Pulse Secure Duo 2FA Authentication

To utilize two-factor authentication with the Pulse Secure client, the Server URL in the Pulse Secure client must be changed to secure.colostate.edu/2FA.

**Edit Existing Pulse Secure Connection**

If the Pulse Secure client has a connection to secure.colostate.edu, this connection can be edited to connect to secure.colostate.edu/2FA.

Open the Pulse Secure client, click on the existing connection and then click on the pencil (Edit) icon.

Edit the Server URL to reflect the correct URL of secure.colostate.edu/2FA and then click the Save button.

**Add a new Connection**

To add a new connection to the Pulse Secure Client, open Pulse Secure and click on the + icon.

Provide a Unique Name in the Name textbox. In the Server URL textbox, enter secure.colostate.edu/2FA and then click on the Add button to add this connection to the list of connections.
Connect using Pulse Secure

When connecting to https://secure.colostate.edu/2fa from off-campus using the Pulse Secure client, users will have to provide a second credential for authentication using Duo.

The Pre Sign-In Notification window appears notifying users about a required 2nd authentication after signing in and the three authentication methods that are accepted.

Click Proceed to log in to the Pulse Secure client.

Enter your eName and ePassword and then click on the Connect button.
Pulse Secure will launch a new window, asking for a second credential to continue.

For the second credential, enter one of the following:

- **push**: Sends a push login request to the Duo Mobile App on the primary smartphone on your list of registered devices.
- **phone**: Calls the primary phone number on your list of registered devices.
  - When using phone, duo will call the top device that has a phone number, which may be a registered smartphone.
- A passcode (**123456**): This is generated from the Duo Mobile App or from a Duo hardware token.

**Note:** If more than one device type (smartphone, landline, etc.) is registered, a number may be added to the end of the secondary password to send requests to a particular device.

- **push2**: Sends a push request to the second smartphone on your list of registered devices.
- **phone2**: Calls the second phone number on your list of registered devices