NIST Onboarders Guide to Telecommuting

Getting Connected

Published April 7, 2020
About This Guide

This NIST Onboarders Guide to Teleworking provides information you need to know before you can begin teleworking at NIST.

Please note that throughout this document, you will come across links to NIST systems, applications, and other resources that you won’t be able to access at this time. Don’t worry, as you don’t need to access these resources prior to your virtual onboarding session. We are providing this content for informational purposes only in order to make you aware of what you will need to do once you gain access to the NIST network. To avoid confusion, any links that are nonoperational prior to your onboarding will be highlighted in blue throughout this document (Example: https://idam.nist.gov).

Are You Ready to Telework?

The Telework Enhancement Act of 2010 defines “telework” or “teleworking” as a work flexibility arrangement under which an employee performs the duties and responsibilities of his or her position, and other authorized activities, from an approved worksite other than the location from which the employee would otherwise work. Telework is a critical tool during emergency situations that also provides employees with a greater work/life balance. Using technology, employees can perform their job duties at a remote location, instead of physically commuting to the office. Telework/telecommuting as an alternative work arrangement has emerged as an essential management tool for the federal government.

NIST is committed to maximizing telework capacity by entering into telework agreements with as many telework-eligible employees as possible. For more information on the NIST Telework Policy, please reference Appendix A, NIST Directive O 3102.00, Telework Program. Once a telework/telecommuting agreement is in place, this guide will introduce you to the practical tasks of preparing to telecommute.

Before you telework, be sure to:

- Read this guide in its entirety while connected to the NIST Network. Obtain any resources you may need in the event you cannot connect.
- Work with your supervisor to put a telework agreement in place.
- Determine what tasks can be done via teleworking
- Obtain your SSL Remote Access account and RSA SecurID Token
- Request a NIST-issued mobile device (smartphone, tablet, mobile hotspot), if necessary.

If you don’t have government-furnished equipment you can take home:

- Understand the requirements for allowing personally owned equipment on the NIST network.
- Obtain Key Files so your personally owned equipment can connect to the NIST network.

Confirm your computer, mobile devices, and personal devices work properly for teleworking by testing this guide at home prior to official telework.
Know how to leverage a variety of tools by:

- Using Office 365, Skype for Business, SharePoint Online, Google Docs, BlueJeans, and the Virtual Desktop Infrastructure (VDI) system for collaborating with your NIST colleagues
- Accessing and managing your voicemail remotely
- Setting up a conference call when teleworking.
Contents

About This Guide ............................................................................................................................................ 1
Are You Ready to Telework? ............................................................................................................................ 1
1. Setting Up Your Computer for Teleworking ................................................................................................. 5
   1.1 Requesting and Obtaining an SSL Remote Access Account and/or RSA SecurID Token .............. 5
   1.2 Obtaining and Installing SSL Remote Access Key Files ............................................................... 6
   1.3 Setting up Remote Access on your NIST Office Computer ............................................................ 6
   1.4 Getting Connected to the NIST Network While You Are Teleworking ........................................... 8
   1.5 Connecting to the NIST Network on a Windows Computer ............................................................. 8
   1.6 Connecting to the NIST Network on a Mac Computer ..................................................................... 11
      1.6.1 PIV Authentication Using Google Chrome ............................................................................. 11
      1.6.2 PIV Authentication Using Edge Client .................................................................................. 12
      1.6.3 Logging into SSL Remote Access Service ............................................................................. 12
      1.6.4 Troubleshooting ..................................................................................................................... 13
      1.6.5 Verifying an Identify Preference ............................................................................................... 13
   1.7 Mobile Devices ....................................................................................................................................... 14
   1.8 Connecting to Your Workstation Remotely ........................................................................................... 15
      1.8.1 How to Remotely Access Your Work Computer (Windows Computer) ............................. 15
      1.8.2 How to Remotely Access your Work Computer (Mac Computer) ...................................... 17
2. Mapping Network Drives ............................................................................................................................ 19
   2.1 Windows 10 Computer ....................................................................................................................... 19
   2.2 Mac Computer ..................................................................................................................................... 21
   2.3 Unix/Linux Computer ......................................................................................................................... 21
3. Collaboration Software ................................................................................................................................. 22
   3.1 Skype for Business .............................................................................................................................. 22
   3.2 Office 365 ............................................................................................................................................ 22
   3.3 SharePoint Online/OneDrive ................................................................................................................ 23
   3.4 Google Docs ......................................................................................................................................... 23
   3.5 BlueJeans ............................................................................................................................................. 23
   3.6 Virtual Desktop Infrastructure System ............................................................................................... 24
4. Telephone Systems ........................................................................................................................................ 24
   4.1 Accessing Voicemail Remotely ........................................................................................................... 24
   4.2 Forwarding Your NIST Desk Phone Number to Any Number Using Xpressions Voicemail Web Assistant  ........................................................................................................................................... 24
1. Setting Up Your Computer for Teleworking

While there may be policies and procedures that must be satisfied in order to be able to telework, there are also several steps related to your computer that must be in place in order to have a successful remote connection to the NIST network.

These include:

- Requesting and obtaining an SSL Remote Access account and/or RSA SecurID Token
- Obtaining and installing SSL Remote Access Key Files
- Setting up Remote Access on your computer.

1.1 Requesting and Obtaining an SSL Remote Access Account and/or RSA SecurID Token

The SSL Remote Access (SSL RA) Service provides access to internal NIST networks and IT services from offsite. SSL Remote Access runs on Windows, MacOS X, and Linux computers as well as iOS and Android mobile devices. SSL Remote Access is available via a web browser or from a browser-free application, called F5 BIG-IP Edge Client (or Edge Client, for short), which is supported on NIST-Managed MacOS and Windows laptops and tablets. Android and iOS mobile devices may also use Edge Client to access NIST remotely.

If you are using a NIST-managed laptop with a PIV card reader, you should use your PIV card to authenticate to SSL Remote Access; however, you may require an RSA SecurID Token if you do not have a PIV Card, you are not using a NIST Issued device that can utilize a PIV card, or you require a backup method of authentication. Note that you are not required to have an RSA Token if you plan to use a NIST-issued device with a PIV card.

The RSA SecurID token, which is used to connect to the internal NIST network from outside networks, provides two-factor authentication, an enhanced security measure that is used to confirm an individual’s identity using two forms of identification.

The RSA SecurID token is a small device (or key fob) that generates a new, six-digit token display code every 60 seconds, as shown in the following example. (A bar on the left of the token display indicates when the current six-digit number will expire and be replaced by a new one.)

The six-digit token code (the one that displays the moment you log in) is used at the end of a user-selected PIN (of six to eight alpha/numeric characters) to form a passcode.

For example, using a PIN of 617548 and number that appears in the above image of a token device, your passcode would be 617548159759.
1.2 **Obtaining and Installing SSL Remote Access Key Files**

A Key File is a file on a computer that contains encryption or license keys. Key Files are required on all operating systems (Windows, Mac, and Linux) and are obtained through iTAC. (The Mac and Linux Key Files are not interchangeable with the Windows Key File.) Key Files have already been installed on NIST-owned computers; however, if you intend to use your personally owned computer for access to the NIST network, you must obtain the NIST SSL RA Key Files.

For future reference, please see Appendix B, Remote Access NIST Key File Installation Instructions.

1.3 **Setting up Remote Access on your NIST Office Computer**

If you will be leaving a workstation in the office and plan to connect to it while you are teleworking, you must enable it to accept Remote Desktop connections (How to make the remote connection is described in Section 1.8, Connecting to Your Workstation Remotely.

For Windows users, NIST is pushing out a BigFix Offer for Remote Desktop Protocol (RDP), allowing you to bypass the steps in this section. The offer is titled, “Allow Remote Desktop Connections to this Computer,” and can be found in the BigFix Support Center, Offers Tab.
The offer will:

- Enable Remote Desktop for your computer
- Ensure the firewall ports are open to allow the connection.
- Add the current user to the remote desktop user group to ensure you’ll be able to login even if you are not an administrator.

It is important that you accept this offer when the window pops up on your computer.

Mac users should submit a ticket as screen sharing will be required, and this is controlled by secure configurations. Users can also contact iTAC at any time for assistance with enabling RDP on their computer.

While it is highly recommended that you use the BigFix offer to configure RDP, in the event you do not receive the offer, use the following instructions.

To set up Remote Desktop on your NIST workstation, you must have administrative rights. If you do not have administrative rights to your workstation, submit a ticket via the NIST Service Portal at [https://services.nist.gov](https://services.nist.gov) ([Submit a Ticket > Hardware and Systems > Admin rights/local account on computer]). You will need to provide your name, your workstation’s property tag, and its operating system. The ticket will automatically be routed for approval.

To access your NIST office workstation with Remote Desktop when you are offsite, you will need to know your workstation’s computer name and IP address. For instructions on how to find your computer name and IP address, please go to Appendix C, Finding Your Computer Name or IP Address.

To enable your workstation to accept Remote Desktop connections, perform the following steps (using Windows 10):

1. In the search field (to the right of the Start button), type **Control Panel**.
2. Click the **Control Panel App**.
3. Click **System and Security**.
4. Click **System**.
5. Click **Remote settings** on the side of the screen. Note that you may need to enter your PIV credentials at this point.
6. Select the **Allow remote connections to this computer** checkbox.
7. Click **Apply** and then click **OK**.

### 1.4 Getting Connected to the NIST Network While You Are Teleworking

Now that you have obtained all the tools necessary to get on the NIST Network, it’s time to connect!

If you are using a NIST-owned Windows or Mac computer or an iOS or Android mobile device, you can access the NIST network remotely using F5 Edge Client. The F5 Edge Client is a software application that minimizes the time and effort required to gain secure, remote access to the NIST network. You can locate it from the Start menu (Windows), in your Dock (Mac), or on your apps screen (called F5 Access) on your mobile device.

**Note:** If Edge Client is not available because you are using a personally owned computer or it is not functioning for some reason on your government device, you can access the NIST network remotely by entering the URL [https://inside.nist.gov](https://inside.nist.gov) in your web browser and authenticating via PIV or RSA and PIN as described in the instructions below.

**Note:** If prompted, install F5 Network Components/Plug-ins.

### 1.5 Connecting to the NIST Network on a Windows Computer

1. From the Start Menu, select **NIST BIG-IP Edge Client** (or select the **F5** button on your taskbar). The following window opens.
2. Click **Connect** and follow the authentication process.

3. If you are using a PIV card:

   **(1.)** Select the authentication certificate tied to your PIV card.

   **Note:** If PIV authentication is not available, and the PIV card Select Certificate popup appears, click **Cancel** to continue with RSA authentication (see instructions on Page 10).

   ![Certificate Selection Window]

   These are your **PIV Authentication Certificate** and **Digital Signature Certificate**. For SSL remote access, you must select the **PIV Authentication Certificate**.

   By default, the certificates displayed on the selection screen look similar and may be differentiated by a description preceding your name in the certificate title.

   **Note:** If you select the wrong certificate, once you enter your PIN, you will receive an error page, “Failed to get UPN from PIV certificate. Please **completely** close browser (all tabs) and try again by selecting the other certificate.” Simply do as the instructions say and choose the next certificate after you close and reopen the browser.

   **(2.)** If you cannot determine what certificate to use, place your cursor (hover) **over your name** on each certificate and select the one that shows **YOURNAME’s U.S. Government PIV Authentication**.

   **(3.)** Click **OK**.
(4.) Type your PIV PIN and click OK.

You are now connected to the NIST network.

If you are using RSA Authentication (using your RSA Token):

(1.) If you are not using PIV authentication (i.e., a mobile device, personally owned device, or your PIV is not functioning), you must enter your NIST username and RSA token passcode (PIN + token code) instead of a PIV PIN.

When logging in through Edge Client or the inside.nist.gov URL for Remote Access, your anti-virus definitions and all operating system (OS) updates must be current. Supported web browsers include Chrome, Safari, and Internet Explorer, and these should also be current.

The system will go through several security checks, including a virus scan, and you may be prompted to allow code to be dynamically downloaded and run. This needs to be permitted because it is required for SSL Remote Access to work properly. You may also be prompted to configure your browser to allow popups from the NIST SSL Remote Access server.

You will receive one of the following messages:

- **Access Denied**: Your system updates and virus definitions are not current.
- **Full access granted**: Virus definitions and Windows updates are current; continue to the login process.

Please see [Appendix D, OS/Browser/Anti-Virus Supported by SSL Remote Access](#), to find out what OS and anti-virus products are recognized by the SSL Remote Access functionality.

(2.) Select NIST Network Access and click Continue.
(3.) Once Connected, minimize the NIST Network Access window by clicking the minimize button ((_(' in the top right of the window.

You are now connected to the NIST network.

1.6 Connecting to the NIST Network on a Mac Computer

Following are instructions on how to connect to NIST’S SSL Remote Access (SSL RA) Service via Google Chrome and the F5 BIG-IP Edge Client using your PIV card and macOS.

1.6.1 PIV Authentication Using Google Chrome

1. Direct your browser to https://inside.nist.gov. The system will run through several security checks, including a virus scan, and you may be prompted to allow code to be dynamically downloaded and run. This needs to be permitted because it is required for the SSL RA to work properly. You may also be prompted to configure your browser to allow popups from the NIST SSL RA server.

2. Upon completion, the following window displays, prompting you to choose the PIV Authentication certificate. Click on Cancel if you want to login using RSA Token.

3. Select the PIV Authentication certificate to authenticate yourself to inside.nist.gov:443. (Verify under Subject Alternative Name Extension that the certificate has username@nist.gov for NT Principal Name.)

4. Click OK. The following popup window opens with a message stating that Google Chrome is trying to authenticate user.
1.6.2 PIV Authentication Using Edge Client

Edge Client is an application installed on your laptop computer or mobile device that allows you to connect to the SSL RA service without having to log in using a web browser.

To use PIV authentication with Edge Client, it is necessary to have an Identify Preference using the Keychain Access app. Without this preference in place, you will be prompted to authenticate using your RSA SecurID token. For NIST-managed macOS laptops, the Identity Preference will be auto-generated.

1.6.3 Logging into SSL Remote Access Service

1. From your dock, select NIST F5 BIG-IP Edge Client for macOS (or CMD + spacebar, search for big-ip) icon to connect to https://inside.nist.gov. An authentication popup window opens, stating that NIST Edge Client is trying to authenticate user.

2. The system will run through several security checks, including a virus scan, and you may be prompted to allow code to be dynamically downloaded and run. This needs to be permitted because it is required for the SSL RA to work properly.

3. Upon completion, the following window displays, prompting you to choose a certificate for the PIV card authentication.

4. The following popup window opens with a message stating that NIST Edge Client is trying to authenticate user.
5. In the field provided, enter your PIV PIN and click OK. The Network Access Type window opens, as shown in the partial screenshot below.

6. From the Network Selection dropdown, select Network Access Below and then click Continue.

7. Upon successful authentication, the following window appears, confirming that you are connected to the NIST network.

1.6.4 Troubleshooting

If your PIV card is inserted, and you are redirected to the Secure Logon for NIST Remote Access Users, you might need to verify the associated Identity Preference.

1.6.5 Verifying an Identify Preference

1. To open the Keychain Access app, enter CMD + spacebar.

2. In the Spotlight Search bar, enter keychain.
3. In the Search bar within Keychain Access, enter *.nist.

4. Two-finger tap on touchpad (Right-click equivalent) on *.nist Identity Preference option and select Get Info.

5. Verify that the Identity Preference is created and is free of errors. The screenshot below verifies it is correct.

6. If there are issues, try removing your PIV card after closing the Keychain Access App and NIST BIG-IP Edge Client for macOS.

7. Insert your PIV card and launch NIST BIP-IP Edge client for macOS to try again.

Please see Appendix E, New SSL Remote Access Service – Guide for Mac OS X, for RSA token (non-PIV) access instructions and references.

1.7 Mobile Devices

NIST-owned, encrypted mobile devices and select mobile operating systems (iOS and Android) are centrally supported by the Office of Information Systems Management (OISM) and may be used to directly synchronize with NIST email (i.e., download and store email messages and/or attachments.)
The F5 Access Client is also available on your NIST-owned mobile device for connecting to the NIST Network (Note that email and calendaring work without F5 Access enabled). Launching the F5 Access application on your mobile device and following the authentication prompts will provide you with mobile device access to NIST network resources. Mobile devices that are not PIV enabled will require authentication with your RSA Token and PIN as described in the above sections.

If you do not currently have a NIST-owned mobile device, your supervisor and Administrative Officer will be able to assist you with eligibility and obtaining a device.

Knowledge Article 0017172, [NIST Mobile Device and Management Price List](#), provides a list of NIST-approved mobile devices as well as a link to the [Mobile Device Request Form](#) in the NIST Service Portal. If you do not currently have a wireless account, be sure to request one when requesting the mobile device account, as well. This request will be sent to your supervisor for approval.

### 1.8 Connecting to Your Workstation Remotely

#### 1.8.1 How to Remotely Access Your Work Computer (Windows Computer)

**NIST-Managed Computer to NIST-Managed Computer**

1. Make sure you have enabled your work computer (that is still at work and turned on) for Remote Access by following the instructions in Section 1.3, Setting up Remote Access on your NIST Office Computer.

2. Follow the steps listed in Section 1.4, Getting Connected to the NIST Network While You Are Teleworking.

3. Once connected, in the search box (to the right of the Start menu), type **Remote Desktop Connection**.

4. Click once on the **Remote Desktop Connection** app in the list.

5. Where it says Computer, type your **Computer Name or the IP Address**.

   **Note:** To find out how to get your Computer Name and IP address, see [Appendix C, Finding Your Computer Name or IP Address](#).

6. **Click Connect.**
The login screen opens.

7. Type in your PIN if you are using a PIV-required device or type your General Realm username and password if you are not on a PIV-required device.

8. Your office desktop displays. You are now connected.

**Personal Computer to NIST-Managed Computer**

1. Follow Step 1 through Step 4 above.

2. In the lower, right corner of the window, click the **Show Options** button.

3. In the Computer field, type your **Computer Name or the IP Address**.

   **Note**: To find out how to get your Computer Name and IP address, see [Appendix C, Finding Your Computer Name or IP Address](#).

4. In the User Name field, type **NIST/General Realm username**

5. **Click Connect**.

   The following screen appears:
6. Select your authentication certification and type in your PIN if you are using a PIV-enabled device or type your General Realm username and password if you are not on a PIV required device.

A Windows screen appears, prompting you to authenticate via Windows Hello or Smart Card.

7. If you are authenticating via Smart Card and it doesn’t automatically bring you to the Smart Card login, click on Sign-in options and then select the Smart Card icon.

You may also log in with your username/password if your device is not PIV enforced.

1.8.2 How to Remotely Access your Work Computer (Mac Computer)

This guide is to assist users with using the Microsoft Remote Desktop client in order to connect to a Windows computer that is set up to accept Remote Desktop connections. This will not work with a Mac to Mac connection, only Mac to Windows.

1. From your Applications folder of your Mac, launch Self Service.
2. Within Self Service, search for **Remote** and then click **Install**. This will install "Microsoft Remote Desktop" in your Applications folder.

3. From your Applications folder, launch **Microsoft Remote Desktop**.
4. For the PC name, you will need to enter the IP address or fully qualified domain name (Example: PN12345.campus.nist.gov). To enable smart card support, when adding a new connection under Devices & Audio, check the Smart cards box to enable passing of your smart card to the remote Windows PC.

![Microsoft Remote Desktop](image)

**Note:** For users who are offsite, an SSL Remote Access connection is required to continue.

5. You will be asked for your username when connecting to the Windows PC, however, the Windows login will accept your smartcard.

2. **Mapping Network Drives**

In the event you need to map a network drive, please refer to the instructions below for Windows, Macintosh and Unix/Linux computers. You will need to be connected to the NIST network to access and map network drives.

2.1 **Windows 10 Computer**

Whether you are onsite or teleworking, it’s always a good idea to map your network drives so that you can access them quickly without having to look for them or type their network address each time.

1. Open **File Explorer** 📁 from either your taskbar or the **Start** menu, or by pressing (⊞️ + E).

2. From the navigation pane on the left, select **This PC**. Then, on the **Computer** tab, as shown below, select **Map network drive**.
The Map Network Drive box opens.

3. In the **Drive** list, select a drive letter. (Any available letter will do.)

4. In the **Folder** box, type the path of the folder or computer (e.g., `\elwood.nist.gov\182\users\doejm`), or select **Browse** to locate and select it. (If you do not know your path or folder name, please see your supervisor.)

5. To connect each time you log onto your PC, select the **Reconnect at sign-in** check box.

6. Select **Finish**.

   **Note:** If you can’t connect to a network drive or folder, the computer you are trying to connect to might be turned off, or you might not have the correct permissions.

If you want to disconnect the network drive, right-click on it and select **Disconnect**.
2.2 Mac Computer

This method connects to and maps a network drive or network share that will disappear if the network connection drops, is disconnected, or if you reboot your Mac:

1. From the Mac OS X Finder, hit **Command+K** to bring up the 'Connect to Server' window.
2. Enter the path to the network drive you want to map (e.g., smb://networkcomputer/networkshare) and click **Connect**.
3. Enter your login/password and click **OK** to mount the network drive.
4. The drive will now appear on your desktop and in the Finder window sidebar.

You can access the network share like any other folder at this point, so long as it's maintained on the same network.

2.3 Unix/Linux Computer

SMB mounting is provided at the Operating Unit level, Division level, and NIST level. Some Unix/Linux client implementations will not permit you to mount at the home directory level; instead mount at the Operating Unit or Division level and navigate to your home directory once the share is mounted.

Owing to the numerous variations among different implementations of Unix and Linux operating systems the OISM does not provide instructions that will necessarily work in all situations.

Generally speaking, the following command appropriately modified will work provided you have the privileges to run the command in your environment:

```
% mount -t cifs -o username='NIST domain userid' //'file server name/path' 'local mount point'
```

The file server name would be one of the following: elwood.nist.gov, cfs2e.nist.gov, cfs2w.nist.gov, or jake.nist.gov.

Although it is possible to use a password argument with this command, we recommend that you omit the argument. You will be prompted for the password once the command is entered.

Some Linux OS versions (Red Hat and CentOS) may require the "sec=ntlmssp" option to be specified in order for the mount to be successful.

Examples:

```
% mount -t cifs -o username=straw,sec=ntlmssp //elwood.nist.gov/18_OISM /mnt
```

or

```
% mount -t cifs -o username=straw,sec=ntlmssp //elwood.nist.gov/184 /mnt
```

In this example, to navigate to your user directory you would:

```
% cd /mnt/users/straw
```

Some OS versions may support the following command appropriately modified:
%smbmount //file server name/path' 'local mount point' -o username='NIST domain userid', workgroup='NIST'

Although it is possible to use a password argument with this command, we recommend that you omit the argument. You will be prompted for the password once the command is entered.

A graphical user interface in your environment may provide dialogs sufficiently similar to those discussed above for Windows and Macintosh such that you can modify those instructions appropriately for your environment.

3. **Collaboration Software**

NIST maintains licenses for collaboration software that can make telecommuting easier and more engaging. This software is managed by OISM and has been specifically provisioned and secured for your use. You should contact your ITSO for guidance before storing NIST data on software that is not in this guide.

Broadly, OISM provides a place to store NIST data for Office365, Google’s G-Suite, Box, Slack, Overleaf, BlueJeans, Gitlab, and others. If you are not sure if you are using supported collaboration software, check https://inet.nist.gov/adlp/open-access-research-oar/collaboration-tools.

Also note that some of these tools come with associated license costs that will be billed to your OU. Work with your OU to get the appropriate approvals to purchase licenses. The following tools have unique concerns while teleworking.

3.1 **Skype for Business**

Skype for Business is a video and chat platform that allows you to talk within NIST and to agencies that also use Office 365 for their email. For example, you can invite @doc.gov, @ita.gov, and other DOC agencies (with the exception of NOAA) to participate in your Skype for Business meetings. When you try to invite an external collaborator, it’s important to emphasize that “Skype for Business” is used, and not “Skype.”

**Important teleworking tips:** Please limit your usage of the “call-me” feature, OISM has a limited number of those minutes available for all NIST staff. Instead, you can get a phone number added to every meeting, which your collaborators can call to participate. Complete https://psd.oism.nist.gov/pstn to get a Skype for Business conference line.

3.2 **Office 365**

Office365 is NIST’s email and internal document collaboration tool. The Office365 Portal (https://portal.office.com) is the central place to get access to this service. From the Office365 Portal you can click “Outlook” to access your NIST email. With this interface, no program is required to be installed. While in the Outlook application, you can also click the calendar button to see your NIST calendar. This is identical to the data you will see on your desktop applications. You’ll notice other applications in this portal, such as Microsoft Word, Excel, and PowerPoint. When you launch these applications, you are creating documents in OneDrive, which is a SharePoint Online platform and described below.

**Important teleworking tips:** When multiple people inside NIST need access to a document, consider uploading that document to Office365 rather than sending the document as an attachment. That way, they’ll see any future updates, and you won’t need to send a new document.
3.3 SharePoint Online/OneDrive

SharePoint Online is a document collaboration system that is designed for Microsoft documents. You can edit these documents at the same time as your collaborators using the “Edit Online” feature. If you have multiple collaborators working on a document at the same time, OISM does not recommend editing those documents in the desktop application. By using the online interface, you can see the sections that your collaborators are editing, and no individual’s work will be lost.

Many NIST users are frustrated by SharePoint Online when they try to edit a Microsoft document using desktop applications. For example, if you disconnect from the VPN while teleworking your changes may be lost. By editing the online versions of your documents, you and your collaborators can edit Microsoft documents in real-time. OISM recommends this approach for any file where your collaborators are within NIST or are other Microsoft Office 365 customers. This also works well when you would like to share a document with anyone at NIST, and you don’t yet know who your NIST collaborators will be on the document.

3.4 Google Docs

Google Docs is an alternative document editing system that works well when you’re not sure if your collaborators can access Office365, and you know the email address of each collaborator. Unlike Office365, specific files are shared with specific people. These people can be internal or external to NIST and are not required to have a .gov email address.

Google Docs can support dozens of collaborators editing a single document using the “Suggestion” feature. In Office365, track changes show every change that has been made but doesn’t show who made those changes. Google Docs shows each collaborator’s edits independently and allows you to reject and add those individual changes. OISM recommends giving new collaborators “Comment” access to your Google Docs documents, so that you can see these individual changes.

The system also allows you to give Edit access to your collaborators, which allows them to directly make changes to documents. Google Docs includes the other Google applications that provide for real-time collaborative editing including, Slides, Sheets, and Google Forms.

OISM does not recommend using Google Docs when you want to share a document broadly inside of NIST, because not everyone at NIST has a NIST Google account. If you or your NIST collaborator would like a Google account, contact iTAC.

3.5 BlueJeans

BlueJeans is an online meeting platform similar to Skype for Business. When you are not sure if all your collaborators have Skype for Business accounts, you might choose to instead host your video meeting in BlueJeans. Think of BlueJeans as a more formal meeting platform than Skype for Business. With BlueJeans, you can mute your meeting attendees, set a meeting password, add encryption, and other meeting features that are more typical for formal scheduled meetings. These meetings can also be recorded, for later viewing on NISTube.

To see who your OU’s BlueJeans account holder is, visit this INET link: https://inet.nist.gov/oism/bluejeans-account-holders. Your OU representative can schedule BlueJeans meetings for you, or you can contact iTAC to get a BlueJeans account.
3.6 Virtual Desktop Infrastructure System

The NIST Virtual Desktop Infrastructure (VDI) service provides Windows 10 virtual desktops for use on a temporary basis. These virtual desktops provide quick and easy access to a Windows 10 instance for use with web-based applications such as CBS and e-approval, Microsoft Office applications, and remote access. Mac and Linux users no longer need to use Parallels or virtual machines to run Windows/Internet Explorer-based apps. These virtual desktops are easily accessed, secure, and require no maintenance by the user.

Teleworking employees and associates may find that they need a Windows 10 computer on the NIST network to access certain web sites or applications that are not available from their remote machine. If this is the case, simply contact iTAC (x5375) and request access to VDI. A VDI Support Team member will be in contact to help you get connected.

Please note that accessing the VDI system does require a connection to the NIST network through the VPN from your remote computer.

4. Telephone Systems

4.1 Accessing Voicemail Remotely

There are two ways that your voicemail can be accessed when you are not in the office. One method is to use the table below to determine the appropriate number to call and then follow the prompts once connected. Note that you will need to know your phone extension and PIN number.

<table>
<thead>
<tr>
<th>Origination</th>
<th>Access Number</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boulder Local</td>
<td>303.497.7070</td>
<td>Follow the prompts.</td>
</tr>
<tr>
<td>Boulder Long Distance</td>
<td>1.800.579.5383</td>
<td>Follow the prompts.</td>
</tr>
<tr>
<td>Gaithersburg Local</td>
<td>301.975.3380</td>
<td>Follow the prompts.</td>
</tr>
<tr>
<td>Gaithersburg Long Distance</td>
<td>1.800.437.4385</td>
<td>When prompted to dial your party's extension, enter 3380# and then follow the prompts.</td>
</tr>
</tbody>
</table>

You can also access your voicemail via the Unify OpenScape Xpressions web system at [https://xpressions.nist.gov](https://xpressions.nist.gov). You will need to enter your NIST general username and password to log into this system.

4.2 Forwarding Your NIST Desk Phone Number to Any Number Using Xpressions Voicemail Web Assistant

4.2.1 Gaithersburg Campus

Any user of the NIST telephone system who currently has a voicemail account may forward their NIST extension to up to eight different numbers on or off campus.

A NIST user may create up to nine different alternate greetings guiding the caller to select the number to choose where the call should be routed.
For example:

- Press 2 to reach me at my alternate number – Mobile Number
- Press 3 to reach me at my alternate number – Telework Site
- Press 4 to reach me at my alternate number – Lab

By using the Xpressions Web Assistant, a NIST user has the flexibility to change the number to any number they wish at any time. Or, once the Mobility feature is activated, the user may also change this service by dialing into the Xpressions Voicemail number at 301.975.3380 and performing the following steps:

1. From the Main Menu, press the **pound key (#)** to continue.
2. Press 8 to change your answering options
3. Press 5 to make changes to the Mobility feature.

For additional information on how to use OpenScape Xpressions, reference Knowledge Article 0010347, *How to Set Up and Use OpenScape Xpressions Voicemail*, and open the attachment entitled, *OpenScape Xpressions Voicemail Mobility Destination.docx*.

### 4.2.2 Boulder Campus

Any user of the NIST Boulder telephone system can forward their NIST extension number to a telework number or mobile phone by submitting a ServiceNow ticket requesting call forwarding.

The request must contain your current NIST extension, and the telework number/mobile number for forwarding. The Telecom Boulder team will then program a **phantom number** and the user will be provided that phantom number.

In order to forward your NIST extension, the user must Press the forward button on your Boulder phone, then enter the phantom number, then press forward again.

After completing these steps your NIST extension will forward automatically to your telework/mobile phone.

### 4.3 Setting up a Conference Call While Teleworking (Boulder Staff)

To make a conference call with more than six participants, or if you are unable to establish the call from a NIST telephone, you may set up a conference bridge with the current provider.

A conference bridge can be established anytime, 24x7x365, by completing the following:

1. Dial **1.800.475.5000** (Verizon Conferencing).
2. Follow the prompts.
3. Press or say 1.
4. Press or say 1 for instant meeting, press or say 2 for audio conferencing. (The two options are the same thing, only with a different setup. The operator can clarify/assist you if you need more information).
5. You are prompted for your authorization code. Say 7134507V. (You must speak it; however, no matter how clearly it is spoken, the system will repeat it back to you and then connect you with an operator.)

6. The operator will ask you to verify your agency: US Dept. of Commerce/NIST/Boulder. The operator should then be able to reserve your audio call.

**Important Tips:**

- Be sure to inform the operator if there will be any callers internationally, as they will have a separate line to dial into the hub.
- The operator offers toll and toll-free lines for national and international callers.
- Make sure to inform the operator of the time zone in which the call will take place. (e.g., Pacific, Mountain, Central and Eastern).

### 4.4 Setting up a Conference Call While Teleworking (Gaithersburg Staff)

Conference calls can be generated when teleworking away from the NIST campus while conducting official government business. You may set up a conference bridge by creating a NIST subscription.

To create your NIST subscription, call Reservations (24x7x365) at 1.866.900.1011 and provide the following information:

- Company Name: NWX-US DEPT OF COMMERCE-1
- Authorization Code: 1453920V

Or, if you would like to create an online My Meetings account, go to [https://www.mymeetings.com/mm/servlet/RequestLoginAudio](https://www.mymeetings.com/mm/servlet/RequestLoginAudio) and register for a login username and password. You will need the above Company Name (NWX-US DEPT OF COMMERCE-1) and Authorization Code (1453920V) information.

For assistance, please reference this [Getting Started Guide](#) or contact Customer Assistance at 1.866.900.1011.
You are now ready to telework!

Any problems, questions, or concerns, please call iTAC:

Boulder: 303.497.5375
Gaithersburg: 301.975.5375

**Hours of Operation:**
Boulder - Monday – Friday 7:30 a.m. to 5:30 p.m.
Gaithersburg – Monday – Friday 7:30 a.m. to 7:30 p.m.

To reset your RSA Token PIN when offsite, call iTAC. You will need to provide the following:

- Serial number of your RSA Token

If you did not set up a profile of questions and answers in EPS, iTAC cannot reset your RSA Token password by telephone.
Appendix A. NIST Directive O 3102.00, Telework Program

Purpose
This Order defines the requirements of the National Institute of Standards and Technology (NIST) telework program. This directive complies with the Department of Commerce (DOC) Telework Program and Policy (05/10/2018).

Applicability
This directive is applicable to all NIST Federal employees.

Where an employee requests telework as a reasonable accommodation, the Department of Commerce “Reasonable Accommodation for Employees or Applicants with Disabilities” (DAO 215-10) applies rather than this policy.

Legal Authority
- Telework Enhancement Act of 2010

References
- Annual Telework Eligibility Notification and Updated Telework Policy Information for Federal Employees (Email from Director, Office of Human Resources Management to all NIST Federal Staff, July 15, 2015).
- NIST P 3100.00 Human Resources (HR) Management
- NIST O 2105.00 Site Access During Site Closure and Delayed Openings

Requirements
NIST shall comply with the DOC Telework Program and Policy (05/10/2018) and all other requirements as identified by NIST below.

Eligibility
An employee shall be eligible to telework if:
- The employee is on a performance plan for at least 120 days; and
- The first-level supervisor has determined that the employee is performing at or above a contributor level.

An employee shall not be eligible to telework if:
- The employee has been officially disciplined for being absent without permission for more than five (5) days in any calendar year; or
- The employee has been officially disciplined for viewing, downloading or exchanging pornography, including child pornography, on a Federal Government computer or while performing official Federal Government duties.
- Except in emergency situations determined by the head of the agency, telework does not apply to any employee whose official duties require, on a daily basis:
- Direct handling of secure materials determined to be inappropriate for telework;
- On-site activity that cannot be handled remotely or at an alternate worksite.

**Participation**

Participation requires:

- A written and signed agreement outlining the specific work arrangement (see [NIST DN-27, NIST Telework Program, Employee/Supervisor Agreement](#));
- That the performance of the employee complies with the terms of the mandatory written agreement;
- That the employee has a complete and signed Performance Management Record (NIST 01) or Executive Performance Agreement in place for at least 120 days, and the supervisor has determined that the employee is performing at or above a contributor level;
- Completion of training, as required by the DOC Telework Program and Policy, by both the employee and the supervisor/manager prior to the implementation of a Telework Agreement;
- A completed and signed Alternative Worksite Safety Checklist -- if the worksite is in a private residence -- where all applicable questions were answered in the affirmative, or, if answered in the negative, confirmation that the employee will take all necessary corrective actions to eliminate any hazard prior to beginning telework (see [NIST DN-27a, Alternative Worksite Safety Checklist](#));
- Emergency contact information be incorporated as part of continuity of operations plans as appropriate.

An employee’s telework privileges may be revoked if:

- The first-level supervisor determines that the employee’s performance does not comply with the terms of the signed NIST Telework Program Employee/Supervisor Agreement.

An employee may elect to terminate his/her participation in the telework program at any time.

**Telework Plans**

An employee shall have the opportunity to choose between one of two telework options, subsequent to the concurrence of the first-level supervisor:

**Situational:**

- The employee shall follow OU policies and procedures for requesting ad hoc/unscheduled telework which shall be approved on a case-by-case basis
- The employee shall be required to telework if NIST announces delayed arrivals, early dismissals, or closures.

**Regular/Recurring:**

- The employee shall be scheduled for regular/recurring telework as outlined in the NIST Telework Program Employee/Supervisor Agreement.
- The employee shall be required to telework if NIST announces delayed arrivals, early dismissals, or closures.

**Incidents at Telework Sites**

Employees shall be covered under the Federal Employee’s Compensation Act (FECA) if injured in the course of performing official duties at the alternative worksite.
An employee shall notify their line management of any incident (e.g., work-related injury, near-miss, property damage, etc.) according to Organizational Unit (OU) policies and procedures for doing so.

Upon notification, NIST may investigate the incident report that occurred at the alternative worksite.

NIST will not be liable for damages to an employee’s personal or real property during the course of performance of official duties or while using NIST material in the employee’s residence or elsewhere, except to the extent NIST is held liable by the Federal Tort Claims Act or the Military Personnel and Civilian Employees Claims Act.

**Emergency Conditions**

- Although a variety of circumstances may affect individual situations, the principles governing administrative leave, dismissals, and closing remain unchanged.
- If teleworking at a GSA telework center:
  - Employees shall follow the arrival, dismissal, and closure procedures of the telework center regardless of NIST announcements of delayed arrivals, early dismissals, or closures.
  - If the arrival, dismissal, and closure procedures of the telework center limit the employee’s ability to perform their duties, the employee must notify his/her first-level supervisor and request administrative leave according to OU policies and procedures. First-level supervisors will consider requests for administrative leave on a case-by-case basis and will consult with the Office of Human Resources Management (OHRM) as necessary. Documentation in support of the request may be required.
- If teleworking from residence:
  - Employees shall be required to work during NIST delayed arrivals, early dismissals, and closures and will not normally be granted hazardous weather leave.
- Extenuating circumstances
  - If conditions at the telework site (e.g., power failure) affect the employee’s ability to perform his/her duties, first-level supervisors will have limited discretion to consider requests for administrative leave.
  - If conditions at NIST impact the ability to work at the telework site (e.g., the servers are shut down), employees at the telework site will be treated in the same manner as those working at NIST.

**Responsibilities**

**NIST Director**

- Serves as final approval authority for the NIST Telework Program.

**NIST Organizational Unit (OU) Directors**

- Authorizes the expenditure of funds for telework.
- Ensures the development of an OU telework program tailored to meet the needs of their employees, in accordance with NIST’s Telework Program.
- Ensures the consistent and appropriate implementation of the telework program within their OU:
  - Ensures that OU employees are not directed or coerced to participate in the telework program;
  - Ensures that telework agreements (NIST DN-27) are current and maintained by the Administrative Officers in the OUs and are available for review by the NIST Telework Coordinator.
- Ensures an annual evaluation of the telework program within their OU.
NIST Division Chiefs

- Review employee requests for participation in telework which have been disapproved by supervisors and the rationale for such decisions and for maintaining documented approvals/disapprovals to facilitate the evaluation, reporting and monitoring of the telework program. The Division Chief will communicate any telework denials to the employee and to the NIST Telework Coordinator.
- Maintain a record of the number of employees participating in the telework program.
- Making decisions regarding whether to permit exceptions to telework procedures on a case-by-case basis and providing these to the NIST Telework Coordinator.

NIST Supervisors

- Reviewing the "Telework Assessment Tool" (Appendix B in the DOC Policy) with the employee to determine the appropriateness of the employee teleworking prior to the employee submitting a formal request to telework.
- Evaluating an employee’s request to participate in telework in a timely manner.
- With advance notice of at least 24 hours, the supervisor or designee has the right to inspect the alternative worksite before the arrangement begins and at periodic intervals during the telework arrangement to ensure that the workspace is safe and that all equipment is adequately installed and performing properly.
- If telework is approved:
  - Orientating employees to the telework program and ensuring that employees new to telework complete training as required by the DOC Telework Program and Policy;
  - Completing training for first-level supervisors, as required by the DOC Telework Program and Policy;
  - Reviewing the employee’s Telework Safety Checklist to ensure it is complete when warranted;
  - Informing employees of those work tasks they are expected to perform while in a telework status;
  - Monitoring and evaluating the employee’s performance based on the employee’s Performance Management Record (NIST 01) or Executive Performance Agreement and the Telework Agreement.
  - Ensuring that telework-ready employees receive the same treatment and opportunities as non-telework-ready employees (e.g., work assignments, awards and recognition, development opportunities, promotions, etc.);
  - Ensuring that applicable policies and procedures are followed under a telework agreement with regard to removal of/accountability for government property, records and documents; and approval of overtime, leave, alternative work schedules, information security policies (particularly access/use, remote access, and mobile devices), etc.;
  - Ensuring employees properly and timely report telework equipment in accordance with NIST processes, including annual renewal and monthly certification as requested by the property custodian or property accountability officer;
  - Establishing communication requirements and methods to ensure the employee is kept informed of relevant information, performance expectations and progress, and is made aware of requirements to be available for contact by the supervisor, co-workers, customers, etc., including, but not limited to, scheduling staff or all-hands meetings on days and at times when the maximum number of employees are present at the regular worksites, and/or making arrangements for conference call connections for employees at alternative worksites;
  - Ensuring accurate employee recordation of telework in the time and attendance system.
  - Investigating employee reports of work-related injury or illness at the alternative worksite in much the same manner as would be the case for injury or illness at the traditional worksite;
During emergency conditions, ensuring that employees working at alternative worksites are aware of their working status if the NIST campus is closed or employees are given early dismissal; and

Terminating, modifying, or temporarily suspending telework agreements at any time for mission-related reasons (such as operational needs, changes in office priorities, vacancies or long-term leave of other employees in the office that cause office coverage issues, employee’s failure to adhere to the terms and conditions of the agreement, employee conduct, or employee performance, in accordance with the law and any applicable Collective Bargaining Agreements (CBA), rather than personal reasons).

- If a telework request is approved, but restricted:
  - Ensuring that restrictions are based on sound business or mission-related criteria (such as operational needs, employee conduct, or employee performance, in accordance with the law and any applicable CBAs, rather than personal reasons).

- If a telework request is denied:
  - Ensuring that denials are based on sound business or mission-related criteria (such as operational needs, employee conduct, or employee performance, in accordance with the law and any applicable CBAs, rather than personal reasons); and
  - If a telework request is denied, supervisors are required to submit a copy of the original request and the written denial to their supervisor and to the NIST Telework Coordinator.

- Responding to requests for information or reporting requirements from the NIST Telework Coordinator in a timely manner.
  - The approving official must deny or immediately terminate the agreement, as applicable, if the employee fails to be eligible to telework due to the reasons set forth in 5 U.S.C. §§ 6502(a)(2) or (b)(3).

**NIST Teleworking Employees**

- Request to participate in the telework program (through submission of DN-27, National Institute of Standards and Technology Telework Program Employee/Supervisor Agreement)

- If telework is approved, adhering to the terms and conditions of the telework arrangements which includes:
  - Completing training, as required by the DOC Telework Program and Policy (this training does not need to be repeated unless otherwise instructed);
  - Completing the **NIST DN-27a Alternative Worksite Safety Checklist** if the telework site is a residence;
  - Maintaining a telework site that is free of distractions and obligations which would impair his/her ability to provide the same time and level of attention to the work product as when onsite;
  - Following all standards governing ethical behavior regardless of where or when work is performed;
  - Adhering to information security policies, particularly related to access/use, remote access, mobile devices, etc.;
  - Ensuring that records subject to the Privacy Act of 1974 or have Personally Identifiable Information (PII), and Business Identifiable Information (BII) are not disclosed to anyone except those who have been authorized access to such information in order to perform their duties.
  - Performing his/her duties and official responsibilities at a “Contributor” level or greater;
  - Maintaining reasonable care of all NIST-owned property and material;
  - Accurately recording their time each pay period as telework in all time and attendance records.
o Covering any utility cost, including high-speed internet connection needed to gain access to NIST information technology (IT) systems, electricity, heating, and lighting used while teleworking at their home; and
o Notifying line management of any incident (e.g., work-related injury, near-miss, property damage, etc.) according to OU policies and procedures for doing so.

- Initiating a grievance, if so desired, if telework is approved but restricted, denied, or revoked.
  o Telework-ready employees who are not covered by a negotiated grievance procedure (NGP) must use the administrative grievance procedure in DAO 202-771, "Administrative Grievance Procedure," to appeal issues relating to their telework status or other telework matters.
  o Employees covered by an NGP that does not specifically exclude this matter must use the applicable NGP.
  o Employees who believe they are the victims of prohibited discrimination may utilize the Equal Employment Opportunity Commission complaint procedures or the negotiated grievance procedure, as appropriate.

NIST Telework Coordinator

- Provides guidance on NIST telework policy and procedures to employees and supervisors.
- Develops and implements a reporting system to capture metrics on telework participation, hours teleworked, terminations, and denials.
- Ensures that the NIST Telework Program is operating in compliance with laws, regulations, and DOC policies and procedures.
Appendix B. SSL Remote Access NIST Key File Installation Instructions

Contact iTAC if you have not already signed for or received the appropriate NIST Key File to add the 'NIST Key File' to your computer, which provides the NIST-owned or personally owned identification needed for 'Full Access' through the SSL Remote Access Service.

Windows 8/10

1. Open Windows Explorer and navigate to this directory: `C:\Users\`
2. Create a directory and name it `NIST`.
3. If your computer is personally owned, copy the file, `SSLRA_Personally-owned.key`, into this directory: `C:\Users\NIST`.
4. If your computer is NIST owned, copy the file, `SSLRA_NIST-owned.key`, into this directory: `C:\Users\NIST`.

macOS

1. Save the Key file to your Home directory.
2. Open a Terminal session (Open Finder | Go | Applications | Utilities | Terminal).
3. Create a directory under /Library and name it "NIST", update permissions.
   - `sudo mkdir -p /Library/NIST`
   - `sudo chmod 755 /Library/NIST`
4. If your computer is personally owned, copy the file “SSLRA_MacLinux_Personally-owned.key” into this directory and update permissions.
   - `sudo cp SSLRA_MacLinux_Personally-owned.key /Library/NIST`
   - `sudo chmod 644 /Library/NIST/SSLRA_MacLinux_Personally-owned.key`
5. If your computer is NIST owned, copy the file “SSLRA_MacLinux_NIST-owned.key” into this directory and update permissions.
   - `sudo cp SSLRA_MacLinux_NIST-owned.key /Library/`
   - `sudo chmod 644 /Library/NIST/SSLRA_MacLinux_NIST-owned.key`

Linux

1. Save the Key file to your Home directory.
2. Open a Terminal session and navigate to your 'HOME (~)' directory:
   - `cd`
3. Create a directory under /etc and name it “NIST”.
   - `sudo mkdir -p /etc/NIST`
   - `sudo chmod 755 /etc/NIST`
4. If your computer is personally owned, copy the file “SSLRA_MacLinux_Personally-owned.key” into this directory - /etc/NIST.
5. If your computer is NIST-owned, copy the file “SSLRA_MacLinux_NIST-owned.key” into this directory - /etc/NIST.

- sudo cp SSLRA_MacLinux_NIST-owned.key /etc/NIST
- sudo chown root:root /etc/NIST /etc/NIST/SSLRA_MacLinux_NIST-owned.key
- sudo chmod 644 /etc/NIST/SSLRA_MacLinux_NIST-owned.key

**Note:** If you already have the key files located under ~/.NIST directory, you can simply move the ~/.NIST directory to /etc/NIST.

- cd
- sudo mv .NIST /etc/NIST
- sudo chmod 755 /etc/NIST
- sudo chown root:root /etc/NIST /etc/NIST/SSLRA_MacLinux*.key
- sudo chmod 644 /etc/NIST/SSLRA_MacLinux*.key
Appendix C. Finding Your Computer Name or IP Address

When You are at Work

You will need your work computer name or IP address when you log in using Remote Access. The following are the various ways to obtain this information.

- **Easiest Method is to use BigFix located on the taskbar**

  If hidden click the caret (^)

  Hover over the BigFix icon. The **Computer Name** and **IP address** display, as shown to the right.

- **Easy way to obtain IP Address using Google**

  ![Google search](image)

  **what is my ip address?**

When You Are at Home

**For Computer Name in Windows 10:** Right-click **This PC > Click Properties.**

<table>
<thead>
<tr>
<th>Computer name, domain, and workgroup settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Computer name:</strong></td>
</tr>
<tr>
<td><strong>Full computer name:</strong></td>
</tr>
<tr>
<td><strong>Computer description:</strong></td>
</tr>
</tbody>
</table>

**WINDOWS 10**

- [NIST ONBOARDERS GUIDE TO TELECOMMUTING](#)
Appendix D. OS/Browser/Anti-Virus Supported by SSL Remote Access

<table>
<thead>
<tr>
<th>Microsoft Windows Operating Systems</th>
<th>Anti-Virus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer 11, Chrome</td>
<td>The following AV products are recognized by the SSL RA functionality:</td>
</tr>
<tr>
<td>Windows 10</td>
<td>• Microsoft Security Essentials 4.x</td>
</tr>
<tr>
<td>Windows 8*</td>
<td>• Trend Micro OfficeScan XG</td>
</tr>
<tr>
<td>Windows 8.1*</td>
<td>• Windows Defender (for Windows 8, 10 only)</td>
</tr>
<tr>
<td></td>
<td>The following AV products may work, but SSL RA functionality has not been tested for these products:</td>
</tr>
<tr>
<td></td>
<td>• AVG Anti-Virus Free Edition (2016.x)</td>
</tr>
<tr>
<td></td>
<td>• Avast! Free Anti-Virus (17.x)</td>
</tr>
<tr>
<td></td>
<td>Avira Internet Security (15.x)</td>
</tr>
</tbody>
</table>

* The SSL Remote Access service will no longer accept connections from devices running the Windows 7 Operating System (OS). OISM does not support devices running Microsoft Windows 8 and 8.1; however, OISM recognizes that some users may only have access to personally owned Windows 8 computers and need to use them for telecommuting purposes. To accommodate that need, OISM provides Windows 8 compatible remote access services within the limitations of the currently supported remote access product. Support is limited to issues dealing directly with the Remote Access service and are not extended to issues with other applications running on the Windows 8 operating systems or personally owned computers.

<table>
<thead>
<tr>
<th>macOS Operating Systems/Browser **</th>
<th>Anti-Virus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chrome</td>
<td>The following AV product is recognized by the SSL RA functionality:</td>
</tr>
<tr>
<td>Apple macOS® X 10.12.x (Sierra)</td>
<td>• Trend Micro Apex 1</td>
</tr>
<tr>
<td>Apple macOS® X 10.13.x (High Sierra)</td>
<td>The following AV products may work, but SSL RA functionality has not been tested for these products:</td>
</tr>
<tr>
<td>Apple macOS® X 10.14.x (Mojave)</td>
<td>• Avast! Free Antivirus (13.x)</td>
</tr>
<tr>
<td>Apple macOS® X 10.15.x (Catalina)</td>
<td>• Avira Free Mac Security (3.x)</td>
</tr>
</tbody>
</table>

** On macOS, the Safari browser is not formally supported because its use, while possible, requires repeatedly clicking to allow software components to run.
The following AV product is recognized by the SSL RA functionality:

- Clamav (0.x)

The F5 Networks support all 64-bit x 86_64 Linux operating systems (OS). 32-bit Linux OS is not supported.

***Debian is used with the latest available Iceweasel.

Notes: (1) The above information is for IPv4/IPv6. The IPv6 pool address will only be provided for Windows and Linux OS at this time. (2) Also, the SSL Remote Access service is provided by a commercial product that can recognize the anti-virus product supported by OISM and a limited number of other anti-virus products. It is possible that anti-virus products installed on a personally owned computer are not supported by the SSL Remote Access service. (3) The SSL Remote Access service is configured to support NIST-owned computers. Access from personally owned or other non-NIST computers configured to meet NIST remote access requirements, including a supported Operating System, browser, anti-virus with current definitions, and an installed NIST key file, is permitted and may work. Support for users with non-NIST computers is limited to the remote access application itself.

Mac SSLVPN Scripts
Version: 2.2
Created: 03/31/16
Updated: 10/11/19

README
#Remote Access Installer/Uninstaller scripts
#Version 1.0 - 11/19/2015
#Maintained by Robert Sorensen

Updates
======
#Version 2.2 - 10/11/2019
   - Updated script to support upgrade to BIG-IP 14.1.2.1
#Version 2.1 – 07/16/19 – Remove Edge Client Cache directory as part of uninstall. Added -c option to remove Edge Client Cache directory independent of uninstall.
#Version 2.0 – 05/07/18 – Updated script to support APM v.13.1.x – component helper apps, now browser independent. Edge Client for Mac is also now installed.
#Version 1.8 - 01/12/18 - Fixed bug associated with upgrading mac_policyserver.tar file. Fixed 0-byte host inspection plugin issue!
#1.7 – 08/16/17 – Updated to pull components from serv.nist.gov. Converted distribution file to base64 for ease of distribution.
#Version 1.6 - 07/14/17 - Updated to pull components from new serv-apm.nist.gov. A few minor bug fixes.
#Version 1.5 - 03/11/16 - Updated logic so can run from any directory. Automatically check for updated components and download if found.
#Version 1.4 - 02/29/16 - Added function to download components and added command line options to main script (-i=install, -u=uninstall)
#Version 1.3 - 02/08/16 - Updated script to verify install directory (MacVPNScripts) is under $HOMEDIR
#Version 1.2 - 12/24/15 - Updated mac_inspectionhost.pkg and mac_sslvpn.pkg (APM 11.6 HF6)
#Version 1.1 - 12/15/15 - Updated scripts to provide better error reporting

Installation
1. Open terminal session
   - Hit `<Command-Space Bar>` (Spotlight search keyboard shortcut), enter ‘terminal’
2. $ base64 -D -i MacSSLVPNScripts_v2.2.tar.b64.txt | tar xvfz - (location downloaded *.tar.b64.txt file). Note: Trailing ‘-’ after tar xvfz command. Will create a new subdirectory 'MacVPNScripts'

For example, if you downloaded MacSSLVPNScripts_v2.2.tar.b64.txt to your Downloads folder, then run:
$ base64 -D -i Downloads/MacSSLVPNScripts_v2.2.tar.b64.txt | tar xvfz -

3. $ cd MacVPNScripts
   Usage: ./goremote option(s)
   Usage: ./goremote option(s)

   Version: 2.2 (10/11/2019)
   Options:
   -c (Clear Edge Client Cache)
   -d (View Script Documentation)
   -i (Install Add-ons)
   -u (Uninstall Add-ons)
   -v (Validate Add-ons)
   -h (Usage options)

   Ex: ./goremote -i     Ex: ./goremote -i

4. $ ./goremote -u
5. $ ./goremote -i

Usage

./goremote -h

Usage: ./goremote option(s)

Version: 2.2 (10/11/2019)
Options:
- c (Clear Edge Client Cache)
- d (View Script Documentation)
- i (Install Add-ons)
- u (Uninstall Add-ons)
- v (Validate Add-ons)
- h (Usage options)
Clear Edge Client Cache

./goremote -c

Running Script v_2.2 (10/11/2019)...
Starting process to clear Edge Client Cache...

* /Users/rsoren/Library/Caches/com.f5networks.EdgeClient directory already removed...

Remote Access Component Uninstallation Results:
===================================
NIST Edge Client Cache:  Success
===================================

Validate Addons

./goremote -v

Running Script v_2.2 (10/11/2019)...
Verifying if new components are available...done. All SSL VPN components are latest version.

Remote Access Component Helper Validation Results:
===================================
Inspector Components:  Failure
Endpoint Insp. Components:  Failure
SSL VPN Components:  Failure
NIST Edge Client:  Success
Scripts PDF:  Success
===================================

**Validation Failed**

...Failed OR if successful...

./goremote -v

Running Script v_2.2 (10/11/2019)...
Verifying if new components are available...done. All SSL VPN components are latest version.

Remote Access Component Helper Validation Results:
===================================
Inspector Components:  Success
Endpoint Insp. Components:  Success
SSL VPN Components:  Success
NIST Edge Client:  Success
Scripts PDF:  Success
===================================

**Validation Successful**
Please make sure to close all instances of browser before connecting to https://inside.nist.gov...

**View Script Documentation**

`./goremote -d`

Running Script v_2.2 (10/11/2019)...  
Verifying and Opening Script Documentation PDF...

Checking for updated SSL VPN documentation...done. SSL VPN documentation is latest version...

`./goremote -d`

Running Script v_2.2 (10/11/2019)...  
-------------------------------------------
Tmp_PKGName=scriptPDF...  
Tmp_PKGMD5=8334d43a5b81df9679e6131059cd159f...  
Tmp_PKGShortName=MacSSLVPNScripts.pdf...  
Tmp_PKGFile=/Users/rsoren/MacVPNScripts//Docs/MacSSLVPNScripts.pdf...  
-------------------------------------------

md5: /Users/rsoren/MacVPNScripts//Docs/MacSSLVPNScripts.pdf: No such file or directory
File /Users/rsoren/MacVPNScripts//Docs/MacSSLVPNScripts.pdf not found.

File '/Users/rsoren/MacVPNScripts//Docs/MacSSLVPNScripts.pdf' doesn't exist or failed checksum...
Downloading file '/Users/rsoren/MacVPNScripts//Docs/MacSSLVPNScripts.pdf'...
Executing command 'curl -k -l -# --retry 2 --connect-timeout 5 https://serv.nist.gov/public/share/MacSSLVPNScripts.pdf -o /Users/rsoren/MacVPNScripts//Docs/MacSSLVPNScripts.pdf'...
########################################################################
100.0%
File /Users/rsoren/MacVPNScripts//Docs/MacSSLVPNScripts.pdf: OK

/Users/rsoren/MacVPNScripts//Docs/MacSSLVPNScripts.pdf downloaded...

Opening Script Documentation PDF...

**Uninstall Session**

`./goremote -u`

Starting process to remove Remote Access Components from system...

Removing local components...

Running Script v_2.2 (10/11/2019)...  
Starting process to remove Remote Access Components from system...

Removing local helper components...
** /Users/rsoren/Library/F5Networks directory found...removing...done...
** /Applications/F5 Endpoint Inspector.app/ directory found...removing...
[Please enter your 'sudo' password]
Enter PIN for 'Certificate For PIV Authentication (USER NAME)'

 PASSWORD: ******
[enter your current user passwd]

..or..
Password: **********

done...
Removing system SSL VPN plugin...

** /Applications/F5 VPN.app/ directory found...removing...done...
** /Applications/BIG-IP Edge Client.app/ directory found...removing...done...
** /Users/rsoren/Library/Caches/com.f5networks.EdgeClient directory found...removing...done...

Running Script v_2.2 (10/11/2019)...

Remote Access Component Uninstallation Results:
=================================================================
 Inspector Components:  Success
 Endpoint Insp. Components:  Success
 SSL VPN Components:  Success
 NIST Edge Client:  Success
 NIST Edge Client Cache:  Success
=================================================================

Congratulations!  All Remote Access Components have been successfully removed.
Run .goremote -i to install Remote Access Components...

Install Session

./goremote -i

Running Script v_2.2 (10/11/2019)...
Starting process to install Remote Access Components...

Checking for updated SSL VPN documentation...done.  SSL VPN documentation is latest version...
Verified most current PDF downloaded...

Running Script v_2.2 (10/11/2019)...
Checking for updated SSL VPN components...done.  All SSL VPN components are latest version...
/Users/rsoren/MacVPNScripts/ found! Continuing install...

------------------------------------------------
Tmp_PkgName=tar1...
Tmp_PkgMD5=d39320629fd0797b26c8279fa9953b55...
Tmp_PkgShortName=mac_policyserver.tar...
Tmp_PkgFile=/Users/rsoren/MacVPNScripts/mac_policyserver.tar...
------------------------------------------------
md5: /Users/rsoren/MacVPNScripts/mac_policyserver.tar: No such file or directory
File /Users/rsoren/MacVPNScripts/mac_policyserver.tar not found..

File '/Users/rsoren/MacVPNScripts/mac_policyserver.tar' doesn't exist or failed checksum...
Downloading file '/Users/rsoren/MacVPNScripts/mac_policyserver.tar'...
Executing command 'curl -k -1 -# --retry 2 --connect-timeout 5
https://serv.nist.gov/public/share/mac_policyserver.tar -o
/Users/rsoren/MacVPNScripts/mac_policyserver.tar'...
########################################################################
100.0%
File /Users/rsoren/MacVPNScripts/mac_policyserver.tar: OK

------------------------------------------------
Tmp_PkgName=oesis...
Tmp_PkgMD5=f708f40d4b3f6bb0b4340090a4ba7c77...
Tmp_PkgShortName=mac_oesisInspector.tar.ver...
Tmp_PkgFile=/Users/rsoren/MacVPNScripts/mac_oesisInspector.tar.ver...
------------------------------------------------
md5: /Users/rsoren/MacVPNScripts/mac_oesisInspector.tar.ver: No such file or directory
File /Users/rsoren/MacVPNScripts/mac_oesisInspector.tar.ver not found..

File '/Users/rsoren/MacVPNScripts/mac_oesisInspector.tar.ver' doesn't exist or failed checksum...
Downloading file '/Users/rsoren/MacVPNScripts/mac_oesisInspector.tar.ver'...
Executing command 'curl -k -1 -# --retry 2 --connect-timeout 5
https://serv.nist.gov/public/download/mac_oesisInspector.tar.ver -o
/Users/rsoren/MacVPNScripts/mac_oesisInspector.tar.ver'...
########################################################################
100.0%
File /Users/rsoren/MacVPNScripts/mac_oesisInspector.tar.ver: OK

------------------------------------------------
Tmp_PkgName=pkgl...
Tmp_PkgMD5=5e146ebfa352b65b16913f66af7e545f...
Tmp_PkgShortName=mac_f5epi.pkg...
Tmp_PkgFile=/Users/rsoren/MacVPNScripts/mac_f5epi.pkg...
------------------------------------------------
md5: /Users/rsoren/MacVPNScripts/mac_f5epi.pkg: No such file or directory
File /Users/rsoren/MacVPNScripts/mac_f5epi.pkg not found..

File '/Users/rsoren/MacVPNScripts/mac_f5epi.pkg' doesn't exist or failed checksum...
Downloading file `/Users/rsoren/MacVPNScripts//mac_f5epi.pkg'...
Executing command 'curl -k -l -# --retry 2 --connect-timeout 5
https://serv.nist.gov/public/download/mac_f5epi.pkg -o
/Users/rsoren/MacVPNScripts//mac_f5epi.pkg'...

100.0%
File `/Users/rsoren/MacVPNScripts//mac_f5epi.pkg': OK

Tmp_PKGName=pkg2...
Tmp_PKGMD5=effc9ad16521080db220aa8a9d150020...
Tmp_PKGShortName=mac_f5vpn.pkg...
Tmp_PKGFile=/Users/rsoren/MacVPNScripts//mac_f5vpn.pkg...

md5: /Users/rsoren/MacVPNScripts//mac_f5vpn.pkg: No such file or directory
File `/Users/rsoren/MacVPNScripts//mac_f5vpn.pkg' not found..

File '/Users/rsoren/MacVPNScripts//mac_f5vpn.pkg' doesn't exist or failed checksum...
Downloading file '/Users/rsoren/MacVPNScripts//mac_f5vpn.pkg'...
Executing command 'curl -k -l -# --retry 2 --connect-timeout 5
https://serv.nist.gov/public/download/mac_f5vpn.pkg -o
/Users/rsoren/MacVPNScripts//mac_f5vpn.pkg'...

100.0%
File `/Users/rsoren/MacVPNScripts//mac_f5vpn.pkg': OK

Tmp_PKGName=macec...
Tmp_PKGMD5=e4a45a0f0f74ee929f82946d3ea70e85...
Tmp_PKGShortName=mac_edgesvpn.pkg...
Tmp_PKGFile=/Users/rsoren/MacVPNScripts//mac_edgesvpn.pkg...

md5: /Users/rsoren/MacVPNScripts//mac_edgesvpn.pkg: No such file or directory
File `/Users/rsoren/MacVPNScripts//mac_edgesvpn.pkg' not found..

File '/Users/rsoren/MacVPNScripts//mac_edgesvpn.pkg' doesn't exist or failed checksum...
Downloading file '/Users/rsoren/MacVPNScripts//mac_edgesvpn.pkg'...
Executing command 'curl -k -l -# --retry 2 --connect-timeout 5
https://serv.nist.gov/public/share/mac_edgesvpn.pkg -o
/Users/rsoren/MacVPNScripts//mac_edgesvpn.pkg'...

100.0%
File `/Users/rsoren/MacVPNScripts//mac_edgesvpn.pkg': OK

Tmp_PKGName=macconfec...
Tmp_PKGMD5=b0e9b9a5a7d11cf71b753e9e7af97140...
Tmp_PKGShortName=config_tmp.f5c...
Tmp_PKGFile=/Users/rsoren/MacVPNScripts//config_tmp.f5c...

md5: /Users/rsoren/MacVPNScripts//config_tmp.f5c: No such file or directory
File /Users/rsoren/MacVPNScripts//config_tmp.f5c not found..

File '/Users/rsoren/MacVPNScripts//config_tmp.f5c' doesn't exist or failed checksum...
Downloading file '/Users/rsoren/MacVPNScripts//config_tmp.f5c'...
Executing command 'curl -k -l -# --retry 2 --connect-timeout 5
https://serv.nist.gov/public/share/config_tmp.f5c -o
/Users/rsoren/MacVPNScripts//config_tmp.f5c'...
100.0%
File /Users/rsoren/MacVPNScripts//config_tmp.f5c: OK

Component packages

- TGZ1 (md5)=/Users/rsoren/MacVPNScripts//mac_policyserver.tar
  (d39320629fda0797b26c82799f96953b55)...  
- PKG1 (md5)=/Users/rsoren/MacVPNScripts//mac_f5epi.pkg
  (5e146ebfa352b5b16913f66af7e545f)...  
- PKG2 (md5)=/Users/rsoren/MacVPNScripts//mac_f5vpn.pkg
  (effc9ad16521080db2200a8a9d150020)...  
- OESIS (md5)=/Users/rsoren/MacVPNScripts//mac_oesisInspector.tar.ver
  (f708f40d4b3f6bb0b4340090a4b7c77)...  
- MACEC (md5)=/Users/rsoren/MacVPNScripts//mac_edgesvpn.pkg
  (e4a45a0f0f74ee929f82946d3ea70e85)...  
- MACCONFEC (md5)=/Users/rsoren/MacVPNScripts//config_tmp.f5c
  (b0d9ba5a7d11c6f71b753e9e7af97140)...  

Installing /Users/rsoren/MacVPNScripts//mac_f5epi.pkg...
Password: *********** [enter your current user passwd]
installer: Package name is F5 Endpoint Inspector
installer: Upgrading at base path / 
installer: The upgrade was successful.

Installing /Users/rsoren/MacVPNScripts//mac_f5vpn.pkg...
installer: Package name is F5 VPN
installer: Upgrading at base path / 
installer: The upgrade was successful.

Installing /Users/rsoren/MacVPNScripts//mac_edgesvpn.pkg...
installer: Package name is BIG-IP Edge Client
installer: Upgrading at base path / 
installer: The upgrade was successful.

Uncompressing SSL Inspector agent components from
/Users/rsoren/MacVPNScripts//mac_policyserver.tar

Removing directory '/Users/rsoren/Library/F5Networks'...
Creating '/Users/rsoren/Library/F5Networks/Inspectors' directory structure...

x OesisInspector.dylib
x OesisInspector4.dylib
x libwalocal.dylib
x libwaapi.dylib
x libwautils.dylib
x libwaresource.dylib
x PolicyServer

Running Script v_2.2 (10/11/2019)...

Remote Access Component Helper Installation Results:

===================================
Inspector Components:  Success
Endpoint Insp. Components:  Success
SSL VPN Components:  Success
  NIST Edge Client:  Success
  Scripts PDF:  Success
===================================

**Install Successful**
Please make sure to close all instances of browser before connecting to https://inside.nist.gov...