

# Two-Factor Authentication Policy

## Category: Security Policies

In the field of security, there are three general ways, called factors, for proving 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

At the NAS facility, the factors used are:

1. Your assigned RSA SecurID fob (sometimes called a key fob or a token)
2. Your password to the NAS systems or your public/private key pair

You are required to authenticate yourself with two of these factors before you can access NAS resources from outside the NAS high-end computing enclave. One of these two factors must be the possession of your SecurID fob. So, you can authenticate yourself with a combination of either SecurID + password, or SecurID + public/private key pair.

Two-factor authentication is required when accessing the following:

- The secure front-end systems, sfe[1-4], from your localhost
- The PFEs (pfe[20-27]), bridge[1-4], cfe2, or Lou[1-2] from your localhost using SSH Passthrough

---

Article ID: 32

Last updated: 14 Dec, 2012

Policies -> Security Policies -> Two-Factor Authentication Policy

<http://www.nas.nasa.gov/hecc/support/kb/entry/32/?ajax=1>