



**Mount  
Sinai**

# The Mount Sinai Health System **Remote Access Reference Guide**

*Information Technology Department*

*March 2020*

## Preface

---

The instructions outlined in this guide, along with the supporting policies and references, aim to better support Mount Sinai Health System staff accessing email, work stations and programs remotely.

For ease of use, this PDF is interactive and links are used to guide you through the instructions ([indicated as such](#)), as well as to various supporting websites ([indicated as such](#)).

## Table of Contents

### Getting Started: Prerequisites

- Symantec VIP Two-Factor Setup
- What is the VIP Access Application?
- How To: Installing and Registering VIP Access

### Quick Reference Chart

### Accessing Your Exchange Email Remotely

#### **RDP Over VPN**

- [For Windows](#)
- [For Mac OSX](#)

#### **VPN Tunnel**

- [For Windows](#)
- [For Mac OSX](#)

### Bring Your Own Devices (BYOD) Best Practices

## Quick Reference Chart

---

You need to...	The best solution is...	Check these prerequisites before you get started...		
		Registered Symantec VIP token	Request 'Hospital VPN Citrix' in Sailpoint	Other/ notes
<p><b><u><a href="#">Access Exchange Email</a></u></b></p>	<p>Logon to the Mount Sinai VPN.</p> <p><a href="#">Hospital log-in</a></p> <p><a href="#">School log-in</a></p>	<a href="#">Yes</a>	No	<i>Note: You do not need to request VPN access</i>
<p><b>Access Office 365 Email, Skype, Teams</b></p>	<p>Use the Microsoft Portal</p> <p><a href="#">Log-in</a> (You will be redirected to the Mount Sinai SSO portal)</p>	<a href="#">Yes</a>		
<p><b>Access the Citrix Desktop</b> (ie. Epic, Cerner, PRISM, etc.)</p>	<p>VPN Citrix Access</p> <p><a href="#">Log-in</a></p> <p>Click on Citrix (You may need to download the Citrix application, which can be found next to the Citrix tile)</p>	<a href="#">Yes</a>	<p>Yes</p> <p><a href="#">Citrix &gt;&gt;</a> <a href="#">Sailpoint &gt;&gt;</a></p>	<p>Mac OSX Catalina download <a href="#">here</a></p>
<p><b>Remote access a Dedicated Workstation</b></p> <p><b><u><a href="#">For Windows</a></u></b> <b><u><a href="#">For Mac OSX</a></u></b></p> <p>(ie. desktop or laptop that is in the office)</p>	<p>VPN RDP Access</p> <p><a href="#">Log-in</a></p>	<a href="#">Yes</a>	<p>Yes</p> <p><a href="#">Citrix &gt;&gt;</a> <a href="#">Sailpoint &gt;&gt;</a></p>	

<b>Direct Network Access</b>  <u><a href="#">For Windows</a></u> <u><a href="#">For Mac OSX</a></u>	VPN Tunnel Access  <a href="#">Hospital log-in</a>  <a href="#">School log-in</a>  <i>Allow the security checker to run.</i>	<a href="#">Yes</a>	Yes  <a href="#">Citrix &gt;&gt;</a> <a href="#">Sailpoint &gt;&gt;</a>	
--	--	---------------------	--	--

## Getting Started: Prerequisites

---

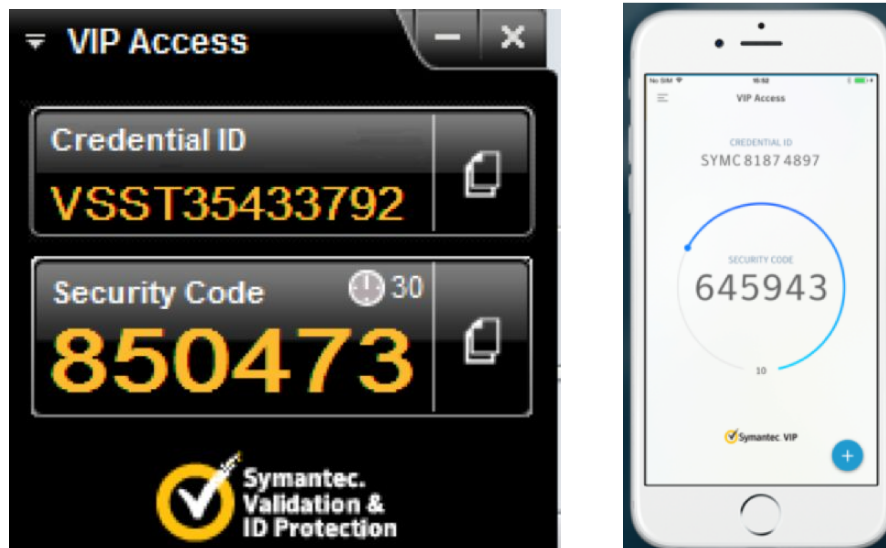
### Symantec VIP Two-Factor Setup

Two-factor authentication (2FA), often referred to as two-step verification, is a security process in which the user provides two authentication factors to verify they are who they say they are. **All users are required to use two-factor authentication to login into the Mount Sinai network over VPN from a remote location.**

In order to use Two Factor Authentication, you must first download and install the Symantec VIP Access application to your mobile device and then register your token which will tie your token to your network account.

### What is the “VIP Access” application?

The VIP Access application is a security code generator that displays a new and secure code every 30 seconds and provides a ‘Credential ID’ that is to be registered with your account. It is available for Windows, Mac, Android, and iOS devices.



*Best practice: It's easiest to use this application on your mobile device/smartphone because you will need it every time you log in remotely (e.g. from home, not on campus).*

## How To: Installing and Registering VIP Access

**STEP 1: On your Windows, Apple, or Android Device, go to <https://vip.symantec.com/> to download the device.**

**Android Devices:**

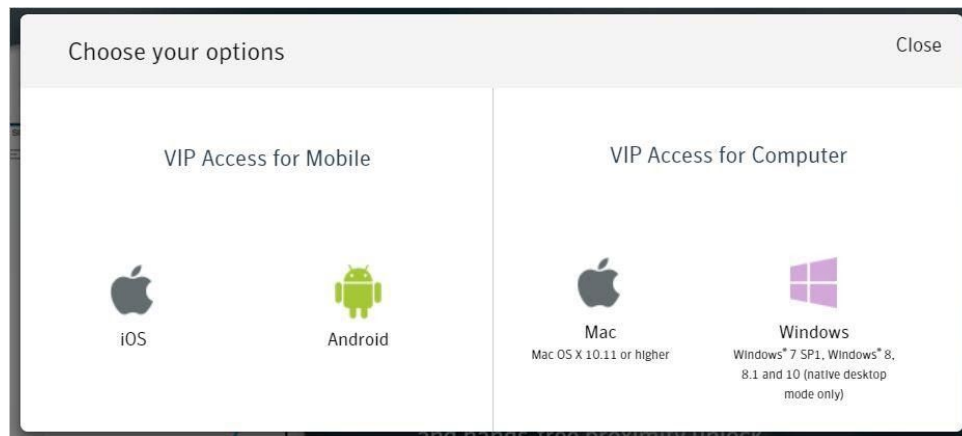
[Download VIP Access by Symantec for Android](#)

**IOS(Apple) Devices:**

[Download VIP Access for Symantec for IOS](#)

**Windows/Mac Device:**

1. Go to <https://vip.symantec.com/>
2. Click on **Download**
3. Select the appropriate download for your operating system or device (Mac or Windows)



4. Install the software

## **STEP 2: Register your Credential ID with your Mount Sinai Network Account**

*Important: To register your VIP Token you MUST be on the Mount Sinai network (you must be on campus.)*

1. Open a web browser and go to the appropriate registration site:  
[Hospital Accounts](#)  
[School Accounts](#)
2. Login in with your AD Account (network ID) and password  
*Note: If you already registered your VIP token, you will need to enter the PIN to login. If you do not remember the token, contact the Helpdesk.*

3. Click **Register**
4. Fill in the form using the information provided by the VIP access application or Hardware Token

### Credential Name

Type in a description of the token device such as: Home PC, iPhone, Android, iPad, key fob, etc...

### Credential ID

The fixed 12-digit code from the security token beginning with: AVTxxxxxxx (key fob) or VSMxxxxxxx (software token)

### Security Code

The 6-digit code from the security token that changes every 30 seconds



**Register Your Credential**

\* Required Information

\*Credential Type: VIP Credential

\*Credential Name:   
Enter a simple name that is easy to remember.

\*Credential ID:

**What is a Credential ID?** Close

**Credential ID examples:**  
Your credential contains a unique alphanumeric ID.

 VIP Security Token (Back)	 VIP Security Card (Front)	 VIP Access
-------------------------------	-------------------------------	----------------

\*Security Code:

**What is a Security Code?** Close

**Security Code examples:**  
Your credential provides a dynamic 6-digit code that changes every 30 seconds.

 VIP Security Token (Front)	 VIP Security Card (Front)	 VIP Access
--------------------------------	-------------------------------	----------------

5. Click **Submit** to register your token
6. Your Token is now linked to your network account; you may log in to the VPN using your network ID, password, and the **6-digit PIN**

If you have any issues while registering the token, contact the Helpdesk.



## Accessing your Exchange Email Remotely

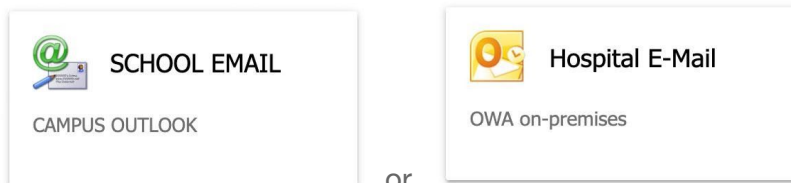
---

### Prerequisites

You must have a registered Two Factor Authentication token.

### Login Instructions

1. Click on the appropriate link:  
**Hospital Employees** who have a @mountsinai.org email address: <https://msvpn.mountsinai.org>  
  
**School Employees** who have a @mssm.edu email address: <https://msvpn.mssm.edu>
2. Enter your AD username (network account ID)
3. Enter your network Password
4. Click on **“Continue”**
5. Enter your 6-Digit VIP Security Code (the code changes every 30 seconds)
6. Click **“Login”**
7. You will be directed to a webpage that offers a link to Webmail. Click this icon in that window to access your mail.



# RDP over VPN for Windows

## System Requirements

Windows 8.1, Windows 10

## Logging into VPN

1. Open a web browser and navigate to the appropriate VPN portal

[Hospital Employees](#)

[School Employees](#)


[Vendors](#)

2. Login using the following:

Enter your AD username

Enter your Password

Click on **“Continue”**

  
**Mount Sinai**

Secure Logon  
for Mount Sinai Health System

VIP code is entered on the next page.

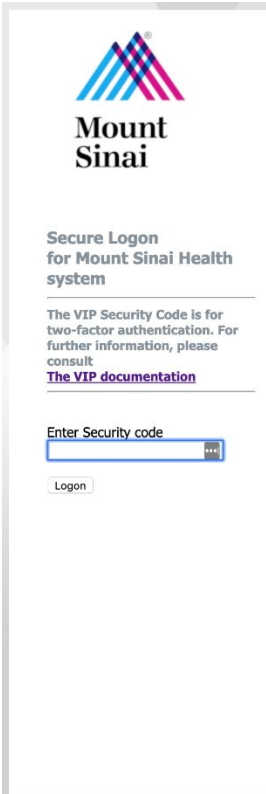
**Windows 7 Not Supported as of Jan 2020**

WARNING: UNAUTHORIZED USE, POSSESSION, DUPLICATION, OR TAMPERING WITH MOUNT SINAI HOSPITAL COMPUTERS, DATA, INFORMATION, PROGRAMS OR SERVICES IS A VIOLATION OF POLICY AND A CRIMINAL OFFENSE. VIOLATORS ARE SUBJECT TO DISMISSAL AND/OR PROSECUTION.

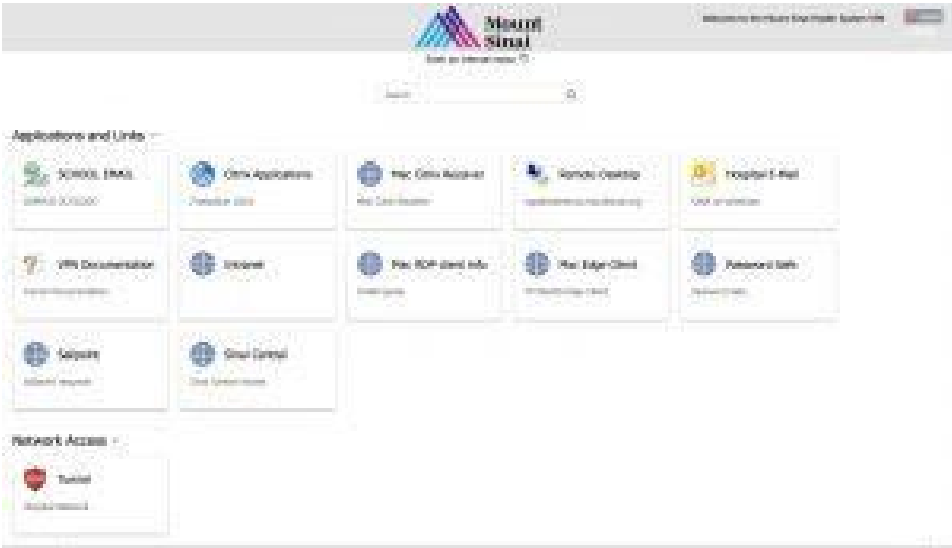
Username

Password

3. Enter the VIP Security Code (the code changes every 30 seconds)

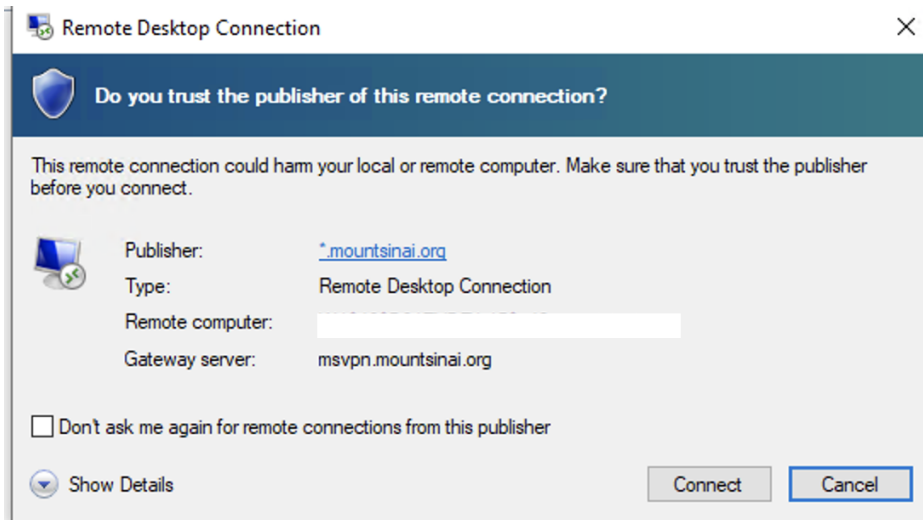


- 4. Click **“Login”**
- 5. Once logged in you will see a window displayed with icons for a number of applications. Click on the icon titled **“Remote Desktop”**



- 6. The RDP connection configuration file will be downloaded to your PC. When the download is complete, click on the **“Open”** button

7. A window titled “**Remote Desktop Connection**” will open. Click on the “**Connect**” button



8. You will now be logged into your assigned Windows Desktop

### **Known Issues and Troubleshooting:**

**Q: I login to the Mount Sinai VPN on a Windows PC, but I do not see the RDP icon.**

**A:** Your workstation was not added to your AD account. Please contact the Helpdesk to have your workstation’s Fully Qualified Domain Name added to your AD account for RDP access.

**Q: The RDP icon appears, but when I click on “Connect” I get the error message “The connection was denied because the user account is not authorized for remote login”.**

**A:** Your AD network account was not added to the AD group to allow Remote Desktop Connection. Please contact the Helpdesk to have them add your account to the RDP Group for Remote Desktop Connection.

# RDP VPN for MAC OSX

## System Requirements

Download and install the [Remote Desktop Client from the Apple Store](#) on your Mac. More information on the Microsoft RDP client for Mac is available [here](#).

## Logging into VPN

1. Open a web browser and navigate to the appropriate VPN portal:

[Hospital Employees](#)

[School Employees](#)


[Vendors](#)

2. Login using the following:

Enter your AD username

Enter your Password

Click on **“Continue”**

  
**Mount Sinai**

Secure Logon  
for Mount Sinai Health System

VIP code is entered on the next page.

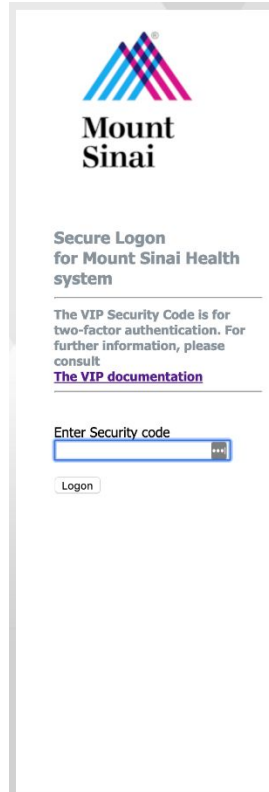
**Windows 7 Not Supported as of Jan 2020**

WARNING: UNAUTHORIZED USE, POSSESSION, DUPLICATION, OR TAMPERING WITH MOUNT SINAI HOSPITAL COMPUTERS, DATA, INFORMATION, PROGRAMS OR SERVICES IS A VIOLATION OF POLICY AND A CRIMINAL OFFENSE. VIOLATORS ARE SUBJECT TO DISMISSAL AND/OR PROSECUTION.

Username

Password

3. Enter the VIP Security Code (the code changes every 30 seconds)



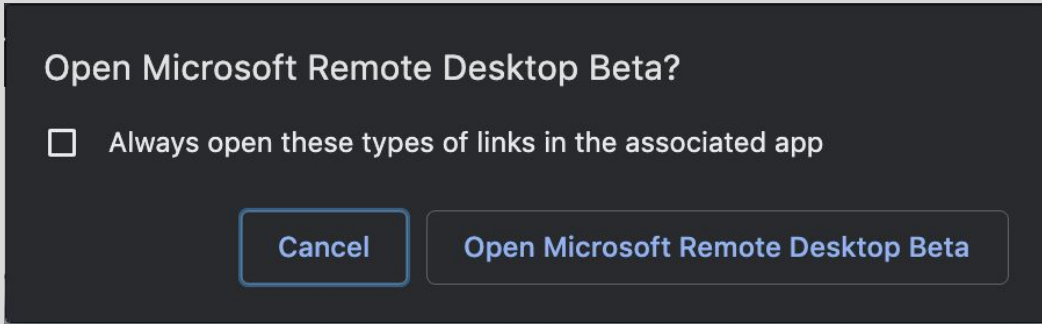
4. Click **“Login”**
5. Once logged in you will see a window displaying icons for a number of applications. Click on the icon titled **“Remote Desktop”**



6. You will see an additional popup to allow you to access Remote Desktop using the Microsoft RDP client for MAC  
Instructions below differ by browser type.

### Chrome Users

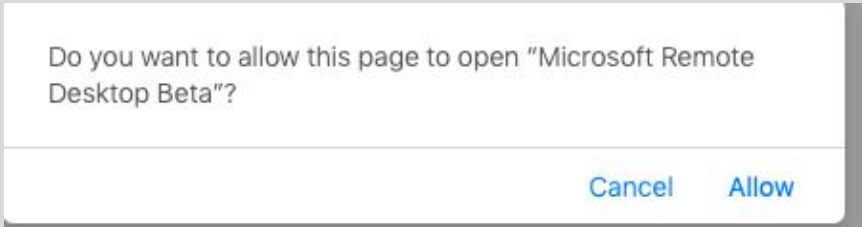
Click on 'Open Microsoft Remote Desktop'



Select 'Always open these types of links in the associate app'

### Safari Users

Click on "Allow"



An additional prompt will ask you to put in your password. Enter your AD Password and click on 'Continue'

*Note: a User ID starting with f5 will be put in the username field. You do not need to put your User ID as this is passthrough from the f5 client.*

**Enter your user account**

This user account will be used to connect to  
[redacted]:3389 (remote PC).

Username: f5\_ [redacted]

Password: [redacted]

Cancel Continue

You will be logged into your assigned Window Desktop

## Known Issues and Troubleshooting

**Q: I login to the Mount Sinai VPN on a Windows PC but I do not see the RDP icon.**

**A:** Your workstation was not added to your AD account. Please contact the Helpdesk to have your workstation's Fully Qualified Domain Name added to your AD account for RDP access.

**Q: The RDP icon appears, but when I click on "Connect" I get the error message "The connection was denied because the user account is not authorized for remote login".**

**A:** Your AD network account was not added to the AD group to allow Remote Desktop Connection. Please contact the Helpdesk to have them add your account to the RDP Group for Remote Desktop Connection.



## VPN Tunnel for Windows

---

### System Requirements

Windows 8.1, Windows 10

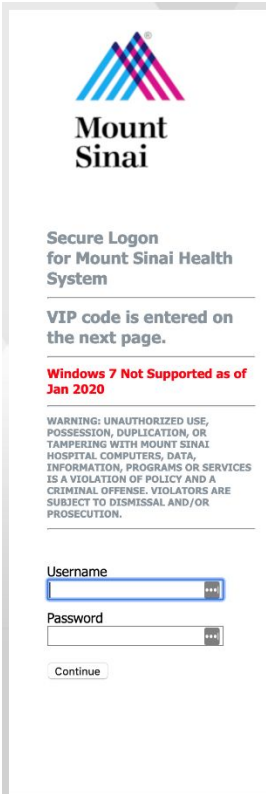
*Note: If you wish to connect via VPN Tunnel, you will need local admin rights to install the F5 Plugin during setup.*

**Antivirus (AV) signatures must have been updated** within 7 days of your last signature update; If you have not been updated, you will not be able to connect to MSHS network via VPN Tunnel.

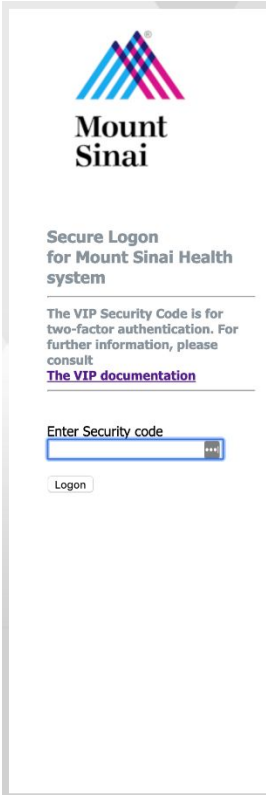
**Home Antivirus (AV) cannot be expired**; if not valid, you will not be able to connect to MSHS network via VPN Tunnel.

### Logging into VPN

1. Launch a web browser and go to the appropriate VPN Portal:  
[Hospital Employees](#)  
[School Employees](#)  
[Vendors](#)
2. Login Using the following:  
Enter your AD Username  
Enter your Password
3. Click on “**Continue**”



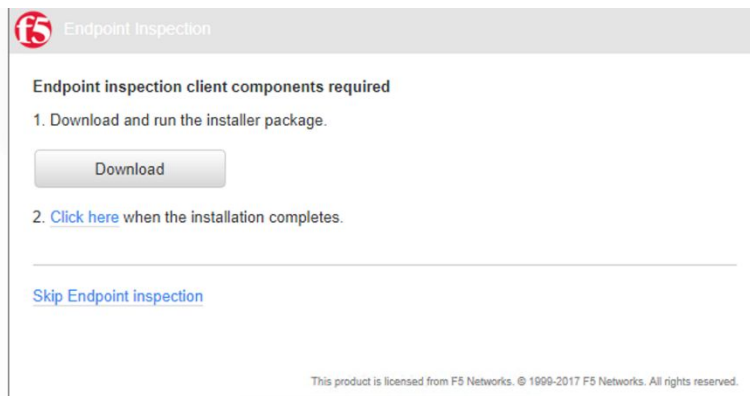
4. Enter the VIP Security Code (the code changes every 30 seconds)



5. Click **“Logon”**

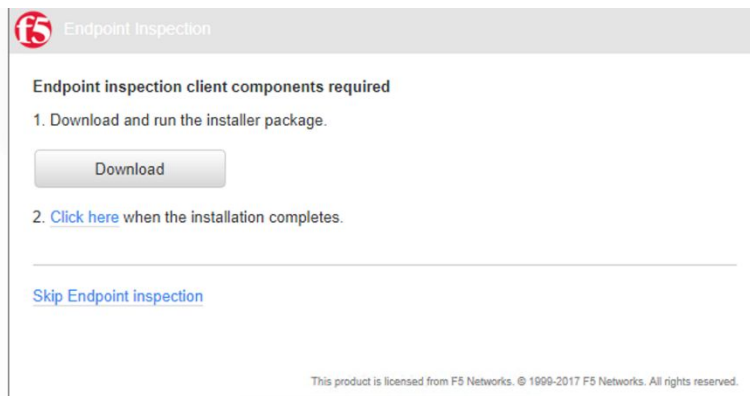
*Note: If you do not have a VIP Security token, visit <https://itsecurity.mssm.edu/wiki/vip-two-factor-setup/> for more information.*

6. Once logged in you will be prompted to download and install the F5 Endpoint Inspection Client



7. Once the file is downloaded, f5epi\_setup.exe, double click to install

8. **“Click here”** when the installation is complete

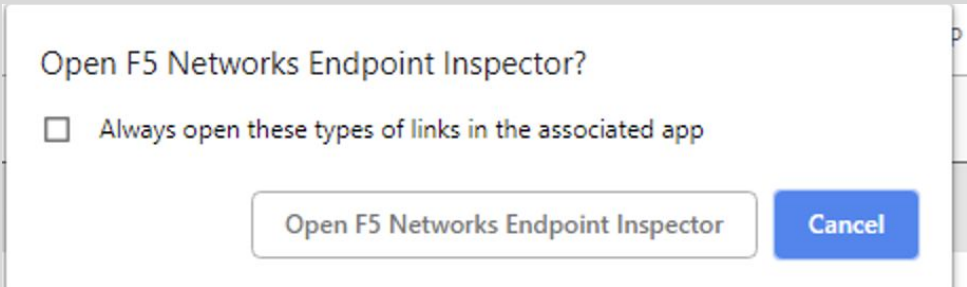


9. For first time install or upgrades to F5 Inspection Client, you will be required to add the site to the computer trusted site list  
*Instructions below differ by browser type.*

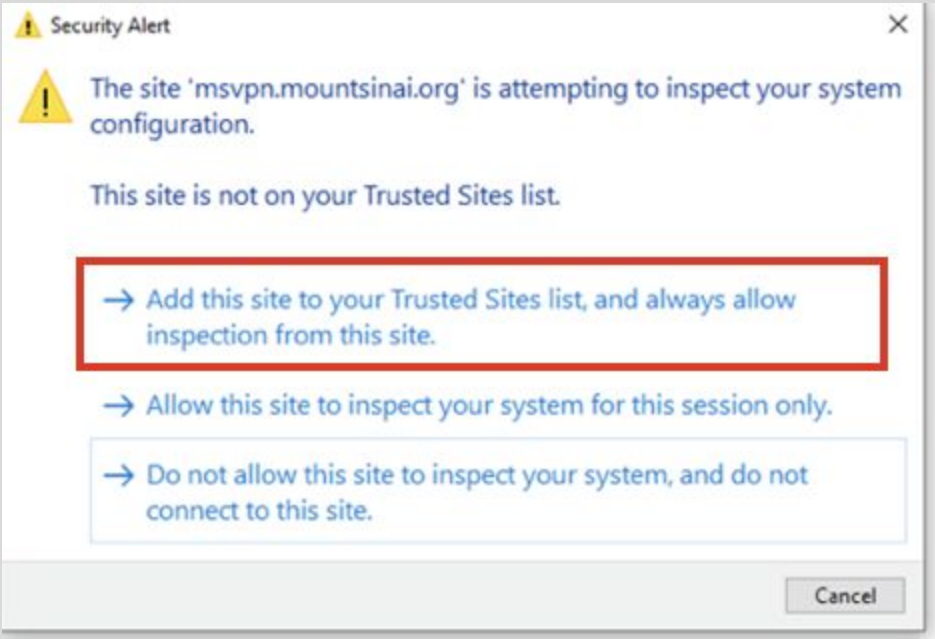
## Chrome Users

You will get a popup asking to Open F5 Network Endpoint Inspector, select **“Always open these types of link in the associated app”**

Click on “Open F5 Network Endpoint Inspector”

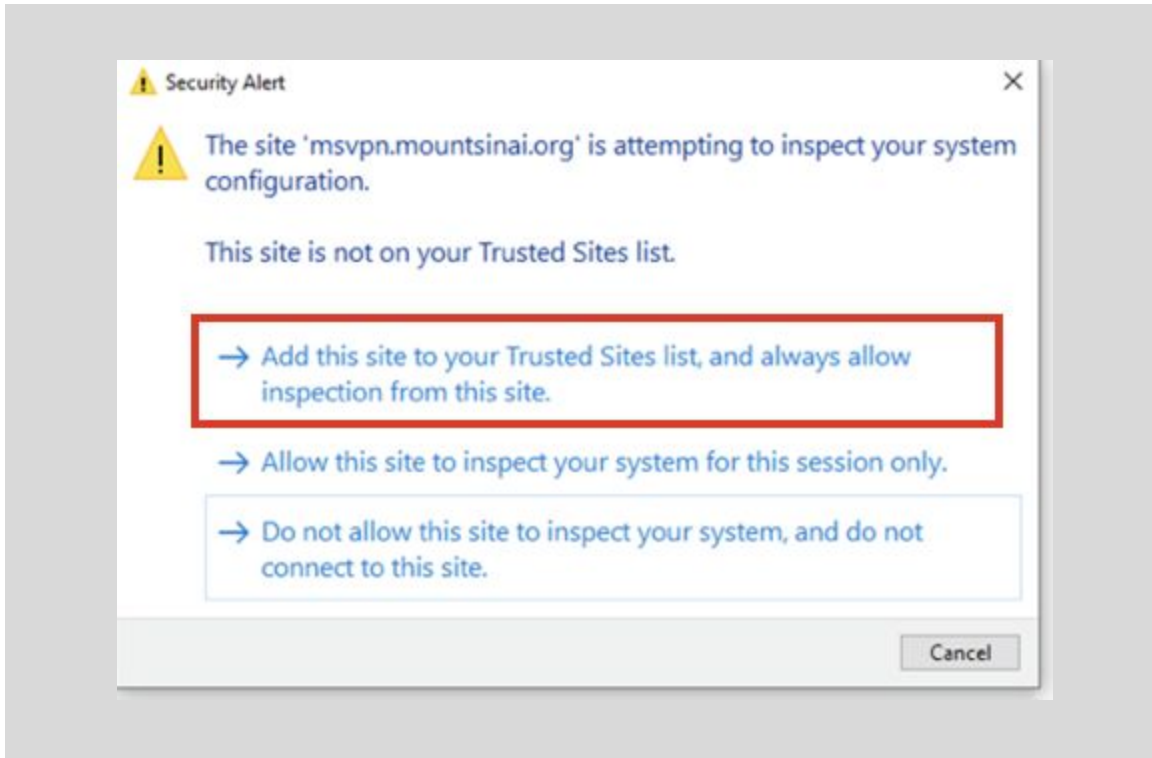


Click on “Add this site to your Trusted Site List” and “Always allow inspection from this site”



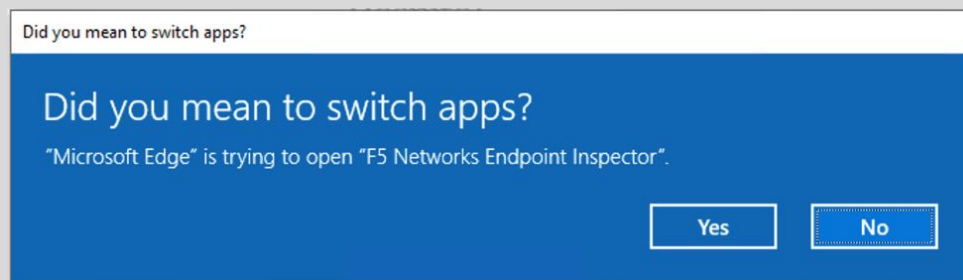
## Internet Explorer Users

You will get a popup asking you to add the site to your trusted site list, select ‘Add this site to your Trusted Site List’, and ‘Always allow inspection from this site’



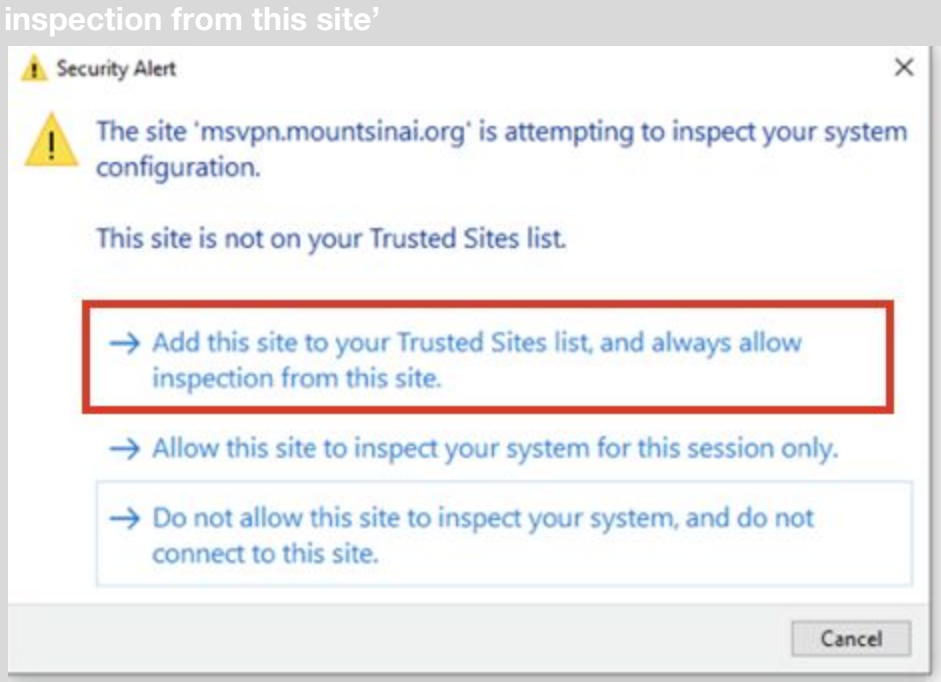
## Microsoft Edge Users

You will get a popup asking 'Did you mean to switch apps?' Microsoft Edge is trying to open the F5 Network Endpoint Inspector.'

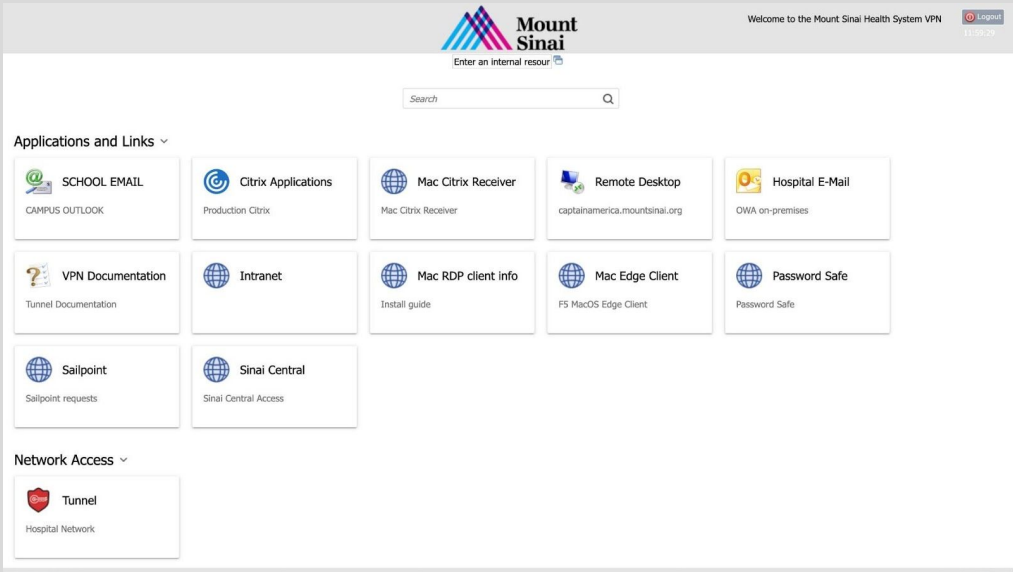


Click on Yes

Click on 'Add this site to your Trusted Site List' and 'Always allow



You will now be redirected to the MSVPN page  
Click on **Network Access** and click on **Tunnel**



Another popup will come up, wait until the tunnel says 'Connected' and then minimize the popup.  
*Note: If you close out of the popup, you will disconnect yourself from the Tunnel Session.*

The screenshot shows a web browser window titled "Network and Application Access - Internet Explorer provided by The Mount Sinai Medica...". The main content area displays a "Connected" status with a green dot and a "Disconnect" button. Below this, the connection duration is shown as "00:00:12". A table provides a breakdown of network traffic:

Traffic Type	Sent	Compression	Received	Compression
<b>Network Access</b>				
- Network Tunnel	18.91 KB	0%	14.18 KB	0%
- Optimized Applications	0 B	0%	0 B	0%
<b>Total</b>	<b>18.91 KB</b>	<b>0%</b>	<b>14.18 KB</b>	<b>0%</b>

Below the table is a link "+ Show details".

# VPN Tunnel for Mac

---

## System Requirements

MAC OSX

*Note: If you are tunneling in for the first time, you will need to install the F5 Plugin during setup which requires local admin rights.*

## Logging into VPN


Open a web browser and navigate to the appropriate VPN Portal:

[Hospital Employees](#)

[School Employees](#)

[Vendors](#)

1. Login using the following:  
Enter your AD username  
Enter your Password  
Click on **“Continue”**

  
**Mount Sinai**

Secure Logon  
for Mount Sinai Health  
System

VIP code is entered on  
the next page.

**Windows 7 Not Supported as of  
Jan 2020**

WARNING: UNAUTHORIZED USE,  
POSSESSION, DUPLICATION, OR  
TAMPERING WITH MOUNT SINAI  
HOSPITAL COMPUTERS, DATA,  
INFORMATION, PROGRAMS OR SERVICES  
IS A VIOLATION OF POLICY AND A  
CRIMINAL OFFENSE. VIOLATORS ARE  
SUBJECT TO DISMISSAL AND/OR  
PROSECUTION.

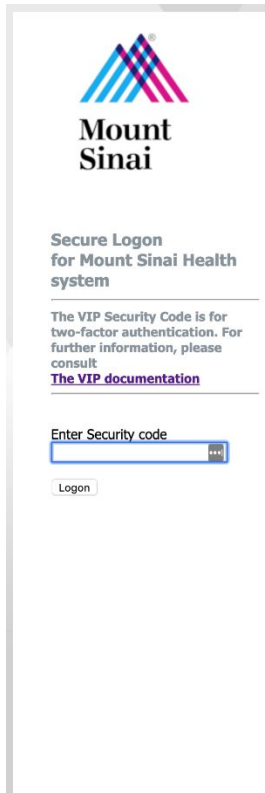
Username

Password

Continue



2. Enter your VIP Security Code (the code changes every 30 seconds)
3. Click on **“Login”**

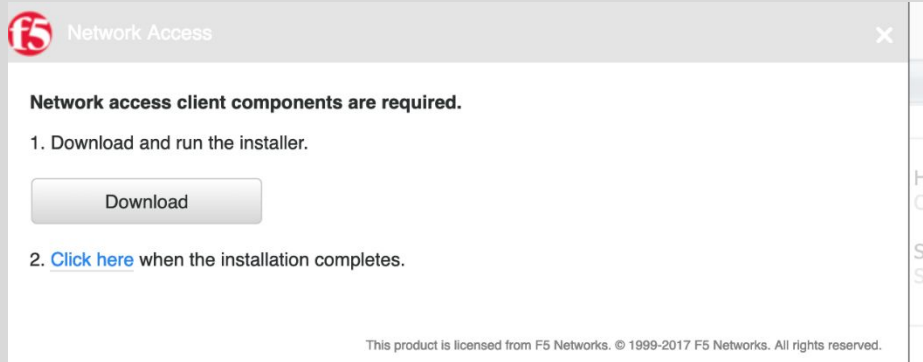


4. If you do not have a VIP Security token, please visit <https://itsecurity.mssm.edu/wiki/vip-two-factor-setup/> for more information.
5. Once logged in, the VPN Webtop App launcher page will be displayed. Click on the icon titled **‘Tunnel’**  
*Instructions below differ by browser type.*



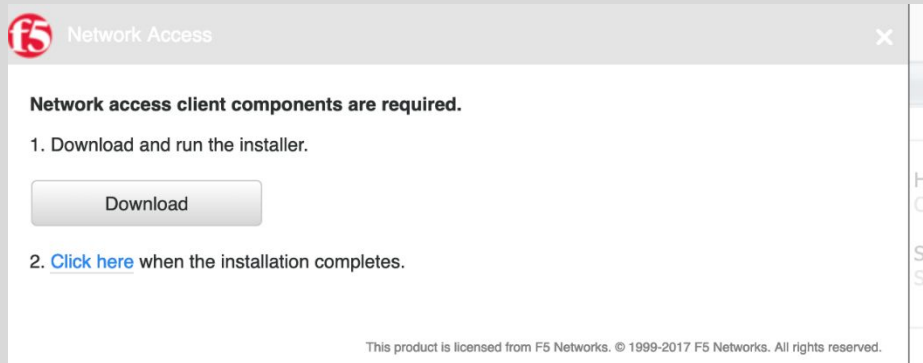
### Chrome Users

You will be prompted to install F5 Endpoint Inspection Client;  
Click **Download**

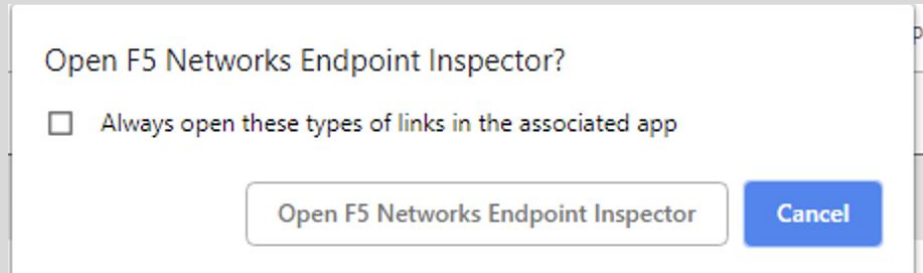


Click on **F5 Download and install** (mac\_f5vpn.pkg)

Once it is installed, click on “**Click here**” when the Installation completes



You will get a popup asking to Open F5 Network Endpoint Inspector –  
Click on “**Always open these types of link in the associated app**”  
Click on “**Open F5 Network Endpoint Inspector**”

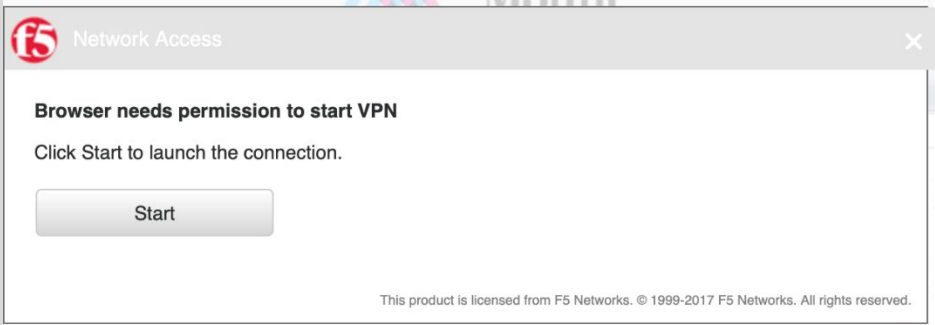


F5 VPN Security Warning will popup, click on “Always allow your VPN connection from this site”

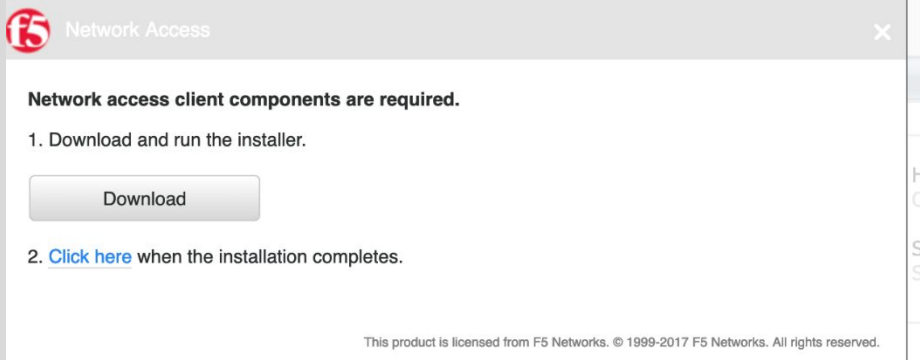


### Safari Users

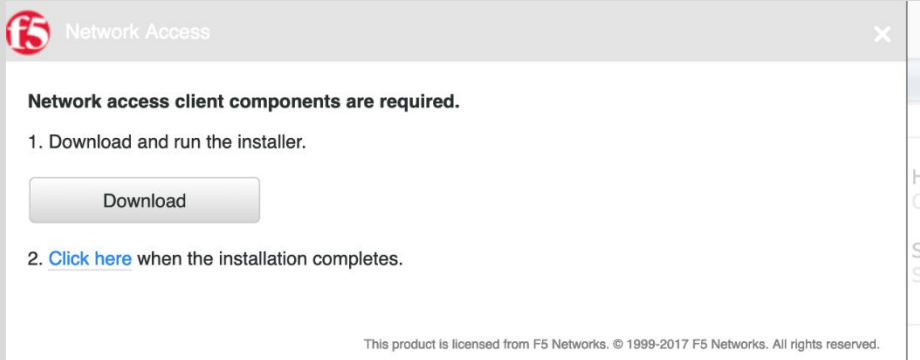
Click on **Start** to give the Safari Browser permission to start the VPN process



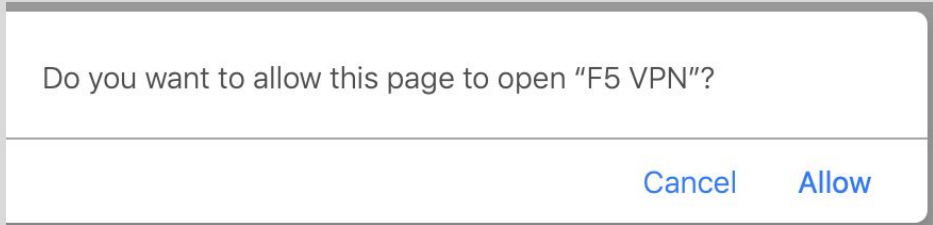
You will be prompted to install F5 Endpoint Inspection Client. Click “Download”



Click on **F5 Download and install** (mac\_f5vpn.pkg)  
“Click here” when the installation completes



A new popup will appear “Do you want to allow this page to open “F5 VPN”. Click on “allow”

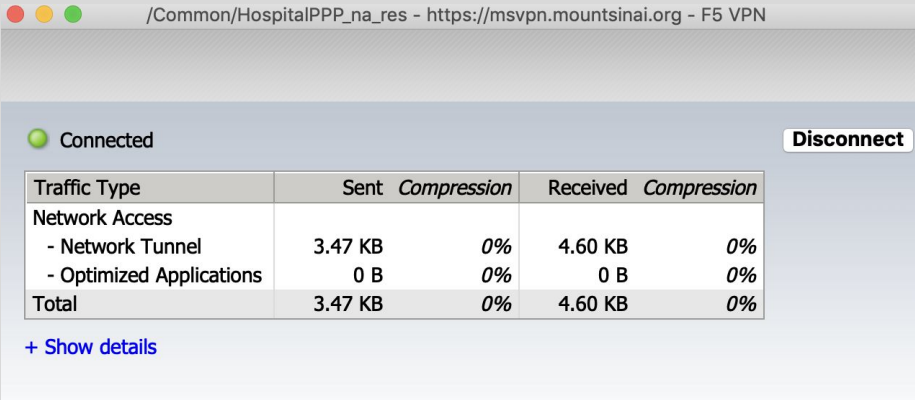


F5 VPN Security Warning will popup. Click on “Always allow your VPN connection from this site”



Another popup will come up. Wait until the “Connected” is displayed and then minimize the popup.

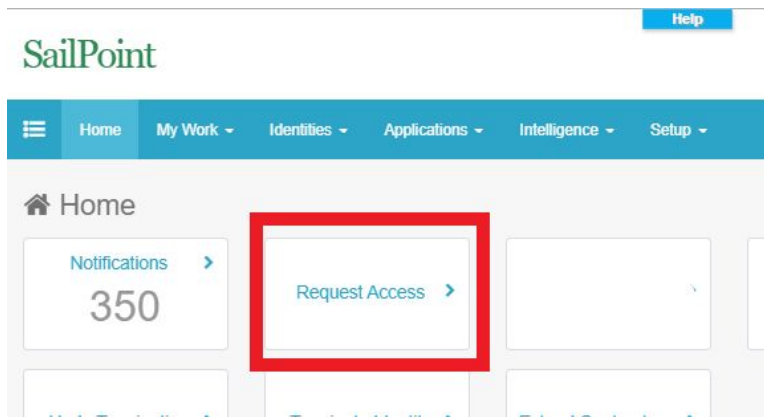
*Note: If you close out of the popup you will disconnect from the Tunnel Session.*



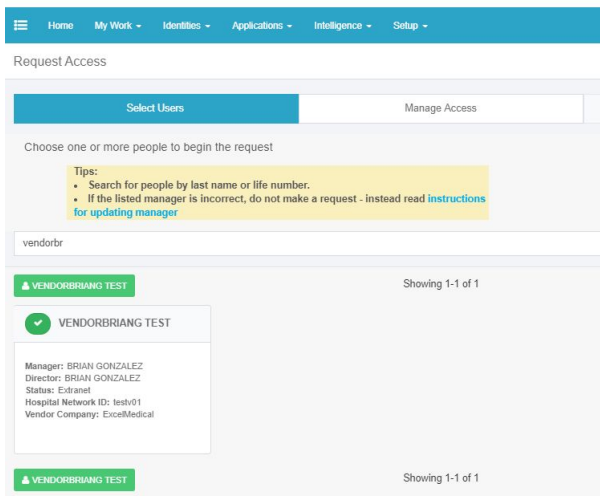
# Sailpoint

## Requesting Access

1. Login into [Sailpoint](#) while on the Mount Sinai network (in the office or VPN)
2. From the home screen click on **'Request Access'**



3. Type in the user's last name, full name or life number to search for the user you want to request access for
4. Select the user by clicking on the check mark



5. Click on **'Manage Access'** tab and Select **'Role Type = IT'** from the dropdown

If you need...	Then search for this Sailpoint entitlement...
Citrix Desktop Access	<b>Hospital VPN Citrix</b>
Meditech Access	<b>NYEE-VPN for Meditech Access</b>
Remote Access to a Dedicated Mount Sinai Workstation – only one user can be connected to a workstation.	<p><b>Hospital VPN RDP</b> (for hospital employees)</p> <p><b>Hospital VPN RDP for Vendors</b> (non-employees)</p> <p><b>School VPN RDP</b> (for ISMMS users)</p>
Tunnel Access – most users should not need this level of access.	<p><b>Hospital VPN Tunnel</b> (for hospital employees)</p> <p><b>Hospital VPN Tunnel for Vendor</b> (non-employees)</p> <p><b>School VPN Tunnel</b> (for ISMMS users)</p>

For RDP and Tunnel access, you will be asked to provide a hostname/domain name after you have submitted the request within Sailpoint. For Mount Sinai built workstations, you can find this information on the desktop wallpaper. Just provide the three lines of information highlighted below:



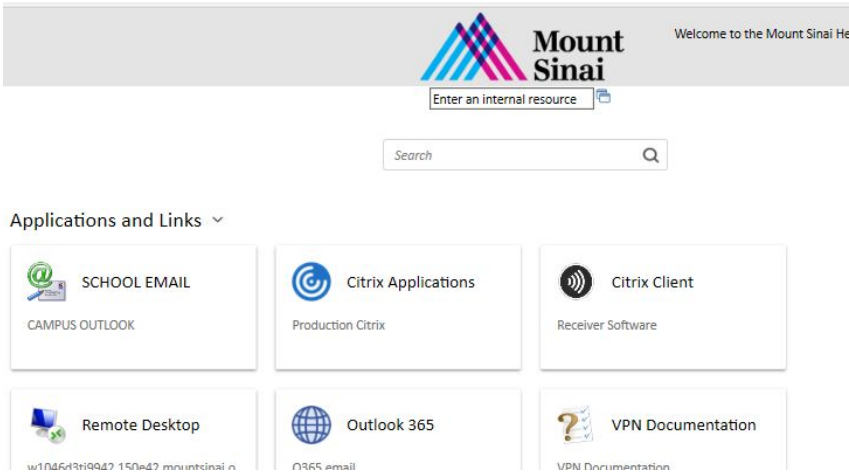
The information can also be obtained by opening a CMD prompt in Windows and entering the command “**ipconfig /all**”. You’ll need to provide the Host Name, the Connection-specific DNS Suffix, and the IPv4 Address.

The manager for the individual will also need to approve the request by logging into Sailpoint.

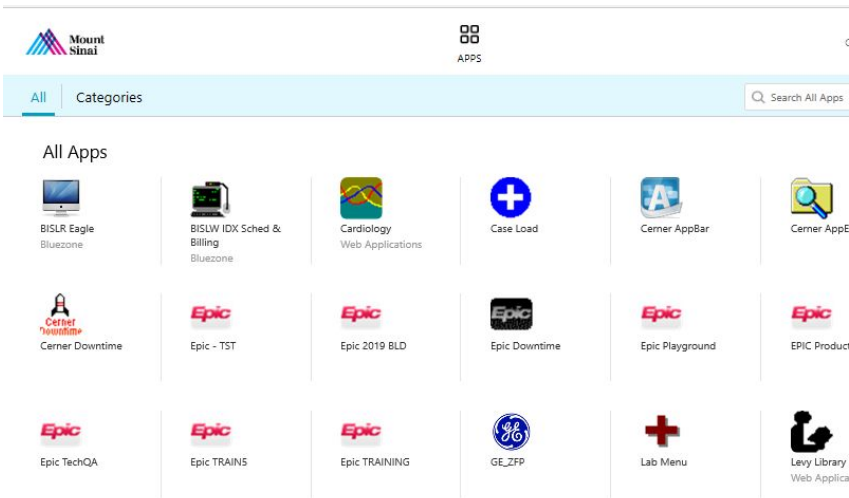


# Citrix Access

After logging into the VPN, you will find a tile to launch the Citrix Applications:



*Note: You may need to install or update the Citrix Client. You will find a tile with the latest software located next to the Citrix Applications tile on the VPN portal. After installing the software, you can click on the Citrix Applications tile. Some browsers may download an .ica file rather than open it automatically in the Citrix Client; in that case, look for the downloaded file and launch the file manually.*



## Bring Your Own Devices (BYOD) Best Practices

---

As an organization with a commitment to security and safety, we are responsible at an individual level to maintaining a secure workspace. The following should be done before setting up remote access and maintained regularly to avoid exposure to security risks.

### 1. Keep your computer operating system (OS) and applications patched

Update Flash, Java, Adobe Reader, and other software.

[Check Qualys](#) offers a good browser checker which will let you know if your software is up to date.

[Microsoft supporting documentation](#)

[Apple supporting documentation](#)

### 2. Enable antivirus

You can enable the built in Windows Defender software or you can opt to purchase a third party antivirus software. [How to enable Windows Defender](#)

### 3. Enable device encryption and password protect your system

Don't use the same password across multiple accounts and don't use your Mount Sinai password for your private email or social media accounts.

[Microsoft supporting documentation](#)

[Apple supporting documentation](#)

### 4. Use trusted software

Use only licensed software, don't download software from file sharing sites. Beware of "free software".

### 5. Secure your home network

National Cyber Security Alliance has a number of good recommendations on [their website](#).

[Safe computing tips](#) from the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA).

[Apple MacOS supporting documentation](#)

[Microsoft Windows supporting documentation](#)