CITO

CENTRAL INFORMATION TECHNOLOGY OFFICE

CITO VPN Secure Connection Manual

Document No: ISMS03-0030

Version 1.1

Publish Date : 20/01/2025
Implementation Date : 16/12/2022

Version Control Log

Version	Date	Changes Included	Company	Author	V&V	Approved by
1.0	15 August 2024	Previous versions of this document can be referenced in: ISMS04-0030_V1.6_CITO VPN Secure Connection Manual	CITO	CITO	Delsie Ku	IS Committee
1.1	20 January 2025	Revised manual procedures and documentation to include VPN MFA Configuration.	CITO	CITO	Ernesto Thimbrel	IS Committee

Contents

1 Installation of Ivanti Pulse Secure Client

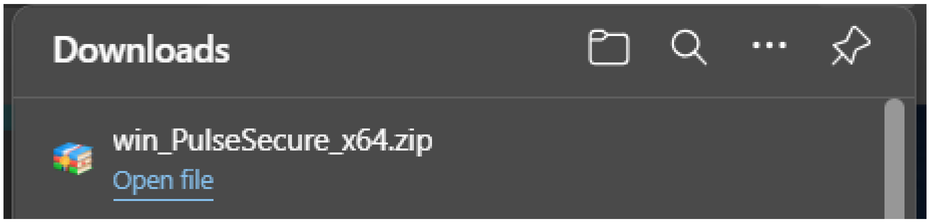
1.1 Prelude:

In this installation, you will be working with:

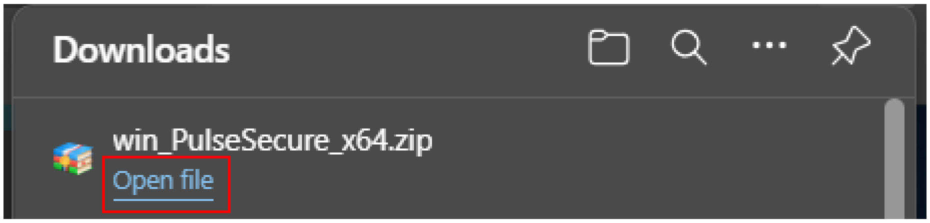
- A desktop / laptop device [device to register for use]
- The Ivanti Pulse Secure installation file [VPN Software to use for VPN access]
- The Microsoft Authenticator app [VPN verification software to establish connection]
- Remote desktop [Software used with VPN access for a registered device]

1.2 Manual Client Installation:

1. Use one of 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
2. When downloading the Ivanti Pulse file, it should look as shown below:

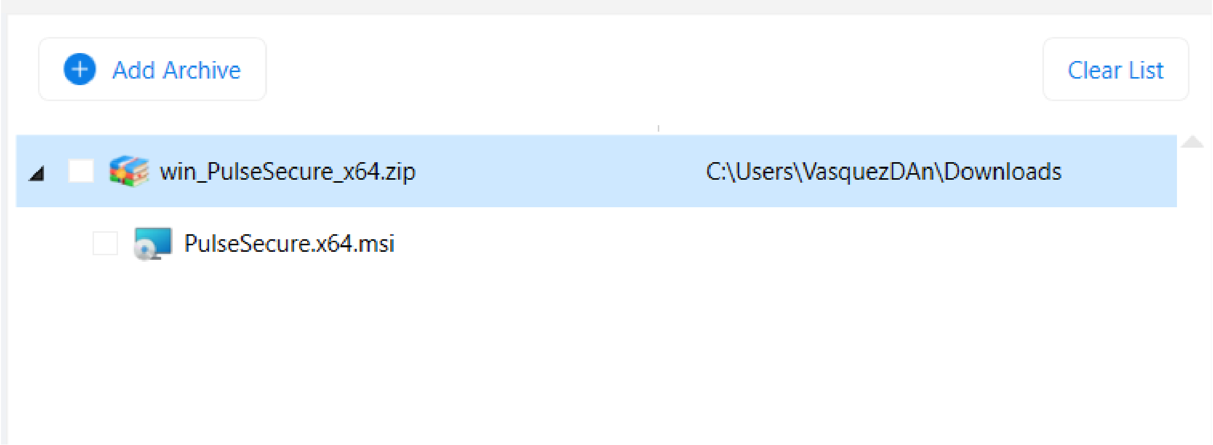


3. When completed, click the **Open File** option to start the installation process, as shown below:



4. Extract the downloaded ZIP File, by selecting the installer package and right click to select the Extract here or Extract All option. The images below show two alternatives of what you may see when extracting:

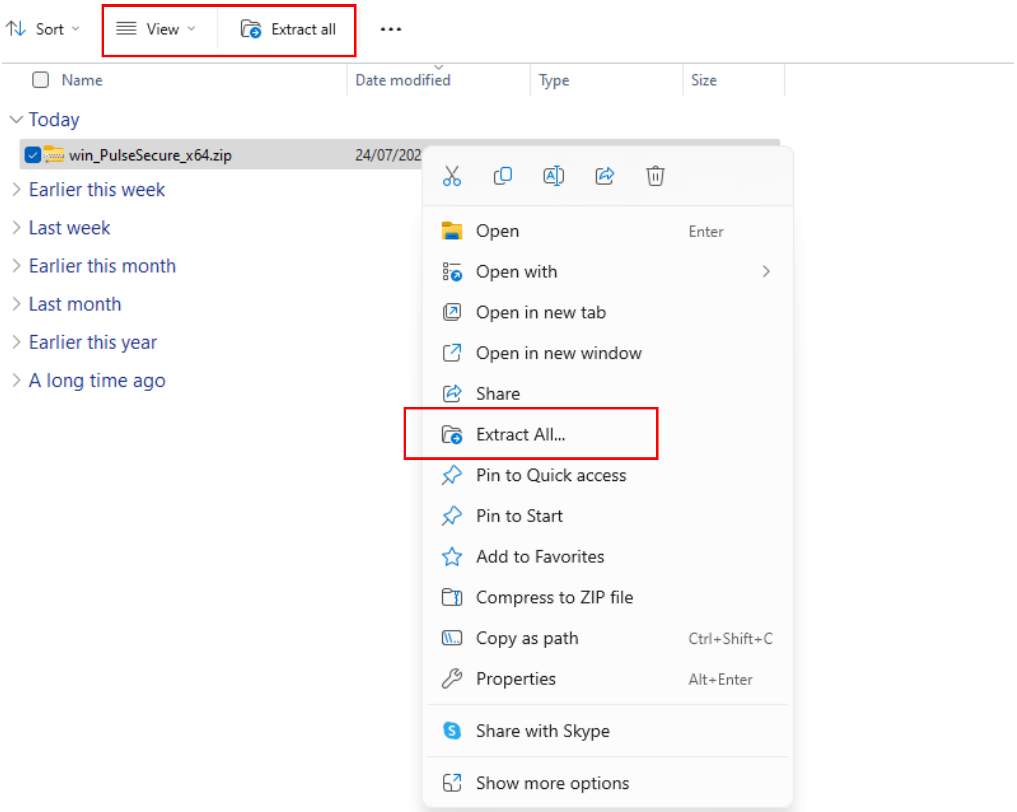
4.1 Using a RAR:



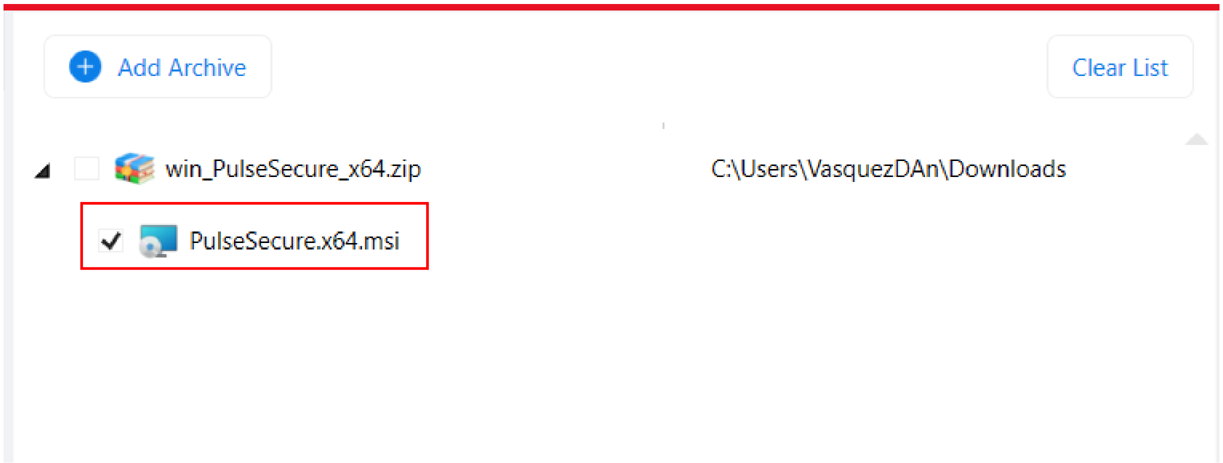
◢ □ win_PulseSecure_x64.zip C:\Users\VasquezDAn\Downloads

□ PulseSecure.x64.msi

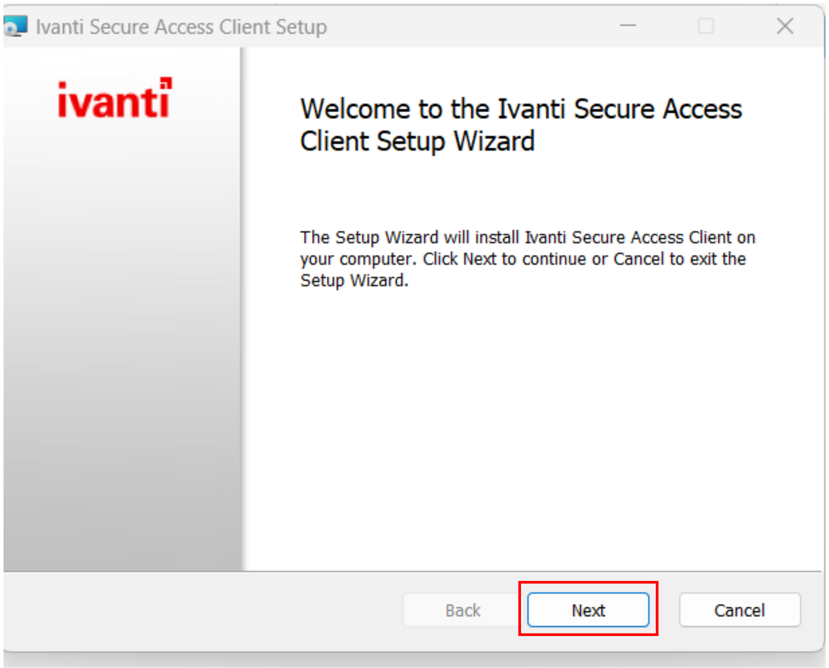
4.2 Using Windows extraction method



4.3 Image of installer file once unzipped:



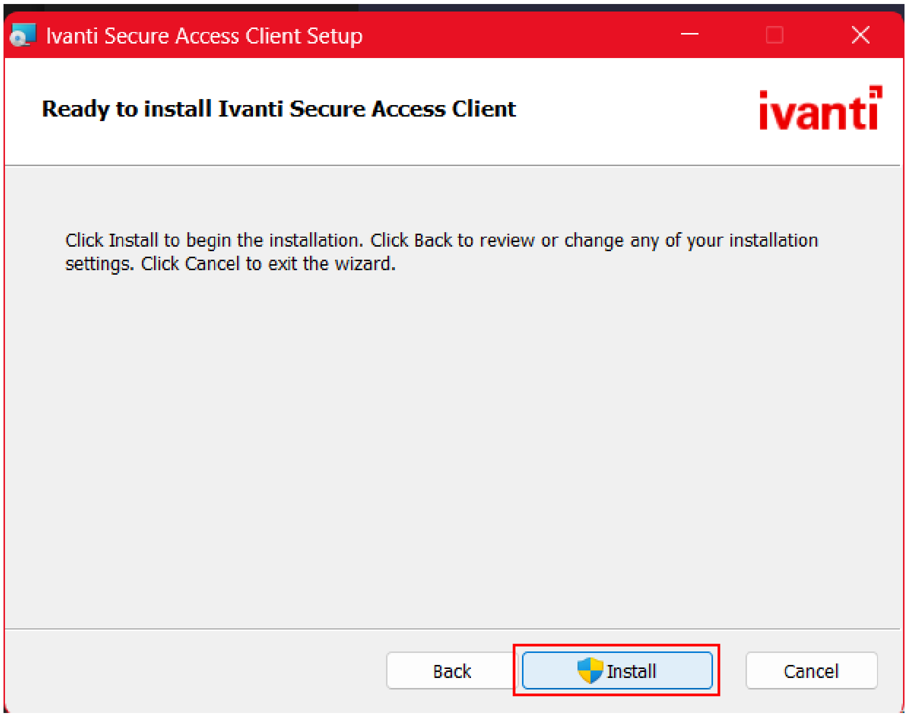
5. Click the extracted package, to start the installation process.
6. Click **Next** on the Ivanti Secure Access Client Setup Wizard screen, as shown below:



Welcome to the Ivanti Secure Access Client Setup Wizard

The Setup Wizard will install Ivanti Secure Access Client on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

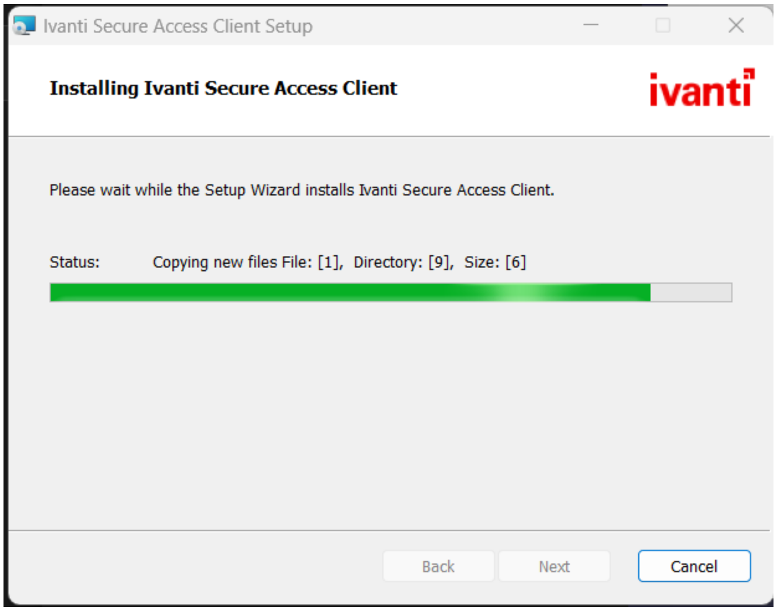
7. Then, click the **Install** button to start the installation.



Ready to install Ivanti Secure Access Client

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

7.1 Installation in progress Below is an image of installation in progress :

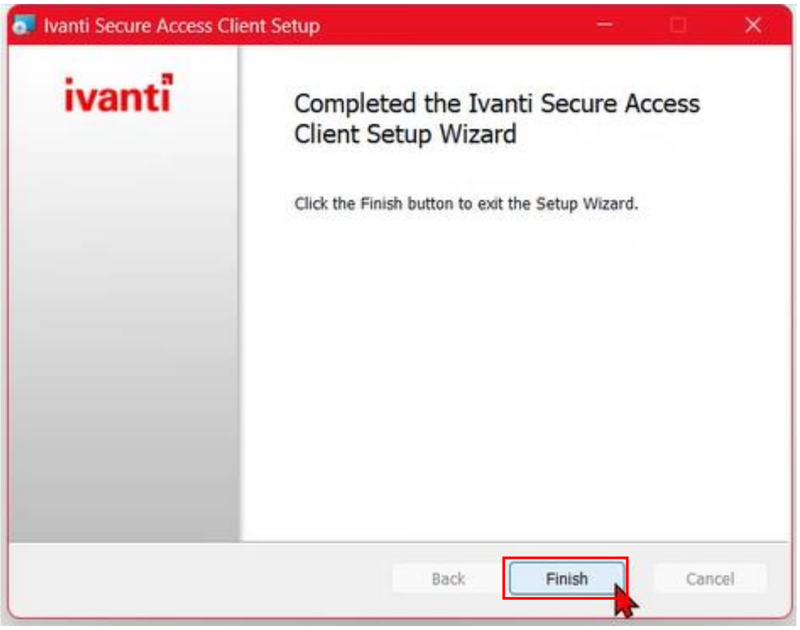


Installing Ivanti Secure Access Client

Please wait while the Setup Wizard installs Ivanti Secure Access Client.

Status: Copying new files File: [1], Directory: [9], Size: [6]

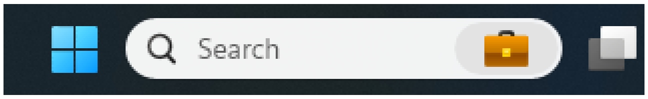
8. Click on Finish when the installation status is completed.



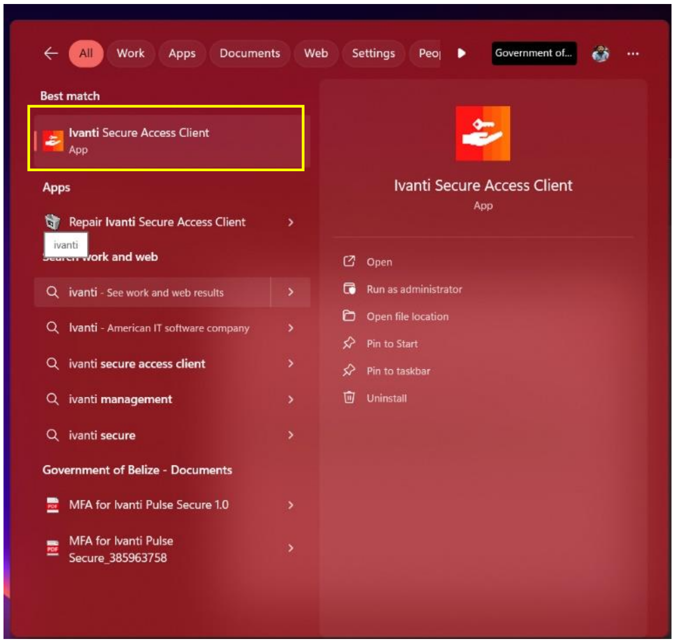
Completed the Ivanti Secure Access Client Setup Wizard

Click the Finish button to exit the Setup Wizard.

9. On a Laptop/ Desktop device, use the Windows search tab (image below) to type the keyword ***Ivanti.***

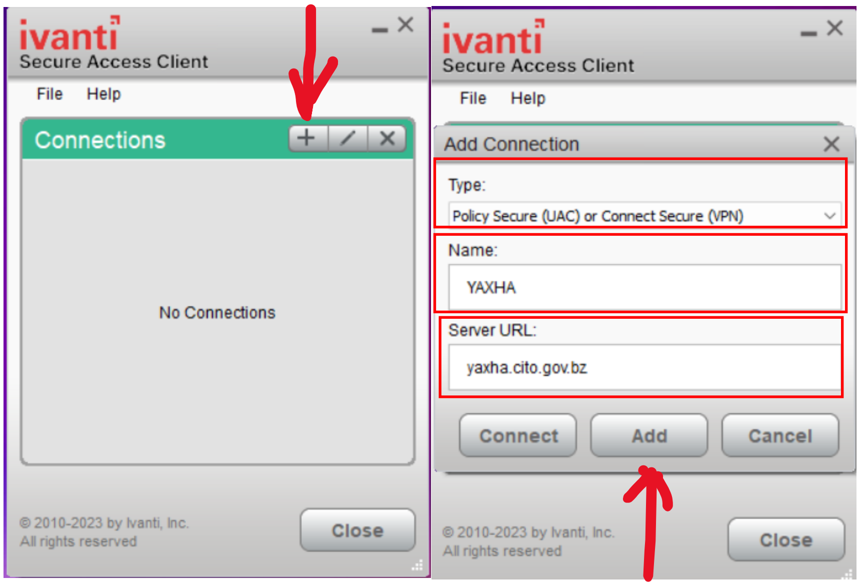


10. From the search results, click on the app **Ivanti Secure Access Client** to Open. See below:



All
Work
Apps
Documents
Web
Settings
Peo
Government of...
Best match
Ivanti Secure Access Client
App
Apps
Repair Ivanti Secure Access Client
ivanti
Search work and web
ivanti - See work and web results
Ivanti - American IT software company
ivanti secure access client
ivanti management
ivanti secure
Government of Belize - Documents
MFA for Ivanti Pulse Secure 1.0
MFA for Ivanti Pulse Secure_385963758
Ivanti Secure Access Client
App
Open
Run as administrator
Open file location
Pin to Start
Pin to taskbar
Uninstall

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

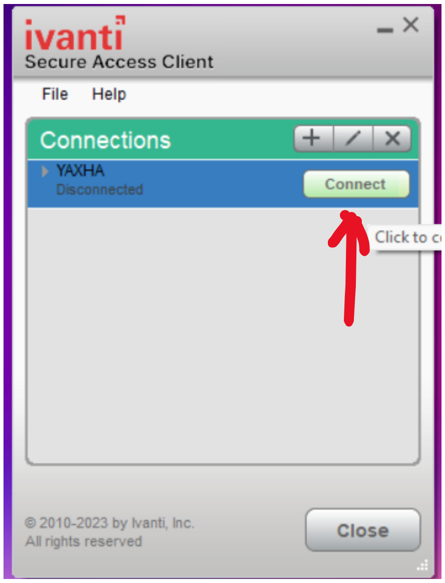


Type: Policy Secure (UAC) or Connect Secure (VPN)

Name: YAXHA

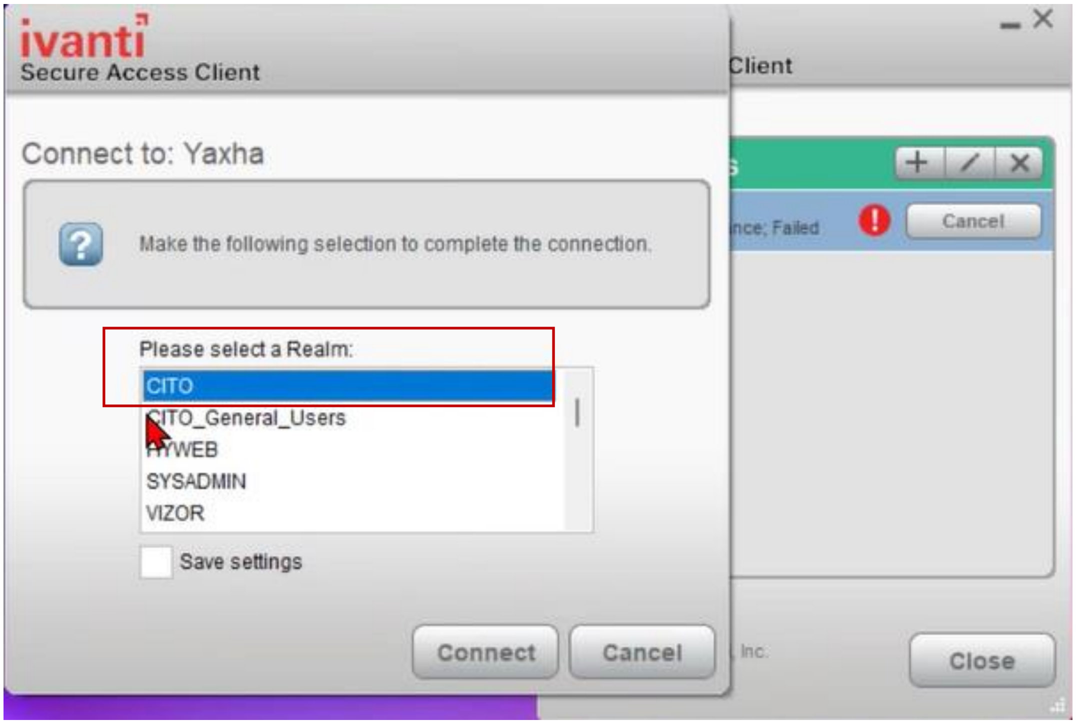
Server URL: yaxha.cito.gov.bz

12. To establish session, click “Connect” and Ivanti Secure Access Client will check if your laptop/desktop device is compliant.



13. Host Check plugin will run and verify that laptop/ desktop device 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.

Seeing the below image indicates that your machine has passed the compliance test and is ready to proceed with the MFA setup.



Connect to: Yaxha

Make the following selection to complete the connection.

Please select a Realm:

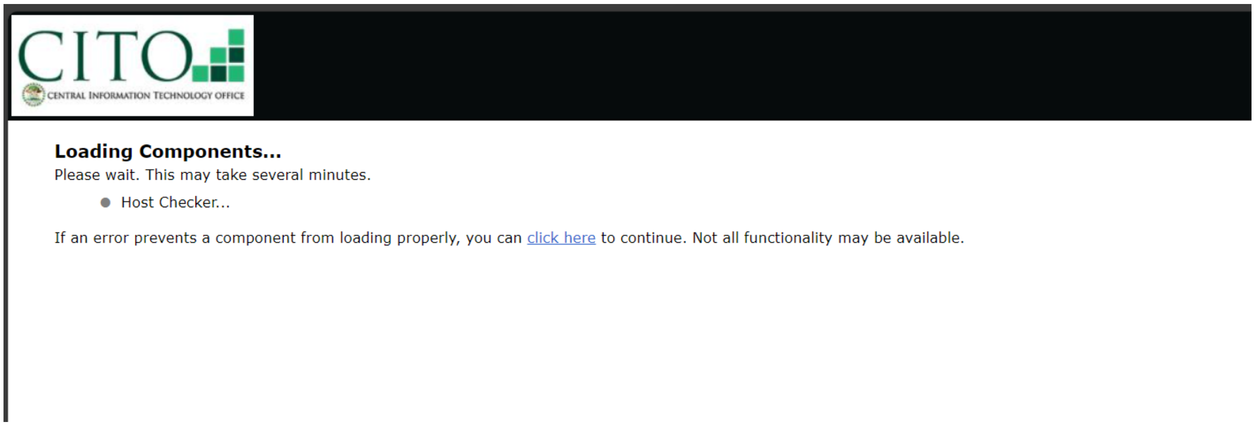
CITO
CITO_General_Users
HYWEB
SYSADMIN
VIZOR

□ Save settings

14. Click the Cancel button to proceed to setup the MFA configuration.

2 CITO VPN with MFA

1. Using an internet browser (e.g. Microsoft Edge or Google Chrome) head over to yaxha.cito.gov.bz to enable your MFA. The host checker will run to verify all is in order with your laptop/desktop device laptop/desktop device.



Loading Components...

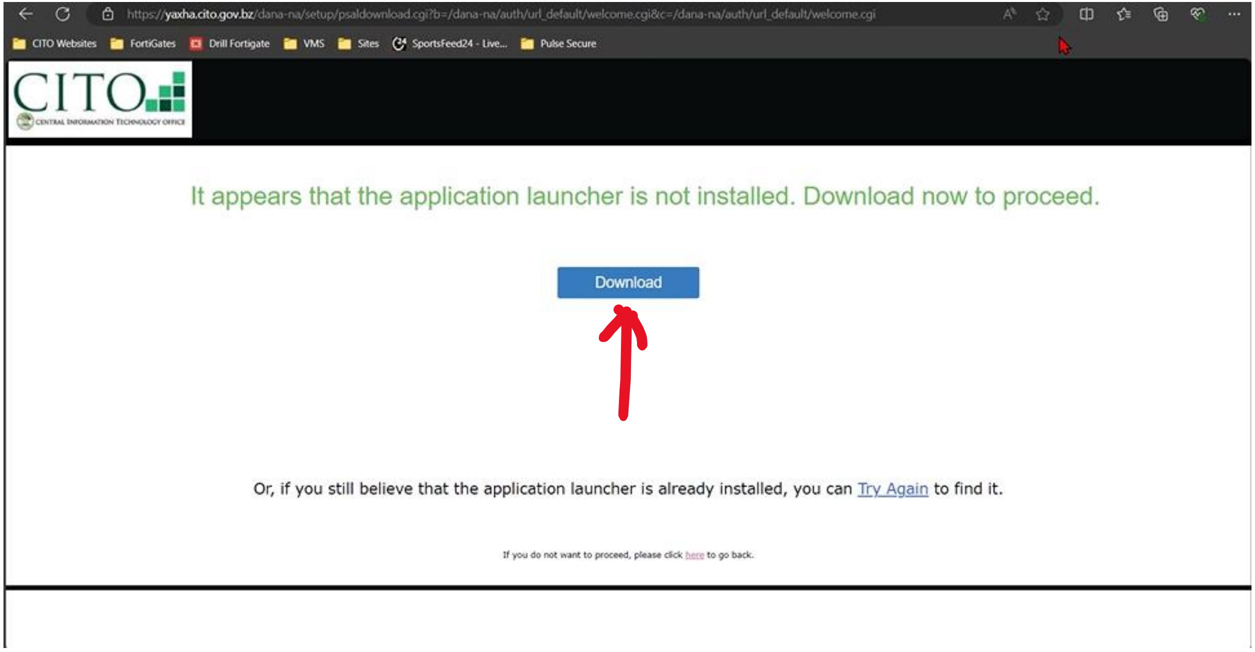
Please wait. This may take several minutes.

- Host Checker...

If an error prevents a component from loading properly, you can click here to continue. Not all functionality may be available.

Thereafter it will ask for you to download the host checker application.

2. Kindly proceed with downloading by clicking the Download button:



https://yaxha.cito.gov.bz/dana-na/setup/psaldownload.cgi?b=/dana-na/auth/url_default/welcome.cgi&c=/dana-na/auth/url_default/welcome.cgi
CITO Websites
FortiGates
Drill Fortigate
VMS
Sites
SportsFeed24 - Live...
Pulse Secure
CITO
CENTRAL INFORMATION TECHNOLOGY OFFICE
Download

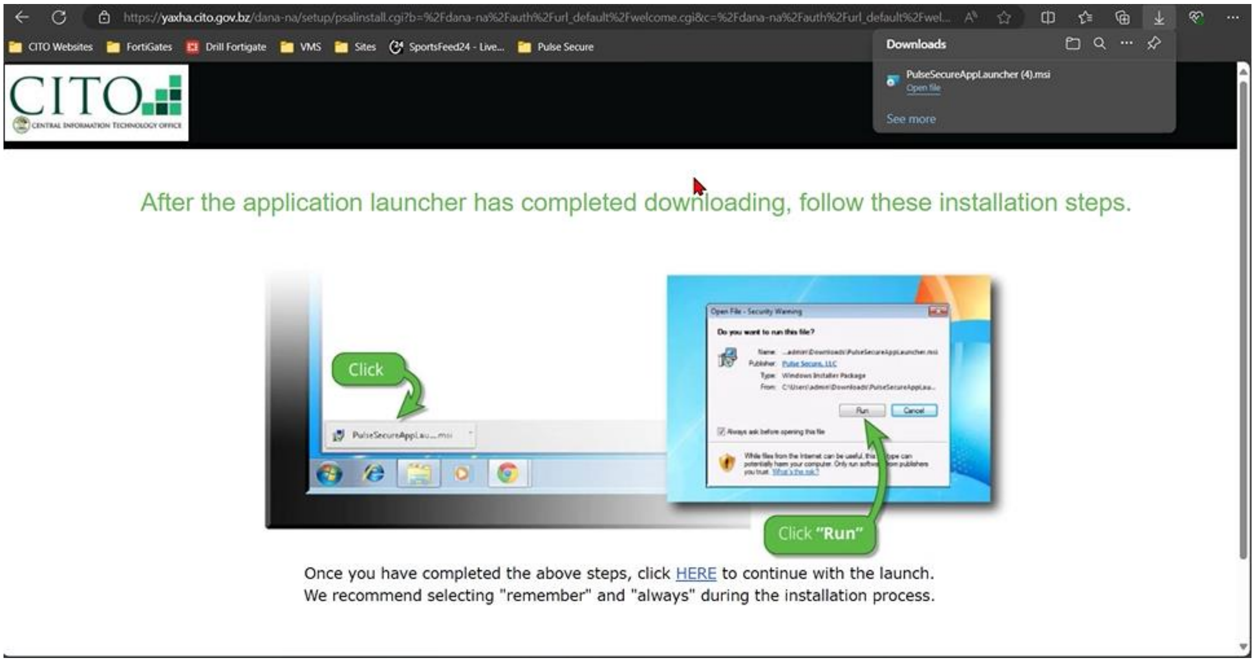
It appears that the application launcher is not installed. Download now to proceed.

Or, if you still believe that the application launcher is already installed, you can Try Again to find it.

If you do not want to proceed, please click here to go back.

It should start downloading in the browser. You are also given a download help page to assist to inform on what the next step should be.
We recommend being cognizant of this screen as you shall return to this help page further in the installation.

Upon clicking the Download button the screen will display as shown below:

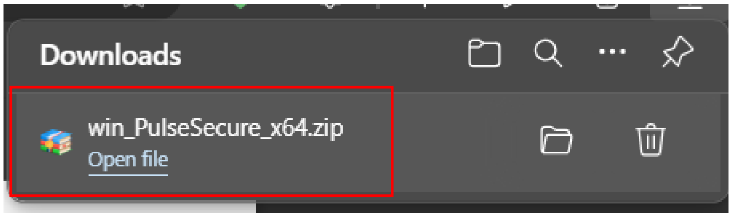

https://yaxha.cito.gov.bz/dana-na/setup/psalinstall.cgi?b=%2Fdana-na%2Fauth%2Furl_default%2Fwelcome.cgi&c=%2Fdana-na%2Fauth%2Furl_default%2Fwel...
CITO Websites
FortiGates
Drill Fortigate
VMS
Sites
SportsFeed24 - Live...
Pulse Secure
Downloads
PulseSecureAppLauncher (4).msi
Open file
See more
CITO
CENTRAL INFORMATION TECHNOLOGY OFFICE
Click
Click "Run"

After the application launcher has completed downloading, follow these installation steps.

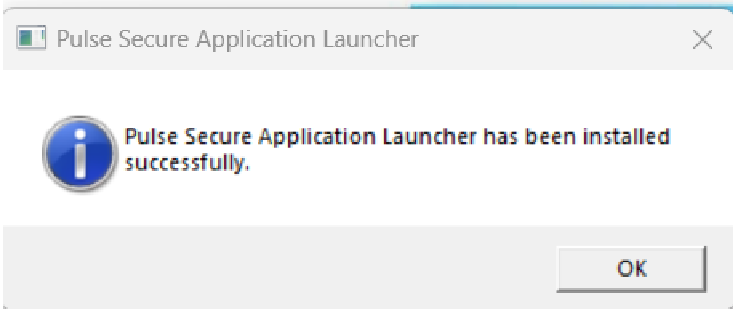
Once you have completed the above steps, click HERE to continue with the launch.
We recommend selecting "remember" and "always" during the installation process.

It downloads needed executables to now configure multi-factor authentication (MFA).

3. To verify installation, when download has been completed, click on the Open file option.



When completed, the screen indicates the installation status as illustrated below:



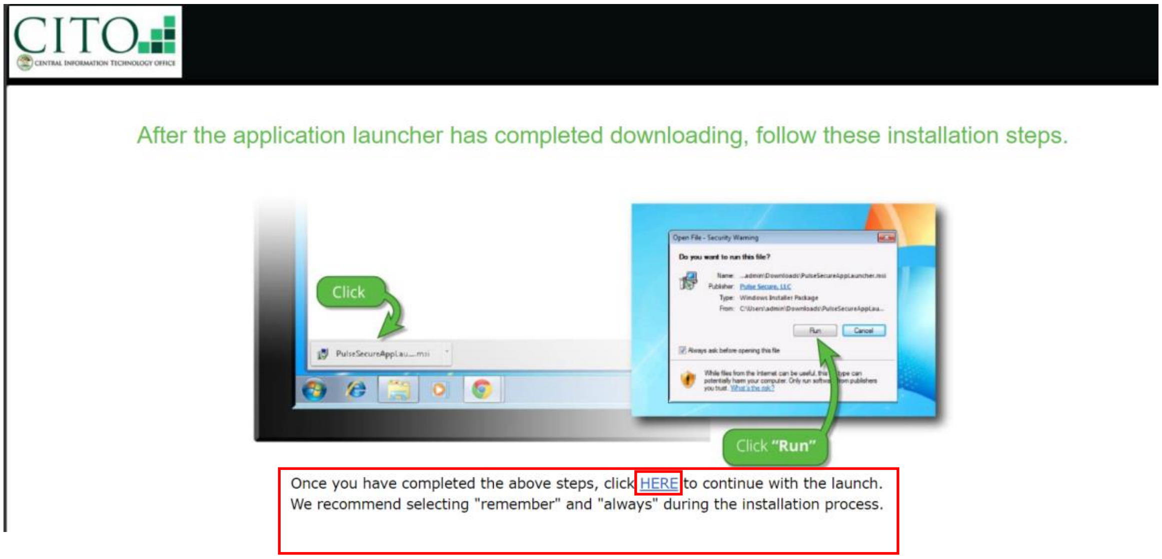
Pulse Secure Application Launcher has been installed successfully.

4. Click the OK button to proceed.

At the bottom of the downloader page, you will see the actual sentence:

“ Once you have completed the above steps, click the **HERE** link to continue with the launch.

We recommend selecting remember” and “always” during the installation process. ”



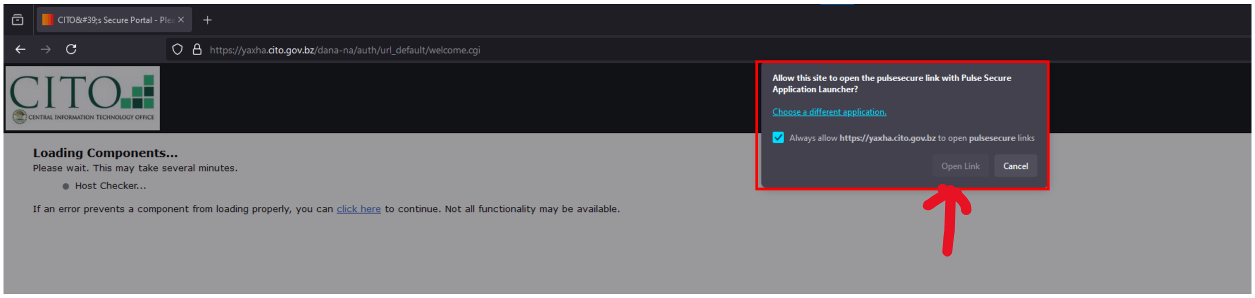
CITO
CENTRAL INFORMATION TECHNOLOGY OFFICE
Click
PulseSecureAppLau....msi
Open File - Security Warning
Do you want to run this file?
Name: ...admin\Downloads\PulseSecureAppLauncher.msi
Publisher: Pulse Secure, LLC
Type: Windows Installer Package
From: C:\Users\admin\Downloads\PulseSecureAppLau...
Run
Cancel
Always ask before opening this file
What's the risk?
Click “Run”

After the application launcher has completed downloading, follow these installation steps.

Once you have completed the above steps, click HERE to continue with the launch.
We recommend selecting "remember" and "always" during the installation process.

5. Kindly proceed with the clicking “HERE” and the pop up to always “remember” and “always” during installation will appear.

Always allow screen:


CITO&#39;s Secure Portal - Plea
https://yaxha.cito.gov.bz/dana-na/auth/url_default/welcome.cgi
CITO
CENTRAL INFORMATION TECHNOLOGY OFFICE
Choose a different application.
Open Link
Cancel

Allow this site to open the pulsesecure link with Pulse Secure Application Launcher?

☑ Always allow **https://yaxha.cito.gov.bz** to open **pulsesecure** links

Loading Components...

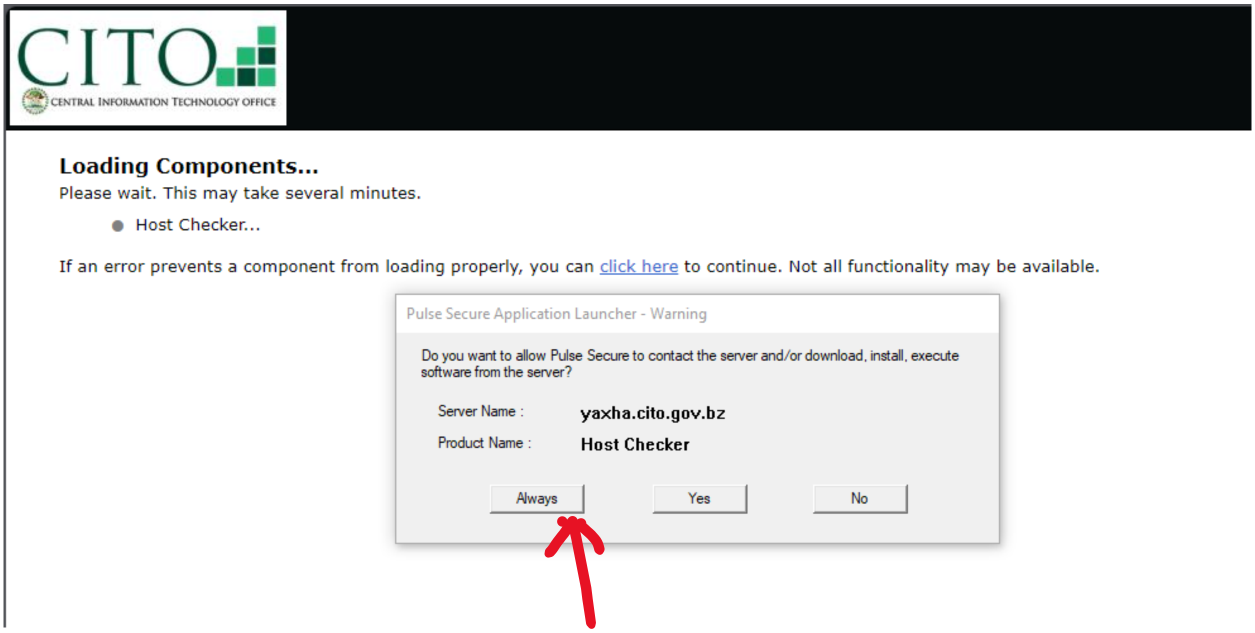
Please wait. This may take several minutes.

- Host Checker...

If an error prevents a component from loading properly, you can click here to continue. Not all functionality may be available.

The screen above may not always appear. It is included to guide if you are prompted with it.

6. Next, choose the Always option as shown below to proceed with the installation:



Loading Components...

Please wait. This may take several minutes.

- Host Checker...

If an error prevents a component from loading properly, you can click here to continue. Not all functionality may be available.

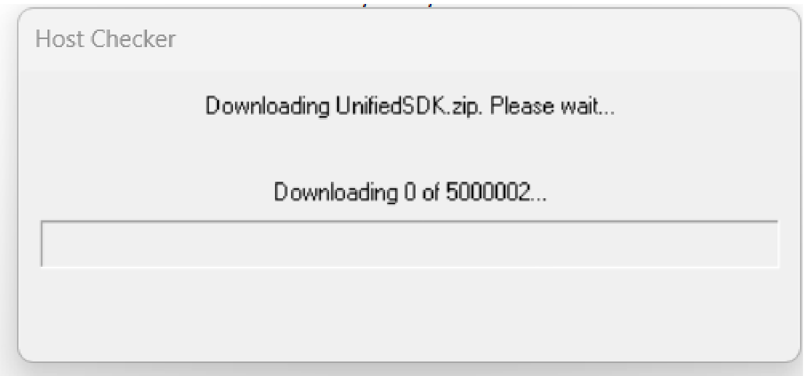
Pulse Secure Application Launcher - Warning

Do you want to allow Pulse Secure to contact the server and/or download, install, execute software from the server?

Server Name : yaxha.cito.gov.bz

Product Name : Host Checker

Host checker then executes again to complete all necessary downloads. A user may or may not see this screen as it downloads quickly.

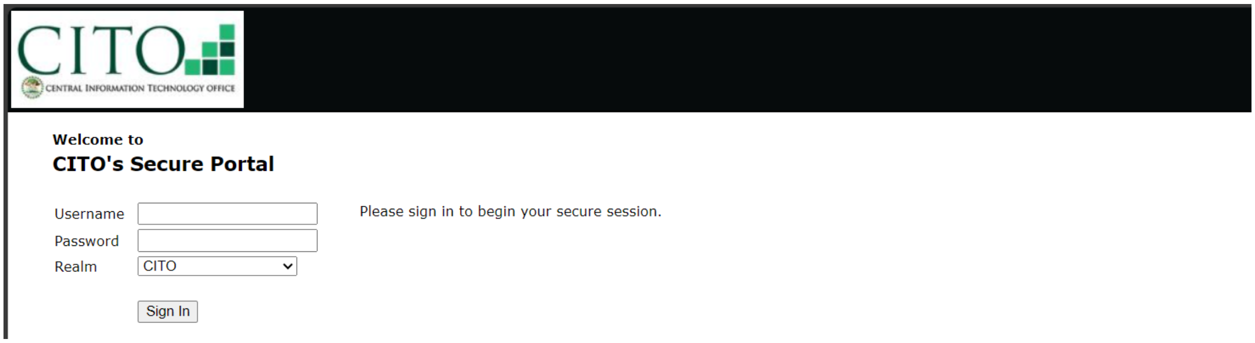


Host Checker

Downloading UnifiedSDK.zip. Please wait...

Downloading 0 of 5000002...

Having completed all previous steps, you will now gain access to the Yaxha sign in page seen below:



Welcome to
CITO's Secure Portal

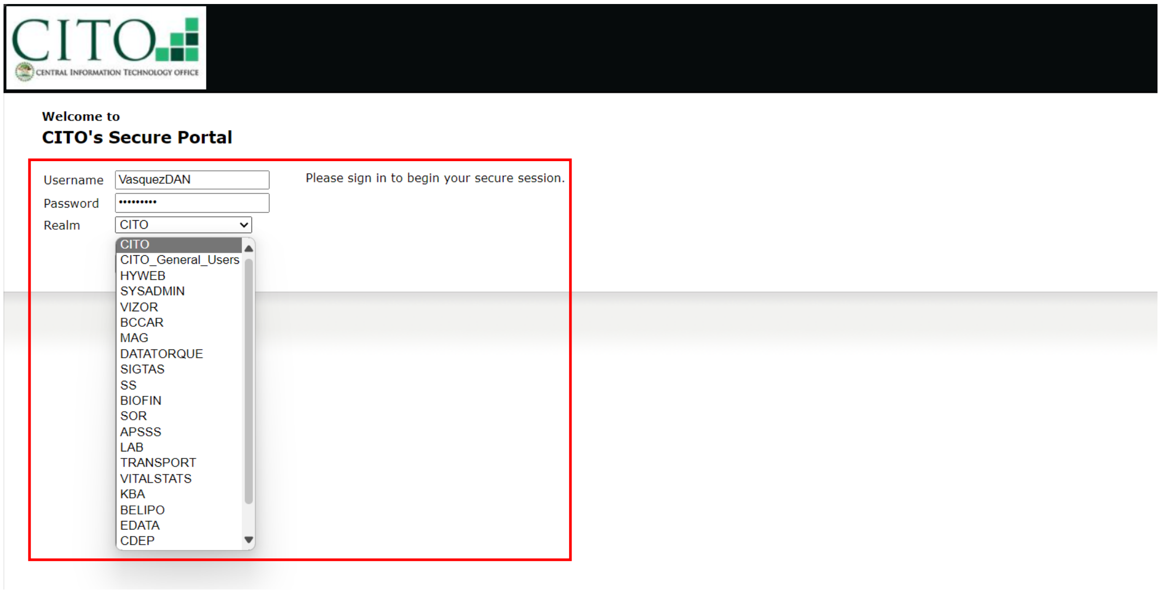
Username
Password
Realm CITO

Please sign in to begin your secure session.

7. Kindly enter your account login information as well as ensuring you are connecting by selecting the correct realm.

N.B. [Use the received realm instruction to determine which realm to connect to from your email.]

For this example, we will be connecting to the CITO Realm, hence, CITO is selected below:



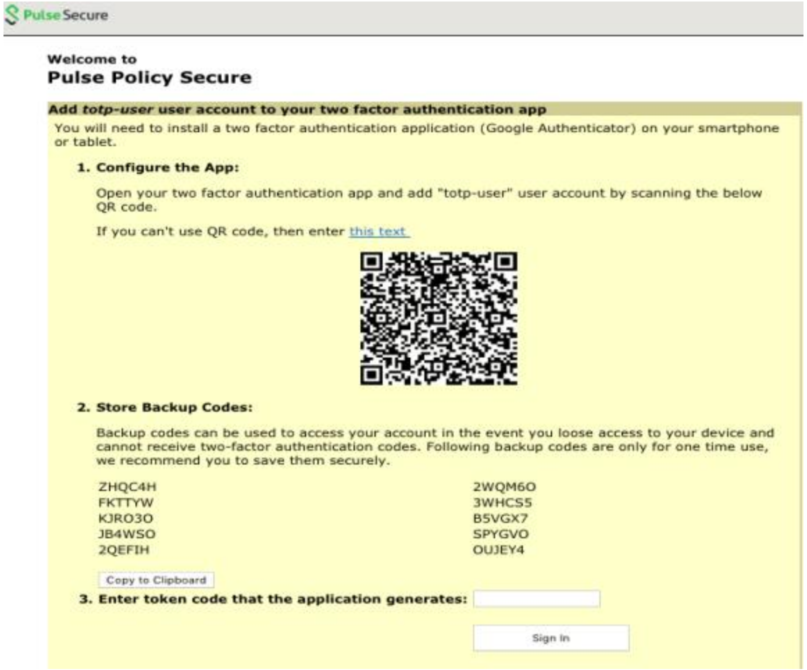
Welcome to
CITO's Secure Portal

Username VasquezDAN
Password •••••••••
Realm CITO

Please sign in to begin your secure session.

Upon successful login, you will then be directed to the Pulse Policy Secure page. If you are seeing options to configure the app using a QR code, and another instruction involving “Store Backup Codes”, stop here for now and prepare to configure your authenticator.

Pulse Policy Secure Page:



Pulse Secure

Welcome to
Pulse Policy Secure

Add *totp-user* user account to your two factor authentication app

You will need to install a two factor authentication application (Google Authenticator) on your smartphone or tablet.

1. Configure the App:

Open your two factor authentication app and add "totp-user" 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.

ZHQC4H
FKTTYW
KJRO3O
JB4WSO
2QEFIH
2WQM6O
3WHCS5
B5VGX7
SPYGVO
OUJEY4

Copy to Clipboard

3. Enter token code that the application generates:

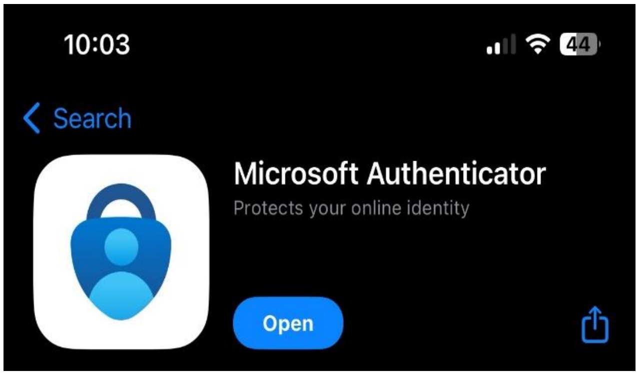
Sign In

3 Authenticator configuration

Ensure that you have the authenticator app downloaded on your device to act as the second verification for multi-factor authentication.

1. On your phone, go to your Appstore (for Mac) or Play Store (for Android) and look for the Microsoft Authenticator app. When found, select the Get or Install option to install.

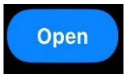
Image of Authenticator:



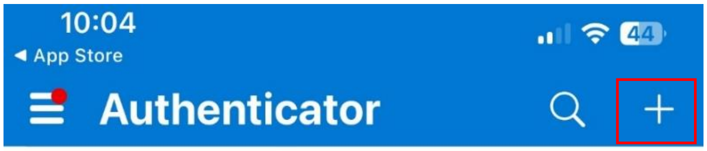
10:03

Microsoft Authenticator

Protects your online identity

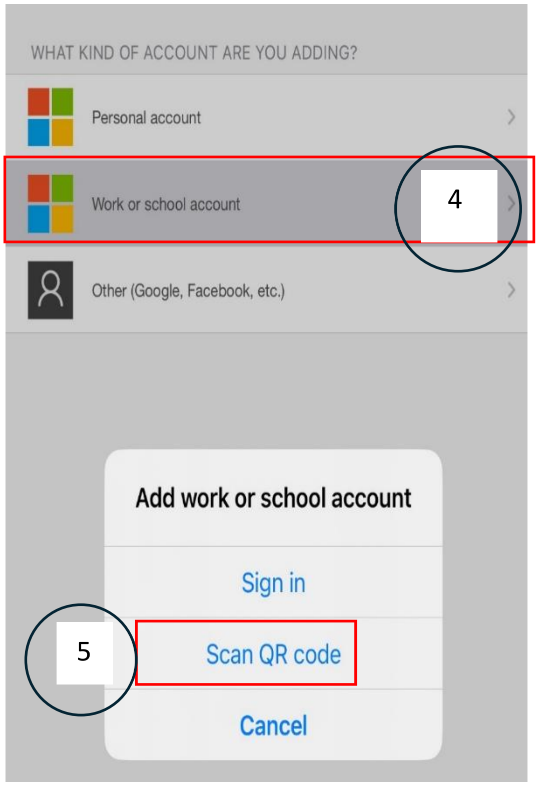
2. Click  to launch the authenticator app after installation.

3. In the authenticator app, click on the + button on the top right corner to scan the new QR code.

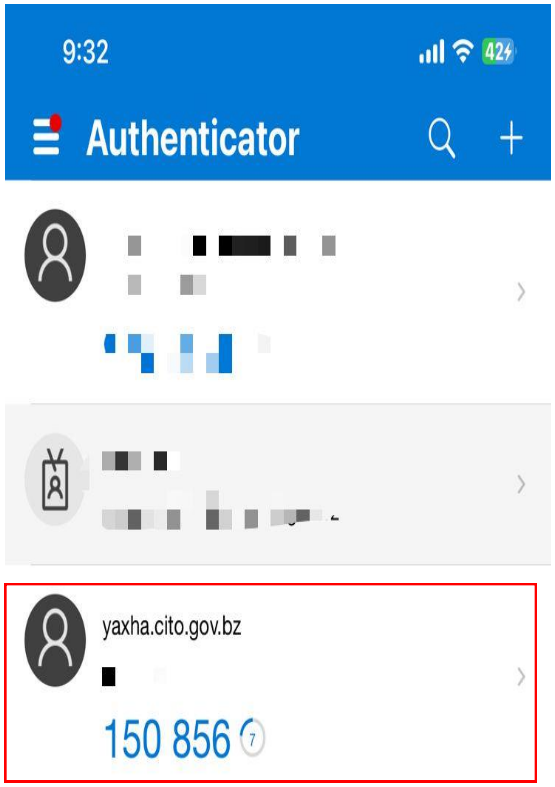


4. Next, select the Work of School account option
5. Select, Scan QR code.

(In this instance we are selecting the Work or school account option)


WHAT KIND OF ACCOUNT ARE YOU ADDING?
Personal account
Work or school account
4
Other (Google, Facebook, etc.)
Add work or school account
Sign in
5
Scan QR code
Cancel

A successful QR Code scan would result in a Yaxha entry to be visible from your Authenticator App list as highlighted below:



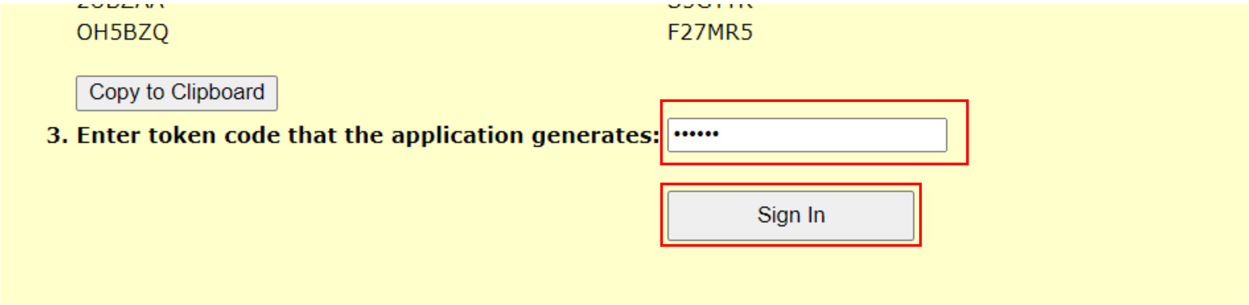
[redacted]

[redacted]

yaxha.cito.gov.bz
[redacted]
150 856

With this Yaxha entry, a new number code is generated for use. **[Expires and renews every 30 seconds]**

6. Go back to the Pulse Policy Secure Page and enter the valid number code shown in Microsoft Authenticator, as shown below.
7. Then, click the Sign In button.



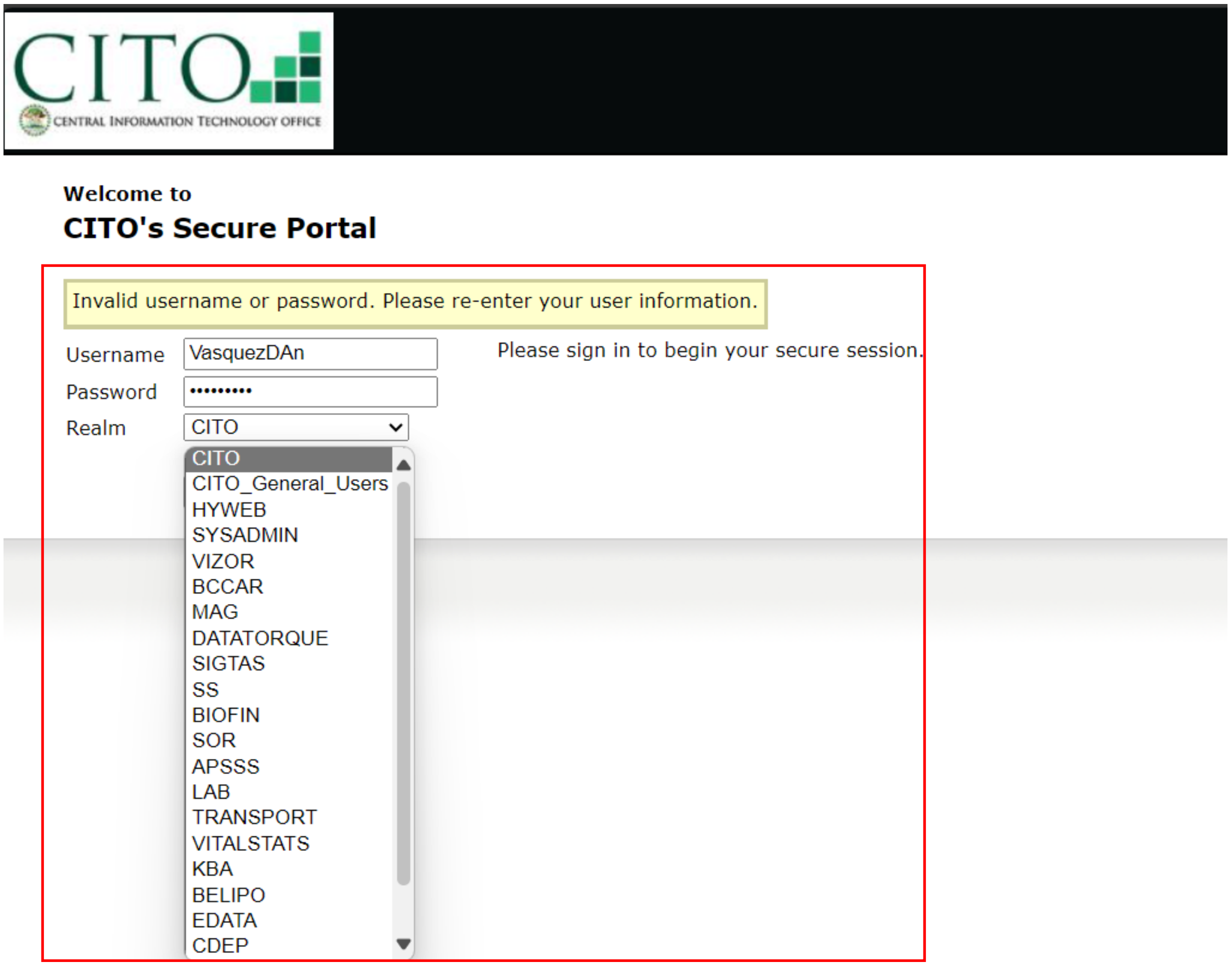
OH5BZQ F27MR5

Copy to Clipboard

3. Enter token code that the application generates: ••••••

Sign In

8. Refresh your browser to go back to the Yaxha login page.
9. Once on the login page, enter your login information and select the correct realm.



Welcome to
CITO's Secure Portal

Invalid username or password. Please re-enter your user information.

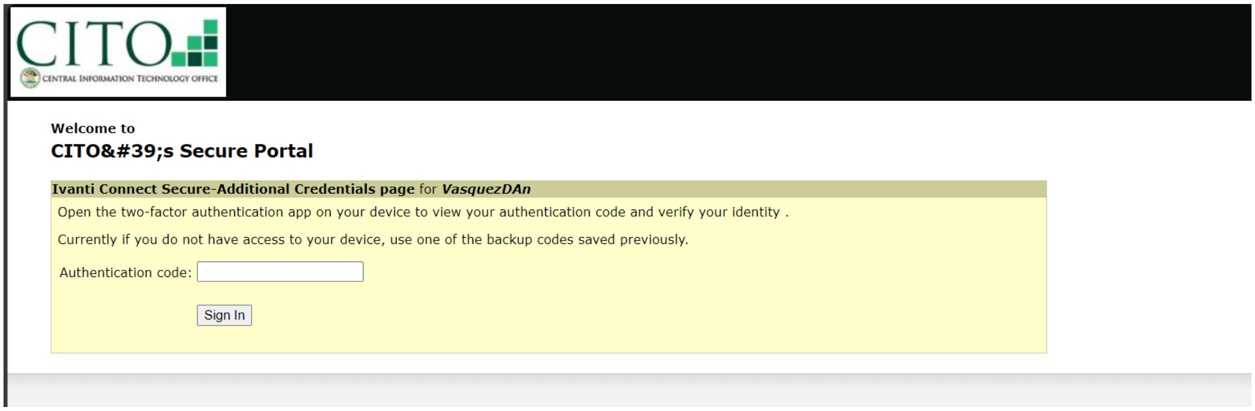
Username VasquezDAn

Password •••••••••

Realm CITO

Please sign in to begin your secure session.

You will be taken to the page where it asks for you to enter your number code once again. If you have arrived this far, your MFA has been set up for your account.



Welcome to
CITO&#39;s Secure Portal

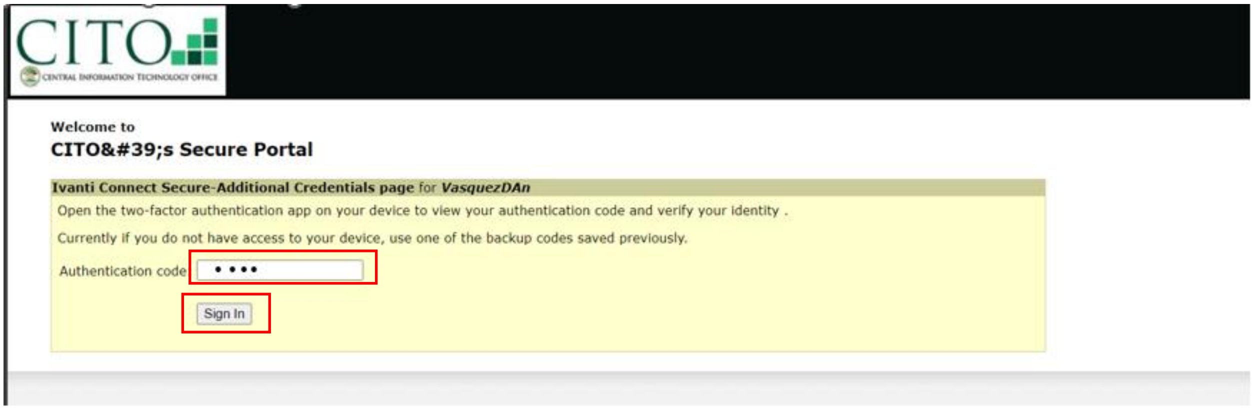
Ivanti Connect Secure-Additional Credentials page for ***VasquezDAn***

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.

Authentication code:

10. Go to the authenticator app for a valid number code and enter it into the authentication code window.
11. Then, click the sign in button.



Welcome to
CITO&#39;s Secure Portal

Ivanti Connect Secure-Additional Credentials page for ***VasquezDAn***

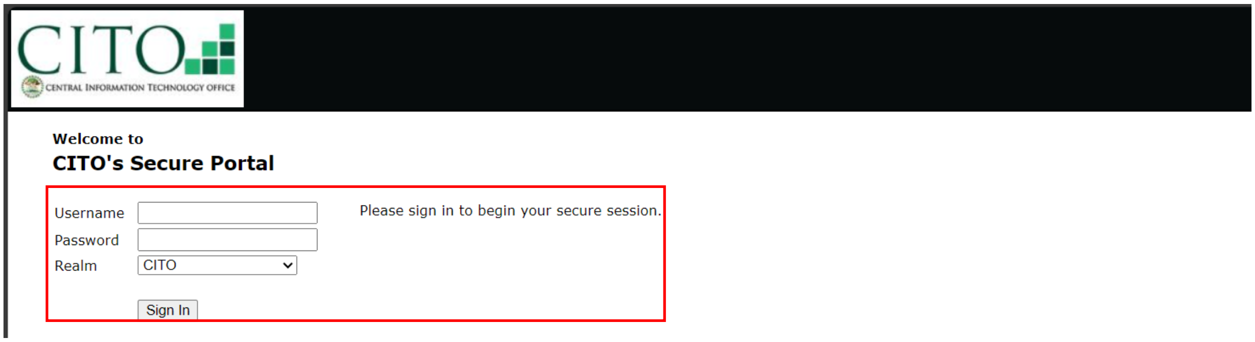
Open the two-factor authentication app on your device to view your authentication code and verify your identity .

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

Authentication code: ••••

This will take you to the secure page login to resubmit your login.

12. Once more, enter your login information.

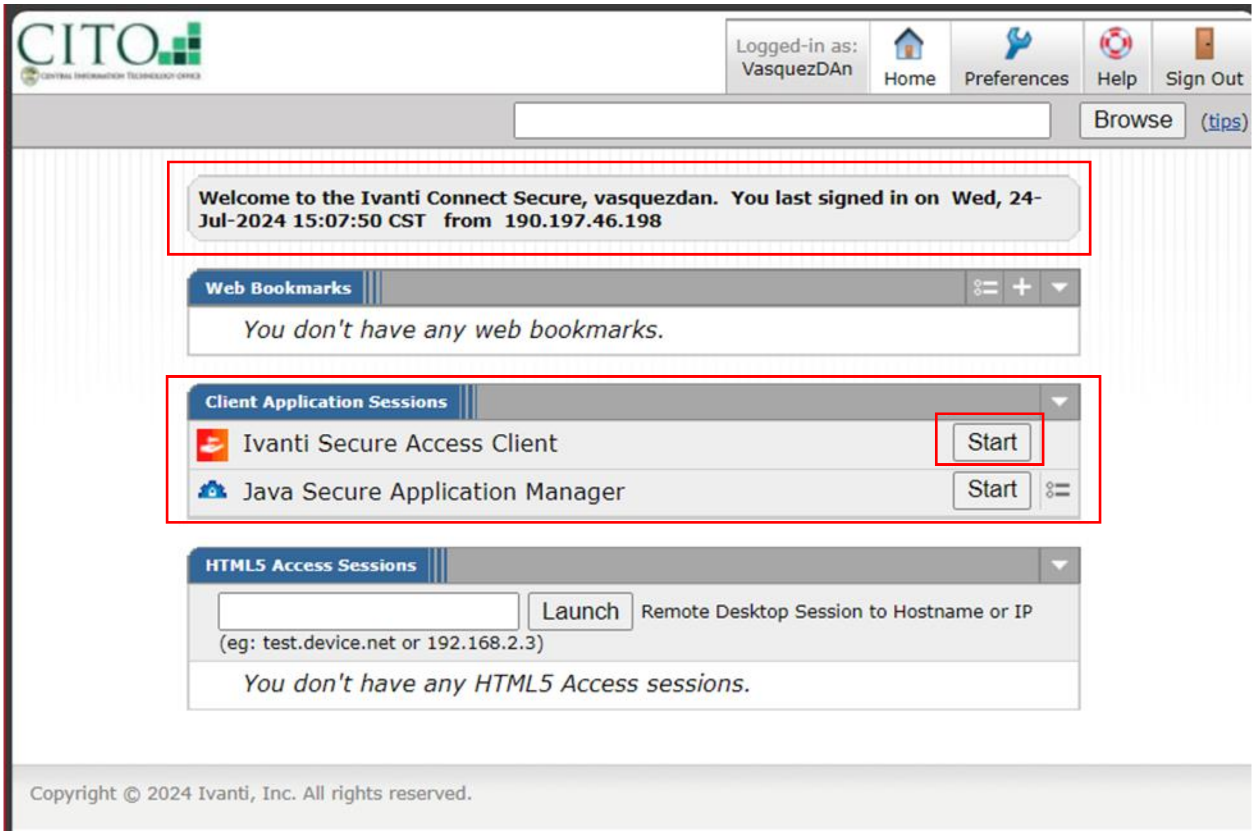


Welcome to
CITO's Secure Portal

Username
Password
Realm: CITO

Please sign in to begin your secure session.

Successfully logging into the CITO's Secure Portal page will take you to your session log (this has where your last VPN sign in information is kept.) as shown below:



Welcome to the Ivanti Connect Secure, vasquezdan. You last signed in on Wed, 24-Jul-2024 15:07:50 CST from 190.197.46.198

You don't have any web bookmarks.

Ivanti Secure Access Client

Java Secure Application Manager

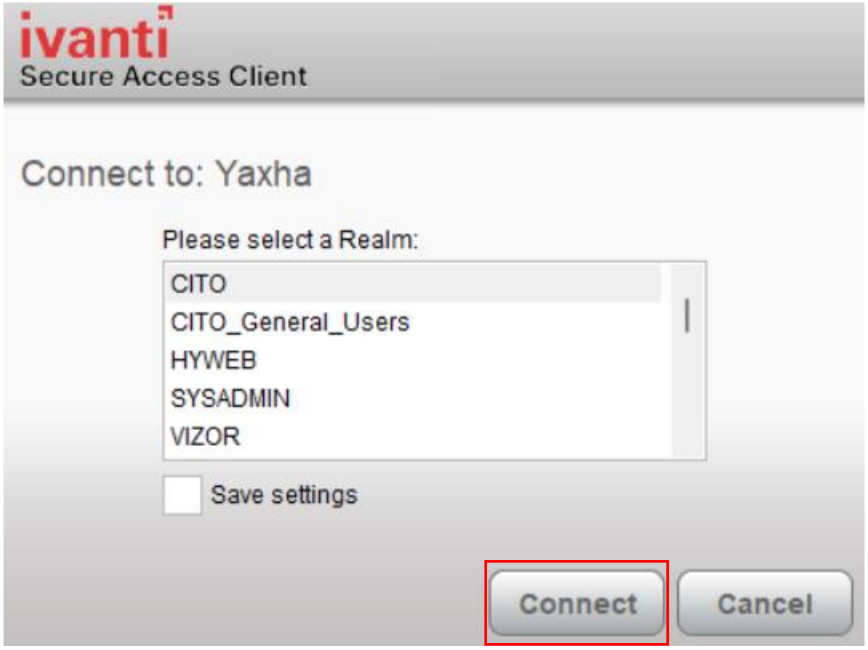
Remote Desktop Session to Hostname or IP (eg: test.device.net or 192.168.2.3)

You don't have any HTML5 Access sessions.

Copyright © 2024 Ivanti, Inc. All rights reserved.

13. Under Client Application Sessions for Ivanti Secure Access Client, click the Start button to gain access to the Ivanti login page.

Image of Ivanti Login page:



Connect to: Yaxha

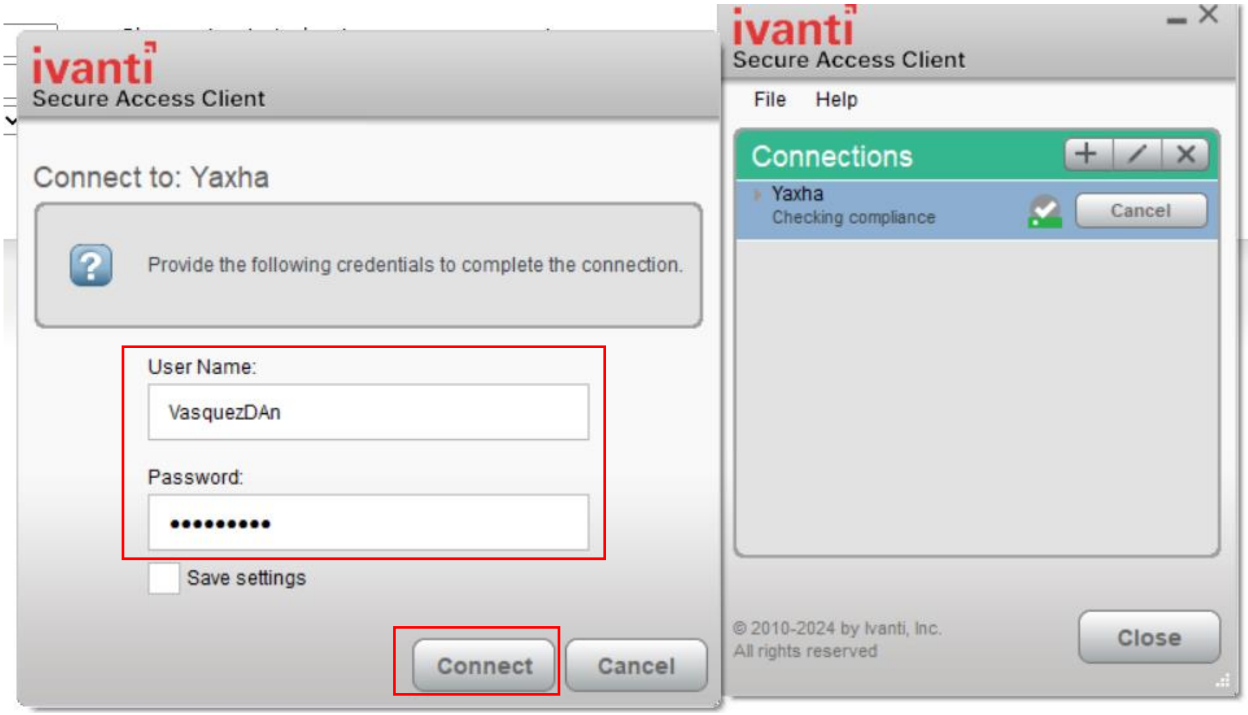
Please select a Realm:

- CITO
- CITO_General_Users
- HYWEB
- SYSADMIN
- VIZOR

□ Save settings

14. Select the Realm from the list and click the Connect button to proceed.

When the Login page is presented, enter your login credentials and click the connect button



Connect to: Yaxha

Provide the following credentials to complete the connection.

User Name: VasquezDAn

Password: ••••••••••

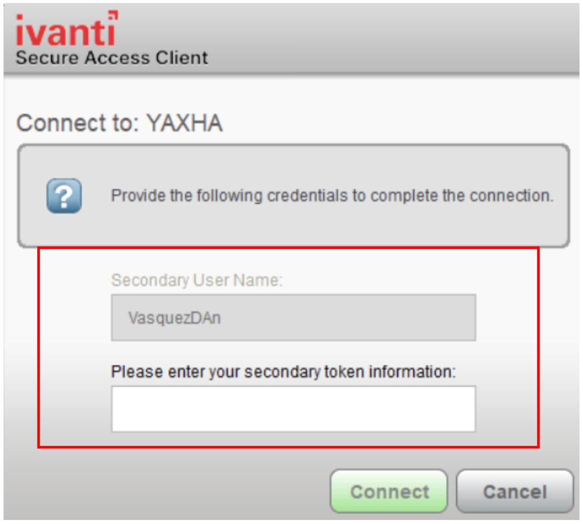
□ Save settings

Yaxha
Checking compliance

© 2010-2024 by Ivanti, Inc.
All rights reserved

15. For first-time configuration setup, upon successful login, you will be asked to enter your secondary number code information. To complete, go to the authenticator app to get a valid number code and enter the code in the secondary token window.

Image of successful login being prompted by MFA validation to enter secondary number code from authenticator app:



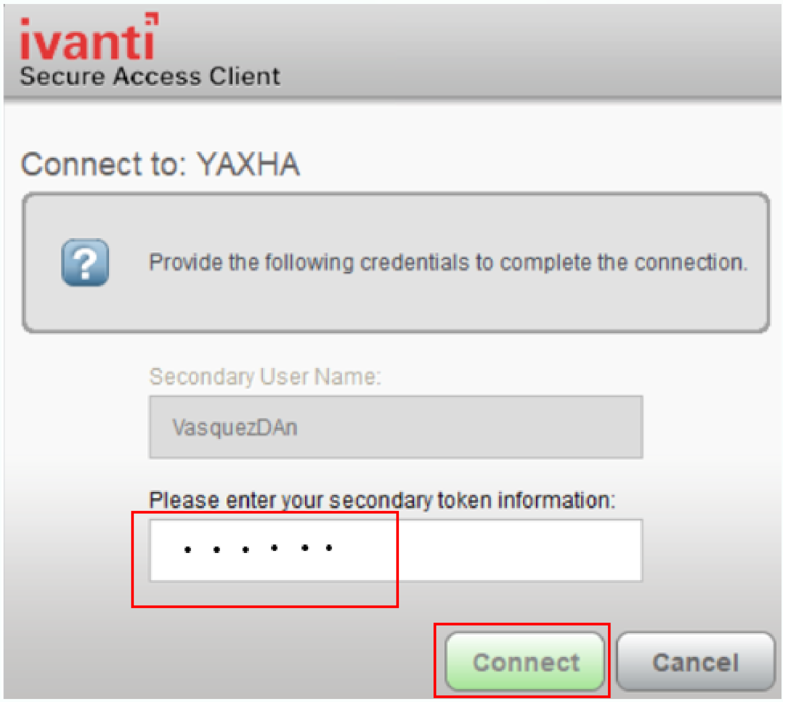
Connect to: YAXHA

Provide the following credentials to complete the connection.

Secondary User Name: VasquezDAn

Please enter your secondary token information:

16 Click the connect button to establish the VPN connection


ivanti Secure Access Client

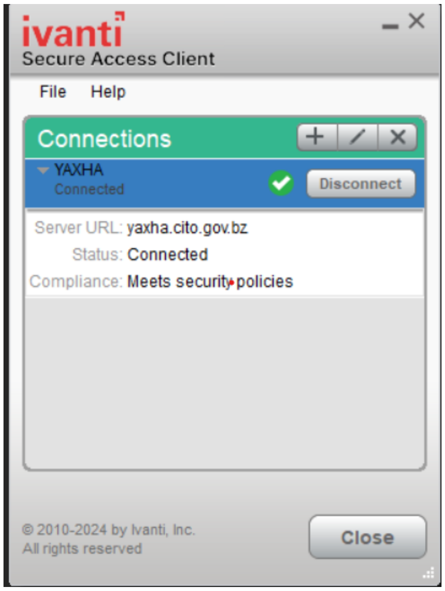
Connect to: YAXHA

Provide the following credentials to complete the connection.

Secondary User Name: VasquezDAn

Please enter your secondary token information: • • • • • •

Thereafter, you should be connected successfully as illustrated below:


ivanti Secure Access Client

YAXHA Connected

Server URL: yaxha.cito.gov.bz

Status: Connected

Compliance: Meets security policies

© 2010-2024 by Ivanti, Inc. All rights reserved

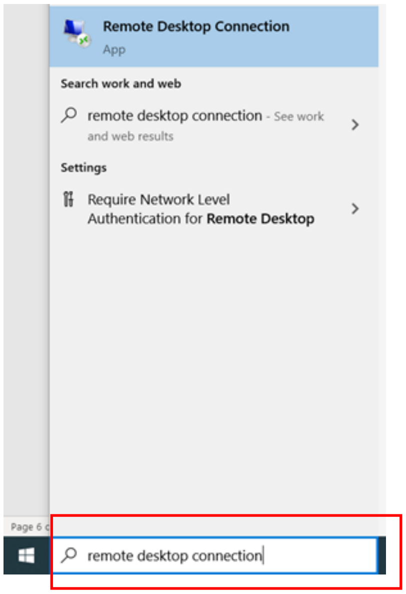
**Once you have successfully logged in there is no need to sign in back on the webpage and re-register your device over as it has already been registered. **

**Keep in mind that now when signing into your realm you will need to have the Microsoft authenticator app valid code readily available to sign in. **

4 Connecting to Your Machine (using RDP)

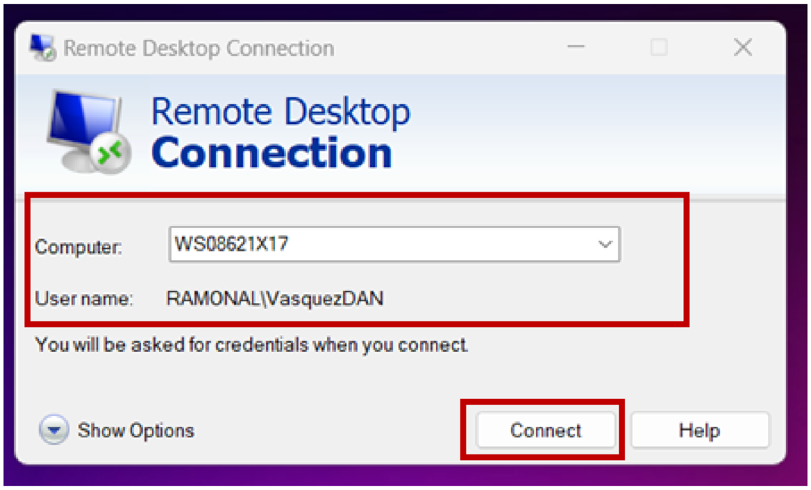
Once with successful login to MFA and Ivanti Yaxha connection showing a Connected status, do the following:

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


Remote Desktop Connection
App
Search work and web
remote desktop connection - See work and web results
Settings
Require Network Level Authentication for Remote Desktop
Page 6 c
remote desktop connection

2. Enter your workstation number.

N. B regarding ***Username***: Ensure that the username is correct before attempting to connect. Use the username provided by CITO's Network administrators. To proceed, click Connect.



Remote Desktop Connection

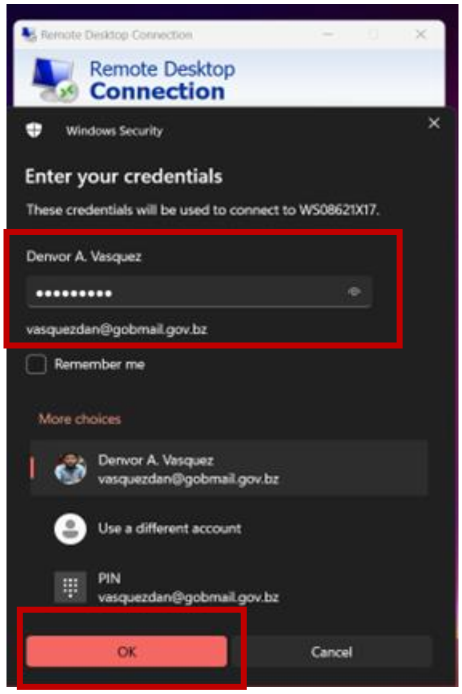
Remote Desktop Connection

Computer: WS08621X17

User name: RAMONAL\VasquezDAN

You will be asked for credentials when you connect.

3. Next, enter your credentials and click ok.



Remote Desktop Connection

Remote Desktop Connection

Windows Security

Enter your credentials

These credentials will be used to connect to WS08621X17.

Denvor A. Vasquez

••••••••••

vasquezdan@gobmail.gov.bz

□ Remember me

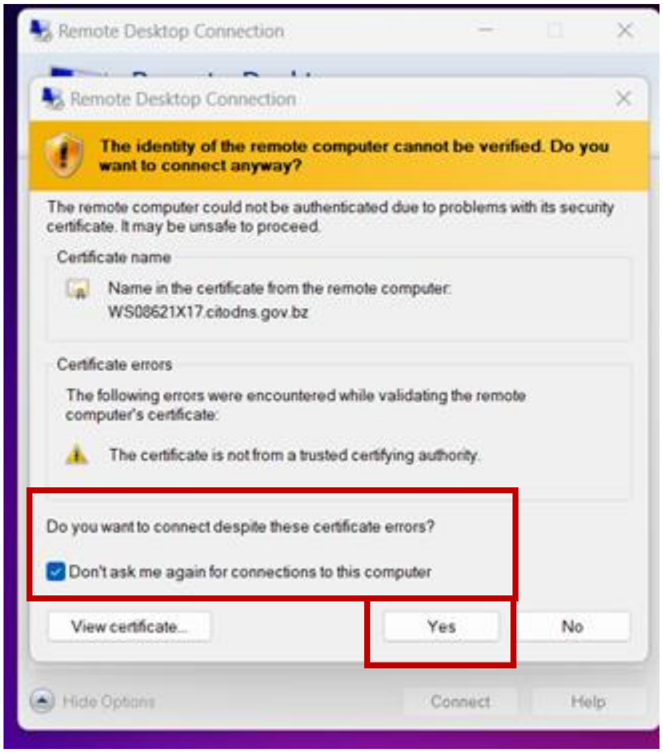
More choices

Denvor A. Vasquez
vasquezdan@gobmail.gov.bz

Use a different account

PIN
vasquezdan@gobmail.gov.bz

4. Upon receiving the Remote Desktop Connection Certificate Warning, User must kindly select the "Don’t ask me again for connections to this computer Check box as seen below.” subsequently click the ok button for validation verification



Remote Desktop Connection

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
WS08621X17.citodns.gov.bz

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

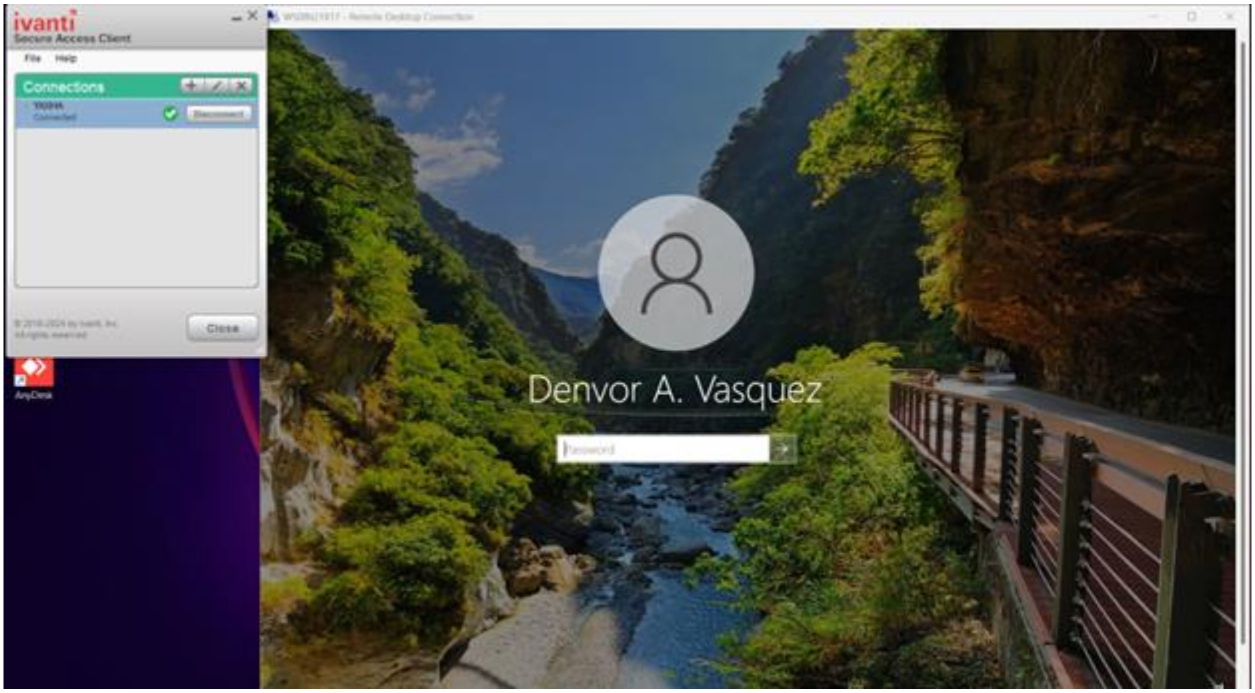
The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

☑ Don't ask me again for connections to this computer

Your teleworking is now successful.

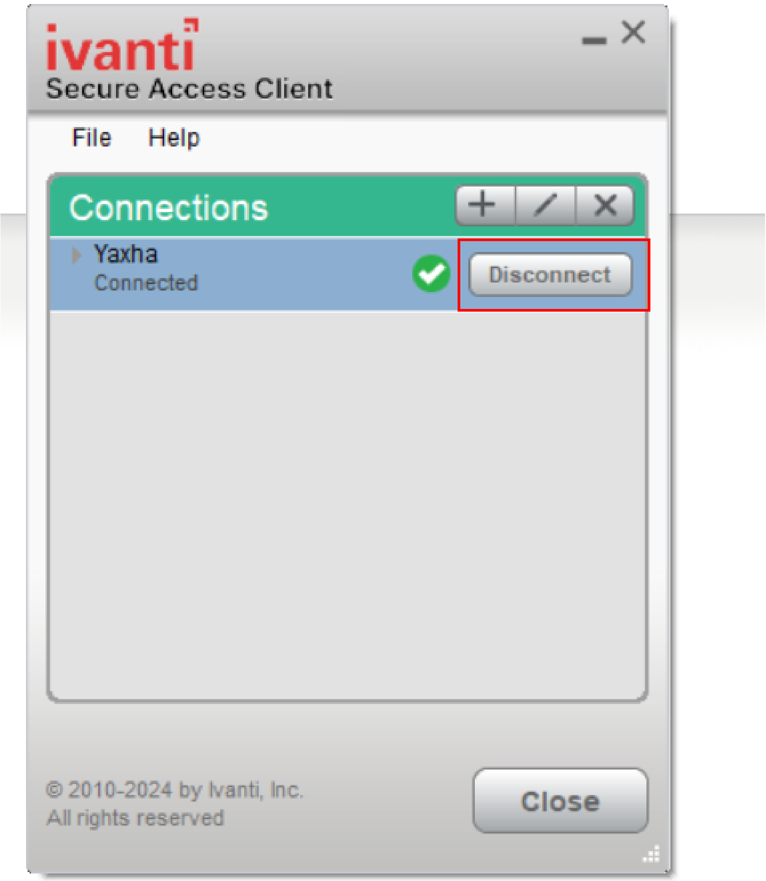
Kindly see connected workstation image with active VPN connection below:



5 Disconnecting a teleworking session

1. At end of your Teleworking session, click disconnect.

To disconnect, a user may click the Disconnect button from the Ivanti secure access as shown below:



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