NAS VPN Service

NAS Staff Only: This article is applicable only to NAS Division staff.

Two virtual private network (VPN) services are available to local NAS staff to provide limited access to some NAS and/or Ames Research Center systems while working remotely, away from the NAS facility.

The NAS VPN service will make your system appear to be logically within the NAS external network, with some access to internal resources.

Using these VPNs requires a NASA PIV Badge or your NAS account and an active RSA SecurID token.

WARNING: All system traffic is routed through NAS while your system is connected via the VPNs, and all traffic is monitored, as if your system were physically connected to NASLAN. The VPNs are intended for government use only; usage requires that you follow the NAS Systems Environment Rules of Behavior. When you are finished with your session, please remember to log out.

VPN Client Application

The VPN client application, called Cisco AnyConnect Secure Mobility Client, is already installed on all NAS-provisioned Windows laptops and MacBooks.

Important: We do not permit VPN connections from non-government-owned personal computers.

If you do not have the Cisco AnyConnect Secure Mobility client application installed on your NAS or NASA-provisioned laptop, please contact the Control Room at support@nas.nasa.gov.

Note: Always connect to the VPNs by using the Cisco AnyConnect Secure Mobility Client, not through your web browser.

Logging Into the VPNs

Complete these steps to log into the NAS VPN:

1. Launch the **Cisco AnyConnect Secure Mobility Client** application from the Applications folder on your Mac. (It might also be available through an icon in your Mac's top navigation bar.)
2. In the **AnyConnect** dialog box, select one of the following options from the dropdown list:
    - **ARC_NAS_(Pri/Sec)** to log in using your NASA PIV badge.
    - **ARC_NAS_RSA_(Pri/Sec)** to log in using your RSA SecurID passcode.
3. Click **Connect**.
4. When the next dialog box pops up, make sure your NASA PIV card is in the card reader and provide your PIN (if you selected the one of the ARC_NAS options) or provide your NAS username and RSA SecurID passcode (if you selected one of the ARC_NAS_RSA options), and click **OK**.
5. Accept our NASA Terms and Conditions by clicking the **Accept** button.

Your system will automatically be logged out of the Cisco AnyConnect Secure Mobility Client after a maximum session length of 24 hours, after which time your system will be disconnected. You will be given a reminder before your system is disconnected.

Using the NAS VPN

You can use the following services while your system is connected via the NAS VPN:

- Apple file sharing (Apple Filing Protocol [AFP] remote mount).
- NAS license server.
- Internal NAS web server.
- Access to some Ames Research Center websites not accessible externally.
- SSH and SCP directly into NASLAN systems (*not* to systems inside the secure enclave).

Several changes are made to your network settings when you connect using the NAS VPN, including a new IP address, default route, search domain, and other minor changes, to enable your system to be virtually situated "inside" the NASLAN.

Important: Due to NAS security protocols, some of your home network services might stop working while your system is connected to the NAS VPN. This includes services such as wireless printing, file sharing, and audio streaming.