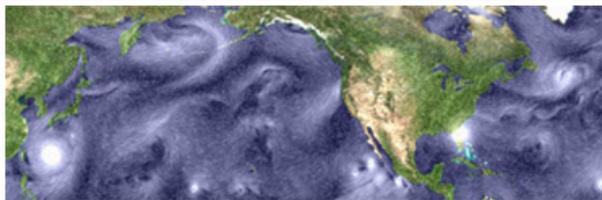




+Home



### COLUMBIA SUPERCOMPUTER

- + Highlights
- + Scientific Projects
- + Press Releases

#### - GETTING ACCOUNTS

- + U.S. CITIZEN
- + NON-CITIZENS
- + PI RESOURCES
- + SYSTEM STATUS
- + FORMS
- + DOCUMENTATION
- + POLICIES & PROCEDURES
- + FAQ

### SecurID

#### What is SecurID?

The RSA SecurID Authenticator functions like an ATM card. Network and desktop users must identify themselves with two unique factors - something they know, and something they have - before they are granted access. More than 15 million people around the world confidently use RSA SecurID Authenticators to securely access VPN and remote access applications, web servers and applications, network operating systems, Microsoft desktops and more.

More information can be found at the RSA SecurID website:  
<http://www.rsasecurity.com/>

#### Using Your New SecurID Token

The enclosed RSA SecurID token (fob) is required for you to access systems, such as Pleiades or Lou, at the NASA Advanced Supercomputing (NAS) Facility. Access is obtained through the secure front-end systems Bouncer, Bruiser, SFE1, and SFE2. Please read all instructions before beginning. Then follow the steps below to enable your fob, obtain a password, select your Personal Identification Number (PIN), and use your fob to log into the NAS systems.

#### How Your SecurID Token Works

Your fob displays a unique pseudo-random number (called the tokencode) that changes every 30 or 60 seconds (depending on what model you received). Notice the set of six bars on the left side of the fob, which disappear over time. Once all bars disappear, the fob displays a new tokencode and a new set of bars appears.

Each time you log into the front-end systems Bouncer, Bruiser, SFE1, or SFE2, you will complete a two-factor identification process, in which you will:

1. Enter a Personal Identification Number (PIN) and the tokencode; this combination demonstrates that the fob assigned to you is in your possession.
2. Do (a) or (b):
  - (a) Enter your system password. First-time users will be given an initial password by NAS Help Desk staff; continuing users will use their existing passwords.
  - (b) If you are not a first-time user and you have set up your SSH public/private key, use public/private key authentication.

When both factors have been correctly completed, you will be authenticated for access to these systems.

#### First Time Login to Secure Front-End

##### Step 1: Enable your Token

Your SecurID fob has been sent in a *disabled* state. To enable your fob:

- Call the NAS Help Desk (650-604-4444 or 1-800-331-8737).

Help Desk staff will confirm your identity by calling you back at your work phone number on record; they will then enable your fob, setting it in New PIN Mode.

**NOTE:** First-time users will be given an initial password by Help Desk staff when they call to enable their fobs.

**IMPORTANT:** Before you begin Step 2, your computer must be set up to log in using SSH.

##### Step 2: Complete the New-PIN Process

The first time you log in to any of the secure front-end machines listed above, you will set up a Personal Identification Number (PIN) and complete a two-factor authentication process. You will be prompted to choose a PIN or to have a PIN automatically selected for you. To complete the new-PIN process:

- A. Log in using secure shell:

```
ssh machine.nas.nasa.gov
```

where *machine* is bouncer, bruiser, sfe1, or sfe2

#### NOTES:

If you get a message that indicates an "ssh\_known\_hosts" error, see "Handling an 'SSH Known Hosts' Error, below.

- B. At the prompt "Enter PASSCODE," enter the tokencode displayed on the fob.

```
-----
Plugin authentication
Enter PASSCODE:
```

#### GET HELP

**Hours of operation:**  
24 hours 7 days a week

**Toll-free:** 1-800-331-8737  
**Local:** 650-604-4444  
**Ames:** 4-4444  
**E-mail:** [support@nas.nasa.gov](mailto:support@nas.nasa.gov)

- C. At the prompt, select whether to create your own PIN (4 to 8 numbers or letters with NO special characters) or to have one created for you (type "yes" or "no"). In either case, memorize your PIN. **Never write down your PIN.**

```
-----  
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)?  
Plugin authentication  
Enter your new PIN (4 to 8 digits or characters)  
New PIN:  
Confirm new PIN:
```

- D. Wait for the tokencode displayed on your fob to change, then enter your PIN, followed immediately by the tokencode, and hit RETURN.

For example, if your PIN is "d70i398" and your fob displays the tokencode "052993" then enter "d70i398052993" and hit RETURN. Note that you can use either a lowercase or an uppercase "D" because PINs are not case sensitive.

```
-----  
Plugin authentication  
Wait for token to change, and enter PASSCODE:
```

The new-PIN process is now complete, even though you may not get clear confirmation on your screen. You will use your new PIN to log into any of the four front-end systems. Your PIN is valid for one year.

Continue to Step 3 to log in using the two-factor authentication process.

### Step 3: Complete First-time Two-factor Authentication

Once you complete the new-PIN process, the system will prompt you to log in using two-factor authentication for the first time. First-time users will also be prompted to change their initial password.

- A. At the prompt asking for your PASSCODE, enter your PIN followed immediately by the tokencode displayed on the fob (same as Step 2D).
- B. At the prompt, enter your system password.

You are now authenticated, and can log into other systems at the NAS Facility on which you have an account.

**NOTE:** Each tokencode displayed on your fob can be used just once. If you have to authenticate twice (for example, because you mistyped your system password), you must wait for your fob to display a new tokencode, and then re-enter the new PASSCODE.

### Subsequent Log-ins: two-factor authentication

You are required to use two-factor authentication whenever you log into Bouncer, Bruiser, SFE1, or SFE2.

You will enter your PASSCODE (PIN + tokencode) and your system password, as done in Step 3, above, or, enter your PASSCODE and public/private authentication if you have set up your public/private key.

Remember, if for any reason you have to authenticate twice, you must wait for your fob to display a new tokencode, and re-enter the new PASSCODE.

### Additional Important Information

#### The 'next tokencode' prompt

The clock in your fob can "drift," causing it to display a tokencode that is a little ahead or a little behind the correct sequence. If there is too much drift, you will be prompted to enter the next tokencode to be displayed on your fob. If this occurs, enter *only* the next tokencode and *not* your PIN and the tokencode.

If entering the next tokencode doesn't authenticate you to SecurID, call the NAS Help Desk at 650-604-4444 or 1-800-331-8737.

### SecurID fob tips

- Never divulge your PIN. **No NAS staff member will ever ask you for your PIN.**
- If you think someone may have learned your PIN, call the NAS Help Desk at (650-604-4444 or 1-800-331-8737).
- If your fob is missing, call the NAS Help Desk.
- Your fob is plastic and can be broken. This electronic device is vulnerable to environmental extremes. If you leave it in a parked car on very cold or hot days, its clock will drift. Please take care of your fob.

### Handling an 'SSH Known-Hosts' Error

Depending on your system's SSH configuration, you may get an error message the first time you log in to one of the NAS secure front-end systems (Bouncer, Bruiser, SFE1, SFE2). The simple solution below is sufficient for many users to fix this error.

Sample Error Message

```
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.
```

**To Correct the Problem:**

A. Type the command:

```
ssh -o stricthostkeychecking=ask machine.nas.nasa.gov
```

where machine is bouncer, bruiser, sfe1, or sfe2

The following message will be displayed:

```
-----  
The authenticity of host 'sfe1.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)?
```

B. Type "yes" at the above prompt, "Are you sure you want to continue connecting (yes/no)?"

This will add the machine fingerprint to your approved list and the warning message should not appear again.

The following message (shown in part) will be displayed:

```
-----  
Warning: Permanently added 'sfe1.nas.nasa.gov,198.9.4.3' (RSA) to the list of known hosts.  
-----
```

```
-----  
Plugin authentication  
Enter PASSCODE:
```

**I can't seem to login after I created my PIN**

You did NOT successfully complete the "New-Pin Process". You might have used a special character in your PIN. Your PIN MAY ONLY consist of alphanumeric characters (Letters , and Numbers) no special characters. **If your session looked like this:**

```
-----  
lou.user 53> ssh sfe1  
(Warning Banner Here)
```

```
user@sfe1'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 your new PIN (4 to 8 digits or characters)  
New PIN:  
Confirm new PIN:  
Plugin authentication  
Enter PASSCODE:  
Plugin authentication  
Enter PASSCODE:  
Permission denied, please try again.  
user@sfe1's password:  
Permission denied, please try again.  
user@sfe1's password:  
Permission denied ().  
-----
```

The system should display:

```
"Wait for token to change, and enter PASSCODE:"
```

immediately after you confirm your pin. This means the PIN you entered has been accepted by the system.



- + Feedback
- + Site Help
- + NASA Privacy Statement, Disclaimer, and Accessibility Certification



Editor: Jill Dunbar  
Webmaster: Ryan Spaulding  
NASA Official: Walt Brooks  
[+ Contact NAS](#)

Last Updated: March 22, 2010