Securing Remote Desktop (RDP) for System Administrators

How secure is Windows Remote Desktop?

Remote Desktop sessions operate over an encrypted channel, preventing anyone from viewing your session by listening on the network. However, there is a vulnerability in the method used to encrypt sessions in earlier versions of RDP. This vulnerability can allow unauthorized access to your session using a man-in-the-middle attack.

Remote Desktop can be secured using SSL/TLS in Windows Vista, Windows 7, Windows 8, Windows 10 and Windows Server 2003/2008/2012/2016. ***Some systems listed are no longer supported by Microsoft and therefore do not meet Campus security standards. If unsupported systems are still in use, a security exception is required.**

While Remote Desktop is more secure than remote administration tools such as VNC that do not encrypt the entire session, any time Administrator access to a system is granted remotely there are risks. The following tips will help to secure Remote Desktop access to both desktops and servers that you support.

Basic Security Tips for Remote Desktop

Use strong passwords

Strong passwords on any accounts with access to Remote Desktop should be considered a required step before enabling Remote Desktop. Refer to the campus password complexity guidelines for tips.

Use Two-factor authentication

Departments should consider using a two-factor authentication approach. This topic is beyond the scope of this article, but RD Gateways can be configured to integrate with the Campus instance of DUO. Other unsupported by campus options available would be a simple mechanism for controlling authentication via two-factor certificate based smartcards. This approach utilizes the Remote Desktop host itself, in conjunction with YubiKey and RSA as examples.

Update your software

One advantage of using Remote Desktop rather than 3rd party remote admin tools is that components are updated automatically with the latest security fixes in the standard Microsoft patch cycle. Make sure you are running the latest versions of both the client and server software by enabling and auditing automatic Microsoft Updates. If you are using Remote Desktop clients on other platforms, make sure they are still supported and that you have the latest versions. Older versions may not support high encryption and may have other security flaws.

Restrict access using firewalls

Use firewalls (both software and hardware where available) to restrict access to remote desktop listening ports (default is TCP 3389). Using an RDP Gateway is highly recommended for restricting RDP access to desktops and servers (see discussion below). As an alternative to support off-campus connectivity, you can use the campus VPN software to get a campus IP address and add the campus VPN network address pool to your RDP firewall exception rule. Visit our page for more information on the campus VPN service.

Enable Network Level Authentication

Windows 10, Windows Server 2012 R2/2016/2019 also provide Network Level Authentication (NLA) by default. It is best to leave this in place, as NLA provides an extra level of authentication before a connection is established. You should only configure Remote Desktop servers to allow connections without NLA if you use Remote Desktop clients on other platforms that don't support it.

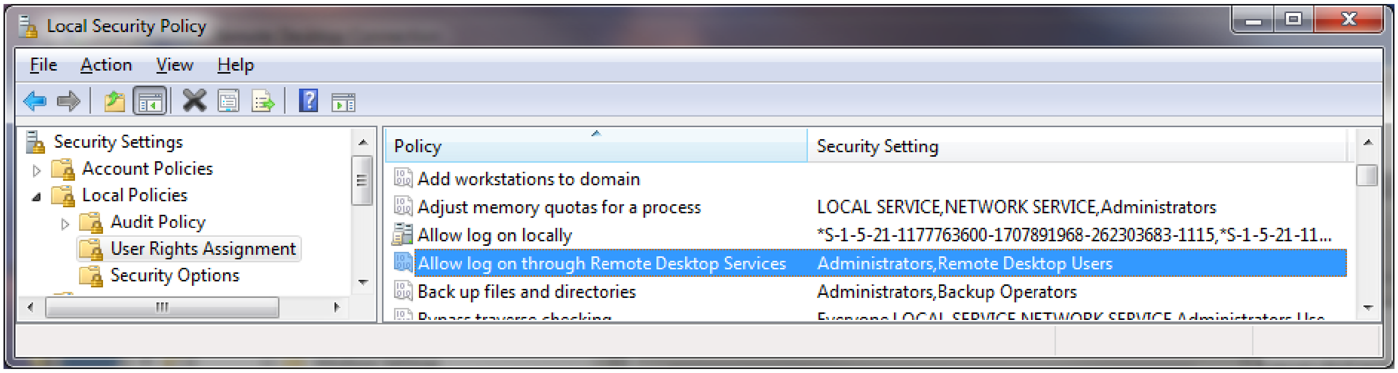
- NLA should be enabled by default onWindows 10, Windows Server 2012 R2/2016/2019.
- To check you may look at Group Policy setting Require user authentication for remote connections by using Network Level Authentication found at Computer\Policies\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security. This Group Policy setting must be enabled on the server running the Remote Desktop Session Host role.
- https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/remote-desktop-allow-access

Limit users who can log in using Remote Desktop

By default, all Administrators can log in to Remote Desktop. If you have multiple Administrator accounts on your computer, you should limit remote access only to those accounts that need it. If Remote Desktop is not used for system administration, remove all administrative access via RDP, and only allow user accounts requiring RDP service. For Departments that manage many machines remotely remove the local Administrator account from RDP access at and add a technical group instead.

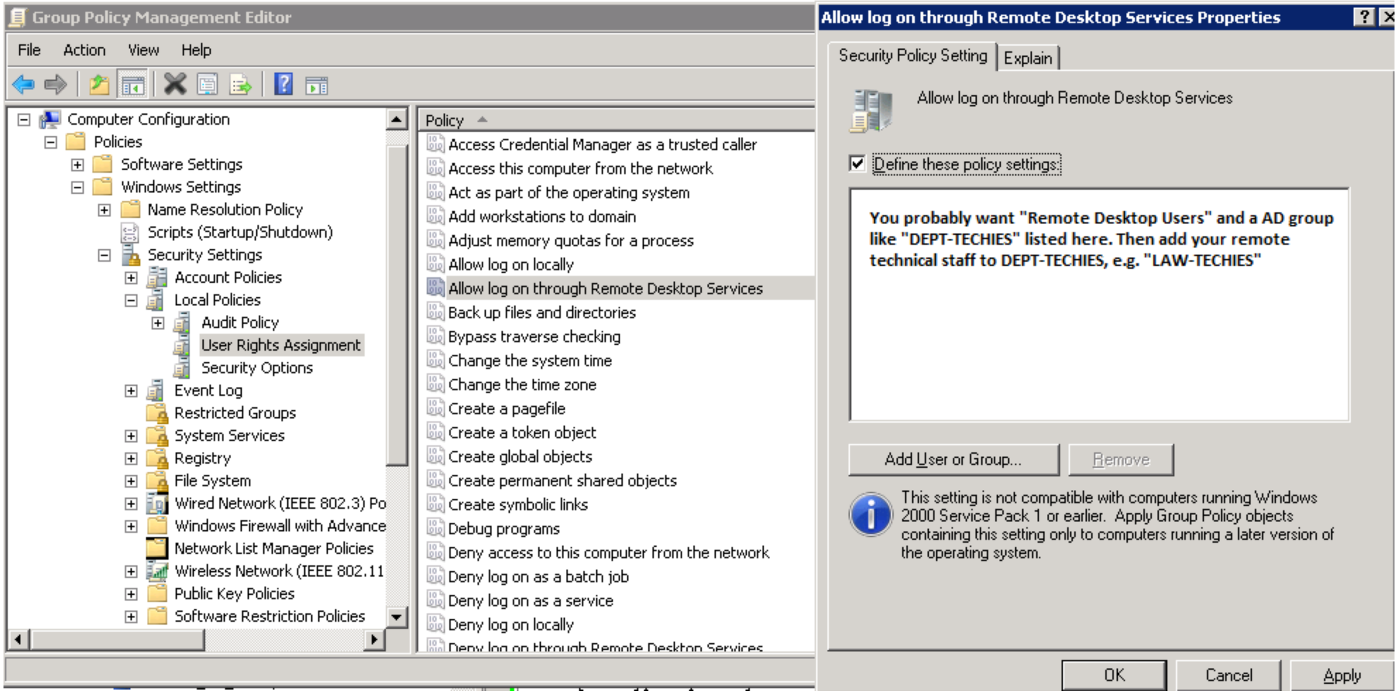
1. Click Start-->Programs-->Administrative Tools-->Local Security Policy
2. Under Local Policies-->User Rights Assignment, go to "Allow logon through Terminal Services." Or “Allow logon through Remote Desktop Services”
3. Remove the Administrators group and leave the Remote Desktop Users group.
4. Use the System control panel to add users to the Remote Desktop Users group.

A typical MS operating system will have the following setting by default as seen in the Local Security Policy:



Policy	Security Setting
Add workstations to domain	
Adjust memory quotas for a process	LOCAL SERVICE,NETWORK SERVICE,Administrators
Allow log on locally	*S-1-5-21-1177763600-1707891968-262303683-1115,*S-1-5-21-11...
Allow log on through Remote Desktop Services	Administrators,Remote Desktop Users
Back up files and directories	Administrators,Backup Operators
Bypass traverse checking	Everyone,LOCAL SERVICE,NETWORK SERVICE,Administrators,Use

The problem is that “Administrators” is here by default, and your “Local Admin” account is in administrators. Although a password convention to avoid identical local admin passwords on the local machine and tightly controlling access to these passwords or conventions is recommended, using a local admin account to work on a machine remotely does not properly log and identify the user using the system. It is best to override the local security policy with a Group Policy Setting.


Group Policy Management Editor
File Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Po
Windows Firewall with Advance
Network List Manager Policies
Wireless Network (IEEE 802.11
Public Key Policies
Software Restriction Policies
Policy
Access Credential Manager as a trusted caller
Access this computer from the network
Act as part of the operating system
Add workstations to domain
Adjust memory quotas for a process
Allow log on locally
Allow log on through Remote Desktop Services
Back up files and directories
Bypass traverse checking
Change the system time
Change the time zone
Create a pagefile
Create a token object
Create global objects
Create permanent shared objects
Create symbolic links
Debug programs
Deny access to this computer from the network
Deny log on as a batch job
Deny log on as a service
Deny log on locally
Deny log on through Remote Desktop Services
Allow log on through Remote Desktop Services Properties
Security Policy Setting
Explain
Allow log on through Remote Desktop Services
Add User or Group...
Remove
OK
Cancel
Apply

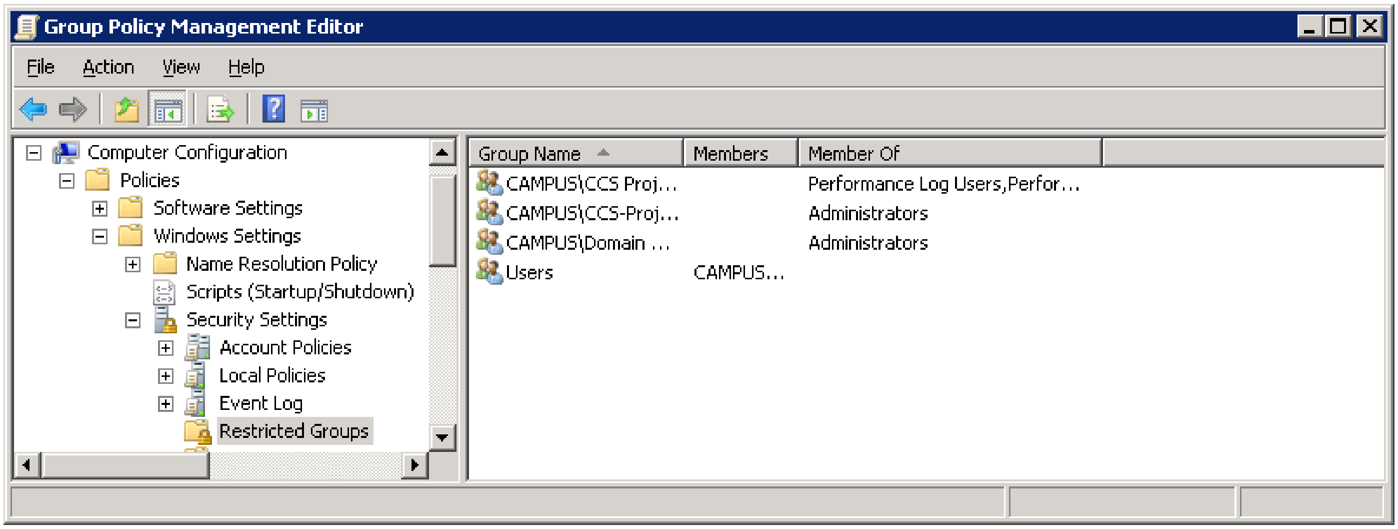
☑ Define these policy settings:

You probably want "Remote Desktop Users" and a AD group like "DEPT-TECHIES" listed here. Then add your remote technical staff to DEPT-TECHIES, e.g. "LAW-TECHIES"

This setting is not compatible with computers running Windows 2000 Service Pack 1 or earlier. Apply Group Policy objects containing this setting only to computers running a later version of the operating system.

To control access to the systems, even more, using “Restricted Groups” via Group Policy is also helpful.

If you use a “Restricted Group” setting to place your group, e.g., “CAMPUS\LAW-TECHIES” into “Administrators” and “Remote Desktop Users,” your techies will still have administrative access remotely, but using the steps above, you have removed the problematic “local administrator account” having RDP access. Going forward, whenever new machines are added in the OU under the GPO, your settings will be correct.



Group Name	Members	Member Of
CAMPUS\CCS Proj...		Performance Log Users,Perfor...
CAMPUS\CCS-Proj...		Administrators
CAMPUS\Domain ...		Administrators
Users	CAMPUS...	

Set an account lockout policy

By setting your computer to lock an account for a set number of incorrect guesses, you will help prevent hackers from using automated password guessing tools from gaining access to your system (this is known as a "brute-force" attack). To set an account lockout policy:

1. Go to Start-->Programs--> Administrative Tools--> Local Security Policy
2. Under Account Policies--> Account Lockout Policies, set values for all three options. Three invalid attempts with 3-minute lockout durations are reasonable choices.

Best Practices for Additional Security

Do not allow direct RDP access to clients or servers from off campus.

Having RDP(3389) open to off campus networks is highly discouraged and is a known vector for many attacks. The options below list ways of improving security while still allowing RDP access to system.

Once an RDP gateway has been set up, hosts should be configured to only allow RDP connections from the Gateway host or campus subnets where needed.

Use RDP Gateways (Best Option)

Using an RDP Gateway is strongly recommended. It provides a way to tightly restrict access to Remote Desktop ports while supporting remote connections through a single "Gateway" server. When using an RD Gateway server, all Remote Desktop services on your desktop and workstations should be restricted to only allow access only from the RD Gateway. The RD Gateway server listens for Remote Desktop requests over HTTPS (port 443) and connects the client to the Remote Desktop service on the target machine.

1. Utilize Campus Gateway Service. Best option to allow RDP access to system categorized as UC P2 (formerly UCB PL1) and lower. Includes DUO integration.
2. Dedicated Gateway Service (Managed). Needed for rdp access to systems that are UC P4 (formerly UCB PL2) or higher. Must also be configured for DUO

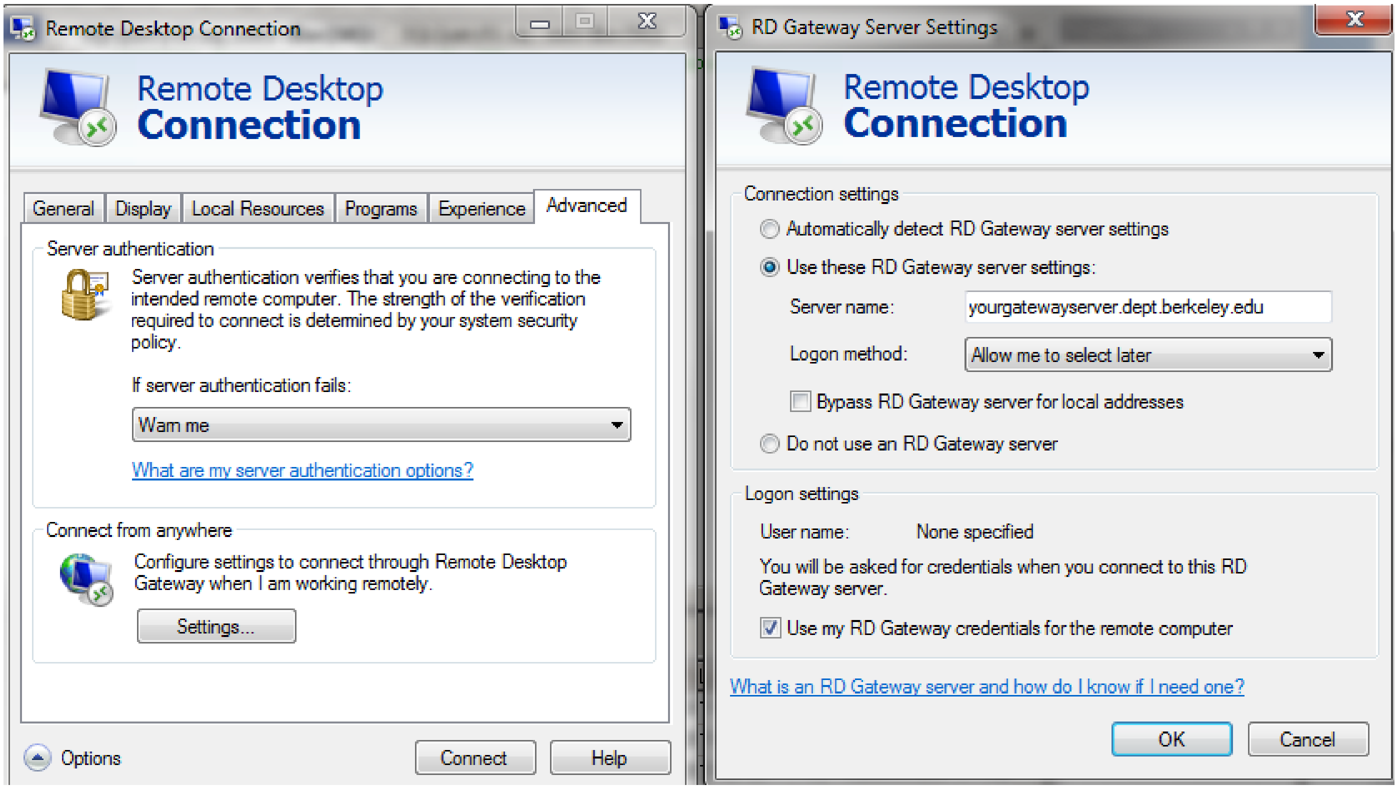
   Some campus units use an IST managed VPS as an RD Gateway. A rough estimate might be that 30-100 concurrent users can use one RD Gateway. The HA at the virtual layer provides enough fault-tolerant and reliable access; however a slightly more sophisticated RD gateway implementation can be done with network load balancing.
3. Dedicated Gateway Service (Unmanaged). Installing and configuring RD Gateway on department run hardware.

   There are many online documents for configuring this embedded Windows 2016/2019 component. The official documentation is here: https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-se...

   Installing the configuring, the role service is mostly as described; however, using a Calnet issued trusted Comodo certificate is recommended. Using a self-signed cert is ok for testing, and using a CalnetPKI cert can work if all clients have trusted the UCB root. The Comodo cert is usually better accepted so that your end users do not receive certificate warnings.

   Configuring your client to use your RD Gateway is simple.The official documentation for the MS Client is here: http://technet.microsoft.com/en-us/library/cc770601.aspx

In essence, a simple change on the advanced tab of your RDP client is all that is necessary:


Remote Desktop Connection
Remote Desktop Connection
General
Display
Local Resources
Programs
Experience
Advanced
Settings...
Options
Connect
Help
RD Gateway Server Settings
Remote Desktop Connection
OK
Cancel

Server authentication

Server authentication verifies that you are connecting to the intended remote computer. The strength of the verification required to connect is determined by your system security policy.

If server authentication fails: Warn me

What are my server authentication options?

Connect from anywhere

Configure settings to connect through Remote Desktop Gateway when I am working remotely.

Connection settings

○ Automatically detect RD Gateway server settings

● Use these RD Gateway server settings:

Server name: yourgatewayserver.dept.berkeley.edu

Logon method: Allow me to select later

□ Bypass RD Gateway server for local addresses

○ Do not use an RD Gateway server

Logon settings

User name: None specified

You will be asked for credentials when you connect to this RD Gateway server.

☑ Use my RD Gateway credentials for the remote computer

What is an RD Gateway server and how do I know if I need one?

Change the listening port for Remote Desktop

Changing the listening port will help to "hide" Remote Desktop from hackers who are scanning the network for computers listening on the default Remote Desktop port (TCP 3389). This offers effective protection against the latest RDP worms such, as Morto. To do this, edit the following registry key (WARNING: do not try this unless you are familiar with the Windows Registry and TCP/IP): HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp. Change the listening port from 3389 to something else and remember to update any firewall rules with the new port. Although this approach is helpful, it is security by obscurity, which is not the most reliable security approach. You should ensure that you are also using other methods to tighten down access as described in this article.

Tunnel Remote Desktop connections through IPSec or SSH

If using an RD Gateway is not feasible, you can add an extra layer of authentication and encryption by tunneling your Remote Desktop sessions through IPSec or SSH. IPSec is built-in to all Windows operating systems since Windows 2000, but use and management are greatly improved in Windows 10 (see: http://technet.microsoft.com/en-us/network/bb531150). If an SSH server is available, you can use SSH tunneling for Remote Desktop connections.

Use existing management tools for RDP logging and configuration

Using other components like VNC or PCAnywhere is not recommended because they may not log in a fashion that is auditable or protected. With RDP, logins are audited to the local security log, and often to the domain controller auditing system. When monitoring local security logs, look for anomalies in RDP sessions such as login attempts from the local Administrator account. RDP also has the benefit of a central management approach via GPO as described above. Whenever possible, use GPOs or other Windows configuration management tools to ensure a consistent and secure RDP configuration across all your servers and desktops.

By enforcing the use of an RDP gateway, you also get a third level of auditing that is easier to read than combing through the domain controller logins and is separate from the target machine so it is not subject to tampering. This type of log can make it much easier to monitor how and when RDP is being used across all the devices in your environment.