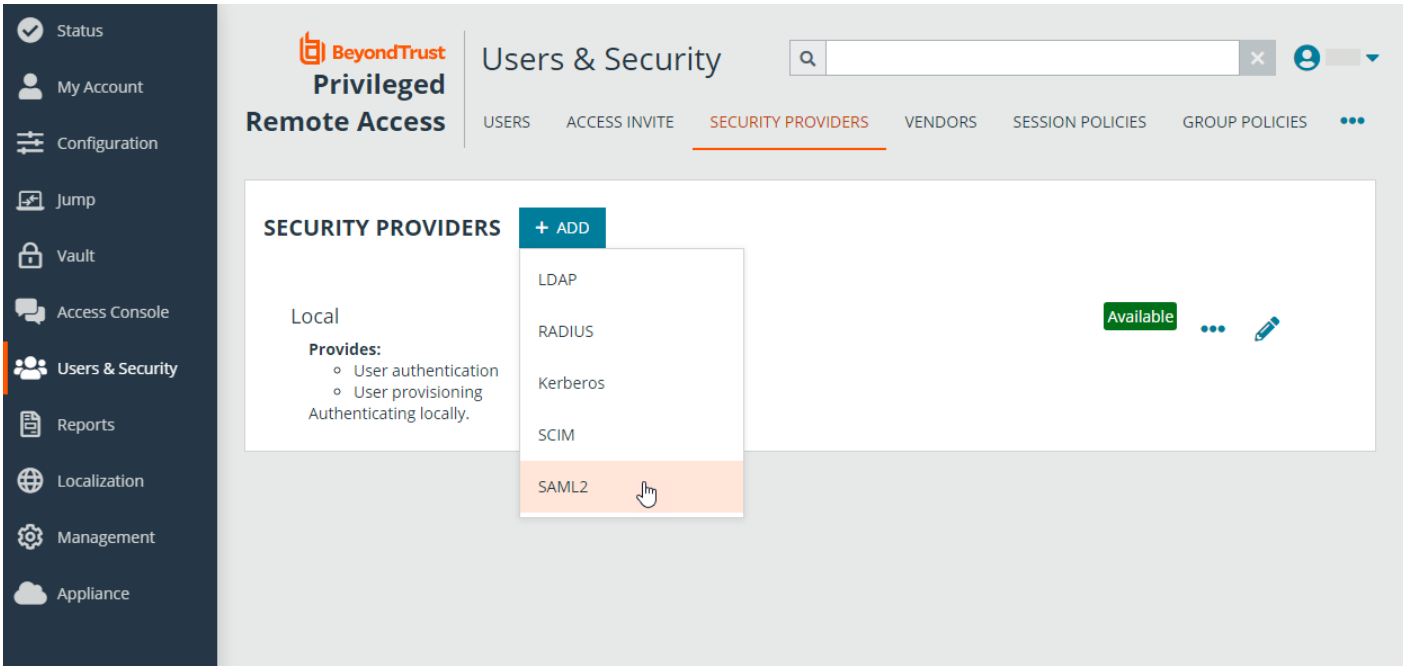
Custom Attributes

Email	Email
Username	Username
FirstName	First name
LastName	Last name
Groups	team_a

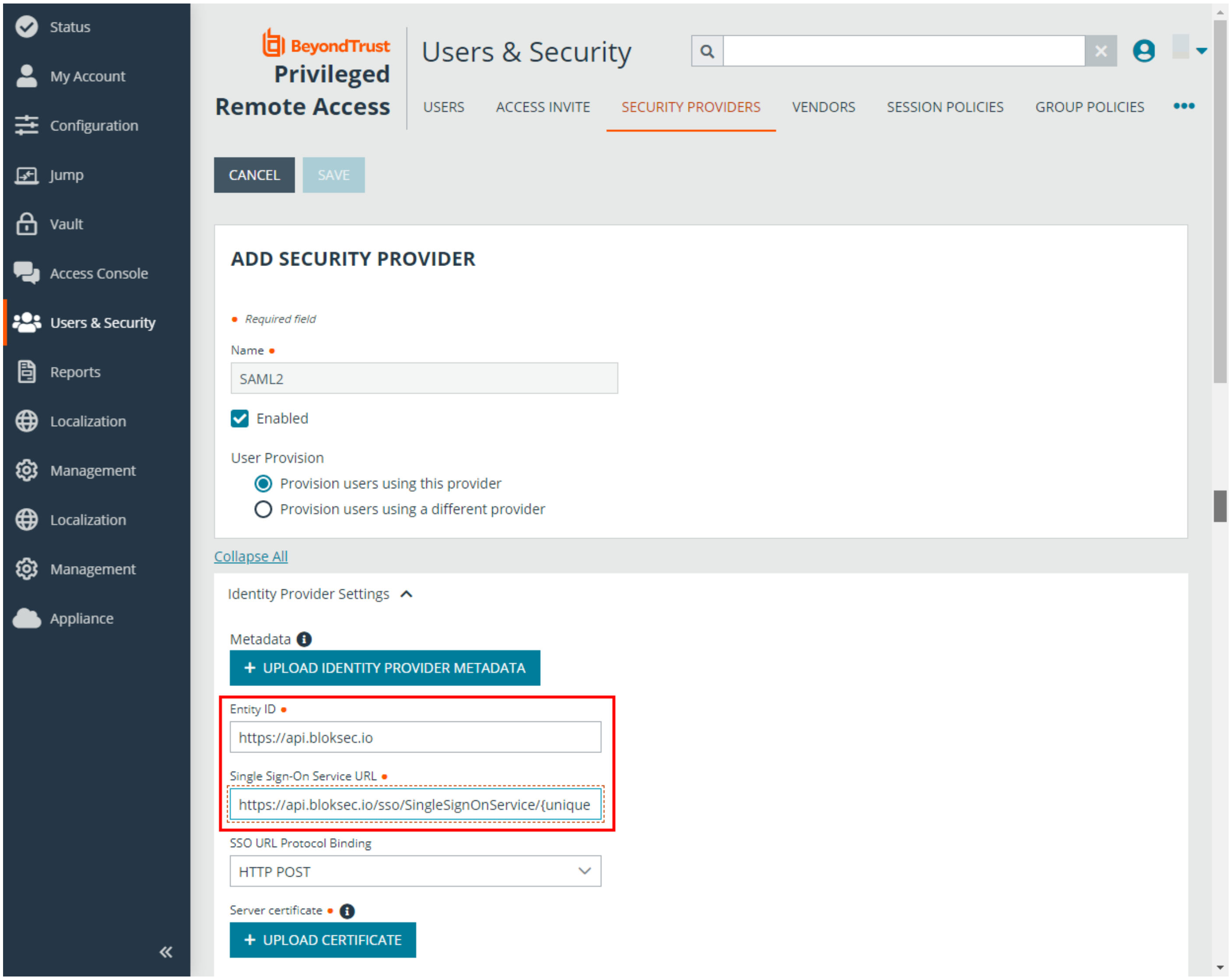
Configure the SAML Identity Provider in BeyondTrust

Log in to BeyondTrust Privileged Remote Access. Continue with the steps below.

1. Click the **Users & Security > Security Providers** tab, click **+ Add**, and select **SAML2**.



2. Under **Identity Provider Settings**:
    - Enter the **Entity ID**: *https://api.bloksec.io*
    - Set the **Single Sign-On Service URL** to the **SSO Uri** value provided by BlokSec when the new application was submitted in the BlokSec Administration Console. For example, *https://api.bloksec.io/sso/SingleSignOnService/{unique ID}*.
    - Click **+ UPLOAD CERTIFICATE** and upload the certificate downloaded from BlokSec when the new application was submitted in the BlokSec Administration Console.



ADD SECURITY PROVIDER

• Required field

Name •
SAML2

☑ Enabled

User Provision
● Provision users using this provider
○ Provision users using a different provider

Identity Provider Settings

Metadata

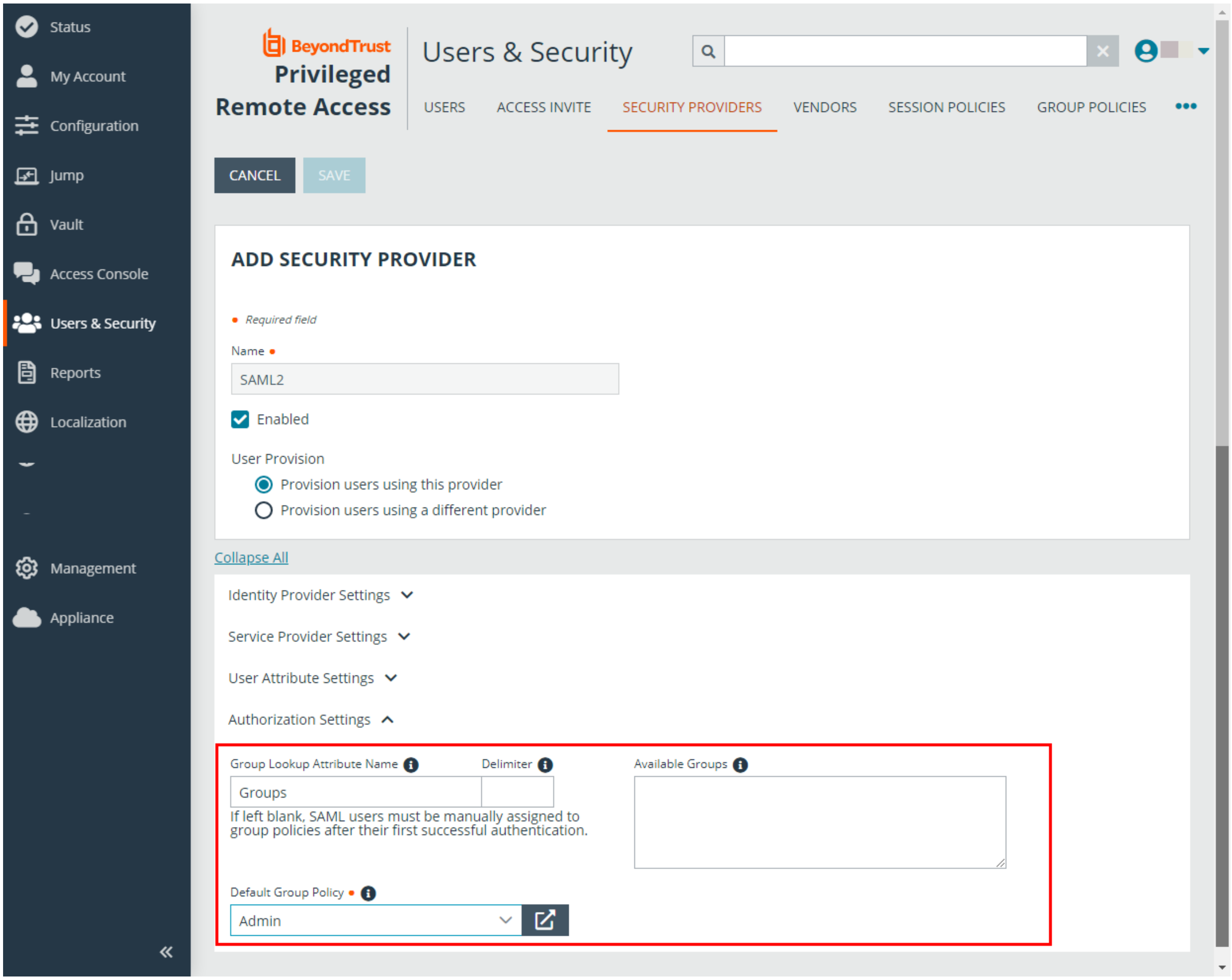
Entity ID •
https://api.bloksec.io

Single Sign-On Service URL •
https://api.bloksec.io/sso/SingleSignOnService/{unique

SSO URL Protocol Binding
HTTP POST

Server certificate •

3. Under **Authorization Setting**s, choose the group to be used for the **Default Group Policy**.



ADD SECURITY PROVIDER

• *Required field*

Name • SAML2

☑ Enabled

User Provision

● Provision users using this provider

○ Provision users using a different provider

Collapse All

Identity Provider Settings

Service Provider Settings

User Attribute Settings

Authorization Settings

Group Lookup Attribute Name: Groups

Delimiter:

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

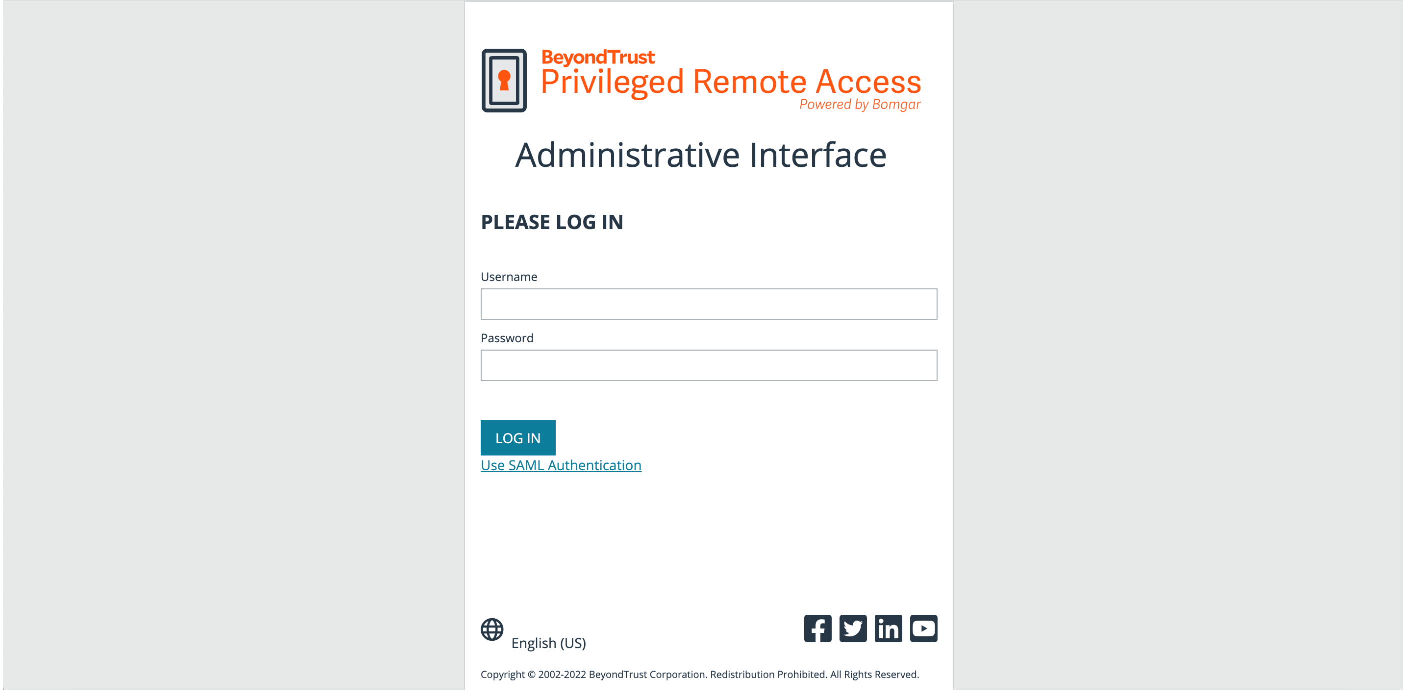
Available Groups:

Default Group Policy •: Admin

Test the Configuration

1. Go to the BlokSec administration console, and navigate to the newly created BeyondTrust Privileged Remote Access application.
2. Click the settings icon.
3. Select **Create Account**.

4. Go to the BeyondTrust instance's login page (for example, https://eval######.beyondtrustcloud.com/login/login) and click **Use SAML Authentication**.



BeyondTrust Privileged Remote Access *Powered by Bomgar*

Administrative Interface

PLEASE LOG IN

Username

Password

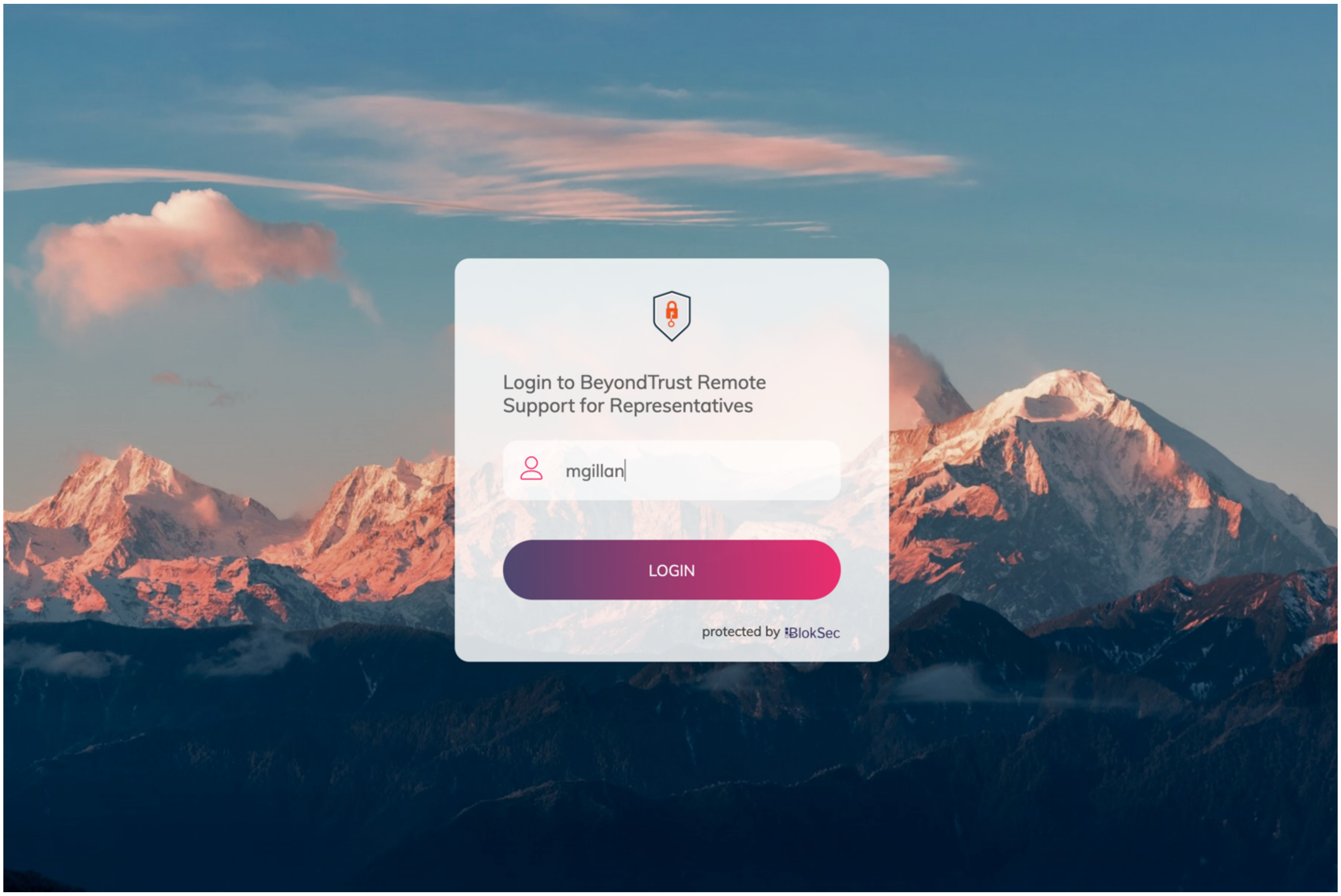
LOG IN

Use SAML Authentication

English (US)

Copyright © 2002-2022 BeyondTrust Corporation. Redistribution Prohibited. All Rights Reserved.

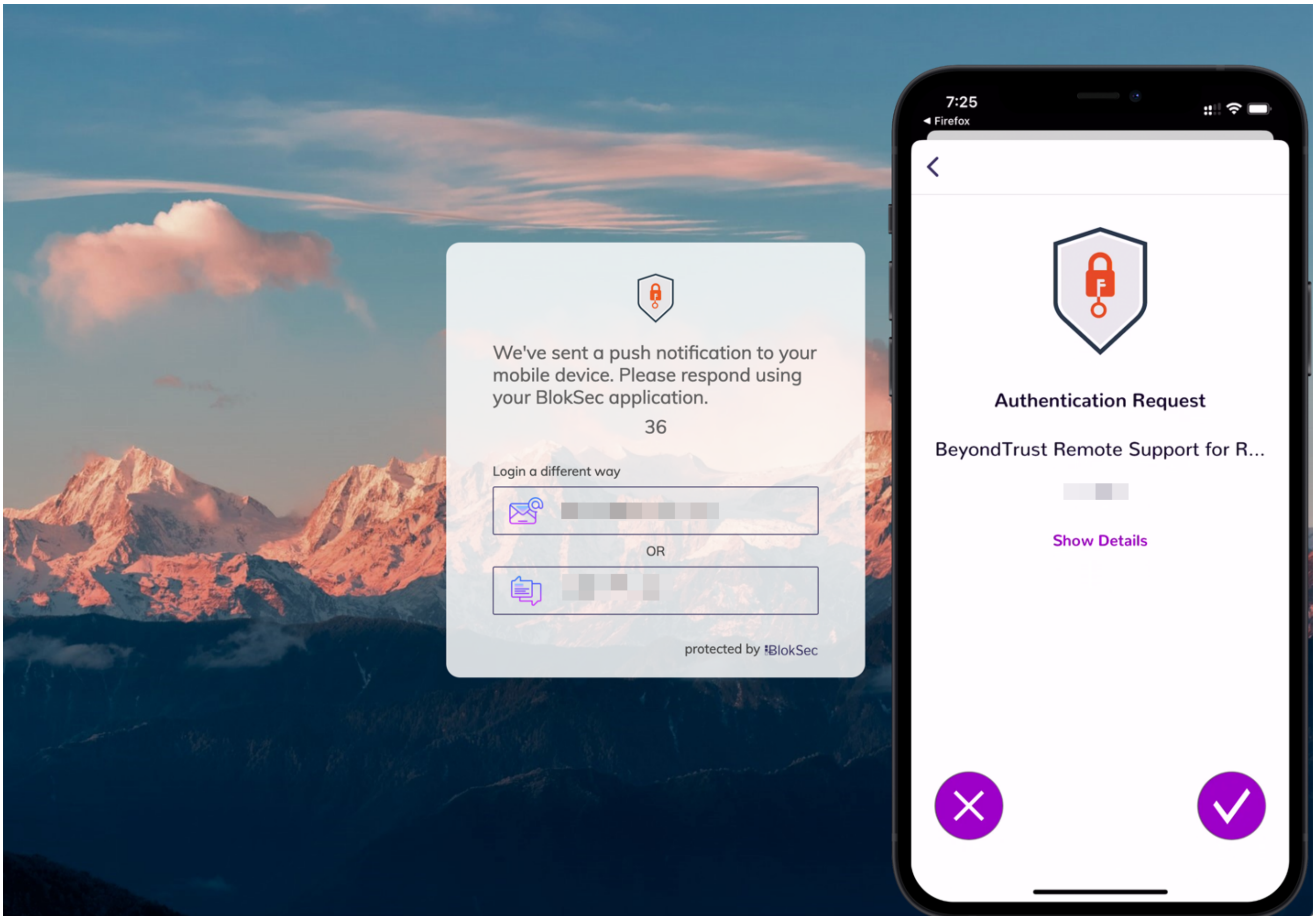
5. Enter the username created in the step above. This screen and the next may show Remote Support instead of Privileged Remote Access.



Login to BeyondTrust Remote Support for Representatives

mgillan

6. BlokSec sends a push notification to the user's mobile application to authenticate the representative.
7. The representative can review the request, and then approve it. The device performs a biometric authentication (e.g., fingerprint or facial recognition depending on the mobile device's capabilities), and then a digital signature is sent to the BlokSec service to verify the representative's authenticity.



We've sent a push notification to your mobile device. Please respond using your BlokSec application.

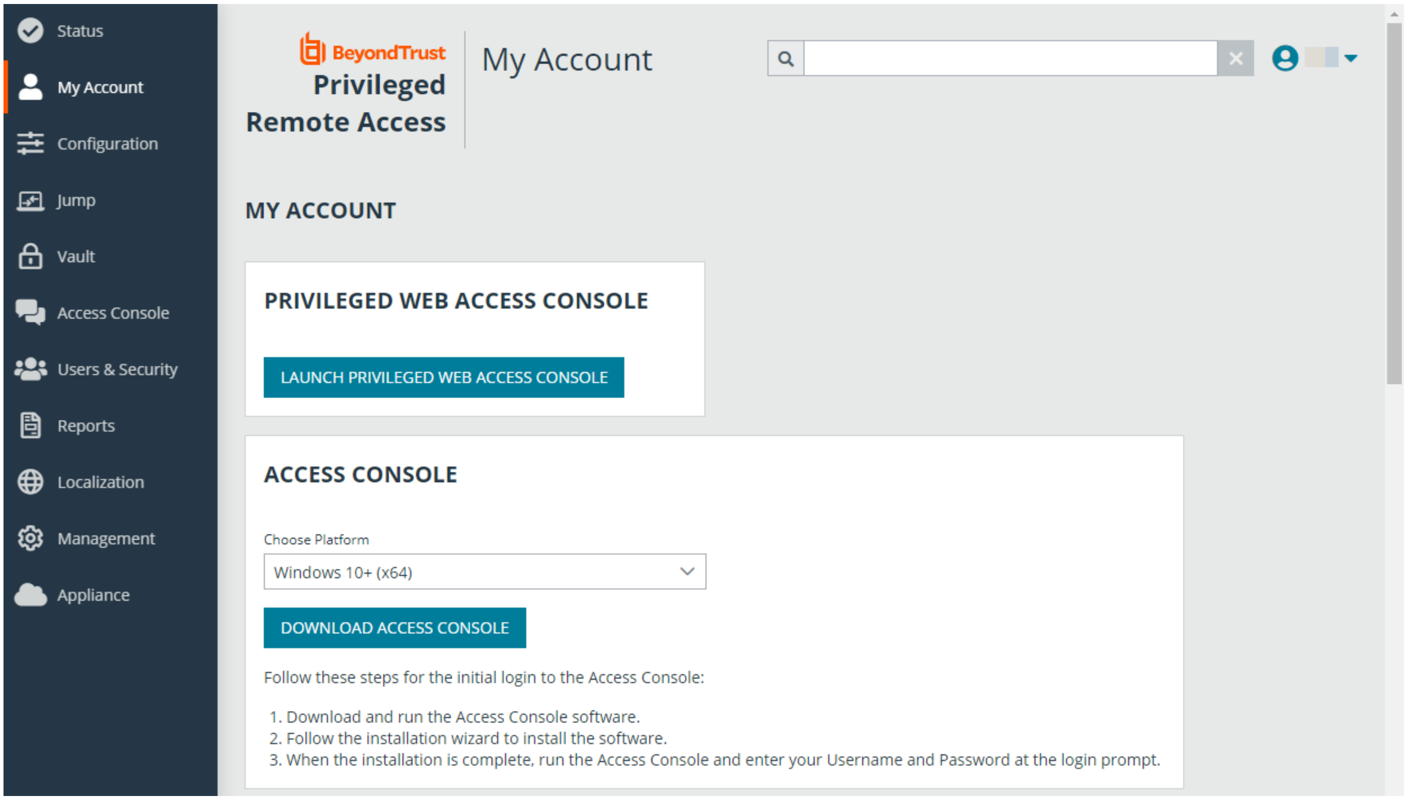
36

Authentication Request

BeyondTrust Remote Support for R...

[redacted]

8. The representative is securely logged into the BeyondTrust Privileged Remote Access console.



MY ACCOUNT

PRIVILEGED WEB ACCESS CONSOLE

ACCESS CONSOLE

Choose Platform: Windows 10+ (x64)

Follow these steps for the initial login to the Access Console:

1. Download and run the Access Console software.
2. Follow the installation wizard to install the software.
3. When the installation is complete, run the Access Console and enter your Username and Password at the login prompt.