CITO

CENTRAL INFORMATION TECHNOLOGY OFFICE

CITO VPN Secure Connection Manual

Document No: ISMS04-0030

Version 1.6

Publish Date： 16/12/2022

Implementation Date：16/12/2022

Table of Contents

Ivanti Secure Access Client Installation Guide

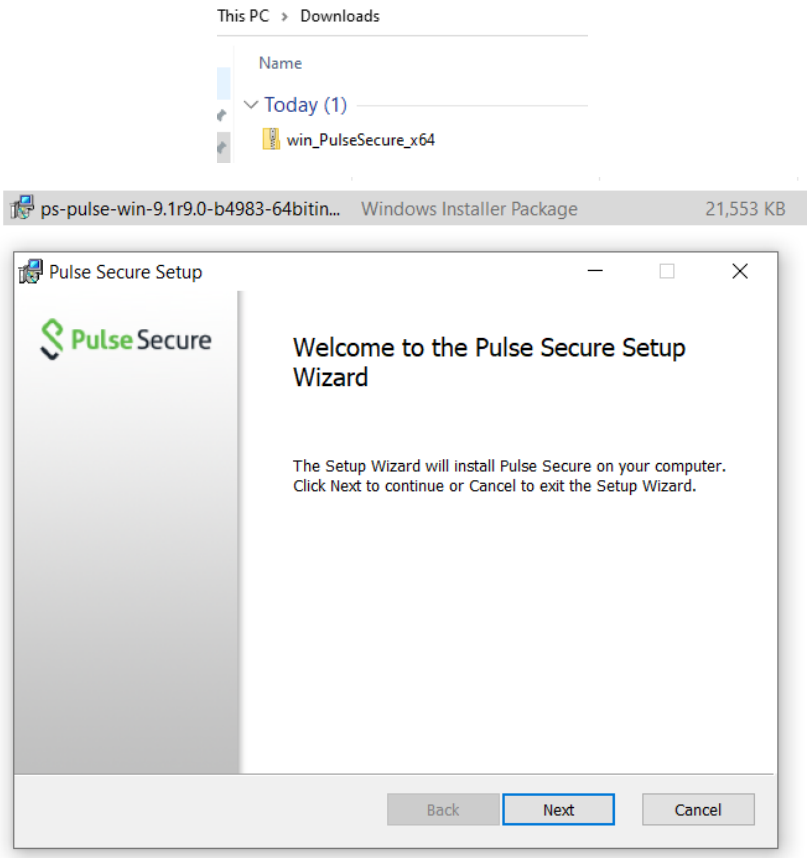
Secure VPN Client: ivanti

Manual Client Installation:

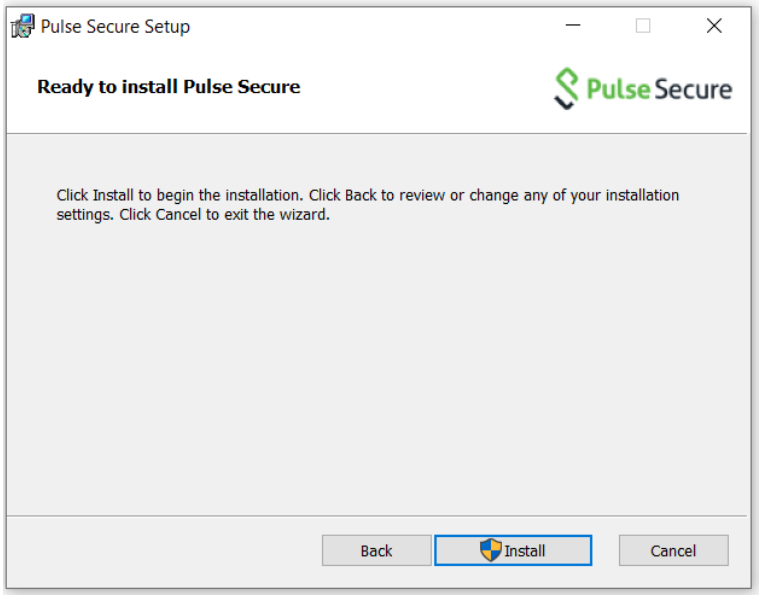
1. Use the followings links to download & install the client:

- *For a **MAC PC,** use the below link: http://cito.gov.bz/pulse/mac_PulseSecure.zip*
- *For a **WINDOWS PC,** use the below link: http://cito.gov.bz/pulse/win_PulseSecure_x64.zip*
- *Clients for iOS & Android can be downloaded from respective app store.*

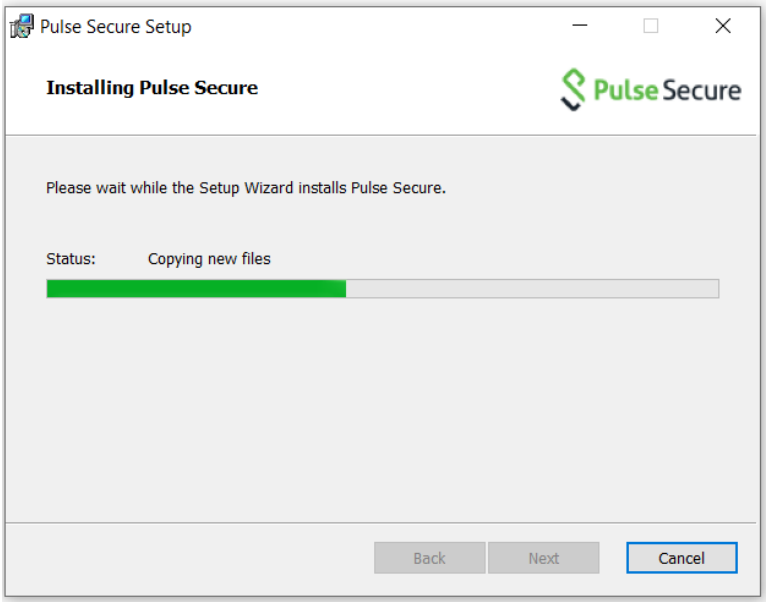
2. Open the downloaded ZIP File and double click on the installer package to start the process:



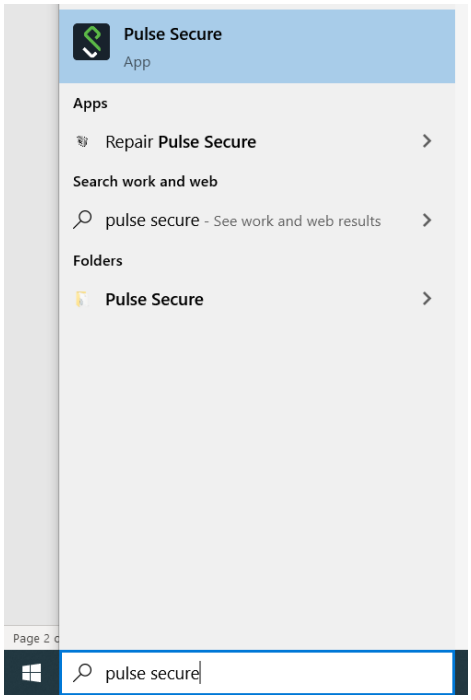
3. Click on next and then install.



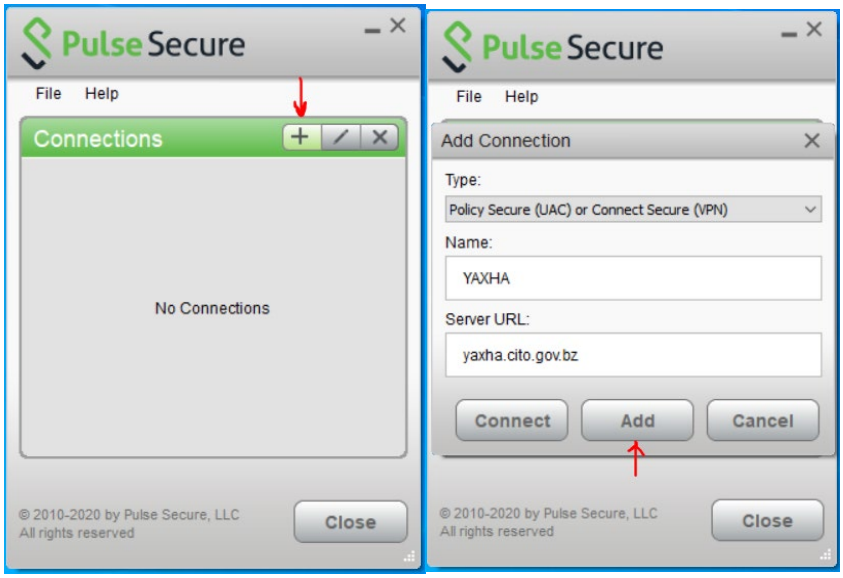
4. When the installation status is completed, click on Finish.



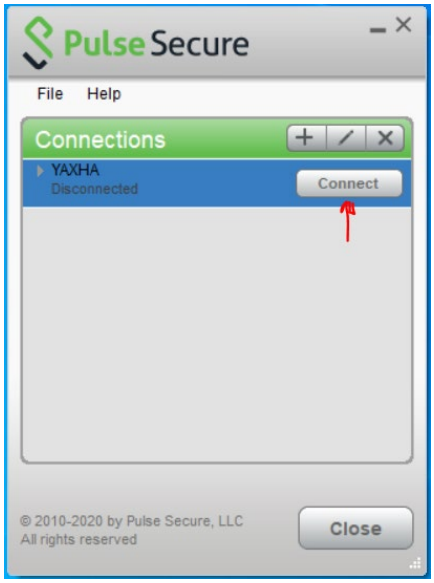
5. On the search tab, type Pulse Secure and open the APP.



6. Click on the **+** button to add a new connection. Fill in the empty field with the information below, and click add:



7. To establish session, click “Connect” and Pulse Secure will check if your computer is compliant.



Host Check plugin will run and verify that computer meets the following criteria:

a. Windows

i. OS: Windows 8.1 & higher (64 & 32 bit)

ii. Antivirus Vendors allowed: AVAST, AVG, Avira, Bitdefender, BullGuard, ESET, F-Secure, Kaspersky, McAfee, Panda, Symantec, Trend Micro. Antivirus Definition Updates should not be older than 10 Days.

iii. Ensure that its respective firewall is turned ON.

b. Mac

i. Ensure that its respective firewall is turned ON.

c. Mobile

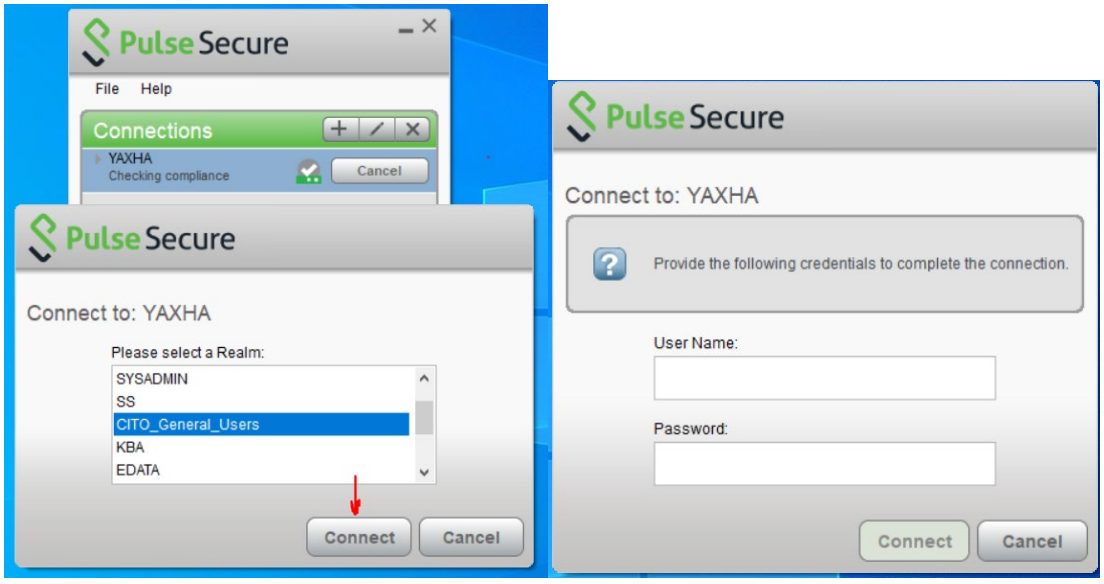
i. Android

1. Rooted devices not allowed
2. OS: version 10.0 or higher.

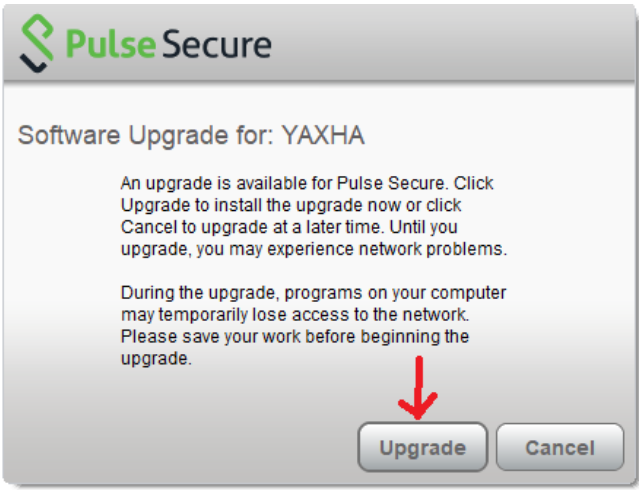
ii. IOS

1. Jailbroken devices not allowed
2. OS: version 13.0 or higher

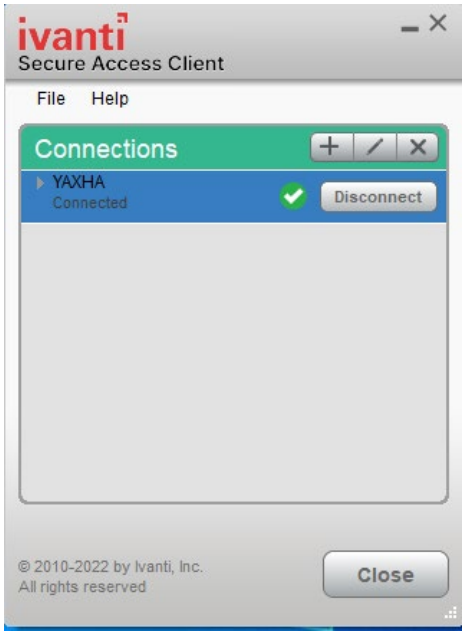
8. If the device meets the criteria, select a **REALM**, and provide your windows credentials to connect:



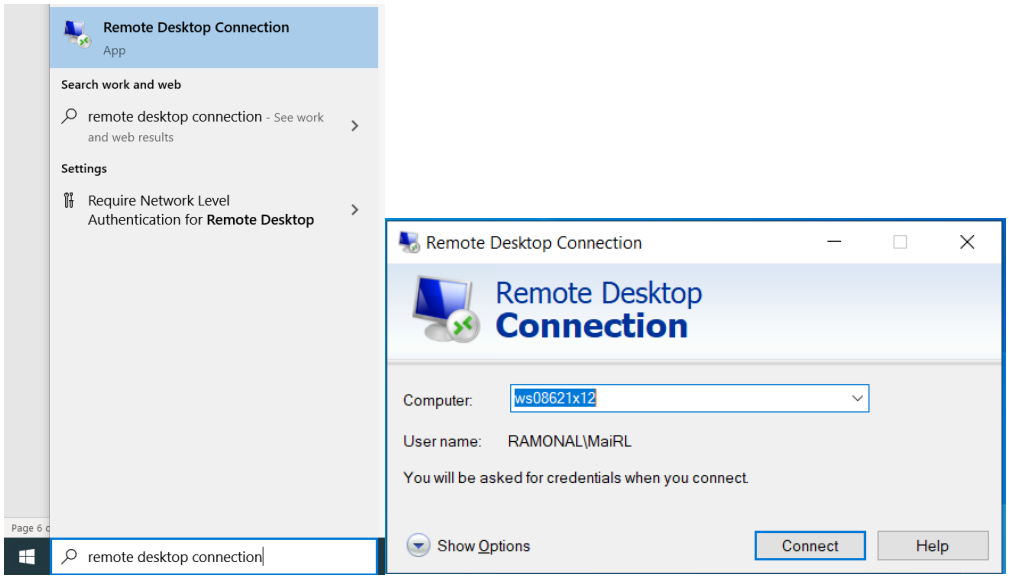
NOTE: *If prompted, select upgrade. This will upgrade the client.*



9. The below shows connection established successfully.



10. On the search bar, type Remote Desktop Connection and open the app:



11. Enter your workstation number and click connect.

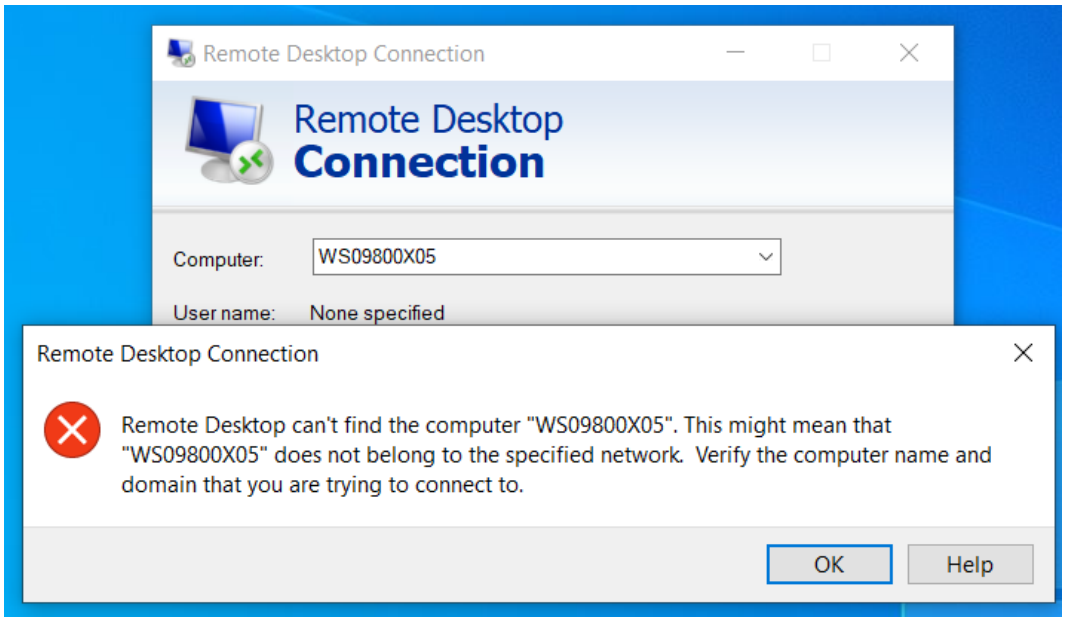
12. Next, enter your credentials and click ok.

NOTE: *Your Teleworking is now successful. At end of your Teleworking session, click* ***disconnect***.

Appendix

1. **Solution to Error Message**

   If the below error appears, contact your Computer/Systems Coordinator to request for CITO Technicians to add you to the "Remote Desktop Users."



2. **VPN Limits:**
   - VPN Idle timeout of 30 minutes.
   - VPN session timeout of 555 minutes.

3. **Local Authentication password policy**

   Non-domain users utilize Pulse Secure Local Authentication with Custom Realm.

   Local Authentication password policy is as follows:

   - Minimum of 8 characters and a maximum of 20 characters.
   - Password must have a number and a mix of uppercase and lower-case letters.
   - Password must be different from username and different from previous password.
   - Users will be forced to change password after 90 days. Users will be prompted to change their password 10 days before current password expires.
   - Whenever a user account is created, Network Administrators will set a default password. Upon first logon, the user will be forced to change the default password.
   - Local accounts are automatically locked for 10 minutes if there are 3 consecutive failed password attempts.

If you have further issues, please contact the Network Administrators via +(501)-822-2478 or network.support@cito.gov.bz

End