Remote Access using FortiClient VPN

Overview

VPN enables specified AHS staff, 3rd-party contractors, and vendors to remotely access their AHS computer from their personal computer or other remote device. VPN provides full access to an AHS computer and requires the installation of a 3rd party VPN client - FortiClient VPN.

This guide provides instructions on how to install and configure the FortiClient VPN client and then use Remote Desktop Connection to remote into your AHS computer.

If you require any assistance, please call the IT Service Desk at 1-877-311-4300.

Contents

Prerequisites

Windows

- Installing and configuring FortiClient VPN (Windows)
- Using Remote Desktop Connection (Windows)

Mac

- Installing Remote Desktop Connection (Mac)
- Installing and configuring FortiClient (Mac)
- Using Remote Desktop Connection (Mac)

General

- Setting up your PIN
- FortiClient Troubleshooting

Prerequisites

For the AHS computer you are remotely accessing, you will need:

• The computer's asset number, such as M555555



• The AHS computer must be turned on and be connected to the AHS network

For your personal computer, you will need:

- A valid RSA SecurID soft or hard token (fob) issued by AHS
- An up-to-date Windows or MAC Operating System
- An up-to-date antivirus software
- An Internet browser such as Microsoft Edge, Internet Explorer, Firefox, or Chrome



Installing and configuring FortiClient VPN (Windows)

For Windows 7, Windows 8, and Windows 10, download the FortiClient VPN Client install file:

- 64 Bit SSLVPN Client (For Windows 7, Windows 8, and Windows 10 64-bit editions) •
- <u>32 Bit SSLVPN Client</u> (For Windows 7, Windows 8, and Windows 10 32-bit editions) •

If you are using Microsoft Edge:

1. Click **Save** on the message bar.



2. When the download is complete, click Run.

FortiClientVPNSetup_6.2.6.0951_x64.exe finished downloading.	Run	Open folder	View downloads	\times

Note: You must have Administrator rights on your computer to install the file.

If you are using Firefox or Chrome:

- 1. Click Save File.
- 2. Click the expand menu and then select **Open** to run the FortiClient install.



To install FortiClient:

- 1. On the **User Account Control** dialog box, click **Yes** to allow the app to make changes to your PC/device.
- 2. On the Welcome to the **FortiClient Setup Wizard** dialog box, select the checkbox accepting the **License Agreement** and then click **Next**.



3. On the **Destination Folder** dialog box, use the default folder and click **Next**.



4. On the **Ready to install FortiClient** dialog box, click **Install**.



5. When the installation completes, click **Finish**.



The **FortiClient** icon is added to your desktop. Proceed to <u>Configuring FortiClient on</u> <u>Windows</u>.

Configuring FortiClient on Windows

1. Double-click the **FortiClient** icon.



2. Select the Acknowledge checkbox and then click I accept.

♥ FortiClient The Security Fabric Agent File Help	-		×
FortiClient VPN		9 0	۵
Welcome to FortiClient VPN!			
This is a free version of ForhClient VPN software with limited feature support. Please upgrade to the licensed version for advanced features and technical support.			
acknowledge that this free software does not come with any product support. I will not contact Fortinet technical support for any issues experienced while using this free software. Iaccept			

3. Click **Configure VPN**.

FortiClient The Security Fabric Agent File Help FortiClient VPN	- 0 X
Upgrade to the full version to access additional features and receive technical support.	
Configure VPN	

- 4. On the **New VPN Connection** screen, enter the following information:
 - Connection Name: Enter a name, such as AHS VPN
 - **Description**: This field is optional
 - Remote Gateway: vpn.albertahealthservices.ca
 - Authentication: Select Save login
 - **Username**: Enter your AHS network user name (optional)

🖽 FortiClient The Security Fabric Agent	_		\times
File Help			
FortiClient VPN	* •	9	
Upgrade to the full version to access additional features and receive technical support.			
New VPN Connection			
VPN SSL-VPN IPsec VPN			
Connection Name AHS VPN Description Image: Connection Name Remote Gateway Image: Vpn.albertahealthservices.ca PAdd Remote Gateway Image: Customize port Client Certificate None Authentication Prompt on login Username Image: Do not Warn Invalid Server Certificate			
Cancel Save			

5. Click Save.

- 6. On the **Connect** screen:
 - The **Connection Name** and **Username** should be automatically populated.
 - Password:
 - If you have an RSA SecurID soft token: Enter the 8-digit token that displays on your device (mobile phone). Do not enter the PIN as part of the FortiClient password.
 - **If you have an RSA SecurID hard token (fob):** Enter your PIN + the 4 digit token (without spaces) that displays on your token.



Note: A new PIN can be set at <u>https://token.ahs.ca</u>. Refer to <u>Setting up your</u> <u>PIN</u>.

FortiClient The Security Fabric Agent		-	
File Help			
FortiClient VPN		# 0	•••
Upgrade to the full version to access additional features a	and receive technical support.		
VPN Name	AHS VPN		
Username	ahs username		
Password	••••••		
	Connect		

- 7. Click **Connect**. A connection to the AHS SSL VPN portal will be established. The window will minimize to the task bar.
- 8. Click the *Show hidden icons* arrow (^) and right-click the FortiClient icon to display the connection information.



Note that this screen displays the assigned IP address from the SSL VPN located inside AHS. It should be an address similar to 10.48.x.x.

When you are connected, proceed to <u>Using Remote Desktop Connection (Windows)</u> to remote into your AHS computer.

Using Remote Desktop Connection (Windows)

After you have successfully connected FortiClient, it can be used with the Remote Desktop Connection (RDP) tool to remotely access an AHS computer from your personal computer.

Note: The target AHS computer must be powered on and no other user can be logged on. FortiClient must be active and connected.

Remote Desktop Connection is provided as part of the Windows.

1. Use the Windows search tool to search for *remote desktop*. Click **Remote Desktop Connection**.



2. Type in the asset number (the number that appears by the barcode, such as M123456) of the AHS computer followed by healthy.bewell.ca. Alternatively, you can enter the AHS computer's IP address (i.e., 10.117.6.xx) if it is known.



3. Enter your AHS network user name in this format: healthy\username. Then enter your AHS network password.

Windows Security	\times
Enter your credentials	
These credentials will be used to connect to Vdwrkstn0032.	
healthy\username ×	
Password	
Domain: healthy	

4. At the AHS computer sign-on prompt, enter your AHS network username and password again.

username
••••••
Log on to: HEALTHY <u>How do I log on to another domain?</u>

You should now be connected and signed into your AHS computer and have full access to your files, applications, and the AHS network.

		FORTIDET.
		9
AHS SSL VPM 10.48.130.8	>	
(Duration	00:02:58	
	5450	
I Bytes Sent	19868	
Disconnec		

When your work is done, **Disconnect** from FortiClient.

Click **Connect** to re-establish your connection to AHS. You will have to enter a new passcode (8-digit token) or PIN + token (if you use a hard token / fob).

Installing Remote Desktop Connection (Mac)

Remote Desktop Connection will need to be installed on your Mac, as the program is does not come with Mac computers by default.

1. Go to the App Store.



2. Search for Microsoft Remote Desktop.



3. Install the app.



Remote Access using FortiClient VPN • 12

4. After the app is installed, from Launchpad, open Microsoft Remote Desktop.



Installing and configuring FortiClient (Mac)

- 1. Download FortiClient VPN for Mac: MacOS SSLVPN Client
- 2. After the file has downloaded, click the expand icon beside the file name, and then select **Open** to the run the installation.

	Open Always Open Files of This Type
	Show in Finder
forticlientvpnsdmg	Cancel

3. Click Install.



4. Click Continue.



5. Click Continue.



6. Click Agree.



7. Click Install.



\bigcirc	Installer is trying to install new software.
Ø	Enter your password to allow this.
(Balling)	User Name: Mac useraccount
	Password:
	Cancel Install Software

8. Enter your Mac credentials and then click Install Software.

9. Click Close.



10. When installation is complete, open the Applications folder and open FortiClient.





11. Select the Acknowledge checkbox and then click I accept.

12. Click Configure VPN.



13. On the **New VPN Connection** dialog box, enter the following information:

- Connection Name: Enter a name, such as AHS VPN
- **Description**: This field is optional
- Remote Gateway: vpn.albertahealthservices.ca
- Authentication: Select Save login
- **Username**: Enter your AHS network user name (optional)

🖾 FortiClient The Security Fabric Agent	_		\times
File Help			
	* 0	1	
Upgrade to the full version to access additional features and receive technical support.			
New VPN Connection			
VPN SSL-VPN IPsec VPN			
Connection Name AHS VPN Description			
Remote Gateway vpn.albertahealthservices.ca x * Add Remote Gateway Customize port 443			
Client Certificate None 🔻			
Authentication O Prompt on login Save login			
Username Do not Warn Invalid Server Certificate			
Cancel Save			

14. On the FortiClient Console – Remote Access screen:

- The **Connection Name** and **Username** should be automatically populated.
- Password:
 - If you have an RSA SecurID soft token: Enter the 8-digit token that displays on your device (mobile phone). Do not enter the PIN as part of the FortiClient password.
 - **If you have an RSA SecurID hard token (fob):** Enter your PIN + the 4 digit token (without spaces) that displays on your token.



Note: A new PIN can be set at <u>https://token.ahs.ca</u>. Refer to <u>Setting up your</u> <u>PIN</u>.

FortiClient The Security Fabric Agent			-		×
File Help					
FortiClient VPN		*	•	90	
Upgrade to the full version to access additional features and re	ceive technical support.				
VPN Name	AHS VPN 🔹				
Username	ahs username				
Password					
	Connect				

15. Click **Connect**. A connection to the AHS SSL VPN portal will be established. The window will minimize to the task bar.



Note that this screen displays the assigned IP address from the SSL VPN located inside AHS. It should be an address similar to 10.48.x.x.

When you are connected, proceed to <u>Using Remote Desktop Connection (Mac)</u> to remote into your AHS computer.

Using Remote Desktop Connection (Mac)

After you have successfully connected FortiClient, it can be used with the Remote Desktop Connection (RDP) tool to remotely access an AHS computer from your personal computer.

Note: The target AHS computer must be powered on and no other user can be logged on. FortiClient must be active and connected.

- 1. Run Remote Desktop Connection.
- 2. Type in the asset number (the number that appears by the barcode, such as M123456) of the AHS computer followed by healthy.bewell.ca. Alternatively, you can enter the AHS computer's IP address (i.e., 10.117.6.xx) if it is known.
- 3. Enter your AHS network user name in this format: healthy\username. Then enter your AHS network password.
- 4. At the AHS computer sign-on prompt, enter your AHS network username and password again.



You should now be connected and signed into your AHS computer and have full access to your files, applications, and the AHS network.

When your work is done, **Disconnect** from FortiClient.

Click **Connect** to re-establish your connection to AHS. You will have to enter a new passcode (8-digit token) or PIN + token (if you use a hard token / fob).

Setting up your PIN

If you have a Soft Token:

- 1. On your device's RSA SecurID App, enter 0000 then click the arrow.
- 2. Browse to https://token.ahs.ca and enter your Username and Passcode (the latest 8digit code displaying in the app) then click Logon.

Authorized Users Only	
User name:	
Passcode (PIN+Tokencode):	
	Logon

3. Enter a new PIN. Click Submit. Re-enter your PIN and then click Submit again.

Additional Information Required Please type your response below.	Additional Information Required Please type your response below.
Enter your new PIN, containing 4 to 8 chars, or to cancel the New PIN procedure:	Please re-enter new PIN:
Submit	Submit

- 4. Go back to the RSA SecurID app on your device and click PIN (top left) to enter your new PIN.
- 5. Enter the new 8-digit code displaying on your RSA SecurID app on the token website.



If successful, the following message appears:

YOU HAVE SUCCESSFULLY COMPLETED THE TOKEN PIN RESET or NEXT TOKENCODE TASK Please close this window.

If you have a Hard Token / Fob:

1. Browse to <u>https://token.ahs.ca</u> and enter your **Username** and **Passcode** (the code displaying on your fob) then click **Logon**.

Authorized Users Only	
User name:	
Baasaada (Bibli Takamaada):	
Passcode (PIN+Tokencode):	
	Logon

2. Enter a new PIN. Click Submit. Re-enter your PIN and then click Submit again.

Additional Information Required Please type your response below. Enter your new PIN, containing 4 to 8 chars, or to carket the New PIN procedure.	on Required v.		Additional Information Required Please type your response below.		
		Submit	Please re-enter new PIN:		Submit

3. Wait the Token to change on your fob, and then on the Token website, enter the new PIN + token code.

PIN + (
Additional Information Required Please type your response below.	
Wait for the code on your card to change, then log in with the new PIN Enter PASSCODE:	
	Submit

If successful, the following message appears:

YOU HAVE SUCCESSFULLY COMPLETED THE TOKEN PIN RESET OF NEXT
TOKENCODE TASK
Please close this window.
Please close this window.

FortiClient Troubleshooting

I am receiving an Unable to establish the VPN connection error message



This message appears:

• When wrong credentials are entered

OR

• You are trying to connect to the SSL VPN from *inside* the AHS network

Possible solutions

- Ensure you use the correct name format.
- The password is your 8-digit code from a soft token or the PIN + the token code from hard token / fob. Your PIN (Personal Identification Number) is numeric and between 6 digits in length.
- Connecting to the SSL VPN is not possible if your personal computer is already connected to the AHS network.
- If authentication issues persist, you can test that your token is operational by logging into: <u>https://token.ahs.ca</u>. After logging on, a message appears indicating if authentication is successful (and setting your PIN if required). After you have tested the token, close the page.
- If you have tested your token and it is functional, but FortiClient is still not connecting, make sure your local Internet is connected.
- If nothing else works, uninstall FortiClient from your computer, reinstall it, and try to connect FortiClient once again.
- Call the IT Service Desk at 1-877-311-4300.