Remote Administration

Windows Remote Desktop

Remote Desktop permits users to remotely run applications on Windows Server from a range of devices over virtually any network connection. You can run Remote Desktop in either Application Server or Remote Administration modes. Unified ICM/ Unified CCE only supports Remote Administration mode.

Note

- Use of any remote administration applications can cause adverse effects during load.
- Use of remote administration tools that employ encryption can affect server performance. The performance level impact is tied to the level of encryption used. More encryption results in more impact to the server performance.

Remote Desktop can be used for remote administration of ICM-CCE-CCH server. The mstsc command connects to the local console session.

Using the Remote Desktop Console session, you can:

- Run Configuration Tools
- Run Script Editor

Note Remote Desktop is not supported for software installation or upgrade.

Note Administration Clients and Administration Workstations can support remote desktop access. But, only one user can access a client or workstation at a time. Unified CCE does not support simultaneous access by several users on the same client or workstation.

Remote Desktop Protocol

Communication between the server and the client uses original Remote Desktop Protocol (RDP) encryption. By default, encryption based on the maximum key strength supported by the client protects all data.

RDP is the preferred remote control protocol due to its security and low impact on performance.

Windows Server Terminal Services enable you to shadow a console session. Terminal Services can replace the need for pcAnywhere or VNC. To launch from the Windows Command Prompt, enter:

Remote Desktop Connection: `mstsc /v:<server[:port]>`

RDP-TCP Connection Security

To protect your RDP-TCP connection, use the Microsoft Remote Desktop Services Manager to set the connection properties appropriately:

- Limit the number of active client sessions to one.
- End disconnected sessions in five minutes or less.
- Limit the time that a session can remain active to one or two days.
- Limit the time that a session can remain idle to 30 minutes.
- Select appropriate permissions for users and groups. Give Full Control only to administrators and the system. Give User Access to ordinary users. Give Guest Access to all restricted users.
- Consider restricting reconnections of a disconnected session to the client computer from which the user originally connected.
- Consider enabling Network Level Authentication (NLA) on the RDP server using one of the following ways:
    - On your remote server, navigate to **Settings > Remote Desktop Settings** and select the **Require devices to use Network Level Authentication to connect (Recommended)** checkbox.
    - In the Group Policy editor, navigate to **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Security** and enable the **Require user authentication for remote connections by using Network Level Authentication** policy.
- Consider setting high encryption levels to protect against unauthorized monitoring of the communications. In the Group Policy Editor, navigate to **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Security**. Click the **Set client connection encryption level** policy, select the **Enabled** option, and then set **Encryption Level** to **High Level**.

Note To prevent man-in-the-middle attacks against your remote Server Message Block (SMB) server, we recommend that you enforce message signing in the host configuration. To do so, set the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature** registry key value to **1**. Alternatively, in the Group Policy Editor, navigate to **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options** and enable the following policies:

- Microsoft network client: Digitally sign communications (always)
- Microsoft network client: Digitally sign communications (if server agrees)
- Microsoft network server: Digitally sign communications (always)
- Microsoft network server: Digitally sign communications (if client agrees)

Per-User Terminal Services Settings

Use the following procedure to set up per-user terminal services settings for each user.

Procedure

Step 1 Using Active Directory Users and Computers, right-click a user and then select **Properties**.

Step 2 On the Terminal Services Profile tab, set a user's right to sign in to terminal server by checking the **Allow logon to terminal server** check box. Optionally, create a profile and set a path to a terminal services home directory.

Step 3 On the Sessions tab, set session active and idle time outs.

Step 4 On the Remote Control tab, set whether administrators can remotely view and control a remote session and whether a user's permission is required.

VNC

SSH Server allows the use of VNC through an encrypted tunnel to create secure remote control sessions. However, Cisco does not support this configuration. The performance impact of running an SSH server has not been determined.