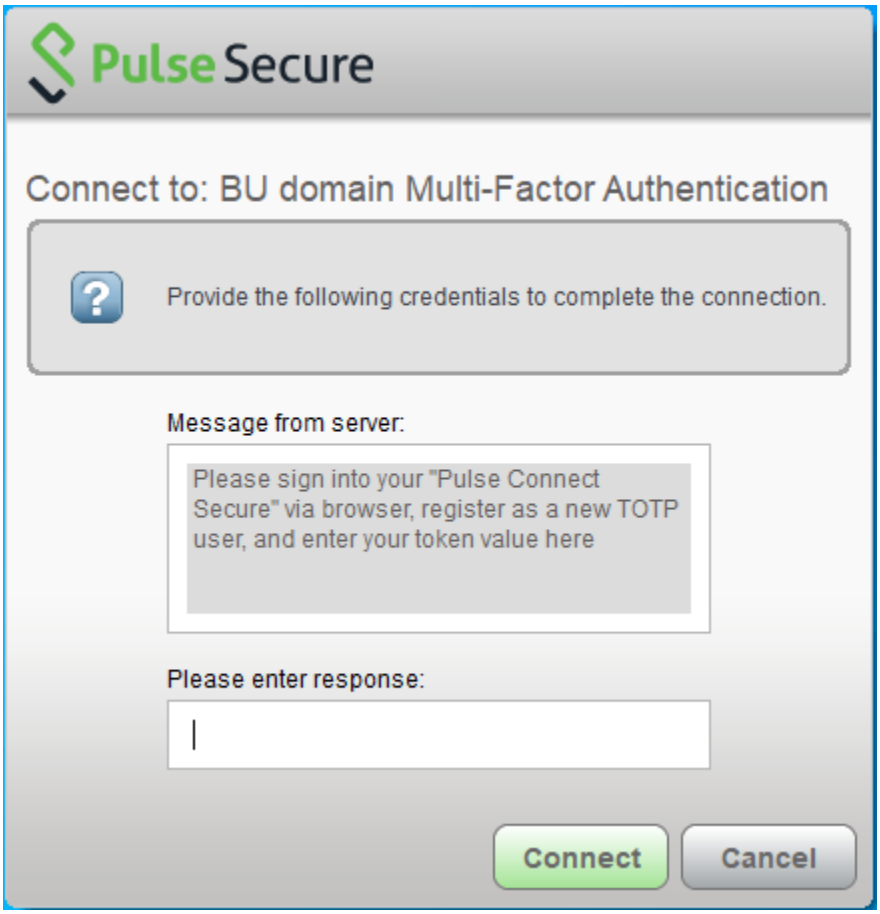
Two-factor authentication on the SSL VPN for the BU Domain was implemented November 10, 2020. This was a critical step for the security of the Binghamton University network.

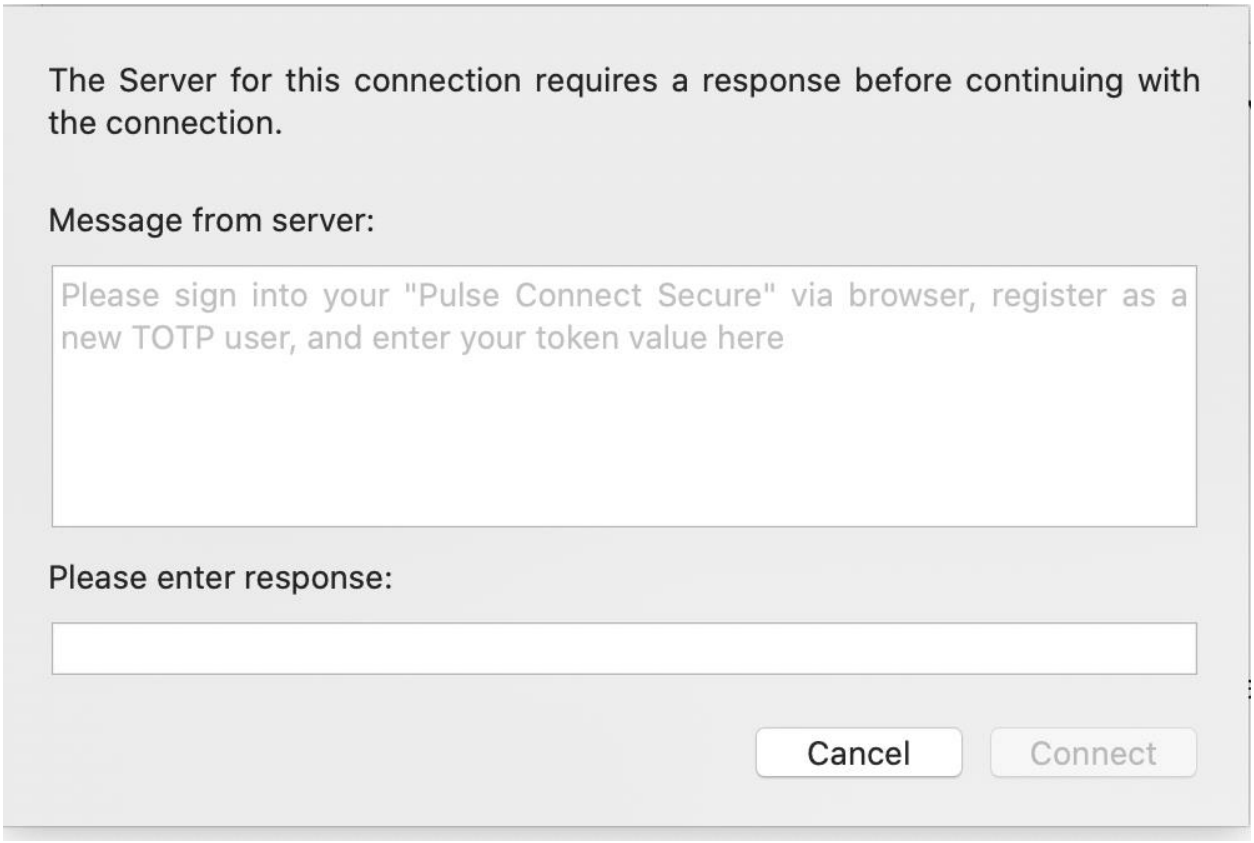
Step 1
Download and install the Google Authenticator to an Android phone from the Google Play
Store or to an iPhone from the App Store. You can also use the Google Authenticator on the Desktop.
You can access the Google Authenticator from within a Chrome browser by googling “chrome web store google authenticator”.

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:



On macOS it will look like this:

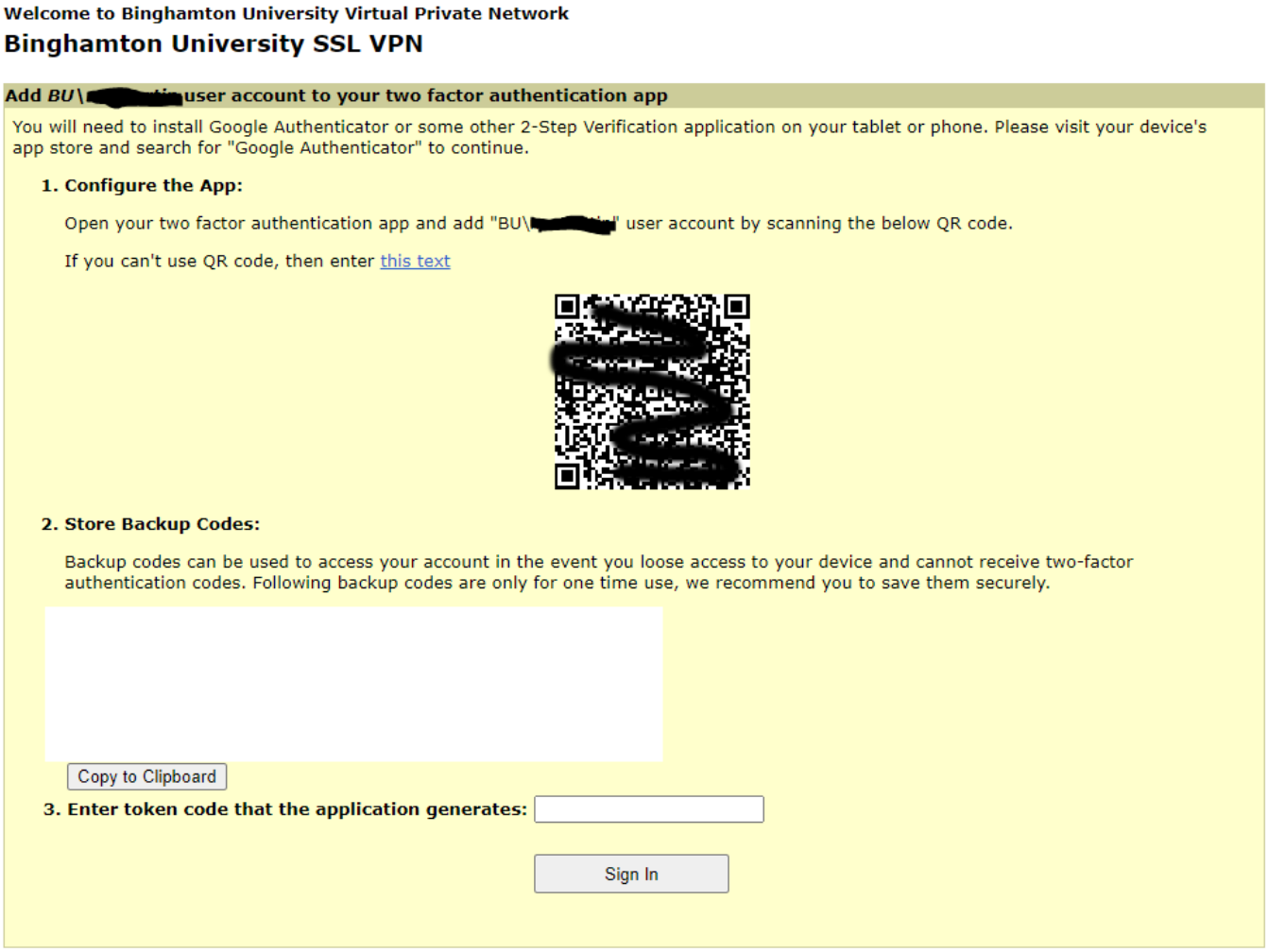


The message is quite cryptic. TOTP means Time-Based One-Time Password.

Step 3

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

This dialog box will display.



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.