

RSA SecurID Tokens

NASA uses RSA SecurID technology to provide secure authentication to its supercomputing resources. To log into the systems in the NAS secure enclave, all NAS users must have an RSA SecurID token.

When you get a new NAS account or need to renew an existing NAS token, you can choose one of two types:

- Hard token (a small hardware device called a fob)
- Soft token (a software app installed on your iPhone or Android device)

Both types of token generate a pseudo-random number, called a tokencode, at regular intervals. The tokencode is used in conjunction with a personal identification number (PIN) to authenticate to NAS systems.

This article describes each type of token and how to enable it. To learn more about RSA SecurID technology, see the [RSA website](#).

Note: If your RSA SecurID token was provided by NAS and you need support, please contact the NAS Control Room at (800) 331-8737 or (650) 604-4444. If your token was provided by another NASA center, please contact your local help desk for assistance.

Hard Token (Fob): Description

The RSA SecurID fob generates and displays a six-digit token code every 30 seconds. Your PIN is combined with the tokencode currently displayed on the device to create a passcode, and the passcode is used to authenticate into NAS systems. This is known as One Time Password (OTP) technology.

For example, a PIN **xyy123zzz** combined with the tokencode shown below creates a one-time passcode, **xy123zzz101568**:



On the left end of the display, six bars serve as a countdown timer for the currently displayed tokencode. Once the bars are gone, a new random number is displayed and the six bars re-appear to restart the countdown process.

The back side of the fob has three identifiers:

- Unique serial number
- Expiration date
- Manufacturer's batch number

Fob Care

Do not expose the fob to extreme temperature, pressure, x-rays, or magnetic fields.

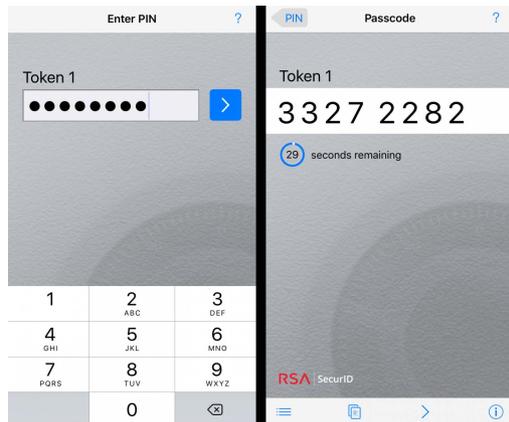
If your NAS-supplied RSA SecurID fob is damaged or lost, immediately contact the NAS Control Room at (800) 331-8737 or (650) 604-4444 to request a replacement fob. Replacement may take a few days, depending on postal delivery times. Therefore, to help you access NAS systems while you wait for your new fob to arrive, the Control Room analyst can issue you a set of 10 temporary passwords (each usable only once and in combination with your PIN). You may request another set if the initial set is used before your fob arrives.

To enable your fob, see "**Enabling Your RSA SecurID Hard Token (Fob)**" on page 3.

Soft Token (App): Description

The RSA SecurID soft token app is available for your iOS or Android device.

Like the fob, the soft token displays a tokencode every 30 seconds. However, the soft token uses a different, two-step method of associating a PIN with a tokencode. First, you enter your PIN into the app, as shown in the first screen below. The second screen displays an eight-digit tokencode:



This eight-digit tokencode is your entire passcode. Because it is associated with the PIN that was used to obtain it via the soft token, it does not need to be combined with the PIN to log into NAS systems or other agency systems.

Tip: Some agency systems may specify that your passcode is your PIN + tokencode. If you have an RSA SecurID soft token, disregard this instruction. Enter only the tokencode.

To enable your soft token, see "**Enabling Your RSA SecurID Soft Token (Mobile App)**" on page 5.

Enabling Your RSA SecurID Hard Token (Fob)

Before You Begin: Use this procedure if you have an RSA SecurID Hard Token (fob). If you have a NAS-provided soft token (mobile app), see "Enabling Your RSA SecurID Soft Token" on page 5.

If you are a new user logging in for the first time, complete Steps 1-3 to enable your RSA SecurID fob, set up a personal identification number (PIN), and change your default NAS password.

If you are a current user and you just need to enable a new fob, complete Steps 1 and 2.

Note: These steps apply only to the agency-wide RSA SecurID fobs that are provided by the NAS Division at NASA Ames Research Center. If your token was provided by another NASA center, please contact your local help desk for assistance.

Step 1: Enable Your RSA SecurID Fob

Your SecurID fob was sent in a disabled state. To enable the fob, call the NAS Control Room at (800) 331-8737 or (650) 604-4444. NAS support staff will enable the fob remotely and set it to New PIN Mode. If you are a first-time user, a default NAS password will also be provided to you during the call.

Please note that NAS support staff will confirm your identity by asking you the security question you submitted with your account request form, or by calling you back at your phone number on record.

Step 2: Log into an SFE and Set Up a PIN

Before You Begin: Your local system must be configured to log in using the Secure Shell (SSH) protocol. You will also need your enabled RSA SecurID fob.

1. On your local system, open a command-line interface terminal.
2. Use SSH to log into an SFE, as follows:

```
your_local_system% ssh sfeX.nas.nasa.gov
```

where **sfeX** is sfe1, sfe2, or sfe3.

Note: If you use different usernames on your local system and NAS systems, add your NAS username before specifying the SFE. For example:

```
your_local_system% ssh zsmith@sfe1.nas.nasa.gov
```

3. At the "Enter PASSCODE" prompt, shown below, type the six-digit tokencode that is displayed on your RSA SecurID fob.

```
-----  
PAM authentication  
Enter PASSCODE:
```

4. Follow the instructions at the next prompt to create a PIN, which must be exactly 8 alphanumeric characters including both letters and numbers (no special characters). Letters are not case-sensitive.

```
-----  
PAM authentication  
To continue you must enter a new PIN. Are you ready to enter a new PIN? (y/n)  
PAM authentication  
Enter a new PIN of 8 alphanumeric characters:  
PAM Authentication  
Re-enter new PIN to confirm:  
PAM Authentication  
New PIN accepted, press enter to continue.
```

Note: Memorize your PIN. Never write down your PIN.

5. Wait for the tokencode displayed on your fob to change. Then, enter your PIN at the prompt, followed immediately by the tokencode. For example, if your PIN is "d701398z" and your fob displays the tokencode "052993," type **d701398z052993** and press **Enter**:

```
-----  
PAM authentication  
Wait for token to change, and enter PASSCODE: d701398z052993
```

Together, your PIN and your current tokencode comprise your RSA SecurID passcode.

The new-PIN process is now complete, although you may not get clear confirmation on your screen. Currently, PINs do not expire, but this may change in the future.

WARNING: Never divulge your PIN. NAS staff members will *never* ask you for your PIN. If you think someone may have learned your PIN, call the NAS Control Room at (800) 331-8737 or (650) 604-4444.

Step 3: Log in Again and Change Your Default NAS Password

After you complete the new-PIN process, the system will prompt you to log in again. If you are a new NAS user, you must complete these steps to change your default NAS password.

1. At the "**Enter PASSCODE**" prompt, enter your RSA SecurID passcode (your PIN followed immediately by the tokencode displayed on your fob).
2. At the next prompt, enter the default NAS password provided to you by NAS support staff.
3. Change your default NAS password. (See "**Password Creation Rules**" on page 7.)

Note: If you are not prompted to update your password after logging into the SFE, you can trigger a prompt by logging into a Lou front-end system (LFE) with the command `ssh lou`. You will be prompted to input your default NAS password, then asked to create and confirm a new password.

4. Wait 15 minutes for the new password to propagate to all systems.

Tip: Each tokencode displayed on your fob can be used only once. If you have to authenticate twice (for example, if you mistype your NAS password), you must wait for your fob to display a new tokencode, and then re-enter the entire passcode (PIN + new tokencode).

You have now completed your first-time authentication to NAS systems using your NAS password and your RSA SecurID token. For information about subsequent logins, see the HECC Knowledge Base article [Logging into NAS Systems](#) (requires RSA SecurID or NASA PIV card authentication).

Enabling Your RSA SecurID Soft Token (Mobile App)

Before You Begin: Use this procedure if you have an RSA SecurID Soft Token (mobile app). If you have a NAS-provided hard token (fob), see "Enabling Your RSA SecurID Hard Token" on page 3.

If you are a new user logging in for the first time, complete steps 1-3 to enable your RSA SecurID soft token, set up a personal identification number (PIN), and change your default NAS password.

If you are a current user and you just need to enable your soft token, complete steps 1 and 2.

Note: These steps apply only to the agency-wide RSA SecurID fobs that are provided by the NAS Division at NASA Ames Research Center. If your token was provided by another NASA center, please contact your local help desk for assistance.

Step 1: Download the RSA SecurID App and Obtain Token Import URL

1. Download the RSA SecurID Software Token app from the Apple App Store or Google Play to your iOS or Android device.
2. Open the RSA SecurID app and locate your Binding ID (iOS) or Device ID (Android).
3. Select **Email Binding ID** (iOS) or **Email Device ID** (Android) and send the email to support@nas.nasa.gov.
4. Wait for a reply from NAS support staff. You will receive an email containing your RSA SecurID soft token import URL and instructions for setting it up.

Step 2: Enable Your Soft Token and Create Your PIN

Follow the setup instructions provided in the email you received from NAS support staff. During this process you will need to switch between your iOS or Android device and a computer with Internet access.

First-time users will also need to contact the NAS Control Room to obtain a default NAS password. Please note that NAS support staff will confirm your identity by asking you the security question you submitted with your account request form or by calling you back at your phone number on record.

WARNING: Never divulge your PIN. A NAS staff member will *never* ask you for your PIN. If you think someone may have learned your PIN, call the NAS Control Room at (800) 331-8737 or (650) 604-4444.

Step 3: Log into the Secure Enclave and Change Your Default NAS Password

If you are a new NAS user, you must complete the steps in this section to log into NAS systems for the first time and change your default password. (If you do not have a default NAS password, contact the NAS Control Room at (800) 331-8737 or (650) 604-4444.)

Before You Begin: Your local system must be configured to log in using the Secure Shell (SSH) Protocol.

1. On your local system, open a command-line interface (CLI) terminal.
2. Use SSH to log into a secure front-end system (SFE), as follows:

```
your_local_system% ssh sfeX.nas.nasa.gov
```

where *sfeX* is sfe1, sfe2, or sfe3.

Note: If you use different usernames on your local system and NAS systems, add your NAS username before specifying the SFE. For example:

```
your_local_system% ssh zsmith@sfe1.nas.nasa.gov
```

3. In the RSA SecurID app, enter your PIN to obtain a passcode.
4. At the "**Enter PASSCODE**" prompt in the CLI terminal, enter the RSA SecurID passcode displayed in the app.
5. At the next prompt, enter your default NAS password.
6. Change your default NAS password. (See "**Password Creation Rules**" on page 7.) It may take up to 15 minutes for the new password to propagate to all systems.

Note: If you are not prompted to update your password after logging into the SFE, you can trigger a prompt by logging into a Lou front-end system (LFE) with the command `ssh lou`. You will be prompted to input your default NAS password, then asked to create and confirm a new password.

Tip: Each passcode displayed in your soft token can be used only once. If you have to authenticate twice (for example, because you mistype your NAS password), you must wait for the token to display a new passcode. You have now completed your first-time authentication to NAS systems using your NAS password and your RSA SecurID token. For information about subsequent logins, see the HECC Knowledge Base article [Logging into NAS Systems](#) (requires RSA SecurID or NASA PIV card authentication).

Password Creation Rules

Strong passwords are required to protect the security of NAS systems.

When you create or change your NAS password, specify a unique password that you have never used anywhere else. Never use your NAS password for any other application under any circumstances.

Follow these rules when you create your password:

1. Use a minimum of 12 characters
2. Include characters from at least three of the following types:
 - ◆ Uppercase letters
 - ◆ Lowercase letters
 - ◆ Numbers
 - ◆ Special characters (e.g., \$! @ #)
3. Do not use a "trivial" password that can be easily guessed; for example, do not use:
 - ◆ Your agency user ID (AUID)
 - ◆ A dictionary word in any language, or a dictionary word with numbers appended or prepended to it (for example, "hello22" or "22hello")
 - ◆ A contractor name
 - ◆ A division or branch name
 - ◆ A password partly or fully composed of any of the following terms: your user ID, name, birth date, Social Security number, family member or pet's name, your name spelled backwards, or any other personal information
 - ◆ The name of any automobile or sports team
 - ◆ The name of any vendor product or product nickname
 - ◆ Repetitive or keyboard patterns (for example, "abc#ABC", "1234", "qwer", "mnbvc", "aaa#aaaa")
4. Do not use any of your previous 24 passwords

After you successfully change your password, you must wait at least one day to change it again. You must change your password every 60 days.

WARNING: *Never* share your password with anyone.