CHAPTER 3

Configuring Client Computers for Cisco Unified Communications for RTX

Revised: February 22, 2011

- About Client Computer Configuration, page 3-1
- Location of Client Services Framework Configuration Data, page 3-1
- Configuring Registry Subkeys for the Client Services Framework Client Integration, page 3-2
- About the Client Services Framework Cache Searches, page 3-8
- How to Configure Cisco UC for RTX Clients for Secure Access to Cisco Unified MeetingPlace, page 3-10
- Installing Security Certificates on Client Computers, page 3-11

About Client Computer Configuration

Before you install Cisco Unified Communications for RTX (Cisco UC for RTX), you must perform some configuration on the computers of your users:

- Specify the RTX settings.
- Specify other security-related settings that you want the client computers to use.
- Deploy the policy changes to the computers in your Cisco Unified Communications system. To do this, you can use a software management system, for example, Active Directory Group Policy, Altiris Deployment Solution, Microsoft System Center Configuration Manager (SCCM), and so on.

Location of Client Services Framework Configuration Data

You specify the configuration for Client Services Framework in the following registry key:

HKEY_CURRENT_USER\Software\Cisco Systems, Inc.\Client Services Framework\AdminData

If you use Active Directory Group Policy to configure Cisco UC for RTX, then Client Services Framework configuration data is specified in the following registry key:

HKEY_CURRENT_USER\Software\Policies\Cisco Systems, Inc.\Client Services Framework\AdminData

Note

- If Client Services Framework configuration data is present in both of these registry keys, the policies configuration data takes precedence.
- Client Services Framework reads only HKEY_CURRENT_USER keys. Client Services Framework does not read HKEY_LOCAL_MACHINE keys.

Configuring Registry Subkeys for the Client Services Framework Client Integration

- Specifying TFTP, CTIManager, and CCMCIP Server Registry Settings, page 3-2
- Specifying Cisco Unified MeetingPlace Server Registry Settings, page 3-3
- Specifying Voicemail Registry Settings, page 3-4
- Specifying Video Registry Settings, page 3-4
- Specifying Security Certificate Registry Settings, page 3-5
- Specifying Account Credential Synchronization Registry Settings, page 3-6
- Specifying Contact Resolution Registry Settings, page 3-6
- Specifying Automatic Device Selection Registry Settings, page 3-6
- Using an Active Directory Group Policy Administrative Template to Configure Client Services Framework Clients, page 3-7

Specifying TFTP, CTIManager, and CCMCIP Server Registry Settings

Table 3-1 lists the registry subkeys that you must use to specify the TFTP, CCMCIP, and CTIManager server configurations.

Table 3-1 TFTP, CCMCIP, and CTIManager Server Registry Subkeys

Subkey Names	Description
TftpServer1, TftpServer2, TftpServer3	Enter the IP address or fully-qualified domain name of the primary TFTP server in your Cisco Unified Communications system, and any other TFTP servers. If you are using certificates, the certificate common name must match the network identifier used to access the server (for example, IP address or hostname).
CtiServer1, CtiServer2	Enter the IP address or fully-qualified domain name of the primary CTIManager server in your Cisco Unified Communications system, and the secondary CTIManager server, if present. If you are using certificates, the certificate common name must match the network identifier used to access the server (for example, IP address or hostname).

Table 3-1 TFTP, CCMCIP, and CTIManager Server Registry Subkeys (continued)

Subkey Names	Description
CcmcipServer1, CcmcipServer2	Enter the IP address or fully-qualified domain name of the primary CCMCIP server in your Cisco Unified Communications system, and the secondary CCMCIP server, if present. If you are using certificates, the certificate common name must match the network identifier used to access the server (for example, IP address or hostname).
CcmcipServerValidation	Enter the type of security certificate validation for Client Services Framework to use with HTTPS to sign in to Cisco Unified Communications Manager to retrieve the device list. Enter one of the following values: • 0: Client Services Framework accepts all certificates. • 1: Client Services Framework accepts certificates that are defined in the keystore and self-signed certificates. • 2: Client Services Framework only accepts certificates that are defined in the keystore. **Note** Client Services Framework uses this certificate to verify the Cisco Unified Communications Manager server. When the certificate is accepted, Client Services Framework must use the credentials of the user to sign in to Cisco Unified Communications Manager.

Related Topics

- Installing Security Certificates on Client Computers, page 3-11

Specifying Cisco Unified MeetingPlace Server Registry Settings

Table 3-2 lists the registry subkeys that you must use to specify the Cisco Unified MeetingPlace server configuration.

Table 3-2 Cisco Unified MeetingPlace Server Registry Subkeys

Subkey Names	Description
WebConfServer	Enter the fully-qualified domain name (FQDN) of the Cisco Unified MeetingPlace server in your Cisco Unified Communications system. Do not include the IP address.

Table 3-2 Cisco Unified MeetingPlace Server Registry Subkeys (continued)

Subkey Names	Description
WebConfPort	Enter the port number for the Cisco Unified MeetingPlace server. The port number for HTTP protocol is usually 80 and the port number for HTTPS protocol is usually 443.
WebConfServerValidation	Specify the type of security certificate validation that Client Services Framework uses with HTTPS to validate requests from the Cisco Unified MeetingPlace web conferencing server. Enter one of the following values: • 0: Client Services Framework accepts all certificates. • 1: Client Services Framework accepts certificates that are defined in the keystore and self-signed certificates. This is the default. • 2: Client Services Framework only accepts certificates that are defined in the keystore.

Related Topics

- Installing Security Certificates on Client Computers, page 3-11

Specifying Voicemail Registry Settings

Table 3-3 lists the registry subkey that you must use to specify the voicemail configuration.

Table 3-3 Voicemail Registry Subkey

Subkey Names	Description
VoicemailPilotNumber	Enter the number of the voice message service in your Cisco Unified Communications system. This value only relates to when users use the desk phone to access their voice messages. If users are using the phone on their computer to access voicemail, the pilot number comes from the voicemail pilot number associated with the voicemail profile configured on the Client Services Framework device.

Specifying Video Registry Settings

Table 3-4 lists the registry subkeys that you must use to specify video values.

Table 3-4 Video Registry Subkeys

Subkey Names	Description
SetVideoEnablePref	This value determines whether the user option to "Show my video automatically" is displayed in the Cisco UC Settings dialog box in Cisco UC for RTX. To hide this option from users, set this value to False. To show this option to users, set this value to True.
SetVideoStaticThrottlingPref	This value determines whether the user option to "Optimize video quality for your computer" is displayed in the Cisco UC Options dialog box in Cisco UC for RTX. If selected, this option enables static video throttling. To hide this option from users, set this value to False. To show this option to users, set this value to True.

Specifying Security Certificate Registry Settings

Table 3-5 lists the registry subkey that you must use to specify the location of security certificates.

Table 3-5 Security Registry Subkey

Subkey Names	Description
SECURITY_CertificateDirectory	Specify the location of the directory where the security certificates are stored. For example, you might store LDAP or CCMCIP certificates in this location. Use this setting to specify a location for the certificates where the certificates will not be overwritten if you reinstall Cisco UC for RTX. If you do not specify a value for this setting, the certificates are stored in the following locations: • Windows XP: <*drive*>:\Documents and Settings\<*username*>\Local Settings\Application Data\Cisco\Unified Communications\Client Services Framework\certificates • Windows Vista and Windows 7: <*drive*>:\Users\<*username*>\AppData\Local\Cisco\Unified Communications\Client Services Framework\certificates

Specifying Account Credential Synchronization Registry Settings

Client Services Framework includes settings that enable you to manage the credentials of Cisco Unified Communications back-end services. You can use these settings to configure the source of credentials for each service.

For example, you might have separate directories for your phone system, voicemail system, and meeting system. If you do not set the appropriate values for these services, your users have to select **File > Cisco UC Settings > Accounts**, then enter their username and password for each service.

Table 3-6 lists the registry subkeys that you must use to specify account credential synchronization.

Table 3-6 Account Credential Synchronization Registry Subkeys

Subkey Names	Description
PhoneService_UseCredentialsFrom ContactService_UseCredentialsFrom WebConfService_UseCredentialsFrom	You must set the ContactService_UseCredentialsFrom subkey to the value, Phone. The other two subkeys are reserved for future use.

Specifying Contact Resolution Registry Settings

Table 3-7 lists the registry subkey that you must use to enable contact resolution.

Table 3-7 Contact Resolution Registry Subkey

Subkey Names	Description
RTX_Mode	Controls whether contact resolution is enabled on Cisco UC for RTX. Contact resolution maps phone numbers to RTX accounts and the other way round. If contact resolution is enabled, detailed contact information, such as contact names, images, phone numbers, and email addresses, is displayed in conversation windows, conversation history, and contact cards. Set the value of this subkey to 1 to enable contact resolution.

Specifying Automatic Device Selection Registry Settings

Table 3-8 lists the registry subkey that you must use to disable automatic device selection.

Table 3-8 Automatic Device Selection Registry Subkey

Subkey Names	Description
AutomaticDeviceSelectionMode	Controls whether automatic device selection is enabled on Cisco UC for RTX. If automatic device selection is enabled, Cisco UC for RTX automatically selects as the default device any audio device or video device that the user adds on their computer. Set the value of this subkey to 0 to disable the automatic device selection.

Using an Active Directory Group Policy Administrative Template to Configure Client Services Framework Clients

A Group Policy administrative template is provided with Cisco UC for RTX. You can use this template to define the Client Services Framework registry settings on a system, or for groups of users.

You can get the administrative templates from the Administration Toolkit for Cisco UC for RTX. To access the Administration Toolkit, navigate to Cisco Unified Communications for RTX from the Download Software page at the following URL:

http://tools.cisco.com/support/downloads/go/Model.x?mdfid=283454590

Procedure

Step 1 Execute the following command to start the Group Policy application:

gpedit.msc

Step 2 Expand the **User Configuration** node.

Step 3 Right-click **Administrative Templates**, then select **Add/Remove Templates**.

Step 4 Add the administrative template to the list of current policy templates in the Add/Remove Templates dialog box, then select **Close**.

Step 5 Open the Cisco Unified Communications for RTX folder in the right pane.

Note In Windows Vista and Windows 7, this folder is in the Administrative Templates > Classic Administrative Templates folder. In Windows XP, this folder is in the Administrative Templates folder.

Step 6 Open the folder for the settings whose value you want to specify.

Step 7 Double-click the setting whose value you want to specify.

Step 8 Enter the value you require, then select **OK**.

After the ADM file is imported and populated, you can apply the resulting policy to an organizational unit using the Group Policy Management Editor.

Related Topics

- About the Client Services Framework Cache Searches, page 3-8

About the Client Services Framework Cache Searches

Cisco Unified Client Services Framework allows users to cache the following user credentials between sign-outs and sign-ins:

- Cisco Unified Communications Manager
- Voicemail
- Cisco Unified MeetingPlace

When you place a call, receive a call, or miss a call, the contacts for the calls are added to your Client Services Framework cache. Any contact that is in your conversation history is automatically placed in your cache. All of the data for the contacts in your contact list in RTX is also cached.

All contacts in the Client Services Framework cache have already had the directory lookup dialing rules applied to all of their numbers. When Cisco UC for RTX displays numbers for contacts that are in the Client Services Framework cache, the numbers have already had the directory lookup dialing rules applied to them.

The Client Services Framework cache is a memory-only cache. The contents of the cache are *not* copied to a local file system. The contents of the Client Services Framework cache are refreshed in the following scenarios:

- Users sign out of Cisco UC for RTX and sign in to it again.
- The cucsf.exe process is restarted.

Incoming Calls

When a user receives a call, the following events occur:

1. When Cisco Unified Communications Manager detects the incoming call, it sends the following data to Client Services Framework:
   - The directory number from which the call originates.
   - The Alerting Name of the directory number that is specified in the Directory Number Configuration screen, if the field is not blank.
2. Client Services Framework sends the directory number and alerting name to Cisco UC for RTX.
3. Cisco UC for RTX displays the directory number and the alerting name in a notification window and, if the call is answered, in the conversation window.
4. Client Services Framework searches the Client Services Framework cache for the number that is returned *after* the directory number is processed by the directory lookup dialing rules.
5. If the processed directory number is in the Client Services Framework cache, and the contact name for that number does not come from RTX contact information, the display name in the conversation window is the Alerting Name from the Cisco Unified Communications Manager.
6. If the processed directory number is in the Client Services Framework cache, and the contact name for that number comes from RTX contact information, Client Services Framework also gets the local path of the photo from RTX. Then Client Services Framework sends the display name and the photo URI to Cisco UC for RTX. Proceed to 8.

If the processed directory number is not in the Client Services Framework cache, Client Services Framework sends the directory number and the Alerting Name from the Cisco Unified Communications Manager to Cisco UC for RTX.

7. Client Services Framework starts an asynchronous thread to search RTX contact information for the processed directory number. If the contact with the number is found, Client Services Framework updates the cache with detailed RTX contact information, including the display name, the RTX account, the office phone number, the mobile phone number, and the email address. Client Services Framework also gets the local path of the photo from RTX.
8. Client Services Framework sends the display name and the photo URI to Cisco UC for RTX.
9. If other party answers the the call, Client Services Framework gets the display name of the directory number from Cisco Unified Communications Manager. If the contact name does not come from RTX contact information, Client Services Framework sends the display name to the Cisco UC for RTX.
10. Cisco UC for RTX updates the conversation window.

Outgoing Calls to Contacts by Names

You can place a call to a contact in the following ways:

- Select the **Start Audio conversation** menu item.
- Select the **Place a Call** menu item.

When you place a call in either of these ways, the following events occur:

1. Cisco UC for RTX sends the RTX account for the contact to be called to Client Services Framework, and asks Client Services Framework to place a call to that number.
2. If the RTX account is not in the Client Services Framework cache, Client Services Framework searches local RTX contact information for details of the party to be called.
3. Client Services Framework sends data about the contact back to Cisco UC for RTX. Cisco UC for RTX uses the contact data during the conversation. If the contact has more than one number, Cisco UC for RTX sends the office phone number to call. Otherwise, Cisco UC for RTX sends that number to call.
4. Client Services Framework applies the application dialing rules and sends the number to Cisco Unified Communications Manager.
5. Cisco Unified Communications Manager places the call.

Outgoing Calls to Contacts by Numbers

You can place a call to a contact the the following ways:

- Select a number of the contact.
- Enter a number in keypad.

When you place a call in either of these ways, the following events occur:

1. Cisco UC for RTX sends the number for the contact to be called to Client Services Framework, and asks Client Services Framework to place a call to that number.
2. Client Services Framework searches the Client Services Framework cache for the number that is returned *after* the directory number is processed by the directory lookup dialing rules.

3. If the contact is in the Client Services Framework cache, and the contact name for that number does not come from RTX contact information, the display name in the conversation window is the Alerting Name from the Cisco Unified Communications Manager.
4. If the contact is not in Client Services Framework cache, Client Services Framework creates a contact with the directory number and a blank display name.
5. Client Services Framework starts an asynchronous thread to search RTX contact information for the processed directory number. If the contact with the number is found, Client Services Framework updates the cache with detailed RTX contact information, including the display name, the RTX account, the office phone number, the mobile phone number, and the email address. Client Services Framework also gets the local path of the photo from RTX.
6. Client Services Framework applies the application dialing rules and sends the number to Cisco Unified Communications Manager.
7. Cisco Unified Communications Manager places the call.
8. Client Services Framework sends the directory number and the display name to Cisco UC for RTX.
9. When Cisco Unified Communications Manager sends Client Services Framework an ALERT message, Cisco Unified Communications Manager sends the Alerting Name of the directory number to Client Services Framework. If the contact information does not come from RTX, the display name of the contact is the Alerting Name from the Cisco Unified Communications Manager. The directory number is processed by the directory lookup dialing rules from the Cisco Unified Communications Manager.
10. Client Services Framework sends updated data to Cisco UC for RTX.
11. If other party answers the call, Client Services Framework gets the display name of the directory number from Cisco Unified Communications Manager. If the contact name does not come from RTX contact information, Client Services Framework sends the display name to Cisco UC for RTX.

How to Configure Cisco UC for RTX Clients for Secure Access to Cisco Unified MeetingPlace

- Configuring Secure Access to Cisco Unified MeetingPlace, page 3-10
- Downloading the IIS Certificate from Cisco Unified MeetingPlace, page 3-11

Configuring Secure Access to Cisco Unified MeetingPlace

For information about how to set up the Cisco Unified MeetingPlace web server for secure access, see the *Administration Documentation for Cisco Unified MeetingPlace* at:

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_installation_and_configuration_guides_list.html

What To Do Next

Downloading the IIS Certificate from Cisco Unified MeetingPlace, page 3-11

Downloading the IIS Certificate from Cisco Unified MeetingPlace

Procedure

Step 1 Open the Internet Services Manager on the Cisco Unified MeetingPlace Web Server.

Select **Start** > **Programs** > **Administrative Tools** > **Internet Information Services Manager**.

Step 2 Navigate to Default Web Site.

Select the + sign beside Local Server > Web Sites to open the appropriate directory trees.

Step 3 Right-click **Default Web Site**.

Step 4 Select **Properties**.

Step 5 Select the **Directory Security** tab.

Step 6 Select **Server Certificate**. The Web Server Certificate wizard displays.

Step 7 Select **Next**.

Step 8 Select **Export the current certificate to a pfx file**, then select **Next**.

Step 9 Select **Browse** and select to save the certificate file to your desktop.

Step 10 Select **Next**.

Step 11 Enter a password to encrypt the certificate.

Step 12 Enter the password again to confirm it, then select **Next**. The Export Certificate Summary Screen displays and the exported certificate file is now on your desktop.

Step 13 Select **Next**.

Step 14 Select **Finish** to close the Web Server Certificate wizard.

What To Do Next

Installing Security Certificates on Client Computers, page 3-11

Installing Security Certificates on Client Computers

Procedure

Step 1 Put the certificate file into the folder where you store your security certificates.

Step 2 Use the SECURITY_CertificateDirectory registry subkey value name to specify the folder where the certificates are stored.

Related Topics

- Specifying Security Certificate Registry Settings, page 3-5