PACS / VPN Installation and Log-in Guide

Table of Contents

Last Updated March 21, 2024

Overview

Background: eHS Multi Factor Authentication (MFA) is required to access the eHealth Saskatchewan (eHS) Virtual Private Network (VPN).

- o MFA adds a second layer of security to a customer's online account. Verifying their identity uses a second factor (*e.g., their personal cell phone - home/work*) to prevent anyone but them from logging in, even if that person knows their password.

2. Log in steps to follow which involve MFA:

  - o The customer enters domain\username and password at the login screen.
  - o The customer's cell phone receives a text message from the Duo Mobile app. Customer selects 'Approve' to verify their identity.
  - o Once identity is verified, access to the network is completed.
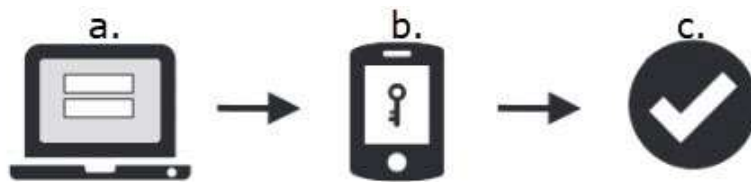
3. To set up MFA the customer needs to have a personal cell phone (home/work) with the **Duo Mobile** App installed. The eHS VPN will deny access unless the cell phone meets the following Pre-Requisites:

  - o **Anonymous Networks:** No using phone through a proxy, Tor, or other VPN networks
  - o **Authentication Methods:** Must use **Duo Push** or **Duo Mobile Passcode** from cell phone.
  - o **Operating Systems:** Android or iOS (Apple)
  - o **Password/Passcode:** Must be enabled.
  - o **Screen Lock:** Must be enabled.
  - o **Tampered Devices:** Phone cannot be 'rooted' (Android) or 'jail broken' (iOS)
  - o **User Location:** Must be in Canada/USA

  NOTE: If you are unable to successfully install/log on to Cisco VPN, please call the Service Desk at **1-888-316-7446** for assistance.
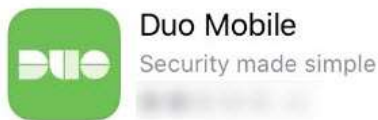
eHealth
Saskatchewan

Pre-Requisite

To install the eHS VPN the user must have the AD credentials.

NOTE: If you have any question or concern, please call the Service Desk at 1-888-316-7446 for assistance.

Install and Activate Duo Mobile App on Cell Phone

1. Download and install Duo Mobile App available on the Apple App Store or Android Google Play.

2. Once the account has been set up, the customer's cell phone will receive an activation text message similar to the one shown below:
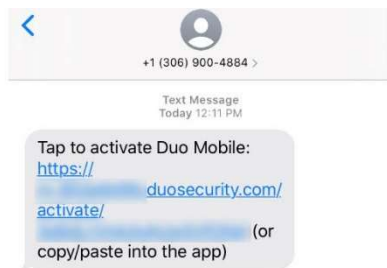
3. Customer clicks on the activation link in the text message and picks Duo Mobile from choices provided.

   IMPORTANT: This link is only good for 24 hours. If the link expires, customer needs to contact the eHS Service Desk to arrange to be sent a new activation link.

4. The link will open the Duo Mobile App to complete activation of the customer's account with the message: "Account added successfully". A DUO-PROTECTED account will be set up within the Duo Mobile App for eHealth Saskatchewan.

5. Customer receives a number of messages:

   NOTE: To get DUO account created/activated, please call the Service Desk at **1-888-316-7446** for assistance.

Install Cisco VPN Client

1. Navigate to https://vpn.ehealthsask.ca.
2. If prompted to install 'ActiveX Control', click the 'Download' button when prompted.

3. Once installed, and if the 'Manual Installation' window is displayed, click 'AnyConnect VPN', then click the 'Download' button.

4. Click 'Save File' | 'Run' downloaded file | 'Install'.

Opening anyconnect-win-4.4.03034-core-vpn-webdeploy-k9.exe ✕

You have chosen to open:

◼ **anyconnect-win-4.4.03034-core-vpn-webdeploy-k9.exe**

which is: Binary File (4.9 MB)

from: https://vpn.ehealthsask.ca

Would you like to save this file?

Save File | Cancel

The anyconnect-win-4.4.03034-core-vpn-webdeploy-k9.exe download has completed. | Run | Open folder | View downloads | ×

This website wants to install the following add-on: 'AnyConnect Secure Mobility Client' from 'Cisco Systems, Inc.'. What's the risk? | Install | ×

5. Otherwise navigate to https://vpn.ehealthsask.ca. Then enter your AD credentials and click on the "Login" button.

Logon

Username health\hdeneve

Password •••••••••••••

Logon

eHealth
Saskatchewan

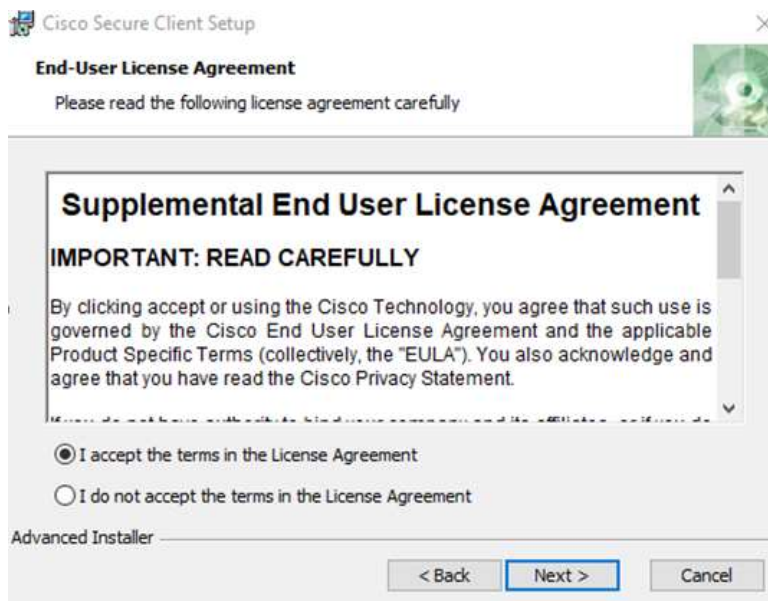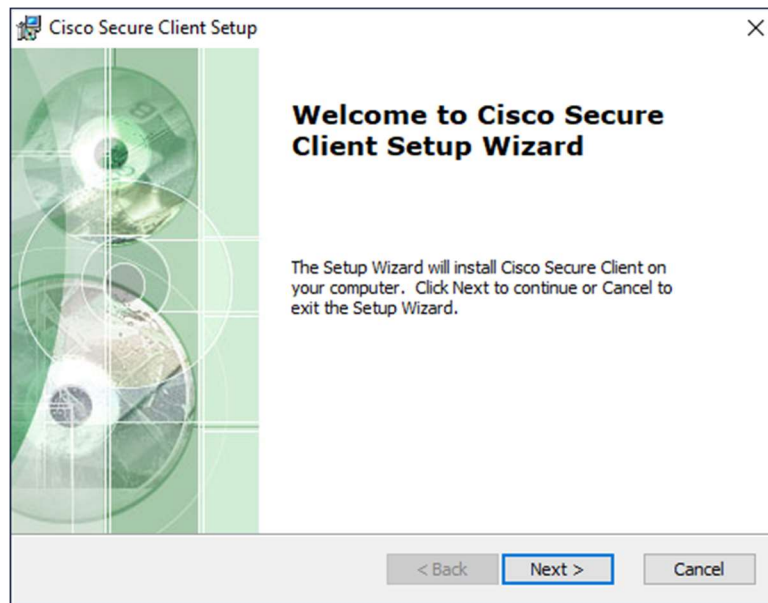6. Then Click the "Download for Windows" button.
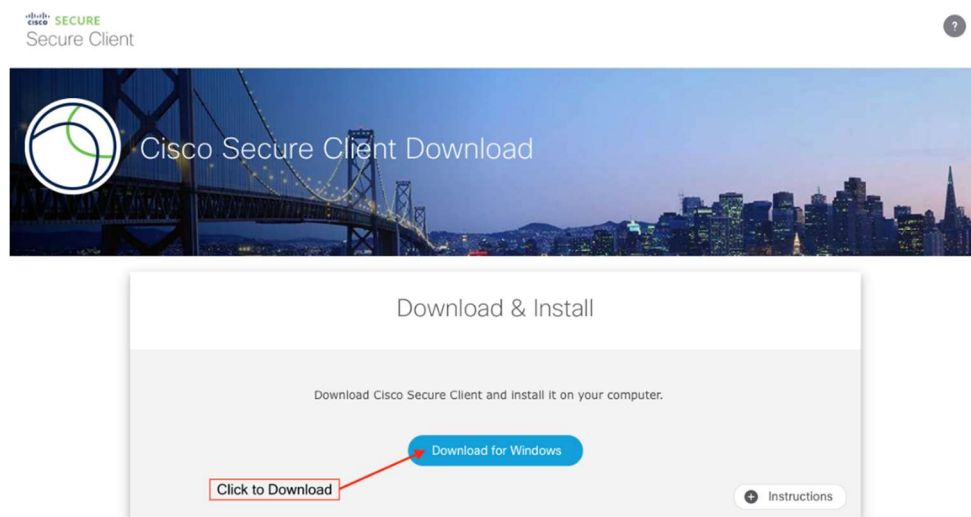
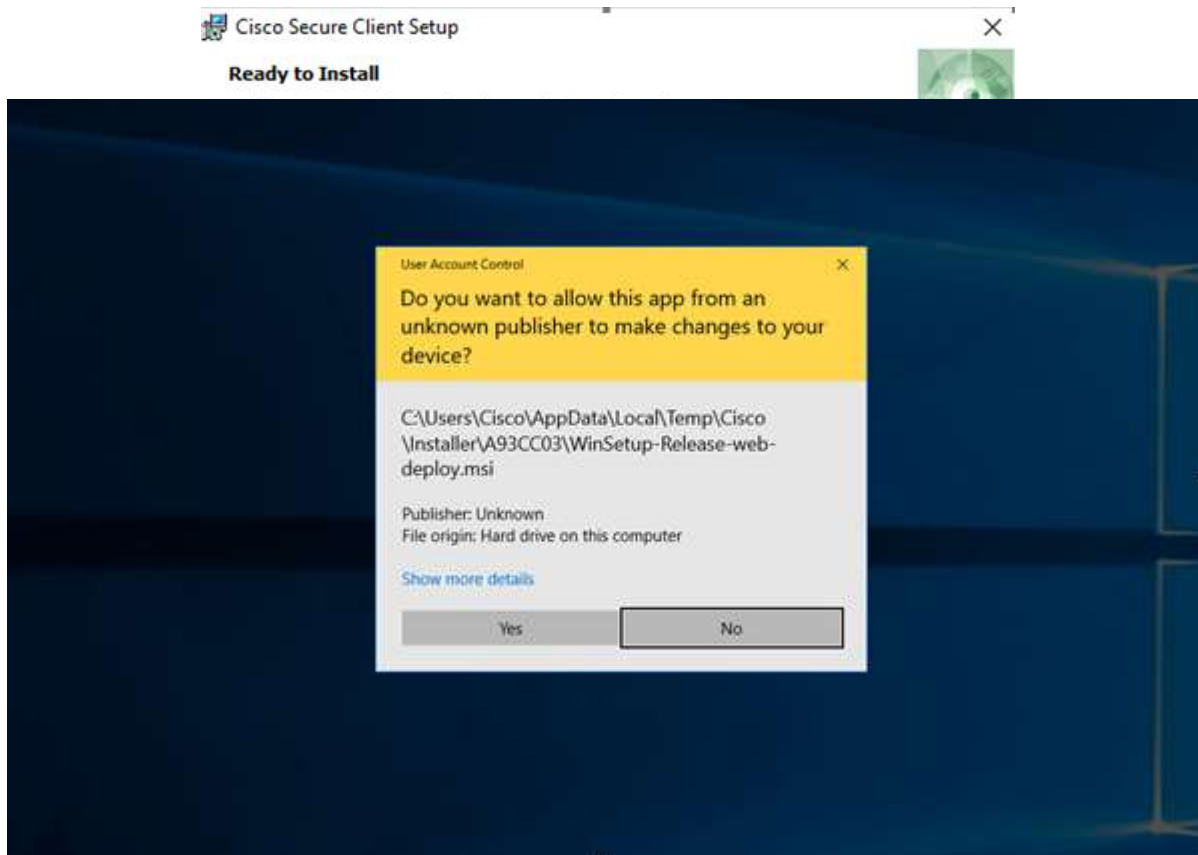7. Locate and open the downloaded install package.
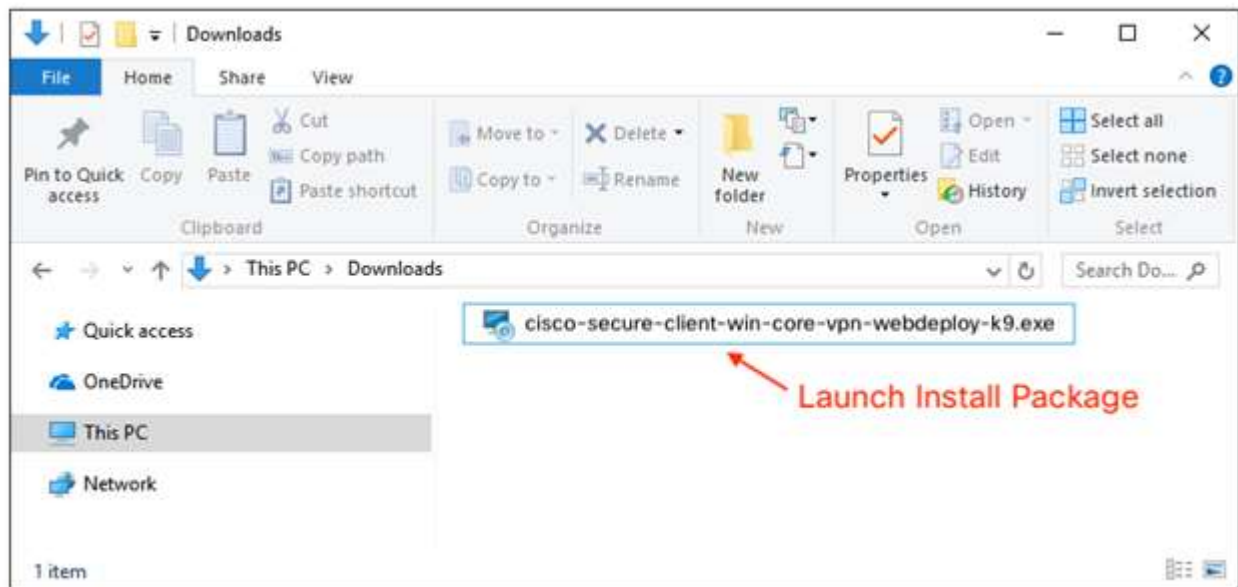
8. Click "Next" button on the "Welcome to the Cisco Secure Client Wizard" screen.

9. Agree to the Software License Agreement and click the "Next" button.

10. Click the "Install" button to begin installation.

11. You must have elevated privileges to install Cisco Secure Client. When prompted, choose the "Yes" button to proceed with the installation.

12. You have successfully installed the Cisco Secure Client and can begin using it. Click the "Finish" button to exit the Setup Wizard.
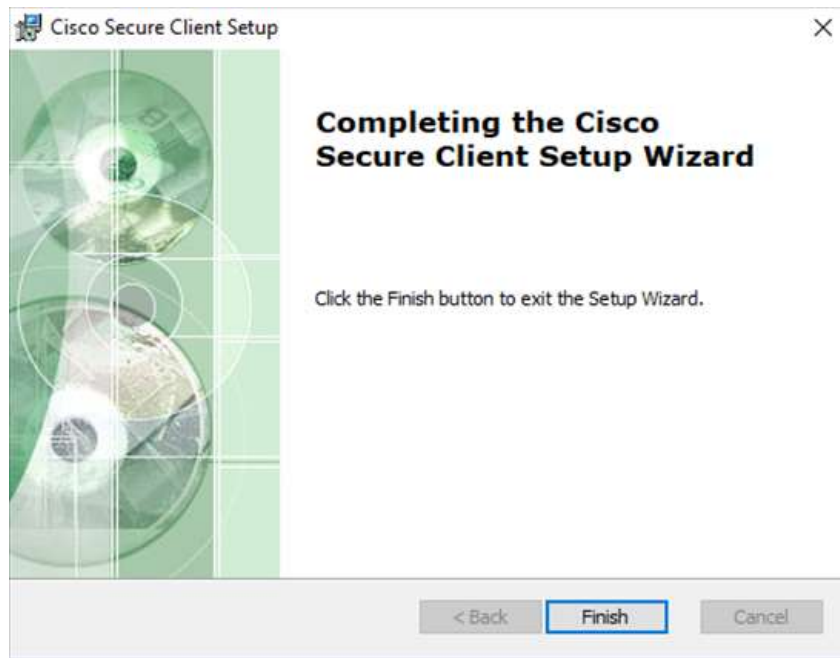
13. Launch the Cisco Secure Client from the Start Menu.
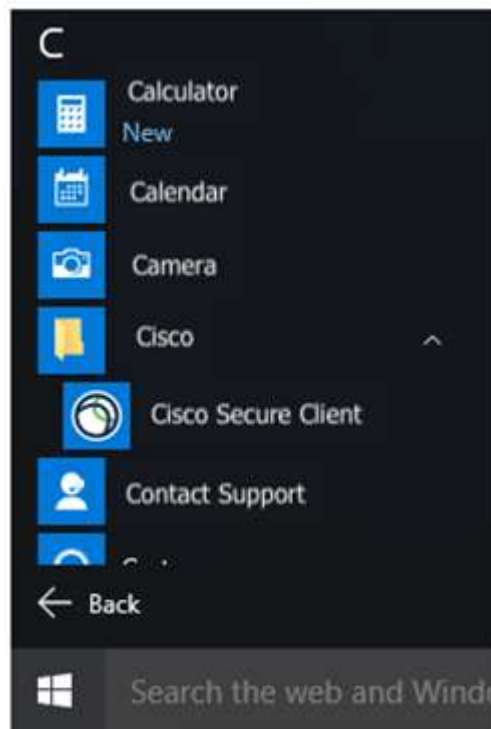
14. Verify you are connected by looking for the following icon in your taskbar. If you are not connected, how to log on instructions are provided below:

NOTE: The lock on the icon indicates you are connected. If the lock is not present, you are not connected.
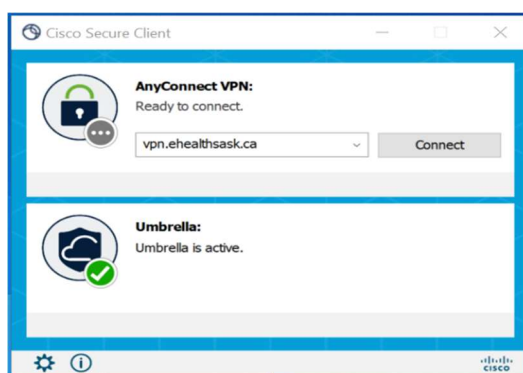

NOTE: If you are unable to successfully log on to Cisco VPN, please call the Service Desk at **1-888-316-7446** for assistance.

Connect to VPN

1. Click on the Cisco VPN Icon in your Task Bar.

2. Ensure the appropriate URL is entered and click 'Connect'.

| Region	VPN URL
All Regions	https://vpn.ehealthsask.ca

3. When presented with the login screen, enter your credentials as provided by eHealth or by your Health Region in the format of DOMAIN\username *(e.g., HEALTH\johndoe)*. Call Service Desk: **1-888-316-7446** if you require assistance.
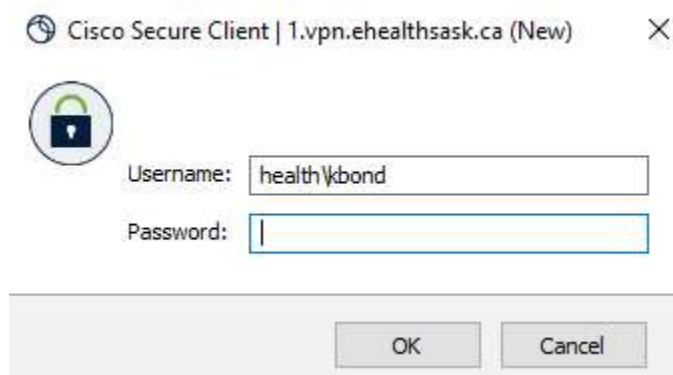
4. A Duo prompt will automatically be pushed to your device to approve.

eHealth
Saskatchewan

DUO Mobile app on mobile devices

- On your mobile device, press **Approve** to the DUO Mobile app notification.
- Make sure that you have notifications turned ON for the DUO Mobile app on your mobile device. If you do not have notifications turned ON, you will need to open the DUO Mobile app to approve.
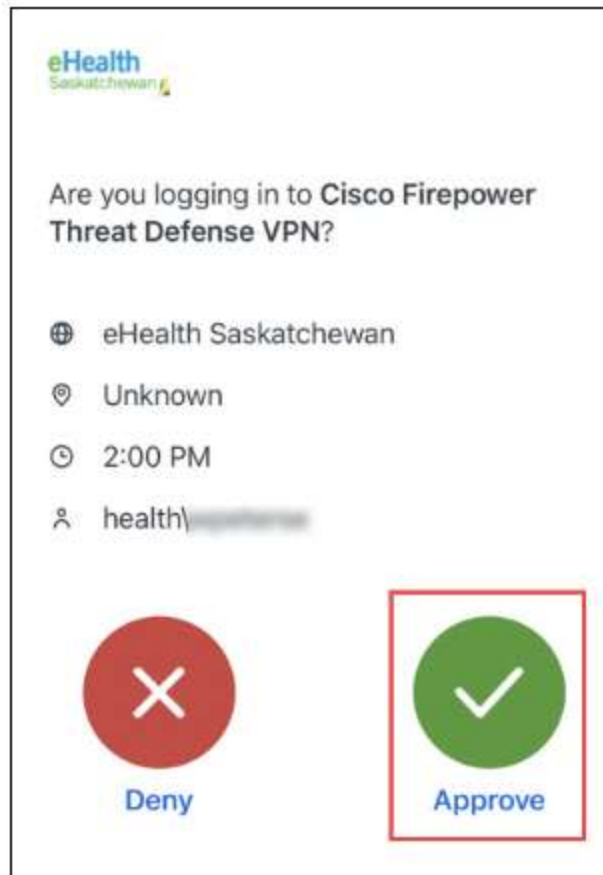

To Turn Notifications ON for the DUO Mobile application on your mobile phone:

1. **iPhone** *Settings > Notification > Duo Mobile > Allow Notification*
2. **Android** *Settings > Apps > Duo Mobile > Show Notification*

Install & Use PACS

1. In Edge (Internet Explorer mode), navigate to http://pacs.ehealthsask.ca.

2. An installer page will launch and will show PACS with a progress bar to indicate the application is installing. You may need to click the 'Click here' link to start the process.
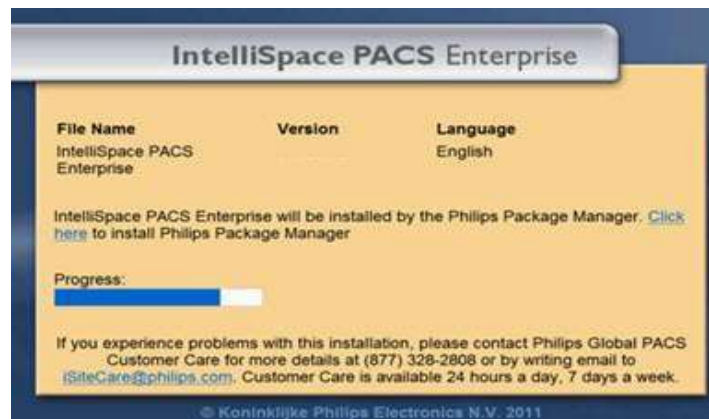
3. Depending on the security permissions on your computer, you may need to click on 'Allow' to continue with the installation.
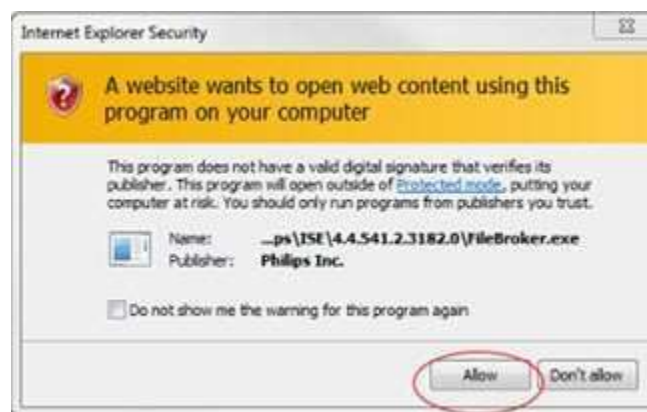
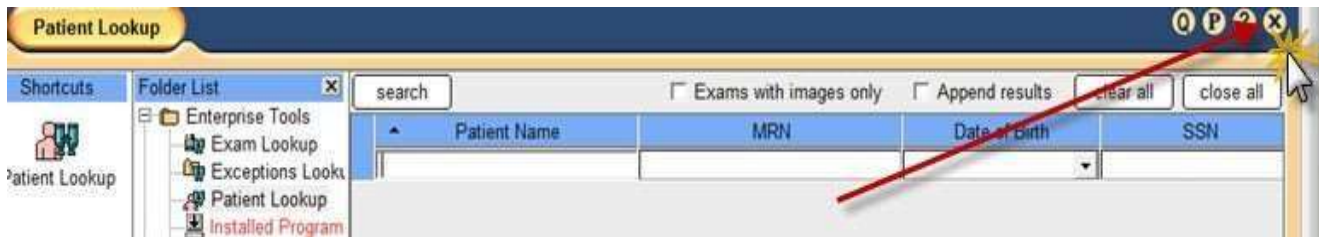4. Once the installation is complete. The PACS Login page will appear.

5. Enter your username and password and select your region from the 'Log on to' drop-down menu.

    NOTE: For Private Clinics (NRC) (e.g., private medical practices, dentists, chiropractors, etc.), use the 'eHealthSask' opt

6. To log out of the application, click the 'X' in the top right corner of the browser window.
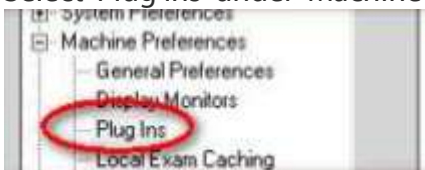

PS360 Plugin for PACS - Configuration/Setup

---

1. **Login to PACS IntelliSpace**.

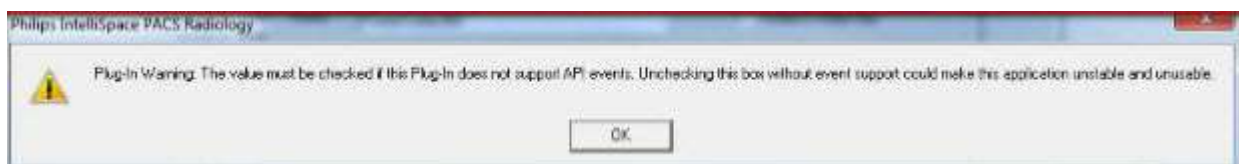2. Click on the 'P' preference icon.

3. In the 'Preferences Dialog' window expand 'Machine Preferences'.

4. Select 'Plug Ins' under 'Machine Preferences'.

5. Click the 'Add' button on the right side under the 'Plug Ins' heading.

6. A 'Plug Ins' dialog window will pop up.

7. Enter 'PowerScribe360' in the 'name field' | enter pertinent URL:

   o PROD: **https://nuance.ehealthsask.ca/RadPortal/pacs/iSite/PowerScribe360plugin.htm**.

8. Deselect the 'Disable API' check box. A "Philips IntelliSpace PACS Radiology" warning window will pop up | click 'OK'.

9. Check the box 'Enable in Radiology' | click on the 'OK' button | 'Apply' | 'OK'.
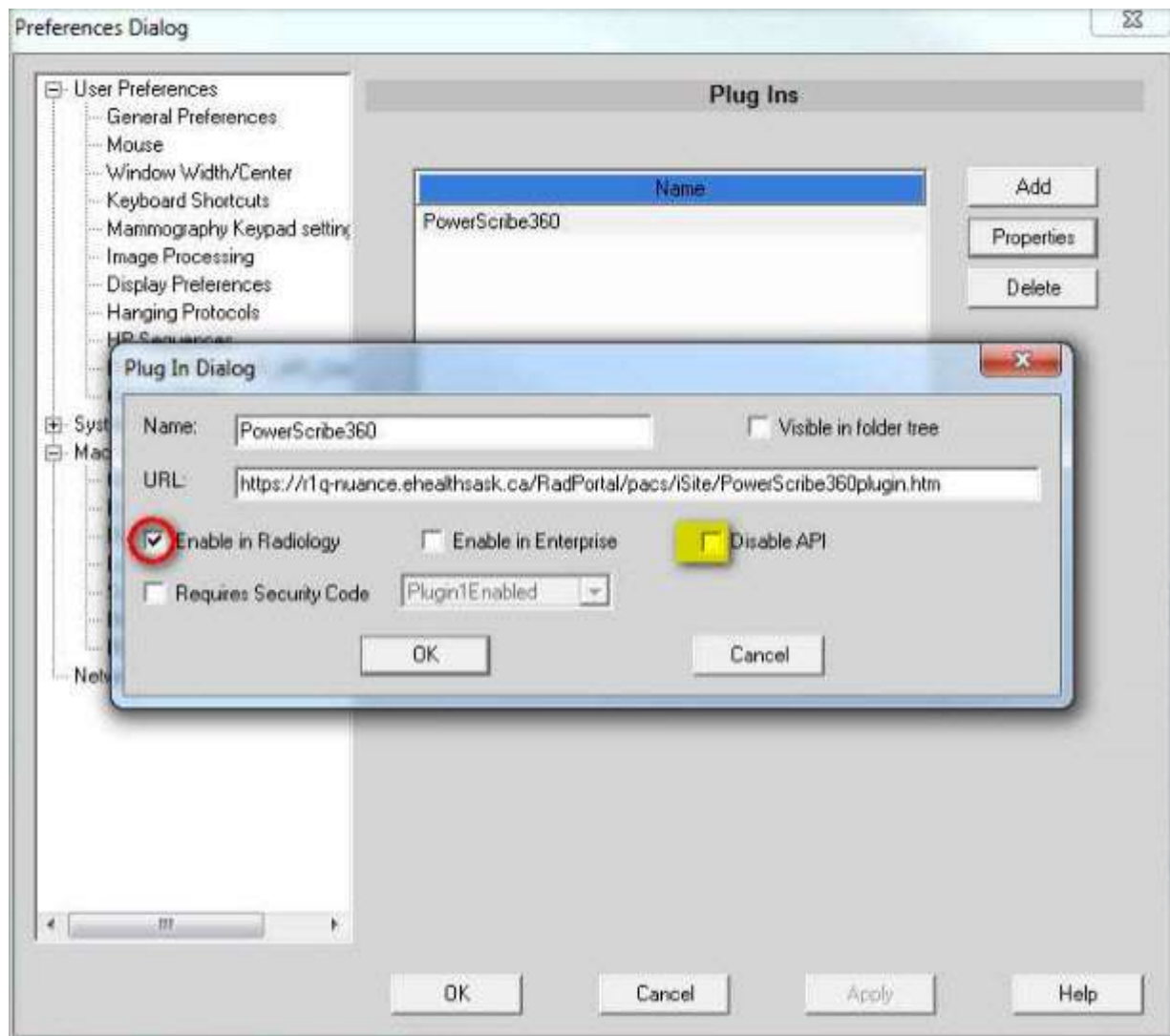
10. Click 'OK' to close the 'Preference Dialog' window.

11. Log out of PACS Radiology and log back in to apply the changes.

12. Click on the 'P' preference icon to launch the 'Preferences Dialog' window.

13. Select 'Powerscribe360 Preferences' under 'User Preferences'.

14. On the right side of the 'Powerscribe360 Preferences' window, scroll down and check on the 'Enable single Sign-on' box | Enter Powerscribe360 User Credentials.
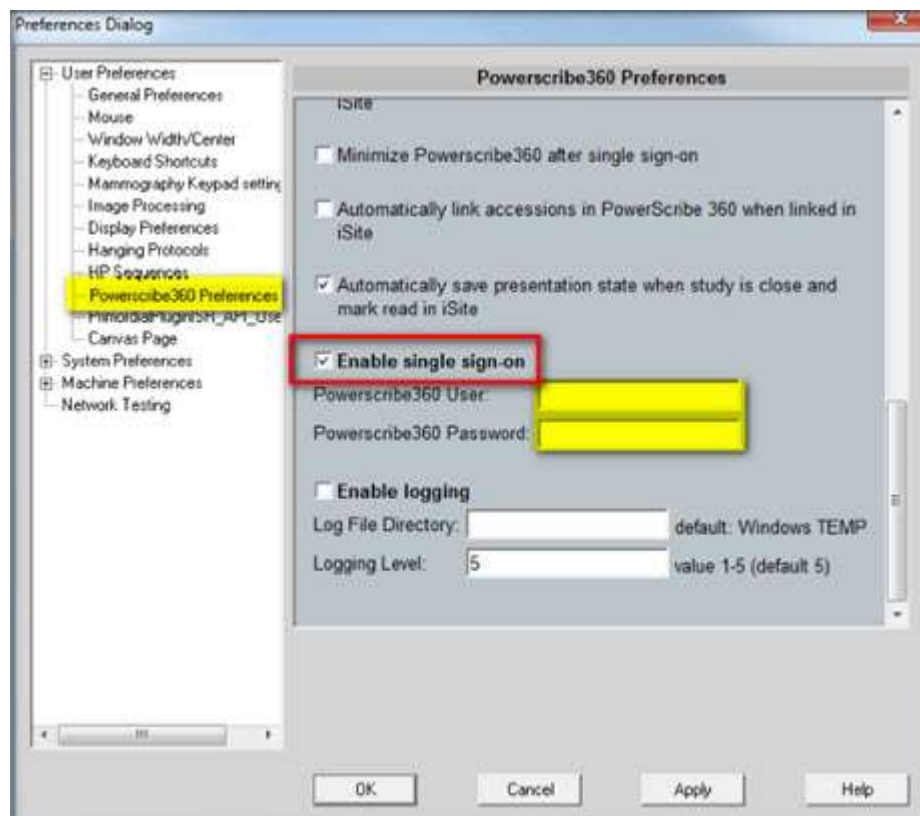
15. Click 'Apply' | Log out of IntelliSpace PACS Radiology and log back in to apply the changes.

   NOTE: This can take approximately 30 seconds and Powerscribe360 will launch automatically.

eHR Viewer Plugin for PACS - Configuration/Setup

1. **Login to PACS IntelliSpace**.

2. Click on the 'P' preference icon.

3. In the 'Preferences Dialog' window expand 'User Preferences'.

4. Select 'eHR Launcher ISE'.
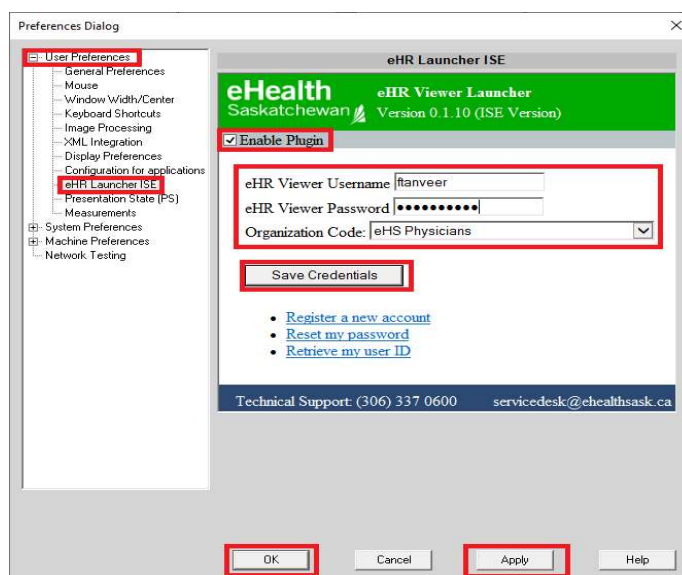
5. Enter your eHR Viewer credentials.

6. Select Enable Plugin

7. Then click on the 'Save Credentials' button.

8. Click 'OK' to close the 'Preference Dialog' window.

9. Log out of PACS Radiology and log back in to apply the changes.

Cisco Secure Client Upgrade Minimum Requirements

Cisco Umbrella supports all vendor-supported, generally available releases of an operating system unless otherwise noted.

- Version 5.1.0 and above
- Windows 10 x86 and x64
- Windows 11 x64 and ARM64
- ARM64 supported only in VPN client, DART, Secure Firewall Posture, Network Visibility Module, Umbrella Module, and ISE Posture
- macOS 11.x or higher

Note: For FYI Only, feel free to provide the users with this link if they have any questions.

SHA Acceptable Use Policy

https://documentfinder.saskhealthauthority.ca/en/permalink/policies13

Any questions in regard to this policy will be directed to SHADigitalHealth@saskhealthauthority.ca