Remote Support
Beyond Identity SAML Integration Guide

TC:3/4/2024

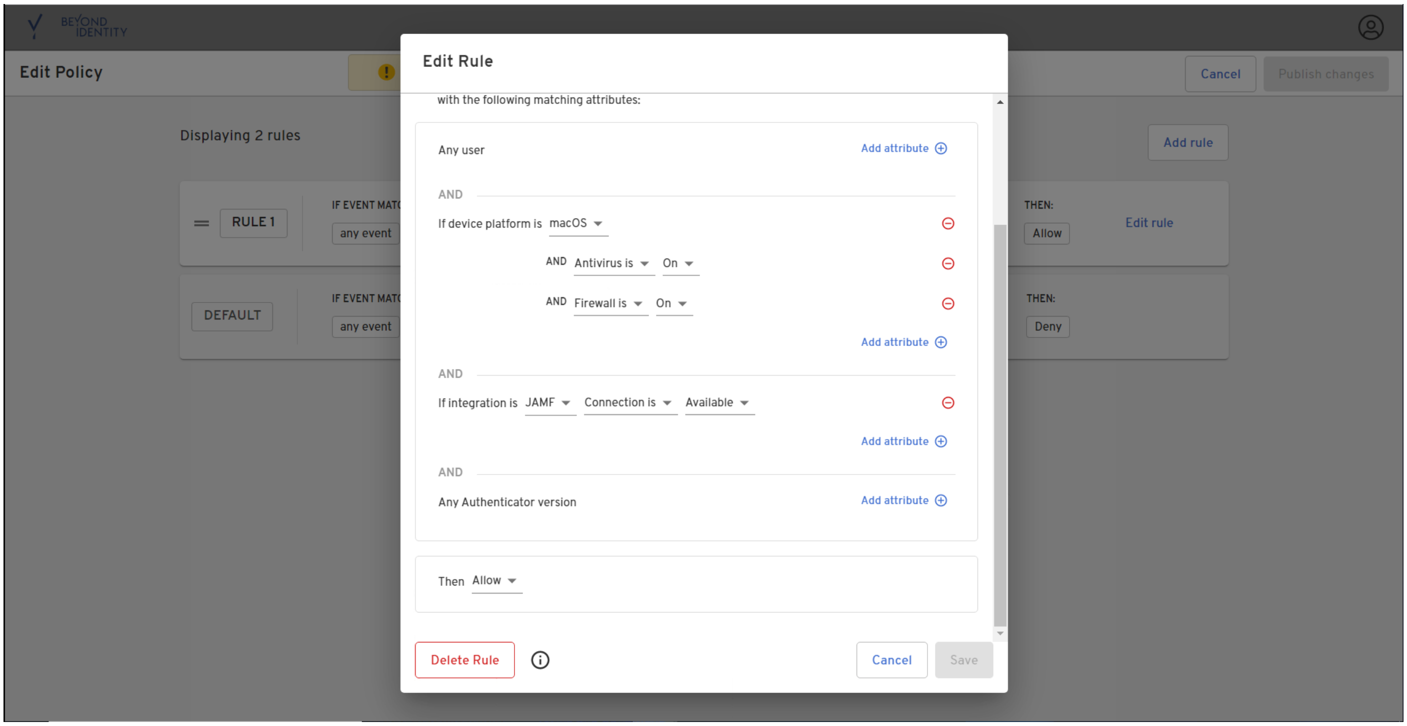
Table of Contents

Configure SAML 2.0 for Remote Support

Using Beyond Identity with SAML for Remote Support provides several benefits:

- Provides strong, unphishable multi-factor access and policy-based access controls to ensure high-trust authentication for admin accounts.
- Ensures only devices that meet the company's security policy have access to admin accounts.
- Establishes identity before privileged actions on an endpoint are allowed, using a frictionless step-up authentication.
- Creates a zero-trust PAM architecture: the system doesn't trust the user until they pass a high-assurance authentication and doesn't trust their device unless it meets security policies.
- Eliminates passwords and the corresponding vulnerabilities from privileged accounts.

Beyond Identity can validate a device's security posture before allowing access to Remote Support.



with the following matching attributes:

Any user

AND

If device platform is macOS

AND Antivirus is On

AND Firewall is On

AND

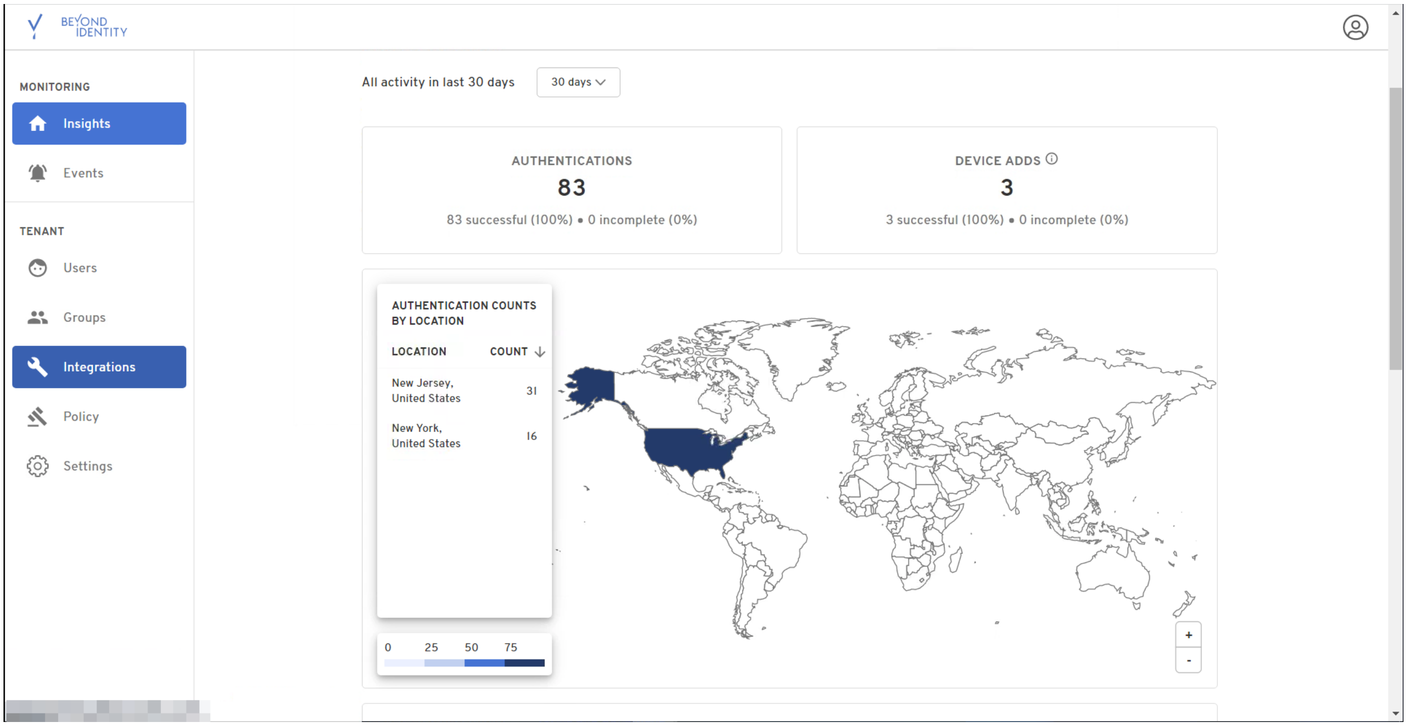
If integration is JAMF Connection is Available

AND

Any Authenticator version

Then Allow

Beyond Identity can provide insights into access activity.



All activity in last 30 days

AUTHENTICATIONS
83
83 successful (100%) • 0 incomplete (0%)

DEVICE ADDS
3
3 successful (100%) • 0 incomplete (0%)

AUTHENTICATION COUNTS BY LOCATION

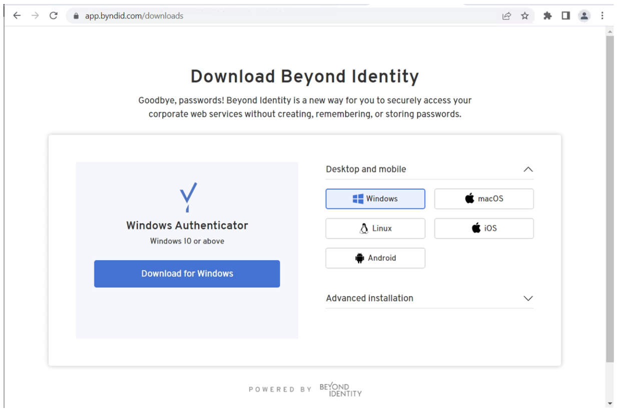
LOCATION	COUNT
New Jersey, United States	31
New York, United States	16

To use the Beyond Identity app, you must download and install the application, and configure it and BeyondTrust Remote Support to work together. The integration is configured using POST, not redirect. The integration can be used to authenticate SAML for representatives and public sites.

Download the Beyond Identity App

Go to the Beyond Identity Download site at https://app.byndid.com.

Download and install the Beyond Identity app, and then use the app to authenticate your instance of Beyond Identity.



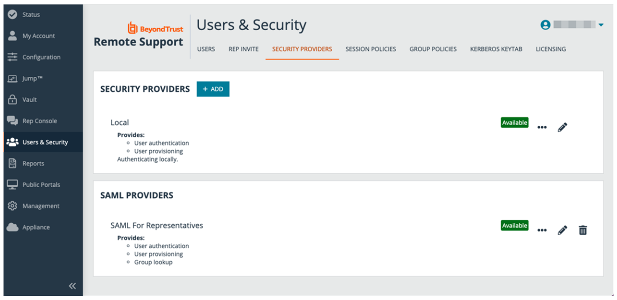
Download Beyond Identity

Goodbye, passwords! Beyond Identity is a new way for you to securely access your corporate web services without creating, remembering, or storing passwords.

Configure Beyond Identity for Representatives

Follow the steps below to download and configure the Beyond Identity app for a representative.

1. If Beyond Identify is already open in a browser tab, open a new browser tab for BeyondTrust Remote Support.
2. Go to the /login interface of the Remote Support instance.
3. Click **Users & Security** on the left menu, and then click the **Security Providers** tab.
4. Click **Add** and select **SAML for Representatives**.



SECURITY PROVIDERS

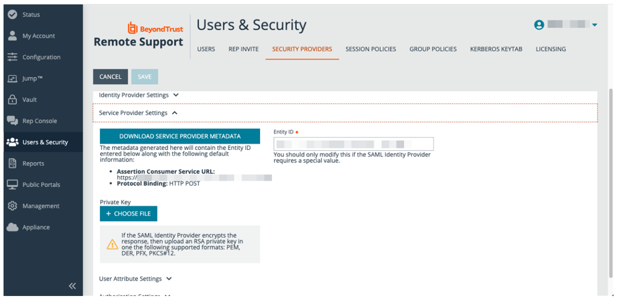
Local
Provides:
- User authentication
- User provisioning

Authenticating locally.

SAML PROVIDERS

SAML For Representatives
Provides:
- User authentication
- User provisioning
- Group lookup

5. Scroll down and expand the **Service Provider Settings**.
6. Locate the **Assertion Consumer Service URL** and the **Entity ID**. These are required for Beyond Identity. Alternately, click **Download Service Provider Metadata**.



The metadata generated here will contain the Entity ID entered below along with the following default information:

- **Assertion Consumer Service URL:** https://[redacted]
- **Protocol Binding:** HTTP POST

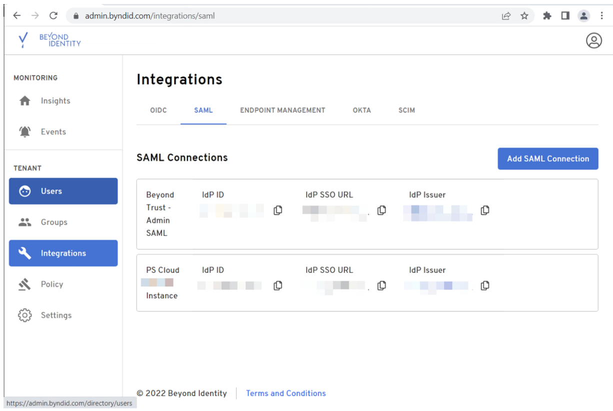
Entity ID • [redacted]

You should only modify this if the SAML Identity Provider requires a special value.

Private Key

If the SAML Identity Provider encrypts the response, then upload an RSA private key in one the following supported formats: PEM, DER, PFX, PKCS#12.

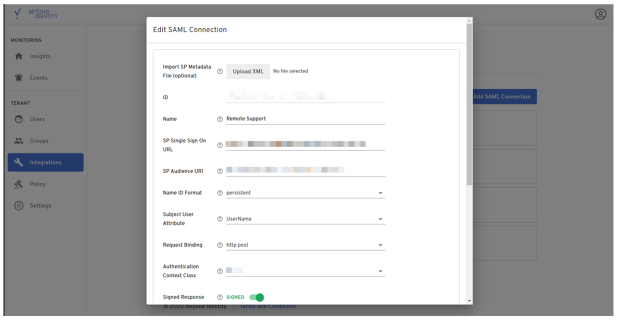
7. If Beyond Identity is not already open, open it in a new browser tab.
8. Click **Integrations** in the left menu.
9. Click the **SAML** tab.
10. Click **Add SAML Connection**.



SAML Connections

	IdP ID	IdP SSO URL	IdP Issuer
Beyond Trust - Admin SAML	[redacted]	[redacted]	[redacted]
PS Cloud [redacted] Instance	[redacted]	[redacted]	[redacted]

11. If you have downloaded the service provider metadata, click **Upload XML** and locate the file on your device.
12. If you have not downloaded the information, then:
    - Copy the **Assertion Consumer Service URL** in Remote Support to **SP Single Sign On URL** in Beyond Identity.
    - Copy the **Entity ID** in Remote Support to **SP Audience URI** in Beyond Identity.



Edit SAML Connection

Import SP Metadata File (optional): No file selected

ID: [redacted]

Name: Remote Support

SP Single Sign On URL: [redacted]

SP Audience URI: [redacted]

Name ID Format: persistent

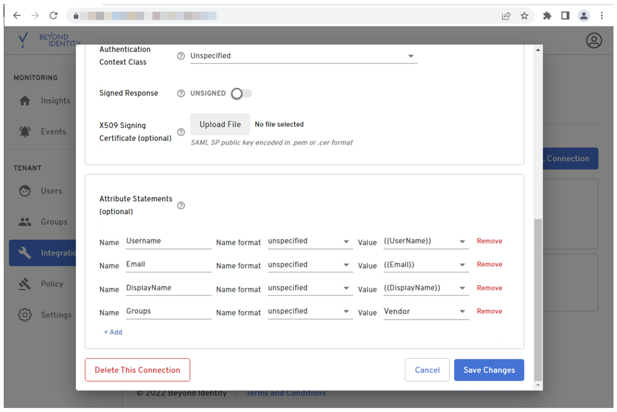
Subject User Attribute: UserName

Request Binding: http post

Authentication Context Class: [redacted]

Signed Response: SIGNED

13. In Beyond Identity, configure **Attribute Statements**. **Groups** includes a RS group to be assigned via the SAML assertion.



Authentication Context Class: Unspecified

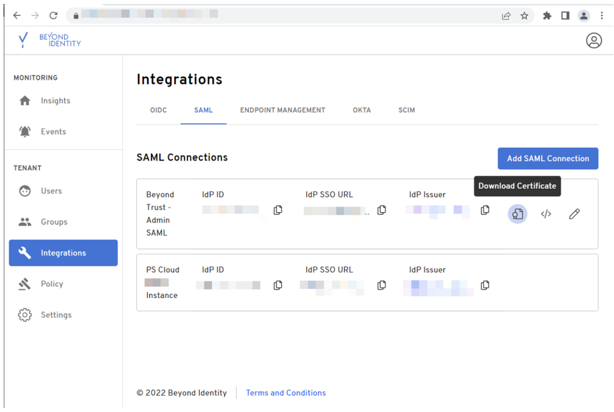
Signed Response: UNSIGNED

X509 Signing Certificate (optional): Upload File No file selected
SAML SP public key encoded in .pem or .cer format

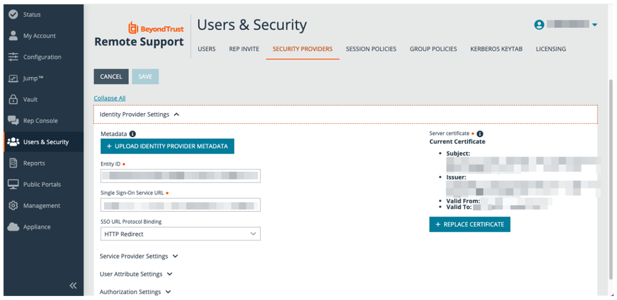
Attribute Statements (optional)

Name	Name format	Value
Username	unspecified	{{UserName}}
Email	unspecified	{{Email}}
DisplayName	unspecified	{{DisplayName}}
Groups	unspecified	Vendor

14. In Beyond Identity, click **Save Changes**.
15. In the **SAML Connections** panel, locate the connection just added.
16. For the new connection:
    - Click the **Download Certificate** icon.
    - Click the **Download Metadata** icon **</>**.

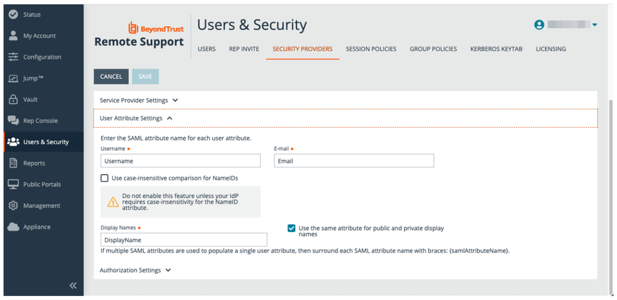


17. Return to the browser tab for the /login interface of the BeyondTrust Remote Support instance.
18. In the Remote Support /login interface:
    - Click **Upload Identity Provider Metadata** and locate the file on your device.
    - Click **Upload Certificate** (or **Replace Certificate**, if required), and locate the file on your device.



SSO URL Protocol Binding: HTTP Redirect

19. Scroll down and expand the **User Attribute Settings**.
20. Configure based on the attribute names configured in Beyond Identity.



Enter the SAML attribute name for each user attribute.

Username: Username

E-mail: Email

☐ Use case-insensitive comparison for NameIDs

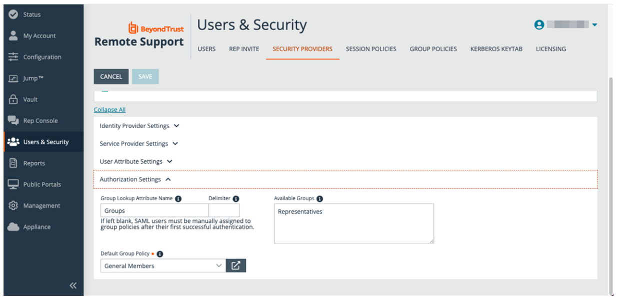
Do not enable this feature unless your IdP requires case-insensitivity for the NameID attribute.

Display Names: DisplayName

☑ Use the same attribute for public and private display names

If multiple SAML attributes are used to populate a single user attribute, then surround each SAML attribute name with braces: {samlAttributeName}.

21. Scroll down and expand **Authorization Settings**.
22. Configure as required. A **Default Group Policy** must be selected.
23. Click **Save**.
24. Log out of BeyondTrust Remote Support.



Group Lookup Attribute Name: Groups

Delimiter:

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

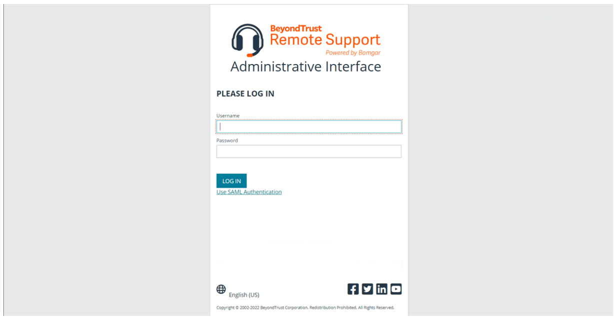
Available Groups: Representatives

Default Group Policy: General Members

Test Beyond Identity on your Device

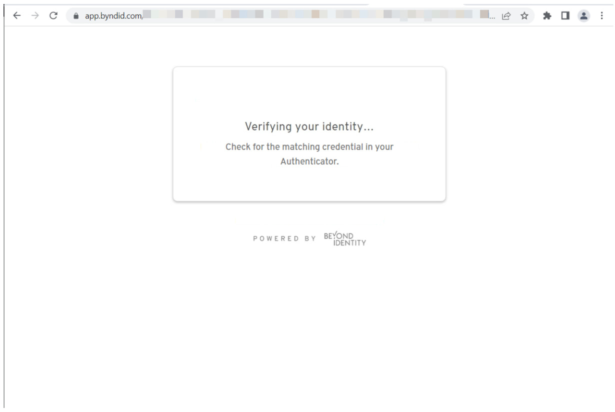
To test Single Sign-On using SAML with the Beyond Identity app, ensure you are logged out of all instances of BeyondTrust Remote Support.

On the login page for Remote Support, click **Use SAML Authentication**.



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

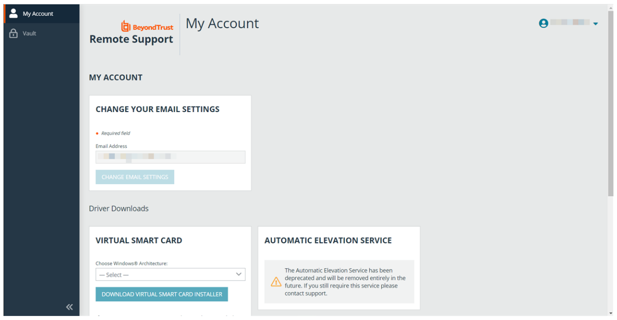
A screen shows the Beyond Identity app verifying Identity.


app.byndid.com[redacted]

Verifying your identity...

Check for the matching credential in your Authenticator.

After successful verification, you are authenticated in Remote Support.



MY ACCOUNT

CHANGE YOUR EMAIL SETTINGS

• Required field

Email Address: [redacted]

Driver Downloads

VIRTUAL SMART CARD

Choose Windows® Architecture: — Select —

AUTOMATIC ELEVATION SERVICE

The Automatic Elevation Service has been deprecated and will be removed entirely in the future. If you still require this service please contact support.

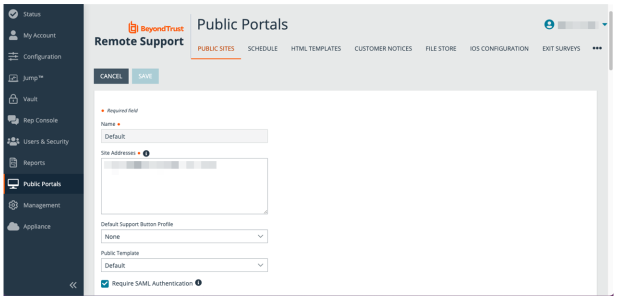
Configure Beyond Identity for Public Portals or Sites

Repeat the steps for "Configure Beyond Identity for Representatives" on page 4 with the following changes:

In step 4, select **SAML For Public Portals**.

After saving the configuration in the Remote Support (step 23), do not log out. Instead, continue with these additional steps:

1. Select **Public Portals** on the left menu, and then the **Public Sites** tab.
2. Click **Add**. In the BeyondTrust instance, click **Public Portals**, and then **Public Sites**.
3. Enter the site information, and check the **Require SAML Authentication** box.
4. Click **Save**.
5. Log out of BeyondTrust Remote Support.



• Required field

Name •: Default

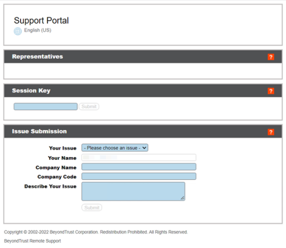
Site Addresses •: [redacted]

Default Support Button Profile: None

Public Template: Default

☑ Require SAML Authentication

When using the URL for your public sites, SAML authentication occurs via Beyond Identity.



Support Portal

English (US)

Your Issue: - Please choose an issue -

Your Name: [redacted]

Company Name

Company Code

Describe Your Issue

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

BeyondTrust Remote Support

For more information, please see Create and Configure the SAML Security Provider at https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/saml/configure-settings.htm.

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