配置安全设置

- 安全概述， 第 1 页
- 安全性设置配置任务流程 ， 第 1 页

安全概述

本章将介绍在 IM and Presence Service 上配置安全设置的程序。 在 IM and Presence Service 上，您可以配置安全 TLS 连接并启用增强的安全设置，例如 FIPS 模式。

IM and Presence Service 与 Cisco Unified Communications Manager 共享一个平台。 有关如何在 Cisco Unified Communications Manager 中配置安全性的信息，请参阅《*Cisco Unified Communications Manager* 安全指南》。

安全性设置配置任务流程

以下可选任务用于通过 IM and Presence Service 设置安全性。

过程

	命令或操作	目的
步骤 1	创建登录提示， 第 2 页	创建用户在登录任何 IM and Presence Service 界面时必须确认的登录提示。
步骤 2	配置安全 XMPP 连接 ， 第 2 页	完成这些任务以配置 XMPP 安全性。
步骤 3	配置 TLS 对等主题， 第 3 页	如果想要设置TLS对等节点，配置这些任务。
步骤 4	配置 TLS 上下文， 第 4 页	为您的 TLS 对等节点配置 TLS 环境和 TLS 密码。

	命令或操作	目的
步骤 5	FIPS 模式，第 4 页	如果您希望部署符合 FIPS 标准，可以启用 FIPS 模式。 为增强安全性，您还可以启用“强化安全性”模式和“通用合规性”模式。

创建登录提示

您可以创建用户在登录任何 IM and Presence Service 界面时确认的提示。 您可以使用任何文本编辑器创建一个 .txt 文件，包括希望用户了解的重要通知，然后将它上传到 Cisco Unified IM and Presence 操作系统管理页面。

此提示随后将于用户登录前在所有 IM and Presence Service 界面上显示，向用户通知重要信息，包括法律警告和义务。 以下界面将在用户登录前后显示此横幅：Cisco Unified CM IM and Presence 管理、Cisco Unified IM and Presence 操作系统管理、Cisco Unified IM and Presence 功能配置、Cisco Unified IM and Presence 报告和 IM and Presence 灾难恢复系统。

过程

步骤 1 创建包含您希望在提示中显示的内容的 .txt 文件。

步骤 2 登录到 Cisco Unified IM and Presence 操作系统管理。

步骤 3 选择**软件升级** > **定制登录消息**。

步骤 4 单击**浏览**并找到 .txt 文件。

步骤 5 单击**上传文件**。

提示将于登录前后在大多数 IM and Presence Service 界面上显示。

注释
.txt 文件必须分别上传到每个 IM and Presence Service 节点。

配置安全 XMPP 连接

此程序用于使用 TLS 启用安全 XMPP 连接。

过程

步骤 1 从 Cisco Unified CM IM and Presence 管理中，选择**系统** > **安全性** > **设置**。

步骤 2 选中相应的复选框以启用以下 XMPP 安全设置：

表 *1: IM and Presence Service* 的 *XMPP* 安全设置

设置	说明
启用 XMPP 客户端 IM/P 服务安全模式	启用后，IM and Presence Service 会与群集中的 XMPP 客户端应用程序建立安全的 TLS 连接。 此设置默认为启用。 建议不要关闭此安全模式，除非 XMPP 客户端应用程序能够在非安全模式下保护客户端登录凭证。 如果确实要关闭安全模式，请确保可以使用其他方法保护 XMPP 客户端-节点通信。
启用 XMPP 路由器-路由器安全模式	如果打开此设置，IM and Presence Service 会在同一群集或不同群集中的 XMPP 路由器之间建立安全 TLS 连接。 IM and Presence Service 会自动在群集中和跨群集复制 XMPP 证书，并将其作为 XMPP 信任证书。 XMPP 路由器将尝试与同一群集或不同群集中的任何其他 XMPP 路由器建立 TLS 连接，且可用于建立 TLS 连接。
启用 Web 客户端 IM/P 服务安全模式	如果打开此设置，IM and Presence Service 会在群集中的 IM and Presence Service 节点和基于 XMPP 的 API 客户端应用程序之间建立安全 TLS 连接。 如果打开此设置，则在 IM and Presence Service 的 cup-xmpp-trust 存放库中上传 Web 客户端的证书或签名证书。

步骤 3 单击**保存**。

下一步做什么

如果您更新了**启用 XMPP 客户端 IM/P 服务安全模式**设置，请重新启动 Cisco XCP 连接管理器。

IM and Presence Service 上的 SIP 安全性设置配置

配置 TLS 对等主题

导入 IM and Presence Service 证书时，IM and Presence Service 会自动尝试将 TLS 对等主题添加到 TLS 对等主题列表和 TLS 上下文列表中。 确认已根据您的要求设置 TLS 对等主题和 TLS 上下文配置。

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中选择**系统** > **安全性** > **TLS 对等主题**。

步骤 2 单击**新增**。

步骤 3 对“对等主题名称”执行以下操作之一：

a) 输入节点显示的证书的主题 CN。

b) 打开证书，查找 CN 并将其粘贴在此处。

步骤 4 在“说明”字段中输入节点的名称。

步骤 5 单击保存。

下一步做什么

继续配置 TLS 上下文。

配置 TLS 上下文

此程序用于将 TLS 环境和 TLS 对等密码分配给您的 TLS 对等主题。

注释 导入 IM and Presence Service 证书时，IM and Presence Service 会自动尝试将 TLS 对等主题添加到 TLS 对等主题列表和 TLS 环境列表中。

开始之前

配置 TLS 对等主题 ， 第 3 页

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中，选择 **系统** > **安全性** > **TLS 环境配置**。

步骤 2 单击**查找**。

步骤 3 选择 **Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context**。

步骤 4 从可用 TLS 对等主题列表中选择已配置的 TLS 对等主题。

步骤 5 使用 > 箭头将此 TLS 对等主题移至**选定 TLS 对等主题**。

步骤 6 配置 **TLS 密码映射**选项：

a) 查看**可用的 TLS 密码**和**所选的 TLS 密码**框中可用的 TLS 密码列表。

b) 如果要启用当前未选定的 TLS 密码，使用 > 箭头将该密码移至**所选的 TLS 密码**。

步骤 7 单击**保存**。

步骤 8 重新启动 Cisco SIP Proxy 服务：

a) 在 Cisco Unified IM and Presence 功能配置中，选择**工具** > **控制中心 - 功能服务**。

b) 从**服务器**下拉列表框中选择 IM and Presence Service 群集节点，然后单击**前往**。

c) 选择 **Cisco SIP Proxy** 服务并单击**重新启动**。

FIPS 模式

IM and Presence Service 包含一组增强的系统安全模式，允许您的系统在一组更严格的安全准则和风险管理控制举措下运行，这些控制举措涉及密码学、数据和信号加密以及审计日志记录等事项。

- FIPS 模式 — IM and Presence Service 可以配置为在 FIPS 模式下运行，这样可确保您的系统符合美国和加拿大加密模块政府标准 — 联邦信息处理标准 (FIPS)。
- 增强的安全模式 — 增强的安全模式在启用 FIPS 的系统上运行，并提供其他风险管理控制举措，如数据加密要求、更严格的凭证策略、联系人搜索用户验证，以及更严格的审计日志记录要求。
- 通用标准模式 — 通用标准模式还在启用 FIPS 的系统上运行，提供额外的控制举措，使得您的系统符合 TLS 等通用标准指南并能够使用 X.509 v3 证书。

注释 如果外部数据库为 MSSQL，要让消息存档程序、文字会议管理器和文件传输管理器等服务在通用条件模式下工作，您必须执行以下操作：

1. 配置托管 MSSQL 数据库的服务器，以支持 TLS 1.1 或更高版本。
2. 将数据库证书重新上传到 IM and Presence Service。
3. 选中**外部数据库配置**页面中的**启用 SSL** 复选框。 选择 **Cisco Unified CM IM and Presence 管理** > **消息** > **外部服务器设置** > **外部数据库**以配置外部数据库。

重要事项 此备注仅适用于版本 12.5(1)SU7。

如果群集上有多服务器 SAN 证书配置，则可将群集移至 FIPS 和通用标准模式。 它会将多服务器 SAN 证书转换为自签证书。

如果旧的多服务器 SAN 证书在 FIPS 和通用标准模式中仍在统一通信管理器服务器上，则需要将其手动删除。

有关如何在 Cisco Unified Communications Manager 和 IM and Presence Service 中启用 FIPS 模式、增强的安全模式和通用标准模式的详细信息，请参阅《*Cisco Unified Communications Manager* 安全指南》的“FIPS 模式设置”一章，网址：https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

Outlook 日历集成的 FIPS

在 IM and Cisco Presence Service 服务器上启用 FIPS 模式时，仅支持使用 NTLMv2 来获取 Exchange Web 服务信息。 如果禁用了 FIPS 模式，则根据现有行为支持 NTLMv1 和 NTLMv2。 在两种情况下均支持基本验证，无论启用还是禁用 FIPS 模式。

引入了一个新的名为 **FIPS 模式 Exchange 服务器身份验证**服务参数，以验证 Presence Engine 使用的身份验证类型，从而通过 Microsoft Outlook 日历集成功能与 Exchange 服务器建立连接。

您可以将 **FIPS 模式 Exchange 服务器身份验证**服务参数设置为**自动**或**仅基本**。

服务参数设置为**自动**：Presence Engine 先协商 NTLMv2，然后在 NTLMv2 协商失败时回退到仅“基本身份验证”。 NTLMv1 在 FIPS 模式下不会协商。

服务参数设置为**仅基本**：即使 Exchange 服务器配置为允许 NTLM 和基本身份验证时，系统会强制 Presence Engine 使用“基本身份验证”。

注释 服务参数设置中的任何更改都要求重新启动 Cisco Presence Engine。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。