Setting Up SSH Passthrough

By investing some time to set up SSH passthrough, you can make your future NAS logins and inbound file transfers easier and faster. The SSH passthrough feature allows you to log into any NAS system in the secure enclave by typing just one SSH command.

- *Without* setting up SSH passthrough, you must first log into a secure front end (SFE), and then log into a system in the enclave, such as a Pleiades or Lou front end (PFE or LFE).
- *With* SSH passthrough, you can "pass through" an SFE directly to a system in the secure enclave, where you will do most of your work.

In other words, if you set up SSH passthrough, you can SSH directly from your local system to a NAS system (such as PFE or LFE) as if you were directly connected, even though all connections are transparently passing through the SFE systems.

How To Set Up SSH Passthrough

At this point, you are just three steps away from streamlining all of your future logins and inbound file transfers. With SSH passthrough, you will be able to log in quickly to any host in the secure enclave, and you will be able to copy files from your local system to any NAS host.

Before You Begin: If you have not already done so, complete the steps for first-time login to NAS systems.

Step 1: Create/Modify the .ssh/config File on Your Local System

You must have a ~/.ssh/config file on your local system to enable SSH passthrough. The file should include entries for the hosts you want to access inside the NAS enclave. Although you can create a customized version of the ~/.ssh/config file, we recommend downloading and using one of the following templates:

- ssh_config.txt
- ssh_config_win10.txt (for Windows users, especially if you do not use Cygwin)

Move the file to the .ssh directory on your local system and rename it to "config". In the fiile, uncomment and replace <nas_login_name> with your NAS username.

The contents of the **ssh_config.txt** template are shown below. In this template, sfe6 is used; in the event that sfe6 is unavailable, or if you want to use a different SFE for SSH passthrough, you can switch to sfe[*7-8*].

Note: In the **ssh_config_win10.txt** template, ssh.exe replaces the ssh command in the **ssh_config.txt** template.

```
#Updated 20211018

Host sfe
  HostName              sfe6.nas.nasa.gov

Host sfe sfe?.nas.nasa.gov
  # Uncomment to allow multiplexing of single connections
  #ControlMaster         auto
  #ControlPath          ~/.ssh/master-%r@sfe:%p
  #ControlPersist        1
  ForwardAgent          yes
  ForwardX11            yes
  ServerAliveInterval   5m

  Host sfe sfe?.nas.nasa.gov sup*.nas.nasa.gov
    LogLevel            info
    ProxyCommand           none

  Host pfe pfe-last pfe.nas.nasa.gov pfe-last.nas.nasa.gov
    HostKeyAlias         pfe20.nas.nasa.gov
    ProxyCommand           ssh -ax -oCompression=no sfe ssh-balance %h

  Host lfe lfe-last lfe.nas.nasa.gov lfe-last.nas.nasa.gov
    HostKeyAlias         lfe5.nas.nasa.gov
    ProxyCommand           ssh -ax -oCompression=no sfe ssh-balance %h

  Host lou lou-last lou.nas.nasa.gov lou-last.nas.nasa.gov
    HostKeyAlias         lfe5.nas.nasa.gov
    ProxyCommand           ssh -ax -oCompression=no sfe ssh-balance %h

  Host lou2 lou2-last lou2.nas.nasa.gov lou2-last.nas.nasa.gov
    HostKeyAlias         lfe5.nas.nasa.gov
    ProxyCommand           ssh -ax -oCompression=no sfe ssh-balance %h

  # Add additional hosts to the list below as needed
  Host *.nas.nasa.gov lou lou? lfe? pfe?? ?fe *-last mfe?
    ForwardAgent          yes
    HostbasedAuthentication no
    Protocol            2
    ProxyCommand           ssh -ax -oCompression=no sfe ssh-proxy %h
```

```
ServerAliveInterval     5m
# Uncomment and replace <NAS_login_name> with your NAS username
# if different than local username
#User                  <NAS_login_name>
```

WARNING: Your .ssh/config file should be set with no group/others write permission. Otherwise, you will get this error message when you connect:
Bad owner or permissions on /u/your_local_username/.ssh/config.

Once you have created your config file, test to confirm it's working by logging into a PFE as follows:

```
your_local_system% ssh pfe
```

If the file is configured properly, you will be prompted for your NAS password once, and for your RSA SecurID passcode twice.

You can continue to streamline your logins and file transfers further by completing steps 2 and 3. You will then be able to log in with just your RSA passcode.

Step 2: Create and Copy OpenSSH Public Key to Hosts Inside the Enclave

Before You Begin: Follow the steps in Setting Up Public Key Authentication to create an SSH public/private key pair and to initialize the SSH public key on the SFEs.

Then, complete these steps to copy your public key to the hosts inside the enclave and place the key in your .ssh/authorized_keys file. The examples in these steps use a PFE.

Note: This must be done for both a PFE and an LFE inside the enclave to which you want to connect using SSH passthrough.

a. Copy Your OpenSSH Public Key

   Ensure that you have a .ssh directory on the NAS host (in this example, a PFE) before issuing thescp command below. Otherwise, the command will copy the file id_rsa.pub to the PFE with the filename ".ssh." To create the directory, log into the PFE and run:

   ```
   pfe% mkdir .ssh
   ```

   On your local system, run:

   ```
   your_local_system% scp ~/.ssh/id_rsa.pub pfe:.ssh
   ```

b. Add Your OpenSSH Public Key to Your .ssh/authorized_keys File on the Enclave Host

   On your local system or on an SFE, run:

   ```
   your_local_system or sfeX% ssh pfe
   ```

   On the PFE, run:

   ```
   pfe% cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
   ```

   If you get the error message "/u/*username*/.ssh/authorized_keys: No such file or directory " after issuing the above command, you likely have set noclobber, which prevents you from overwriting files. You can use the command unset noclobber first to avoid this problem.

   WARNING: The permission for the authorized_keys file must be set to 600. To set this permission, run the command chmod 600 authorized_keys. Group/others write permissions on /u/*username* and /u/*username*/.ssh are not allowed for public key authentication.

   Repeat this step for the other NAS hosts you plan to use, such as an LFE.

   Note: If your local ~/.ssh/config file is not based on the NAS config template, you may need to change thescp and ssh commands. To change the scp command:

   ```
   your_local_system% scp -oProxyCommand='ssh username@sfeX.nas.nasa.gov
                ssh-proxy %h' ~/.ssh/id_rsa.pub username@pfe:.ssh
   ```

   where *sfeX* is sfe[*6-9*].

   Note: Because of a formatting issue, this command is shown broken into two lines. It should be on only one line (with a space before ssh-proxy.).

   To change the ssh command:

   ```
   sfeX% ssh username@pfe
   ```

   Substitute your NAS username for *username.* (If your local host username and your NAS username are the same, you can omit *username@* from the command line.)

Step 3: Set Up SSH Agent

The ssh-agent program holds and manages the private key on your local system and responds to key challenges from remote hosts.

The private key is not initially stored in the agent and is added through the ssh-add program.

Typically, ssh-agent is started at the beginning of an X session or a login session, and you provide your passphrase to unlock your private key for this originating session. For any SSH connection to a remote host (for example, sfe*X*) made from this original session, the ssh-agent remembers your private key and will respond to challenges automatically without prompting you to type in your passphrase again.

Run one of the following command lines to launch ssh-agent:

- **For csh or tcsh:**

  ```
  your_local_system% eval `ssh-agent -c`
  ```

- **For sh or bash:**

  ```
  your_local_system% eval `ssh-agent -s`
  ```

  If the bash command line shown above results in error, try running this one instead:

  ```
  your_local_system% eval "$(ssh-agent -s)"
  ```

To add your private key to ssh-agent, run:

```
your_local_system% ssh-add private_key
```

Example:

```
your_local_system% ssh-add ~/.ssh/id_rsa
Enter passphrase for /Users/username/.ssh/id_rsa: type your passphrase
Identity added: /Users/username/.ssh/id_rsa (username@....)
```

Once you've completed these steps, you can now SSH from your local system to a NAS system inside the secure enclave, and be prompted for only your RSA SecurID passcode.

Note: If you get the following error when starting ssh-agent from a terminal on Windows 10, the most likely reason is that thessh-agent service is set to disabled state:

```
unable to start ssh-agent service, error :1058
```

To resolve this error, set the service to start manually in the Services GUI or run the following command in admin mode:

```
% Get-Service -Name ssh-agent | Set-Service -StartupType Manual
```

Article ID: 232
Last updated: 27 Jun, 2023
Updated by: Moyer M.
Revision: 107
Logging In -> Setting Up Public Key & SSH Passthrough -> Setting Up SSH Passthrough
https://www.nas.nasa.gov/hecc/support/kb/entry/232/