Securing the Connection between Cisco Unity Connection, Cisco Unified Communications Manager, and IP Phones

- Securing the Connection between Cisco Unity Connection, Cisco Unified Communications Manager, and IP Phones, on page 1

Securing the Connection between Cisco Unity Connection, Cisco Unified Communications Manager, and IP Phones

Introduction

In this chapter, you would find descriptions of potential security issues related to connections between Cisco Unity Connection, Cisco Unified Communications Manager, and IP phones; information on any actions you need to take; recommendations that helps you make decisions; discussion of the ramifications of the decisions you make; and best practices.

Security Issues for Connections between Unity Connection, Cisco Unified Communications Manager, and IP Phones

A potential point of vulnerability for a Cisco Unity Connection system is the connection between Unity Connection voice messaging ports (for an SCCP integration) or port groups (for a SIP integration), Cisco Unified Communications Manager, and the IP phones.

Possible threats include:

- Man-in-the-middle attacks (when the information flow between Cisco Unified CM and Unity Connection is observed and modified)
- Network traffic sniffing (when software is used to capture phone conversations and signaling information that flow between Cisco Unified CM, Unity Connection, and IP phones that are managed by Cisco Unified CM)
- Modification of call signaling between Unity Connection and Cisco Unified CM

- Modification of the media stream between Unity Connection and the endpoint (for example, an IP phone or a gateway)
- Identity theft of Unity Connection (when a non-Unity Connection device presents itself to Cisco Unified CM as a Unity Connection server)
- Identity theft of the Cisco Unified CM server (when a non-Cisco Unified CM server presents itself to Unity Connection as a Cisco Unified CM server)

Cisco Unified Communications Manager Security Features for Unity Connection Voice Messaging Ports

Cisco Unified CM can secure the connection with Unity Connection against the threats listed in the Security Issues for Connections between Unity Connection, Cisco Unified Communications Manager, and IP Phones. The Cisco Unified CM security features that Unity Connection can take advantage of are described in Table 1: Cisco Unified CM Security Features Used by Cisco Unity Connection.

Table 1: Cisco Unified CM Security Features Used by Cisco Unity Connection

Security Feature	Description
Signaling authentication	The process that uses the Transport Layer Security (TLS) protocol to validate that no tamp occurred to signaling packets during transmission. Signaling authentication relies on the c the Cisco Certificate Trust List (CTL) file. This feature protects against: • Man-in-the-middle attacks that modify the information flow between Cisco Unified Unity Connection. • Modification of the call signalling. • Identity theft of the Unity Connection server. • Identity theft of the Cisco Unified CM server.
Device authentication	The process that validates the identity of the device and ensures that the entity is what it c be. This process occurs between Cisco Unified CM and either Unity Connection voice me ports (for an SCCP integration) or Unity Connection port groups (for a SIP integration) w device accepts the certificate of the other device. When the certificates are accepted, a sec connection between the devices is established. Device authentication relies on the creatio Cisco Certificate Trust List (CTL) file. This feature protects against: • Man-in-the-middle attacks that modify the information flow between Cisco Unified Unity Connection. • Modification of the media stream. • Identity theft of the Unity Connection server. • Identity theft of the Cisco Unified CM server.

Security Feature	Description
Signaling encryption	The process that uses cryptographic methods to protect (through encryption) the confi all SCCP or SIP signaling messages that are sent between Unity Connection and Cisco Signaling encryption ensures that the information that pertains to the parties, DTMF d entered by the parties, call status, media encryption keys, and so on are protected again or unauthorized access. This feature protects against: • Man-in-the-middle attacks that observe the information flow between Cisco Unif Unity Connection. • Network traffic sniffing that observes the signaling information flow between Cisc and Unity Connection.
Media encryption	The process whereby the confidentiality of the media occurs through the use of crypto procedures. This process uses Secure Real Time Protocol (SRTP) as defined in IETF R ensures that only the intended recipient can interpret the media streams between Unity and the endpoint (for example, a phone or gateway). Support includes audio streams o encryption includes creating a Media Player key pair for the devices, delivering the ke Connection and the endpoint, and securing the delivery of the keys while the keys are Unity Connection and the endpoint use the keys to encrypt and decrypt the media strea This feature protects against: • Man-in-the-middle attacks that listen to the media stream between Cisco Unified C Connection. • Network traffic sniffing that eavesdrops on phone conversations that flow betwee Unified CM, Unity Connection, and IP phones that are managed by Cisco Unifie

Authentication and signaling encryption serve as the minimum requirements for media encryption; that is, if the devices do not support signaling encryption and authentication, media encryption cannot occur.

Cisco Unified CM security (authentication and encryption) only protects calls to Unity Connection. Messages recorded on the message store are not protected by the Cisco Unified CM authentication and encryption features but can be protected by the Unity Connection private secure messaging feature. For details on the Unity Connection secure messaging feature, see the Handling Messages Marked Private and Secure.

Self-encrypting drive

Cisco Unity Connection also supports self-encrypting drives (SED). This is also called Full Disk Encryption (FDE). FDE is a cryptographic method that is used to encrypt all the data that is available on the hard drive. The data include files, operating system and software programs. The hardware available on the disk encrypts all the incoming data and decrypts all the outgoing data. When the drive is locked, an encryption key is created and stored internally. All data that is stored on this drive is encrypted using that key and stored in the encrypted form. The FDE comprises a key ID and a security key.

For more information, see https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/gui/config/guide/2-0/b_Cisco_UCS_C-series_GUI_Configuration_Guide_201/b_Cisco_UCS_C-series_GUI_Configuration_Guide_201_chapter_010011.html#concept_E8C37FA4A71F4C8F8E1B9B94305AD844.

Security Mode Settings for Cisco Unified Communications Manager and Unity Connection

Cisco Unified Communications Manager and Cisco Unity Connection have the security mode options shown in Table 2: Security Mode Options for voice messaging ports (for SCCP integrations) or port groups (for SIP integrations).

Caution The Cluster Security Mode setting for Unity Connection voice messaging ports (for SCCP integrations) or port groups (for SIP integrations) must match the security mode setting for the Cisco Unified CM ports. Otherwise, Cisco Unified CM authentication and encryption fails.

Table 2: Security Mode Options

Setting	Effect
Non-secure	The integrity and privacy of call-signaling messages are not ensured because call-signaling messages are sent as clear (unencrypted) text connected to Cisco Unified CM through a non-authenticated port rather than an authenticated TLS port. In addition, the media stream cannot be encrypted.
Authenticated	The integrity of call-signaling messages are ensured because they are connected to Cisco Unified CM through an authenticated TLS port. However, the privacy of call-signaling messages are not ensured because they are sent as clear (unencrypted) text. In addition, the media stream is not encrypted.
Encrypted	The integrity and privacy of call-signaling messages are ensured because they are connected to Cisco Unified CM through an authenticated TLS port, and the call-signaling messages are encrypted. In addition, the media stream can be encrypted. Both end points must be registered in encrypted mode for the media stream to be encrypted. However, when one end point is set for non-secure or authenticated mode and the other end point is set for encrypted mode, the media stream are not encrypted. Also, if an intervening device (such as a transcoder or gateway) is not enabled for encryption, the media stream is not encrypted.

Best Practices for Securing the Connection between Unity Connection, Cisco Unified Communications Manager, and IP Phones

If you want to enable authentication and encryption for the voice messaging ports on both Cisco Unity Connection and Cisco Unified Communications Manager, see the *Cisco Unified Communications Manager SCCP Integration Guide for Unity Connection Release 15*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/integration/cucm_sccp/b_15cucintcucmskinny.html