

Two-factor authentication on the SSL VPN for the BU Domain was implemented November 10, 2020. This was a critical step for the security of the Binghamton University network.

Step 1

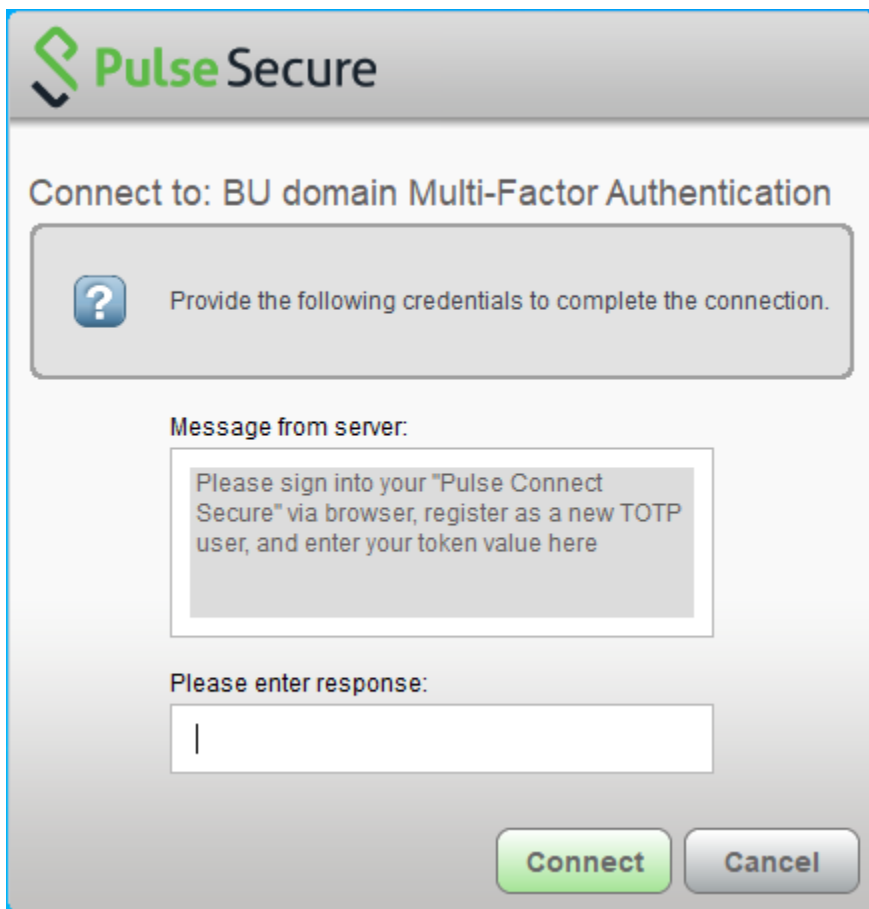
Download and install the Google Authenticator to an Android phone from the Google Play Store or to an iPhone from the App Store. You can also use the Google Authenticator on the Desktop. You can access the Google Authenticator from within a Chrome browser by googling “chrome web store google authenticator”.

See this link for a general overview:

<https://www.labnol.org/internet/google-authenticator-for-desktop/25341/>

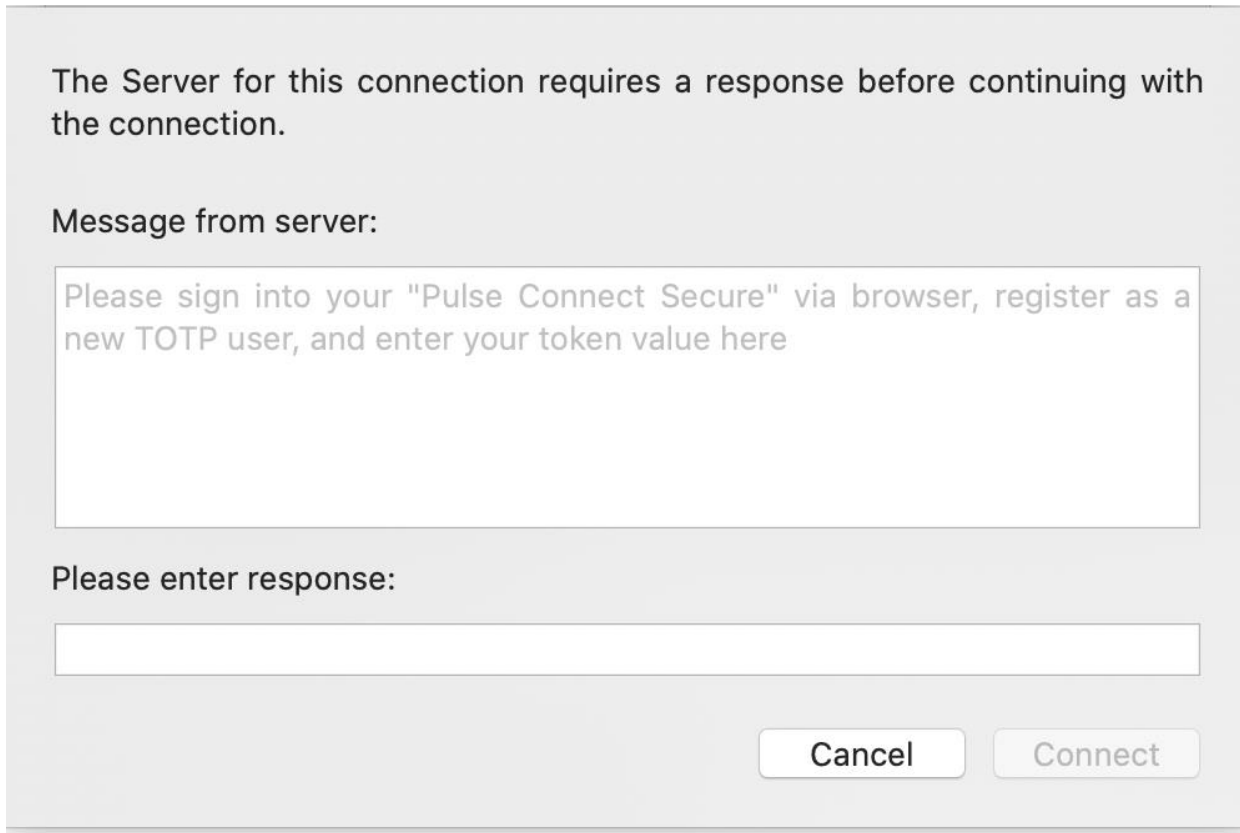
Step 2

Log into the Pulse Desktop Client (PDC) and on Windows you will see this dialog box:



The image shows a dialog box titled "Pulse Secure" with a green logo. The main heading is "Connect to: BU domain Multi-Factor Authentication". Below this is a grey box with a question mark icon and the text "Provide the following credentials to complete the connection." Underneath is a section labeled "Message from server:" containing a text box with the message: "Please sign into your 'Pulse Connect Secure' via browser, register as a new TOTP user, and enter your token value here". Below the message is a section labeled "Please enter response:" with an empty text input field. At the bottom right are two buttons: "Connect" (highlighted in green) and "Cancel".

On macOS it will look like this:



The Server for this connection requires a response before continuing with the connection.

Message from server:

Please sign into your "Pulse Connect Secure" via browser, register as a new TOTP user, and enter your token value here

Please enter response:

The message is quite cryptic. TOTP means Time-Based One-Time Password.

Step 3

Point your browser to ssl.binghamton.edu and Log in to the BU domain.

This dialog box will display.

Welcome to Binghamton University Virtual Private Network Binghamton University SSL VPN

Add BU\██████████ user account to your two factor authentication app

You will need to install Google Authenticator or some other 2-Step Verification application on your tablet or phone. Please visit your device's app store and search for "Google Authenticator" to continue.

1. Configure the App:

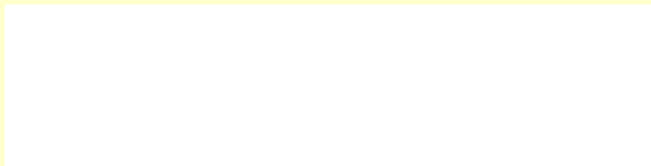
Open your two factor authentication app and add "BU\██████████" user account by scanning the below QR code.

If you can't use QR code, then enter [this text](#)



2. Store Backup Codes:

Backup codes can be used to access your account in the event you lose access to your device and cannot receive two-factor authentication codes. Following backup codes are only for one time use, we recommend you to save them securely.



Copy to Clipboard

3. Enter token code that the application generates:

Sign In

Step 4

Use the Google Authenticator on your phone to scan the QR code and enter the token code it generates.

Alternatively, on the desktop you will need to use the GAUth add-on for Chrome.

In subsequent connection attempts you will not have to use a QR code. You will have to log into BU domain and use Google Authenticator every time you connect to Binghamton University SSL VPN.