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.

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.

pcAnywhere

Security is one of the most important considerations in implementing a remote control solution.

pcAnywhere addresses security in the following ways:

1. Restricting access to internal machines.
2. Preventing unauthorized connections to a pcAnywhere host.
3. Protecting the data stream during a remote control session.
4. Preventing unauthorized changes to the installed product.
5. Identifying security risks.
6. Logging events during a remote control session.

For more information about pcAnywhere, see the Symantec web site.

Note This discussion applies to all approved versions of pcAnywhere. Refer to the Compatibility Matrix for the versions qualified and approved for your release of ICM.

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.

Restricted Access to Internal Machines

An important security technique is to restrict connections from outside your organization. pcAnywhere provides these ways to accomplish that objective:

- **Limiting connections to a specific TCP/IP address range**—pcAnywhere hosts can be configured to only accept TCP/IP connections that fall within a specified range of addresses.
- **Serialization**—A feature that enables the embedding of a security code into the pcAnywhere host and created remote objects. This security code must be present on both ends to make a connection.

Unauthorized Connections to pcAnywhere Host

The first line of defense in creating a secure remote computing environment is to prevent unauthorized users from connecting to the host. pcAnywhere provides several security features to help you achieve this objective.

Feature	Description
Authentication	Authentication is the process of taking a user's credentials and verifying them against a directory or access list to determine if the user is authorized to connect to the system.
Mandatory passwords	pcAnywhere now requires a password for all host sessions. This security feature prevents users from inadvertently launching an unprotected host session.
Callback security (for dial-up connections)	pcAnywhere lets dial-up users specify a call-back number for remote control sessions. In a pcAnywhere session, the remote connects to the host, and the session begins. When callback is enabled, the remote calls the host, but then the host drops the connection and calls back the remote at the specified phone number.

Table 1: General pcAnywhere Security Settings

Settings	Default	Change to	Description
Restrict connections after an end of session	no	(optional)	With pcAnywhere, host users can prevent remote users from reconnecting to the host if the session is stopped suddenly.

Settings	Default	Change to	Description
Wait for anyone	Yes	Yes	
and secure by	no	Yes (lock computer)	

Table 2: Security Options - Connection Options

Settings	Default	Change to	Description
Prompt to confirm connection	no	(optional)	This feature prompts the host user to acknowledge the remote caller and permit or reject the connection. By enabling this feature, users know when someone is connecting to their host computer. This feature depends on the remote administration policy of whether users must be physically present at the remotely accessed server.

Table 3: Security Options - Login Options

Settings	Default	Change to	Description
Make password case sensitive	no	yes	Lets you use a combination of uppercase and lowercase letters in a password. This setting applies to pcAnywhere Authentication only.
Limit login attempts per call	3	3	pcAnywhere lets host users limit the number of times a remote user can attempt to login during a single session to protect against hacker attacks.
Limit time to complete login	3	1	Similarly, host users can limit the amount of time that a remote user has to complete a login to protect against hacker and denial of service attacks.

Table 4: Security Options - Session Options

Settings	Default	Change to	Description
Disconnect if inactive	no	Yes (2 Minutes)	Limits time of connection. pcAnywhere lets host users limit the amount of time that a remote caller can stay connected to the host to protect against denial of service attacks and improper use.

Data Stream Protection During Remote Control Session

Encryption prevents the data stream (including the authorization process) from being viewed using readily available tools.

pcAnywhere offers three levels of encryption:

- pcAnywhere encryption
- Symmetric encryption
- Public key encryption

Table 5: Encryption Configuration

Settings	Default	Change to	Description
Level	<none>	Symmetric	Lists the following encryption options: **None:** Sends data without encrypting it. **pcAnywhere encoding:** Scrambles the data using a mathematical algorithm so a third party cannot easily interpret the data. **Symmetric:** Encrypts and decrypts data using a cryptographic key. **Public key:** Encrypts and decrypts data using a cryptographic key. Both the sender and recipient must have a digital certificate and an associated public/private key pair.
Deny lower encryption level	no	Yes	Refuses a connection with a computer that uses a lower level of encryption than the one you selected.
Encrypt user ID and password only	no	no	Encrypts only the remote user's identity during the authorization process. This option is less secure than encrypting an entire session.

Unauthorized Changes to Installed Product

Integrity checking verifies that the host and remote objects, DLL files, executables, and registry settings have not changed since the initial installation. If pcAnywhere detects changes to these files on a computer, pcAnywhere does not run. This security feature guards against hacker attacks and employee changes that can hurt security.

Identifying Security Risks

The Symantec Remote Access Perimeter Scanner (RAPS) lets administrators scan their network and telephone lines to identify unprotected remote access hosts and address security holes. This tool provides administrators with a way to access the vulnerability of their network in terms of remote access products. Using RAPS, you can automatically shut down an active pcAnywhere host that is not password protected and inform the user.

Event Logging During Remote Control Session

You can log every file and program that is accessed during a remote control session for security and auditing purposes. Previous versions only tracked specific pcAnywhere tasks such as login attempts and activity within pcAnywhere. The centralized logging features in pcAnywhere let you log events to pcAnywhere log, NT Event Log, or an SNMP monitor.

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.