Installation Planning

The following sections provide information about the installation requirements.

- Requirements and Limitations, on page 1
- Licensing Requirements, on page 8
- Required Installation Information, on page 11
- Export Restricted and Export Unrestricted Software, on page 15

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 IM and Presence Service serivce.

Caution Do not modify any of the IM and Presence Service Service server entries on the Application Server or Server configuration pages of the Cisco Unified CM Administration interface. The IM and Presence Service 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 IM and Presence Service Service and Unified Communications Manager. If such failures occur, you must restart the entire upgrade process for both Unified Communications Manager and IM and Presence Service Service clusters.

Limitations

This section describes the limitations that apply when you install or upgrade Unified Communications Manager or the IM and Presence Service Service.

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 IM and Presence Service nodes in a cluster is 6.

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

Network Requirements

This section lists the requirements that your network must meet before you can deploy Unified Communications Manager and the IM and Presence Service.

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 IM and Presence Service must either use or not use DNS.
- If your deployment uses DNS—Unified Communications Manager and IM and Presence Service should use the same DNS server. If you use different DNS servers between IM and Presence Service 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 IM and Presence Service, 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

In this release, you cannot install or run Unified Communications Manager and the IM and Presence Service directly on server hardware; you must run these applications on virtual machines.

Before you can install or upgrade the software on a virtual machine, you must:

- configure the platform
- install and configure ESXi virtualization software
- deploy the correct OVA template for the release

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.

Software Requirements

The following sections provide information about the software requirements that your deployment must meet.

Supported Versions

The following software versions apply to Release 12.0(1):

- Unified Communications Manager 12.0.1.10000-10
- IM and Presence Service Service 12.0.1.10000-12

Version Mismatches

This release offers two main deployment options for this release of Unified Communications Manager and the IM and Presence Service Service:

- Standard Deployments—Both Unified Communications Manager and the IM and Presence Service Service must be running the above 12.0(1) version for your deployment to be supported. A version mismatch is not supported.
- Centralized Deployments of IM and Presence Service Service—If you have the Centralized Deployment option configured on theIM and Presence Service Service, then within the IM and Presence Service central cluster, both the Unified Communications Manager instance and the IM and Presence Service Service must be running a 12.0(1) version. However, the telephony cluster that the central cluster connects to does not have to be running a 12.0(1) version.

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*.

Browser Requirements

Unified Communications Manager and the IM and Presence Service both provide interfaces that you can use to configure and manage the system. You can access the interfaces by using the browsers and operating systems listed in the following table. Cisco does not support or test other browsers.

Table 1: Supported Browsers and Operating Systems

You can use this browser...	...with one of these operating systems
Google Chrome (latest browser version)	Microsoft Windows 10 (64 bit)
Microsoft Internet Explorer 11	• Microsoft Windows 10 (64 bit) • Microsoft Windows 8.1 (64 bit) • Microsoft Windows 7 (64 bit)
Microsoft Edge	Microsoft Windows 10 (32 bit/64 bit)
Mozilla Firefox (latest browser version)	Microsoft Windows 10 (64 bit)
Safari	Apple Mac OS 10.x (or newest OS release available)

User Name and Password Requirements

The following sections provide information about the account names and passwords that you must configure for Unified Communications Manager and the IM and Presence Service.

Accounts and Passwords for Unified Communications Manager

User Name and Password Requirements

Note The system checks your passwords for strength. See topics related to password considerations for guidelines on creating a strong password.

During the installation, you must specify the following user names and passwords:

- Administrator Account user name and password

- Application User name and password
- Security password

Administrator Account User Name and Password

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 Name and Password

When you install Cisco 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 name - The Application User name 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

During the installation, you must specify a security password. Unified Communications Manager systems use this password to authorize communications between nodes in the cluster, including IM and Presence Service nodes. The security password must be identical on all nodes in the cluster.

The Security password must be minimum six characters long and can contain alphanumeric characters, hyphens, and underscores.

If you are enabling FIPS, Common Criteria, or Enhanced Security mode on the cluster, ensure that the security password is minimum 14 characters.

If your security password is less than 14 characters:

- Upgrades from any previous versions of FIPS enabled Unified Communications Manager to Release 12.5 or later aborts with an error message.
- You must set the security password to a minimum of 14 characters to resume the upgrade process.

Accounts and Passwords for IM and Presence Service

Required passwords

During installation of the IM and Presence Service, you must specify the following usernames and passwords:

Administrator account username and password

During installation, you must create an Administrator Account username and password to log into the following areas:

- Cisco Unified Operating System Administration interface
- Disaster Recovery System Administration interface
- Command Line Interface (CLI)

The Administrator login must start with an alphabetic character, be at least six characters long, and can contain alphanumeric characters, hyphens, and underscores.

If you lose the Administrator password and cannot access the system, you can recover the Administrator password in CiscoUnified Communications Operating System Administration.

If you need to reset the Administrator password, use the CLI.

Application username and password

During the installation of Unified Communications Manager, you are prompted to create an Application User name and password. Use this same Application User name and password when you sign into the CiscoUnified CM IM and Presence Administration interface.

If you need to reset the Application User password, use the CLI.

InterCluster Peer-User and Admin-CUMA Application User Roles Deprecated

The application user group roles InterCluster Peer-User and Admin-CUMA are deprecated from release 10.0(1). Any application users with these roles configured in releases 8.x or 9.x have the roles removed during an upgrade to any 10.x release. After the upgrade the administrator must configure appropriate roles for these users.

Note For intercluster to function correctly, the AXL user defined on the IM and Presence Service user interface (**Presence** > **Inter-Clustering**) must have a Standard AXL API Access role associated with it on the Unified Communications Manager application user page.

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, zyxwvuts, 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 IM and Presence Service

Note As of Unified Communications Manager Release 12.0(1), Smart Licensing replaces Prime License Manager. Smart Licensing requires you to have a Smart Account created and configured before you upgrade or migrate the Unified Communications Manager server.

Several deployment options through which Unified Communications Manager can connect to Cisco Smart Software Manager or Cisco Smart Software Manager satellite are:

- Direct—Unified Communications Manager sends usage information directly over the internet. No additional components are needed.
- Cisco Smart Software Manager satellite—Unified Communications Manager sends usage information to an on-premise Smart Software Manager. Periodically, an exchange of information is performed to keep the databases in synchronization. For more information on installation or configuration of the Smart Software Manager satellite, go to this URL: https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html.

  Note Cisco Smart Software Manager satellite is an on-premises collector similar to standalone Prime License Manager.

- Proxy Server—Unified Communications Manager sends usage information over the internet through a proxy server.

Cisco Unified Communications Manager License Requirements

Cisco Smart Software Licensing is a new way of thinking about licensing. It adds flexibility to your licensing and simplifies it across the enterprise. It also delivers visibility into your license ownership and consumption.

Cisco Smart Software Licensing helps you to procure, deploy, and manage licenses easily where devices self-register and report license consumption, removing the need for product activation keys (PAK). It pools license entitlements in a single account and allows you to move licenses freely through the network, wherever you need them. It is enabled across Cisco products and managed by a direct cloud-based or mediated deployment model.

The Cisco Smart Software Licensing service registers the product instance, reports license usage, and obtains the necessary authorization from Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Cisco Smart Software Manager replaces Prime License Manager in Unified Communications Manager Release 12.0(1) and later versions. Cisco Prime License Manager is no longer used as of Release 12.0(1) and no longer appears in the Installed Applications pre-login screen.

If you have enabled the mixed-mode prior to upgrade and have not registered to Cisco Smart Software Manager or Cisco Smart Software Manager satellite then,

- You see the warning message in the Cisco Unified CM Administration page and Cisco Unified OS Administration page as stated below:

Warning The system is currently running Mixed mode. To continue running Mixed mode, please ensure Smart Licensing registration is completed using the Registration Token received from the Smart/Virtual Account that has Allow export-controlled functionality checked.

- An alert named *SmartLicenseExportControlNotAllowed* is sent, when the Unified Communications Manager is not registered with the Registration Token.

For details on how to configure Cisco Smart Software Licensing, see "Smart Software Licensing" chapter, located within the "Configure Initial Parameters for the System" at System Configuration Guide for Cisco Unified Communications Manager.

For more details on Cisco Smart Software Manager satellite, including the *Smart Software Manager satellite Installation Guide*, see http://www.cisco.com/go/smartsatellite.

Migration of PLM Licenses to Smart Entitlement

If you are eligible to upgrade to the Smart Licensing version of the product, then you are able to initiate the migration through the License Registration Portal or Cisco Smart Software Manager. You can self-initiate this process by downloading and installing the Smart Licensing version of the software and registering the device to a Smart Account using a Registration Token. The migration of any entitlements tracked by Cisco automatically migrates to the Customers Smart Account. You will also be able to initiate the migration of unused classic PAKs to Smart Accounts for future consumption by products in Smart Mode. This process is available through the License Registration Portal or Cisco Smart Software Manager.

Unified Communications Manager 9.0x and later version of 12.0(1)

- If you are holding an active Cisco Software Support Service (SWSS) contract, then you can convert the classic licenses to smart entitlements through the Cisco Smart Software Manager at https://software.cisco.com/#SmartLicensing-LicenseConversion.

- Two types of Migration are supported:
  - PAK based—Supported for already fulfilled, partially fulfilled and unfilled PAKs
  - Device based
- Partial Conversion supports mixed environment of older and Unified Communications Manager 12.0(1) clusters.

Upgrade to Smart Entitlement

Unified Communications Manager Pre 9.0x (Device based) to 12.0(1)

You may contact Cisco Global Licensing Operations (GLO) for helping with migrating Device-based licenses to Smart Entitlement.

Customer may establish equivalent user-based licensing required by running License Count Utility (LCU). For more details, see http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/upgrade/uct/CUCM_BK_UCT_Admin_Guide/CUCM_BK_UCT_Admin_Guide_chapter_01.html.

From the LCU report, Customer may order respective quantity of Upgrade Licenses through Cisco Commerce Workspace. Beyond this, they would have to buy additional new licenses. For more details, see the Ordering Guide at http://www.cisco.com/c/en/us/partners/tools/collaboration-ordering-guides.html.

IM and Presence license requirements

The IM and Presence Service Service does not require a server license or software version license. However, you must assign users and enable the IM and Presence Service 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 IM and Presence Service on a per user basis, regardless of the number of clients you associate with each user. When you assign IM and Presence Service to a user, this enables the user to send and receive IMs and availability updates. If users are not enabled for IM and Presence Service, they will not be able to log in to the IM and Presence Service 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 IM and Presence Service 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 IM and Presence Service to a feature group template which you can reference from the **Quick User/Phone Add** window in Unified Communications Manager.

For more information, see System Configuration Guide for Cisco Unified Communications Manager.

IM and Presence Service capabilities are included within both User Connect Licensing (UCL) and Cisco Unified Workspace Licensing (CUWL). IM and Presence Service 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.

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

Configuration data	Description	Editable after installation
Administrator Credentials		
Administrator Login	Specifies the name that you want to assign to the Administrator account.	No After installation, you can create additional administrator accounts, but you cannot change the original administrator account user ID.
Administrator Password	Specifies the password for the Administrator account.	Yes CLI: **`set password user admin`**
Application User Credentials		
Application User Username	Specifies the user ID for applications installed on the system.	Yes CLI: **`utils reset_application_ui_administrator_name`**
Application User Password	Specifies the password for applications on the system.	Yes CLI: **`utils reset_application_ui_administrator_password`**
Security Password		

Configuration data	Description	Editable after installation
Security password for Unified Communications Manager	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.	Yes. You can change the security password on all nodes in the cluster using the following command: CLI: **`set password user security`**
Certificate Information		
Organization	Used to create the Certificate Signing Request.	Yes CLI: **`set web-security [orgunit] [orgname] [locality] [state] [country]`**
Unit	Used to create the Certificate Signing Request.	Yes CLI: **`set web-security [orgunit] [orgname] [locality] [state] [country]`**
Location	Used to create the Certificate Signing Request.	Yes CLI: **`set web-security [orgunit] [orgname] [locality] [state] [country]`**
State	Used to create the Certificate Signing Request.	Yes CLI: **`set web-security [orgunit] [orgname] [locality] [state] [country]`**
Country	Used to create the Certificate Signing Request.	Yes CLI: **`set web-security [orgunit] [orgname] [locality] [state]`**
(Optional) SMTP		
SMTP Location	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.	Yes • In Cisco Unified Communications Operating System Administration: select **Settings** > **SMTP** and enter the IP address or Hostname in the SMTP Host Field. • CLI: **`set smtp [host]`**

Configuration data	Description	Editable after installation
NIC Interface Settings		
NIC Speed	If you do not enable automatic negotiation of the ethernet Network Interface Card (NIC) speed, you must select the NIC speed (either 10 megabit or 100 megabit).	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.
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 **Note** The MTU setting must be the same on all nodes in a cluster.	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.	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]`**

Configuration data	Description	Editable after installation
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]`**
(Optional) DNS		

Configuration data	Description	Editable after installation
DNS Primary	If you have a Domain Name Server (DNS), IM and Presence contacts this DNS server first when attempting to resolve hostnames.	Yes CLI: **`set network dns primary [address]`**
DNS Secondary	When a primary DNS server fails, IM and Presence will attempt to connect to the secondary DNS server.	Yes CLI: **`set network dns secondary [address]`**
Domain	Represents the name of the domain in which this machine is located	Yes CLI: **`set network domain [name]`**
Timezone		
Time Zone	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.	Yes CLI: **`set timezone [zone`**
Network Time Protocol		
NTP Server IP Address	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.	Yes In Cisco Unified Communications Operating System Administration, select **Settings** > **NTP Servers**

Export Restricted and Export Unrestricted Software

This release of Unified Communications Manager and IM and Presence Service supports an export unrestricted (XU) version, in addition to the export restricted (K9) version.

Note 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 IM and Presence Service 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).

Note 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 ofUnified Communications Manager and IM and Presence Service.

GUI Item	Location	Description
Cisco Unified CM Administration		
VPN Configuration	**Advanced Features** > **VPN**	This menu and its options are not available.
Phone Security Profile Configuration	**System** > **Security** > **Phone Security Profile**	The **Device Security Mode** is set to **Non Secure** and is not configurable.
Cisco Unified CM IM and Presence Administration		

GUI Item	Location	Description
Security Settings	**System** > **Security** > **Settings**	• You cannot check the **Enable XMPP Client to IM/P Service Secure Mode** setting. • You cannot check the **Enable XMPP Router-to-Router Secure Mode** setting. • You cannot check the **Enable Web Client to IM/P Service Secure Mode** setting. • The option to set **SIP intra-cluster Proxy-to-Proxy Transport Protocol** to **TLS** have been removed.
Service Parameter Configuration for Cisco SIP Proxy service	**System** > **Service Parameters** and choose **Cisco SIP Proxy** as the **Service**	• All TLS options have been removed for the **Transport Preferred Order** parameter. • The TLS option have been removed from the **SIP Route Header Transport Type** parameter.
SIP Federated Domains	**Presence** > **Inter-domain Federation** > **SIP Federation**	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.
XMPP Federation Settings	**Presence** > **Inter-domain Federation** > **XMPP Federation** > **Settings**	You cannot configure the security mode; It is set to **NO TLS**.
Proxy Configuration Settings	**Presence** > **Routing** > **Settings**	You cannot set any TLS or HTTPS listeners as the preferred proxy listener.