Remote Support
BlokSec Integration

TC:3/4/2024

Table of Contents

BlokSec and BeyondTrust Remote Support for Representatives

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 Secure 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. Representatives and public portals are supported.

Remote Support for representatives provides the ability to configure a SAML authentication provider, which needs to be configured to point to BlokSec instance. Configuration is required in both products.

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

Prerequisites

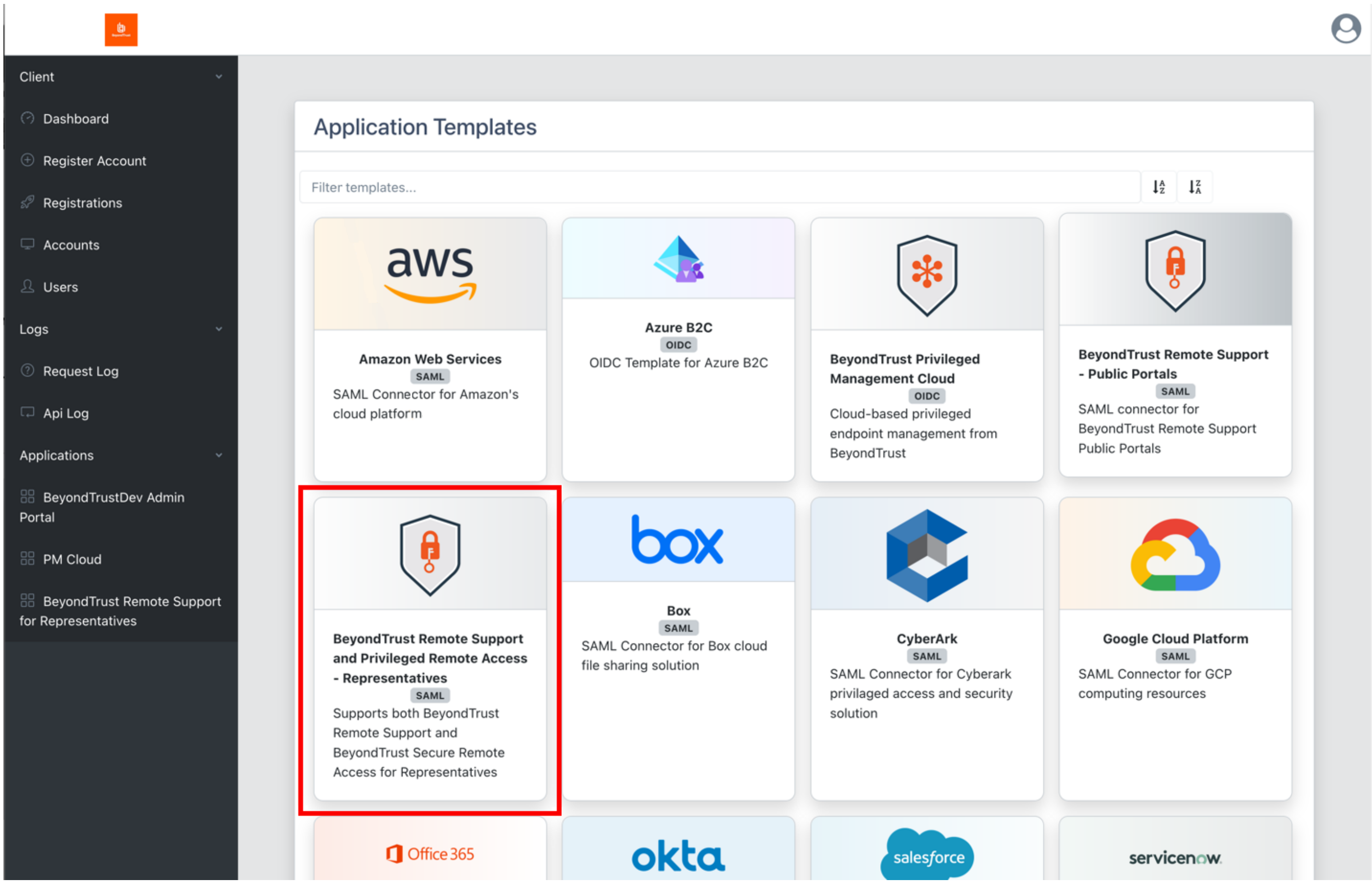
- Installed BeyondTrust Remote Support instance
- Installed BlokSec instance
- BlokSec test users with mobile app installed

Remote Support for Representatives

Create Remote Support for Representatives 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

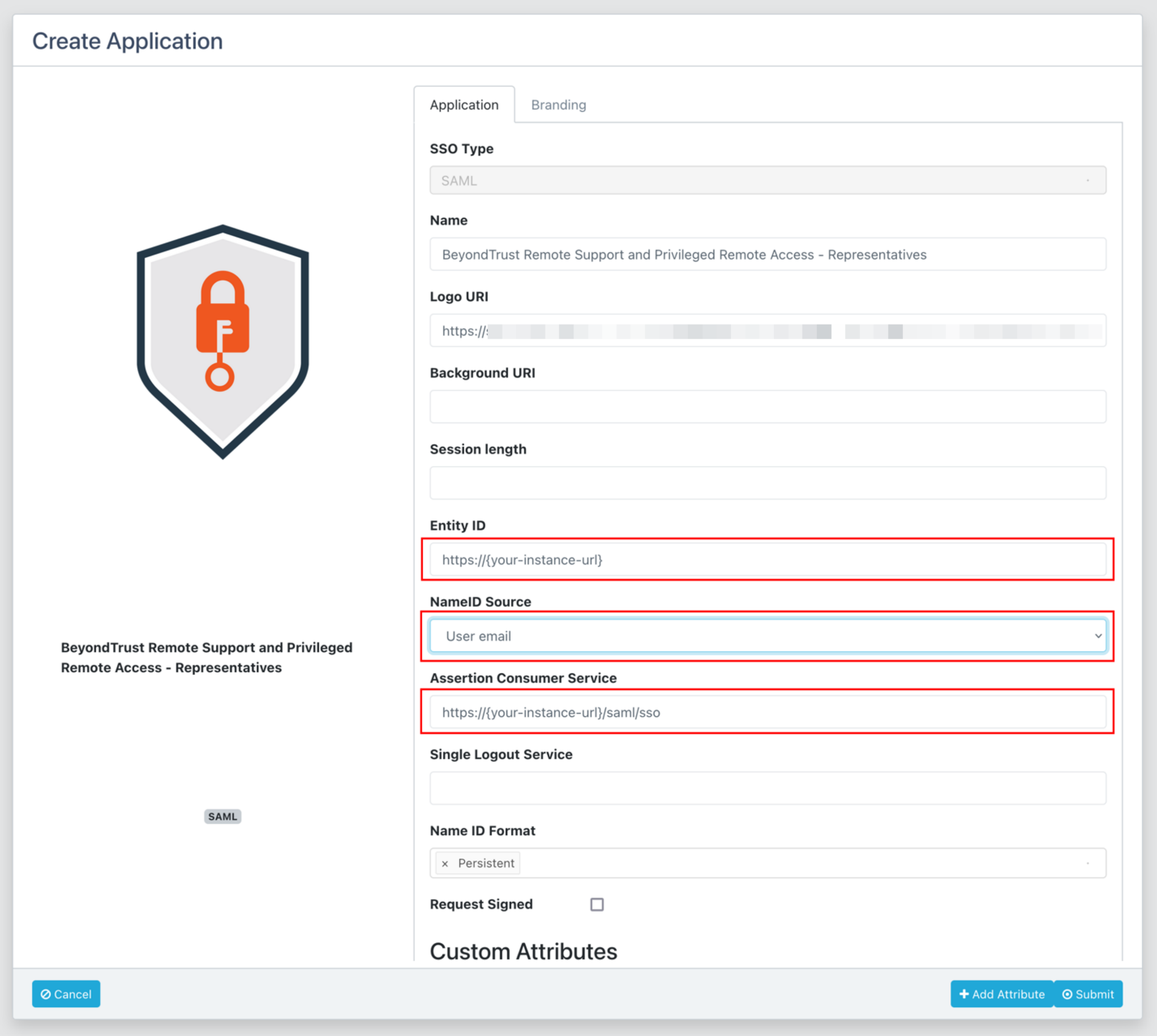
BeyondTrust Remote Support and Privileged Remote Access - Representatives
SAML
Supports both BeyondTrust Remote Support and BeyondTrust Secure Remote Access for Representatives

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

SAML

Application | Branding

SSO Type: SAML

Name: BeyondTrust Remote Support and Privileged Remote Access - Representatives

Logo URI: https://

Background URI:

Session length:

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

NameID Source: User email

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

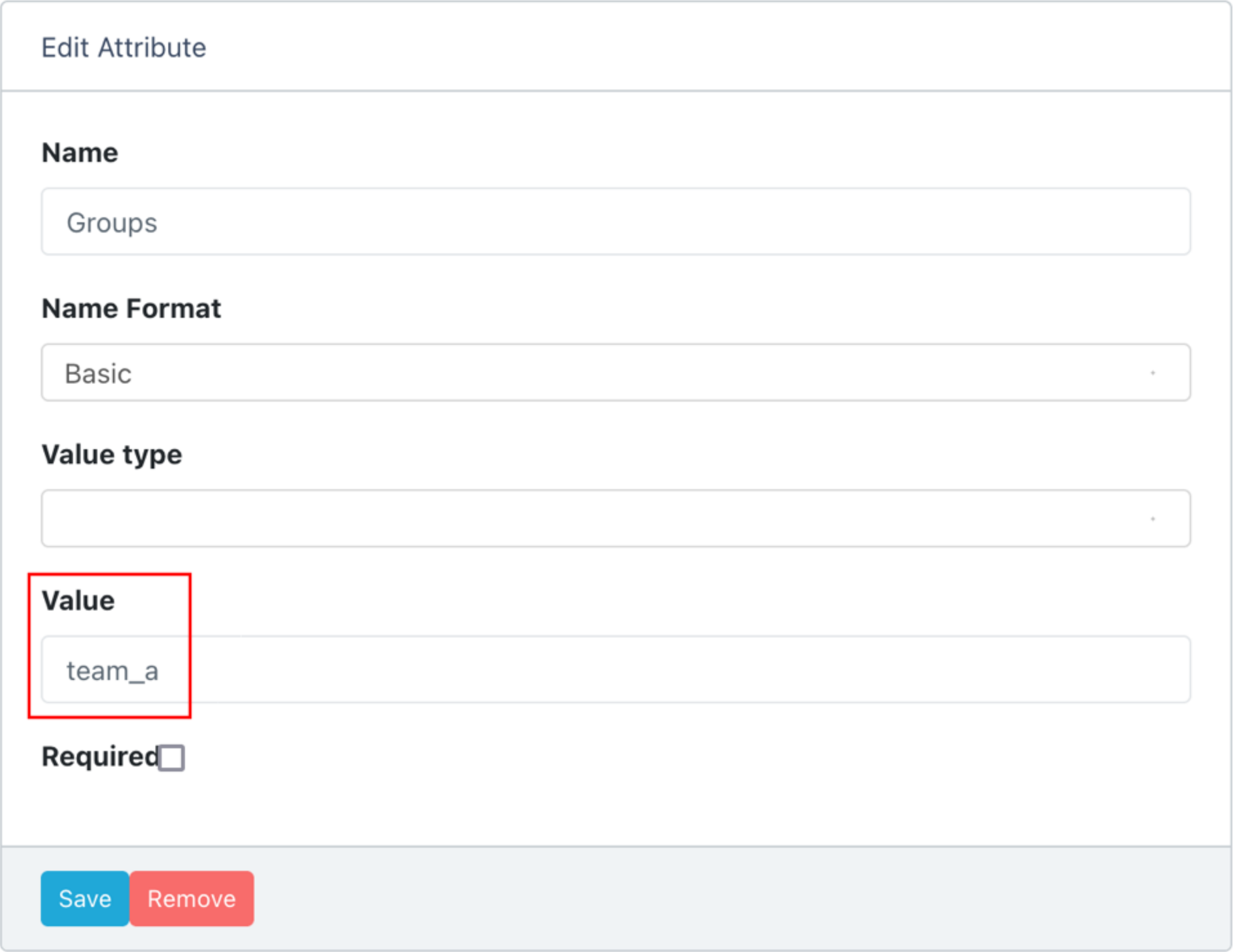
Single Logout Service:

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

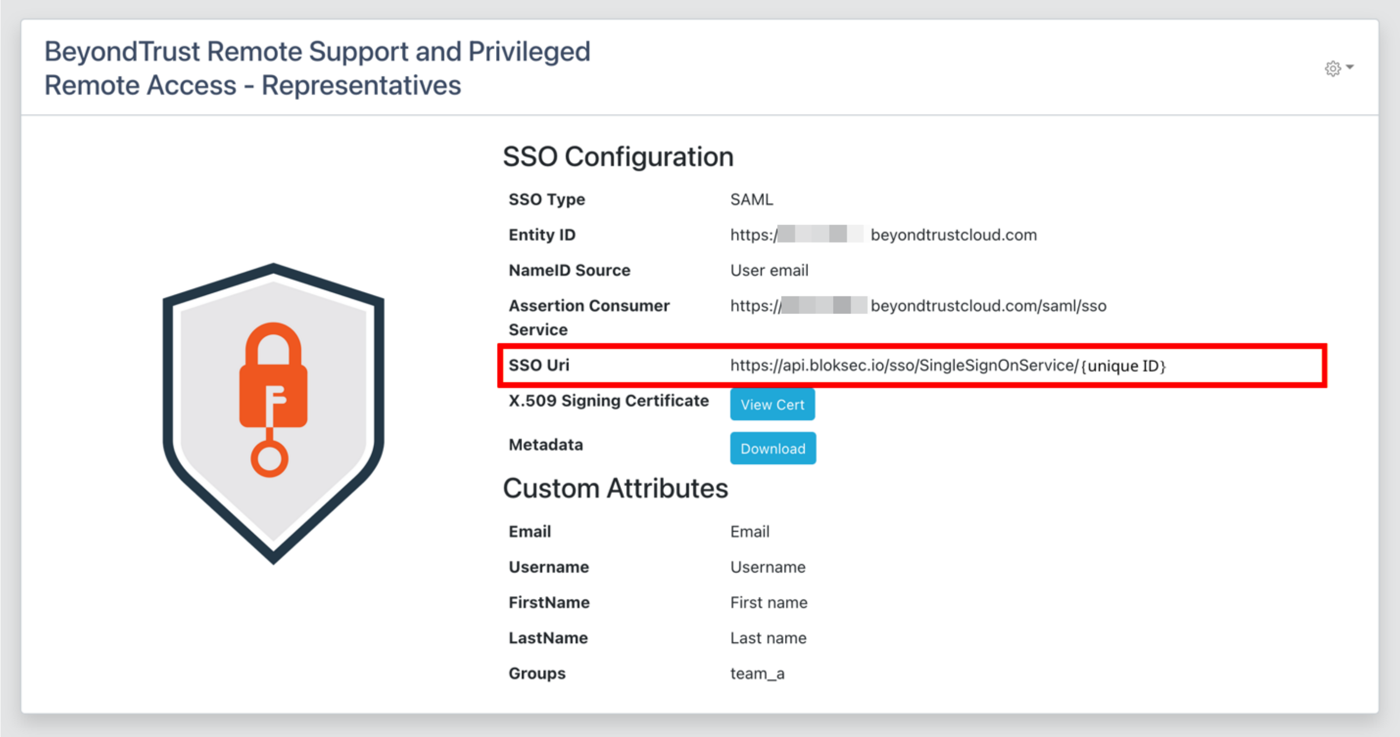
Name Format: Basic

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

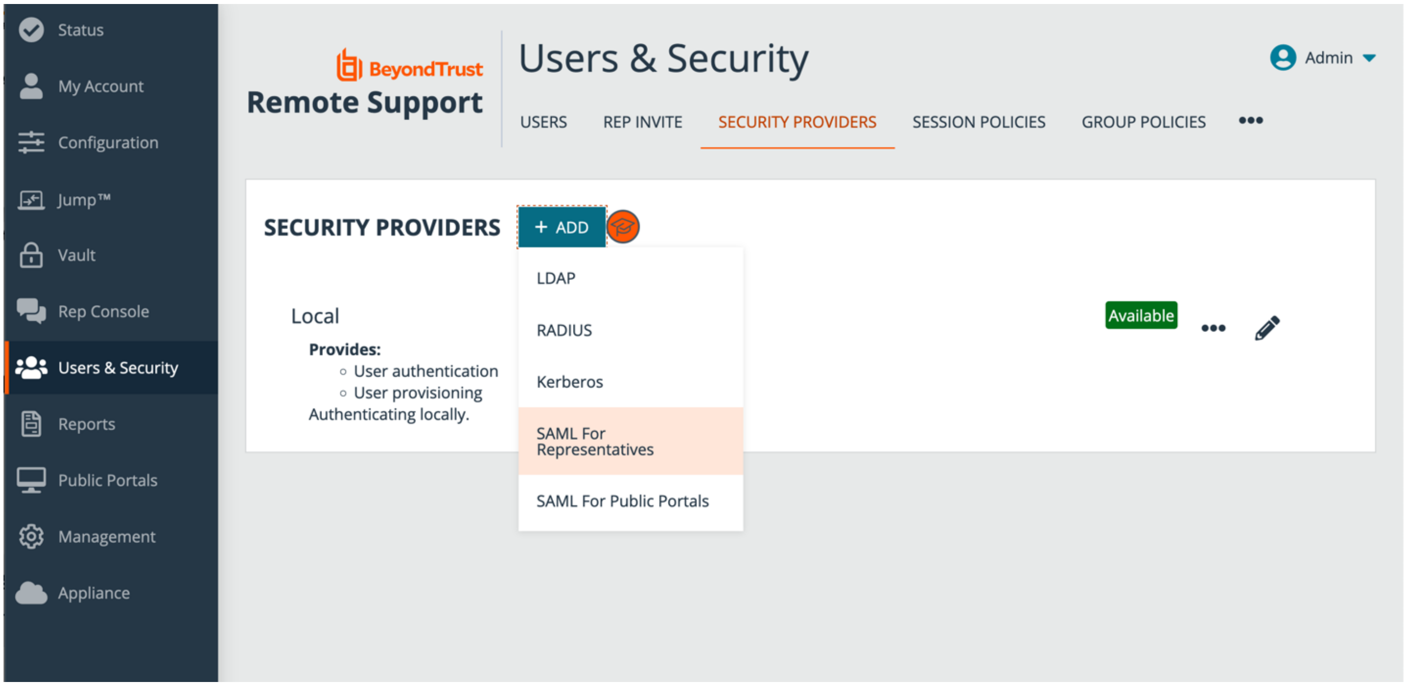
Custom Attributes

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

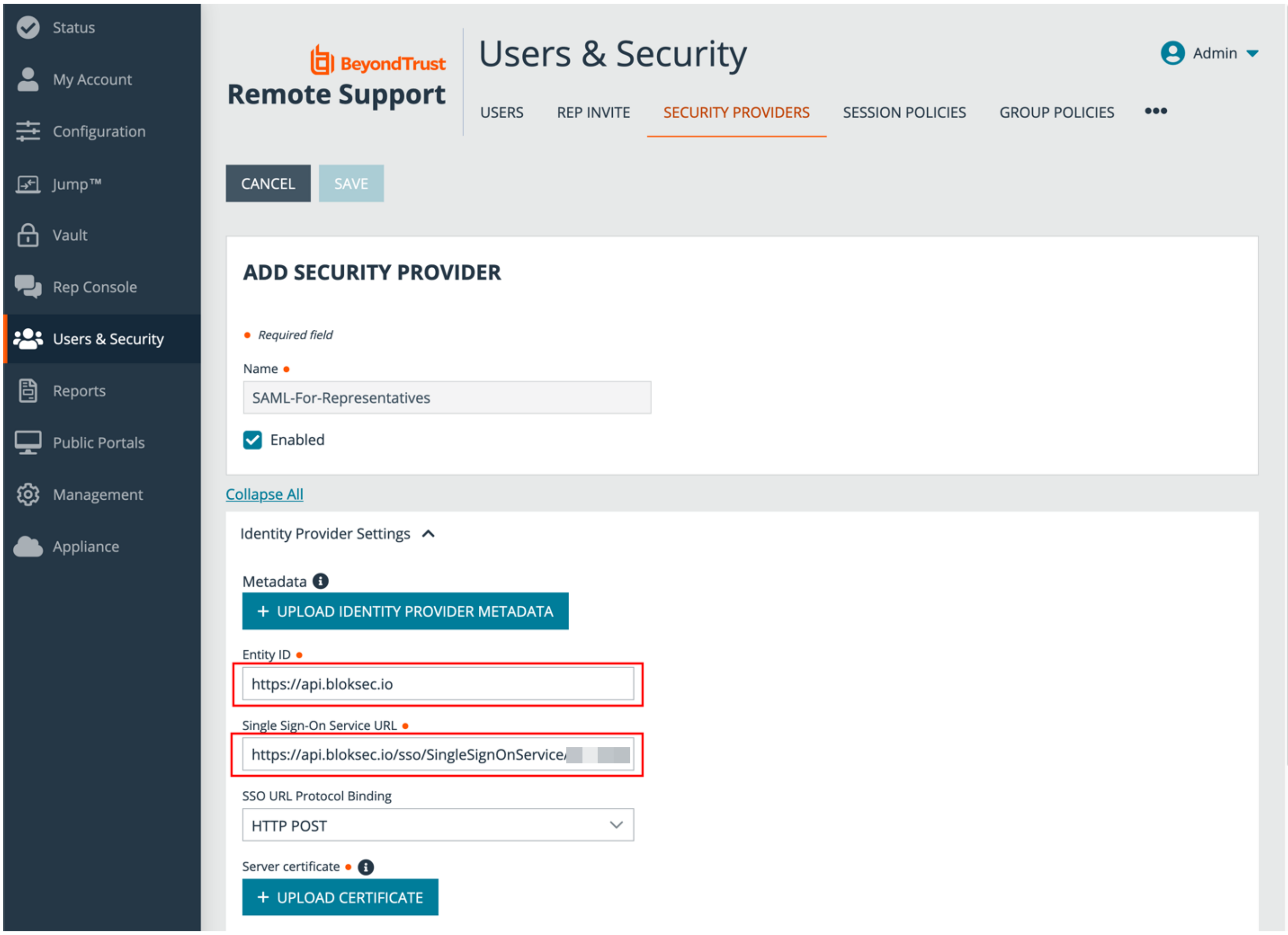
Configure the SAML for Representatives Identity Provider in BeyondTrust

Log in to BeyondTrust Remote Support. Continue with the steps below.

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



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 ●
SAML-For-Representatives

☑ Enabled

Collapse All

Identity Provider Settings

Metadata
+ UPLOAD IDENTITY PROVIDER METADATA

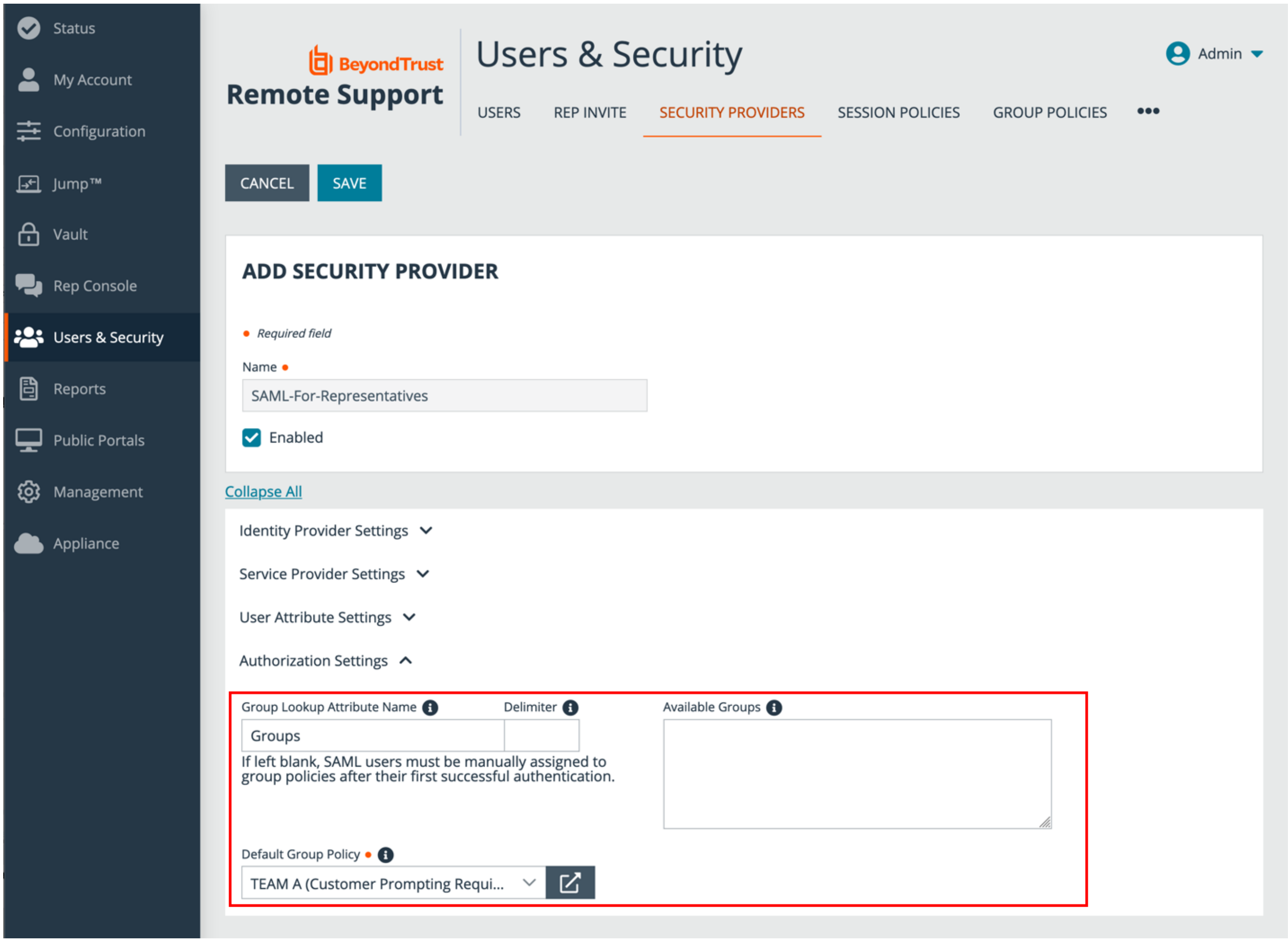
Entity ID ●
https://api.bloksec.io

Single Sign-On Service URL ●
https://api.bloksec.io/sso/SingleSignOnService/[redacted]

SSO URL Protocol Binding
HTTP POST

Server certificate ●
+ UPLOAD CERTIFICATE

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



ADD SECURITY PROVIDER

● *Required field*

Name ●
SAML-For-Representatives

☑ Enabled

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.

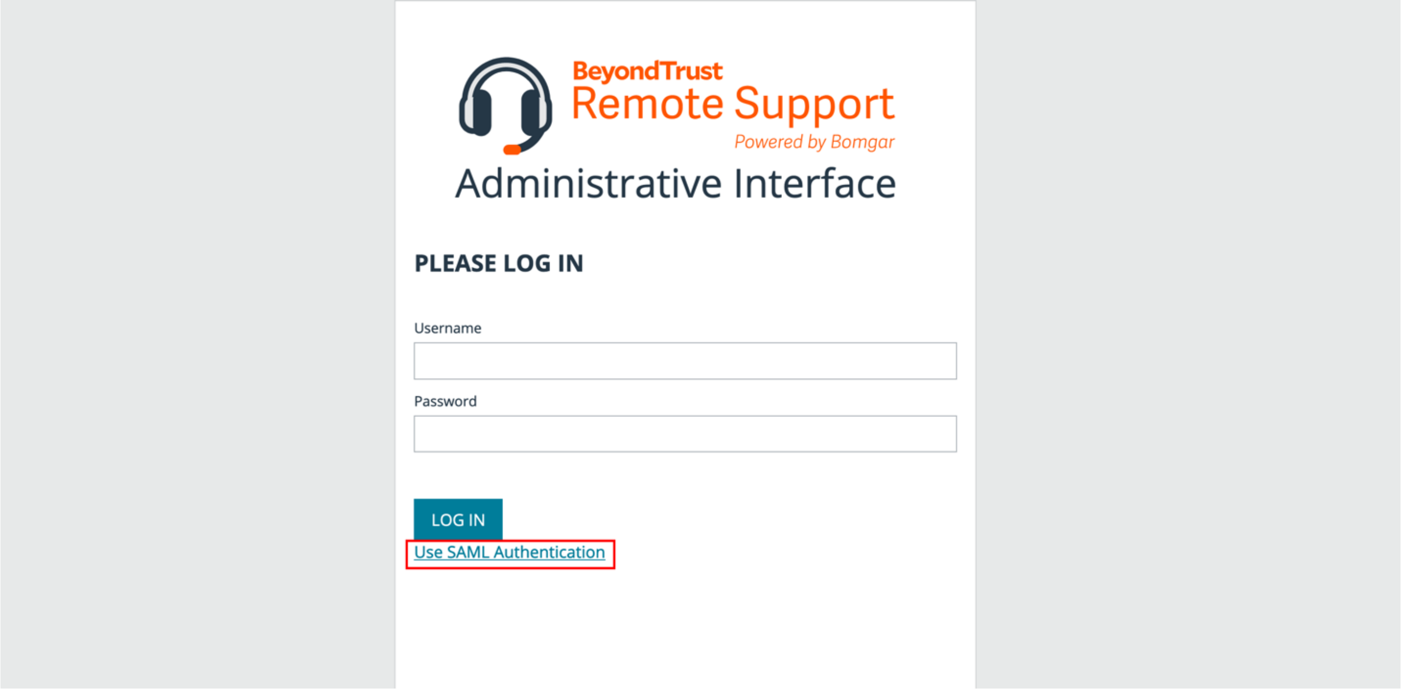
Available Groups:

Default Group Policy ●: TEAM A (Customer Prompting Requi...

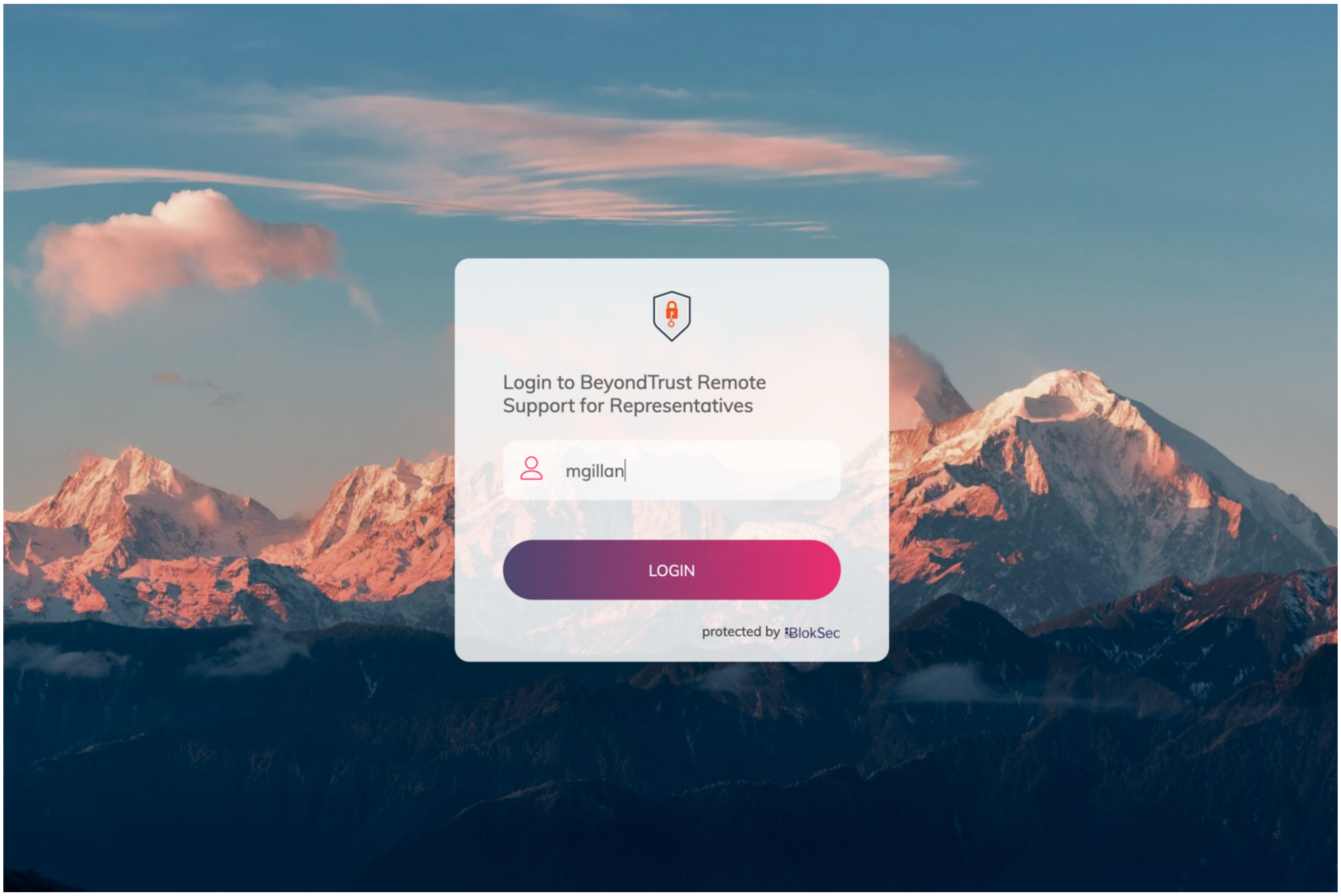
Test the Configuration

1. Go to the BlokSec administration console, and navigate to the newly created **BeyondTrust Remote Support for Representatives 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**.



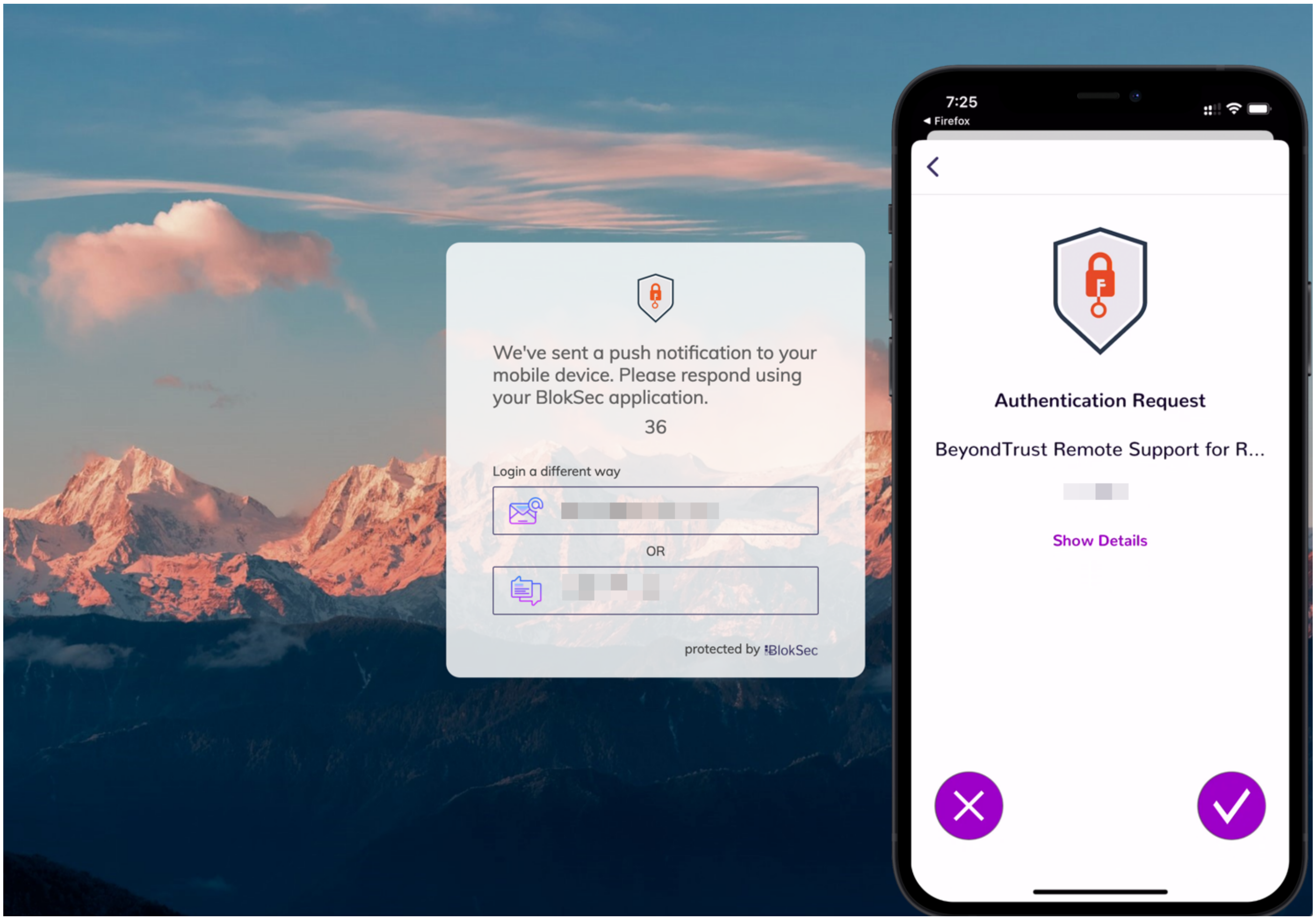
5. Enter the username created in the step above.



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

Login a different way

[redacted]

OR

[redacted]

protected by BlokSec

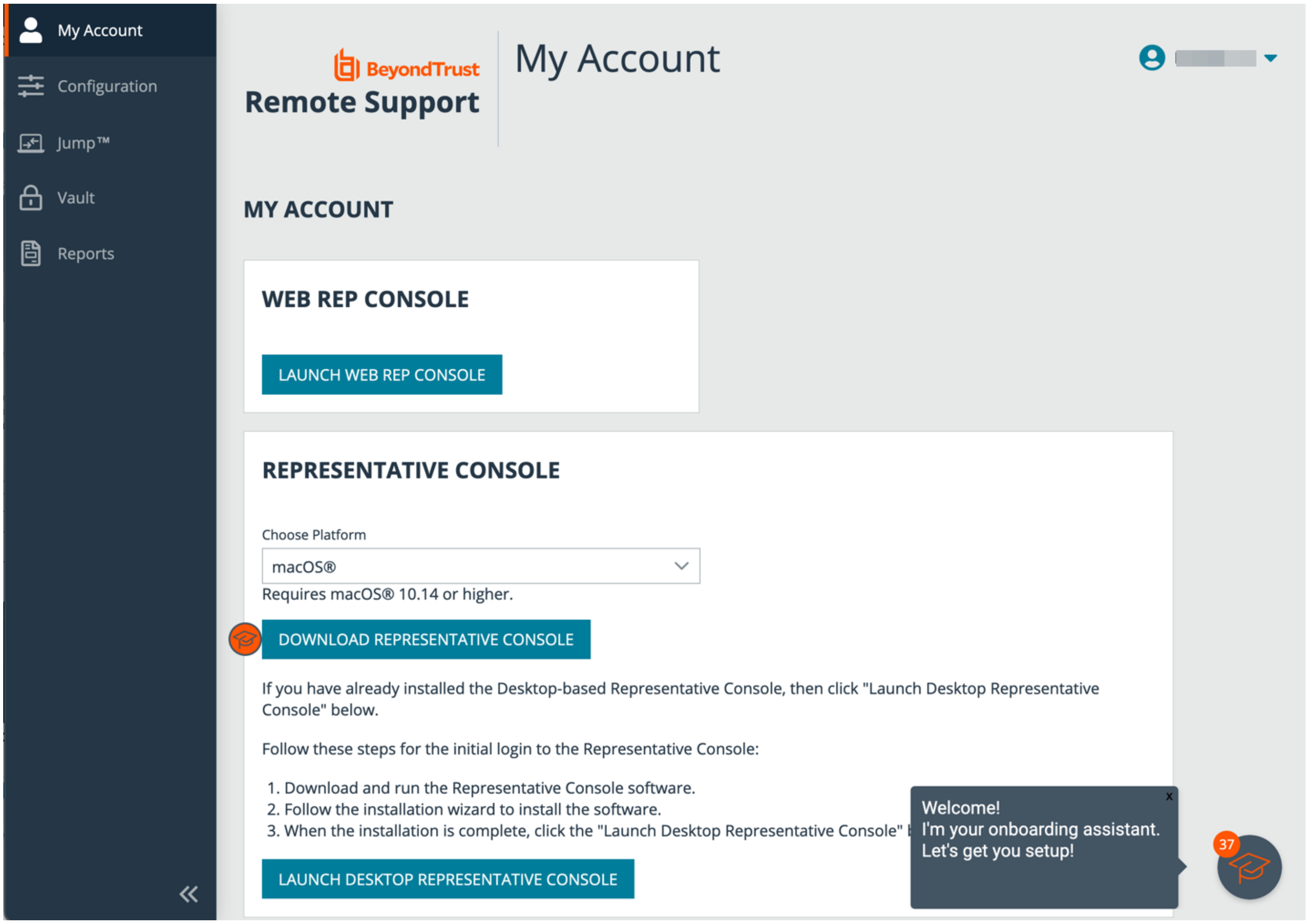
Authentication Request

BeyondTrust Remote Support for R...

[redacted]

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs 13
©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority. TC: 3/4/2024

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



MY ACCOUNT

WEB REP CONSOLE

REPRESENTATIVE CONSOLE

Choose Platform: macOS®

Requires macOS® 10.14 or higher.

If you have already installed the Desktop-based Representative Console, then click "Launch Desktop Representative Console" below.

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

1. Download and run the Representative Console software.
2. Follow the installation wizard to install the software.
3. When the installation is complete, click the "Launch Desktop Representative Console" b

Welcome!
I'm your onboarding assistant.
Let's get you setup!

BlokSec and BeyondTrust Remote Support for Public Portal

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 Secure 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. Representatives and public portals are supported.

Remote Support for representatives provides the ability to configure a SAML authentication provider, which needs to be configured to point to BlokSec instance. Configuration is required in both products.

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

Prerequisites

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

Remote Support for Public Portal

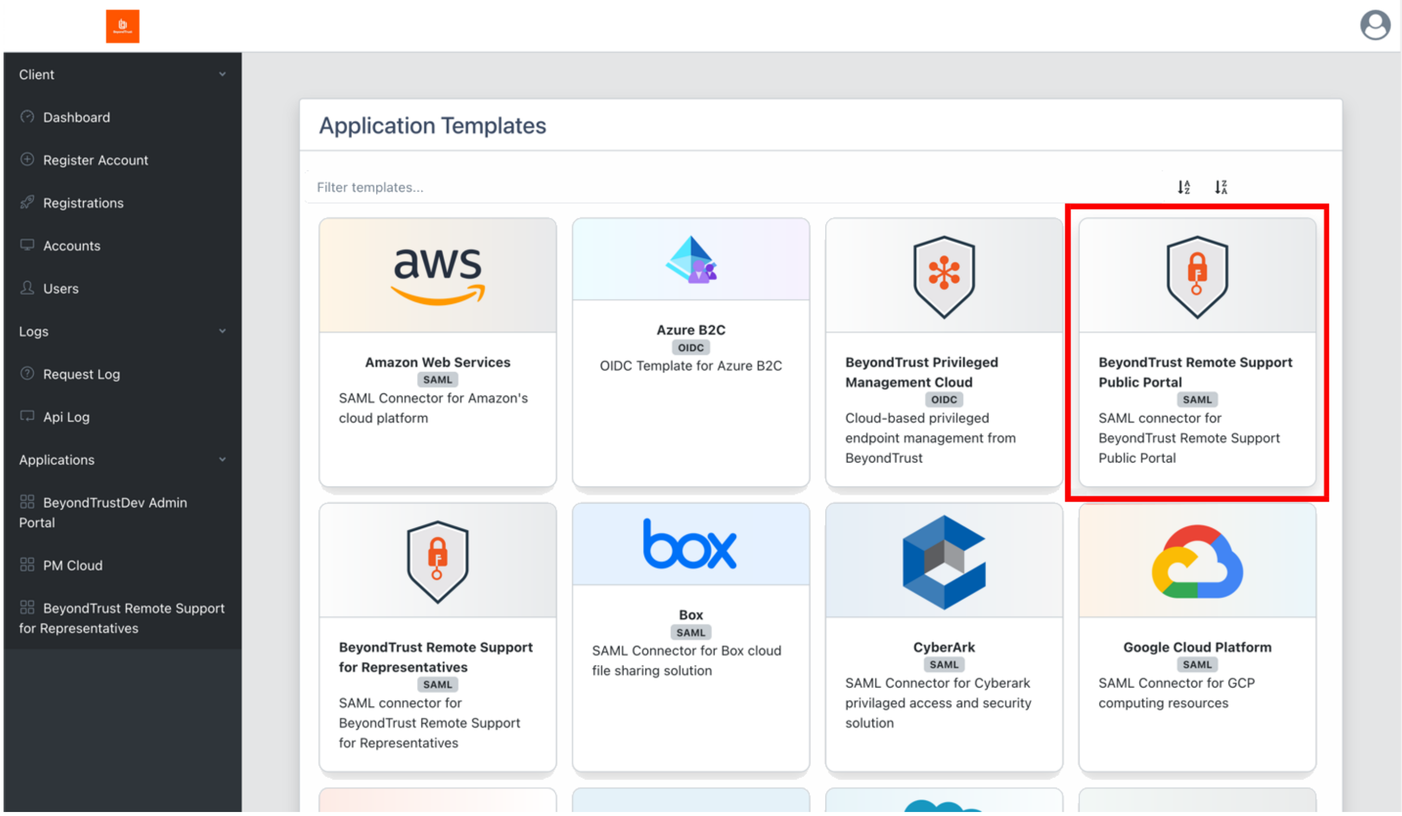
Create Remote Support for Public Portal Application in the BlokSec Administration Console

Remote Support for the public portal provides the ability to configure a SAML authentication provider, which needs to be configured to point to the BlokSec instance.

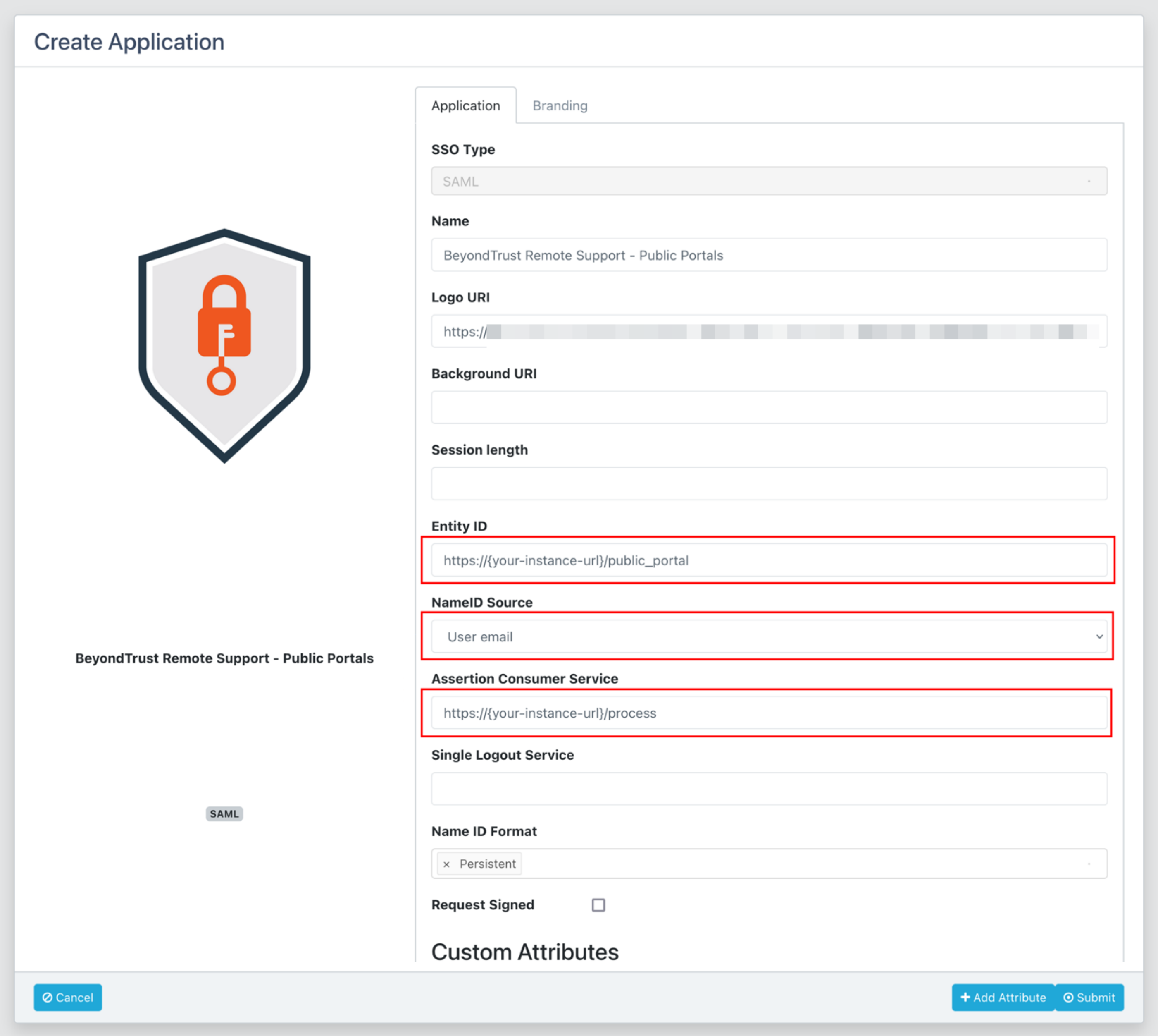
Log in to Bloksec and follow the steps below.

1. From the dashboard, click **+ Add Application**.
2. Select **Create from Template**.

3. Select the **BeyondTrust Remote Support Public Portal** template.


Client
Dashboard
Register Account
Registrations
Accounts
Users
Logs
Request Log
Api Log
Applications
BeyondTrustDev Admin Portal
PM Cloud
BeyondTrust Remote Support for Representatives
Application Templates
Filter templates...
aws
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 Portal
SAML
SAML connector for BeyondTrust Remote Support Public Portal
BeyondTrust Remote Support for Representatives
SAML
SAML connector for BeyondTrust Remote Support for Representatives
box
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

SSO Type: SAML

Name: BeyondTrust Remote Support - Public Portals

Logo URI: https://

Background URI:

Session length:

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

NameID Source: User email

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

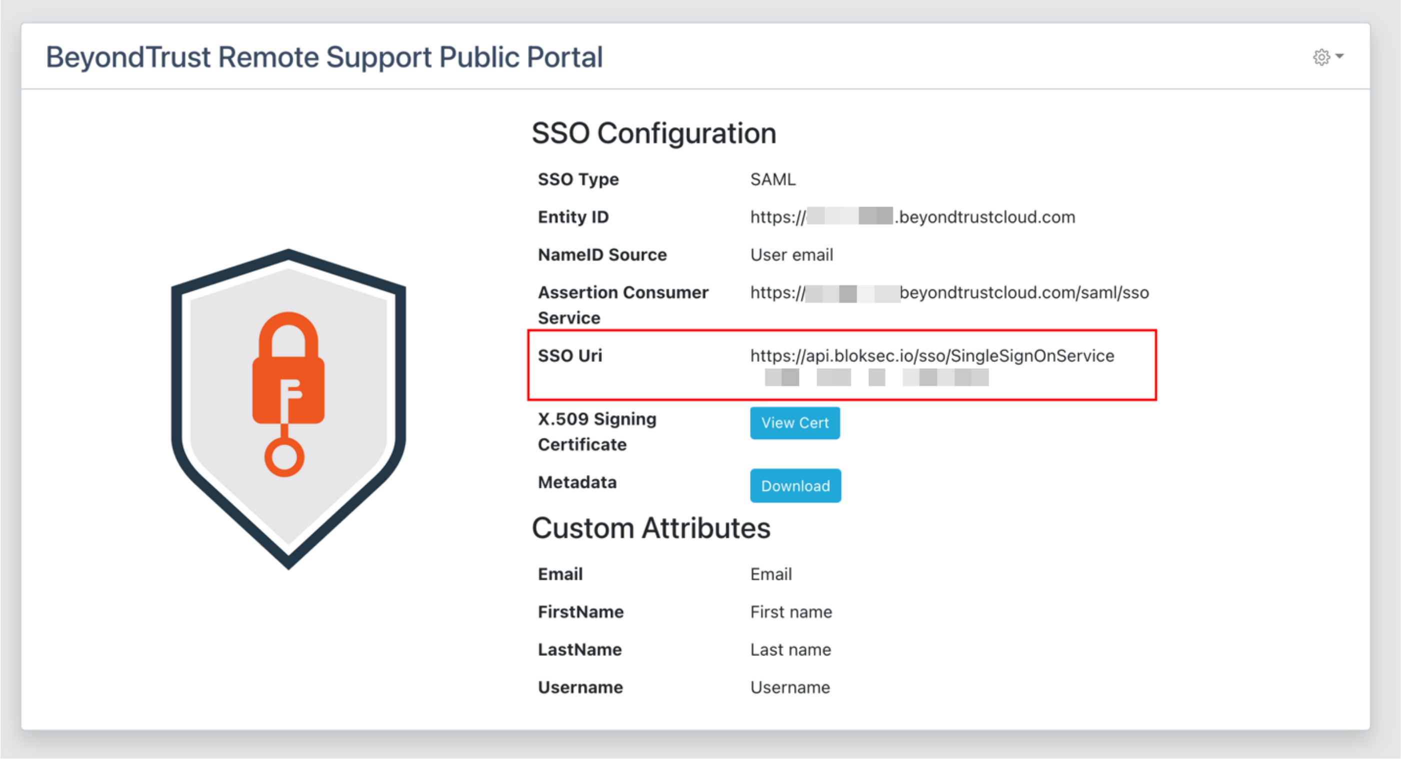
Single Logout Service:

Name ID Format: × Persistent

Request Signed □

Custom Attributes

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



BeyondTrust Remote Support Public Portal

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 [redacted]
X.509 Signing Certificate	View Cert
Metadata	Download

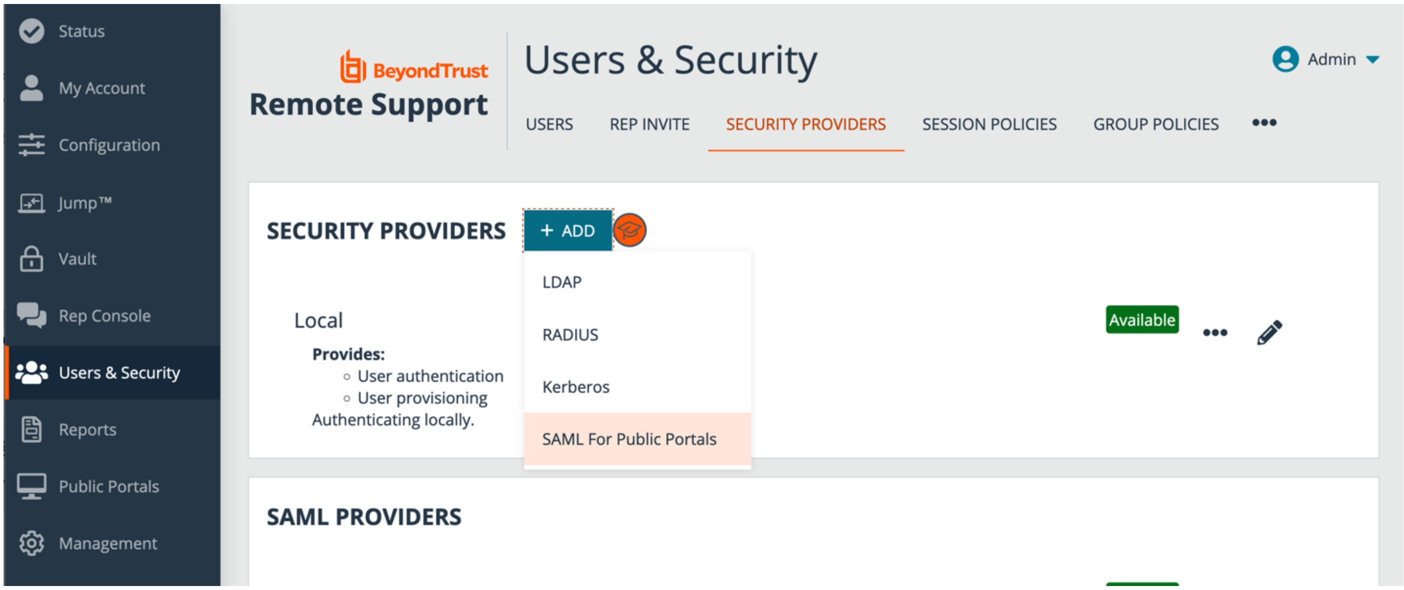
Custom Attributes

Email	Email
FirstName	First name
LastName	Last name
Username	Username

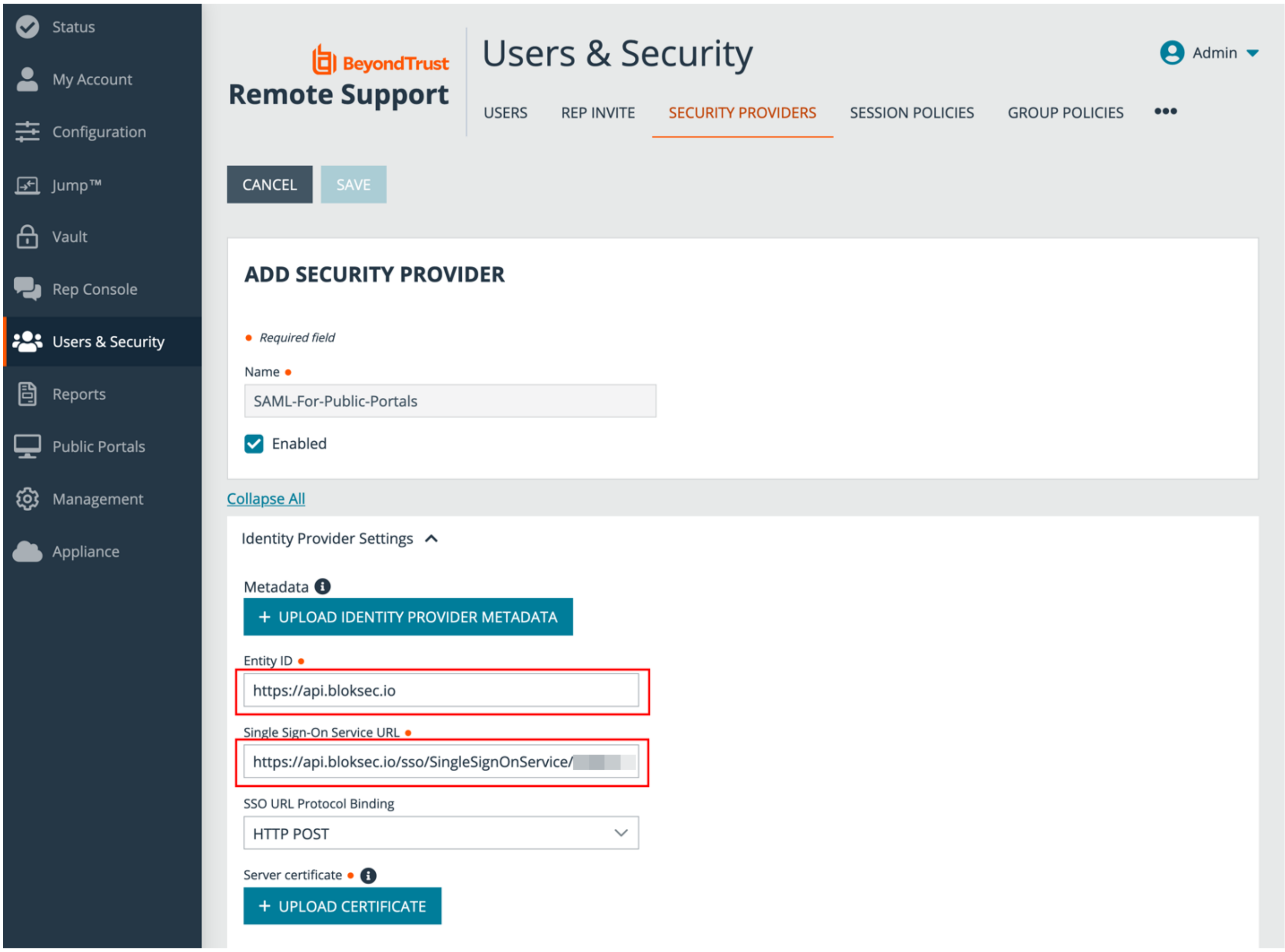
Configure the SAML for Public Portals Identity Provider in BeyondTrust

Log in to BeyondTrust Remote Support. Continue with the steps below.

1. Click the **Users & Security > Security Providers** tab, click **+ Add**, and select **SAML for Public Portals**.



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.



Users & Security

ADD SECURITY PROVIDER

• Required field

Name •
SAML-For-Public-Portals

☑ Enabled

Identity Provider Settings

Metadata

Entity ID •
https://api.bloksec.io

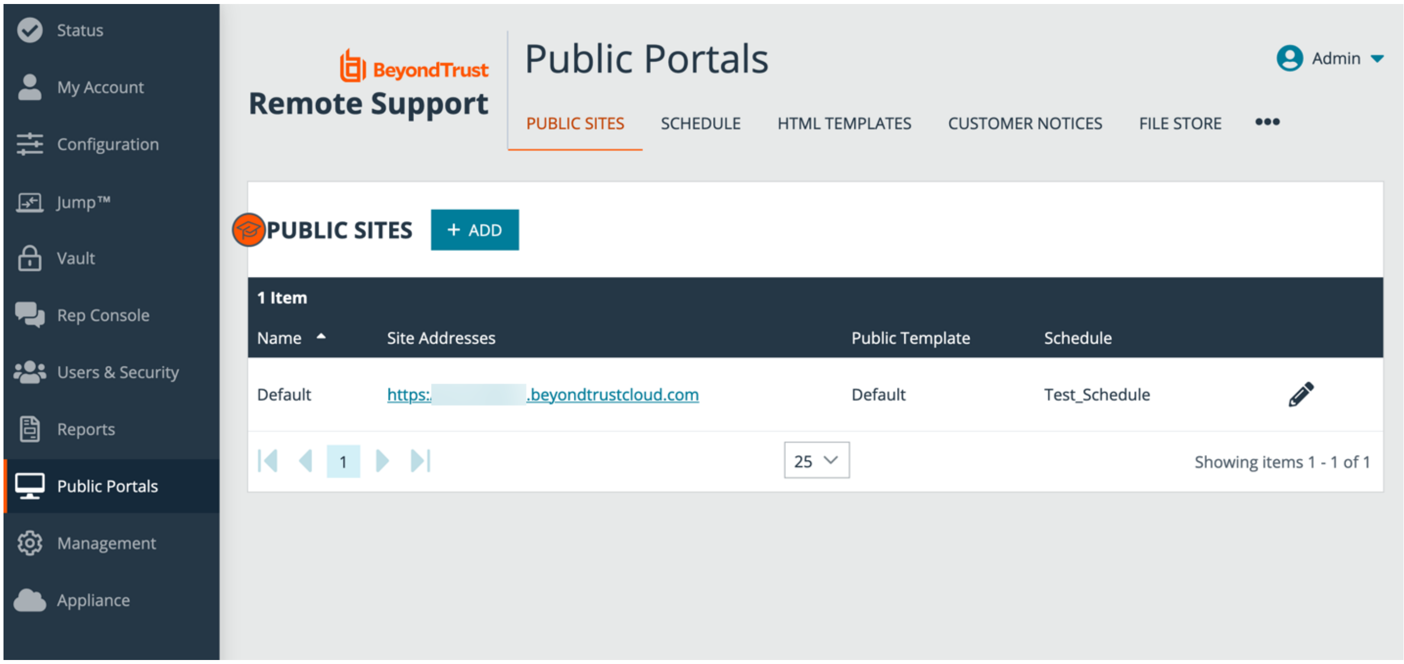
Single Sign-On Service URL •
https://api.bloksec.io/sso/SingleSignOnService/[redacted]

SSO URL Protocol Binding
HTTP POST

Server certificate •

Configure the Public Portal to Require SAML Authentication

1. On the **Public Portals > Public Sites** tab, edit the public site for the portal to be authenticated with BlokSec.



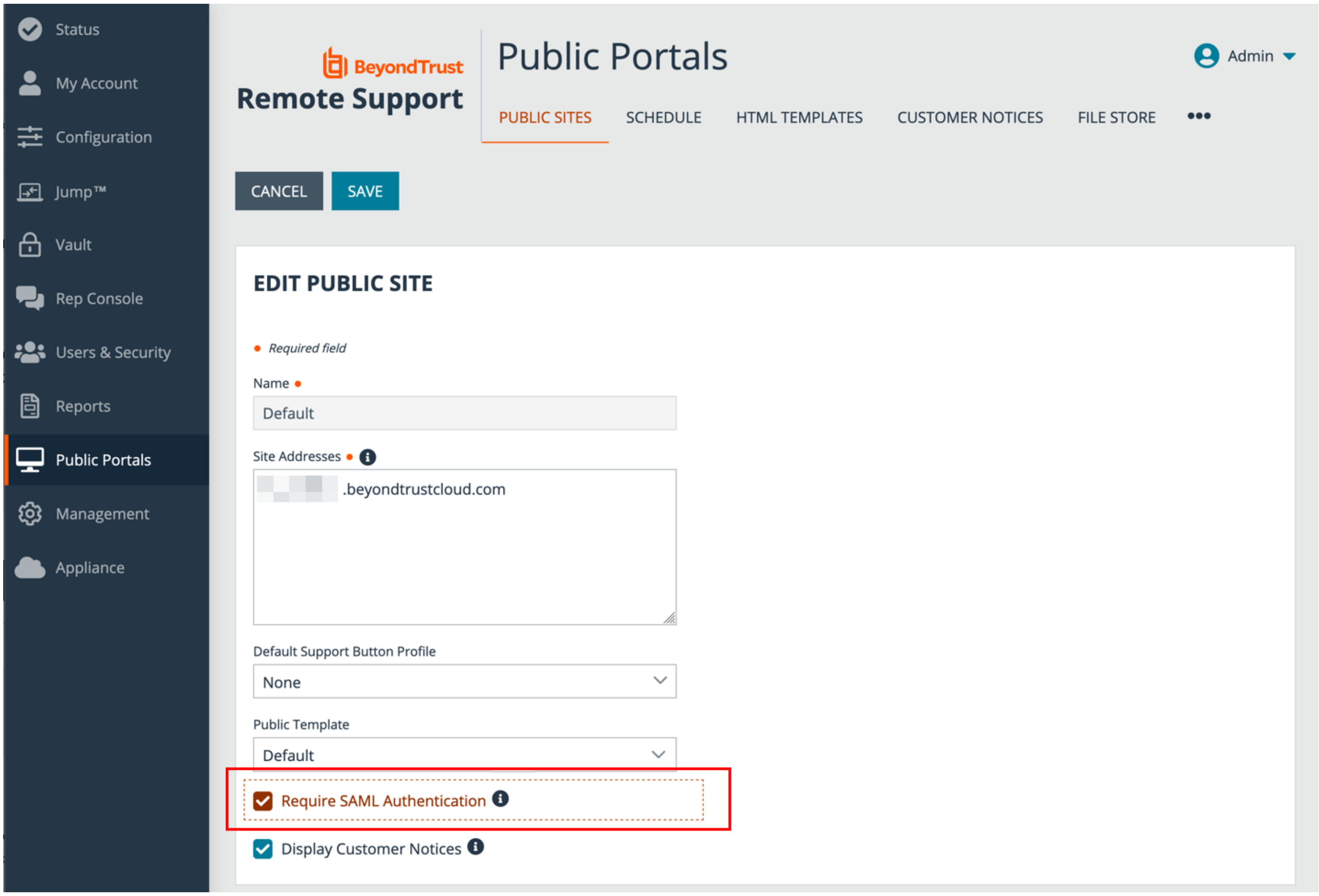
1 Item

Name	Site Addresses	Public Template	Schedule
Default	https:[redacted].beyondtrustcloud.com	Default	Test_Schedule

25

Showing items 1 - 1 of 1

2. Check the **Require SAML Authentication** box.
3. Click **Save**.



EDIT PUBLIC SITE

● *Required field*

Name ●
Default

Site Addresses ●
.beyondtrustcloud.com

Default Support Button Profile
None

Public Template
Default

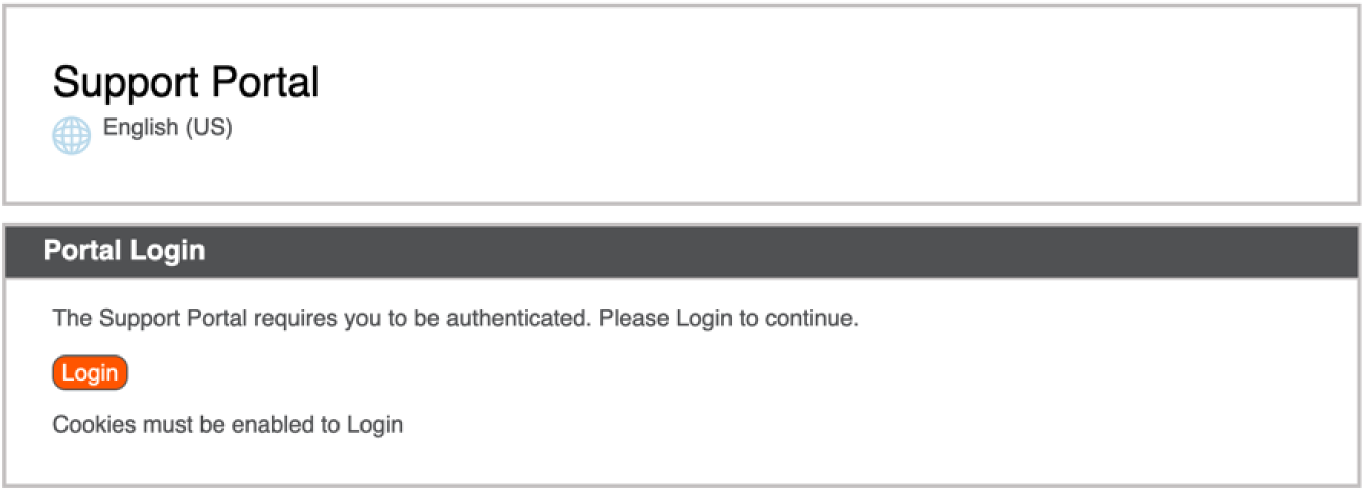
☑ Require SAML Authentication

☑ Display Customer Notices

Test the Configuration

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

4. Go to your BeyondTrust instance's public site (for example, https://eval######.beyondtrustcloud.com) and click the **Login** button.



Support Portal

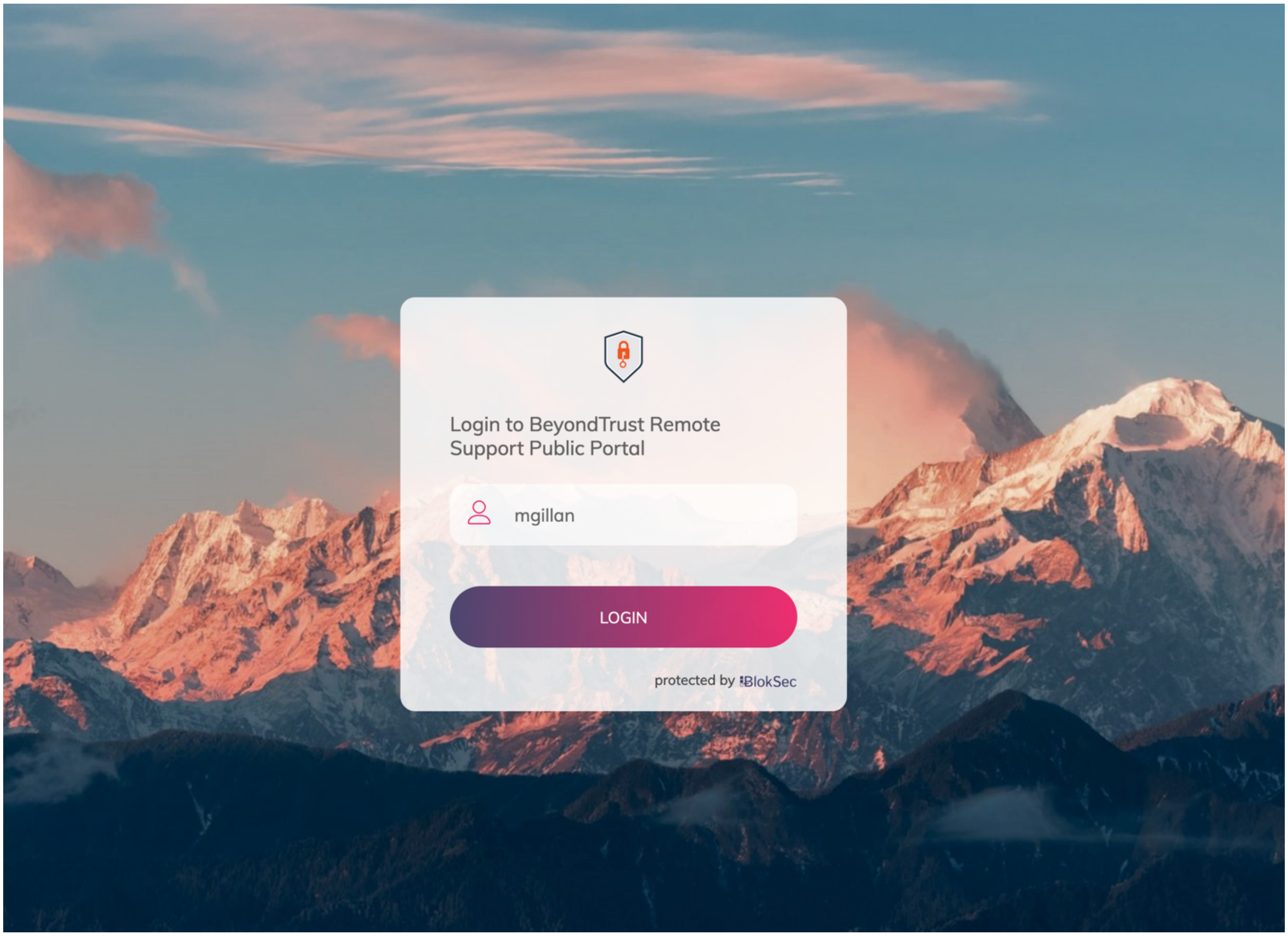
English (US)

Portal Login

The Support Portal requires you to be authenticated. Please Login to continue.

Cookies must be enabled to Login

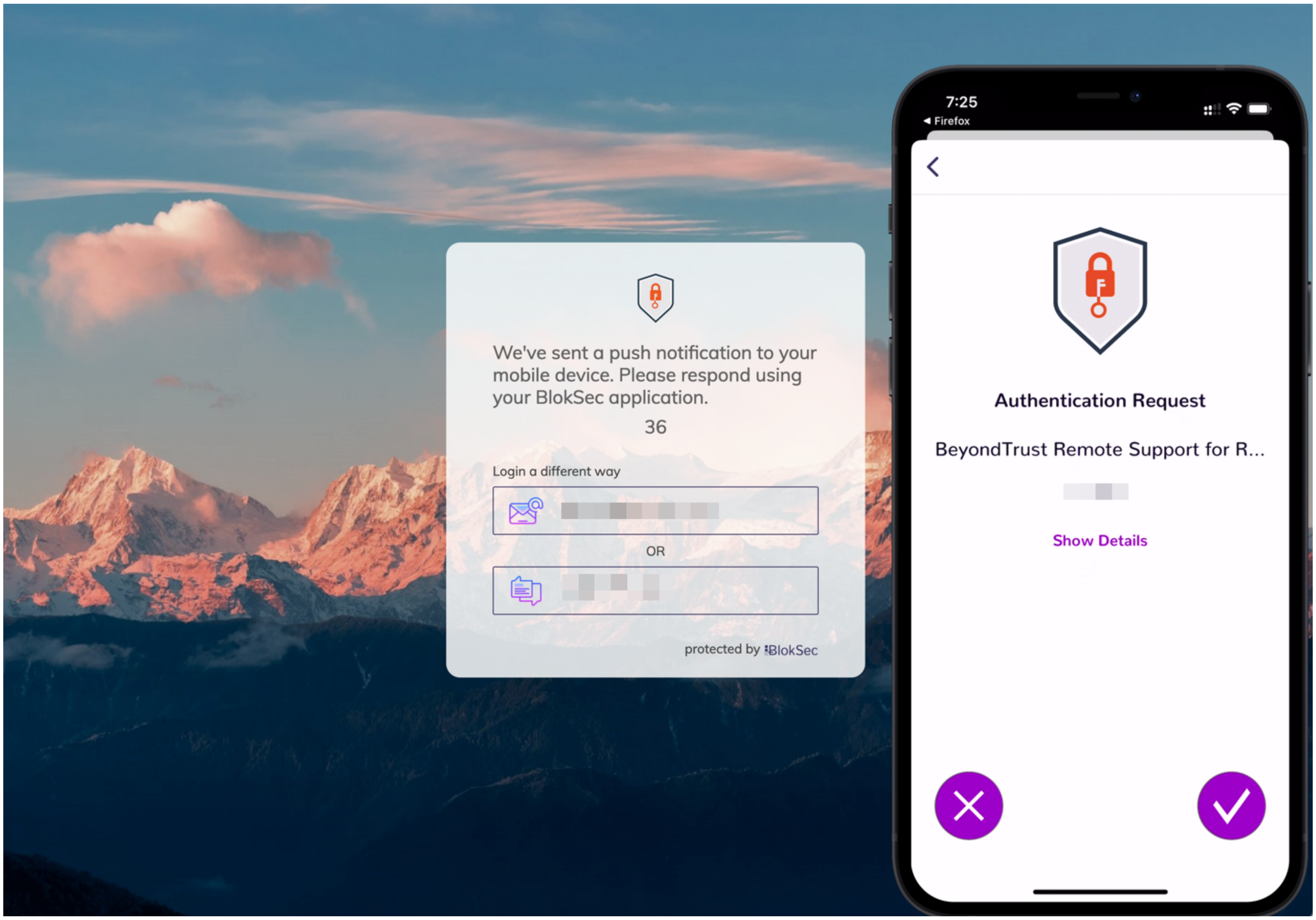
5. Enter the username created in the step above.



Login to BeyondTrust Remote Support Public Portal

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), 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

Login a different way

[redacted]

OR

[redacted]

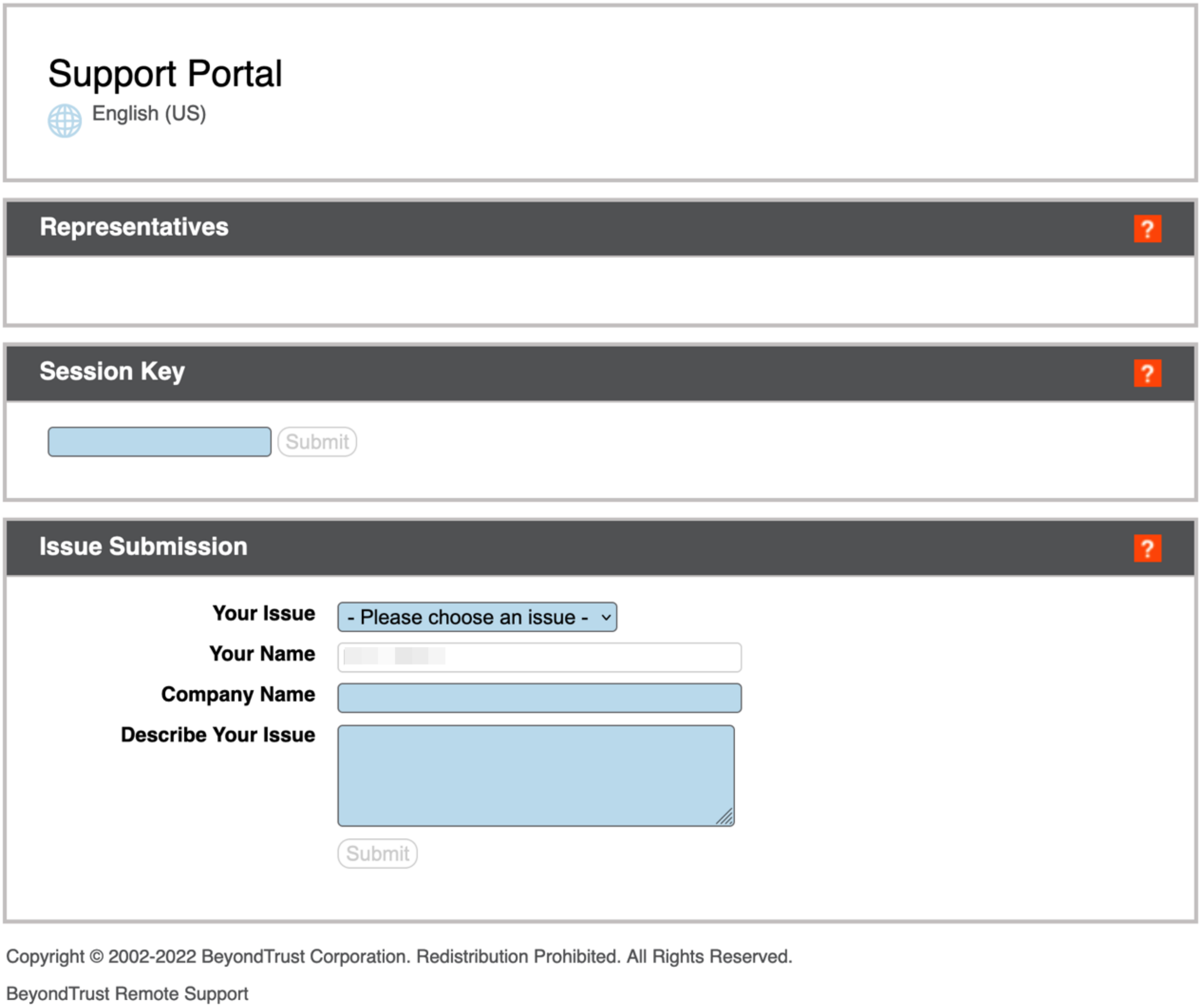
protected by BlokSec

Authentication Request

BeyondTrust Remote Support for R...

[redacted]

8. The representative is securely logged into the BeyondTrust Remote Support portal.



Support Portal

English (US)

Representatives

Session Key

Submit

Issue Submission

Your Issue: - Please choose an issue -

Your Name

Company Name

Describe Your Issue

Submit

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

BeyondTrust Remote Support