Cisco Unified Communications Manager IM and Presence Service (IM & P) 11.5SU3 running on Cisco Unified Computing System™ (Cisco UCS) C220 M4S and UCS C240 M4S

Common Criteria Configuration Guide

Version 1.0

15 November 2017
Table of Contents

1 Introduction .......................................................................................................................... 9
  1.1 Audience ......................................................................................................................... 9
  1.2 Purpose ........................................................................................................................... 9
  1.3 Document References .................................................................................................... 9
  1.4 Supported Hardware and Software .............................................................................. 11
  1.5 Operational Environment ............................................................................................. 12
    1.5.1 Supported non-TOE Hardware/Software/Firmware ........................................... 12
  1.6 Excluded Functionality .................................................................................................. 13
2 Secure Acceptance of the TOE ....................................................................................... 14
3 Secure Installation and Configuration ............................................................................... 16
  3.1 Physical Installation ....................................................................................................... 16
  3.2 Initial Setup of IM&P ..................................................................................................... 16
    3.2.1 Enabling FIPS Mode .............................................................................................. 16
    3.2.2 Administrator Configuration, Credentials and Session Termination ................... 18
    3.2.3 Logging Configuration ............................................................................................ 19
  3.3 Services, Management and User Association .............................................................. 24
  3.4 Network Protocols and Cryptographic Settings ............................................................ 25
    3.4.1 Remote Administration Protocols ......................................................................... 25
    3.4.2 Certificates .............................................................................................................. 26
    3.4.3 Generating a Certificate Signing Request (CSR) .................................................. 28
    3.4.4 Clusters and Nodes ............................................................................................... 29
4 Secure Management ........................................................................................................ 30
  4.1 User Roles ....................................................................................................................... 30
  4.2 Clock Management ........................................................................................................ 31
  4.3 Identification and Authentication .................................................................................. 31
  4.4 Login Banners ................................................................................................................. 32
  4.5 Product Updates ............................................................................................................. 32
Cisco Unified Communications Manager IM and Presence Service (IM&P)

Common Criteria Guidance

5 Security Relevant Events ................................................................. 32
6 Network Services and Protocols ...................................................... 34
7 Modes of Operation ........................................................................ 35
8 Security Measures for the Operational Environment .......................... 36
9 Related Documentation .................................................................... 37
  9.1 Documentation Feedback ............................................................ 37
  9.2 Obtaining Technical Assistance .................................................. 37
10 COP FILE INSTALL README INSTRUCTIONS ............................... 39
  10.1 Introduction: ................................................................................. 39
  10.2 Updates in This Release .............................................................. 39
  10.3 Important Notes: ......................................................................... 39
  10.4 Installation Instructions: .............................................................. 39
List of Tables

Table 1: Acronyms .......................................................................................................................... 5
Table 2  Terminology ....................................................................................................................... 7
Table 3  Cisco Documentation ......................................................................................................... 9
Table 4: Operational Environment Components .............................................................................. 12
Table 5 Excluded Functionality ........................................................................................................ 13
Table 6 TOE External Identification .................................................................................................. 14
Table 7 Evaluated Software Images .................................................................................................. 15
Table 8 Audit Entries ........................................................................................................................ 22
Table 10: Protocols and Services .................................................................................................... 34
Table 11 Operational Environment Security Measures ..................................................................... 36
Cisco Unified Communications Manager IM and Presence Service (IM&P)
Common Criteria Guidance

List of Acronyms

The following acronyms and abbreviations may be used in this document:

<table>
<thead>
<tr>
<th>Acronyms / Abbreviations</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Administration, Authorization, and Accounting</td>
</tr>
<tr>
<td>ACL</td>
<td>Access Control Lists</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>BRI</td>
<td>Basic Rate Interface</td>
</tr>
<tr>
<td>CC</td>
<td>Common Criteria for Information Technology Security Evaluation</td>
</tr>
<tr>
<td>CEM</td>
<td>Common Evaluation Methodology for Information Technology Security</td>
</tr>
<tr>
<td>CM</td>
<td>Configuration Management</td>
</tr>
<tr>
<td>IM&amp;P</td>
<td>Cisco Unified Communications Manager</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name Server</td>
</tr>
<tr>
<td>EAL</td>
<td>Evaluation Assurance Level</td>
</tr>
<tr>
<td>EHWIC</td>
<td>Ethernet High-Speed WIC</td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulating Security Payload</td>
</tr>
<tr>
<td>GE</td>
<td>Gigabit Ethernet port</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hyper-Text Transport Protocol</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hyper-Text Transport Protocol Secure</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td>IGMP</td>
<td>Internet Group Management Protocol</td>
</tr>
<tr>
<td>IM&amp;P OS</td>
<td>The proprietary operating system developed by Cisco Systems.</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPsec</td>
<td>IP Security</td>
</tr>
<tr>
<td>ISDN</td>
<td>Integrated Services Digital Network</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>NDcPP</td>
<td>collaborative Network Device Protection Profile</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>Packet</td>
<td>A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.</td>
</tr>
<tr>
<td>PBKDF2</td>
<td>Password-Based Key Derivation Function version 2</td>
</tr>
<tr>
<td>PoE</td>
<td>Power over Ethernet</td>
</tr>
<tr>
<td>PP</td>
<td>Protection Profile</td>
</tr>
<tr>
<td>PRNG</td>
<td>Pseudo Random Number Generator</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial In User Service</td>
</tr>
<tr>
<td>RNG</td>
<td>Random Number Generator</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest, Shamir and Adleman (algorithm for public-key cryptography)</td>
</tr>
<tr>
<td>SA</td>
<td>Security Association</td>
</tr>
<tr>
<td>SFP</td>
<td>Small–form-factor pluggable port</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Standard</td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol</td>
</tr>
<tr>
<td>SM</td>
<td>Service Module</td>
</tr>
<tr>
<td>SSHv2</td>
<td>Secure Shell (version 2)</td>
</tr>
<tr>
<td>ST</td>
<td>Security Target</td>
</tr>
<tr>
<td>TCP</td>
<td>Transport Control Protocol</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Transmission Control Protocol/Internet Protocol</td>
</tr>
</tbody>
</table>
### Acronyms / Abbreviations

<table>
<thead>
<tr>
<th>Acronyms / Abbreviations</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOE</td>
<td>Target of Evaluation (in this evaluation the TOE is the Cisco Unified Communications Manager IM and Presence Service product)</td>
</tr>
<tr>
<td>TSC</td>
<td>TSF Scope of Control</td>
</tr>
<tr>
<td>TSF</td>
<td>TOE Security Function</td>
</tr>
<tr>
<td>TSP</td>
<td>TOE Security Policy</td>
</tr>
<tr>
<td>UCM</td>
<td>Unified Communications Manager</td>
</tr>
<tr>
<td>UDP</td>
<td>User datagram protocol</td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice over IP</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>WIC</td>
<td>WAN Interface Card</td>
</tr>
</tbody>
</table>
Terminology

Table 2 Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorized Administrator</td>
<td>Any user which has been assigned to a privilege level that is permitted to perform all TSF-related functions.</td>
</tr>
<tr>
<td>Peer IM&amp;P</td>
<td>Another IM&amp;P on the network that the TOE interfaces.</td>
</tr>
<tr>
<td>Security Administrator</td>
<td>Synonymous with Authorized Administrator for the purposes of this evaluation.</td>
</tr>
<tr>
<td>CUCM</td>
<td>Cisco Unified Communications Manager (CUCM) serves as the software-based call-processing component of the Cisco Unified Communications family of products. The CUCM extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications.</td>
</tr>
<tr>
<td>User</td>
<td>Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.</td>
</tr>
<tr>
<td>Firmware (per NIST for FIPS validated cryptographic modules)</td>
<td>The programs and data components of a cryptographic module that are stored in hardware (e.g., ROM, PROM, EPROM, EEPROM or FLASH) within the cryptographic boundary and cannot be dynamically written or modified during execution.</td>
</tr>
</tbody>
</table>
DOCUMENT INTRODUCTION

Prepared By:
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134

This document provides supporting evidence for an evaluation of a specific Target of Evaluation (TOE), the Cisco Unified Communications Manager IM and Presence Service (IM&P). This Operational User Guidance with Preparative Procedures addresses the administration of the TOE software and hardware and describes how to install, configure, and maintain the TOE in the Common Criteria evaluated configuration.
1 Introduction
This Operational User Guidance with Preparative Procedures documents the administration of the Cisco Unified Communications Manager IM and Presence Service (IM&P) 11.5 SU3 running on Cisco Unified Computing System™ (Cisco UCS) C220 M4S, UCS C240 M4S, the TOE, as it was certified under Common Criteria. The Cisco Unified Communications Manager IM and Presence Service (IM&P) may be referenced below as the Cisco Unified Communications Manager IM and Presence Service, IM&P, or simply TOE.

1.1 Audience
This document is written for administrators configuring the TOE. This document assumes that you are familiar with Cisco or equivalent enterprise instant messaging (IM) and network-based presence unified communications products. It is also assumed that you have a general understanding and knowledge with the basic concepts and terminologies used in enterprise communication features and functions to instant messaging, presence, video, visual voicemail, and web collaboration and multimedia applications, that you are a trusted individual, and that you are trained to use the operating systems on which you are running your network.

1.2 Purpose
This document is the Operational User Guidance with Preparative Procedures for the Common Criteria evaluation. It was written to highlight the specific TOE configuration and administrator functions and interfaces that are necessary to configure and maintain the TOE in the evaluated configuration. The evaluated configuration is the configuration of the TOE that satisfies the requirements as defined in the Security Target (ST). This document covers all of the security functional requirements specified in the ST and as summarized in Section 3 of this document. This document does not mandate configuration settings for the features of the TOE that are outside the evaluation scope, which should be set according to your organizational security policies.

This document is not meant to detail specific actions performed by the administrator but rather is a road map for identifying the appropriate locations within Cisco documentation to get the specific details for configuring and maintaining IM&P operations. It is recommended that you read all instructions in this document and any references before performing steps outlined and entering commands. Section 9 of this document provides information for obtaining assistance.

1.3 Document References
This section lists the Cisco Systems documentation that is also the Common Criteria Configuration Item (CI) List. The documents used are shown below in Table 3. Throughout this document, the guides will be referred to by the “#”, such as [1].

Table 3 Cisco Documentation

<table>
<thead>
<tr>
<th>#</th>
<th>Title</th>
<th>Link</th>
</tr>
</thead>
</table>

Page 9 of 42
# Title | Link
--- | ---
[2] Hardware Install Guides:  
[8] Cisco Unified Communications Manager IM & Presence Security Target, version 1.0 | See NIAP webpage for certified products - [https://www.niap-ccevs.org/CCEVS_Products/pcl.cfm](https://www.niap-ccevs.org/CCEVS_Products/pcl.cfm)

1.4 Supported Hardware and Software

Only the hardware and software listed in Section 1.5 of the Security Target (ST) is compliant with the Common Criteria evaluation. Using hardware not specified in the ST invalidates the secure configuration. Likewise, using any software version other than the evaluated software listed in the ST will invalidate the secure configuration. The TOE is a hardware and software solution that makes up the IM&P system as follows:

- The hardware is comprised of the Cisco Unified Computing System™ (Cisco UCS) C220 M4 Rack Server [1RU] or UCS C240 M4 2 Rack Server [2RU]
- The software is comprised of the IM&P software image Release 11.5SU3

The software comes pre-installed on the UCS C220 M4 Server or UCS C240 M4 2 Rack Server [2RU] though it may not be the CC evaluated and certified version, to include the COP file. See 10 COP FILE INSTALL README INSTRUCTIONS.

Cisco IM&P Administration is a web-based application that is the main administration and configuration interface for Cisco IM&P. The IM&P Administration is used to manage the system, features, server settings, and end users. IM&P Administration supports the following operating system browsers:

- Microsoft Internet Explorer (IE) 8 and later when running on Microsoft Windows 8 and later
- Firefox 4.x and later when running on Microsoft Windows 8 and later

Cisco IM&P works as an Appliance on a non-Windows-based Operating System. The Cisco IM&P appliance refers to the following functions:

- Works on a specific hardware platform(s) that Cisco specifies and supplies and, in some cases, the customer supplies
- Works in a carefully controlled software environment that Cisco specifies and installs
- Includes all software that is required to operate, maintain, secure, and manage servers

Cisco IM&P servers get preinstalled with software to ease customer and partner deployment and automatically search for updates and notify administrators when key security fixes and software upgrades are available for their system. This process comprises Electronic Software Delivery.

Since Cisco IM&P is a software application, enhancing its capabilities in production environments requires only upgrading software on the server platform.

### 1.5 Operational Environment

#### 1.5.1 Supported non-TOE Hardware/Software/Firmware

The TOE supports (in some cases optionally) the following hardware, software, and firmware in its environment:

<table>
<thead>
<tr>
<th>Component</th>
<th>Required</th>
<th>Usage/Purpose Description for TOE performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Console</td>
<td>Yes</td>
<td>This includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.</td>
</tr>
<tr>
<td>Management Workstation using web browser for HTTPS</td>
<td>Yes</td>
<td>This includes any IT Environment Management workstation with a web browser installed that is used by the TOE administrator to support TOE administration through HTTPS protected channels. Any web browser that supports TLSv1.1 with the supported ciphersuites may be used.</td>
</tr>
<tr>
<td>NTP Server</td>
<td>Yes</td>
<td>The TOE supports communications with CUCM in order to synchronize the date and time on the TOE. CUCM maintains and synchronizes with an NTP server for a reliable timestamp. The NTP Server is required in the IT environment in support of synchronize time stamps for both CUCM and subsequently the TOE.</td>
</tr>
<tr>
<td>RADIUS or TACACS+ AAA Server</td>
<td>No</td>
<td>This includes any IT environment RADIUS or TACACS+ AAA server that provides single-use authentication mechanisms. This can be any RADIUS or TACACS+ AAA server that provides single-use authentication.</td>
</tr>
<tr>
<td>Syslog Server</td>
<td>Yes</td>
<td>This includes any syslog server to which the TOE would transmit syslog messages using TLS to secure the connection. The audit records are automatically sent to the remote syslog once the configuration and settings are complete.</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager (CUCM)</td>
<td>Yes</td>
<td>CUCM serves as the component of the Cisco Unified Communications family of products with which the TOE communicates with to provide instant messaging (IM) and network-based presence to the end points over a protected TLS channel.</td>
</tr>
<tr>
<td>DNS Server</td>
<td>Yes</td>
<td>The TOE supports communications with the DNS Server that is</td>
</tr>
</tbody>
</table>
Common Criteria Guidance

<table>
<thead>
<tr>
<th>Component</th>
<th>Required</th>
<th>Usage/Purpose Description for TOE performance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>required for communications with other components (CUCM and other IM&amp;P clusters). The DNS is required to support IP addressing schemes for traffic and access control. Cisco recommends that all IM and Presence Service node names in the cluster be set to the FQDN or IP address rather than the hostname.</td>
</tr>
</tbody>
</table>

1.6 Excluded Functionality

Table 5 Excluded Functionality

<table>
<thead>
<tr>
<th>Excluded Functionality</th>
<th>Exclusion Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-FIPS 140-2 mode of operation on the TOE</td>
<td>This mode of operation includes non-FIPS allowed operations.</td>
</tr>
</tbody>
</table>

These services will be disabled by configuration. The exclusion of this functionality does not affect compliance to the collaborative Protection Profile for Network Devices Version 1.0.
2 Secure Acceptance of the TOE

In order to ensure the correct TOE is received, the TOE should be examined to ensure that it has not been tampered with during delivery.

Verify that the TOE software and hardware were not tampered with during delivery by performing the following actions:

Step 1 Before unpacking the TOE, inspect the physical packaging the equipment was delivered in. Verify that the external cardboard packing is printed with the Cisco Systems logo and motifs. If it is not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 2 Verify that the packaging has not obviously been opened and resealed by examining the tape that seals the package. If the package appears to have been resealed, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 3 Verify that the box has a white tamper-resistant, tamper-evident Cisco Systems bar coded label applied to the external cardboard box. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This label will include the Cisco product number, serial number, and other information regarding the contents of the box.

Step 4 Record the serial number of the TOE on the shipping documentation. The serial number displayed on the white label affixed to the outer box will be that of the device. Verify the serial number on the shipping documentation matches the serial number on the separately mailed invoice for the equipment. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 5 Verify that the box was indeed shipped from the expected supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This can be done by verifying with the supplier that they shipped the box with the courier company that delivered the box and that the consignment number for the shipment matches that used on the delivery. Also, verify that the serial numbers of the items shipped match the serial numbers of the items delivered. This verification should be performed by some mechanism that was not involved in the actual equipment delivery, for example, phone/FAX or other online tracking service.

Step 6 Inspect the TOE according to the instructions in [2] Unpack and Inspect the Cisco Unified Computing System™ (Cisco UCS) C220 M4 [1RU] or UCS C240 M4 2 Rack Server [2RU]. Rack Server installed with IM&P software image Release 11.5. Verify that the serial number displayed on the unit itself matches the serial number on the shipping documentation and the invoice. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). Also, verify that the unit has the following external identification as described in Table 6 below.

### Table 6 TOE External Identification

<table>
<thead>
<tr>
<th>Product Name</th>
<th>Model Number</th>
<th>External Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Computing System™ (Cisco UCS)</td>
<td>C220 M4S</td>
<td>UCS C220 M4S</td>
</tr>
<tr>
<td>Cisco Unified Computing System™ (Cisco UCS)</td>
<td>C240 M4S</td>
<td>UCS C240 M4S</td>
</tr>
</tbody>
</table>
Step 7 To verify the software version and to register the license, from a PC in your network that has been installed with one of the supported browsers, browse into a server that is running Cisco IM&P Administration and log in with administrative privileges. Follow the instructions in [3] Administration Overview -> Getting Started -> Sign In

Step 8 To verify the software version IM&P 11.5 from the Cisco Unified Operating System Administration window, choose Show > Software and review the fields in the Software Packages window. See Table 7 below for the details that must be checked to ensure the software has not been modified in anyway.

<table>
<thead>
<tr>
<th>Software Version</th>
<th>Image Name</th>
<th>Hash</th>
</tr>
</thead>
</table>
| Cisco Unified Communications Manager IM and Presence Service (IM&P) Version 11.5SU3 and COP file | Bootable_UCSI install_CUP_11.5.1.13000-13.sgn.iso | MD5 Checksum: 451e92e33e722ef9ff8c43246ada5b81
|                                                                                  |                                                                             | SHA512 Checksum: cff3e4b9a74095053094cb2bd1cb1638d4ffece4df62c76b85e31ee72bbbd52e2984118e9c4060fd7a253dcece2cd125b11f49938e161773cdd4700cda4d32bf |
|                                                                                  | Bootable SU3 update - UCSInstall_UCOS_11.5.1.14058-7.sgn.iso               | MD5 Checksum: 480e95e490d3334ff26d1b7dde4b0e83
|                                                                                  |                                                                             | SHA512 Checksum: b9f176de939f4d9e78bffdd93b601d9b4f4ac0bd10c8141f190ea2e017c2c4141a68b5639e53df5bb9579997047086a40b2c78ae8ffe8d23e51401fcaabf1d1c81 |

After determining that the checksums match, click Next to proceed with the software upgrade. If the file, checksums or certificate signatures were tampered with or modified in anyway, the installation would halt and a warning may be displayed at which time you need to call Cisco TAC, refer to, 9.2 Obtaining Technical Assistance.

When installing the COP file it is important to follow the instructions in the README file. The COP file was developed to restrict the use of 3DES ciphers. The instructions are included at the end of this document for ease of use. Refer to 10 COP FILE INSTALL README INSTRUCTIONS. Note: the COP file checksums are verified the same as the IM&P software file checksum described above.
3 Secure Installation and Configuration

3.1 Physical Installation

Follow the instructions in [2](a)(b) Preparing for Server Installation following with Installing the Server In a Rack and Initial Setup. There are network requirements that must be met before deploying IM&P.

3.2 Initial Setup of IM&P

Follow the System Configuration -> Cisco Unified Communications Manager configuration for integration with IM and Presence Service instructions in [3] for the initial setup configurations. There are CUCM settings and network requirements that must be met before deploying IM&P, such as user and device configurations, port configurations, IP addressing, software versioning, supported browsers and their associated certificates.

During the initial startup of the Cisco IM&P you will be required to reset the Administrator default setting. Refer to the password requirements listed below in Section 3.2.2 Administrator Configuration, Credentials and Session Termination.

The Initial configuration setup includes licensing requirements, the server name and ports, system-wide parameters that are required when you setup a node for the first time and the core settings for server groups, time zone information and regions.

The Post-Installation Tasks for Cisco Unified Communications Manager in [9] will guide you through activating services and installing the license.

After the initial setup and activating licenses and services are completed, the remainder of this guide will guide you through setting up IM (chat), presence services and migration for devices and end users [3]. The default method to administer is IM&P is securely connecting to the IM&P GUI interface using TLS. Using a secure TLS connection is required in the evaluated configuration [10] and [15] to set the minimum TLS version for use to TLSv1.1 or TLSv1.2 with support for the following ciphers,

**TLS RSA Ciphers**
- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268

**ECDHE RSA Ciphers**
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

If local administration is required via directly connected to the UCS appliance, refer to Administration in [11] using vSphere client. In the evaluated configuration, only authorized administrators are granted access and privileges to manage the TOE.

3.2.1 Enabling FIPS Mode

The TOE must be run in the FIPS mode of operation. Refer to [5] Security for SRST References, Trunks, and Gateways -> FIPS 140-2 Mode Setup for the configuration settings.
The self-tests for the cryptographic functions in the TOE are run automatically during power-on as part of the POST. The same POST self-tests for the cryptographic operations are also run periodically during operational state.

If any self-tests fail, the TOE transitions into an error state. In the error state, all secure management and data transmission that is affected by the failure is halted and the TOE outputs status information indicating the failure. In an error state the Administrator may be able to log in to troubleshoot the issue.

During the POST, all ports are blocked from moving to forwarding state. If all components of all modules pass the POST, the system is placed in FIPS PASS state and ports are allowed to forward management and data traffic. If the POST fails, the TOE will continuously reboot in attempts to correct the failure. During this state no one can login, no traffic is passed, the TOE is not operational. If the problem is not corrected by the reboot, Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. Contact Cisco TAC as described in 9.2 Obtaining Technical Assistance.

In this 11.5 release of IM&P, the TOE provides support to monitor the Entropy Monitoring Daemon. This feature does not require any configuration, though it can be turned off by using the CLI. In the evaluated configuration, this service should not be turned off [5] Default Security Setup -> ECDSA Support for Common Criteria for Certified Solutions -> Entropy. Certificates

The IM&P supports self-signed and third party signed certificates. The certificates are used to securely authenticate devices, encrypt data and to hash data to ensure its integrity. The most important part of certificates is that you know and define how your data is encrypted and shared with entities such as the intended website, phone, or FTP server. When your system trusts a certificate, this means that there is a preinstalled certificate on your system which states it is fully confident that it shares information with the correct destination. Otherwise, it terminates the communication between these points. In order to trust a certificate, trust must already be established with a third-party certificate authority (CA). Your devices must know that they can trust both the CA and intermediate certificates first, before they can trust the server certificate presented by the exchange of messages called the secure sockets layer (SSL) handshake. Refer to Manage Certificates in [3] and Security Overview -> Certificates and Security Overview -> Certificate Setup in [5].

For third-party signed certificates or certificate chain, you will need to upload the certificate authority root certificate of the certificate authority that signed an application certificate. If a subordinate certificate authority signs an application certificate, you must upload the certificate authority root certificate of the subordinate certificate authority. You can also upload the PKCS#7 format certificate chain of all certificate authority certificates. You can upload certificate authority root certificates and application certificates by using the Upload Certificate dialog box. When you upload a certificate authority root certificate or certificate chain that contains only certificate authority certificates, choose the certificate name with the format certificate type-trust. When you upload an application certificate or certificate chain that contains an application certificate and certificate authority certificates, choose the certificate name that includes only the certificate type.
To download certificates, on the Cisco Unified OS Administration page, choose Security > Certificate Management. Next, specify the search criteria and then click Find, then choose the file name of the certificate or certificate trust list (CTL) and click Download.

To upload any new certificates or certificate chains that you want your system to trust, from the Cisco Unified OS Administration, choose Security > Certificate Management, click Upload Certificate/Certificate Chain, choose the certificate name from the Certificate Purpose drop-down list, then choose the file to upload by performing one of the following steps:

- In the Upload File text box, enter the path to the file.
- Click Browse, navigate to the file, and then click Open.

To upload the file to the server, click Upload File

Certificates will also be required for each device that communicates with IM&P.


3.2.2 Administrator Configuration, Credentials and Session Termination

The IM&P must be configured to use a username and password for each administrator. Once the IM&P has been setup and configured, the Administrator can create additional administrative user accounts, refer to [3] Administration -> End User Setup and Handling.

The security policies for administrative users include the settings for:

- idle timeouts (session termination) is set by default to 30 minutes
- password criteria
  - by default, is set to a minimum of six (6) characters. In the evaluated configuration the password must be set to a minimum of at least 15 characters
  - password complexity include the following settings:
    - password must be a combination of upper and lower case letters (a-z and A-Z), numbers (0-9) and the following special characters “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“)“)
  - pins (personal identification number) needs to be set to at least eight (8) characters

The credential policies control the authentication process for resources (users) of the TOE. The defines password requirements and account lockout details such as failed login attempts, expiration periods and lockout durations for end user passwords, end user PINs, and application user passwords. Credential policies can be assigned broadly to all accounts of a specific credential type, such as all end user PINs, or they can be customized for a specific application user, or end user. The inactivity settings must trigger termination of the administrator session. The default value for the IM&P Web Interface is 30 minutes. If the TOE detects there is no activity for 30 minutes, the IM&P Web Interface times out and the Administrator will be logged off. These settings are only configurable by using the Command Line Interface. It is recommended to accept the default time in the evaluated configuration as the CLI was not included.

It is recommended to not leave the IM&P Web Interface unattended and that all active sessions be logged out and closed when not being used.
3.2.3 Logging Configuration

Once the TOE becomes operational, auditing is on by default, though can be configured via the access the Audit Log Configuration window in the serviceability GUI to configure the settings for the audit logs [3] Troubleshooting IM and Presence Services -> Traces Used To Troubleshoot IM and Presence Service and [4] Alerts and Traces and Logs for setup and configuration of the various alerts, logging of events and log files. In addition, see [10] Cisco Unified Communications Manager cache responses to A/AAAA queries -> Logging and Log File.

When audit logging has been enabled, without the detailed logging option selected, the audit logging includes configuration changes to the system are logged in separate log files for auditing. The Cisco Audit Event Service, which displays under Control Center - Network Services in the serviceability GUI, monitors and logs any configuration changes to the system that are made by a user or as a result of the user action [12].

Cisco Unified Serviceability logs the following events:

- Activation, deactivation, start, or stop of a service
- Changes in trace configurations and alarm configurations
- Review of any report in the Serviceability Reports Archive (this log is viewed on the reporter node).

Cisco IM and Presence Administration Standard Events Logging

- Administrator logging (logins and logouts)
- User role membership updates (user added, user deleted, user role updated)
- Role updates (new roles added, deleted, or updated)
- Device updates (phones and gateways)
- Server configuration updates (changes to alarm or trace configurations, service parameters, enterprise parameters, IP addresses, hostnames, Ethernet settings, and IM and Presence server additions or deletions)

IM and Presence Application Standard Events Logging

- End user logging on IM clients (user logins, user logouts, and failed login attempts)
- User entry to and exit from IM Chat Rooms
- Creation and destruction of IM Chat Rooms

Command Line Interface Standard Events Logging

- All commands issued through the command line interface are logged

System Audit Logs

- System audit logs track activities such as the creation, modification, or deletion of users, log tampering, and any changes to file or directory permissions. This type of audit log is
disabled by default due to the high volume of data gathered. To enable this function, you must manually enable `utils auditd` using the CLI [13].

To setup remote logging to a syslog server, first you must have the syslog server setup and operational. Refer to Audit Logs -> Configure Remote Audit Log Transfer Protocol (Chapter 7) in [12].

To set up audit logging, the steps are as follows [12]:

**Step 1** In Cisco Unified Serviceability, choose Tools > Audit Log Configuration.

**Step 2** From the Server drop-down menu, select any server in the cluster and click Go.

**Step 3** To log all cluster nodes, check the Apply to All Nodes check box.

**Step 4** In the Server Name field, enter the IP Address or fully qualified domain name of the remote syslog server.

**Step 5** Optional. To log configuration updates, including items that were modified, and the modified values, check the Detailed Audit Logging check box.

**Step 6** Complete the remaining fields in the Audit Log Configuration window. For help with the fields and their descriptions, see the online help.

**Step 7** Click Save.

The default transfer protocol to the syslog server is UDP. You will need to change this setting.

**Step 1** Log in to the Command Line Interface.

**Step 2** Run the `utils remotesyslog show protocol` command to confirm which protocol is configured.

**Step 3** If you need to change the protocol on this node, do the following:
- To configure TCP, run the `utils remotesyslog set protocol tcp` command.
- To configure UDP, run the `utils remotesyslog set protocol udp` command.

**Step 4** If you changed the protocol, restart the node.

**Step 5** Repeat this procedure for all Cisco Unified Communications Manager and IM and Presence Service cluster nodes.

In the evaluated configuration, you must use TLS to secure the connection to the remote syslog server. You will have to configure TLS to secure the connection to the syslog server using the run the `utils remotesyslog set protocol tls` command. The connection is using TLSv1.2 and
associated ciphersuites that was configured during installation as defined in 3.2 Initial Setup of IM&P. Refer to Security Configurations on IM and Presence Service [3] Chapter 9, page 107, Security Configuration on IM and Presence Service, section Enhanced TLS Encryption on IM and Presence Service.

Refer to Audit Log Configuration Settings in [12] to set remote syslog audit event level, log rotation, maximum number of files and size and warning threshold for log rotation overwrite.

By default, the logs are configured to rotate. If the AuditLogAlarmMonitor cannot write an audit event, the AuditLogAlarmMonitor logs this failure as a critical error in the syslog file. The Alert Manager reports this error as part of a SeverityMatchFound alert. The actual operation continues even if the event logging fails.

Audit logging contains the following parts:

- Audit logging framework - The framework comprises an API that uses an alarm library to write audit events into audit logs. An alarm catalog that is defined as GenericAlarmCatalog.xml applies for these alarms. Different system components provide their own logging. The following example displays an API that a Cisco IM&P component can use to send an alarm:

  User ID: CIMPAdministrator
  Client IP Address: 172.19.240.207
  Severity: 3
  EventType: ServiceStatusUpdated
  ResourceAccessed: CIMPService
  EventStatus: Successful
  Description: IMP Service status is stopped

- Audit event logging - An audit event represents any event that is required to be logged. The following example displays a sample audit event:

  CCM_TOMCAT-GENERIC-3-AuditEventGenerated: Audit Event Generated UserID:CIMPAdministrator Client IP Address:172.19.240.207 Severity:3
  EventType:ServiceStatusUpdated ResourceAccessed: CIMPService EventStatus:Successful Description: IMP Service status is stopped App ID:Cisco Tomcat Cluster ID:StandAloneCluster Node ID:sa-cm1-3

For additional information, refer to [3] Troubleshooting IM and Presence Services -> Traces Used To Troubleshoot IM and Presence Service

3.2.3.1 Audit Trail Log Entries

The following table identifies the elements of the IM&P audit records.
Table 8 Audit Entries

<table>
<thead>
<tr>
<th>Heading</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>The user that triggered the event, e.g. CIMPAdministrator Client</td>
</tr>
<tr>
<td>Client IP Address</td>
<td>IP address of the client device used, e.g. 172.19.240.207</td>
</tr>
<tr>
<td>Severity</td>
<td>Level of the event, e.g. 3</td>
</tr>
<tr>
<td>EventType</td>
<td>The type of event that was performed, e.g. ServiceStatusUpdated</td>
</tr>
<tr>
<td>ResourceAccessed</td>
<td>The resource that was accessed, e.g. CIMPService</td>
</tr>
<tr>
<td>EventStatus</td>
<td>The status of the event; e.g. successful</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the event; e.g. IMP Service status is stopped</td>
</tr>
</tbody>
</table>

Audit trail records capture the following activities and any additional information:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Auditable Events</th>
<th>Additional Audit Record Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCS_HTTPS_EXT.1</td>
<td>Failure to establish a HTTPS Session</td>
<td>Reason for failure.</td>
</tr>
<tr>
<td>FCS_TLSS_EXT.1</td>
<td>Failure to establish a TLS Session</td>
<td>Reason for failure</td>
</tr>
<tr>
<td>FIA_UIA_EXT.1</td>
<td>All use of the identification and authentication mechanism. Adminstrative Actions: Logging into TOE.</td>
<td>Provided user identity, origin of the attempt (e.g., IP address).</td>
</tr>
<tr>
<td>FIA_UAU_EXT.2</td>
<td>All use of the authentication mechanism.</td>
<td>Origin of the attempt (e.g., IP address).</td>
</tr>
<tr>
<td>FIA_X509_EXT.1</td>
<td>Unsuccessful attempt to validate a certificate</td>
<td>Reason for failure</td>
</tr>
<tr>
<td>FMT_MOF.1(1)/Trusted Update</td>
<td>Any attempt to initiate a manual update</td>
<td></td>
</tr>
<tr>
<td>FMT_MTD.1</td>
<td>All management activities of TSF data</td>
<td></td>
</tr>
<tr>
<td>Requirement</td>
<td>Auditable Events</td>
<td>Additional Audit Record Contents</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>FPT_STM.1</td>
<td>Changes to the time.</td>
<td>The old and new values for the time.</td>
</tr>
<tr>
<td></td>
<td>Administrative Actions:</td>
<td>Origin of the attempt (e.g., IP address).</td>
</tr>
<tr>
<td></td>
<td>Changes to NTP settings.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manual changes to the system time.</td>
<td></td>
</tr>
<tr>
<td>FPT_TUD_EXT.1</td>
<td>Initiation of update. result of the update attempt (success or failure)</td>
<td>No additional information.</td>
</tr>
<tr>
<td></td>
<td>Administrative Actions:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Software updates</td>
<td></td>
</tr>
<tr>
<td>FTA_SSL_EXT.1</td>
<td>Any attempts at unlocking of an interactive session.</td>
<td>No additional information.</td>
</tr>
<tr>
<td></td>
<td>Administrative Actions:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specifying the inactivity time period.</td>
<td></td>
</tr>
<tr>
<td>FTA_SSL.3</td>
<td>The termination of a remote session by the session locking mechanism.</td>
<td>No additional information.</td>
</tr>
<tr>
<td></td>
<td>Administrative Actions:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specifying the inactivity time period.</td>
<td></td>
</tr>
<tr>
<td>FTA_SSL.4</td>
<td>The termination of an interactive session.</td>
<td>No additional information.</td>
</tr>
<tr>
<td>FTA_TAB.1</td>
<td>Administrative Action:</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Configuring the banner displayed prior to authentication.</td>
<td></td>
</tr>
<tr>
<td>FTP_ITC.1</td>
<td>Initiation of the trusted channel. Termination of the trusted channel.</td>
<td>Identification of the initiator and target of failed trusted channels establishment attempt.</td>
</tr>
<tr>
<td></td>
<td>Failure of the trusted channel functions.</td>
<td></td>
</tr>
<tr>
<td>FTP_TRP.1</td>
<td>Initiation of the trusted channel. Termination of the trusted channel.</td>
<td>Identification of the claimed user identity.</td>
</tr>
<tr>
<td></td>
<td>Failure of the trusted channel functions.</td>
<td></td>
</tr>
</tbody>
</table>
3.2.3.2 Audit Trail Capacities

Log Partition Monitoring (LPM), which is installed automatically with the IM&P, uses configurable thresholds to monitor the disk usage of the log partition on a server. The Cisco Log Partition Monitoring Tool service starts automatically after installation of the IM&P.

Every 5 minutes, Log Partition Monitoring uses the following configured thresholds to monitor the disk usage of the log partition and the spare log partition on a server:

- **LogPartitionLowWaterMarkExceeded (% disk space):** When the disk usage is above the percentage that you specify, LPM sends out an alarm message to syslog.
- **LogPartitionHighWaterMarkExceeded (% disk space):** When the disk usage is above the percentage that you specify, LPM sends an alarm message to syslog.
- **SparePartitionLowWaterMarkExceeded (% disk space):** When the disk usage is above the percentage that you specify, LPM sends out an alarm message to syslog.
- **SparePartitionHighWaterMarkExceeded (% disk space):** When the disk usage is above the percentage that you specify, LPM sends an alarm message to syslog.

To utilize log partition monitor, verify that the Cisco Log Partitioning Monitoring Tool service, a network service, is running on Cisco Unified Serviceability on the server or on each server in the cluster (if applicable). **Warning**, stopping the service causes a loss of feature functionality.

When the log partition monitoring services starts at system startup, the service checks the current disk space utilization. If the percentage of disk usage is above the low water mark, but less than the high water mark, the service sends an alarm message to syslog.

To configure Log Partitioning Monitoring, set the alert properties for the LogPartitionLowWaterMarkExceeded and LogPartitionHighWaterMarkExceeded alerts in Alert Central.

If the percentage of disk usage is above the high water mark that you configured, the system sends an alarm message to syslog and automatically purges log files until the value reaches the low water mark.

Also see Alarms, Trace and Tools and Reports in [12].

3.3 Services, Management and User Association

The TOE supports enterprise instant messaging (IM) and network-based presence as part of Cisco Unified Communications. IM and Presence Service is tightly integrated with Cisco and third-party compatible desktop and mobile presence and IM clients, including the Cisco Jabber™ messaging integration platform. This integration provides users with instant messaging, presence, video, visual voicemail, and web collaboration.

To allow users to receive availability and Instant Messaging (IM) services on IM&P, you must assign users to nodes, and presence redundancy groups. This can be done manually or automatically. You manage user assignment using the User Assignment Mode for Presence
Server Enterprise Parameter setting. This parameter specifies the mode in which the sync agent distributes users to the nodes in the cluster.


For end user setup and management refer to [3] Administration -> End User Setup and Handling.

The sessions can be secured using certificates. See 3.4.2 Certificates in this document for more information, setup and configuration.

3.4 Network Protocols and Cryptographic Settings

3.4.1 Remote Administration Protocols

The Authorized Administrates manages the TOE by connecting via a web browser. The remote administration sessions are protected by HTTPS/TLS.

The evaluated configuration requires that when connecting to the TOE over HTTPS/TLS for administrative management. You will need to disable SSL on your web browser to use TLS for secure HTTPS communications. TLS1.2 is used with the following ciphersuites, TLS_RSA_WITH_AES_128_CBC_SHA and optionally any of the following ciphersuites:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

To enable HTTPS, you must download a certificate that identifies the server during the connection process. You can accept the server certificate for the current session only, or you can download the certificate to a trust folder (file) to secure the current session and future sessions with that server. The trust folder stores the certificates for all your trusted sites.

Cisco IM&P supports these browsers for connection to the Cisco Tomcat web server application in Cisco IM&P Service:

- Microsoft Internet Explorer (IE) 8 and later when running on Microsoft Windows 8 and later
- Firefox 4.x and later when running on Microsoft Windows 8 and later

How to download and store the certificate, see 3.4.2 Certificates in this document for more information, setup and configuration.

After the initial configuration, use the following procedures to log into the server and log in to Cisco IM&P Administration.

Step 1 Start your preferred operating system browser.

Step 2 In the address bar of the web browser, enter the following case-sensitive URL:

https://<Unified IMP-server-name>:8443/cimpadmin/showHome.do
where: <Unified IMP-server-name> equals the name or IP address of the server

You can optionally specify a port number.

Step 3 A Security Alert dialog box displays. Click the appropriate button.

Step 4 At the main Cisco IM&P Administration window, enter the username and password that you specified during Cisco Unified IM&P installation and click Login.

For security purposes, Cisco IM&P Administration logs you out after 30 minutes of inactivity, and you must log back in with correct username and password credentials.

If the HTTPS/TLS connection fails for an unknown reason, you can attempt to re-establish the connection and/or you will want to check the alert and trace logs for a possible cause. You may also need to use the Cisco Unified Serviceability application to start or restart services on the Cisco Unified Communications Manager nodes. Cisco Unified Serviceability is a web-based troubleshooting tool. Refer to [3] Deployment Planning and [3] Security Configuration on IM and Presence Service.

3.4.2 Certificates

IM&P uses certificates to secure client and server identities. After root certificates are installed, certificates are added to the root trust stores to secure connections between users and hosts, including devices and application users. To enable the secure communications on IM&P service nodes, perform the following steps from the IM&P Administrator GUI:

- Configure certificate exchange between IM&P Service and Cisco Unified Communications Manager.
- Upload CA signed certificates to IM&P Service.
- Configure SIP security settings on IM&P Service for the TLS peer subject.


To find a certificate, perform the following steps from the IM&P Administrator GUI:

**Step 1** In Cisco IM&P Administration, choose System > Security > Certificate.

The Find and List Certificates window displays. Records from an active (prior) query may also display in the window.

**Step 2** To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records

a. From the first drop-down list box, choose a search parameter.
b. From the second drop-down list box, choose a search pattern.
c. Specify the appropriate search text, if applicable.

To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

Step 3 Click Find.

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Step 4 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

To upload certificates, perform the following steps from the IM&P Administrator GUI:

Step 1 From Cisco IM&P Administration, choose Security > Certificate Management. The Certificate List window appears.


Step 3 From the Certificate Purpose drop-down box, select a system security certificate, such as CallManager-CERT.

Step 4 In the Description field, enter a name for the certificate.

Step 5 In the Upload File field, click Choose File to browse for the certificate file that you want to distribute for all the servers in the cluster.

Step 6 Click Upload.

The following procedure describes how to import the Cisco IM&P certificate to the root certificate trust store for Internet Explorer 8.

Step 1 Browse to application on the Tomcat server (for example, enter the hostname, localhost, or IP address for Cisco IM&P Administration in the browser).

The browser displays a Certificate Error: Navigation Blocked message to indicate that this website is untrusted.
Cisco Unified Communications Manager IM and Presence Service (IM&P)
Common Criteria Guidance

**Step 2** To access the server, click Continue to this website (not recommended).

The Cisco IM&P Administration window displays, and the browser displays the address bar and Certificate Error status in red.

**Step 3** To import the server certificate, click the Certificate Error status box to display the status report. Click the View Certificates link in the report.

**Step 4** Verify the certificate details.

**Step 5** Select the General tab in the Certificate window and click Install Certificate.

The Certificate Import Wizard launches.

**Step 6** To start the Wizard, click Next.

The Certificate Store window displays.

**Step 7** Verify that the Automatic option, which allows the wizard to select the certificate store for this certificate type, is selected and click Next.

**Step 8** Verify the setting and click Finish.

A security warning displays for the import operation.

**Step 9** To install the certificate, click Yes.

The Import Wizard displays "The import was successful."

**Step 10** Click OK. The next time that you click the View certificates link, the Certification Path tab in the Certificate window displays "This certificate is OK."

**Step 11** To verify that the trust store contains the imported certificate, click Tools > Internet Options in the Internet Explorer toolbar and select the Content tab. Click Certificates and select the Trusted Root Certifications Authorities tab. Scroll to find the imported certificate in the list.

After importing the certificate, the browser continues to display the address bar and a Certificate Error status in red. The status persists even if you reenter the hostname, localhost, or IP address or refresh or relaunch the browser.

If the validity of a certificate cannot be established, refer to Manage Certificates [14] for troubleshooting certificate errors.

### 3.4.3 Generating a Certificate Signing Request (CSR)

You can generate a certificate signing request (CSR) that contains the certificate application information that the certificate authority uses to generate the trusted certificate. Following are the primary steps to follow, also refer to [14] for more details.

**Procedure**
Cisco Unified Communications Manager IM and Presence Service (IM&P)

Common Criteria Guidance

Step 1 From Cisco Unified OS Administration, choose Security > Certificate Management.

Step 2 Click Generate CSR.

Step 3 Configure the fields on the Generate Certificate Signing Request window. See the online help for more information about the fields and their configuration options.

Step 4 Click Generate CSR.

After the CSR has been generated, you will need to download the CSR to submit to the certificate authority.

**Procedure**

Step 1 From Cisco Unified OS Administration, choose Security > Certificate Management.

Step 2 Click Download CSR.

Step 3 Choose the certificate name from the Certificate Purpose drop-down list.

Step 4 Click Download CSR.

Step 5 (Optional) If prompted, click Save.

The CSR can now be submitted to your certificate authority.

### 3.4.4 Clusters and Nodes

A cluster comprises a set of Cisco IM&P servers that share the same database and resources. You can configure the servers in a cluster in various ways to perform various functions such as database replication.

For the Cisco IM&P servers that form a cluster, you should, as much as possible, evenly balance the IM and presence services load across the system by distributing the devices (such as users per cluster and number of contacts per user) among the various Cisco IM&P servers in the cluster.

Following are the stability requirements for IM&P:

- Six nodes per cluster
- 45,000 users per cluster with a maximum of 15,000 users per node in a full Unified Communication (UC) mode deployment
- 15,000 users per cluster in a presence redundancy group, and 45,000 users per cluster in a deployment with High Availability.
- Administrable customer-defined limit on the maximum contacts per user (default unlimited)
- The IM and Presence Service continues to support inter-cluster deployments with the multi-node feature.

Scalability depends on the number of clusters in your deployment. IM and Presence Service clusters can support up to six nodes. If you originally installed less than six nodes, then you can install additional nodes at any time. Refer to [3] Deployment Planning -> Multinodes Scalability

You will also need to ensure the DNS Server is configured to include the all IM and Presence Service node names in the cluster and set to the FQDN or IP address rather than the hostname. Refer to Security Configurations on IM and Presence Service [3].

4 Secure Management

4.1 User Roles
During the initial setup of the TOE the user that installs the TOE is deemed the Authorized Administrator and has full permissions and access to manage the TOE. Refer to [3], [4] and [5]

The Authorized Administrator is responsible for managing users and users’ access. The end users can be assigned to access control groups that are associated to a role. Each role defines a set of permissions for a specific resource within Cisco Unified Communications Manager IM and Presence Service.

When you assign a role to an access control group and then assign end users to that access control group, you grant those end users all the access permissions that are defined by the role. Upon installation Cisco Unified Communications Manager IM and Presence Service comes with predefined default roles that are assigned to predefined default access control groups. You can assign your end users to the default access control groups, or you can customize access settings by setting up new access control groups and roles. Refer to [3] Administration.

The Authorized Administrator will also need to configure end users. The end users are the consumers of the TOE. You can setup the authorization policy for IM and Presence Service end users, perform bulk user contact list imports and exports, as well as manage duplicate and invalid end user instances.

Following are the procedures to configure the Authorization Policy:

**Step 1** Choose Cisco IM&P Administration > Presence > Settings.

**Step 2** Configure the authorization policy. Perform one of the following actions:

- To turn on automatic authorization, **check** Allow users to view the availability of other users without being prompted for approval.
- To turn off automatic authorization, **unccheck** Allow users to view the availability of other users without being prompted for approval.

**Step 3** Click Save.

**Step 4** Restart the Cisco XCP Router service.

Following are the procedures to restart the service:

**Step 1** On IM&P Service, choose Cisco Unified IM and Presence Serviceability > Tools > Control Center - Network Services.

**Step 2** Choose the node from the Server list box and select Go.
Step 3  Click the radio button next to the Cisco XCP Router service in the IM and Presence Service section.

Step 4  Click Restart.

Step 5  Click OK when a message indicates that restarting may take a while.

Users must read the IM&P Service policy settings to determine how to handle presence subscription requests. Users configure the policy settings from their client (e.g. Cisco Jabber for Windows). A user policy contains the following configuration options:

- Blocked list - a list of local and external (federated) users that will always see the availability status of the user as unavailable regardless of the true status of the user. The user can also block a whole federated domain.
- Allowed list - a list of local and external users that the user has approved to see their availability. The user can also allow a whole external (federated) domain.
- Default policy - the default policy settings for the user. The user can set the policy to block all users, or allow all users.


4.2 Clock Management

The TOE maintains a clock that is used as the source for the date and time stamp in the audit trail records to record the time of the event. The clock timing is also used to monitor inactivity of administrator sessions.

In the evaluated configuration, Cisco Unified Communications Manager (CUCM) is a required component in the operating environment. CUCM serves as the component of the Cisco Unified Communications family of products with which the TOE communicates with over a protected TLS channel. The TOE supports communications with CUCM in order to synchronize the date and time on the TOE.

The time stamp is applied to the generated audit records and used to track inactivity of administrative sessions. This source is also used for cryptographic functions. Following are a few additional reasons why it is critical for an accurate and reliable time stamp on IM&P:

- It allows Cisco clients to display the correct date and time
- It assigns the correct date and time to IM and chat tags

For this reason, IM&P synchronizing with CUCM timestamp always have an accurate time clock than and all associated Cisco IM&P clients on the network will have the exact same time.

4.3 Identification and Authentication

Configuration of Identification and Authentication settings is restricted to the Administrator.

The IM&P can be configured to use any of the following authentication methods. Local authentication is the default setting and is required in the evaluated configuration.

- Local authentication (password authentication);
This is the default authentication configuration and should also be configured as a fallback authentication mechanism if the remote authentication server is not available.

4.4 Login Banners

The TOE may be configured by the Administrator to display a login warning banner that displays in the following IM&P interfaces: Cisco Unified CM IM and Presence Administration, Cisco Unified IM and Presence Operating System Administration, Cisco Unified IM and Presence Serviceability, Cisco Unified IM and Presence Reporting, and IM and Presence Disaster Recovery System. System Configuration -> Security Configuration on IM and Presence Service.

To upload a customized log-on message, follow this procedure:

**Step 1** Create a .txt file with the contents you want to display in the banner.

**Step 2** Sign in to Cisco Unified IM and Presence Operating System Administration.

**Step 3** Choose Software Upgrades > Customized Logon Message.

**Step 4** Click Browse and locate the .txt file.

**Step 5** Click Upload File.

The banner will appear before and after login on most IM and Presence Service interfaces.

The .txt file must be uploaded to each IM and Presence Service node separately.

This banner is displayed before the username and password prompts.

4.5 Product Updates

Verification of authenticity of updated software is done in the same manner as ensuring that the TOE is running a valid image. See Section 2 in this document for the method to download and verify an image prior to running it on the TOE. Also, refer to Upgrades [10].

5 Security Relevant Events

The TOE is able to generate audit records that are stored internally within the TOE whenever an audited event occurs, as well as archiving to a remote storage area/syslog server. The details for protection of that communication are covered in Section 3.2.3 Logging Configuration of this document. Also refer to [12] Alarms, [12] Trace and [12] Tools and Reports.

The TOE generates an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include, cryptography related events, identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in the table below). Each of the events is specified in syslog records in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred. Additionally, the startup and shutdown of the audit functionality is audited.
The local audit trail consists of the individual audit records; one audit record for each event that occurred. Refer to 3.2.3 Logging Configuration of this document for the security relevant events that are applicable to the TOE.
6 Network Services and Protocols

The table below lists the network services/protocols available on the TOE as a client (initiated outbound) and/or server (listening for inbound connections), all of which run as system-level processes. The table indicates whether each service or protocol is allowed to be used in the certified configuration.

For more detail about each service, including whether the service is limited by firewall mode (routed or transparent), or by context (single, multiple, system), refer to the Command Reference guides listed in Table 3.

<table>
<thead>
<tr>
<th>Service or Protocol</th>
<th>Description</th>
<th>Client (initiating)</th>
<th>Allowed</th>
<th>Server (terminating)</th>
<th>Allowed</th>
<th>Allowed use in the certified configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>n/a</td>
<td>Use HTTPS instead.</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Use HTTPS instead.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol Secure</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No restrictions.</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>n/a</td>
<td>If used for time synchronization, secure through HTTPS or TLS..</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
<td>Yes (snmp-trap)</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Outbound (traps) only.</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Use HTTPS instead.</td>
</tr>
<tr>
<td>SSL (not TLS)</td>
<td>Secure Sockets Layer</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Use TLS instead.</td>
</tr>
<tr>
<td>Telnet</td>
<td>A protocol used for terminal emulation</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Use HTTPS instead.</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>As described in the section 3.3 of this document.</td>
</tr>
</tbody>
</table>

The table above does not include the types of protocols and services listed here:
7 Modes of Operation

The IM&P has two modes of operation, a non-secure mode (default mode) and a mixed mode (secure mode). The Non-secure mode is the default mode when an IM&P cluster (or server) is installed fresh. In this mode, IM&P cannot provide secure signaling or media services. To enable secure mode on an IM&P server/cluster, the Certificate Authority Proxy Function (CAPF) service must be enabled on the publisher and the Certificate Trust List (CTL) service must be enabled on the publisher and subscribers. Then the cluster can be changed from non-secure mode to mixed mode. The reason it is known as mixed mode is that in this mode IM&P can support both secured and non-secured endpoints. For endpoint security, Transport Layer Security (TLS) is used for signaling and Secure RTP (SRTP) is used for media.
8 Security Measures for the Operational Environment

Proper operation of the TOE requires functionality from the environment. It is the responsibility of the authorized administrator of the TOE to ensure that the Operational Environment provides the necessary functions, and adheres to the environment security objectives listed below. The environment security objective identifiers map to the environment security objectives as defined in the Security Target.

<table>
<thead>
<tr>
<th>Security Objective for the Operational Environment</th>
<th>Definition of the Security Objective</th>
<th>Responsibility of the Administrators</th>
</tr>
</thead>
<tbody>
<tr>
<td>OE.PHYSICAL</td>
<td>Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.</td>
<td>The IM&amp;P must be installed to a physically secured location that only allows physical access to authorized personnel.</td>
</tr>
<tr>
<td>OE.NO_GENERAL_PURPOSE</td>
<td>There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.</td>
<td>None. IM&amp;P OS is not a purpose-built operating system that does not allow installation of additional software.</td>
</tr>
<tr>
<td>OE.NO_THRU_TRAFFIC_PROTECTION</td>
<td>The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.</td>
<td>Administrators will ensure protection of any critical network traffic (administration traffic, authentication traffic, audit traffic, etc.) and ensure appropriate operational environment measures and policies are in place for all other types of traffic.</td>
</tr>
<tr>
<td>OE.TRUSTED_ADMIN</td>
<td>TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.</td>
<td>Administrators must read, understand, and follow the guidance in this document to securely install and operate the TOE and maintain secure communications with components of the operational environment.</td>
</tr>
<tr>
<td>OE.UPDATES</td>
<td>The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.</td>
<td>Administrators must download updates, including psirts (bug fixes) to the evaluated image to ensure that the security functionality of the TOE is maintained</td>
</tr>
<tr>
<td>OE.ADMIN_CREDENTIALS_SECURE</td>
<td>The administrator’s credentials (private key) used to access the TOE must be protected on any other platform on which they reside.</td>
<td>Administrators must securely store and appropriately restrict access to credentials that are used to access the TOE (i.e. private keys and passwords)</td>
</tr>
</tbody>
</table>
9 Related Documentation

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation at:

With CCO login:

Without CCO login:

Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

9.1 Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click Feedback in the toolbar and select Documentation. After you complete the form, click Submit to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc., Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

9.2 Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in
the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com
10 COP FILE INSTALL README INSTRUCTIONS

Cisco Unified IM and Presence Restrict3DESCiphers Update

Release Notes Version 1
April 28, 2017

10.1 Introduction:
These release notes contain important information about installation procedures for the ciscocm.cup-restrict3des-11.5-SU3.k3.cop.sgn for Cisco Unified IM and Presence.
Before you install this Cisco Options Package (COP) file, Cisco recommends that you review the Important Notes section for information about issues that may affect your system.

10.2 Updates in This Release
DST updates are cumulative, so installing this patch will provide the ability to remove 3DES ciphers on port 8443 when Common Criteria mode is enabled.

10.3 Important Notes:
It is strongly recommended that this COP file has to be installed only If Common Criteria mode is enabled.
The changes introduced by this cop file will be lost, If there is any upgrade to new release of Cisco Unified IM Presence. So please reinstall the COP files after upgrade to new release. Please contact TAC to verify whether these COP files work on the target release or not.

10.4 Installation Instructions:
As with any installation or upgrade, it is recommended that you apply this Update during off peak hours.
When applying this Update be advised that tomcat restart is required.
This update must be installed on all machines in the cluster before the tomcat is restarted.
Tomcat can be restarted by running the following command “utils service restart Cisco Tomcat” from CLI.

Installation to all machines in the cluster is required; you must start with the Publisher. After the Update has been applied to all servers you will need to restart tomcat on all nodes in the cluster.

This package will install on the following System Versions:
- 11.5.1.13900-10 or any higher version starting with 11.5.1.13900-x

You can install a patch or upgrade version from a DVD (local source) or from a computer (remote source) that the server being upgraded can access.

Be sure to back up your system data before starting the software upgrade process. For more information, see the Disaster Recovery System Administration Guide

From Local Source:
- Step 1: Download ciscocm.cup-restrict3des-11.5-SU3.k3.cop.sgn
- Step 2: Copy the upgrade file above to a writeable CD or DVD.
- Step 3: Insert the new CD or DVD into the disc drive on the local server that is to be upgraded.
- Step 4: Open Cisco Unified Communications Operating System Administration directly by entering the following URL:
  o http://server-name/cmplatform
    - Where server-name is the host name or IP address of the admin server.
- Step 5: Enter your OS Administrator username and password.
- Step 6: Choose Software Upgrades > Install/Upgrade.
- Step 7: For the software location source, choose DVD/CD.
- Step 8: If you burned the patch file to a subdirectory on the CD or DVD, enter the path in the Directory field.
- Step 9: To continue the upgrade process, click next.
- Step 10: Choose “ciscocm.cup-restrict3des-11.5-SU3.k3.cop.sgn” and click next.
- Step 11: In the next window, monitor the progress of the download, which includes the filename and the number of megabytes that are being transferred.
  - When the download completes, the Checksum window displays.
- Step 12: Verify the checksum value:
- Step 13: After determining that the checksums match, click next to proceed with the software upgrade.
  - A Warning window displays the selected option.
Step 14: Click Install.
  - The Install Status window displays the Install log.
Step 15: When the installation completes, click Finish
Step 16: Verify the COP file version using this command from the CLI:
  - admin:show version active
    ▪ Active Master Version: 11.5.1.xxxxx-xx
  - Active Version Installed Software Options:
    ▪ ciscocm.cup-restrict3des-11.5-SU3.k3.cop<- Note: Other COP files such as this may or may not already be present on your system
    ▪ Ciscocm.dst-update.2011h-1.el5.8.6.2.cop

From Remote Source:
  - Step 1: Download ciscocm.cup-restrict3des-11.5-SU3.k3.cop.sgn
  - Step 2: Copy the upgrade to an ftp or sftp server.
  - Step 3: Open Cisco Unified Communications Operating System Administration directly by entering the following URL:
    - http://server-name/cmplatform
    ▪ Where server-name is the host name or IP address of the admin server.
  - Step 4: Enter your OS Administrator username and password.
  - Step 5: Choose Software Upgrades > Install/Upgrade.
  - Step 6: For the software location source, choose Remote File System.
  - Step 7: Enter the directory name for the software upgrade, if required.
    ▪ If the upgrade file is located on a Linux or UNIX server, you must enter a forward slash at the beginning of the directory path. For example, if the upgrade file is in the patches directory, you must enter /patches.
    ▪ If the upgrade file is located on a Windows server, check with your system administrator for the correct directory path.
  - Step 8: Enter the required upgrade information as described in the following table:
    ▪ Server: Host name or IP address of the remote server from which software will be downloaded.
    ▪ Remote User: Name of a user who is configured on the remote server.
    ▪ Remote Password: Password that is configured for this user on the remote server.
    ▪ Download Protocol: Choose sftp or ftp.
  - Step 9: To continue the upgrade process, click next.
  - Step 10: Choose “ciscocm.cup-restrict3des-11.5-SU3.k3.cop.sgn” and click Next.
  - Step 11: In the next window, monitor the progress of the download, which includes the filename and the number of megabytes that are being transferred.
    ▪ When the download completes, the Checksum window displays.
  - Step 12: Verify the checksum value:
    ▪ Checksum value for ciscocm.cup-restrict3des-11.5-SU3.k3.cop.sgn -
Cisco Unified Communications Manager IM and Presence Service (IM&P)

Common Criteria Guidance

- Step 13: After determining that the checksums match, click next to proceed with the software upgrade.
  - A Warning window displays the selected option.
- Step 14: Click Install.
  - The Install Status window displays and displays the install log.
- Step 15: When the installation completes, click Finish
- Step 16: Verify the COP file version using this command from the CLI:
  - admin:show version active
    - Active Master Version: 11.5.1.xxxxx-xx
    - Active Version Installed Software Options:
      - ciscocm.cup-restrict3des-11.5-SU3.k3.cop<-- Note: Other COP files such as this may or may not already be present on your system
      - Ciscocm.dst-updater.2011h-1.el5.8.6.2.cop