

Overview

If you are away from a DCRI facility and you need to access DCRI/Duke network resources, the recommended remote access option with a PC (desktop or laptop) is **AnyConnect** from Cisco Systems, a Desktop application in the DCRIconnect family. This quick reference card (QRC) summarizes basic AnyConnect operations on Windows 7, 8, 8.1, or 10.

This document assumes you have installed the application according to the instructions in the *Cisco AnyConnect: Installing on a Home Windows Computer* QRC.

About Cisco AnyConnect

With this Virtual Private Network (VPN) application, you can use your own personal Windows computer to access remotely:

- Resources on the DCRI Intranet and protected web applications and websites, such as the Duke LMS (Learning Management System) and secure SharePoint sites.
- (if applicable) A Virtual Machine (VM) or a DCRI-issued Windows computer running at your desk at a DCRI facility.

Requirements

To access this service, you must have:

- Windows 7, 8, 8.1, or 10.
- A high-speed Internet connection (wired or wireless).
- A valid NetID and working password.
- Multi-Factor Authentication (MFA) enabled. For more information, see <http://library.dcri.duke.edu/dtmi/IT/Remote/Q/MFA.pdf>.

Logging On

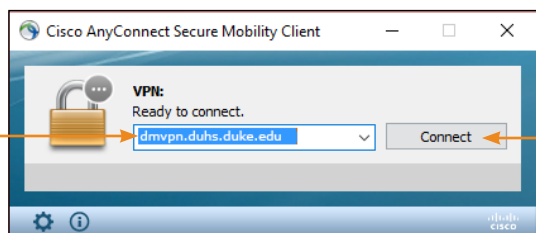
- 1 Launch the **Cisco AnyConnect Secure Mobility Client** application.

Using the Windows' search or Cortana, just entering the word **any** generally finds the application.



Tip: If you will be using this application often, consider pinning it to the Start menu or the Taskbar.

The Cisco AnyConnect Secure Mobility Client connect dialog appears.

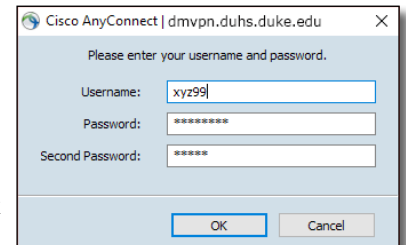


- 2 Ensure the address in the combo box is: **dmvpn.duhs.duke.edu**

Note: This address is different from the one provided by the installer.

- 3 Click **Connect**.

Wait for the log on dialog to appear.



- 4 In **Username**, enter your Duke NetID, and then enter your network **Password**.

- 5 In the **Second Password** field (sometimes seen as **Security Key**), enter your Multi-Factor Authentication (MFA):



Enter into this field a **Duo Mobile** app code (by tapping the app's key icon), YubiKey code, or an unused SMS (Short Message Service) code. Otherwise, you are expected to enter one of the following *words*:

- Enter **phone** to have the system call the top phone you listed on the Duke Office of Information Technology (OIT) MFA website. You can enter **phone2** or **phone3** to have the system call the second or third phone on your list.
- Enter **push** to have the system push notification to the Duo Mobile app on the top smartphone or tablet you listed in the OIT website. You can enter **push2** or **push3** to send to the second or third device on your list.
- Enter **sms** to have the system text you a batch of passcodes. Enter one of them into this field to authenticate this session.

- 6 Click **OK**.

After you complete your MFA verification, the application securely logs you on to the DCRI/Duke network. When done, the following banner appears in the lower right area of the computer screen for a few seconds, and then fades away.



This application works “behind the scenes”—there are no application-specific screens or other controls to “operate” this VPN application.

Accessing DCRI Intranet and Secure SharePoint Sites

You can use your choice of browser to reach resources on the DCRI Intranet and secure SharePoint sites (Team, Collaboration, and TMF [Trial Master File] site collections).

Here are a few commonly visited addresses on the DCRI Intranet.

DCRI Intranet Home Page	https://dcrihome.dcri.org
Duke LMS (Learning Management System)	https://lms.duhs.duke.edu/Saba/Web/Cloud
Duke@Work Portal	hr.duke.edu/selfservice
EPM Time Card	timecard.dcri.duke.edu (if a Certificate warning appears, you can click Continue to this website)

Accessing a VM or the Desktop of a DCRI-issued Windows Computer at Work

If you have access to a Windows Virtual Machine (VM) or have a DCRI-issued Windows computer (desktop or laptop) currently running at your desk in a DCRI facility, you can use AnyConnect to access the VM or the Desktop of your Windows computer from any remote location.

For this feature to work, the following must be in place.

- To access a VM, you must have its address available to complete Step 2.
- To access a DCRI-issued Windows computer, you must have:
 - The DCRI computer's name (the number that begins with "DCRI-" on the asset tag) available to complete Step 2.
 - The DCRI computer powered *on* and connected to the wired network, with you logged *off*. External monitors, if used, can be powered *off*.

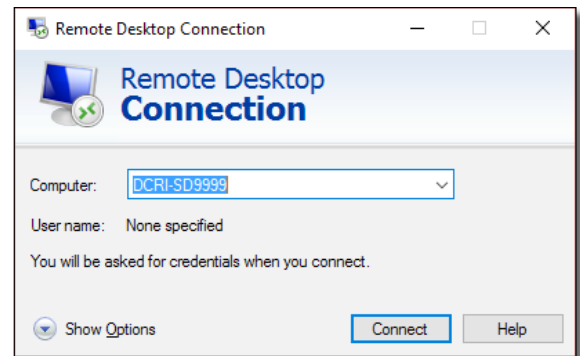
- Find and launch **Remote Desktop Connection** (mstsc.exe).

Using the Windows' search or Cortana, just entering the word **remote** generally finds the application.



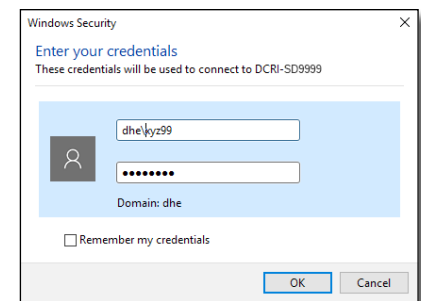
Tip: If you will be using this application often, consider pinning it to the Start menu or the Taskbar.

The initial dialog appears.



- In the **Computer** field, enter the VM address or DCRI Computer name.

- Click **Connect**. The Enter your Credentials dialog appears.



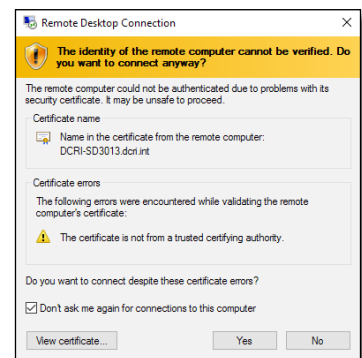
- In the top box, enter **dhe**, followed by your Duke NetID (example: dhe\xyz99).

- In the bottom box, enter your network password, and then click **OK**.

Note: For security, do **not** select *Remember my credentials*. A bar shows the progress of connecting.

- If the Remote Desktop Connection certificate message appears, complete the following.

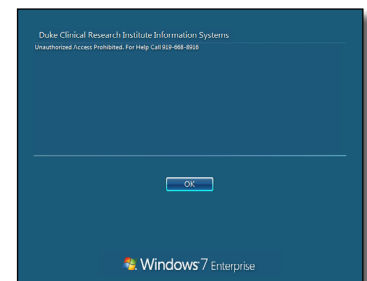
- (optional) You can select the **Don't ask me again for connections to this computer** checkbox near the bottom.



- Click **Yes**.

- When the blue DCRI Information Systems screen appears, click the **OK** button near the center.


A full-screen version of your Windows Desktop on your work computer appears.




At the top of the window is a blue toolbar.



Use your local keyboard and mouse as if you were seated in front of your computer at work, including browsing to folders on network drives (that you have permission to access).

- 8 To reduce the page size (so you can cut and paste files to or from your local computer), click  on the blue toolbar.

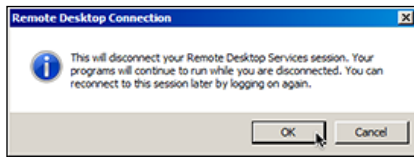
Note: To return to full screen, double-click anywhere in the window's title bar (across the top).

- 9 To minimize, click  on the blue toolbar. The window minimizes while the icon on the right appears in the Taskbar. Click this icon to maximize the window.



▶ Ending the Session and Logging Out



- 1 To end the session, click  on the blue toolbar. A confirmation message appears.



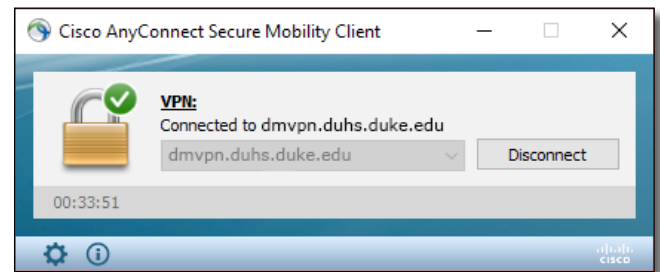
- 2 Click **OK**. Both the window to the remote computer and the Remote Desktop Connection application close.

Ending Your AnyConnect Session

Whenever you are not actively using Cisco AnyConnect, please **end your session** to free up network resources for the benefit of other users.

- 1 Do either of the following.
 - If you have the application pinned to your Taskbar, click the app's icon.
 - In the System Tray, click the AnyConnect icon (if not seen, click the triangle  to view hidden icons). 

The main Cisco AnyConnect Secure Mobility Client dialog appears.



- 2 Click **Disconnect**. After the dialog shows the app is *Ready to connect*, you can close this window.

Getting Help

If you have questions or comments about the content of this QRC, please email [IT Training \[dcrittrain@dm.duke.edu\]](mailto:dcrittrain@dm.duke.edu). If you experience any technical problems working with Cisco AnyConnect that you are unable to resolve, email the [DCRI Service Desk \[dcriservicedesk@dm.duke.edu\]](mailto:dcriservicedesk@dm.duke.edu) or, for time-sensitive issues, call them Monday through Friday (6 a.m. to midnight, Eastern time, except holidays) at 919.668.8916.