BeyondTrust

Privileged Remote Access
Two-Factor Authentication

TC:5/14/2019

Table of Contents

Two-Factor Authentication Setup 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 into the administrative interface and the BeyondTrust access 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 every 60 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 appliance's clock. If a wider time gap is experienced, the appliance may fail to recognize the codes generated by the user's device.

Activate Two-Factor Authentication

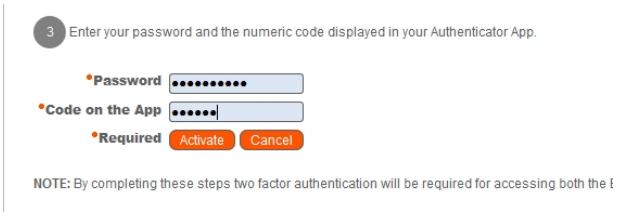
Depending on your company's security settings, users may have the option to activate two-factor authentication on their own. Alternatively, activation may be pushed by the administrator, in which case users would be asked to do so when logging in. While the activation process described below is similar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

Before you begin, make sure to have a compatible authenticator app on your smartphone. In the examples below, we use Google Authenticator.

1. Go to **/login > My Account** and scroll down to the bottom of the page. Under **Two Factor Authentication**, click **Activate Two Factor Authentication**.

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

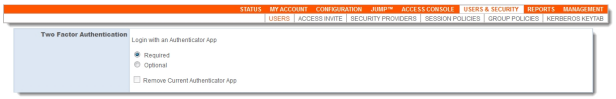
5. Enter your password and the token, and click **Activate**.



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 access console, you will be required to use 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 access console, a screen displays requiring the activation of two-factor authentication. The setup process is the same as outlined in the previous section.

Require Two-Factor Authentication in Group Policies

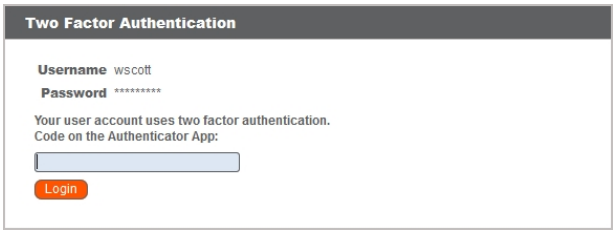
Two-factor authentication can also be defined when creating or editing group policies. Go to **Users & Policies > Group Policies > Account Settings > Two Factor Authentication** and select **Required** or **Optional**, depending on how you want to enforce its use.

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.*

Log in Using Two-Factor Authentication

Log into the administrative interface

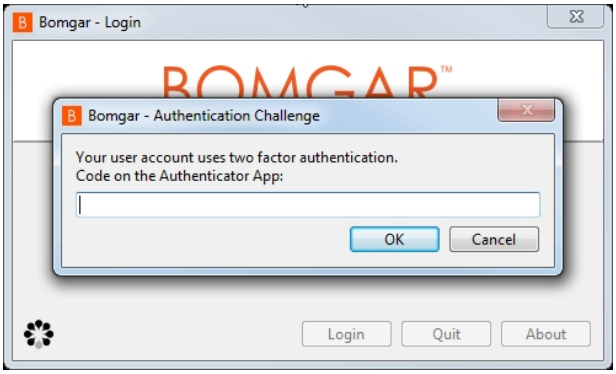
Enter your username and password. When prompted, enter the code from your authenticator app and click **Login**.



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

Log into the BeyondTrust Access Console

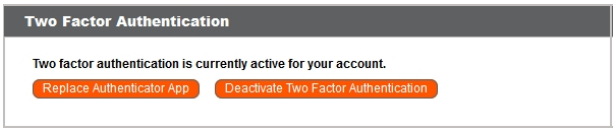
Enter your username and password. When prompted, enter the code from your authenticator app and click **Login**.



Change or Disable the Authenticator App

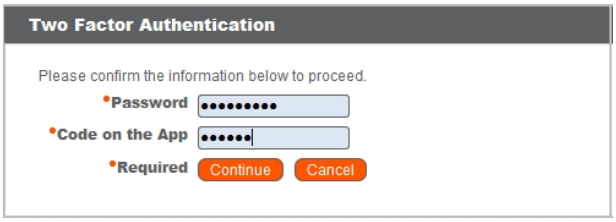
Change Authenticator App

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**.

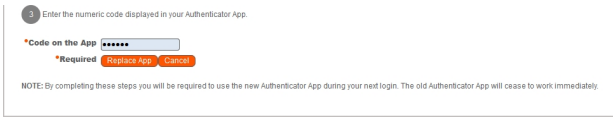


In the next screen, enter your password and the code on the app, and click **Continue**.

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 App**. 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.



> ***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.*

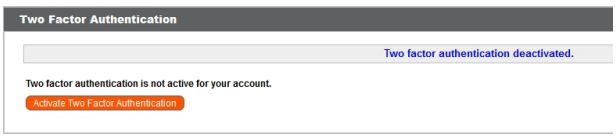
Disable Authenticator App - User Side

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

IMPORTANT!

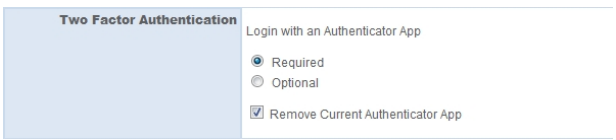
*Due to the enhanced level of security provided by this feature, it is **NOT** a best practice to disable two-factor authentication.*

To disable two-factor authentication, go to **/login > My Account > Two Factor Authentication** and click **Deactivate Authenticator App**. Enter your password and code on the app, and then click **Deactivate**. A message displays confirming the feature has been deactivated.



Disable Authenticator App - Admin Side

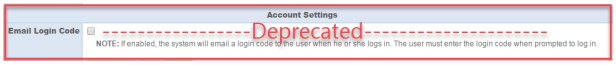
As an administrator, you may remove a user's current authenticator app. Go to the user's settings page, and under **Account Settings > Two Factor Authentication**, select **Remove Current Authenticator App**. Scroll to the bottom of the page and click **Save**. The next time the user



logs in, only their username and password is needed to log into the administrative interface and the BeyondTrust access 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.*

Transitioning from Previous Forms of Two-Factor Authentication (Email Codes)



The two-factor authentication method previously in place, known as robust authentication, relied on email codes to verify the user's identity. With BeyondTrust Privileged Remote Access version 17.1, this method has been deprecated and replaced with two-factor authentication using a time-based, one-time password (TOTP).

Users who were receiving codes to log in will be automatically upgraded to two-factor authentication. When logging in, they will see a message indicating that login codes by email have been deprecated and instructing them to use a time-based, one-time password capable device.

The user may, however, continue to use email codes until they register an authenticator app, such as Google Authenticator. This not only ensures backwards compatibility with existing security settings for a user's account, but also takes into consideration that an app or device may not be immediately available.

In this scenario, a user would continue to see a request to register an authenticator app until they begin using the new two-factor authentication method. Once the user registers an app and begins using the new method, the email code option is permanently disabled.

Because email codes are no longer an admin option, the feature cannot be re-enabled once the user begins using the new method.

IMPORTANT!

*A user could request that the administrator stop pushing requests for a device-based two-step authentication at each login. The admin has the option to do so by changing the user's permission from **Required** to **Optional** under the user's account settings. However, this will also disable emailed login codes permanently. BeyondTrust does not recommend this procedure, since it degrades the security level on that user's account. It is a best practice and highly recommended that two-factor authentication be enabled.*