Planning the Installation

Installation Methods

This guide covers the following installation methods for Cisco Unified Communications Manager and the IM and Presence Service:

<table>
<thead>
<tr>
<th>Installation Method</th>
<th>Description</th>
</tr>
</thead>
</table>
| Basic Install of Cluster    | This method contains the typical installation of a Cisco Unified Communications Manager and IM and Presence Service cluster. In this method, you must install the publisher node first, and then add and install your subscriber nodes. Basic Installation includes the following custom cases:  
  • Apply a Patch During an Upgrade—If a newer version exists than the image that you are installing, you can apply a patch to your install image and upgrade to the newer version. This option is available for Unified Communications Manager only.  
  • Pre-installed Software—If you have a new server with either Unified Communications Manager or IM and Presence Service software pre-installed (for example, Cisco Business Edition) you can configure the pre-installed software. |
| Touchless Install of Cluster| Touchless installation allows you to complete a full cluster installation for Unified Communications Manager and IM and Presence Service in one seamless process. Once you provide the server details for all cluster nodes and start the installation, the system installs software on all cluster nodes dynamically, without manual intervention from the administrator. This method is particularly useful if you have a large cluster to install. |
### Topology Options

This section provides an overview of the system topology and describes the relationship between the types of nodes in the topology.

#### Clusters

Clusters provide a mechanism for distributing call processing, presence status, and database replication among multiple servers. They provide transparent sharing of resources and features and enable system scalability.

A cluster comprises a set of Unified Communications Manager nodes and IM and Presence nodes that run compatible software versions.

#### Publisher Nodes and Subscriber Nodes

Within a cluster, there is a database publisher for each type of node that you install.

When you install Unified Communications Manager, the installation wizard prompts you to specify whether the node you are installing is the first node in the cluster. The first Unified Communications Manager node that you install becomes the publisher node, because it publishes the voice and video database to the other Unified Communications Manager nodes in the cluster. All subsequent nodes in the cluster are called subscriber nodes. Each subscriber node must be associated with the publisher node. You must set up all subscriber nodes in the system topology on the publisher node before you install the software on the subscriber nodes.

When you install IM and Presence nodes, the first node that you install functions as the server for the IM and Presence database. Because this node publishes the database for all of the IM and Presence nodes in the cluster, it is referred to as the IM and Presence database publisher; however, you must install this and all other IM and Presence nodes as subscribers of the Unified Communications Manager publisher node. As with other subscriber nodes, you must add these in the system topology before you install the software.

#### Topology Options

When installing your cluster, you must decide on the topology that you want to deploy. For example:

- The number of cluster nodes required.
- Whether you will install all cluster nodes in a single location, or if you will install your nodes in separate geographic sites connected via a WAN in order to provide geographic redundancy.
- For IM and Presence deployments, install a standard deployment or an IM and Presence Central Cluster deployment.

Cluster Topology for IM and Presence

If you are deploying the IM and Presence Service, you must decide before you begin the installation whether you want a Standard Deployment (IM and Presence Service on Unified Communications Manager) or an IM and Presence Central Cluster deployment. Refer to the following table for a description of each option.

<table>
<thead>
<tr>
<th>IM and Presence Deployment</th>
<th>Description</th>
</tr>
</thead>
</table>
| Standard Deployment (Decentralized) | The IM and Presence cluster is installed on the same servers as the Unified Communications Manager telephony cluster. The IM and Presence cluster shares a platform and many of the same services as the telephony cluster. This option requires a 1x1 mapping of telephony clusters to IM and Presence clusters. Basic installations follow this process:  
1. Install the Unified Communications Manager publisher node  
2. Install the Unified Communications Manager subscriber nodes  
3. Install the IM and Presence Service publisher node  
4. Install the IM and Presence Service subscriber nodes  
For touchless installations, you can install all Unified Communications Manager and IM and Presence Service cluster nodes in a single process. |
| Centralized Deployment | The IM and Presence Service central cluster is installed separately from your telephony cluster and may be located on completely different hardware servers. This deployment removes the 1x1 mapping requirement between telephony clusters and IM and Presence clusters. This allows you to scale your telephony deployment and IM and Presence deployment separately. For basic installations:  
1. Install a local Unified Communications Manager publisher node in the central cluster. This node is not a part of your telephony deployment. The node handles functions like database and user provisioning for the central cluster.  
2. Install the IM and Presence Service database publisher node.  
3. Install any IM and Presence subscriber nodes.  
For touchless installations, you can install your local Unified Communications Manager publisher node and your IM and Presence Service central cluster in a single process. However, your telephony cluster must be installed separately. |
Requirements and Limitations

The following sections provide information about the requirements that your system must meet, and limitations that apply when you install or upgrade Unified Communications Manager or Instant Messaging and Presence service.

⚠️ Caution

Do not modify any of the Instant Messaging and Presence Service server entries on the Application Server or Server configuration pages of the Cisco Unified CM Administration interface. The Instant Messaging and Presence Service upgrade process automatically updates these entries on the Unified Communications Manager cluster during the final stages (switch version) of the upgrade process.

For upgrades from Release 8.x or 9.x to Release 10.x or later, any manual modification of these entries during the upgrade process will result in data migration failures between Instant Messaging and Presence Service and Unified Communications Manager. If such failures occur, you must restart the entire upgrade process for both Unified Communications Manager and Instant Messaging and Presence Service clusters.

Subnet Limitations

Do not install Unified Communications Manager in a large Class A or Class B subnet that contains a large number of devices.

Cluster Size

The number of Unified Communications Manager subscriber nodes in a cluster cannot exceed 4 subscriber nodes and 4 standby nodes, for a total of 8 subscribers. The total number of servers in a cluster, including the Unified Communications Manager publisher node, TFTP server, and media servers, cannot exceed 21.

The maximum number of Instant Messaging and Presence nodes in a cluster is 6.

For more information, see “Cisco Collaboration Solutions Design Guidance” at http://www.cisco.com/go/ucsrnd

IP Address Requirements

A complete collaboration solution relies on DNS in order to function correctly for a number of services and thus requires a highly available DNS structure in place. If you have a basic IP telephony deployment and do not want to use DNS, you can configure Unified Communications Manager and IM and Presence Service to use IP addresses rather than hostnames to communicate with gateways and endpoint devices.

You must configure the server to use static IP addressing to ensure that the server obtains a fixed IP address. Using a static IP address also ensures that Cisco Unified IP Phones can register with the application when you plug the phones into the network.

DNS requirements

Note the following requirements:
• Mixed-mode DNS deployments not supported—Cisco does not support mixed-mode deployments. Both Unified Communications Manager and Instant Messaging and Presence must either use or not use DNS.

• If your deployment uses DNS—Unified Communications Manager and Instant Messaging and Presence should use the same DNS server. If you use different DNS servers between Instant Messaging and Presence and Unified Communications Manager, it is likely to cause abnormal system behavior.

• If your deployment does not use DNS, will need to edit the following Host Name/IP Address fields:
  • Server—In the Cisco Unified CM Administration Server Configuration window, set IP addresses for your cluster nodes.
  • IM and Presence UC Service—In the Cisco Unified CM Administration UC Service Configuration window, create an IM and Presence UC service that points to the IP address of the IM and Presence database publisher node
  • CCMCIP Profiles—In the Cisco Unified CM IM and Presence Administration CCMCIP Profile Configuration window, point any CCMCIP profiles to the IP address of the host.

• Multinode considerations—If you are using the multinode feature in Instant Messaging and Presence, see the section regarding multinode deployments in the Configuration and Administration of IM and Presence on Cisco Unified Communications Manager for DNS configuration options.

Firewall Requirements

Ensure that you configure your firewall so that connections to port 22 are open, and are not throttled. During the installation of IM and Presence subscriber nodes, multiple connections to the Unified Communications Manager publisher node are opened in quick succession. Throttling these connections could lead to a failed installation.

Platform Requirements

This section provides information about the platform requirements that you must meet before you can deploy Unified Communications Manager and the IM and Presence Service on virtual machines.

Version Requirements

All servers in a cluster must run the same release of Unified Communications Manager. The only exception is during a cluster software upgrade, during which a temporary mismatch is allowed.

If you are installing IM and Presence nodes, the software version of the first IM and Presence node (the IM and Presence database publisher node) must match the first three numbers of the software version installed on the Unified Communications Manager publisher node. For example, IM and Presence Service software version 10.0.1.10000-1 is compatible with Unified Communications Manager software version 10.0.1.30000-2. Refer to the following table for sample Unified Communications Manager versions and IM and Presence Service versions that are compatible. The bolded numbers must match.
Table 1: Examples of Compatible Unified Communications Manager and IM and Presence Service Versions

<table>
<thead>
<tr>
<th>Sample Unified Communications Manager Version</th>
<th>Example of Compatible IM and Presence Service Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.1.30000-2</td>
<td>10.0.1.10000-1</td>
</tr>
<tr>
<td>10.5.1.10000-7</td>
<td>10.5.1.10000-9</td>
</tr>
<tr>
<td>10.5.2.10000-5</td>
<td>10.5.2.10000-9</td>
</tr>
</tbody>
</table>

After you install the first IM and Presence node, the software version of any IM and Presence subscriber nodes that you install must match all five version numbers of the first IM and Presence node. For example, if the IM and Presence database publisher node is at version 10.0.1.10000-1, then all IM and Presence subscriber nodes must also be 10.0.1.10000-1.

Software Restrictions

You cannot install or use third-party or Windows-based software applications. The system can upload and process only software that Cisco Systems approves. You must perform all software installations and upgrades using Cisco Unified Communications Operating System Administration.

For information about software compatibility for IM and Presence nodes, see the *Hardware and Software Compatibility Information for IM and Presence Service on Cisco Unified Communications Manager*.

For information about software compatibility for Unified Communications Manager, see the *Cisco Unified Communications Manager Software Compatibility Matrix*.

Username and Password Requirements

During the installation, you must specify the following usernames and passwords:

- Administrator Account user name and password
- Application User name and password
- Security password

Administrator Account

You use the Administrator Account user name and password to log in to the following areas:

- Cisco Unified Communications Operating System Administration
- Disaster Recovery System
- Command Line Interface

To specify the Administrator Account user name and password, follow these guidelines:

- Administrator Account user name—The Administrator Account user name must start with an alphabetic character and can contain alphanumeric characters, hyphens and underscores.
- Administrator Account password—The Administrator Account password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores.
You can change the Administrator Account password or add a new Administrator account by using the command line interface. For more information, see the Command Line Interface Reference Guide for Cisco Unified Communications Solutions.

**Application User**

When you install Unified Communications Manager, you must enter an Application User name and password. You use the Application User name and password to access applications that are installed on the system, including the following areas:

- Cisco Unified CM Administration
- Cisco Unified Serviceability
- Real Time Monitoring Tool
- Cisco Unified Reporting

To specify the Application User name and password, follow these guidelines:

- Application User username - The Application User username must start with an alphabetic character and can contain alphanumeric characters, hyphens, and underscores.
- Application User password - The Application User password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores.

> **Caution**

Do not use the system application name as the Application User name. Using a system application name causes the installation to fail with an unrecoverable error during the installation of the database.

System application names are:

- CCMSysUser
- WDSysUser
- CCMQRTSysUser
- IPMASysUser
- WDSecureSysUser
- CCMQRTSecureSysUser
- IPMASecureSysUser
- TabSyncSysUser
- CUCService

You can change the Application User name and password by using the command line interface. For more information, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

**Security Password**

The Security password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores.
Password Recommendations

The installation wizard ensures that you enter a strong password. To create a strong password, follow these recommendations:

• Mix uppercase and lowercase letters.
• Mix letters and numbers.
• Include special symbols.
• Remember that longer passwords are stronger and more secure than shorter ones.

Avoid the following types of passwords:

• Do not use recognizable words, such as proper names and dictionary words, even when combined with numbers.
• Do not invert recognizable words.
• Do not use word or number patterns, such as aaabbb, qwerty, zyxvuts, 123321, and so on.
• Do not use recognizable words from other languages.
• Do not use personal information of any kind, including birthdays, postal codes, names of children, or pets, and so on.

Installation Time Requirements

Time Requirements for Unified Communications Manager

The entire installation process, excluding pre- and post-installation tasks, takes 45 to 90 minutes, depending on your server type.

Time Requirements for IM and Presence Nodes

The entire IM and Presence installation process, excluding pre- and post-installation tasks, takes approximately 45 to 90 minutes per server, depending on your server type.

Licensing Requirements

The following sections provide information about the licensing requirements for Unified Communications Manager and the Instant Messaging and Presence

Cisco Unified Communications Manager License Requirements

Use the Cisco Prime License Manager to allocate and monitor the licenses for Unified Communications Manager, its applications, and endpoints. See the Cisco Prime License Manager User Guide for information about generating and installing licenses.
IM and Presence license requirements

The Instant Messaging and Presence Service does not require a server license or software version license. However, you must assign users and enable the Instant Messaging and Presence Service for each assigned user.

Note

With the Jabber for Everyone offer, no end user licenses are required to enable IM and Presence functionality. For more information, see “Jabber for Everyone Quick Start Guide”.

You can assign Instant Messaging and Presence on a per user basis, regardless of the number of clients you associate with each user. When you assign Instant Messaging and Presence to a user, this enables the user to send and receive IMs and availability updates. If users are not enabled for Instant Messaging and Presence, they will not be able to log in to the Instant Messaging and Presence server to view the availability of other users, send or receive IMs, and other users will not see their availability status.

You can enable a user for Instant Messaging and Presence using any of the following options:

- The End User Configuration window in Unified Communications Manager. For more information, see Administration Guide for Cisco Unified Communications Manager.
- The Bulk Administration Tool (BAT)
- Assign Instant Messaging and Presence to a feature group template which you can reference from the Quick User/Phone Add window in Unified Communications Manager.

For more information, see the Instant Messaging and Presence chapter in the Cisco Unified Communications Manager Features and Services Guide.

Instant Messaging and Presence capabilities are included within both User Connect Licensing (UCL) and Cisco Unified Workspace Licensing (CUWL). Instant Messaging and Presence capabilities can also be acquired for users that are not Unified Communications Manager IP Telephony users through the Jabber for Everyone Offer. For more information, see Jabber for Everyone Quick Start Guide.

Required Installation Information

When you install either Unified Communications Manager or the IM and Presence Service on a server, the installation process requires you to provide specific information. You can provide this information manually during the installation process or you can provide it using an answer file. For each server that you install in a cluster, you must gather this information before you begin the installation process.

The following table lists the information that you must gather before you begin the installation.

<table>
<thead>
<tr>
<th>Required Installation Information</th>
</tr>
</thead>
</table>

Note

Because some of the fields are optional, they may not apply to your configuration. For example, if you decide not to set up an SMTP host during installation, the parameter still displays, but you do not need to enter a value.

You cannot change some of the fields after the installation without reinstalling the software, so be sure to enter the values that you want. The last column in the table shows whether you can change a parameter after installation, and if you can, it provides the appropriate menu path or Command Line Interface (CLI) command.
We recommend that you make copies of this table and record your entries for each server in a separate table, even if you are planning to use the DMABackupInfo.inf file to configure your system.

Table 2: Required Installation Information

<table>
<thead>
<tr>
<th>Configuration data</th>
<th>Description</th>
<th>Editable after installation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Administrator Credentials</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administrator Login</td>
<td>Specifies the name that you want to assign to the Administrator account.</td>
<td>No</td>
</tr>
<tr>
<td>Administrator Password</td>
<td>Specifies the password for the Administrator account.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>After installation, you can create additional administrator accounts, but you cannot change the original administrator account user ID.</td>
<td>CLI: <code>set password user admin</code></td>
</tr>
<tr>
<td><strong>Application User Credentials</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application User Username</td>
<td>Specifies the user ID for applications installed on the system.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>CLI: <code>utils reset_application_ui_administrator_name</code></td>
<td></td>
</tr>
<tr>
<td>Application User Password</td>
<td>Specifies the password for applications on the system.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>CLI: <code>utils reset_application_ui_administrator_password</code></td>
<td></td>
</tr>
<tr>
<td><strong>Security Password</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security password for Unified Communications Manager</td>
<td>Servers in the cluster use the security password to communicate with one another. Set this password on the Unified Communications Manager publisher node, and enter it when you install each additional node in the cluster, including IM and Presence nodes.</td>
<td>Yes. You can change the security password on all nodes in the cluster using the following command: CLI: <code>set password user security</code></td>
</tr>
<tr>
<td><strong>Certificate Information</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organization</td>
<td>Used to create the Certificate Signing Request.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>CLI: <code>set web-security [orgunit] [orgname] [locality] [state] [country]</code></td>
<td></td>
</tr>
<tr>
<td>Configuration data</td>
<td>Description</td>
<td>Editable after installation</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>Unit</td>
<td>Used to create the Certificate Signing Request.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>CLI: <code>set web-security [orgunit] [orgname] [locality] [state] [country]</code></td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td>Used to create the Certificate Signing Request.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>CLI: <code>set web-security [orgunit] [orgname] [locality] [state] [country]</code></td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Used to create the Certificate Signing Request.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>CLI: <code>set web-security [orgunit] [orgname] [locality] [state] [country]</code></td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td>Used to create the Certificate Signing Request.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>CLI: <code>set web-security [orgunit] [orgname] [locality] [state] [country]</code></td>
<td></td>
</tr>
<tr>
<td>(Optional) SMTP</td>
<td>Specifies the name of the SMTP host that is used for outbound email. You must fill in this field if you plan to use electronic notification. If not, you can leave it blank.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>• In Cisco Unified Communications Operating System Administration: select Settings &gt; SMTP and enter the IP address or Hostname in the SMTP Host Field.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CLI: <code>set smtp [host]</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NIC Interface Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIC Speed</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Configuration data</td>
</tr>
<tr>
<td>--------------------</td>
</tr>
</tbody>
</table>
| NIC Duplex         | If you do not enable automatic negotiation of the ethernet Network Interface Card (NIC) duplex setting, you must select the NIC duplex setting (either Full or Half). | Yes, CLI: `set network nic eth0 {auto | {en| dis}} {speed| {10| 100}} {duplex half| {half| full}}`  
Note: 1000BASE-T can only be enabled via auto-negotiation.  
Note: Virtual machines do not support this command. |
| MTU Size            | The maximum transmission unit (MTU) represents the largest packet, in bytes, that this host will transmit on the network.  
The value must not exceed the lowest MTU size that is configured on any link in your network.  
Default: 1500 bytes | Yes, CLI: `set network mtu [size]` |

**Network Information**

**DHCP**  
(Dynamic Host Configuration Protocol)  
Select **Yes** if you want to use DHCP to automatically configure the network settings on your server.  
If you select **No**, you must enter a hostname, IP Address, IP Mask, Gateway, and DNS configuration.  

Note:  
**Yes**.  
- In Cisco Unified Operating System Administration: select **Settings > IP > Ethernet**  
- CLI: `set network dhcp eth0 [enable]`  
- CLI: `set network dhcp eth0 disable [node_ip] [net_mask] [gateway_ip]`
<table>
<thead>
<tr>
<th>Configuration data</th>
<th>Description</th>
<th>Editable after installation</th>
</tr>
</thead>
</table>
| Hostname           | If DHCP is set to No, you must enter a hostname for this machine. | Yes; for Unified Communications Manager nodes, choose one of the following:  
  
  • In Cisco Unified Communications Operating System Administration, select *Settings > IP > Ethernet*  
  
  • CLI: `set network hostname`
  
  You will be prompted to enter the parameters.

  To change the hostname on a IM and Presence server, see *Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service.* |
| IP Address         | If DHCP is set to No, you must enter the IP address of this machine. | Yes; for Unified Communications Manager nodes, choose one of the following:  
  
  • In Cisco Unified Communications Operating System Administration, select *Settings > IP > Ethernet*  
  
  • CLI: `set network IP eth0 [ip-address] [ip-mask]`

  To change the IP address on a IM and Presence server, see *Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service.* |
| IP Mask            | If DHCP is set to No, you must enter the IP subnet mask of this machine. The subnet mask together with the IP address defines the network address and the host address. The subnet mask must use the following format: 255.255.255.0 | Yes

  • In Cisco Unified Communications Operating System Administration, select *Settings > IP > Ethernet*  
  
  • CLI: `set network IP eth0 [ip-address] [ip-mask]` |
| Gateway Address    | If DHCP is set to No, you must enter the gateway address. | Yes

  • In Cisco Unified Communications Operating System Administration, select *Settings > IP > Ethernet*  
  
  • CLI: `set network gateway [addr]` |
<p>| (Optional) DNS     |                                      |                                      |</p>
<table>
<thead>
<tr>
<th>Configuration data</th>
<th>Description</th>
<th>Editable after installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Primary</td>
<td>If you have a Domain Name Server (DNS), IM and Presence contacts this DNS server first when attempting to resolve hostnames.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>CLI: set network dns primary [address]</td>
<td></td>
</tr>
<tr>
<td>DNS Secondary</td>
<td>When a primary DNS server fails, IM and Presence will attempt to connect to the secondary DNS server.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>CLI: set network dns secondary [address]</td>
<td></td>
</tr>
<tr>
<td>Domain</td>
<td>Represents the name of the domain in which this machine is located.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>CLI: set network domain [name]</td>
<td></td>
</tr>
<tr>
<td><strong>Timezone</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time Zone</td>
<td>Reflects the local time zone and offset from Greenwich Mean Time (GMT). Select the time zone that most closely matches the location of your machine.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>CLI: set timezone [zone]</td>
<td></td>
</tr>
<tr>
<td><strong>Network Time Protocol</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTP Server IP Address</td>
<td>During installation of the IM and Presence publisher node, you must specify the IP address of an external Network Time Protocol (NTP) server. Cisco recommends that you use the Unified Communications Manager publisher node as the NTP server.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>In Cisco Unified Communications Operating System Administration, select Settings &gt; NTP Servers</td>
<td></td>
</tr>
</tbody>
</table>

## Export Restricted and Export Unrestricted Software

This release of Unified Communications Manager and Instant Messaging and Presence supports an export unrestricted (XU) version, in addition to the export restricted (K9) version.
Unrestricted versions of software are intended only for a very specific set of customers who do not want various security capabilities; unrestricted versions are not intended for general deployments.

Export unrestricted versions differs from restricted versions as follows:

- Encryption of user payload (information exchange) is not supported.
- External SIP interdomain federation with Microsoft OCS/Lync or AOL is not supported.
- After you install an unrestricted release, you can never upgrade to a restricted version. A fresh install of a restricted version on a system that contains an unrestricted version is also not supported.
- All nodes within a single cluster must be in the same mode. For example, Unified Communications Manager and Instant Messaging and Presence in the same cluster must either all be in unrestricted mode or all be in restricted mode.
- IP phone security configurations are modified to disable signaling and media encryption (including encryption provided by the VPN phone feature).

Be aware that after you install an unrestricted release, you can never upgrade to a restricted version. You are not allowed to perform a fresh installation of a restricted version on a system that contains an unrestricted version.

For all Graphical User Interfaces (GUIs) and Command Line Interfaces (CLIs), the Administrator can view the product version (restricted or export unrestricted).

The following table describes the GUI items that are not available for the export unrestricted version of Instant Messaging and Presence.

<table>
<thead>
<tr>
<th>GUI Item</th>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco Unified CM Administration</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>VPN Configuration</strong></td>
<td>Advanced Features &gt; VPN</td>
<td>This menu and its options are not available.</td>
</tr>
<tr>
<td><strong>Phone Security Profile</strong></td>
<td>System &gt; Security &gt; Phone Security Profile</td>
<td>The <strong>Device Security Mode</strong> is set to <strong>Non Secure</strong> and is not configurable.</td>
</tr>
</tbody>
</table>

<p>| <strong>Cisco Unified CM IM and Presence Administration</strong> |                           |                                                                            |</p>
<table>
<thead>
<tr>
<th>GUI Item</th>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Settings</td>
<td>System &gt; Security &gt; Settings</td>
<td>• You cannot check the Enable XMPP Client to IM/P Service Secure Mode setting. &lt;br&gt;• You cannot check the Enable XMPP Router-to-Router Secure Mode setting. &lt;br&gt;• You cannot check the Enable Web Client to IM/P Service Secure Mode setting. &lt;br&gt;• The option to set SIP intra-cluster Proxy-to-Proxy Transport Protocol to TLS have been removed.</td>
</tr>
<tr>
<td>Service Parameter Configuration for Cisco SIP Proxy service</td>
<td>System &gt; Service Parameters and choose Cisco SIP Proxy as the Service</td>
<td>• All TLS options have been removed for the Transport Preferred Order parameter. &lt;br&gt;• The TLS option have been removed from the SIP Route Header Transport Type parameter.</td>
</tr>
<tr>
<td>SIP Federated Domains</td>
<td>Presence &gt; Inter-domain Federation &gt; SIP Federation</td>
<td>When you configure interdomain federation to OCS/Lync, you will receive warning popup to indicate that it is only possible to directly federate with another OCS/Lync within the enterprise. Interdomain federation to OCS/Lync outside the enterprise is not supported in unrestricted mode.</td>
</tr>
<tr>
<td>XMPP Federation Settings</td>
<td>Presence &gt; Inter-domain Federation &gt; XMPP Federation &gt; Settings</td>
<td>You cannot configure the security mode; It is set to NO TLS.</td>
</tr>
<tr>
<td>Proxy Configuration Settings</td>
<td>Presence &gt; Routing &gt; Settings</td>
<td>You cannot set any TLS or HTTPS listeners as the preferred proxy listener.</td>
</tr>
</tbody>
</table>