VPN

What is Remote Access VPN?

Obtaining remote access through a Virtual Private Network - or VPN - means connecting to an organization's private network with an encryption-secured connection. To ensure the highest security for our users and the data residing on the network, NIEHS employs highly secure login procedures for Remote Access VPN.

VPN Remote Access at NIEHS

NIEHS supports the VPN encrypted-secured connection to your government information from a remote location by adhering to the NIH Remote Access Policy, The policy mandates that all staff who have an HHS "Smartcard" ID badge with a small gold square, as shown on the image to the right, must use their badge along with their personal identification number (PIN) for remote access to the NIH network.

Your ID badge serves as personal identification verification (PIV) and is sometimes referred to as a PIV card. This ID badge is a secure and reliable form of identification that is strongly resistant to identity fraud. Using your ID badge and PIN for login is referred to as "two-factor authentication" which enhances security, since it requires two different types of identification: something you have (ID badge) and something you know (PIN).

Steps to Request Remote Access at NIEHS

All NIEHS employees who wish to utilize VPN must complete the following steps.

Step 1: Complete Required Training for Remote Access

All NIEHS employees who wish to utilize VPN must complete the mandatory NIH Secure Remote Access Training courses.

Note: For more online courses, see NIH Information Security and Information Management Training. Courses here include the privacy course and the annual security awareness course. Before you take the training, be aware of several notes:

- The training application tracks which modules you have completed.

- To get credit for completing a module, you must reach the last screen of the module.
- There are 3 courses: only the Refresher must be taken each year.
- The one-time primary course and one-time remote access course may be completed in 20-60 minutes, depending upon how much information you want to access.
- Even though you may print a certificate, it does not count as credit in the reporting system - the computer's database logs your activity for credit through the 'checkmarks' next to the login screen's notes.
- Once you have completed your training and signed your certificate NED should allow the request for remote access to continue.
- Please ensure that your NED information is always current because the information workflow depends on this contact information.

Step 2: Sign User Certification Agreement

Electronically sign the agreement and Rules of Behavior within the training module in Step 1, above.

Step 3: Speak with your Supervisor or COR

- Once you have completed your training and signed your certificate, meet with yoursupervisor (federal employees) or COR (contractors) to request VPN remote accessprivileges.
- Your supervisor or COR will send your request to your AO, who will update your NEDentry.

Step 4: Request the VPN client profiles if you do not have them on your portable computer.

- Requests for VPN clients need to be made as new IT tickets if you do not have a VPN client installed on your portable computer such as in the case of contractor furnished equipment.

Using the AnyConnect VPN Client

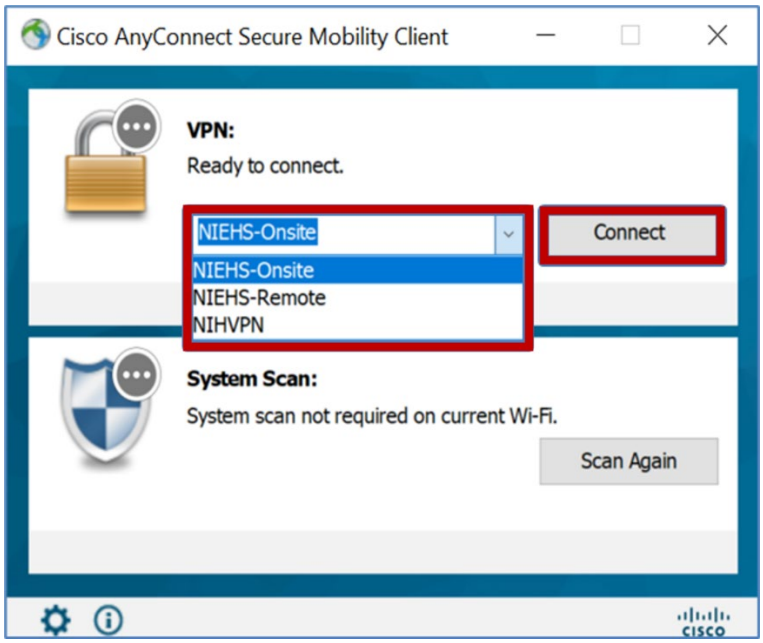
Software called *Cisco AnyConnect VPN Client* has already been installed on your NIEHS laptop to support VPN.

If do not see this icon  on your government computer, submit a NIH Help Desk ticket or call 866-319-4357. A technician will come to install the software on your machine.

PC Users:

1. Before inserting your badge into the card reader, launch the *Cisco AnyConnect VPN Client* from the **Start menu** in Windows: **Start/Programs/Cisco/Cisco AnyConnect VPN Client**.
2. Once you receive the *Cisco AnyConnect VPN Clien*t pop-up menu, choose the **NIEHS-Remote** option in the **Connect to:** box and click **Select**. **Note:** There are typically three options in this window.
    - **NIEHS-Onsite:****PREFERRED* used for accessing on-campus NIEHS wireless network.
    - **NIEHS-Remote:** **PREFERRED* used for working remotely and accessing the NIEHS network.

- **NIHVPN:** Used for working remotely and accessing the NIH network.
    - **Note:** If you connect to NIHVPN you may **not** receive weekly security patches. The Office of Information Technology (OIT) recommends NIEHS users to connect to one of the preferred options above for one entire workday, at least once a week.

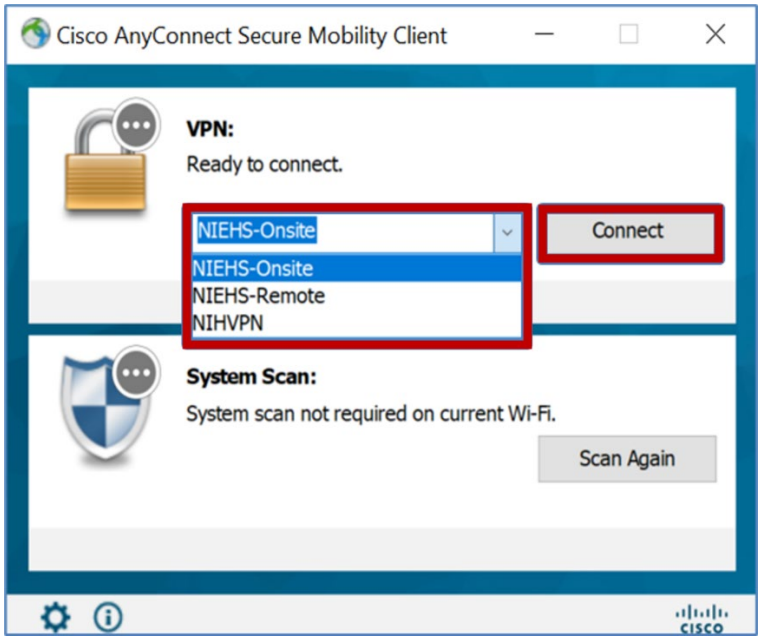


3. If your menu options do not include **NIEHS-Onsite or NIEHS-Remote** as indicated above, please contact the NIH Help Desk for assistance or call 866-319-4357.
4. Once prompted, insert your **ID Badge** into the computer's badge reader.
5. Type your **PIN** when prompted. You chose a PIN when you were issued your NIH ID badge (PIV Card).
6. If the connection is successful, you will see an icon in the lower right corner of your computer screen (in the taskbar), confirming the client is connected.
7. To disconnect from Remote Access, **right click** on the **AnyConnect icon** in the task bar and select **Disconnect** on the Connection tab of your AnyConnect software.

Mac Users:

1. Insert your ID Badge/PIV card into the computer's badge reader.
2. Launch the *Cisco AnyConnect VPN Client* through Applications. Go to **Applications**, then the **Cisco folder**, then double-click the Cisco ***AnyConnect VPN Client***.
3. Once you receive the *Cisco AnyConnect VPN Client* pop-up menu, choose the **NIEHS-Remote** option in the **Connect to:** box and click **Select. Note:**There are typically three options in this window.
    - **NIEHS-Onsite:****PREFERRED* used for accessing on-campus NIEHS wireless network.
    - **NIEHS-Remote:** **PREFERRED* used for working remotely and accessing the NIEHS network.
    - **NIHVPN:** Used for working remotely and accessing the NIH network.
        - **Note:** If you connect to NIHVPN you may **not** receive weekly security patches. The Office of Information Technology (OIT) recommends

NIEHS users to connect to one of the preferred options above for one entire workday, at least once a week.



4. If your menu options do not include **NIEHS-Onsite or NIEHS-Remote** as indicated above, please contact the NIH Help Desk for assistance or call 866-319-4357.
5. Type your **PIN** when prompted. You chose a PIN when you were issued your NIH ID badge (PIV Card).
6. Read the Warning banner and **Accept**. You are now connected to Remote Access.
7. To disconnect from Remote Access, click on the **Disconnect** button on the Connection tab of your AnyConnect software.

More Information

There are a few items to keep in mind when using VPN:

- Beginning September 18, 2019, NIEHS began enforcing NIH policy to block non-compliant government-furnished equipment (GFE) from accessing NIEHS VPN and NIHVPN. If your access to VPN is blocked, submit a ticket via the NIH IT Help Desk.
- Per NIH policy, VPN can only be utilized from a government or contractor furnished computer.
- Only Federal employees are granted RA privileges based on "Telework" requirements. Contractors are ineligible for remote access based on "Telework" requirements.
- To learn more about VPN Remote Access, see the NIEHS Public Website page covering Remotely Accessing NIEHS Resources: Network Access for NIEHS Staff.
- Also visit the NIH HHS ID Badge Smart Card website.

VPN Frequently Asked Questions (FAQ)

1. **What is a "Smartcard" ID badge/PIV Card?**
   A "Smartcard" ID Badge (also referred to as a PIV card) is an NIH-issued card that serves as Personal Identify Verification (PIV). If your NIH ID badge has a gold-colored chip in the middle of it, you have a PIV card.

2. **What if I need a card reader?**
   If your system doesn't have a built-in card reader, you will need an external card reader and associated software. Please submit an IT Support Ticket requesting assistance: NIH Help Desk or call 866-319-4357.
3. **What if I don't know my PIN/forgot my PIN?**
   If you've forgotten the PIN you set when you received your HHS ID badge, you will need to reset it. Your PIN can be reset by simply bringing your ID badge to the NIEHS Security office (located in Building 101, Room B-114A) between the hours of 8:15 a.m. – 3:45 p.m. on normal workdays. Though resetting your PIN takes less than ten minutes, if you are under tight time constraints it is recommended that you call the Security office at 984-287-4500 to verify one of the issuers is available: listing of all Badge Issuance Stations.
4. **How Do I Renew my Smart Card Digital Certificates?**
   You will receive an email notification from the HHS six weeks before the digital certificates embedded in your smart card expire. If your digital certificates expire, you will not be able to use your smart card until you renew your certificates.

   You can renew your certificates right from your desktop using the 'Access Card Utility' (ACU) 42 days prior to expiration through the actual expiration date (noted in email alerts you'll receive from HHS when it's time to renew). This tool should already be installed on your computer and is listed on the 'Start' menu under 'All Programs."

   If your certificates have expired, visit the NIEHS Security Office and a Security Issuance Official will renew the digital certificates loaded in your smart card. The NIEHS Security Office is located in Building 101 (Rall Building), Room B114A. Please schedule an appointment during the hours of 8:00 a.m. – 4:00 p.m. by contacting the Security Office at 984-287-4500 or fac-security@niehs.nih.gov. The appointment will take 20 minutes. Remember to bring your badge with you!