

Common Login Failures or Issues

Category: Troubleshooting

SSH Known-Hosts Error

SSH offers the ability to verify the identity of the remote host to which you are connecting. A successful host verification indicates that your SSH client has established a secure connection with the SSH server and no intermediate machines have access to that connection.

The identity of the remote host can be verified by checking the host public key of the remote host stored either in the system-wide `/etc/ssh/ssh_known_hosts` file (or `/etc/ssh/known_hosts` for some systems) or your personal `~/.ssh/known_hosts` file on your localhost.

SSH has three ways it can react to an unrecognized or changed SSH host key, based on the value of the `StrictHostKeyChecking` variable in either the system-wide `/etc/ssh/ssh_config` file (or `/etc/ssh_config` for some systems) or your personal `~/.ssh/config` file:

`StrictHostKeyChecking=no`

This is the most insecure setting as it will blindly connect to the server. It will add the server's key if it's not present locally, and if the key has changed it will add the key without asking.

`StrictHostKeyChecking=ask`

With this setting, if you have no host key for the server, it will show you the fingerprint and ask you to confirm. If you connect and the key does not match, it will prevent you from logging in, and will tell you where to find the conflicting key inside the `known_hosts` file.

`StrictHostKeyChecking=yes`

This is the most secure setting. If you have no host key for this server, then it will prevent you from logging in at all.

If `StrictHostKeyChecking` is set to `yes` and you get errors similar to the following the first time you log in to one of the SFEs, the simple solution is to add `-o "stricthostkeychecking=ask"` in your ssh command. `sfe1` is used in this example.

Sample Error

```
your_localhost% ssh sfel.nas.nasa.gov
```

```
WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!  
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!  
Someone could be eavesdropping on you right now (man-in-the-middle attack)!  
It is also possible that the RSA host key has just been changed.  
The fingerprint for the RSA key sent by the remote host is  
11:9f:ae:09:56:2d:45:66:8e:9a:df:15:52:d6:88:5e.  
Please contact your system administrator.  
Add correct host key in /Users/userid/.ssh/known_hosts2 to get rid  
of this message.  
Offending key in /etc/ssh_known_hosts2:24  
RSA host key for sfel.nas.nasa.gov has changed and you have  
requested strict checking.  
No RSA host key is known for sfel.nas.nasa.gov and you have  
requested strict checking.  
Host key verification failed.
```

Solution

```
your_localhost% ssh -o "stricthostkeychecking=ask" sfel.nas.nasa.gov
```

```
-----  
The authenticity of host 'sfel.nas.nasa.gov (198.9.4.3) '  
can't be established.  
RSA key fingerprint is  
11:9f:ae:09:56:2d:45:66:8e:9a:df:15:52:d6:88:5e.  
Are you sure you want to continue connecting (yes/no)? yes  
-----  
Warning: Permanently added 'sfel.nas.nasa.gov,198.9.4.3' (RSA) to  
the list of known hosts.  
-----  
Plugin authentication  
Enter PASSCODE: type your passcode
```

Common SecurID Passcode Problems

If you cannot log in after you created your new PIN, it is possible that you did not successfully complete the "New-Pin Process". You might have used a special character in your PIN. Your PIN must consist of EXACTLY 8 alphanumeric characters, with at least one letter and at least one number, but no special characters.

```
your_localhost% ssh sfel  
user@sfel's password:  
Authenticated with partial success.  
Plugin authentication  
Enter PASSCODE:  
Plugin authentication  
You may create your own PIN or accept a server assigned PIN.  
Would you like to create your own new PIN (yes/no)? yes
```

```
Plugin authentication
Enter a new PIN of 8 alphanumeric characters:
Re-enter new PIN to confirm:
Enter PASSCODE:
Plugin authentication
Enter PASSCODE:
Permission denied, please try again.
user@sfel's password:
Permission denied, please try again.
user@sfel's password:
Permission denied ().
```

Each SecurID 6-digit tokencode can be used only once. If you try to use a tokencode that has just been used, you will be prompted again to enter a new passcode.

```
your_localhost% ssh sfel.nas.nasa.gov
PAM Authentication
Enter PASSCODE: enter PIN and a tokencode which was just used
PAM Authentication
Enter PASSCODE: ener PIN and a new token code
```

If you failed to provide a correct PIN + tokencode in a few consecutive attempts, your SecurID fob will be temporarily disabled. NAS Help Desk can help you unlock your fob (even for fobs provided by your local center). Call NAS Help Desk at (800) 331-USER (8737) or (650) 604-4444 for assistance.

Common Passthrough Problems

If you set up SSH passthrough correctly, you should be prompted for your SecurID passcode only, and be transferred to the desired host. The following describes a few common problems and their solutions:

Authentication Failure

If the authentication failed when you entered the passcode, it is possible that you have different usernames between your localhost and the NAS systems and you did not include your NAS username in your `.ssh/config` file.

There are two ways to include your NAS username in the `.ssh/config` file:

- If you use the `.ssh/config` file for connecting to multiple computer sites, then you should add your NAS username to the ProxyCommand lines for corresponding NAS hosts, for example:

```
Host lou1
ProxyCommand ssh username@sfel.nas.nasa.gov /usr/local/bin/ssh-proxy lou1
```

In this case, you will still need to issue your **ssh** command as the following example in order to avoid being prompted for a password:

```
%ssh nas_username@lou1
```

- If you use the **.ssh/config** file only for connecting to NAS, then you can simply add the following at the beginning of your **.ssh/config** file:

```
User nas_username
```

You do not need to add your NAS username to the ProxyCommand line. In addition, you can simply use the following command and won't be prompted for a password:

```
%ssh lou1
```

Prompted for Password

If you are prompted for password in addition to the passcode, there are multiple possible causes:

- You may have a different username and need to use:

```
your_localhost% %ssh nas_username@lou1
```

- Either your home directory or the **.ssh/authorized_keys** file under your NAS account have write permission for group or others. You need to correct the permission so that they have write permission only to you.
- Either one or both of the following files is missing:
 - ◆ **.ssh2/authorization** of sfe[1,2]
 - ◆ **.ssh/authorized_keys** of the NAS HECC host that you want to connect to

Prompted for Passphrase

If you are prompted for passphrase in addition to the passcode, likely, you did not use the commands **ssh-agent** and **ssh-add ~/.ssh/id_rsa** to forward your private key before you issue the **ssh** command.

Incorrect Ciphers

A cipher is an algorithm for performing encryption or decryption. The SSH client and server must have a matching cipher in order to successfully verify the keys. If you get an error

similar to the following:

```
no matching cipher found: client blowfish-cbc
server aes128-cbc,aes192-cbc,aes256-cbc,3des-cbc
```

Check your `./ssh/config` file or `/etc/ssh/ssh_config` file on your localhost and add the appropriate ciphers.

To modify `/etc/ssh_config`, system administrator's privilege may be needed.

Password Expiration

Your NAS password is valid for 60 days. An email is sent to you by NAS reminding you to change your password. If it has expired, you can still log in. However, you will be prompted to change it right away.

Account Expiration or Deactivation

Your NAS account is active if you have a valid project and a valid account request form on file at NAS. If your account has expired, it will be removed from NAS database and the `/etc/passwd` files. When this happens, no login will be allowed.

Please note that the account request form has to be filled out once every year. When the form has expired, you should receive an email from the NAS account administrator asking you to fill out a new one.

If you violate NAS security rules such as those listed in the [Acceptable Use Statement](#), your account can be deactivated.

Article ID: 162

Last updated: 08 Aug, 2012

Troubleshooting -> Common Login Failures or Issues

<http://www.nas.nasa.gov/hecc/support/kb/entry/162/?ajax=1>