EFiT Application Onboarding Guide

for

Sentara Health Employer Group Partners

Contents

EFiT Introduction

Sentara Health has partnered with a new application called **EFiT** (Eligibility File Integration and Transmission). EFiT is a web-based, multi-platform application through which Employer Groups, TPAs, and Exchanges can submit their EDI (Electronic Data Interchange) eligibility files.

Inside the EFiT ENR application, the files are checked for errors and other issues. If file concerns are found during processing, questions are sent from the Health Plan through the **EFiT Account Portal** back to the group or their partners. Groups will experience quicker and more standardized resolution of any file concerns, including technical, enrollment, and eligibility questions. Concerns can also be monitored over time, and tracked and analyzed through reporting. This allows proactive identification of ways to improve and streamline enrollment processes.

For new Employer Groups establishing an initial EDI process with the Health Plan, the EFiT onboarding process improves on the current way we set up an EDI file process. EFiT allows new EDI groups to onboard EDI more rapidly. The EFiT application also facilitates communication between the onboarding partner and the Health Plan during the new file testing process.

EFiT Process for MFT Connection

EFiT uses a more secure and flexible connection called **MFT (Managed File Transfer)**. MFT does not involve a password, and does require the communication of an Employer or TPA credentials called a “public key” for securing the shared data. MFT also involves the use of a separate file transfer application, which many groups and partners already use.

If groups or their partners are not already using a file transfer application that can generate a public key, many applications are available, and some for no cost, including FileZilla Client and WinSCP (please note, these applications are not affiliated with Sentara Health or EFiT but are

suggested options only). The Sentara Health EFiT team will help support the group and their partners with technical onboarding to the EFiT MFT file transfer connection.

A benefit of the EFiT software for groups and their technical partners is that it creates standards for the **electronic eligibility files** sent to Sentara Health. Because the checks performed on enrollment files within EFiT are automatic, the group's 834 file must be aligned with nationally accepted 834 5010 EDI and HIPAA formatting standards. The first part of the internal onboard process evaluates the group's current production file and then identifies any potential formatting issues.

EFiT uses the most up-to-date file configurations with Sentara Health standards. For faster onboarding, it is recommended that the group be able to work with the Sentara Health to correct any identified file format concerns. If the group is unable to bring their files into alignment with current standards, it may be possible to make some programming changes in the EFiT configuration to allow certain nonstandard formatting to be accepted. Be aware that custom programming may present significant delays in EFiT onboarding.

4417 Corporation Lane
Virginia Beach, VA 23462

EFiT Group Onboarding Requirements

During the EFiT Onboarding Process, the Sentara Health EFiT Team will need the following information from the Employer Group or their current technical partner:

☐	A public key credential for MFT setup and file transfer.
☐	All documents provided by Sentara Health must be completed.

Generating a Public Key

As part of the EFiT Onboarding Project, all current and new Employer Groups or their administrative partners will need to set up a new direct MFT connection for file transfer with the EFiT application. This new connection for Sentara Health eligibility files does not use a password-based login like the current file-transfer system. Instead, this more secure file transfer protocol uses SSH encryption public/private "key pairs" to protect the information transmitted between the Employer/partner and EFiT.

SSH or Secure Shell is an encrypted network protocol for operating network services securely over an unsecured network. While passwords may sometimes be compromised with brute-force attacks, SSH keys cannot be brute-forced—they are too complex.

Q. What is a public/private key pair and how is it used?

A. The "public key" is like a shared identifier. It allows two parties to verify that they are communicating with the right people. The "private key" both secures the data while it is moving and decrypts it when the information gets where it needs to go, so the data can be used as intended.

Public keys are shared, but private keys are **never** shared. The owner of the private key keeps it on their own machine for use during the file transfer and encryption process.

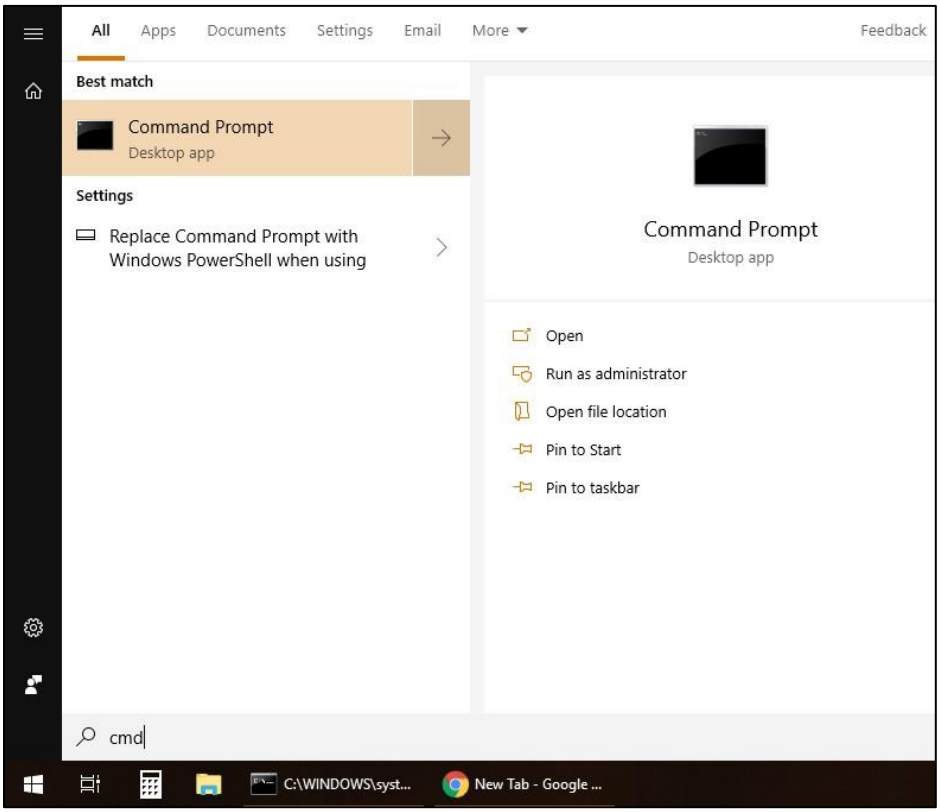
Q. How do I generate a public and private key pair, and how do I get my public key to send to Sentara Health for EFiT?

A. The key pair generation process depends on your operating system. Please see the following instructions based on whether you are using a Windows 10 or Mac OS.

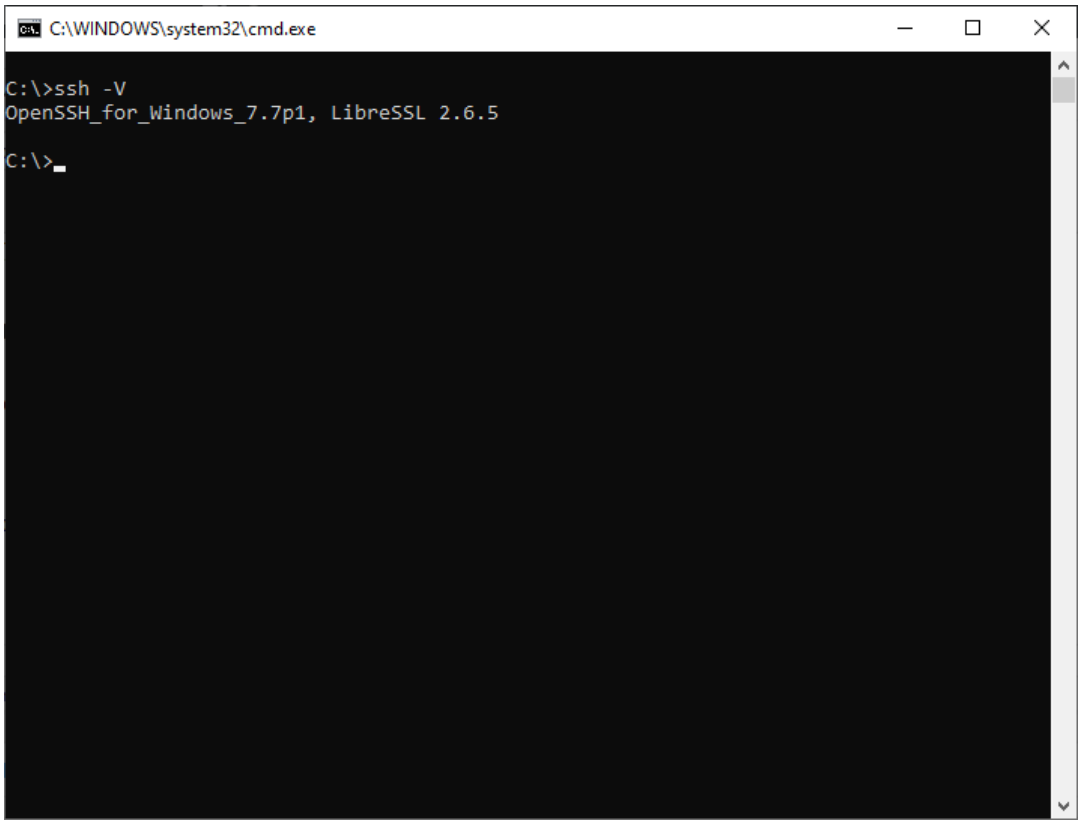
Windows 10

In 2019, Windows 10 began to include an OpenSSH client in the software. The steps below detail how to generate a public/private key pair using Windows Command Prompt:

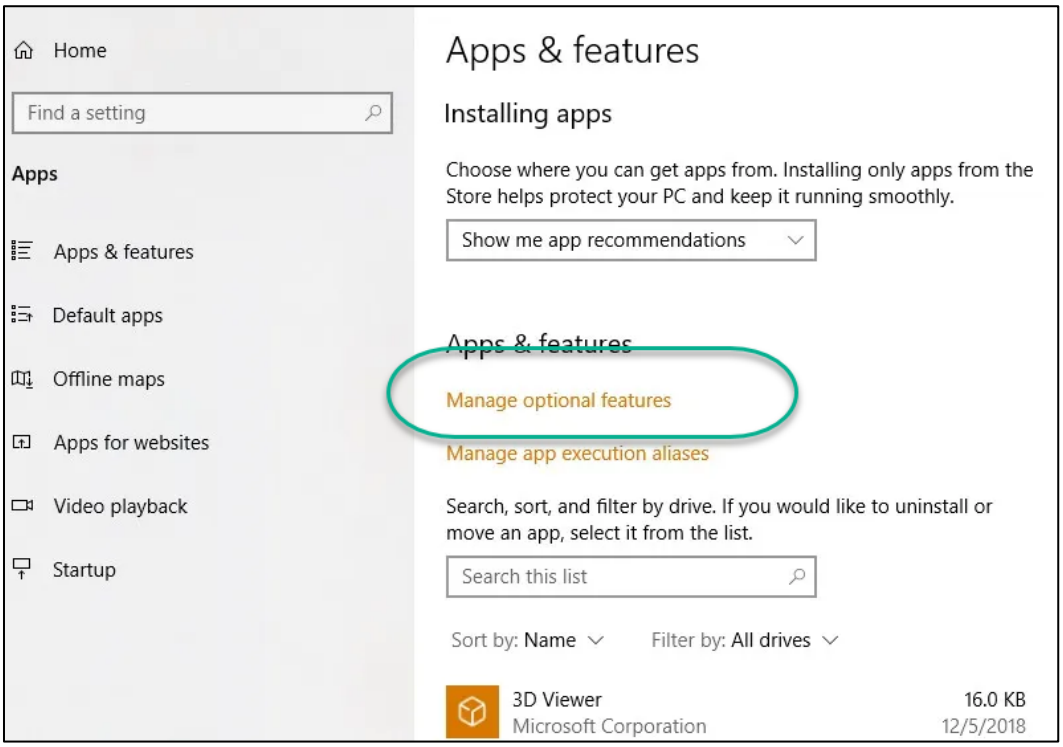
1. From the Start Menu, open Command Prompt:
    a. Press the Windows logo key on your keyboard or click on the Start Menu.
    b. Type **cmd** and open Command Prompt.



2. Check to see if you have SSH installed.
    a. Type **ssh –V** and then **<Enter>.**
    b. If you have SSH installed in your version of Windows, then you will see the below; Command Prompt will be ready for the next command, and you can skip to step 3.

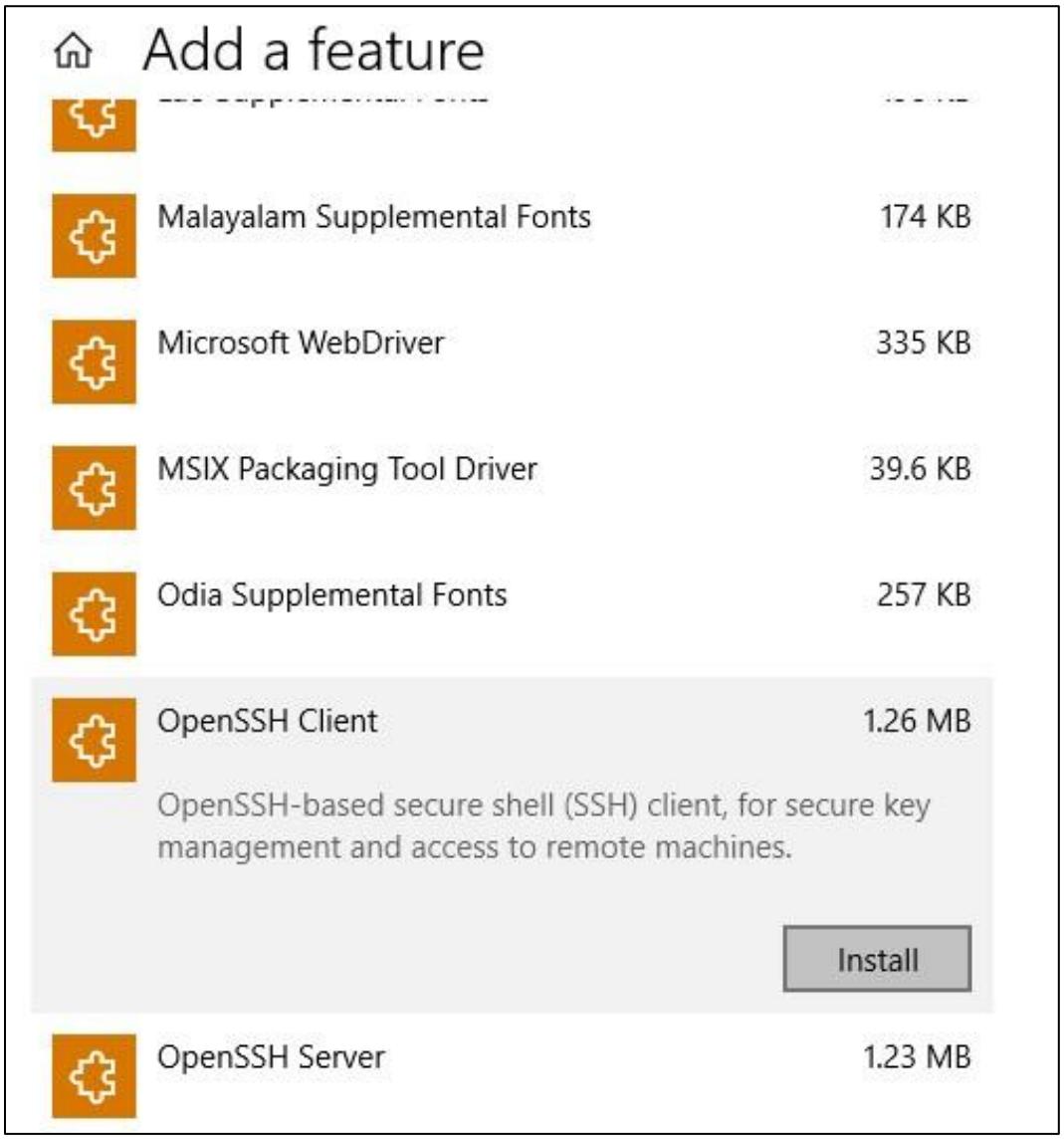


    c. If you get an error message that states “command not recognized”, this is due to an older version of Windows 10 that hasn’t been upgraded.
        i. Follow these steps:
            1. Click on the Start Menu and type **features**.
            2. Open “Apps & features” and click on “Manage optional features.”



ii. Next, click on “Add a feature.”

iii. Scroll down until you find “OpenSSH Client.”



iv. Click on “Install” for OpenSSH Client.

3. These steps will allow you to generate your public/private key pair:

   a. At the current line in Command Prompt, type **ssh-keygen** and then **<Enter>**.

   b. You will receive a prompt: “Enter file in which to save the key.”

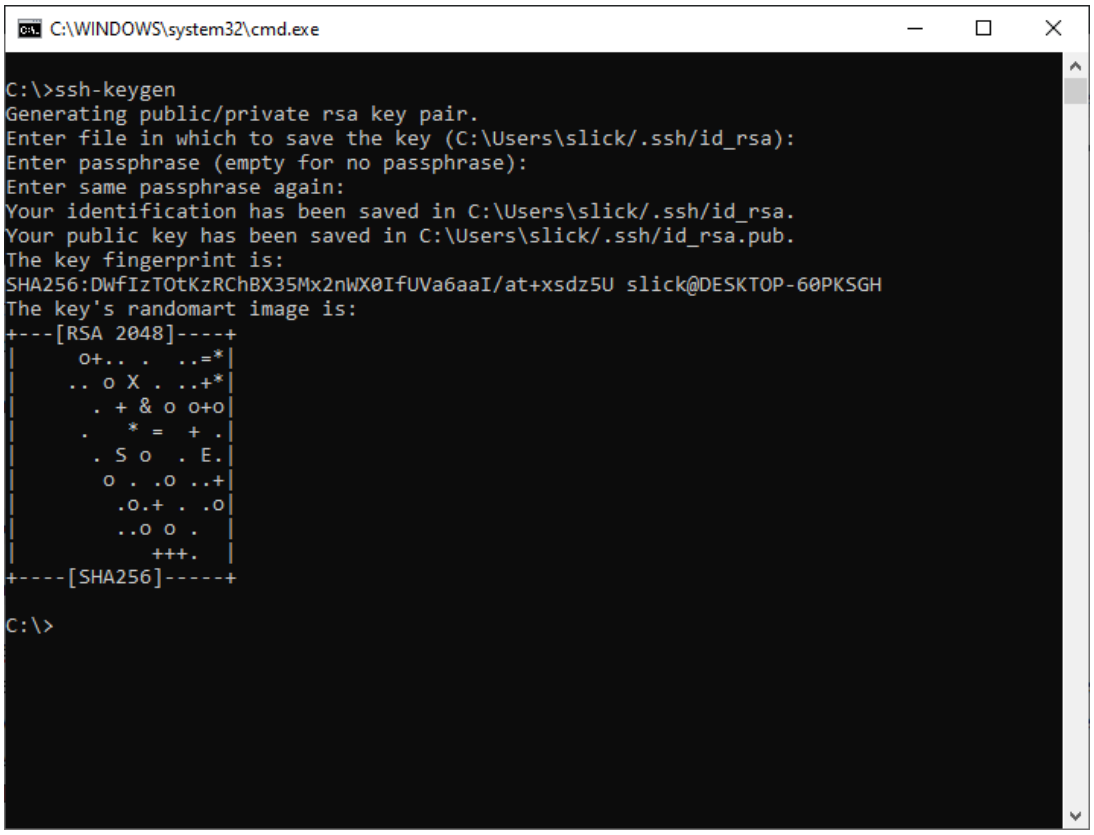
   c. Press **<Enter>** to save in the default location, which will be provided.

d. A second prompt will ask: “Enter passphrase (empty for no passphrase),” you have two options:

   i. Press **<Enter>** to create unencrypted key. If you’re the only one that uses the computer, this is safe.

   ii. Type a password. This will encrypt your key. It’s a good idea to do this if you share your computer with someone else who should not have access to the private key.

e. When you’re done with step d, you will see something similar to the below image.



4. This last step will open your **public** key so that you can copy and paste it into an email to send to Sentara Health for EFiT setup.

   a. Enter or copy/paste the following in the next line of Command Prompt:

notepad %userprofile%\.ssh\id_rsa.pub

b. Save the notepad file, attach it to an email and send the file to shp_edi_enr@sentara.com and the Sentara Health Plans Business Analyst assigned to your group's Implementation.

MAC OS

You can generate an SSH key pair in Mac OS following these steps:

1. Open up the Terminal by going to Applications > Utilities > Terminal.
2. In the terminal, use the following command to start the key generation:

ssh-keygen -t rsa

3. Next, you will be prompted to provide the location where you want to create the private key file:

Enter file **in** which to save the key (/home/youruser/.ssh/id_rsa):

a. Leave this empty to create the key in the default location, which is */home/youruser/.ssh/**id_rsa**.*
b. The public key file will be created in the very same location, and with the same name, but with the .PUB extension.

4. Afterwards you will be prompted to choose a password. This is the password required to use the private key.

Enter passphrase (empty **for** no passphrase):

That completes the key generation. On the next page is an example of the entire process.

Mac_user: **ssh-keygen -t rsa**

Generating public/private rsa key pair.

Enter file in which to save the key (/home/user/.ssh/id_rsa).

Enter passphrase (empty for no passphrase).

Enter same passphrase again.

Your identification has been saved in id_rsa.

Your public key has been saved in id_rsa.pub.

The key fingerprint is:
16:8e:e8:f2:1d:c9:b9:cf:43:9a:b3:3c:c1:1f:95:93 Mac_user

This will create a private key written to */home/user/.ssh/**id_rsa***
and a public key written to */home/user/.ssh/**id_rsa.pub.***

After that you will have to upload the public key in
Site Tools > Devs > SSH Keys Manager; go to Import and paste the key.

Load the private key in your Terminal using the **ssh-add** command:
ssh-add /home/user/.ssh/id_rsa

You will be asked for the passphrase of your key when loading it in the Terminal.