

Remote Access Overview

Digital Health's Remote Access service provides authorized users with access to various Digital Health services through a secured Virtual Private Network (VPN) when connecting a device from an external network. Access to this service must be requested through formal intake by submitting a [Remote Access Service \(RAS\) Request Form](#) to Shared Health's Service Desk. Please reference [Appendix D: Work from Home Security Tips](#) outlining important best practices.

Digital Health has taken steps to ensure the remote access solution can scale to support provisioned users demand. While the service is very robust, there are variables that can slow or degrade your Remote Access experience:

- Your internet connection speed
- The use of additional bandwidth consuming devices or services, such as Netflix, Spotify, video streaming and gaming on your local network.
- Connecting over WIFI or hotspot
- Out of province use
- ISP Networks that are in development or are disrupted

A user's remote access authentication, service options and available resources will vary depending on your connected device type. A user's presented experience may also vary based on browser type. The following table outlines each device type's service delivery and requirements.

1. Shared Health Managed Device - Digital Health Owned Asset

Prerequisites:	Shared Health Managed Laptop, Provisioned VPN Account; Installed Certificate on Managed Device
Authentication:	User's Shared Health Network Account
Provided Service:	<ul style="list-style-type: none"> • <u>Extended Office</u> <ul style="list-style-type: none"> - Enables authorized users to securely access applications and resources with a similar workplace experience. - Connects to the Digital Health network from any location within North America, using a Digital Health-managed laptop. • <u>Shared Health Hosted Applications</u> <ul style="list-style-type: none"> - Enables authorized users to securely access a limited number of applications that have been configured to be accessible remotely based on a user's application privileges. - Provides a fall back to the Extended Office selection should the device fail endpoint security analysis minimum requirements.

2. Non-Shared Health Device - Customer Owned Asset

Prerequisites:	Customer Owned Device (Windows 10 with a current browser), Provisioned VPN Account; Imprivata Account/Enrollment Service requires Windows 10 with Internet Explorer 11 or Current Chrome Browser and latest Citrix Receiver.
Authentication:	Two-factor: User's Shared Health Network Account + Imprivata Enrollment Method
Provided Service:	<ul style="list-style-type: none"> • <u>Shared Health Hosted Applications</u> <ul style="list-style-type: none"> - Enables authorized users to securely access a limited number of applications that have been configured to be accessible remotely based on a user's application privileges using a personal device (Windows 10 OS and current internet browser). - Requires the user to be provisioned with an additional second factor authentication service.

3. Shared Health Webmail Access - Shared Health Managed or Non-Shared Health Device - Corporate or Customer Owned Asset

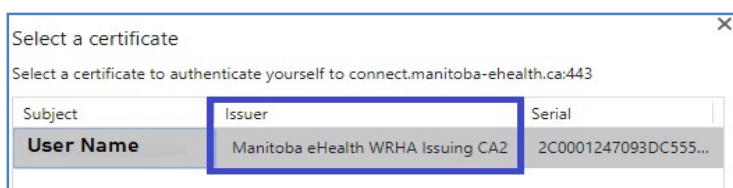
Prerequisites:	Corporate/Customer Owned Device (Windows 10 with a current browser), Provisioned Access to Webmail Service requires Windows 10 with Internet Explorer 11 or Current Chrome Browser
Authentication:	User's Shared Health Network Account
Provided Service:	<ul style="list-style-type: none"> Shared Health Webmail Access <ul style="list-style-type: none"> Enables authorized users to access Outlook Web Access for email and calendar remotely from within Canada using a personal device and current internet browser. <p>NOTE: Webmail will be disabled if not accessed externally within 90 days. To re-enable access, a Remote Access Service (RAS) Request Form must be submitted to Shared Health's Service Desk.</p>

Reference the following sections for instructions on how to access service options by device type. **Ensure all steps have been validated prior to [contacting Shared Health Service Desk](#)** at (204)-940-8500 or 1-866-999-9698.

1. Connecting with Shared Health Managed Device

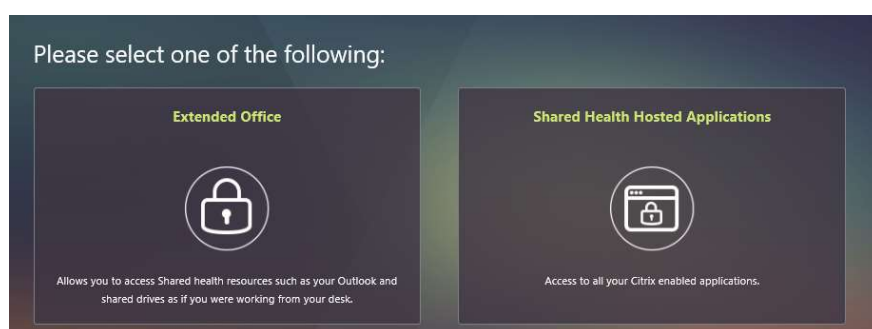
Connect Instructions

1. Connect to <https://connect.sharedhealthmb.ca>.
2. You may be presented with multiple certificates to select when connecting (in some cases a scroll down list will display). If you are presented with a certificate selection window, ensure you locate and select the certificate with **only your 'Full First and Full Last Name'**, issued by 'Manitoba eHealth WRHA Issuing CA2'. All other certificates will not work. Select Ok.



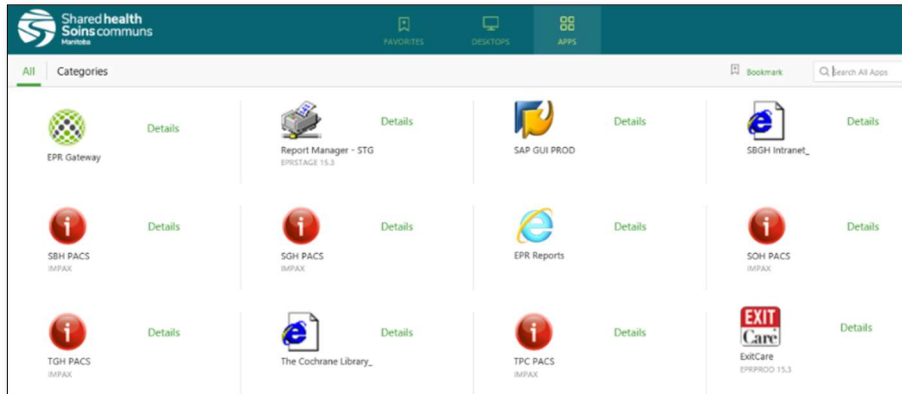
3. If you are asked to run the Endpoint Analysis (EPA) scan, select '**Always**'. If scan fails, contact Shared Health Service Desk to bring the managed laptop up-to-date with the latest security software.

If all security and certificates are passed, you will see the following 'client choices' page. Select your service option: **Extended Office** or **Shared Health Hosted Applications**



If the client choices page does not appear, you will automatically be directed to the **Shared Health Hosted Applications** page only (step 4 screen shot) without Extended Office workspace experience. Contact Shared Health Service Desk to have your device configuration checked.

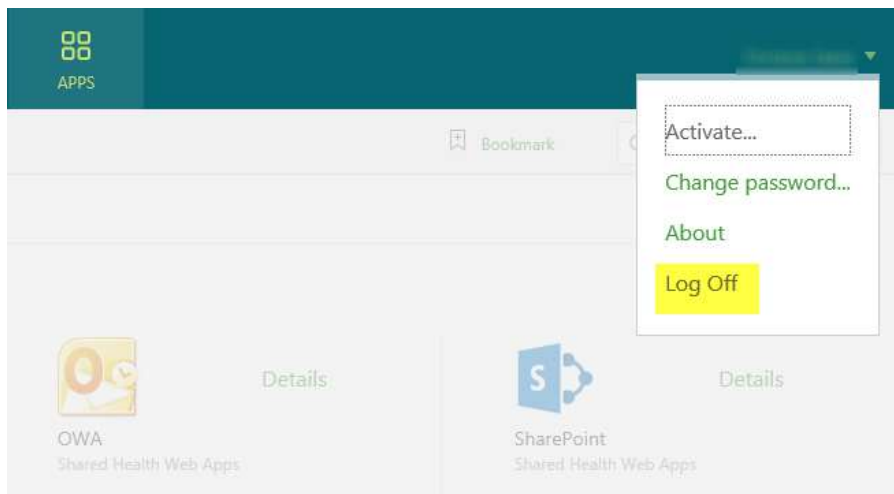
- Once log in is authenticated with security and certificates passed, your Shared Health Hosted Application page displays. NOTE: Your page may appear differently depending on your provisioned applications.



- To display your **Desktop**, minimize or close the Shared Health Hosted Application browser page.

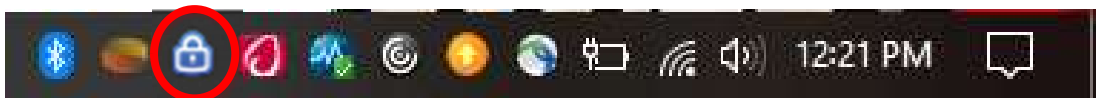
Log Off Instructions

- From your Shared Health Hosted Application page (if browser still open), select **Log Off** from the drop down menu located by your name in the top right hand side.

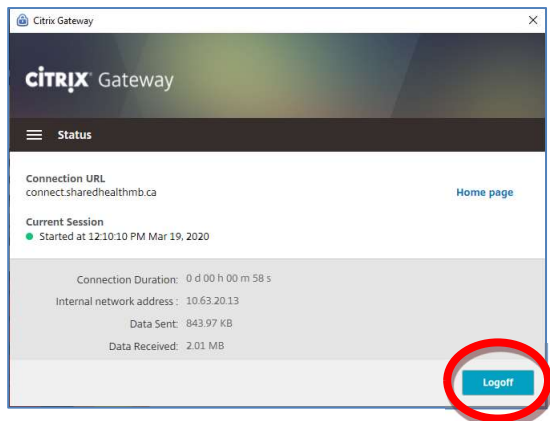


- OR -

- If browser is closed, click the 'Blue' padlock icon from your lower taskbar to launch Citrix Gateway popup window.





Once the Citrix Gateway window appears, click the '**Logoff**' button. This may take a few minutes to complete. A small pop up message (bottom right screen) will inform you of successful log off.



2. Connecting with Non-Shared Health Device

Connect Instructions - Shared Health Hosted Applications

1. Connect to <https://connect.sharedhealthmb.ca> and enter log in credentials. Each connection will require two-factor authentication.
2. Once your Shared Health log in has been authenticated, you will be required to use a secondary method of identification. The following identification methods are supported for you to choose from:
 - a. **Imprivata ID App - Mobile application available for Android and iOS.**
 - b. **SMS Access Code** - Text message with a code is sent to user's registered mobile phone number.
 - c. **Physical-token** - Traditional VASCO physical token. An access code is read from the device.

 <p>Imprivata ID App (Android and iOS)</p> <p>OR</p> <p>Download the Imprivata ID app from the Google or Apple App Stores. Open the app and tap the arrow to show the serial number.</p> <p>At the prompt, you will need to enter the 12 digit serial number including the prefix 'IMPR'.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Enroll Imprivata ID (TM) in 4 steps. (1) Install the Imprivata ID app on your smartphone, (2) Open the app, (3) Locate the 12 character Serial Number and enter it below, or enter S to skip.</p> <input style="width: 100%;" type="text"/> <p style="text-align: center; background-color: #0070c0; color: white; padding: 5px;">Submit</p> </div> <p>Finish setup by entering the 6-digit Token Code that is displaying on the app.</p> <p>Ensure Imprivata ID is allowed to receive notifications on your mobile device.</p>	 <p>Mobile Phone SMS</p> <p>OR</p> <p>Enter 'S' to skip the Imprivata ID registration prompt.</p> <p>To enroll SMS code verification, provide your cell phone number including the area code.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Enroll SMS code verification in 2 steps. (STEP 1) Enter your mobile phone number with area code, or enter S to skip. Message and data rates may apply.</p> <input style="width: 100%;" type="text"/> <p style="text-align: center; background-color: #0070c0; color: white; padding: 5px;">Submit</p> </div> <p>You will receive a message on your phone, finish the setup by providing the verification code sent to you.</p>	<p>Physical Token</p> <p>You must have received a physical VASCO token from Shared Health.</p> <p>Push the button on the token to reveal the code and enter it on screen.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Enter OTP Token passcode, or enter S to skip.</p> <input style="width: 100%;" type="text"/> <p style="text-align: center; background-color: #0070c0; color: white; padding: 5px;">Submit</p> </div>
--	--	--

After successfully enrolling, you will not be prompted to enroll again. Each time you connect the portal will try the following sequence to verify your identity. If you need to re-register your mobile phone, call the contact Shared Health Service Desk.

a. Imprivata ID

If you are enrolled with Imprivata ID, the portal will automatically send a notification to your smartphone. Tap "Approve" to verify your log on.

If there is no response, an option to skip Imprivata ID or enter the token code manually will be presented. To enter the code manually, open the app on your phone and enter the Token Code.



b. SMS

If you are enrolled with the SMS option, an access code will be sent to your phone from Imprivata 781-676-3201.

887257 is your Imprivata one-time verification code.

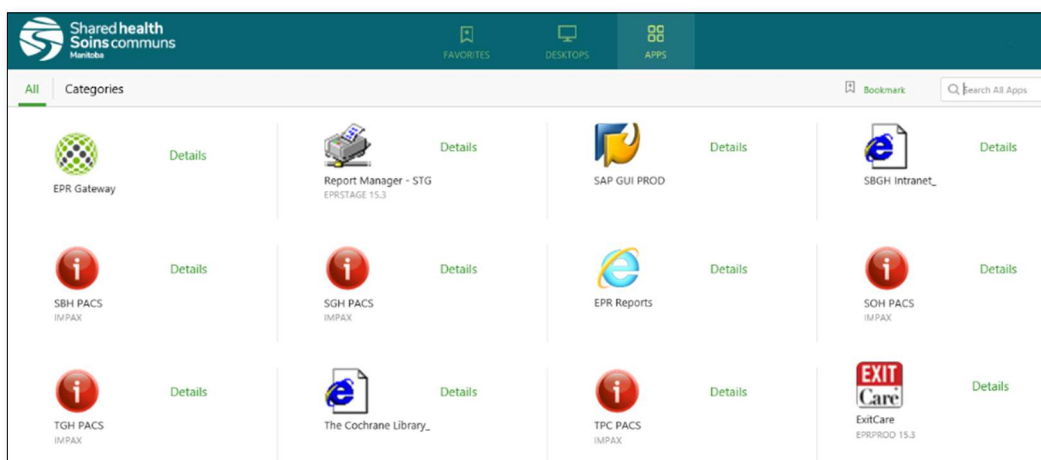
c. VASCO Physical Token

If you are enrolled with a physical token, push the button on the device to receive your access code.

Important: Should you wish to re-enroll, or if you would like to register a new mobile phone, you will need to contact the Shared Health Service Desk and ask to have your Imprivata ID reset. Call the Shared Health Service Desk at 204-940-8500 or 1-866-999-9698.

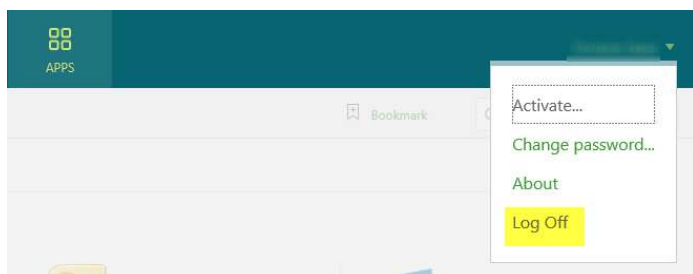
- Once two-factor log in is complete, your Shared Health Hosted Application page will display (picture below).
NOTE: Your page may appear differently depending on your provisioned applications.

It is important to NOT close this browser window as it will end your remote access session.



Log Off Instructions - Shared Health Hosted Applications

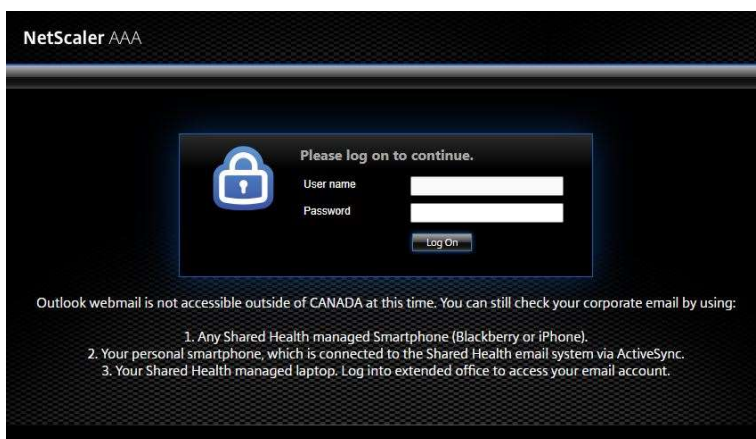
- From your Shared Health Hosted Application page, select **Log Off** from the drop down menu located by your name in the top right hand side.



3. Outlook Webmail Access

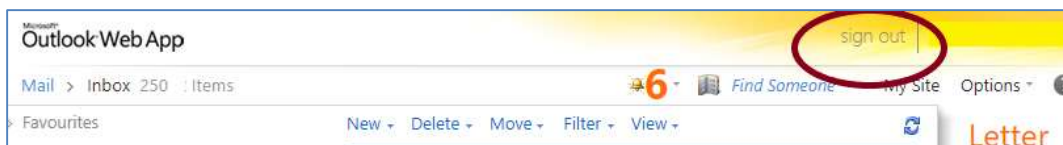
Connect Instructions – Outlook Webmail Access

1. Connect to <https://webmail.manitoba-ehealth.ca> and enter log in credentials. Each connection will require user to be within Canada.



Log Off Instructions – Outlook Webmail Access

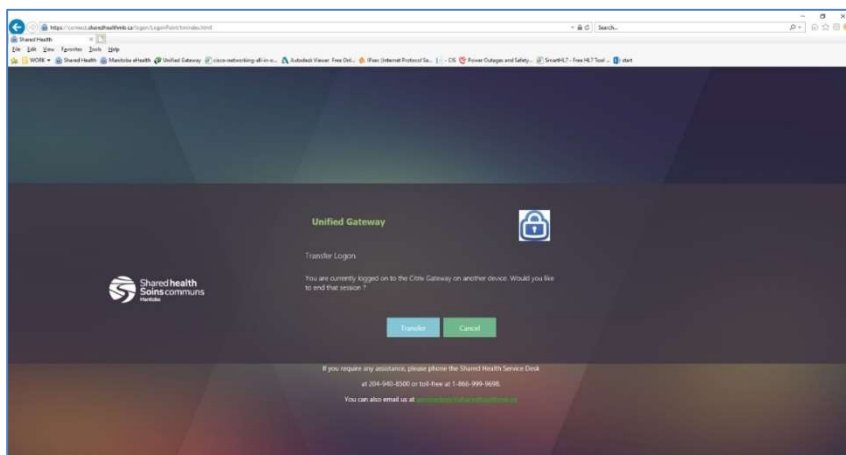
1. From your Webmail main page, select sign out from the upper right hand window location.



Restarting Remote Access

If you wish to log on again when already logged out, or have logged out incorrectly, restart your computer and open browser and connect to <https://connect.sharedhealthmb.ca> – or – completely close/exit the browser you are using and open a new browser session and connect to <https://connect.sharedhealthmb.ca>.

NOTE: If you logged out incorrectly from Remote Access you may be presented with a window to Transfer Login. Select the **Transfer** button to reconnect into remote access session (may take a few minutes to complete).



Appendix A: Installing Citrix Receiver or Citrix Workspace App

When logging into Remote Access, the website will require the use of Citrix Receiver or Citrix Workspace App. When you connect, the website will detect the presence of Citrix Receiver or Citrix Workspace App software.



Step 1 - Detecting Citrix Receiver or Workspace App

Log into Remote Access. Depending on your browser, the website may prompt you to detect the Citrix Receiver software. Click 'Detect Receiver'. Do not use the light version.

If the receiver software is detected, the Shared Health Hosted Application page will appear. If the software is not detected, the website will prompt you to install. Click Install and follow the prompts to download the software.

After the download completes run the Installer software. Find the file in your downloads folder if it does not automatically launch after downloading.



Step 2- Installing Citrix Receiver

Open the installer and click Start to begin the install. Accept the license agreement and proceed through the prompts. Skip the prompt to 'add an account' prompt, select 'ok' or 'continue' without providing any address.

If you are prompted to give Citrix Receiver or Citrix Workspace access to your downloads folder, allow this.

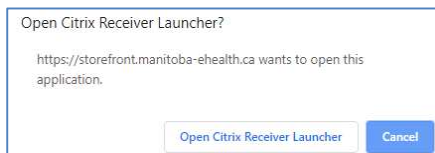
Once the Receiver is installed, you will receive an "Installation successful" window. Click finish and return to your browser.



Step 3 – Loading Citrix Shared Health Hosted Application page

Once you return to your browser, the page should refresh. If the page does not refresh automatically, reload the page(F5 or refresh button) to detect the installed software.

Depending on your browser and OS, a message may appear in your web browser at the bottom of the window or via popup to trust Citrix plugin software. Click "Allow" to proceed.



Citrix Launcher

If you are using Google Chrome or Firefox you may be prompted to allow Citrix Launcher to run the application, select 'Open in Citrix Launcher' or 'Allow'.

If you are using iOS or Android devices, you will be prompted to open links and applications using Citrix Workspace App. Always use the 'open in Citrix Workspace' option.

Appendix B: Launching to EPR Gateway

All personal computers or devices accessing the Clinical EPR require a name that follows a specific naming convention setup in the application. You will need to rename your personal device to match this convention as outlined below.

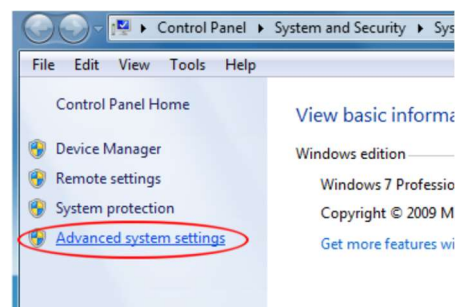
Important: Before you change your device's name, record its current name. If you experience issues with your device or networks, you may need to revert to the original name to resolve them.

Devices should be named with your Shared Health username prefixed with "RA". For example, a John Smith with username jsmith3, his authorized device name is RAJSMITH3. If registering a second device, use the postfix "-2", so for John his second device would be RAJSMITH3-2. **You should have received notification of your approved device name. If you are unsure contact the Shared Health Service Desk.**

1. Changing Your Device Name

Windows 7, 10

In Windows 7, Click on Start and then right click on My Computer. Select Properties from the menu. Click Advanced System Settings menu option on the left side, as shown.

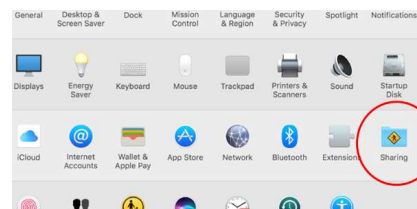


In Windows 10, use the builtin search tool beside the Start button, searching for 'Advanced System Settings'. Or right click the Start button, and choose settings. Search for 'Advanced System Settings' in the search tool.

In the Systems Settings popup window, select the Computer Name tab. You will see current computer name listed under Full Computer Name. Click the Change button. Change the Computer name as required.

Mac OS

On Mac OS, click the Apple logo from the Menu Bar at the top of the screen. Select System Preferences. Click the Sharing icon as pictured to the right.



Change the Computer name as required.

Other Devices

Other devices that support the Citrix Receiver or Citrix Workspace App client may be compatible, consult your device's documentation to change its device/network name.

2. EPR Gateway Error, "Workstation HTML- xxxx-xxxx is not in the database"

If you receive an error trying to launch EPR and the error says the workstation name starts with 'HTML', then your device browser is using the Citrix Light Receiver. From the Shared Health Hosted Application page screen, open the drop down menu and select Change Receiver (see section below). Follow the onscreen prompts to detect Citrix Receiver or Citrix Workspace App.

If Citrix Receiver or Workspace App cannot be detected, please clear your browser cookies and saved data, (see instructions at end of the document) and try connecting again. If the issue persists, try reinstalling the Citrix software (see instructions below).

If you have not received an authorized EPR workstation name please contact the Shared Health Service Desk.

Appendix C: Common Issues and Troubleshooting

1. Citrix Light Receiver and Changing Receiver Modes

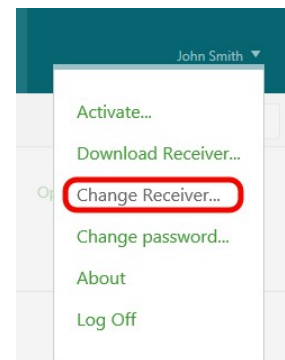
It may be possible to use the web plugin, or 'light' receiver to access most applications if your device does not support the Citrix Receiver client.

Some applications, such as **EPR Gateway**, are not compatible. Additionally, some features are not available through the light receiver, like printing and saving files to your device.

If you need to change the Receiver mode, from the apps list page, select the drop down menu on the top right hand side and select "Change Receiver...".

If your browser will not give an option to change receiver and you find you are stuck in light mode, clear your browser cookies and saved data (See section on) and restart your browser.

If your browser displays the detect Citrix receiver screen, allow it to detect the client. You may be prompted to install receiver, click install and the page should then detect the receiver. If the issue persists uninstall Citrix Receiver and try accessing the page again. See below.



2. Citrix applications won't launch, or are stuck loading

If a Citrix application has difficulty launching, shut down the browser completely. On Mac, ensure you quit the browser application, while the browser is the active window, click the Menu bar and select "Quit".

Close Citrix Receiver if it is running. Look for the Citrix Receiver icon in your system tray by the clock, right click and select Exit. On Mac, click the Citrix icon in the Menu bar, right hand corner, beside the clock/Wi-Fi indicator, select Exit.

Clear your browser cookies and saved data (See end of document) and try connecting again. If unsuccessful, try restarting your computer. If the issue persists, uninstall the Citrix Receiver (see next section).

3. Uninstalling and Reinstalling Citrix Receiver or Citrix Workspace App (Windows and Mac)

On Windows, uninstall Citrix Receiver by using the Add or Remove Programs utility. Once Receiver is uninstalled, restart the computer and try connecting once more. To download the latest Receiver client visit Citrix.com directly:

<https://www.citrix.com/downloads/workspace-app/windows/workspace-app-for-windows-latest.html>

On Mac, download the latest version from Citrix.com directly:

<https://www.citrix.com/downloads/workspace-app/mac/workspace-app-for-mac-latest.html>

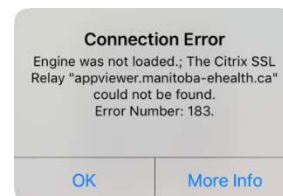
Inside the package are both an Installer and an Uninstaller utility. First use the Uninstaller. Reboot the computer, and then install Citrix Workspace App using the Installer utility.

4. The browser is stuck at "Loading Apps"

This issue occurs on Mac and iOS devices using Safari browser. Use either Google Chrome or Firefox browsers instead.

5. Receiver Connection Error, and Mobile Receiver Error 183

The remote access does not currently support connecting to the service from within the Citrix Receiver or Workspace App directly. Please access the service by using your device's web browser instead.



6. eChart: Incompatible Browser Error

The eChart Manitoba webpage requires Internet Explorer 11 browser. If another browser version is detected a wrong browser page is displayed.

7. Deleting Cookies and Saved Data

The remote access portals save cookies and browser data on your device. Sometimes it may be necessary to clear this data to resolve an issue when trying to connect.

Note: Clearing your browser cookies and data may remove saved settings and preferences from many of your favorite websites. See the instructions below for your specific browser to either delete all cookies and data, or to delete specific data for Manitoba-ehealth.ca sites.

Google Chrome

To clear all Cookies and website data

At the top right, click More (three dots). Click the '**More**' button (three dots) right hand corner. Click More tools and then Clear browsing data. At the top, choose a time range. To delete everything, select All time.

Next to "Cookies and other site data" and "Cached images and files," check the boxes. Click Clear data.

To delete a specific cookie and website data

At the top right, click More (three dots). Click the **Settings**. On the left hand side, open the **Advanced** menu. Select **Privacy and Security** settings and select the **Site Settings**. Then, select **Cookies and Site Data**, finally, select **See all cookies and site data**.

Use the Search cookies tool, and search for Manitoba-ehealth.ca. Select all Manitoba-ehealth.ca cookies, and then delete them by clicking the trash can button.

See <https://support.google.com/accounts/answer/32050> for more information.

Firefox

To clear all cookies and site data

Click the **Menu button**(three horizontal lines) in the right hand corner , select **Options**.

Select **Privacy and Security** panel, go to the **Cookies and Site Data** section. Select **Clear Data**. Then click **Clear** to confirm.

To delete a specific cookie and website data

From the **Privacy and Security Panel**, go to the **Cookies and Site Data** section. Select **Manage Data**. Use the search tool to locate Manitoba-ehealth.ca cookies. Select the cookies, and click **Remove Selected**.

See <https://support.mozilla.org/en-US/kb/clear-cookies-and-site-data-firefox> for more information.

Internet Explorer

To delete all cookies and website data

Click the **Tools** button (cog) at the right hand corner. Click the **Safety** menu option. Select **Delete browsing history**. Select the **Cookies and website data** check box, and then click **Delete**.

See <https://support.microsoft.com/en-ca/help/17442/windows-internet-explorer-delete-manage-cookies> for more information.

Safari

Click **Safari** in your menu bar, left hand corner. Select **Preferences**, and then click **Privacy**. Select **Manage Website Data**. Select the cookie you want to delete, and click **Remove**. Or, click **Remove All** to delete all cookies and saved data.

See <https://support.apple.com/en-ca/guide/safari/sfri11471/mac> for more information.

8. Unable to connect to network drive(s) or prompts from Outlook for a user ID and password after resetting network password

The credentials should be synchronized with computer in order to access network resources.

- To synchronize credentials, remain connected to Extended Office VPN and lock laptop from the Start Menu or via **Win + L** on the keyboard. Immediately unlock the PC using new password. Reboot laptop and log back into Extended Office to reconnect shared network drives.
- If the password changed and restarted before synchronizing the laptop, then you will need to first log in with old password, connect to Extended Office with new password, once connected lock the machine and log back in with their new credentials, the machine will now have the correct password. You should be able to restart now and log back into Remote Access.

Appendix D: Work from Home Security Tips

- Avoid public Wi-Fi; Do not connect to the Shared Health network with any unsecured public Wi-Fi.
- When using Shared Health supplied equipment,
 - Use your device for work related matters only and not for personal use
 - Avoid unnecessary video and audio streaming while connected to the Shared Health VPN
 - Always follow the Shared Health security policies and understand your security obligations
 - <https://policies.sharedhealthmb.ca/information-technology/#48-health-information-services>
 - <https://home.sharedhealthmb.ca/digital-health/standards/>
 - Do not connect personal data storage devices to your work computer
- When using your personal device to access Shared Health resources such as email,
 - Restrict computer use to you only (i.e. do not allow family members or others to use your account created for Telework use)
 - Use trusted anti-malware software that provides real-time protection as well as (minimum) full disk weekly scans
 - Ensure that your operating system and applications are receiving regular patch updates.
- Lock your workstation (Windows Key + L) while unattended to prevent unauthorized access.
- Take measures to protect/prevent equipment from theft i.e. cable lock, in a locked drawer, stored out of sight when not in use.
- Refrain from clicking links and buttons or opening attachments in any unsolicited email, tweet, post, or online advertisement.
- Make sure all of your personal and work passphrases or passwords are unique, and use a different password for each account
- Do not locate Home Smart Speakers (e.g. Alexa, Google Home, Ring Doorbells) near your work area to avoid the unintended loss of sensitive data.

For additional security tips for working from home, reference the following resources:

- <https://terranovasecurity.com/cyber-security-and-working-from-home/>
- <https://cyber.gc.ca/sites/default/files/publications/itsap.10.016-eng.pdf>