How do I configure remote access on my computer?

How do I configure remote access on my computer?

On this page:

Overview
Prerequisites for all platforms
Security requirements for all platforms (client and remote server)
Additional security requirements for remote server you are connecting to
Connect Remotely From a Windows Workstation
Connect Remotely from MacOS
    Microsoft Remote Desktop for MacOS - Access a Windows Machine from MacOS
    Apple Remote Desktop - Access a MacOS Machine from a MacOS Machine
Linux:
Troubleshooting
See Also
Have Questions or Still Need Help?

Overview

When working remotely, you may find it necessary to connect to a Desktop Computer on MIT campus from a remote computer (i.e. home computer). There are many ways to do this. The following options are provided for informational purposes. Some of the software mentioned is not licensed by MIT and may require purchasing.

If you don't normally do or are not comfortable doing administrative tasks, contact your local IT support provider or the IS&T Service Desk for assistance.

Prerequisites for all platforms

- The computer that will be accessed remotely must have a permanent reserved IP address. You can request one from IS&T.
- You need to know the hostname of the machine that will be accessed remotely.
- You need to connect your remote (home) machine to MITnet via the VPN. Without this connection, you will be unable to remotely access machines on MITnet.

Security requirements for all platforms (client and remote server)

- The computer you are connecting from, as well the the system you are connecting to, must be running a currently supported operating system that is up to date on patches. Older implementations of RDP have known vulnerabilities, such as BlueKeep, allowing them to be remotely taken over and fully controlled. Windows 7 and older are no longer supported and should not be used for remote access.
- Systems should have modern and updated anti-malware protection. Sophos and Crowdstrike are available free of charge to the MIT community.
- At a minimum, systems should implement all of the infoprotect.mit.edu tasks for Low Risk.

Additional security requirements for remote server you are connecting to

- A target Windows system should be configured to use Network Level Authentication (default in modern versions of Windows)
- The users allowed to connect to the system should be restricted to only those who need it
- An account lockout policy should be turned on, to temporarily restrict logins after a number of failed attempts, in order to stop brute force password guessing
- Accounts should have passwords that are strong and unique
- The host firewall should restrict RDP (UDP port 3389) or SSH (TCP port 22) to only hosts from MIT to prevent attacks from the outside. Ideally, only MIT VPN addresses should be allowed, currently 18.28.0.0/16 and 18.30.0.0/16.

Connect Remotely From a Windows Workstation

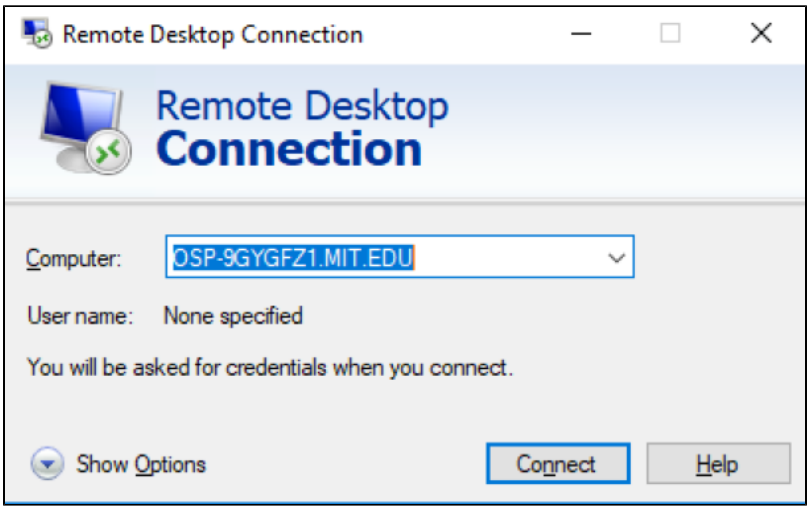
Microsoft Remote Desktop - Access a Windows Machine from a Windows Machine

Anyone who is not an Administrator will need to be added to the Remote Desktop Users group on the windows machine.

- Acquire: Usually included with the operating system. If needed, download: Microsoft Remote Desktop
  - Windows 10: How to Use Remote Desktop
  - Windows 7/8: Connect to another computer using Remote Desktop Connection

Connecting:

1. Connect to the MIT VPN (Prisma Access VPN Landing Page)
2. Search your computer for “Remote Desktop Connection.”
3. Enter the hostname of the computer on MITnet you wish to connect to.



4. Press **Connect**. If you receive additional prompts please select Allow or OK to continue.
5. When prompted you will login to your work computer using the same credentials you would if you were using this computer in person. Most of the time this means your Kerberos credentials, though though there may be certain local credentials to the machine as well.
6. When finished remoting, disconnect/log off your work computer and disconnect from the VPN.

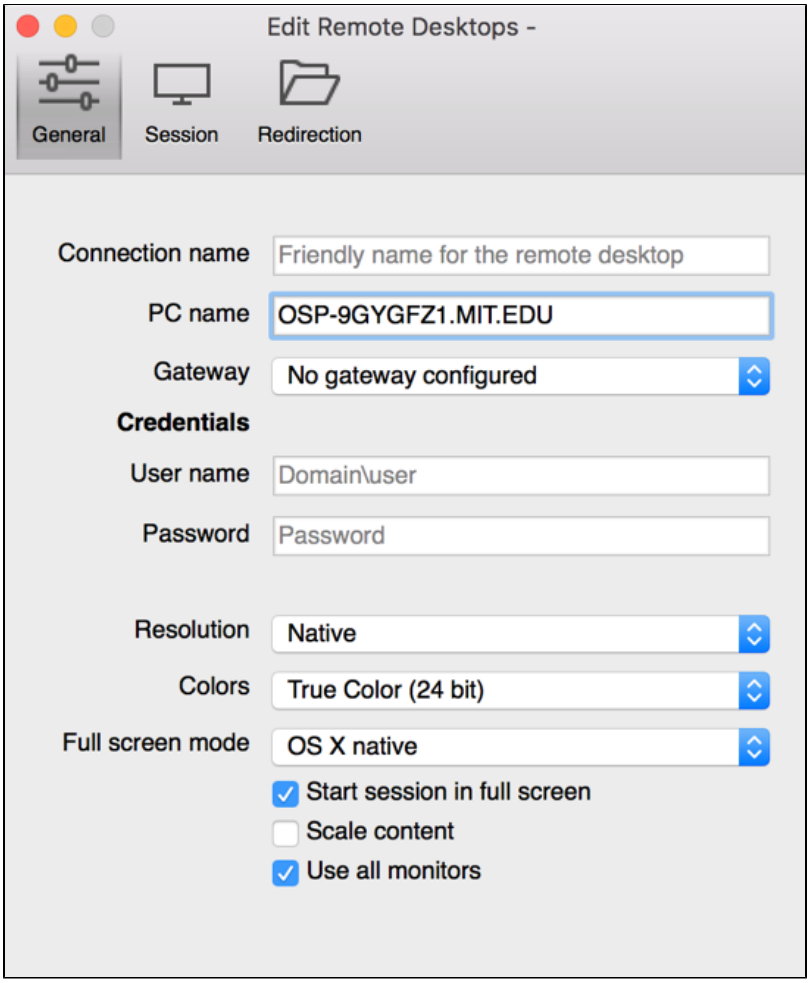
Connect Remotely from MacOS

Microsoft Remote Desktop for MacOS - Access a Windows Machine from MacOS

- Acquire: Microsoft Remote Desktop In the App Store
- Getting Started with the MacOS Client
- Allow a Remote Computer to Access your Mac

Connecting:

1. Connect to the VPN
2. Launch Microsoft Remote Desktop.
3. **Click** the **New** Button Upper Left
4. Enter in the hostname of the machine on MITnet you want to connect to in the PC Name line.



5. **Click** on the **red dot** in the upper-left to close the window.
6. **Double Click** the newly created ***Hostname*** in the list to connect to your work computer. If you receive additional prompts please select **Allow** or **OK** to continue.
7. When prompted you will login to your work computer using the same credentials you would if you were using this computer in person. Most of the time this means your Kerberos credentials, though though there may be certain local credentials to the machine as well.
8. When finished remoting, disconnect/log off your work computer and disconnect from the VPN.

Apple Remote Desktop - Access a MacOS Machine from a MacOS Machine

1. Users without the need for Remote Management tools can use Screen Sharing
    - Connect to MIT's network through a VPN
    - How to use Screen Sharing
2. System Administrators may want to use Apple Remote Desktop
    - Acquire: Apple Remote Desktop in the App Store
    - Apple Remote Desktop Documentation
    - Allow Apple Remote Desktop to Access your Mac
    - Install and Setup Apple Remote Desktop Client

Linux:

1. Setup the Linux machine to allow remote access:
    - Ubuntu: How to enable SSH on Ubuntu
    - DebAthena: http://kb.mit.edu/confluence/x/eSVB and https://kb.mit.edu/confluence/pages/viewpage.action?pageId=4269212
2. Use a client application to access the machine:
    - Secure CRT Windows
    - SSH on MacOS
    - SSH Command - Usage, Options, Configuration on Linux and in the MacOS Terminal

Troubleshooting

- If you’re not sure how to find out your hostname or if your computer has a permanent reserved IP address, contact the IS&T Service Desk.
- Make sure your firewall settings aren’t preventing remote connections.
- Make sure you’ve started the VPN before trying to connect.

See Also

- How can I connect to the Athena dialup servers?
- Prisma Access VPN Landing Page

Have Questions or Still Need Help?

- Send email to helpdesk@mit.edu or call the IS&T Service Desk at 617.253.1101.