Remote Support
Two-Factor Authentication

Table of Contents

Two-Factor Authentication Setup for BeyondTrust Remote Support Using a Time-Based, One-Time Password (TOTP)

BeyondTrust offers you a higher level of security with two-factor authentication, using a time-based, one-time password (TOTP). Besides entering their username and password to log in to the administrative interface and the BeyondTrust representative console, users who have this option enabled can use an authenticator app of their choice to receive a one-time code that allows them to securely log in.

TOTP Requirements

Users must have access to a device capable of generating one-time passwords. This is most often done through a smartphone authenticator app. Users are free to choose a compatible option, unless otherwise directed by their administrator. Examples of compatible authenticators include:

- Google Authenticator (Android, iOS)
- Authy (Android, iOS, WIndows, Linux, Mac)
- YubioAth Desktop (Windows, Linux, Mac)
- GAuth Authenticator (Windows Phone)
- Authentication Codes (Windows 8, Windows 10)
- OATHTool (command line)
- 1Password (Android, iOS, Mac, Windows)

Time-Based Considerations

With TOTP, an authenticator app generates a new password approximately every 30 seconds. Because of this, both the authenticator service and the device must be roughly in sync. BeyondTrust allows the clock on the user's device to be one minute off either way of the B Series Appliance's clock. If a wider time gap is experienced, the B Series Appliance may fail to recognize the codes generated by the user's device.

Activate Two-Factor Authentication

Depending on your company's security settings, users may have the option to activate two-factor authentication on their own. Alternatively, activation may be pushed by the administrator, in which case users would be asked to do so when logging in. While the activation process described below is similar either way, the differences are also covered.

Before you begin, make sure to have a compatible authenticator app on your smartphone.

1. Go to **/login > My Account**. Under **Two Factor Authentication**, click **Activate Two Factor Authentication**.

TC: 3/4/2024

2. The window changes to display the QR code and your next steps. If you have not already done so, download and install an authenticator app for your device.

3. Follow your app's procedure to scan the code. Alternatively, you can type in the alphanumeric code that appears under the QR code. This can be useful if the QR code is not displaying properly or if your device is having issues capturing the image. Scanning the code is the preferred method.

4. Once the app successfully captures the QR code, it generates a 6 digit token.

5. Enter your password and the token, and then click **Activate**.

TWO FACTOR AUTHENTICATION

● *Required field*

1. Use a time-based one-time password (TOTP) authenticator app.
2. To register your account with the authenticator app, scan the QR code below or manually enter the alphanumeric code in the app.

T2NM4QLMSERY4Z6A

3. Enter your password and the six-digit code generated by your authenticator app below.

Password ●

••••••••

Code on the App ●

••••••

ACTIVATE   CANCEL

⚠ By completing these steps two factor authentication will be required for accessing both the Representative Console and this site.

6. Once the screen refreshes, it displays a confirmation that two-factor authentication is now enabled for your account. The next time you login to /login or the representative console, you are required to use two-factor authentication.

TWO FACTOR AUTHENTICATION

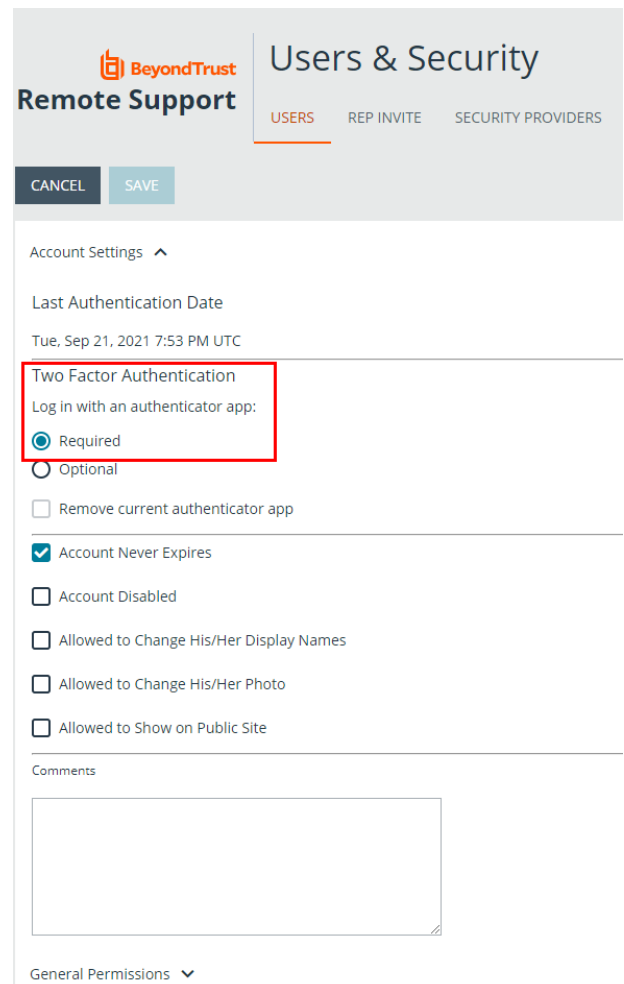Two factor authentication is currently active for your account.

REPLACE AUTHENTICATOR APP

DEACTIVATE TWO FACTOR AUTHENTICATION

Activate and Require Two-Factor Authentication

Administrators can require that users enable two-factor authentication on their accounts. To do this, go to **Users & Security > Users**, select a user to edit and under **Account Settings > Two Factor Authentication**, and check the **Required** button.
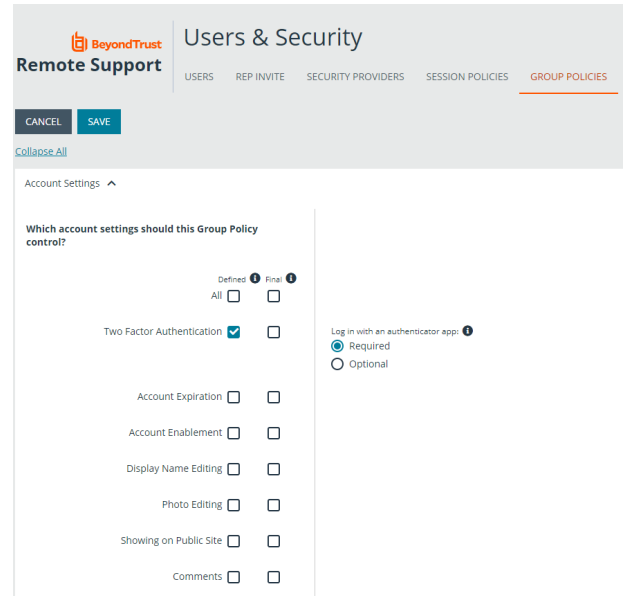
The next time this user tries to login to either the administrative interface or the representative console, a screen displays requiring the activation of two-factor authentication. The setup process is the same as outlined in the previous section.

Users & Security

Remote Support

USERS   REP INVITE   SECURITY PROVIDERS

CANCEL   SAVE

Account Settings ⌃

Last Authentication Date

Tue, Sep 21, 2021 7:53 PM UTC

Two Factor Authentication
Log in with an authenticator app:
◉ Required
◯ Optional

☐ Remove current authenticator app

☑ Account Never Expires

☐ Account Disabled

☐ Allowed to Change His/Her Display Names

☐ Allowed to Change His/Her Photo

☐ Allowed to Show on Public Site

Comments

General Permissions ⌄

Require Two-Factor Authentication in Group Policies

Two-factor authentication can also be defined when creating or editing group policies. Go to **Users & Policies > Group Policies > Account Settings > Two Factor Authentication** and select **Required** or **Optional**, depending on how you want to enforce its use.

Note: Like other account settings in group policies, the administrator can decide if two-factor authentication is defined for a specific policy, and if it can be overridden.

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

7

Log in to BeyondTrust Remote Support Using Two-Factor Authentication

Log in to the Administrative Interface

Enter your username and password. When prompted, enter the code from your authenticator app and click **OK**, and then click **Login**.

> 📌 ***Note:*** *Keep in mind that each code is valid for only 60 seconds, after which a new one is automatically generated. Apps like Google Authenticator may show a clock or some other form of tracking time.*

SALES: www.beyondtrust.com/contact **SUPPORT:** www.beyondtrust.com/support **DOCUMENTATION:** www.beyondtrust.com/docs

8

Log in to the BeyondTrust Representative Console

Enter your username and password. When prompted, enter the code from your authenticator app and click **OK**, and then click **Login**.
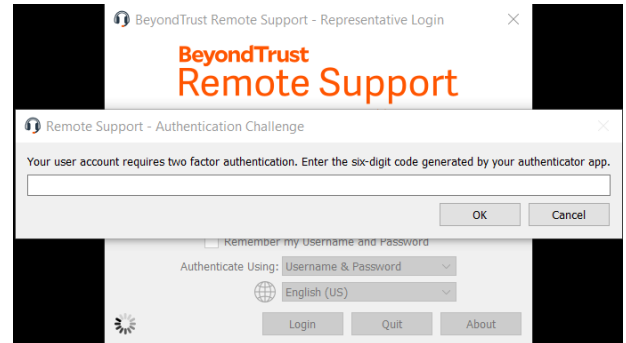
Change or Disable the Authenticator App in BeyondTrust Remote Support

Change the Authenticator App

Once you have set up two-factor authentication for your account using a specific app, you still have the option of changing to a different one. To do so, go to **/login > My Account > Two Factor Authentication** and click **Replace Authenticator App**.

TWO FACTOR AUTHENTICATION

⊘ Two factor authentication is currently required by your administrator.

REPLACE AUTHENTICATOR APP

In the next screen, enter your password and the code on the app, and click **Continue**.

TWO FACTOR AUTHENTICATION

● *Required field*

Please confirm the information below to proceed.

Password ●

●●●●●●●●

Code on the App ●

●●●●●●

CONTINUE   CANCEL

REMOTE SUPPORT
TWO-FACTOR AUTHENTICATION

You are taken to the initial setup screen. Repeat the initial setup process but this time with the new authenticator app you wish to use. If this is an app you already used and registered, simply enter the code. If it is a new app, you must scan the QR code again.

When done, click **Replace**. The previous app is disabled, and you must use the new app selected at the next login. You can always change back or select a different one by repeating the steps above.

TWO FACTOR AUTHENTICATION

● *Required field*

1. Use a time-based one-time password (TOTP) authenticator app.
2. To register your account with the authenticator app, scan the QR code below or manually enter the alphanumeric code in the app.

FWO7QIFUNRQKXPTT

3. Enter the six-digit code generated by your authenticator app below.

Code on the App ●

●●●●●●

REPLACE   CANCEL

⚠ By completing these steps you will be required to use the new authenticator app during your next login. The old authenticator app will cease to work immediately.

📌 ***Note:*** *If you decide to replace you current app, you must begin using a new one. It is not possible to disable two-step authentication from this point.*

Disable Authenticator App - User Side

If you are not required by your administrator to use two-factor authentication, you can disable this feature.

(!) IMPORTANT!

*Due to the enhanced level of security provided by this feature, it is **NOT** a best practice to disable two-factor authentication.*

To disable two-factor authentication, go to **/login > My Account > Two Factor Authentication** and click **Deactivate Two Factor Authentication**.

TWO FACTOR AUTHENTICATION

⊘ Two factor authentication is currently active for your account.

REPLACE AUTHENTICATOR APP

DEACTIVATE TWO FACTOR AUTHENTICATION

Enter your password and code on the app, and then click **Deactivate**. A message displays confirming the feature has been deactivated.

TWO FACTOR AUTHENTICATION

• *Required field*

Please confirm the information below to proceed.
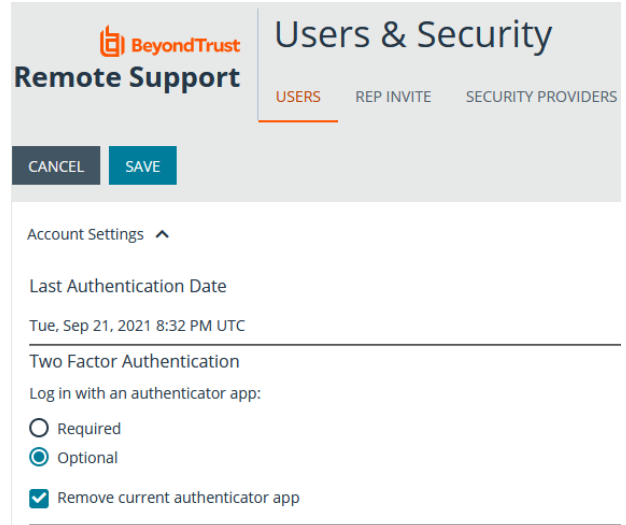
Password •

●●●●●●●●

Code on the App •

●●●●●●

DEACTIVATE   CANCEL

Disable Authenticator App - Admin Side

As an administrator, you may remove a user's current authenticator app. Go to the user's settings page, and under **Account Settings > Two Factor Authentication**, select **Remove Current Authenticator App**. Scroll to the bottom of the page and click **Save**. The next time the user logs in, only their username and password will be needed to log in to the administrative interface and the BeyondTrust representative console.

> 📌 **Note:** *An administrator may remove a user's current authenticator app whether the user is required to use two-factor authentication or simply chooses to use it.*

> ⚠️ **IMPORTANT!**
>
> *If a user's device used for two-factor authentication is lost or reset, a BeyondTrust admin must remove that user's current authenticator app and require that the user set up two-factor authentication again.*