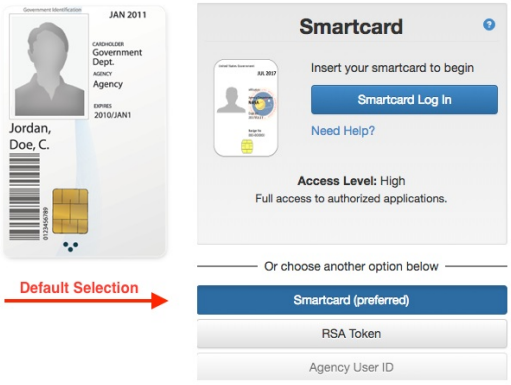
In order to perform some basic tasks that use NAS web applications, such as changing your NAS password or logging into the myNAS portal, you must authenticate to NASA's Access Launchpad using your NASA Smartcard or RSA SecurID token.

Using Your NASA Smartcard

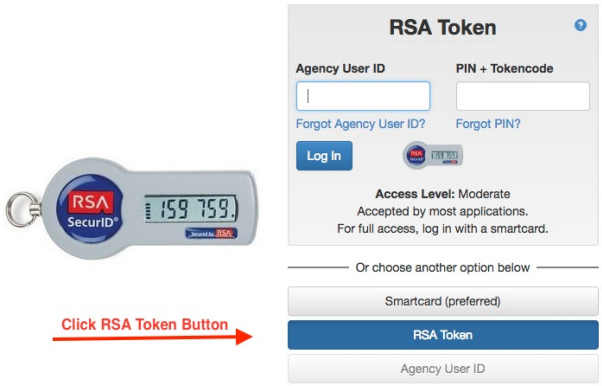
This is Launchpad's default option. Make sure **Smartcard (preferred)** is selected, insert your NASA smartcard into your workstation's card reader, and click **Smartcard Log In**, as shown below. Enter your PIN when prompted.



Using Your RSA SecurID Token

Select the **RSA Token** option, provide your Agency User ID, and enter your passcode, as shown below.

If you have an RSA SecurID fob, your passcode is your PIN + the token code displayed on the fob. If you have a soft token, enter your PIN in the RSA SecurID app to get the token code, then enter *only* the token code in the **PIN + Tokencode** field.



Once you are authenticated to Launchpad, you will be connected to the NAS password change form, the myNAS web portal, or another NAS web application to complete your task.

As a NAS user, you are responsible for being aware of the following account-related policies:

- Users must comply with the NAS Systems Environment (NSE) Rules of Behavior.
- Users and NAS staff requesting either a new or a renewed account must complete the CYBERSECURITY AND PRIVACY AWARENESS TRAINING course available at https://satern.nasa.gov/. The course must be completed annually.
- Users and NAS staff requesting either a new or renewed account must fill out an Account Request form for the annual New Operational Period (NOP).

Account Deactivation

Users who do not comply with the rules listed in the NSE Rules of Behavior will have their accounts disabled either temporarily or permanently. Account deactivation will result after 60 days of inactivity and data may be deleted after 90 days unless a user or project makes arrangements with NAS User Services to preserve their data.

In the field of security, there are three general factors that can be used to prove that you are who you claim to be:

- Something you have (such as an ID card)
- Something you know (such as a password)
- Something you are (such as your fingerprint)

Two-factor authentication refers to using any two of these factors to authenticate a person before access to systems is granted.

NAS Two-Factor Authentication Policy

The NAS facility uses the following factors:

1. Your assigned RSA SecurID token
2. Your public/private key pair (or your NAS password, which is accepted by the SFEs but not the PFEs)

You must authenticate yourself with these factors before you can access NAS resources from outside the NAS secure enclave. One of these factors must be your RSA SecurID token.

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. For more information about user requirements and responsibilities, read the Security Training Requirements and the NAS System Environment Rules of Behavior.

Public-key authentication is a means of identifying yourself by proving that you know the private key associated with a given public key. This method is more secure than password authentication, but it requires more effort to set up.

Public-Key Basics

To use this method, you use the ssh-keygen program to generate a public/private key pair on your local system. You will be prompted for a passphrase which is used to encrypt the private key. By default, the private key is stored in ~/.ssh/id_rsa and the public key is stored in ~/.ssh/id_rsa.pub.

The private key should only be kept on your local system and should be encrypted using a passphrase that is at least as strong as any password you would normally use. The security of this method depends on keeping the private key safe and secure.

The public key can be safely copied to other systems and appended to ~/.ssh/authorized_keys on those systems. The server uses this copy of the public key to confirm that you possess the private key.

When you authenticate to a server using public-key authentication, the SSH client offers a copy of the public key to the server and the server then compares it against the keys listed in your ~/.ssh/authorized_keys file. If it matches, the server indicates that it is able to proceed with the authentication. At that point, the SSH client will prompt you for the passphrase in order to decrypt the private key. The private key is then used to sign a message that includes data specific to the SSH session. The server can then use its copy of the public key to verify the signature.

If the server can verify the signature, you are authenticated.

Why Are Public/Private Keys More Secure Than Passwords?

- The passphrase is never sent over the network
- The private key is never sent over the network
- It is extremely computationally expensive to derive the private key from the public key
- Protects against man-in-the-middle attacks

SUID/SGID Scripts

Users are prohibited from creating and using privileged SUID and/or SGID scripts under their home, scratch, /nobackup, and /tmp filesystems.

SUID scripts (that is, with permission u+s) and SGID scripts (with permission g+s) could allow someone (other than the owner) to gain unauthorized access to users' files, posing a security hazard.

WARNING: The high end computing systems at the NAS facility are configured to disable the execution of any SUID/SGID shell scripts.

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.

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)

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

To learn how to create your PIN and log into NAS systems, see Enabling Your RSA SecurID Hard Token (Fob).

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.

Soft Token

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 learn how to create your PIN and log into NAS systems, see Enabling Your RSA SecurID Soft Token (App).

The secure front ends (SFEs) are the bastion hosts protecting the NAS secure computing enclave. The enclave includes all of the major HECC systems, including: Aitken, Electra, Endeavour, Lou, and the hyperwall.

To access resources inside the enclave from your local system, you must first use Secure Shell (SSH) to connect to one of the SFEs (sfe[*6-8*]) and log in using one of the following two-factor authentication methods:

- RSA SecurID + NAS password
- RSA SecurID + NASA personal identity verification (PIV)
- RSA SecurID + public key

Once authenticated, you can then use SSH to access any of the NAS systems from the SFE.

You can avoid having to log in twice (first to an SFE and then to a system inside the enclave) by setting up SSH Passthrough.

Note: Using SSH to connect from the SFEs to hosts outside of the enclave is not allowed.

New SFE Features and Changes

The SFEs (sfe[*6-8*]), which replaced some old SFEs in 2021, have some new features as well as some changed functionality:

- The new SFEs are built on a different and more restrictive architecture than the old ones. You can no longer directly read or write any file on the SFEs. You can only execute the commands ssh, ssh-balance, and a new command called ssh-key-init.
- SSH public keys used for SSH passthrough are managed using the new ssh-key-init command. For instructions on using this command to initialize public keys, see: Setting Up Public Key Authentication
- Transfers to and from the SFEs themselves are no longer allowed. Existing mechanisms using SSH passthrough and SUP/Shift are still supported as previously. For transfer instructions, see: Inbound File Transfer Through SFEs: Examples
- When you log into an SFE using the RSA SecurID passcode + NAS password method, the password will now be prompted *before* the RSA SecurID passcode (instead of after).
- A new authentication method, RSA SecurID passcode + NASA PIV, is now available for users who hold NASA personal identity verification (PIV) badges. When your NASA badge is attached to your workstation via a card reader, this method enables you to log in using your PIV personal identification number (PIN) and RSA SecurID passcode.

You will receive a default password for your NAS account as part of the first-time login process. You will also be prompted to change the default password the first time you log in.

Note: Your NAS password is sometimes referred to as your "Lou" or "LDAP" password.

If you are a current user with an existing account on a NAS system and you are approved to get an account on another NAS system, your password on the new system is the same as your current NAS password. If you do not remember this password, call the NAS Control Room at (800) 331-8737 or (650) 604-4444 to obtain a new default password.

NAS passwords expire every 60 days. You will receive an automated email prompting you to change your password several days prior to expiration. There are two ways to change your password:

- Type passwd from one of the NAS compute resources or a Lou front-end system (such as a PFE or LFE) and follow the prompts.
- Use the NAS Password Change Form (you'll be prompted to authenticate via NASA's Access Launchpad).

When you change your password, be sure to follow the Password Creation Rules. If your password has already expired, you may need to contact the Control Room to change it.

Note: Due to security requirements, Control Room staff will confirm your identity by asking you the security question that you submitted with your account request form, or by calling you back at your phone number on record. If your phone number has changed due to office moves or reorganizations, your Principal Investigator must contact the Control Room and provide the reason for the change, either by phone or by sending an email to support@nas.nasa.gov.

The Secure Shell (SSH) protocol provides secure, encrypted communication between two untrusted hosts over an unsecured network, requiring users to prove their identities to successfully connect to a remote system. SSH is used both for interactive login sessions and for executing arbitrary commands on remote systems. Authentication information, such as a password or passcode, as well as data are both encrypted over the network.

SSH uses a client-server model. On the client, you initiate an SSH connection with the `ssh` command, which connects to the `sshd` daemon on the remote system.

OpenSSH at NAS

All NAS systems use the OpenSSH implementation of the SSH protocol. This implementation includes `ssh`, `scp`, `sftp`, `sshd`, and utilities such as `ssh-add`, `ssh-agent`, and `ssh-keygen`. Although OpenSSH includes support for both the SSH-1 and SSH-2 protocols, NAS systems accept connections using SSH-2 only.

WARNING: Due to security and performance issues with older versions of OpenSSH, we strongly recommend that you use OpenSSH 5.2 or later for best performance, security, and functionality.

Operating System Considerations

MacOS and Linux

MacOS and most Linux distributions include a version of OpenSSH. However, it is important to keep up with the latest security updates for your operating system to ensure that you have the latest version of OpenSSH supported by the vendor.

Windows/Cygwin

On systems running the Windows operating system, you must install a client that supports the SSH-2 protocol.

We recommend using Cygwin, which provides a Linux-like environment for Windows, and OpenSSH. For download and installation instructions, see Installing Cygwin (PDF).

To learn more about OpenSSH, see the **ssh(1)** and **ssh_config(5)** man pages.

See the following Wikipedia pages for more information:

- Secure Shell
- OpenSSH
- Cygwin

This document outlines the requirements for use of the computing systems, resources, and facilities located at and/or operated by the NASA Advanced Supercomputing (NAS) Division at NASA Ames Research Center (collectively, "NAS Systems Environment").

As a user of the NAS Systems Environment (NSE), I agree to the following and understand that failure to abide by these provisions may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution:

1. I will abide by all requirements in the "NASA Cybersecurity and Privacy Rules of Behavior" document.
2. NSE accounts are to be used only for the purpose for which they are authorized and are not to be used for non-NASA related activities.
3. If issued any Government Furnished Equipment (GFE), I will use only GFE to connect to NSE systems.
4. If issued any GFE, I will connect to the NASA VPN prior to and while utilizing NSE resources when my GFE is not directly connected to a NASA network.
5. I am responsible for using the computing systems, resources, and facilities in an efficient and effective manner. I understand that account deactivation will result after 60 days of inactivity and data may be archived after 90 days unless my project or I make arrangements with NAS User Services to preserve my data.
6. NSE resources support many users. I agree not to consume more resources than I have been authorized to use. If my activity is deemed to be excessive or has an adverse impact on other users, I understand that my processes may be terminated without warning.
7. I understand that these computing systems are unclassified systems. Processing and storing of Classified National Security Information is prohibited.
8. I understand that these computing systems are categorized as moderate risk according to FIPS 199; therefore, processing and storing information that is categorized as high risk is prohibited. Furthermore, these computing systems are NOT authorized to process or store Sensitive Personally Identifiable Information (PII). I will not introduce Sensitive PII into any NSE systems.
9. I understand that I am responsible for protecting any information processed or stored in my accounts and will take appropriate precautions to protect CONTROLLED UNCLASSIFIED INFORMATION (CUI) or other sensitive information, regardless of whether explicitly marked as sensitive, which may include encrypting the data to provide protection that goes beyond the standard operating system (OS) protections provided by the computing systems.
10. I understand that I shall not share my NSE user account credentials or authenticator tokens or facilitate unauthorized access to any NSE system. *This includes logging in to an NSE system and letting an unauthorized user access or use my session.*
11. I understand that I shall not engage in activities that compromise or weaken the security of NSE systems or have been identified as prohibited and high-risk practices by the NAS Security Team. These activities include, but are not limited to, keeping unauthorized world-writable directories, running password cracking programs, downloading, or introducing malicious software, running unauthorized software, *opening unauthorized listeners/port numbers, conducting unauthorized data transfers,* and copying or making available system and password configuration files to others.
12. I understand that I shall not make copies of copyrighted software except as permitted by law or by the owner of the copyright. I understand that I shall not use licensed software in a manner that violates the licensing agreement.
13. I understand that I shall not attempt to access any data or programs contained on systems for which I do not have authorization or explicit consent from the owner of the data/program, the NAS Division Chief, or the NAS Computer Security Official, nor shall I attempt to bypass any security controls without authorization.
14. I understand that I am required to report *immediately* any security weaknesses in the systems or any IT security incidents, including misuse or violation of this agreement, to the NASA Security Operations Center at +1 877.NASA.SEC or soc@nasa.gov.
15. I understand that I am required to access NSE systems only from remote systems that are safe from malicious programs and activity.
16. I understand that I will be required to complete the NASA mandatory CYBERSECURITY AND PRIVACY AWARENESS TRAINING course available at: https://satern.nasa.gov/. (Note: Additional details are available from NAS User Services.)
17. I understand that I may not disseminate information on behalf of the NAS Division on social media without export review and explicit authorization from an authorized NASA official. This limitation applies only to information owned by the NAS Division.
18. I understand that this/these system(s) and resources are subject to monitoring and recording and I will have no expectation of privacy in my use of and content on these systems and the computer equipment.
19. I understand that failure to comply with NAS Rules of Behavior may lead to loss of access, administrative action, and/or criminal prosecution.

The NAS Systems Rules of Behavior were last updated on December 11, 2023.