Remote Desktop (RDC)

Through the Brandeis VPN, faculty and staff members can remotely connect to their campus computer (referred to as the target computer going forward) from other locations (either somewhere else on-campus or off-campus entirely). There are some preliminary steps which must be performed on your target computer first to enable this, and they vary by operating system.

Before you begin

1. The target computer needs to have a static IP.
   a. The following link has more details about static IP addresses
2. Connect the non-target (usually off-campus) computer to the VPN with Pulse Secure even if both computers are on campus.
   a. See instructions on this page: Using the Brandeis VPN

Setting up a Connection

There’s a different process for RDC depending on what operating systems are involved.

- **Windows -> Windows**
  1. Set up the target Windows computer with these instructions: For Windows 10, For Windows 7, For Windows XP
  2. Use Windows RDC to establish the remote connection. Instructions can be found on this page: RDC: PC to PC
- **Mac -> Windows**
  1. Set up the target Windows computer with these instructions: For Windows 10, For Windows 7, For Windows XP
  2. Use Microsoft Remote Desktop to establish the remote connection. See instructions on this page: RDC: Mac to PC
- **Mac -> Mac**
  1. Use MacOS Screen Sharing. Instructions can be found on this page: Screen Sharing in OS X

Important Notes on Wormhole and Security

If you’ve configured your target and other computers as detailed above and are unable to connect, ensure that you’re running the latest version of Java.

Using the Brandeis VPN service subjects the user to the same restrictions and responsibilities as a campus user. Connections via VPN are considered direct connections to the campus network. All connection attempts are logged.

VPN users will be automatically disconnected from the Brandeis network after a predetermined amount of inactivity. The user can immediately login again to reconnect to the Brandeis network - no work will have been lost.

Additionally, please be mindful of where you use the VPN to connect to your desktop. All computers connected to Brandeis internal networks via VPN must use the most up-to-date anti-virus software; this includes personal computers. Malicious software can log your keystrokes and steal your password. Do not use the VPN in cyber cafes, public clusters or from any computer that you do not completely trust.

Related articles

- Network Shares
- Pulse Secure
- VPN (Wormhole)
- Remote Access Best Practices
- Set Up RDC for Windows XP