About Client Computer Configuration

Before you install Cisco UC Integration for Microsoft Office Communicator, you must perform some configuration on the computers of your users:

- Specify the Client Services Framework client settings.
- Specify the Microsoft Office Communicator settings.
- Specify the Microsoft Office 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 software management system, for example, Active Directory Group Policy, Altiris Deployment Solution, Microsoft System Center Configuration Manager (SCCM), and so on.
• Configure the Client Services Framework on the computers of your users so that the Client Services Framework can function as the phone device for that user, to specify where Client Services Framework can connect to, and to specify the LDAP parameters.

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 Integration for Microsoft Office Communicator, 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 Value Names for the Client Services Framework

Client Integration

• Specifying TFTP, CTIManager, and CCMCIP Server Value Names, page 3-3
• Specifying Cisco Unified MeetingPlace Server Value Names, page 3-4
• Specifying Voicemail and Visual Voicemail Value Names, page 3-4
• Specifying Video Value Names, page 3-6
• Specifying Security Certificate Value Names, page 3-6
• Specifying LDAP Value Names, page 3-7
• Specifying Account Credential Synchronization Value Names, page 3-10
• Using an Active Directory Group Policy Administrative Template to Configure Client Services Framework Clients, page 3-10
Specifying TFTP, CTIManager, and CCMCIP Server Value Names

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

<table>
<thead>
<tr>
<th>Value Names</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TftpServer1, TftpServer2, TftpServer3</td>
<td>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, this value must match the name of the server as specified on the certificate.</td>
</tr>
<tr>
<td>CtiServer1, CtiServer2</td>
<td>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, this value must match the name of the server as specified on the certificate.</td>
</tr>
<tr>
<td>CcmcipServer1, CcmcipServer2</td>
<td>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, this value must match the name of the server as specified on the certificate.</td>
</tr>
<tr>
<td>CcmcipServerValidation</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• 0: Client Services Framework accepts all certificates.</td>
</tr>
<tr>
<td></td>
<td>• 1: Client Services Framework accepts certificates that are defined in the keystore and self-signed certificates.</td>
</tr>
<tr>
<td></td>
<td>• 2: Client Services Framework only accepts certificates that are defined in the keystore.</td>
</tr>
<tr>
<td>Note</td>
<td>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.</td>
</tr>
</tbody>
</table>

Related Topics

- Installing Security Certificates on Client Computers, page 3-21
Specifying Cisco Unified MeetingPlace Server Value Names

Table 3-2 lists the name-value pairs that you must use to specify the Cisco Unified MeetingPlace server configuration.

**Table 3-2  Cisco Unified MeetingPlace Server Value Names**

<table>
<thead>
<tr>
<th>Value Names</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebConfServer</td>
<td>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.</td>
</tr>
<tr>
<td>WebConfProtocol</td>
<td>The protocol to use between Client Services Framework and the Cisco Unified MeetingPlace server. The options are HTTP or HTTPS.</td>
</tr>
<tr>
<td>WebConfPort</td>
<td>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.</td>
</tr>
<tr>
<td>WebConfServerValidation</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• 0: Client Services Framework accepts all certificates.</td>
</tr>
<tr>
<td></td>
<td>• 1: Client Services Framework accepts certificates that are defined in the keystore and self-signed certificates. This is the default.</td>
</tr>
<tr>
<td></td>
<td>• 2: Client Services Framework only accepts certificates that are defined in the keystore.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Installing Security Certificates on Client Computers, page 3-21

Specifying Voicemail and Visual Voicemail Value Names

Table 3-3 lists the name-value pairs that you must use to specify the voicemail and visual voicemail configuration.

**Table 3-3  Voicemail and Visual Voicemail Value Names**

<table>
<thead>
<tr>
<th>Value Names</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VoicemailPilotNumber</td>
<td>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.</td>
</tr>
<tr>
<td>VVM_SystemServer_0¹</td>
<td>Enter the IP address or fully-qualified hostname of the Cisco Unity or Cisco Unity Connection voicemail server.</td>
</tr>
</tbody>
</table>
Chapter 3 Configuring Client Computers for Cisco Unified Communications Integration for Microsoft Office

Configuring Value Names for the Client Services Framework Client Integration

Table 3-3 Voicemail and Visual Voicemail Value Names

<table>
<thead>
<tr>
<th>Value Names</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VVM_SystemServer_VmwsPort_01</td>
<td>Enter the port number for the Cisco Unity Voicemail Web Service (VMWS) on the Cisco Unity or Cisco Unity Connection voicemail server. This value is optional with Cisco Unity and Cisco Unity Connection for synchronizing voicemail-related preferences, but the value is required with Cisco Unity for secure message playback.</td>
</tr>
<tr>
<td>VVM_SystemServer_VmwsProtocol_01</td>
<td>Enter the protocol to use for the VMWS. The options are HTTP or HTTPS. This value is optional with Cisco Unity and Cisco Unity Connection for synchronizing voicemail-related preferences, but the value is required with Cisco Unity for secure message playback.</td>
</tr>
<tr>
<td>VVM_Mailstore_Server_01</td>
<td>Enter the IP address or hostname of the IMAP mailstore server that is peers with the Cisco Unity or Cisco Unity Connection server. For Cisco Unity voicemail servers, this is typically the IP address of the peer Microsoft Exchange server. For Cisco Unity Connection voicemail servers, this is typically the IP address of the Cisco Unity Connection server itself.</td>
</tr>
<tr>
<td>VVM_Mailstore_ImapPort_01</td>
<td>Enter the port number to use for IMAP for visual voicemail. The IMAP port number is usually 143. Enter 7993 for this value name if you want to implement secure messages on a Cisco Unity Connection server.</td>
</tr>
<tr>
<td>VVM_Mailstore_ImapProtocol_01</td>
<td>Enter the protocol to use for IMAP for visual voicemail. Enter TCP for this value name. If you want to implement secure messages on a Cisco Unity Connection server, enter TLS.</td>
</tr>
<tr>
<td></td>
<td>If you want to implement secure signing between a Cisco Unity server and a Microsoft Exchange server, enter TLS.</td>
</tr>
<tr>
<td></td>
<td>If you use secure transport protocols like TLS and HTTPS, the certificate presented by the server must be a trusted certificate, signed by a trusted authority. If you use a local authority or a self-signed certificate, you must add these to the Client Services Framework keystore and mark them as trusted.</td>
</tr>
<tr>
<td>VVM_Mailstore_EncryptedConnection</td>
<td>Set this value to True to enable an encrypted IMAP connection to the voicemail server.</td>
</tr>
<tr>
<td>VVM_Mailstore_InboxFolderName</td>
<td>Enter “INBOX” as the name of your voicemail message inbox on the voicemail server.</td>
</tr>
<tr>
<td>VVM_Mailstore_PollingInterval</td>
<td>Enter the number of seconds that pass between calls to the visual voicemail server to check for new, updated, deleted or purged voice messages. For example, enter 60 seconds.</td>
</tr>
<tr>
<td>VVM_Mailstore_TrashFolderName</td>
<td>Enter the name of the folder to which deleted voice messages are moved on the Cisco Unity voicemail server. For example, “Deleted Items”. This value is not required for Cisco Unity Connection voicemail servers.</td>
</tr>
<tr>
<td>VVM_Mailstore_IdleEnabled</td>
<td>Set this value to True to enable an idle timeout.</td>
</tr>
<tr>
<td>VVM_Mailstore_IdleExpireTimeInMin</td>
<td>Specify the number of minutes that must elapse to trigger an idle timeout. The value can be between 5 and 29. The default is 29.</td>
</tr>
</tbody>
</table>

1. The last character of this value name can be 0 or 1 depending on whether the voicemail server is a primary (0) or secondary (1) server.
Specifying Video Value Names

Table 3-4 lists the name-value pair that you must use to specify video values.

Table 3-4 Video Value Names

<table>
<thead>
<tr>
<th>Value Names</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SetVideoEnablePref</td>
<td>This value determines whether the user option to “Show my video automatically” is displayed in the Cisco UC Options dialog box in Cisco UC Integration for Microsoft Office Communicator. To hide this option from users, set this value to False. To show this option to users, set this value to True.</td>
</tr>
<tr>
<td>SetVideoStaticThrottlingPref</td>
<td>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 Integration for Microsoft Office Communicator. 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.</td>
</tr>
</tbody>
</table>

Specifying Security Certificate Value Names

Table 3-5 lists the name-value pair that you must use to specify the location of security certificates.

Table 3-5 Security Value Names

<table>
<thead>
<tr>
<th>Value Names</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 Integration for Microsoft Office Communicator.  
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\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 LDAP Value Names

Table 3-6 lists the name-value pairs that you must use to specify the LDAP configuration.

Table 3-6   LDAP Value Names

<table>
<thead>
<tr>
<th>Value Names</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP_AttributeName_primaryPhoneNumberForSearches</td>
<td>Specify the phone number that you use to resolve most LDAP queries. This value must match one of the values specified for the following LDAP keys:</td>
</tr>
<tr>
<td></td>
<td>• LDAP_AttributeName_businessPhone</td>
</tr>
<tr>
<td></td>
<td>• LDAP_AttributeName_homePhone</td>
</tr>
<tr>
<td></td>
<td>• LDAP_AttributeName_mobilePhone</td>
</tr>
<tr>
<td></td>
<td>• LDAP_AttributeName_otherPhone</td>
</tr>
<tr>
<td></td>
<td>The values that are valid for the LDAP attribute keys listed above are:</td>
</tr>
<tr>
<td></td>
<td>• telephoneNumber</td>
</tr>
<tr>
<td></td>
<td>• homePhone</td>
</tr>
<tr>
<td></td>
<td>• mobilePhone</td>
</tr>
<tr>
<td></td>
<td>• otherTelephone</td>
</tr>
<tr>
<td></td>
<td>• a custom LDAP attribute value, for example, myCustomPhoneNumber</td>
</tr>
<tr>
<td></td>
<td>The value of the LDAP_AttributeName_primaryPhoneNumberForSearches key must match one of the values in the list above, for example, telephoneNumber. Otherwise, the value of the LDAP_AttributeName_businessPhone key is used.</td>
</tr>
<tr>
<td>LDAP_enableWildcardMatchesForPhoneNumberSearches</td>
<td>Set this value to True if you want to enable wildcard searches for phone numbers in the LDAP.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you set this key to True, the speed of searches of the LDAP might be affected.</td>
</tr>
<tr>
<td>LDAP_MaxCacheSize</td>
<td>Specify the maximum number of LDAP directory records to retain in the cache of the user.</td>
</tr>
</tbody>
</table>
Table 3-6  LDAP Value Names

<table>
<thead>
<tr>
<th>Value Names</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP_Server_1</td>
<td>Enter the protocol name, followed by the fully-qualified domain name (FQDN) of your LDAP server. For example: ldap://ldap.example.com</td>
</tr>
<tr>
<td></td>
<td>If you want to use a port number other than the default 389, add a colon to the value, followed by the port number. For example: ldap://ldap.example.com:19389</td>
</tr>
<tr>
<td></td>
<td>If you want to use LDAP over SSL, this IP address must begin with ldaps://. For example: ldaps://ldap.example.com</td>
</tr>
<tr>
<td></td>
<td>If you want to use a port number other than the default 636, add a colon to the value, followed by the port number. For example: ldaps://ldap.example.com:19636</td>
</tr>
<tr>
<td></td>
<td>For more information about how to enable LDAP over SSL, see Enabling LDAP Over SSL, page 3-11.</td>
</tr>
<tr>
<td>LDAP_SearchBaseDN_1,</td>
<td>Specify the primary distinguished name for the location in the LDAP directory from which searches begin. For example, specify a distinguished name similar to the following: OU=Sales,DC=example,DC=com</td>
</tr>
<tr>
<td>LDAP_SearchBaseDN_2,</td>
<td>Specify any further search bases also.</td>
</tr>
<tr>
<td>LDAP_SearchBaseDN_3,</td>
<td></td>
</tr>
<tr>
<td>LDAP_SearchBaseDN_4,</td>
<td></td>
</tr>
<tr>
<td>LDAP_SearchBaseDN_5</td>
<td></td>
</tr>
<tr>
<td>LDAP_ResultSetMaxSize</td>
<td>Specify the maximum number of records to return when the user searches the LDAP directory. That is, when the user searches for contacts in Microsoft Office Communicator.</td>
</tr>
<tr>
<td>LDAP_UserLogonDomain</td>
<td>Enter the name of the domain that contains the LDAP account of the user.</td>
</tr>
<tr>
<td>LDAP_EnableAnonymousBind</td>
<td>Set this value to True if the LDAP server is enabled for anonymous access. If this is the case, users do not have to supply credentials to access the LDAP server.</td>
</tr>
</tbody>
</table>
Table 3-7 lists the values you must enter for LDAP attribute key names to enable Client Services Framework searches to map to the appropriate fields of the Active Directory.

<table>
<thead>
<tr>
<th>For This Value Name...</th>
<th>Enter the Following Active Directory Field...</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP_AttributeName_objectclassKey</td>
<td>objectclass</td>
</tr>
<tr>
<td>LDAP_AttributeName_objectclassValue</td>
<td>person</td>
</tr>
<tr>
<td>LDAP_AttributeName_userLogonName</td>
<td>userPrincipalName</td>
</tr>
<tr>
<td>LDAP_AttributeName_displayName</td>
<td>displayName</td>
</tr>
<tr>
<td>LDAP_AttributeName_commonName</td>
<td>cn</td>
</tr>
<tr>
<td>LDAP_AttributeName_firstName</td>
<td>givenName</td>
</tr>
<tr>
<td>LDAP_AttributeName_lastName</td>
<td>sn</td>
</tr>
<tr>
<td>LDAP_AttributeName_email</td>
<td>mail</td>
</tr>
<tr>
<td>LDAP_AttributeName_uri</td>
<td>msRTCSIP-PrimaryUserAddress</td>
</tr>
<tr>
<td>LDAP_AttributeName_photoUri</td>
<td>photoUri</td>
</tr>
<tr>
<td>LDAP_AttributeName_businessPhone</td>
<td>telephoneNumber</td>
</tr>
<tr>
<td>LDAP_AttributeName_homePhone</td>
<td>homePhone</td>
</tr>
<tr>
<td>LDAP_AttributeName_mobilePhone</td>
<td>mobilePhone</td>
</tr>
<tr>
<td>LDAP_AttributeName_otherPhone</td>
<td>otherTelephone</td>
</tr>
<tr>
<td>LDAP_AttributeName_title</td>
<td>title</td>
</tr>
<tr>
<td>LDAP_AttributeName_companyName</td>
<td>company</td>
</tr>
<tr>
<td>LDAP_AttributeName_userAccountName</td>
<td>sAMAccountName</td>
</tr>
</tbody>
</table>

**Note** Do not use any other Active Directory field for this key name.
Specifying Account Credential Synchronization Value Names

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 in the Cisco UC pane, then enter their username and password for each service.

Table 3-8 lists the name-value pair that you must use to specify the location of security certificates.

<table>
<thead>
<tr>
<th>Value Names</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ContactService_UseCredentialsFrom</td>
<td>You can set each of these names to one of the following values:</td>
</tr>
<tr>
<td>VoicemailService_UseCredentialsFrom</td>
<td>• CONTACT</td>
</tr>
<tr>
<td>WebConfService_UseCredentialsFrom</td>
<td>• PHONE</td>
</tr>
<tr>
<td></td>
<td>• VOICEMAIL</td>
</tr>
<tr>
<td></td>
<td>• WEBCONF</td>
</tr>
</tbody>
</table>

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

A Group Policy administrative template is provided with Cisco UC Integration for Microsoft Office Communicator. You can use this template to define the Client Services Framework registry settings on a system, or for groups of users. The template file is CUCIMOC.adm.

Procedure

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

```plaintext
gpedit.msc
```

Step 2 Expand the User Configuration node.

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

Step 4 Add the file CUCIMOC.adm to the list of current policy templates in the Add/Remove Templates dialog box, then select Close.

Step 5 Open the Cisco Unified Communications Integration for Microsoft Office Communicator 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.
Chapter 3      Configuring Client Computers for Cisco Unified Communications Integration for Microsoft Office

Enabling LDAP Over SSL

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
- Configuration of Policies for Microsoft Office Applications, page 3-14

Enabling LDAP Over SSL

- Creating a Certificate on the Active Directory Server, page 3-11
- Installing the Certificate on the Client Computer, page 3-11
- Configuring Client Services Framework, page 3-12

Creating a Certificate on the Active Directory Server

Before You Begin
Ensure that the LDAP server is configured to support LDAP over SSL (LDAPS).

Procedure

Step 1 Sign in to the Active Directory server.
Step 2 Execute the following command:
certutil -ca.cert cucimoc.crt
This command generates a file called cucimoc.crt. You must install this certificate on each client computer.

What to Do Next
- Installing the Certificate on the Client Computer, page 3-11

Installing the Certificate on the Client Computer

Before You Begin
Before you install the certificate on the client computer, ensure that neither of the following processes are running:
- Client Services Framework, that is, the cucsf.exe process.
- Cisco UC Integration for Microsoft Office Communicator, that is, the cucimoc.exe process.
Enabling LDAP Over SSL

Chapter 3  Configuring Client Computers for Cisco Unified Communications Integration for Microsoft Office

Procedure

Step 1  You install the cucimoc.crt file in the keystore of the Java Runtime Environment (JRE) that Client Services Framework is using. If you configured Client Services Framework to use the default JRE, the JRE is located in %CSF_INSTALL%\jre.

Step 2  Execute the following command:

```
keytool -importcert -keystore <path to cacerts> -storepass changeit -file <path to cert file>
```

For example, if the path to the Client Services Framework installation is C:\Program Files\Common Files\Cisco Systems\Client Services Framework\jre\bin, and the cucimoc.crt file is stored in C:\temp, you execute the following command:

```
"C:\Program Files\Common Files\Cisco Systems\Client Services Framework\jre\bin\keytool" -importcert -keystore "C:\Program Files\Common Files\Cisco Systems\Client Services Framework\jre\lib\security\cacerts" -storepass changeit -file "C:\temp\cucimoc.crt"
```

The default password for the cacerts keystore is changeit.

Step 3  When asked if you trust this certificate, enter yes.

What to Do Next

- Configuring Client Services Framework, page 3-12

Configuring Client Services Framework

Procedure

Step 1  Set the value for the LDAP_Server_1 value name to set the URL of the LDAP server. For example, set the value of LDAP_Server_1 to the following:

```
ldaps://ldap.example.com
```

The only change from using standard LDAP is that you specify the protocol as ldaps instead of ldap. Use the FQDN of the LDAP server as specified in the certificate. You cannot use the IP address of the LDAP server, or the server name alone. Ensure that the FQDN is reachable. If the FQDN cannot be reached using DNS, add an appropriate entry to your hosts file.

If your LDAP server does not use the default port for LDAPS, specify the port with the URL. For example, enter a value such as the following:

```
ldaps://ldap.example.com:19636
```

Step 2  Restart Cisco UC Integration for Microsoft Office Communicator.

Step 3  To verify that you are connected to LDAPS, select the Menu button in the Microsoft Office Communicator title bar, then select Tools > Server Status.

Read the server protocol information in the Server Status tab. The protocol is displayed as ldap. Read the server port field to verify that you are connected to LDAPS.

Related Topics

- Configuring Value Names for the Client Services Framework Client Integration, page 3-2
Configuring Microsoft Office Communicator 2007 to Use HTTPS to Access Custom Availability Statuses

Cisco UC Integration for Microsoft Office Communicator includes custom availability statuses such as “On the Phone”. These statuses are stored in the custom availability status file cisco-presence-states-config.xml.

For information about how to apply this policy setting to Microsoft Office Communicator, see the following URL:


**Microsoft Office Communicator 2007 R1**

The location of the cisco-presence-states-config.xml file is set in the Custom presence states URL Microsoft Office Communicator group policy setting. In Microsoft Office Communicator 2007 R1 this URL can use any of the following protocols:

- file://
- http://
- https://

Cisco UC Integration for Microsoft Office Communicator installs the cisco-presence-states-config.xml file in the local file system of the computer of the user. Cisco UC Integration for Microsoft Office Communicator also updates the Custom presence states URL group policy setting to refer to this file with the file:// protocol.

**Microsoft Office Communicator 2007 R2**

By default, in Microsoft Office Communicator 2007 R2, the URL specified in the Custom presence states URL group policy setting must begin with https://.

As a result, Microsoft Office Communicator 2007 R2 cannot use the Cisco UC Integration for Microsoft Office Communicator custom availability statuses. In this case, Cisco UC Integration for Microsoft Office Communicator uses the generic Microsoft Office Communicator “Busy” availability status instead of the Cisco UC Integration for Microsoft Office Communicator “Busy: On the phone” custom availability status.

To enable the custom availability statuses, do the following:

1. Put a copy of the cisco-presence-states-config.xml file on a secure web server, that is, a server that you can access with the https:// protocol. You can use the same IIS server that runs on your OCS server.
2. Update the “Custom presence states URL” group policy setting or registry setting on the computers of your users with the https:// URL of the cisco-presence-states-config.xml file.

For information about how to apply these policy settings to Microsoft Office Communicator, see Microsoft Office Communications Server 2007 R2 Client Group Policy Documentation at the following URL:

Location of Custom Availability Statuses File

On computers that have Cisco UC Integration for Microsoft Office Communicator installed, the cisco-presence-states-config.xml file is in the following location:

\<drive>\Program Files\Cisco Systems\Cisco UC Integration TM for Microsoft Office Communicator\Config\presence

Configuration of Policies for Microsoft Office Applications

- Microsoft Office Communicator Policies, page 3-14
- Microsoft Office Phone Policy, page 3-15

Microsoft Office Communicator Policies

We recommend that you configure Microsoft Office Communicator policies to allow only IM and availability status traffic on all Cisco UC Integration for Microsoft Office Communicator user groups. If you do not do this, voice traffic is allowed from both Cisco UC Integration for Microsoft Office Communicator and Microsoft Office Communicator. This can result in the following problems:

- A confusing user experience, as users can place and receive calls from a mixture of user interface elements in both applications.
- Inconsistent voice traffic. That is, calls from Cisco UC Integration for Microsoft Office Communicator might give a different audio experience to Microsoft Office Communicator.
- A mixed configuration is more difficult to manage, as administrators must track traffic from two sources. You might want to monitor voice usage in your network and if you use both applications, you must configure your monitoring tools to track traffic from both applications.

We recommend that you configure the Microsoft Office Communicator policies as shown in the following table:

<table>
<thead>
<tr>
<th>Policy</th>
<th>Set Value To...</th>
</tr>
</thead>
<tbody>
<tr>
<td>TelephonyMode</td>
<td>5 = IM and Presence Only</td>
</tr>
<tr>
<td>DisableAVConferencing</td>
<td>1</td>
</tr>
</tbody>
</table>

For information about how to apply these policy settings to Microsoft Office Communicator, see the following URL:


You can also find the policy administrative template file Communicator.adm on that web site. Alternatively, you can apply the following keys to set the policies manually:

[HKEY_CURRENT_USER\Software\Policies\Microsoft\Communicator]\"TelephonyMode"=dword:00000005

[HKEY_CURRENT_USER\Software\Policies\Microsoft\Communicator]\"DisableAVConferencing"=dword:00000001
Microsoft Office Phone Policy

We recommend that you configure a Microsoft Office policy to disable the Call menu that appears when you select a contact in a Microsoft Office application. This Call menu only appears if you have the correct smart tag switched on in the relevant Microsoft Office application.

Cisco UC Integration for Microsoft Office Communicator provides an Additional Actions menu that enables you to call contacts that you select in your Microsoft Office applications. If you do not disable the Call menu, this can result in a confusing user experience, as users might think that they can perform similar actions from a mixture of user interface elements.

To disable the Call menu in Microsoft Office, set the value of the Phone policy to zero (0).

Alternatively, you can apply the key to set the policy manually.

[HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\PersonaMenu] "Phone"=dword: 00000000

Note

In the registry keys, the values 11.0 and 12.0 refer to the different versions of Microsoft Office; 11.0 refers to Microsoft Office 2003 and 12.0 refers to Microsoft Office 2007.

About the Client Services Framework Cache and LDAP 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
- LDAP
- Cisco Unified MeetingPlace

Client Services Framework also maintains a cache of LDAP contacts. This cache is only updated from LDAP when Client Services Framework is restarted.

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 Microsoft Office Communicator is also cached.

If a contact for a call already exists in the cache, Client Services Framework does not search LDAP. If a contact does not exist in the cache, Client Services Framework searches LDAP. LDAP searches are only performed when you place a call to, or receive a call from a contact who is not in your conversation history or your Microsoft Office Communicator contact list.

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 Integration for Microsoft Office Communicator 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. When the cucsf.exe process is restarted, the contents of the Client Services Framework cache are refreshed.

- Incoming Calls, page 3-16
- Outgoing Calls to Contacts Who Are Enabled for OCS, page 3-16
- Outgoing Calls to Contacts Who Are Not Enabled for OCS, page 3-17
- Outgoing Calls to Microsoft Outlook Contacts, page 3-17

## 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 Integration for Microsoft Office Communicator.
3. Cisco UC Integration for Microsoft Office Communicator displays the directory number and the LDAP name (if resolved, otherwise the alerting name) in a notification window and, if the call is answered, in the conversation window.
4. If the directory number is not in the Client Services Framework cache, Client Services Framework applies any directory lookup dialing rules to the directory number. This occurs while Client Services Framework transmits the data to Cisco UC Integration for Microsoft Office Communicator.
5. If the directory number is not in the Client Services Framework cache, Client Services Framework searches LDAP for the number that is returned after the directory number is processed by the directory lookup dialing rules.
6. LDAP sends the LDAP data for any matches back to Client Services Framework, including data such as other phone numbers, and a URI of a photo of the caller.
7. Client Services Framework updates the data for the contact and sends the updated data to Cisco UC Integration for Microsoft Office Communicator.
8. Cisco UC Integration for Microsoft Office Communicator updates the conversation window. For example, at this point a photo of the caller might be displayed as the photoURI field from LDAP is passed to Cisco UC Integration for Microsoft Office Communicator by Client Services Framework.

## Outgoing Calls to Contacts Who Are Enabled for OCS

When a user places a call to a contact who is enabled for OCS, the following events occur:

1. Cisco UC Integration for Microsoft Office Communicator 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. If the contact is not in the Client Services Framework cache, Client Services Framework searches LDAP for details of the party to be called.
3. LDAP sends data back to Client Services Framework.

4. Client Services Framework sends data about the contact back to Cisco UC Integration for Microsoft Office Communicator. If the contact has several numbers, Cisco UC Integration for Microsoft Office Communicator displays a window from which the user selects the number to call. If the contact has only one number, Cisco UC Integration for Microsoft Office Communicator places the call.

5. Client Services Framework applies any directory lookup dialing rules to the number to be called.

6. Client Services Framework searches LDAP for the number that is returned after the directory lookup dialing rules are applied.

7. Client Services Framework applies the application dialing rules and sends the number to Cisco Unified Communications Manager.

8. Cisco Unified Communications Manager places the call.

**Outgoing Calls to Contacts Who Are Not Enabled for OCS**

When a user places a call to a contact who is not enabled for OCS, the following events occur:

1. Cisco UC Integration for Microsoft Office Communicator sends the display name for the contact to Client Services Framework.

2. If the contact is not in the Client Services Framework cache, Client Services Framework searches LDAP for the contact associated with the display name. The operator for this search is *contains* rather than *equals*.

3. If the LDAP search returns more than one contact, Cisco UC Integration for Microsoft Office Communicator displays a window from which the user selects the number to call. If the contact has only one number, Cisco UC Integration for Microsoft Office Communicator places the call.

4. Client Services Framework applies any directory lookup dialing rules to the number to be called.

5. Client Services Framework searches LDAP for the number that is returned after the directory lookup dialing rules are applied.

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.

**Outgoing Calls to Microsoft Outlook Contacts**

When a user places a call to a Microsoft Outlook contact, the following events occur:

1. The user drags a contact from the Microsoft Office Communicator to the Cisco UC pane.

2. Cisco UC Integration for Microsoft Office Communicator searches the Microsoft Outlook contacts for a user that matches the display name. If a contact is found, then the contact is added to the Client Services Framework cache.

3. Client Services Framework applies any directory lookup dialing rules to the phone numbers of the contact.

4. Client Services Framework searches LDAP for the number that is returned after the directory lookup dialing rules are applied.
5. Client Services Framework applies the application dialing rules and sends the number to Cisco Unified Communications Manager.
6. Cisco Unified Communications Manager places the call.

How to Configure Cisco UC Integration for Microsoft Office Communicator Clients for Secure Access to Cisco Unified MeetingPlace

- Configuring Secure Access to Cisco Unified MeetingPlace, page 3-18
- Downloading the IIS Certificate from Cisco Unified MeetingPlace, page 3-18

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:

What To Do Next
Download the IIS Certificate from Cisco Unified MeetingPlace, page 3-18

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 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 3-21

How to Configure Cisco UC Integration for Microsoft Office Communicator Clients to Enable Secure Voicemail Access

- Configuring Secure Voicemail Access to a Cisco Unity Server, page 3-19
- Configuring Secure Voicemail Access to a Cisco Unity Connection Server, page 3-20

Configuring Secure Voicemail Access to a Cisco Unity Server

Procedure

Step 1 Set the following registry values:

<table>
<thead>
<tr>
<th>Value Name</th>
<th>Set Value to</th>
</tr>
</thead>
<tbody>
<tr>
<td>VVM_SystemServer_0</td>
<td>The IP address of the Cisco Unity Server</td>
</tr>
<tr>
<td>VVM_SystemServer_VmwsProtocol_0</td>
<td>HTTPS</td>
</tr>
<tr>
<td>VVM_SystemServer_VmwsPort_0</td>
<td>443</td>
</tr>
</tbody>
</table>

1. The last character in the value names described in this table can be 0 or 1 depending on whether the server is a primary or secondary server.

Step 2 Download a certificate for secure access to Cisco Unity. For more information, see Downloading the IIS Certificate from Cisco Unity, page 3-19.

Step 3 Install the certificate on the client computer, see Enabling LDAP Over SSL, page 3-11.

Downloading the IIS Certificate from Cisco Unity

Procedure

Step 1 Start a browser on the Cisco Unity server.

Step 2 Use the HTTPS protocol to access the URL of the Cisco Unity server.

You can access the URL structured as follows:

https://<localhost>
For example, access:
https://unityserver/

Step 3 Select View Certificate on the security dialog box.
Step 4 Select the Details tab.
Step 5 Select Copy to File.
Step 6 Select DER encoded binary X.509 (.CER), then select Next.
Step 7 Enter a filename for the certificate, then select Next.
Step 8 Verify the details of your certificate on the Completing the Certificate Export Wizard screen, then select Finish.

What To Do Next
Enabling LDAP Over SSL, page 3-11

Configuring Secure Voicemail Access to a Cisco Unity Connection Server

Procedure

Step 1 Set the following registry values:

<table>
<thead>
<tr>
<th>Value Name</th>
<th>Set Value to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>VVM_Mailstore_Server_0(^1)</td>
<td>The IP address of the Cisco Unity Connection server</td>
</tr>
<tr>
<td>VVM_Mailstore_ImapProtocol_0</td>
<td>TLS</td>
</tr>
<tr>
<td>VVM_Mailstore_ImapPort_0</td>
<td>7993</td>
</tr>
<tr>
<td>VVM_Mailstore_EncryptedConnection</td>
<td>True</td>
</tr>
</tbody>
</table>

\(^1\) The last character in the first three value names described in this table can be 0 or 1 depending on whether the server is a primary or secondary server.

Step 2 Download a certificate for secure access to Cisco Unity Connection. For more information, see Downloading the Tomcat Certificate from Cisco Unity Connection, page 3-20.
Step 3 Install the certificate on the client computer, see Enabling LDAP Over SSL, page 3-11.

Downloading the Tomcat Certificate from Cisco Unity Connection

Procedure

Step 1 Select Security > Certificate Management in Cisco Unified Operating System Administration.
Step 2 Find the Tomcat certificate.
Step 3 Select the tomcat.der link.
Step 4  Select **Download**, then save the tomcat.der file to your computer.

**What To Do Next**

*Enabling LDAP Over SSL, 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 key value name to specify the folder where the certificates are stored.

### Related Topics

- *Specifying Security Certificate Value Names, page 3-6*