TWO-FACTOR AUTHENTICATION ON THE PULSE SECURE SSL VPN

Two-factor authentication on the Pulse Secure SSL VPN for the BU Domain was implemented Nov. 10, **as a critical step for the security of the Binghamton University network.** *Below are the instructions to download and install the Google Authenticator for added security.* ***For more information review the SSL page. (/its/about/organization/operations-and-infrastructure/networking/off-campus-connecting.html)***

Step 1

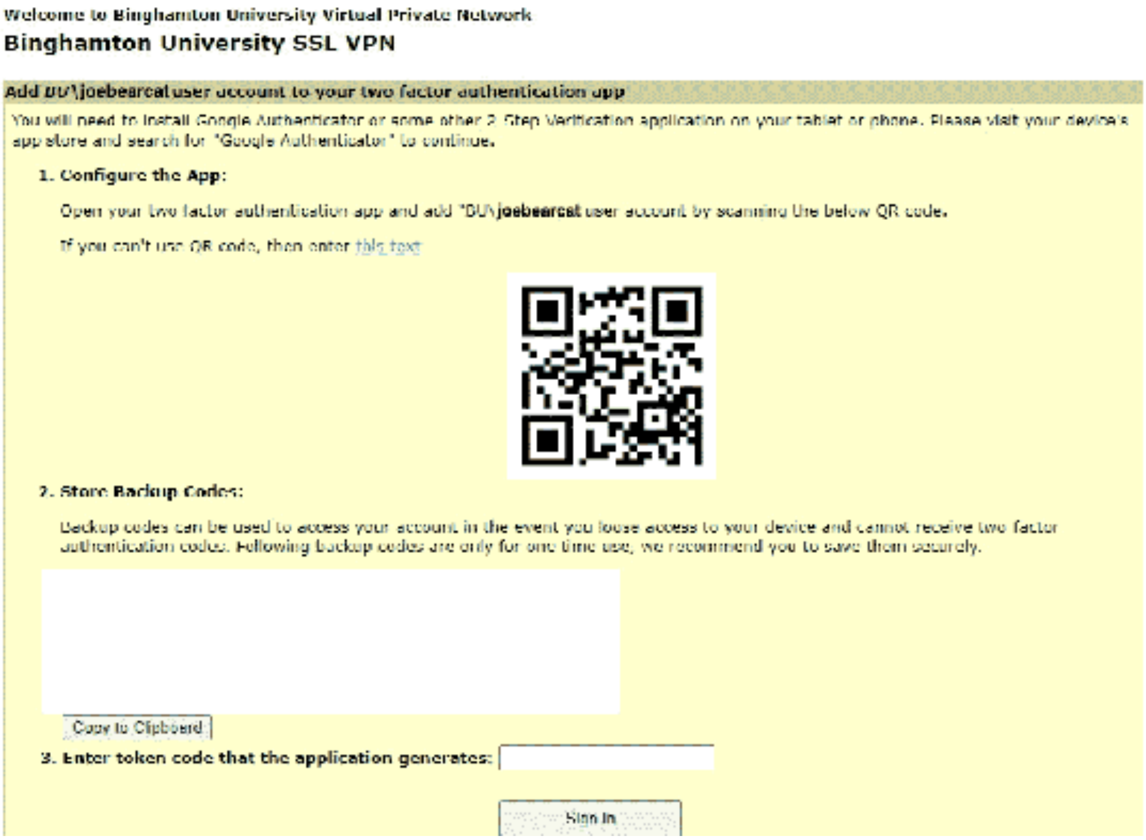
Download and install the Google Authenticator to an Android phone from the Google Play Store or to an iPhone from the App Store. You can also use the Google Authenticator on a laptop/computer if you do not have a smartphone. You can access the Google Authenticator from any browser by googling “web store google authenticator”.

Open the Google Authenticator on your device.

Step 2

In a browser on your phone or computer, browse to **ssl.binghamton.edu (https://ssl.binghamton.edu/)** and **log in to the BU domain**. A similar dialog box as seen below will display.

(Click on image for larger version.)



Welcome to Binghamton University Virtual Private Network

Binghamton University SSL VPN

Add BU\joebearcat 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\joebearcat user account by scanning the below QR code.

   If you can't use QR code, then enter this text

2. Store Backup Codes:

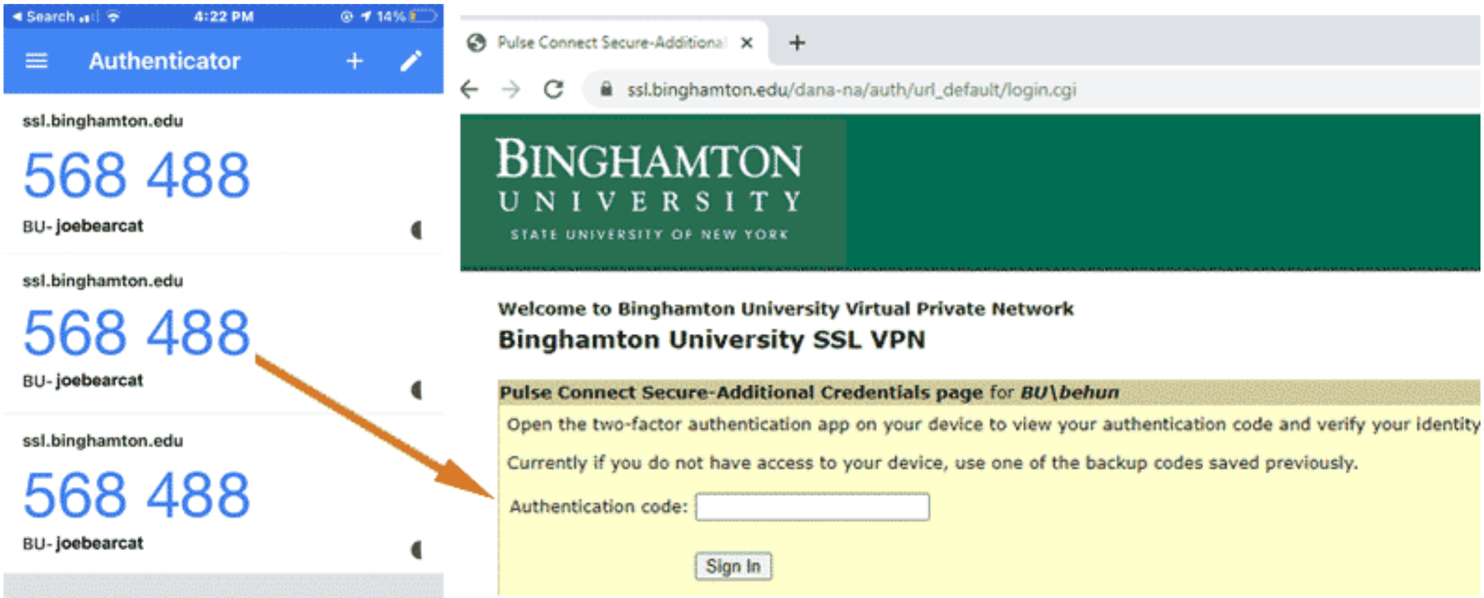
   Backup codes can be used to access your account in the event you loose access to your device and cannot receive two factor authentication codes. Following backup codes are only for one time use, we recommend you to save them securely.

3. Enter token code that the application generates:

(https://binghamton.edu/its/about/organization/operations-and-infrastructure/networking/img/qrc-code-graphic-large2.jpg)

NOTE: The QR code in the image above is just for placement, it is unique for every person. Store Backup Codes are also generated for you for a one-time use in case you lose access to your device and cannot receive two-factor authentication codes. You can securely save these for later use.

Use the Google Authenticator App on your phone to scan the QR code and enter the 6-digit token it generates (no spaces). If you are using a browser you will need to use the GAuth Authenticator add-on for Chrome. The Google Authenticator generates a new 6-digit number token every 30 seconds.



Welcome to Binghamton University Virtual Private Network

Binghamton University SSL VPN

Pulse Connect Secure-Additional Credentials page for *BU\behun*

Open the two-factor authentication app on your device to view your authentication code and verify your identity

Currently if you do not have access to your device, use one of the backup codes saved previously.

After the first time you activate the QR code the Binghamton University SSL VPN server will associate that device with your login credentials and the QR code that was activated. **You will not have to scan the QR code again unless your SSL VPN account has to be reset.**

After a successful sign in you will be directed to the Binghamton University SSL VPN web page. You can log out of the web page and launch the Pulse Secure Desktop Client (PDC). You may be prompted to update the PDC.

You will have to log into BU domain and use Google Authenticator every time you connect to Binghamton University SSL VPN.