Cisco Unified Communications Manager 和 IM and Presence 服务管理指南，版本 12.0 (1)

首次发布日期: 2017 年 08 月 23 日

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

本手册中有关产品的规格和信息如有更改，恕不另行通知。我们相信本手册中的所有声明、信息和建议均准确可靠，但不为其提供任何明示或暗示的担保。用户必须承担使用产品的全部责任。

随附产品的软件许可和有限保证在随产品一起提供的信息包中阐明，且构成本文的一部分。如果您无法找到软件许可证或有限保证，请向您的思科代表索取。

思科所采用的TCP报头压缩是加州大学伯克利分校(UCB)开发的一个程序的改版，是UCB的UNIX操作系统公共域版本的一部分。保留所有权利。版权所有© 1981, Regents of the University of California。

无论本手册中是否有任何其他保证，这些供应商的所有文档文件和软件均“按原样”提供，并可能包含缺陷。思科和上述供应商拒绝作任何明示或暗示的保证，包括（但不限于）适销性、特定目的适用性、非侵权或出于交易、使用或买卖而产生的保证。

在任何情况下，对于任何间接、特殊、连带发生或偶发的损坏，包括（但不限于）因使用或无法使用本手册而导致的任何利润损失或数据损失或损坏，思科及其供应商概不负责，即使思科及其供应商已获知此类损坏的可能性也不例外。

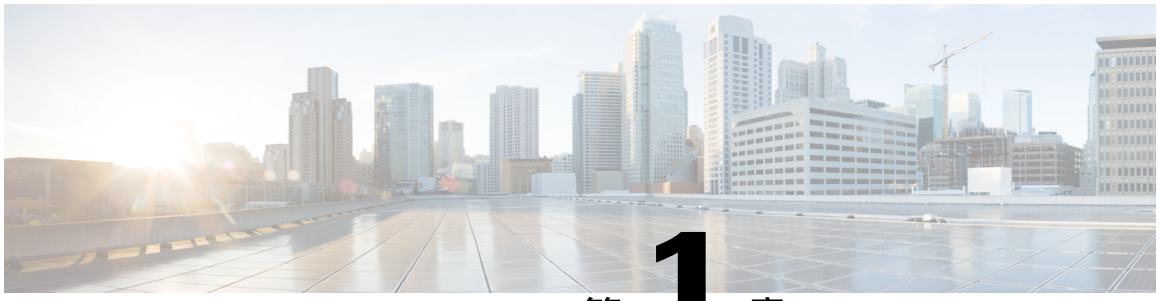
本文档中使用的所有互联网协议 (IP) 地址和电话号码都是虚构的。此文档中的所有示例、命令显示输出、网络拓扑图和其它图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。

Cisco和Cisco徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标列表，请访问此URL：http://www.cisco.com/go/trademarks。文中提及的第三方商标均属于其各自所有者。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。(1110R)

目 录

第 I 部分

管理概述



第 1 章

管理概述

Cisco Unified CM 管理概述

“Cisco Unified CM 管理”是一个基于 Web 的应用程序，是 Cisco Unified Communications Manager 的主要管理和配置界面。您可以使用“Cisco Unified CM 管理”为您的系统配置广泛的项目，包括一般系统组件、功能、服务器设置，呼叫路由规则、电话、最终用户，以及媒体资源。

配置菜单

“Cisco Unified CM 管理”的配置窗口组织于以下菜单下：

- 系统 — 使用此菜单下的配置窗口配置常规系统设置，例如服务器信息、NTP 设置、日期和时间组、区域、DHCP、LDAP 集成，以及企业参数。
- 呼叫路由 — 使用此选项卡下的配置窗口配置有关 Cisco Unified Communications Manager 如何路由呼叫的项目，包括路由模式、路由组、寻线引导、拨号规则、分区、呼叫搜索空间、目录号码，以及转换模式。
- 媒体资源 — 使用此选项卡下的配置窗口配置媒体资源组、会议桥、报警器和代码转换器等项目。
- 高级功能 — 使用此选项卡下的配置窗口配置诸如语音邮件引导、留言通知以及呼叫控制坐席配置文件等功能。

- 设备 — 使用此选项卡下的配置窗口设置设备，例如电话、IP 电话服务、干线、网关、软键模板和 SIP 配置文件。
- 应用程序 — 使用此选项卡下的配置窗口下载并安装插件，例如 Cisco Unified JTAPI、Cisco Unified TAPI 和 Cisco Unified 实时监控工具。
- 用户管理—使用“用户管理”选项卡下的配置窗口为您的系统配置最终用户和应用程序用户。
- 批量管理 — 使用批量管理工具一次导入和配置大量最终用户或设备。
- 帮助 — 单击此菜单可访问联机帮助系统。联机帮助系统包含诸多文档，可帮助您为系统上不同的配置窗口配置设置。

操作系统管理概述

使用“Cisco Unified Communications 操作系统管理”配置和管理您的操作系统并执行以下管理任务：

- 检查软件和硬件状态
- 检查和更新 IP 地址
- Ping 其他网络设备
- 管理 NTP 服务器
- 升级系统软件和选项
- 管理节点安全性，包括 IPsec 和证书
- 管理远程支持帐户
- 重新启动系统

操作系统状态

您可以检查各种操作系统组件的状态，包括以下组件：

- 群集和节点
- 硬件
- 网络
- 系统
- 安装的软件和选项

操作系统设置

您可以查看和更新以下操作系统设置：

- IP — 更新安装应用程序时您输入的 IP 地址和 DHCP 客户端设置。
- NTP 服务器设置 — 配置外部 NTP 服务器的 IP 地址；添加 NTP 服务器。

- SMTP 设置 — 配置操作系统将用来发送电子邮件通知的简单邮件传输协议 (SMTP) 主机。

操作系统安全配置

您可以管理安全证书和 IPsec 设置。从**安全**菜单中，您可以选择以下安全选项：

- 证书管理 — 管理证书和证书签名请求 (CSR)。您可以显示、上载、下载、删除和重新生成证书。通过证书管理，您还可以监控节点上的证书过期时间。
- IPsec 管理 — 显示或更新现有的 IPsec 策略；设置新的 IPsec 策略和关联。

软件升级

您可以升级运行在操作系统上的软件版本，或者安装特定的软件选项，包括 Cisco Unified Communications 操作系统区域设置安装程序、拨号方案，以及 TFTP 服务器文件。

从**安装/升级**菜单选项，您可以从本地磁盘或远程服务器升级系统软件。升级后的软件安装在非活动分区上，然后您可以重新启动系统并切换分区，这样系统就可以在较新的软件版本上运行。有关详细信息，请参阅《*Cisco Unified Communications Manager* 升级指南》，位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html。

注释 您必须通过 Cisco Unified Communications 操作系统界面和 CLI 中包含的软件升级功能执行所有的软件安装和升级。系统只能上载和处理 Cisco Systems 认可的软件。您无法安装或使用第三方或基于 Windows 的软件应用程序。

服务

应用程序提供以下操作系统实用程序：

- Ping — 检查与其他网络设备的连通性。
- 远程支持 — 设置一个 Cisco 支持人员可以用来访问系统的帐户。此帐户会在您指定的天数后自动过期。

CLI

您可以从操作系统或通过到服务器的安全外壳连接访问 CLI。有关详细信息，请参阅《*Cisco Unified Communications* 解决方案的命令行界面参考指南》，位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

验证的网络时间协议支持

此发行版支持 Cisco Unified Communications Manager 的验证的网络时间协议 (NTP) 功能。增加此支持是为了保护 NTP 服务器到 Cisco Unified Communications Manager 的连接。在以前的版本中，Cisco Unified Communications Manager 到 NTP 服务器的连接没有安全保护。

此功能以基于对称密钥的验证为基础，并受 NTPv3 和 NTPv4 服务器支持。Cisco Unified Communications Manager 仅支持基于 SHA1 的加密。基于 SHA1 的对称密钥支持可从 NTP 版本 4.2.6 或更高版本获得。

- 对称密钥
- 无身份验证

您可以通过 **Cisco Unified 操作系统管理**应用程序的管理 CLI 或 **NTP 服务器列表**页面检查 NTP 服务器的验证状态。

Cisco Unified 功能配置概述

“Cisco Unified 功能配置”是基于 Web 的故障排除工具，提供许多服务、警报和协助管理员管理其系统的工具。“Cisco Unified 功能配置”为管理员提供的功能包括：

- 启动和停止服务 — 管理员可以设置各式各样的服务，以帮助管理员管理其系统。例如，您可以启动 Cisco CallManager 功能配置 RTMT 服务，从而允许管理员使用实时监控工具监控系统的运行状况。
- SNMP — SNMP 便于在网络设备（例如节点、路由器等等）之间交换管理信息。作为 TCP/IP 协议组的一部分，SNMP 可让管理员远程管理网络性能、查找并解决网络问题，以及计划网络增长。
- 警报 — 警报提供有关运行时状态和系统状态的信息，以便您能够对与系统有关的问题进行故障排除。
- 跟踪 — 跟踪工具可以帮助您排查语音应用程序问题。
- Cisco 功能配置报告程序 — Cisco 功能配置报告程序会在“Cisco Unified 功能配置”中生成每日报告。
- SNMP — SNMP 便于在网络设备（例如节点、路由器等等）之间交换管理信息。作为 TCP/IP 协议组的一部分，SNMP 可让管理员远程管理网络性能、查找并解决网络问题，以及计划网络增长。
- CallHome — 配置 Cisco Unified Communications Manager Call Home 功能，允许 Cisco Unified Communications Manager 与 Smart Call Home 后端服务器通信，并将诊断告警、库存，以及其他消息发送给该服务器

附加管理界面

使用 Cisco Unified 功能配置，您可以启动允许您使用以下附加管理界面的服务：

- 实时监控工具 —“实时监控工具”是一个基于 Web 的界面，可帮助您监控系统的运行状况。使用 RTMT，您可以查看警报、计数器和包含系统运行状况详细信息的报告。
- 被叫号码分析器—"被叫号码分析器"是一个基于Web的界面，可以帮助管理员排查拨号方案问题。

- Cisco Unified CDR 分析和报告 — “CDR 分析和报告”会收集呼叫详细信息记录，显示您系统上发出的呼叫的详细信息。

有关如何使用 Cisco Unified 功能配置的详细信息，请参阅《*Cisco Unified* 功能配置管理指南》，位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

Cisco Unified 报告概述

Cisco Unified 报告 Web 应用程序在 Cisco Unified Communications Manager 和 Cisco Unified Communications Manager IM and Presence 服务控制台访问，会为故障排除或检查群集数据生成汇总的报告。

此工具提供了一种简单的方法来大概了解群集数据。该工具可从现有来源收集数据、比较数据，以及报告违规。当您在“Cisco Unified 报告”中生成报告时，报告会将来自一台或多台服务器上的一个或多个来源的数据合并到一个输出视图中。例如，您可以查看以下报告以帮助管理您的系统：

- Unified CM 群集概要 — 查看此报告可大概了解您的群集，包括 Cisco Unified Communications Manager 和 IM and Presence 服务版本、服务器主机名，以及硬件详细信息。
- 电话功能列表—如果您要配置功能，可查看此报告。此报告会提供一个哪些电话支持哪些Cisco Unified Communications Manager 功能的列表。
- 没有线路的 Unified CM 电话 — 查看此报告可了解您群集中的哪些电话没有电话线路。

要查看通过“Cisco Unified 报告”提供的报告的完整列表，以及如何使用应用程序的说明，请参阅《*Cisco Unified* 报告管理指南》，位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

灾难恢复系统概述

灾难恢复系统 (DRS) 可从 Cisco Unified Communications Manager 管理调用，它提供完整的数据备份和恢复功能。灾难恢复系统允许您定期执行计划的自动或用户调用的数据备份。

DRS 恢复其自己的设置（备份设备设置和计划设置）作为平台备份/恢复的一部分。DRS 备份和恢复 `drfDevice.xml` 和 `drfSchedule.xml` 文件。使用这些文件恢复服务器时，您无需重新配置 DRS 备份设备和计划。

灾难恢复系统包括以下功能：

- 用于执行备份和恢复任务的用户界面。
- 用于执行备份和恢复功能的分布式系统体系结构。
- 计划的备份。
- 将备份存档到物理磁带驱动器或远程 SFTP 服务器。

批量管理工具概述

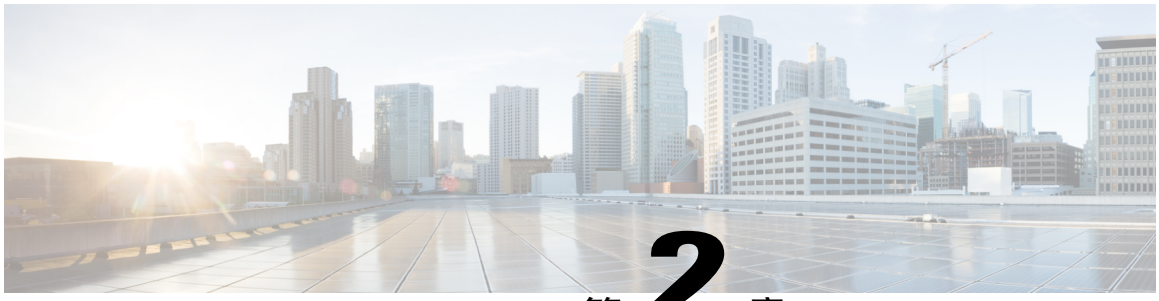
在 Cisco Unified CM 管理中，使用“批量管理”菜单和子菜单选项通过批量管理工具在 Cisco Unified Communications Manager 中配置实体。

Cisco Unified Communications Manager 批量管理工具 (BAT) 是一个基于 Web 的应用程序，让管理员可以批量处理 Cisco Unified Communications Manager 数据库中的事务。BAT 可用于同时添加、更新或删除大量类似的电话、用户或端口。使用 Cisco Unified CM 管理时，每个数据库事务都需要个别的手动操作，而 BAT 可以自动执行处理，实现更快的添加、更新和删除操作。

您可以对下列类型的设备和记录使用 BAT：

- 添加、更新和删除 Cisco Unified IP Phone，网关、电话、计算机电话接口 (CTI) 端口和 H.323 客户端
- 添加、更新及删除用户、用户设备配置文件、Cisco Unified Communications Manager Assistant 经理和助理
- 添加或删除强制授权码和客户码
- 添加或删除呼叫代答组
- 填充或清空区域矩阵
- 插入、删除或导出访问列表
- 插入、删除或导出远程目标和远程目标配置文件
- 添加基础设施设备

有关如何使用批量管理工具的详细信息，请参阅《*Cisco Unified Communications Manager* 批量管理指南》。



第 2 章

入门

登录到管理界面

使用此步骤登录系统中的任何管理界面。

过程

步骤 1 打开 Web 浏览器上的 Unified Communications Manager 界面。

步骤 2 选择**导航**下拉列表中的管理界面。

步骤 3 单击**转至**。

步骤 4 输入您的用户名和密码。

步骤 5 单击**登录**。

重置管理员或安全密码

如果管理员密码丢失，不能访问系统，请按照此步骤重置密码。

开始之前

- 您需要对执行此步骤的节点拥有物理访问权限。
- 任何时候，当要求插入 CD 或 DVD 介质时，您必须通过 vSphere 客户端为 VMWare 服务器安装 ISO 文件。请参阅此处的“《添加 DVD 或 CD 驱动器至虚拟机》”。

- 群集中所有节点的安全密码都必须匹配。修改所有机器的安全密码，否则群集节点不会通信。

过程

步骤 1 使用以下用户名和密码登录发布方节点上的 CLI：

a) 用户名：pwrecovery

b) 密码：pwreset

步骤 2 按任意键继续。

步骤 3 如果光盘驱动器中有有效 CD/DVD 或您已安装 ISO 文件，将其从 VMWare 客户端删除。

步骤 4 按任意键继续。

步骤 5 将有效 CD 或 DVD 插入驱动器，或安装 ISO 文件。

注释 对于此测试，必须使用仅含有数据的光盘或 ISO 文件。

步骤 6 系统确认上一步后，将提示您输入以下选项之一继续：

- 输入 **a** 重置管理员密码。
- 输入 **s** 重置安全密码。

  注释 更改安全密码后，必须重置群集中的各节点。重新启动节点失败将导致系统服务问题以及订阅方节点管理窗口出现问题。

步骤 7 输入新密码，然后再次输入以确认。

管理员凭证必须以字母字符开头，并且长度至少为六个字符，可以包含字母数字字符、连字符和下划线。

步骤 8 系统确认新密码的强度后，密码将被重置，且系统会提示您按任意键退出密码重置实用程序。

如果要设置不同的管理员密码，可使用 CLI 命令 **set password**。有关详细信息，请参阅《*Cisco Unified* 解决方案的命令行界面指南》：http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

关闭或重新启动系统

如果需要（例如在配置更改后）关闭或重新启动系统，请执行此步骤。

开始之前

如果服务器被强制从虚拟机关闭并重新启动，文件系统可能会损坏。为避免强制关闭，此步骤之后或从 CLI 运行 **utils system shutdown** 命令后等待服务器正确关闭。

过程

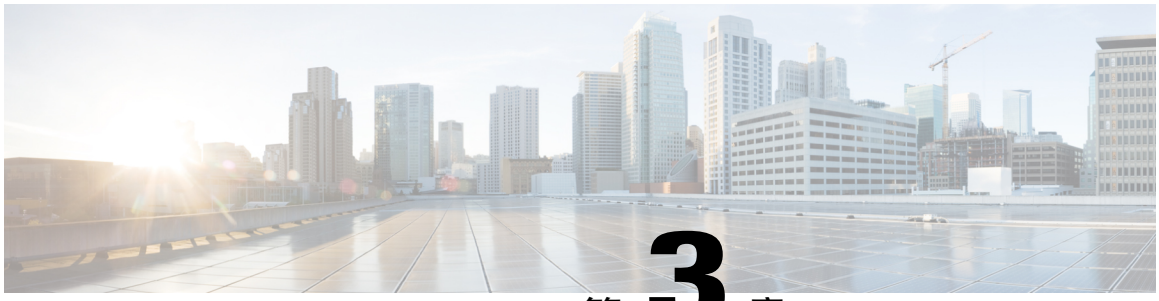
步骤 1 从 Cisco Unified 操作系统管理中，选择**设置** > **版本**。

步骤 2 执行以下操作之一：

- 单击**关闭**停止所有进程并关闭系统。
- 单击**重新启动**停止所有进程并重新启动系统。

第 II 部分

管理用户



第 3 章

管理用户访问

用户访问概述

您可以通过将以下项目分配给最终用户，管理用户对 Cisco Unified Communications Manager 的访问：

- 角色
- 访问控制组
- 用户等级

角色、访问控制组和用户等级控制措施可为 Cisco Unified Communications Manager 提供多个级别的安全性。每个角色定义一组对于 Cisco Unified Communications Manager 中特定资源的权限。当您将一个角色分配给一个访问控制组，然后将最终用户分配给该访问控制组时，您会授予那些最终用户由该角色定义的所有访问权限。

用户等级框架会覆盖角色和访问控制组框架，并控制哪些组可以用于最终用户。最终用户和应用程序用户只能被分配给用户等级允许的访问控制组。

角色概述

当部署最终用户时，您必须决定要将什么角色分配给您的用户。您可以将角色分配给最终用户、应用程序用户或访问控制组。您可以向单个用户分配多个角色。

每个角色都包含一组连接到特定资源或应用程序的权限。例如，“标准 CCM 最终用户”角色为分配了该角色的用户提供访问 Cisco Unified Communications Self Care 门户的权限。您还可以分配提供

权限访问各种资源的角色，这些资源例如 Cisco Unified Communications Manager 管理，Cisco CDR 分析和报告、被叫号码分析器，以及 CTI 接口。对于具有图形用户界面的大多数资源，例如特定配置窗口，附加到角色的权限允许用户在该窗口或一组相关窗口中查看或更新数据。

配置和分配角色

您必须决定是要将标准角色分配给用户，还是创建自定义角色：

- 标准角色 — 标准角色是预定义的默认角色，在 Cisco Unified Communications Manager 中预先安装。您无法以任何方式编辑权限或修改角色。
- 自定义角色 — 自定义角色是您创建的角色。当没有标准角色包含要分配给用户的权限时，您可以创建自定义角色。例如，如果您想分配一个标准角色，但想要修改其中一个权限，您可以将标准角色的权限复制到自定义角色中，然后编辑该自定义角色的权限。

权限类型

每个角色都包含一组连接到特定资源的权限。您可以为资源分配两种类型的权限：

- 读取 — 读取权限使用户能够查看该资源的设置，但用户无法进行任何配置更新。例如，该权限可以允许用户查看特定配置窗口上的设置，但该应用程序的配置窗口不会显示更新按钮或图标。
- 更新 — 更新权限使用户能够修改该资源的设置。例如，该权限可以允许用户在特定配置窗口中进行更新。

最终用户和管理员角色

“标准 CCM 最终用户”角色为最终用户提供访问 Cisco Unified Communications Self Care 门户的权限。对于其他权限，例如 CTI 访问，您必须分配其他角色，例如“启用标准 CTI”角色。

“标准 CCM 管理员用户”角色是所有管理任务的基础角色，可用作验证角色。此角色为用户提供对“Cisco Unified Communications Manager 管理”用户界面的管理性访问权限。“Cisco Unified Communications Manager 管理”将此角色定义为登录“Cisco Unified Communications Manager 管理”所必需的角色。

相关主题

标准角色和访问控制组 ， 第 28 页

访问控制组概述

您可以使用访问控制组与角色，快速将网络访问权限分配给一组具有相似访问需求的用户。

访问控制组是一个包含最终用户和应用程序用户的列表。您可以将具有类似访问需求的最终用户或应用程序用户分配给一个包含其所需角色和权限的访问控制组。对于要分配到访问控制组的最终用户或应用程序用户，用户必须符合该访问控制组的最低等级要求。例如，如果最终用户的用户等级为 4，则该用户只可以分配到最低等级要求介于 4 到 10 之间的访问控制组。

系统包含一组预定义的标准访问控制组。每个标准访问控制组有一组默认分配的角色。当您将用户分配到该访问控制组时，这些角色也会被分配给该最终用户。

您无法编辑分配给标准访问控制组的角色。但是，您可以创建自定义的访问控制组，并将选择的角色分配到您的自定义访问控制组。

相关主题

标准角色和访问控制组，第 28 页

用户等级概述

“用户等级访问控制”提供了一组对于访问级别的控制，管理员可以提供给最终用户或应用程序用户。**用户等级**参数是一个 1 到 10 的整数，1 为可能的最高等级。用户等级会被分配给用户和访问控制组，从而创建一个等级层次结构，该层次结构管理哪些用户可以被分配给特定的访问控制组。

在部署最终用户或应用程序用户时，管理员必须为每个用户分配用户等级。管理员还必须为每个访问控制组分配用户等级。管理员可以将用户仅分配到那些具有相同或更低等级的访问控制组。例如，如果最终用户的用户等级为 3，则他们可以分配到用户等级介于 3 到 10 之间的访问控制组。该用户不能分配给要求用户等级为 1 的访问控制组。

管理员可以在**用户等级配置**窗口中自定义用户等级层次结构，然后将这些等级分配给最终用户、应用程序用户和访问控制组。

用户访问前提条件

在创建新角色或访问控制组之前，请查看您的系统中预安装的标准角色和访问控制组，以检查现有访问控制组是否包含您需要为用户配置的角色和权限。

有关详细信息，请参阅标准角色和访问控制组，第 28 页。

用户访问配置任务流程

执行以下任务以配置用户访问。

过程

	命令或操作	目的
步骤 1	创建自定义用户等级，第 18 页	通过创建自定义用户等级设置用户等级层次结构。
步骤 2	使用以下方法之一创建新角色： • 创建自定义角色，第 19 页 • 复制角色，第 19 页	使用“创建”程序进行创建，并从头开始配置新角色。 如果新角色与标准角色具有相似的设置，可使用“复制”命令。您可以从现有的标准角色将权限设置复制到新角色。然后，可以编辑新角色中的设置。
步骤 3	使用以下方法之一创建访问控制组：	使用“创建”程序进行创建，并配置一个新的访问控制组。

	命令或操作	目的
	• 创建访问控制组，第 20 页 • 复制访问控制组，第 21 页	如果新的访问控制组与默认组之一非常相似，则可以使用“复制”命令。您可以从现有组中将角色分配复制到新组，然后进行编辑。
步骤 4	为访问控制组分配角色，第 21 页	通过添加或删除角色，更新访问控制组已分配的角色。
步骤 5	向访问控制组分配用户，第 22 页	通过添加或从组中删除用户，更新访问控制组的用户列表。分配到该群组的所有用户都将具有在分配给该组的角色中配置的权限。
步骤 6	查看用户权限报告，第 23 页	可选。如需查看已为用户分配的访问权限，请查看该用户的权限报告。
步骤 7	为访问控制组配置重叠权限策略，第 24 页	可选。配置 Cisco Unified Communications Manager 如何处理可能由访问控制组分配导致的重叠用户权限。这是为了涵盖最终用户被分配到多个访问控制组，而每个访问控制组都有冲突的角色和权限设置的情况。
步骤 8	创建自定义技术支持角色任务流程，第 24 页	可选。有些公司希望其技术支持人员拥有能够执行某些管理任务的权限。为技术支持团队成员配置角色和访问控制组，以允许他们执行一些任务，例如添加电话和添加最终用户。
步骤 9	删除访问控制组，第 27 页	可选。如需从系统中删除访问控制组，请使用此程序。

创建自定义用户等级

使用此程序为您的等级层次结构创建自定义用户等级。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**用户管理** > **用户设置** > **用户等级**。

步骤 2 单击**新增**。

步骤 3 从**用户等级**下拉菜单中，选择一个介于 1 到 10 之间的等级设置。最高等级为 1。

步骤 4 输入**等级名称**和**说明**。

步骤 5 单击**保存**。

创建自定义角色

执行此程序创建一个自定义角色并为该角色配置权限。如果没有系统定义的标准角色与您要分配给用户的权限匹配，您不妨创建一个自定义角色。

过程

步骤 1 在 Cisco Unified CM 管理中，单击**用户管理** > **用户设置** > **角色**。

步骤 2 从**应用程序**下拉列表框中，选择与此角色关联的应用程序。
此时将显示**角色配置**窗口。

步骤 3 单击**下一步**。

步骤 4 在**名称**文本框中，输入角色的名称。
名称最多可包含 128 个字符。有效字符包括字母、数字、连字符、点（英文句号）、空格以及下划线。

步骤 5 在**说明**文本框中，输入角色的说明。
说明最多可包含 128 个字符。

步骤 6 对于新角色中的每种资源，按如下说明编辑权限：

- 如果希望角色能够查看该资源，单击**读取**复选框
- 如果希望角色能够编辑该资源，单击**更新**复选框
- 如果希望角色能够查看和编辑该资源，将**读取**和**更新**复选框都选中
- 如果不希望角色对该资源有任何访问权限，将两个复选框都保留未选中状态。

步骤 7 单击**授予所有访问权限**或**拒绝所有访问权限**按钮，以授予或删除此角色访问页面上显示的所有资源的权限。

注释 如果资源列表包含多个页面，则此按键仅适用于当前页面上显示的资源。要更改对其他页面上所列资源的访问权限，必须显示这些页面并在各页面上单击此按钮。

步骤 8 单击**保存**。

接下来的操作

执行以下程序之一设置新的访问控制组：

- 创建访问控制组，第 20 页
- 复制访问控制组，第 21 页

复制角色

执行以下程序，通过将设置从标准角色复制到新角色，从而创建一个新角色。Cisco Unified Communications Manager 不允许您在标准角色中编辑权限，但您可以在您创建的角色中编辑权限。

过程

步骤 1 在 Cisco Unified Communications Manager 管理中，单击**用户管理** > **用户设置** > **角色**。

步骤 2 单击**查找**并选择要复制其资源和权限的角色。

步骤 3 单击**复制**。

步骤 4 输入新角色的名称，然后单击**确定**。
角色配置窗口将会显示新角色的设置。新角色的权限与您复制的角色的权限相同。

步骤 5 对于新角色中的任何资源，按如下说明编辑权限：

- 选中**读取**复选框以允许用户查看资源。
- 选中**更新**复选框以允许用户编辑资源。
- 要限制对资源的访问，将两个复选框都保留未选中状态。

步骤 6 单击**保存**。

接下来的操作

要为用户分配角色，您必须创建一个新的访问控制组，并将角色分配给该组。请执行以下程序之一创建新的访问控制组：

- 创建访问控制组，第 20 页
- 复制访问控制组，第 21 页

创建访问控制组

执行此程序以创建新的访问控制组。

开始之前

如果访问控制组与现有的组具有相似的设置，您可以使用“复制”命令将现有组的设置复制到您创建的新组。

复制访问控制组，第 21 页

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户设置** > **访问控制组**。

步骤 2 单击**新增**。

步骤 3 输入访问控制组的**名称**。

步骤 4 从**可用于具有以下用户等级的用户**下拉列表中，为要分配给该组的用户选择最低用户等级。默认用户等级为 1。

步骤 5 单击**保存**。

接下来的操作

为访问控制组分配角色， 第 21 页

复制访问控制组

执行以下任务，通过将角色设置从现有的访问控制组复制到可以编辑的新组，从而创建一个新的访问控制组。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户设置** > **访问控制组**。

步骤 2 单击**查找**并选择要复制其设置的访问控制组。

步骤 3 单击**复制**。

步骤 4 输入新访问控制组的名称并单击**确定**。

步骤 5 从**可用于具有以下用户等级的用户**下拉列表中，为要分配给该组的用户选择最低用户等级。

步骤 6 单击**保存**。

接下来的操作

如需查看和编辑分配给访问控制组的角色：

为访问控制组分配角色， 第 21 页

为访问控制组分配角色

使用此程序将角色分配给访问控制组。如果您从现有组中复制访问控制组设置，则您可能还需要删除角色。

具有完全访问权限的用户，例如管理员，可以为访问控制组分配角色或删除角色。已分配有角色的访问控制组有权访问角色所包含的所有资源。

注释 当您向访问控制组分配角色时，应当分配“标准 Unified CM 管理用户”角色。此角色使用户可以登录 Unified CM 管理。

开始之前

如果您需要创建新的访问控制组，请执行以下任务之一：

- 复制访问控制组， 第 21 页
- 创建访问控制组， 第 20 页

过程

步骤 1 选择**用户管理** > **用户设置** > **访问控制组**。
此时将显示**查找并列出访问控制组**窗口。

步骤 2 单击**查找**并选择要向其分配角色的访问控制组。
此时将显示“访问控制组配置”窗口。

步骤 3 从**相关链接**下拉列表中，选择**将角色分配到访问控制组**，然后单击**转至**。
随即会显示**角色分配**窗格。

步骤 4 如果想要向访问控制组添加新角色，请执行以下操作：

a) 单击**将角色分配到组**。
b) 单击**查找**以搜索角色列表。
c) 选择您想要添加到此访问控制组的角色。
d) 单击**添加选定项**。
新角色会出现在“角色”列表框中。

步骤 5 如果您想要从访问控制组删除已分配的角色，请执行以下操作：

a) 在**角色**列表框中，突出显示您要删除的角色。
b) 单击**删除角色分配**。

步骤 6 单击**保存**。
角色分配将添加到数据库中的访问控制组。

接下来的操作

向访问控制组分配用户， 第 22 页

向访问控制组分配用户

完成此任务，以通过分配新用户或删除现有用户，更新访问控制组中的最终用户或应用程序用户列表。

注释 您只能添加那些用户等级与访问控制组的最低用户等级相同或更高的用户。

开始之前

为访问控制组分配角色，第 21 页

过程

步骤 1 选择**用户管理** > **用户设置** > **访问控制组**。
此时将出现**查找并列出访问控制组** 窗口。

步骤 2 单击**查找**并选择要为其更新用户列表的访问控制组。

步骤 3 单击**查找**以显示用户列表。

步骤 4 如果想要将最终用户或应用程序用户添加到访问控制组，请执行以下操作：

a) 单击**将最终用户添加到访问控制组**或**将应用程序用户添加到访问控制组**。
b) 选择要添加的用户。
c) 单击**添加选定项**。

步骤 5 如果想要从访问控制组删除用户：

a) 选择要删除的用户。
b) 单击**删除选定项**。

步骤 6 单击**保存**。

接下来的操作

可选。如果需要查看特定最终用户或应用程序用户的用户权限报告，请参阅以下内容：

- 查看用户权限报告，第 23 页

查看用户权限报告

执行以下程序以查看现有最终用户或现有应用程序用户的用户权限报告。用户权限报告会显示访问控制组、角色和分配给最终用户或应用程序用户的访问权限。

过程

步骤 1 在 Cisco Unified CM 管理中，执行以下步骤之一：

- 对于最终用户，选择**用户管理** > **最终用户**。

- 对于应用程序用户，选择**用户管理** > **应用程序用户**。

步骤 2 单击**查找**并选择您要为其查看访问权限的用户

步骤 3 从**相关链接**下拉列表中，选择**用户权限报告**，然后单击**转至**。
随即会出现“用户权限”窗口。

为访问控制组配置重叠权限策略

配置 Cisco Unified Communications Manager 如何处理可能由访问控制组分配导致的重叠用户权限。这是为了涵盖最终用户被分配到多个访问控制组，而每个访问控制组都有冲突的角色和权限设置的情况。

过程

步骤 1 在“Cisco Unified CM 管理”中，选择**系统** > **企业参数**。

步骤 2 在**用户管理参数**下方，如下所示为**重叠用户组和角色的有效访问权限**配置以下值之一：

- **最大值** — 有效权限代表所有重叠访问控制组的最大权限。这是默认选项。
- **最小值** — 有效权限代表所有重叠访问控制组的最小权限。

步骤 3 单击**保存**。

创建自定义技术支持角色任务流程

有些公司希望其技术支持人员拥有能够执行某些管理任务的权限。按照此任务流程中的步骤为技术支持团队成员配置角色和访问控制组，以允许他们执行一些任务，例如添加电话和添加最终用户。

过程

	命令或操作	目的
步骤 1	创建自定义技术支持角色，第 25 页	为技术支持团队成员创建自定义角色，并为添加新电话和添加新用户等项目分配角色权限。
步骤 2	创建自定义技术支持访问控制组，第 25 页	为技术支持角色创建新的访问控制组。
步骤 3	将技术支持角色分配到访问控制组，第 26 页	将技术支持角色分配到技术支持访问控制组。分配到此访问控制组的任何用户都将分配到技术支持角色的权限。

	命令或操作	目的
步骤 4	将技术支持成员分配到访问控制组，第 26 页	为技术支持团队成员分配自定义技术支持角色的权限。

创建自定义技术支持角色

执行此程序以创建自定义技术支持角色，您可以将该角色分配给组织内的技术支持成员。

过程

步骤 1 在 Cisco Unified Communications Manager 管理中，选择**用户管理** > **用户设置** > **角色**。

步骤 2 单击**新增**。

步骤 3 从“应用程序”下拉列表中，选择要分配给此角色的应用程序。例如，**Cisco CallManager 管理**。

步骤 4 单击**下一步**。

步骤 5 输入新角色的**名称**。例如，Help Desk。

步骤 6 在**读取和更新权限**下方，选择您要为技术支持用户分配的权限。例如，如果您希望技术支持成员能够添加用户和电话，请在“用户”网页和“电话”网页上选中**读取**和**更新**复选框。

步骤 7 单击**保存**。

接下来的操作

创建自定义技术支持访问控制组，第 25 页

创建自定义技术支持访问控制组

开始之前

创建自定义技术支持角色，第 25 页

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户设置** > **访问控制组**。

步骤 2 单击**新增**。

步骤 3 输入访问控制组的名称。例如，Help_Desk。

步骤 4 单击**保存**。

接下来的操作

将技术支持角色分配到访问控制组， 第 26 页

将技术支持角色分配到访问控制组

执行以下步骤为技术支持访问控制组配置来自技术支持角色的权限。

开始之前

创建自定义技术支持访问控制组， 第 25 页

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户设置** > **访问控制组**。

步骤 2 单击**查找**并选择您为技术支持创建的访问控制组。
此时将显示**访问控制组配置**窗口。

步骤 3 在**相关链接**下拉列表框中，选择**将角色分配到访问控制组**选项，然后单击**转至**。
随即将显示**查找并列出角色**弹出窗口。

步骤 4 单击**将角色分配到组**按钮。

步骤 5 单击**查找**并选择技术支持角色。

步骤 6 单击**添加选定项**。

步骤 7 单击**保存**。

接下来的操作

将技术支持成员分配到访问控制组， 第 26 页

将技术支持成员分配到访问控制组

开始之前

将技术支持角色分配到访问控制组， 第 26 页

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户设置** > **访问控制组**。

步骤 2 单击**查找**并选择您创建的自定义技术支持访问控制组。

步骤 3 请执行以下步骤之一：

- 如果您的技术支持团队成员被配置为最终用户，请单击**将最终用户添加到组**。

- 如果您的技术支持团队成员被配置为应用程序用户，请单击**将应用程序用户添加到组**。

步骤 4 单击**查找**并选择您的技术支持用户。

步骤 5 单击**添加选定项**。

步骤 6 单击**保存**。
Cisco Unified Communications Manager 会向您的技术支持团队成员分配您创建的自定义技术支持角色的权限。

删除访问控制组

使用以下程序完全删除访问控制组。

开始之前

删除访问控制组时，Cisco Unified Communications Manager 会从数据库中删除所有访问控制组数据。确保您了解哪些角色正在使用访问控制组。

过程

步骤 1 选择**用户管理** > **用户设置** > **访问控制组**。
此时将显示**查找并列出访问控制组**窗口。

步骤 2 找到您要删除的访问控制组。

步骤 3 单击要删除的访问控制组的名称。
此时将显示所选的访问控制组。列表按字母顺序显示此访问控制组中的用户。

步骤 4 如果要完全删除访问控制组，请单击**删除**。
此时将显示一个对话框，警告您无法撤消访问控制组的删除。

步骤 5 要删除访问控制组，请单击**确定**；要取消该操作，请单击**取消**。如果单击**确定**，Cisco Unified Communications Manager 将从数据库中删除访问控制组。

撤销现有的 OAuth 刷新令牌

使用 AXL API 撤销现有的 OAuth 刷新令牌。例如，如果一名员工离开了您的公司，您可以使用此 API 撤销该员工当前的刷新令牌，以使他们不能获得新的访问令牌，并且将不能再登录到公司帐户。该 API 是一个基于 REST 的 API，受 AXL 凭证保护。您可以使用任何命令行工具来调用 API。下面的命令提供了一个可用于撤销刷新令牌的 cURL 命令的示例：

```
curl -k -u "admin:password" https://<UCMaddress:8443/ssosp/token/revoke?user_id=<end_user>
```

其中：

- `admin:password` 是登录 ID 和 Cisco Unified Communications Manager 管理员帐户的密码。
- `UCMaddress` 是 Cisco Unified Communications Manger 发布方节点的 FQDN 或 IP 地址。
- `end_user` 是您要对其撤销刷新令牌的用户的用户 ID。

设置远程帐户

配置一个远程帐户，以便思科支持人员能够暂时访问您的系统进行故障排除。

过程

步骤 1 从“Cisco Unified 操作系统管理”中，选择**服务** > **远程支持**。

步骤 2 在**帐户名**字段中，输入远程帐户的名称。

步骤 3 在**帐户期限**字段中，输入帐户期限，以天为单位。

步骤 4 单击**保存**。
随即会出现显示有关远程支持帐户信息的字段。请参阅联机帮助，获取有关字段的详细信息。

步骤 5 与思科支持人员联系，向其提供远程支持帐户名和密码短语。

标准角色和访问控制组

下表总结了标准角色和在 Cisco Unified Communications Manager 上预先配置的访问控制组。标准角色的权限是默认配置的。此外，与标准角色关联的访问控制组也是默认配置的。

对于标准角色和关联的访问控制组，您都无法编辑任何权限或角色分配。

表 *1*：标准角色、权限和访问控制组

标准角色	角色的权限/资源	关联的标准访问控制组
标准 AXL API 访问	允许访问 AXL 数据库 API	标准 CCM 超级用户
标准 AXL API 用户	授予登录权限以执行 AXL API。	
标准 AXL 只读 API 访问	默认情况下允许您执行 AXL 只读 API（list API、get API、executeSQLQuery API）。	
标准管理员报告工具管理	允许您查看和配置 Cisco Unified Communications Manager CDR 分析和报告 (CAR)。	标准 CAR 管理员用户、标准 CCM 超级用户

标准角色	角色的权限/资源	关联的标准访问控制组
标准审计日志管理	允许您执行审计日志记录功能的以下任务： • 在 Cisco Unified 功能配置的“审计日志配置”窗口中查看和配置审计日志记录 • 在 Cisco Unified 功能配置中查看和配置跟踪并在实时监控工具中收集审计日志功能的跟踪 • 在 Cisco Unified 功能配置中查看和启动/停止 Cisco Audit Event 服务 • 在 RTMT 中查看和更新关联的告警	标准审计用户
标准 CCM 管理员用户	授予 Cisco Unified Communications Manager 管理的登录权限。	标准 CCM 管理员用户、标准 CCM 网关管理、标准 CCM 电话管理、标准 CCM 只读、标准 CCM 服务器监控、标准 CCM 超级用户、标准 CCM 服务器维护、标准信息包探查器用户
标准 CCM 最终用户	授予 Cisco Unified Communications Self Care 门户网站的最终用户登录权限	标准 CCM 最终用户
标准 CCM 功能管理	允许您在 Cisco Unified Communications Manager 管理中执行以下任务： • 使用批量管理工具查看、删除和插入以下项目： 客户码和强制授权码 呼叫代答组 • 在 Cisco Unified Communications Manager 管理中查看和配置以下项目： 客户码和强制授权码 呼叫暂留 呼叫代答 Meet-me 号码/模式 留言通知 Cisco Unified IP Phone 服务 语音信箱引导、语音信箱端口向导、语音信箱端口和语音信箱配置文件	标准 CCM 服务器维护

标准角色	角色的权限/资源	关联的标准访问控制组
标准 CCM 网关管理	允许您在 Cisco Unified Communications Manager 管理中执行以下任务： • 在批量管理工具中查看和配置网关模板 • 查看和配置网守、网关和干线	标准 CCM 网关管理
标准 CCM 电话管理	允许您在 Cisco Unified Communications Manager 管理中执行以下任务： • 在批量管理工具中查看和导出电话 • 在批量管理工具中查看和插入用户设备配置文件 • 在 Cisco Unified Communications Manager 管理中查看和配置以下项目： BLF 快速拨号 CTI 路由点 默认设备配置文件或默认配置文件 目录号码和线路显示 固件加载信息 电话按键模板或软键模板 电话 特定电话的电话按键重新排序信息（通过单击“电话配置”窗口中的“修改按键项”按钮）	标准 CCM 电话管理
标准 CCM 路由计划管理	允许您在 Cisco Unified Communications Manager 管理中执行以下任务： • 查看和配置应用程序拨号规则 • 查看和配置呼叫搜索空间和分区 • 查看和配置拨号规则，包括拨号规则模式 • 查看和配置寻线列表、寻线引导和线路组 • 查看和配置路由过滤器、路由组、路由寻线列表、路由列表、路由模式和路由计划报告 • 查看和配置时段和时间表 • 查看和配置转换模式	

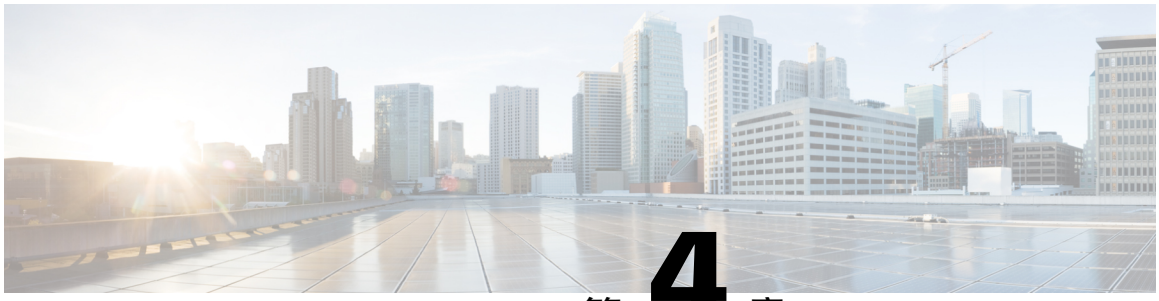
标准角色	角色的权限/资源	关联的标准访问控制组
标准 CCM 服务管理	允许您在 Cisco Unified Communications Manager 管理中执行以下任务： • 查看和配置以下项目： 信号器、会议桥和转码器 音频来源和 MOH 服务器 媒体资源组和媒体资源组列表 媒体终结点 Cisco Unified Communications Manager Assistant 向导 • 在批量管理工具中查看和配置“删除经理”、“删除经理/助理”和“嵌入经理/助理”窗口	标准 CCM 服务器维护

标准角色	角色的权限/资源	关联的标准访问控制组
标准 CCM 系统管理	允许您在 Cisco Unified Communications Manager 管理中执行以下任务： • 查看和配置以下项目： 自动路由迂回 (AAR) 组 Cisco Unified Communications Manager (Cisco Unified CM) 和 Cisco Unified Communications Manager 组 日期和时间组 设备默认值 设备池 企业参数 企业电话配置 位置 网络时间协议 (NTP) 服务器 插件 用于运行信令呼叫控制协议 (SCCP) 或会话发起协议 (SIP) 的电话的安全性配置文件；用于 SIP 干线的安全性配置文件 可存活远程站点电话 (SRST) 引用 服务器 • 在批量管理工具中查看和配置“作业计划程序”窗口	标准 CCM 服务器维护
标准 CCM 用户权限管理	允许您在 Cisco Unified Communications Manager 管理中查看和配置应用程序用户。	
标准 CCMADMIN 管理	允许您访问 CCMAdmin 系统的所有方面	
标准 CCMADMIN 管理	允许您在 Cisco Unified Communications Manager 管理和批量管理工具中查看和配置所有项目。	标准 CCM 超级用户
标准 CCMADMIN 管理	允许您在被叫号码分析器中查看和配置信息。	
标准 CCMADMIN 只读	允许所有 CCMAdmin 资源的读取访问权限	

标准角色	角色的权限/资源	关联的标准访问控制组
标准 CCMADMIN 只读	允许您在 Cisco Unified Communications Manager 管理和批量管理工具中查看配置。	标准 CCM 网关管理、标准 CCM 电话管理、标准 CCM 只读、标准 CCM 服务器维护、标准 CCM 服务器监控
标准 CCMADMIN 只读	允许您在被叫号码分析器中分析路由配置。	
标准 CCMUSER 管理	允许访问 Cisco Unified Communications Self Care 门户网站。	标准 CCM 最终用户
标准 CTI 允许呼叫监控	允许 CTI 应用程序/设备监控呼叫	标准 CTI 允许呼叫监控
标准 CTI 允许呼叫暂留监控	允许 CTI 应用程序/设备使用呼叫暂留	标准 CTI 允许呼叫暂留监控
标准 CTI 允许呼叫录音	允许 CTI 应用程序/设备录音呼叫	标准 CTI 允许呼叫录音
标准 CTI 允许主叫号码修改	允许 CTI 应用程序在通话期间转换主叫方号码	标准 CTI 允许主叫号码修改
标准 CTI 允许控制所有设备	允许控制所有 CTI 可控制设备	标准 CTI 允许控制所有设备
标准 CTI 允许控制支持已连接转接和会议的电话	允许控制支持已连接转接和会议的所有 CTI 设备	标准 CTI 允许控制支持已连接转接和会议的电话
标准 CTI 允许控制支持跳转模式的电话	允许控制支持跳转模式的所有 CTI 设备	标准 CTI 允许控制支持跳转模式的电话
标准 CTI 允许接收 SRTP 重要材料	允许 CTI 应用程序访问和分发 SRTP 重要材料	标准 CTI 允许接收 SRTP 重要材料
标准 CTI 已启用	启用 CTI 应用程序控制	标准 CTI 已启用
标准 CTI 安全连接	启用到 Cisco Unified Communications Manager 的安全 CTI 连接	标准 CTI 安全连接
标准 CU 报告	允许应用程序用户生成各种来源的报告	
标准 CU 报告	允许您在 Cisco Unified 报告中查看、下载、生成和上载报告	标准 CCM 管理用户、标准 CCM 超级用户
标准 EM 验证代理权限	管理应用程序的 Cisco 分机移动 (EM) 验证权限；与 Cisco 分机移动交互的所有应用程序用户（例如，Cisco Unified Communications Manager Assistant 和 Cisco Web Dialer）必需	标准 CCM 超级用户、标准 EM 验证代理权限

标准角色	角色的权限/资源	关联的标准访问控制组
标准信息包探查	允许您访问 Cisco Unified Communications Manager 管理以启用数据包探查（捕获）。	标准信息包探查器用户
标准实时和跟踪收集	允许您访问 Cisco Unified 功能配置和实时监控工具视图并使用以下项目： • 简单对象访问协议 (SOAP) 功能配置 AXL API • SOAP 呼叫记录 API • SOAP Diagnostic Portal (Analysis Manager) 数据库服务 • 配置审计日志追踪功能 • 配置实时监控工具，包括收集跟踪	标准实时和跟踪收集
标准功能配置	允许您在Cisco Unified 功能配置或实时监控工具中查看和配置以下窗口： • “警报配置”和“警报定义”（Cisco Unified 功能配置） • 审计追踪（标记为只读/仅查看） • SNMP 相关窗口（Cisco Unified 功能配置） • “跟踪配置”和“跟踪配置故障排除”（Cisco Unified 功能配置） • 日志分区监控 • 告警配置 (RTMT)、配置文件配置 (RTMT)，以及跟踪收集 (RTMT) 允许您查看和使用 SOAP 功能配置 AXL API、SOAP 呼叫记录 API 和 SOAP Diagnostic Portal (Analysis Manager) 数据库服务。 对于 SOAP 呼叫记录 API，RTMT Analysis Manager 呼叫记录权限通过此资源进行控制。 对于 SOAP Diagnostic Portal 数据库服务，RTMT Analysis Manager 托管数据库通过此资源控制访问。	标准CCM服务器监控、标准CCM超级用户
标准功能配置管理	功能配置管理员可在 Cisco Unified Communications Manager管理中访问“插件”窗口并从此窗口中下载插件。	
标准功能配置管理	允许您管理被叫号码分析器功能配置的所有方面。	

标准角色	角色的权限/资源	关联的标准访问控制组
标准功能配置管理	允许您在Cisco Unified功能配置和实时监控工具中查看和配置所有窗口。（审计追踪仅支持查看） 允许您查看和使用所有 SOAP 功能配置 AXL API。	
标准功能配置只读	允许您查看被叫号码分析器中组件的所有功能配置相关数据。	标准 CCM 只读
标准功能配置只读	允许您在Cisco Unified功能配置和实时监控工具中查看配置。（“审计配置”窗口除外，该窗口由“标准审计日志管理”角色代表） 允许您查看所有 SOAP 功能配置 AXL API、SOAP 呼叫记录 API 和 SOAP Diagnostic Portal (Analysis Manager) 数据库服务。	
标准系统服务管理	允许您在 Cisco Unified 功能配置中查看、激活、启动和停止服务。	
标准 SSO 配置管理员	允许您管理 SAML SSO 配置的所有方面	
标准保密访问级别用户	允许您访问所有保密访问级别页面	标准 Cisco Call Manager 管理
标准 CCMADMIN 管理	允许您管理 CCMAdmin 系统的所有方面	标准 Cisco Unified CM IM and Presence 管理
标准 CCMADMIN 只读	允许所有 CCMAdmin 资源的读取访问权限	标准 Cisco Unified CM IM and Presence 管理
标准 CU 报告	允许应用程序用户生成各种来源的报告	标准 Cisco Unified CM IM and Presence 报告



第 4 章

管理最终用户

最终用户概述

在管理启动并运行的系统时，您可能需要在您的系统中更新所配置的最终用户的列表。其中包括：

- 设置新用户
- 为新的最终用户设置电话
- 为最终用户更改密码或个人识别码
- 为 IM and Presence 服务启用最终用户

您可以使用“Cisco Unified CM 管理”中的**最终用户配置**窗口添加、搜索、显示和维护 Unified CM 最终用户的相关信息。您还可以使用**快速用户/电话添加**窗口，快速配置新的最终用户并为该最终用户配置新电话。

最终用户管理任务

过程

	命令或操作	目的
步骤 1	配置用户模板， 第 38 页	如果您尚未使用用户配置文件或包含通用线路和设备模板的功能组模板配置您的系统，请执行这些任务以进行设置。 您可以将这些模板应用于任何新的最终用户，以便快速配置新用户和电话。

	命令或操作	目的
步骤 2	使用以下方法之一添加新的最终用户 • 从 LDAP 导入最终用户，第 42 页 • 手动添加最终用户，第 42 页	如果您的系统与公司 LDAP 目录同步，可以直接从 LDAP 导入新的最终用户。如果您已配置 此外，您可以手动添加和配置最终用户。
步骤 3	通过执行以下任务之一将电话分配给新的或现有的最终用户： • 为最终用户添加新电话，第 43 页 • 将现有电话移至最终用户，第 44 页	您可以使用“添加新电话”程序，使用通用设备模板的设置为最终用户配置新电话。 您还可以使用“移动”程序分配已经配置好的现有电话。
步骤 4	更改最终用户个人识别码，第 45 页	（可选）在 Cisco Unified Communications Manager 管理中为最终用户更改个人识别码。
步骤 5	更改最终用户密码，第 45 页	（可选）在 Cisco Unified Communications Manager 管理中为最终用户更改密码。
步骤 6	创建 Cisco Unity Connection 语音信箱，第 46 页	（可选）在 Cisco Unified Communications Manager 管理中创建单独的 Cisco Unity Connection 语音信箱。

配置用户模板

执行以下任务以设置用户配置文件和功能组模板。当您添加新的最终用户时，可以使用线路和设备设置快速配置最终用户并为最终用户配置任何电话。

过程

	命令或操作	目的
步骤 1	配置通用线路模板，第 39 页	使用通常应用于目录号码的通用设置配置通用线路模板。
步骤 2	配置通用设备模板，第 39 页	使用通常应用于电话的通用设置配置通用设备模板。

	命令或操作	目的
步骤 3	配置用户配置文件， 第 40 页	将通用线路和通用设备模板分配给用户配置文件。如果已经配置了自我部署功能，您可以为使用此配置文件的用户启用自我部署。
步骤 4	配置功能组模板， 第 41 页	将用户配置文件分配给功能组模板。对于 LDAP 同步用户，功能组模板会将用户配置文件设置关联到最终用户。

配置通用线路模板

使用通常应用于目录号码的通用设置配置一个通用线路模板。您可以创建一个或多个通用线路模板，以创建一组设置，反映您的组织中最常见的目录号码配置，并且，通过用户配置文件，您可以将这些设置应用到您为最终用户部署的新目录号码。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户/电话添加** > **通用线路模板**。

步骤 2 单击**新增**。

步骤 3 配置**通用线路模板配置**窗口中的字段。请参阅联机帮助，了解有关字段及其配置选项的更多信息。

步骤 4 单击**保存**。

接下来的操作

配置通用设备模板， 第 39 页

配置通用设备模板

配置通用设备模板。通用设备模板包含一组通用设置，通常应用于电话、远程目标配置文件或分机移动配置文件。您可以创建一个或多个通用设备模板，反映您的组织中最常见的设备配置，并且，通过用户配置文件，您可以将这些设置应用到您为最终用户配置的任何新设备。

开始之前

配置通用线路模板， 第 39 页

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户/电话添加** > **通用设备模板**。

步骤 2 单击**新增**。

步骤 3 填写**通用设备模板配置**窗口中的字段。要查看字段说明，请参阅联机帮助。

步骤 4 单击**保存**。

接下来的操作

配置用户配置文件，第 40 页

配置用户配置文件

配置一个用户配置文件，包含您要分配给使用该配置文件的用户的通用线路模板和通用设备模板。您还可以为使用此服务配置文件的用户启用自我部署。

开始之前

配置通用设备模板，第 39 页

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户设置** > **用户配置文件**。

步骤 2 单击**新增**。

步骤 3 输入用户配置文件的**名称**和**描述**。

步骤 4 分配**通用设备模板**以应用到用户的**桌面电话、移动和桌面设备**，以及**远程目标/设备配置文件**。

步骤 5 分配**通用线路模板**以应用到此用户配置文件中的用户的电话线路。

步骤 6 如果您希望此用户配置文件中的用户能够使用自我部署功能部署他们自己的电话，请执行以下操作：

a) 选中**允许最终用户部署自己的电话**复选框。

b) 在**一旦最终用户拥有这么多电话即限制部署**字段中，输入允许用户部署的最大电话数量。最大值为 20。

步骤 7 如果您希望与此用户配置文件关联的 Cisco Jabber 用户，能够使用移动和远程访问 (MRA) 功能，请选中**启用移动和远程访问**复选框。

注释 默认情况下，此复选框为选中状态。当取消选中此复选框时，**Jabber 策略**部分会被禁用，并且默认情况下会选中“无服务”客户端策略选项。

注释 此设置仅对 Cisco Jabber 用户是必需的。非 Jabber 用户无需此设置即可使用 MRA。MRA 功能仅适用于 Jabber MRA 用户，不适用于任何其他终端或客户端。

步骤 8 为此用户配置文件分配 Jabber 策略。从 **Jabber 桌面客户端策略**，以及 **Jabber 移动客户端策略**下拉列表框中，选择以下选项之一：

- 无服务—此策略禁止访问所有 Jabber 服务。

- 仅 IM & Presence—此策略仅启用即时消息和在线状态功能。
- IM & Presence、语音和视频呼叫—此策略为所有拥有音频和视频设备的用户启用即时消息、在线状态、语音邮件和会议功能。这是默认选项。

注释 Jabber 桌面客户端包括 Windows 版 Cisco Jabber 用户和 Mac 版 Cisco Jabber 用户。Jabber 移动客户端包括 iPad 和 iPhone 版 Cisco Jabber 用户和 Android 版 Cisco Jabber 用户。

步骤 9 单击**保存**。

接下来的操作

配置功能组模板，第 41 页

配置功能组模板

功能组模板包含一组通用线路、设备和功能设置。当您将功能组模板应用于新用户时，那些线路、设备和功能设置会应用于用户的电话和电话线路。功能组模板可帮助您非常快速地为部署的用户配置电话、线路和功能，从而为您的系统部署提供帮助。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户/电话添加** > **功能组模板**。

步骤 2 单击**新增**。

步骤 3 如果您想要使用本地群集作为所有使用此模板的用户的主群集，请选中**主群集**复选框。

步骤 4 如果您希望使用此模板的用户能够使用 IM and Presence 服务来使用即时消息，请选中**使用户能够使用 Unified CM IM and Presence** 复选框。

步骤 5 从下拉列表菜单中，选择一个**服务配置文件**和**用户配置文件**。

步骤 6 填写**功能组模板配置**窗口中的其余字段。请参阅联机帮助中的字段说明。

步骤 7 单击**保存**。

接下来的操作

添加新的最终用户。如果您的系统与公司 LDAP 目录集成，可以直接从 LDAP 目录导入用户。否则，请手动创建最终用户。

- 从 LDAP 导入最终用户，第 42 页
- 手动添加最终用户，第 42 页

从 LDAP 导入最终用户

执行以下程序以手动从公司 LDAP 目录导入新的最终用户。如果您的 LDAP 同步配置包含一个带有用户配置文件（包含通用线路和设备模板）的功能组模板，以及一个 DN 池，那么导入过程会自动配置最终用户和主分机。

开始之前

此程序假定您已将 Cisco Unified Communications Manager 与公司 LDAP 目录同步。LDAP 同步必须包含一个带有通用线路和设备模板的功能组模板。

过程

步骤 1 在 Cisco Unified CM 管理中，依次选择**系统** > **LDAP** > **LDAP 目录**。

步骤 2 单击**查找**并选择要向其添加用户的 LDAP 目录。

步骤 3 单击**执行完全同步**。
Cisco Unified Communications Manager 会与外部 LDAP 目录同步。LDAP 目录中任何新的最终用户都会导入到 Cisco Unified Communications Manager 数据库中。

接下来的操作

如果为用户启用了自我部署，则最终用户可以使用自我部署互动语音响应 (IVR) 来部署新电话。否则，执行以下任务之一将电话分配给最终用户：

- 为最终用户添加新电话，第 43 页
- 将现有电话移至最终用户，第 44 页

手动添加最终用户

执行以下程序添加新的最终用户并为该最终用户配置访问控制组和主线路分机。

开始之前

确认您配置有包含通用线路模板的用户配置文件。如果您需要配置新的分机，Cisco Unified Communications Manager 将使用通用线路模板中的设置配置主分机。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户/电话添加** > **快速用户/电话添加**。

步骤 2 输入用户的**用户 ID** 和**姓氏**。

步骤 3 从**功能组模板**下拉列表中，选择功能组模板。

步骤 4 单击**保存**。

步骤 5 从**用户配置文件**下拉列表中，验证所选的用户配置文件包含通用线路模板。

步骤 6 从**访问控制组成员资格**部分，单击 + 图标。

步骤 7 从**用户属于**下拉列表中，选择一个访问控制组。

步骤 8 在**主分机**下方，单击 + 图标。

步骤 9 从**分机**下拉列表中，选择一个显示为（**可用**）的目录号码。

步骤 10 如果所有线路分机都显示为（**已使用**），请执行以下步骤：

a) 单击**新建...** 按钮。
随即将显示**添加新分机**弹出窗口。

b) 在**目录号码**字段中，输入新的线路分机。

c) 从**线路模板**下拉列表框中，选择一个通用线路模板。

d) 单击**确定**。
Cisco Unified Communications Manager 会使用通用线路模板的设置配置目录号码。

步骤 11 可选。填写**快速用户/电话添加配置**窗口中的任何其他字段。

步骤 12 单击**保存**。

接下来的操作

执行以下程序之一将电话分配给该最终用户：

- 为最终用户添加新电话，第 43 页
- 将现有电话移至最终用户，第 44 页

为最终用户添加新电话

执行以下程序为新的或现有的最终用户添加新电话。此程序假定最终用户的用户配置文件包含通用设备模板。Cisco Unified Communications Manager 会使用通用设备模板设置配置电话。

开始之前

请执行以下程序以添加最终用户：

- 手动添加最终用户，第 42 页
- 从 LDAP 导入最终用户，第 42 页

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户/电话添加** > **快速用户/电话添加**。

步骤 2 单击**查找**并选择您要为其添加新电话的最终用户。

步骤 3 单击**管理设备**按钮。
将出现“管理设备”窗口。

步骤 4 单击**添加新电话**。
此时将显示“添加电话至用户”弹出窗口。

步骤 5 从**产品类型**下拉列表中，选择电话型号。

步骤 6 从**设备协议**下拉列表中，选择 SIP 或 SCCP 作为协议。

步骤 7 在**设备名称**文本框中，输入设备的 MAC 地址。

步骤 8 从**通用设备模板**下拉列表中，选择一个通用设备模板。

步骤 9 如果电话支持扩展模块，输入您要部署的扩展模块数量。

步骤 10 如果您想使用分机移动访问电话，选中**在分机移动中**复选框。

步骤 11 单击**添加电话**。
此时“添加新电话”弹出窗口会关闭。Cisco Unified Communications Manager 会将电话添加至用户，并使用通用设备模板配置电话。

步骤 12 如果您想对电话配置进行其他编辑，单击对应的铅笔图标以在“电话配置”窗口中打开电话。

接下来的操作

将现有电话移至最终用户，第 44 页

将现有电话移至最终用户

执行此程序以将现有电话移至新的或现有的最终用户。

开始之前

为最终用户添加新电话，第 43 页

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户/电话添加** > **快速用户/电话添加**。

步骤 2 单击**查找**并选择您要向其移动现有电话的用户。

步骤 3 单击**管理设备**按钮。

步骤 4 单击**查找要移至此用户的电话**按钮。

步骤 5 选择您想要移至此用户的电话。

步骤 6 单击**移动选定项**。

更改最终用户个人识别码

过程

步骤 1 在 Cisco Unified Communications Manager 管理中，选择**用户管理** > **最终用户**。
此时将出现**查找并列出用户**窗口。

步骤 2 要选择现有用户，请在**查找用户位置**字段中指定合适的过滤器，并单击**查找**以检索用户列表，然后从列表中选择用户。
随即会显示**最终用户配置**窗口。

步骤 3 在**个人识别码**字段中，双击现有的个人识别码（已加密），然后输入新的个人识别码。至少必须输入分配的凭证策略中指定的最少字符数（1-127 个字符）。

步骤 4 在**确认个人识别码**字段中，双击已加密的现有个人识别码，然后再次输入新的个人识别码。

步骤 5 单击**保存**。

注释 如果 Cisco Unity Connection 的 **应用服务器配置**窗口中的**最终用户个人识别码同步**复选框已启用，您可以使用相同的最终用户个人识别码登录到分机移动、立即开会、移动连接，以及 Cisco Unity Connection 语音邮件。最终用户可以使用相同的个人识别码登录到分机移动和访问其语音邮件。

更改最终用户密码

LDAP 验证启用时，您无法更改最终用户密码。

过程

步骤 1 在 Cisco Unified Communications Manager 管理中，选择**用户管理** > **最终用户**。
此时将出现**查找并列出用户**窗口。

步骤 2 要选择现有用户，请在**查找用户位置**字段中指定合适的过滤器，并单击**查找**以检索用户列表，然后从列表中选择用户。
随即会显示**最终用户配置**窗口。

步骤 3 在**密码**字段中，双击现有的密码（已加密），然后输入新密码。至少必须输入分配的凭证策略中指定的最少字符数（1-127 个字符）。

步骤 4 在**确认密码**字段中，双击已加密的现有密码，然后再次输入新密码。

步骤 5 单击**保存**。

创建 Cisco Unity Connection 语音信箱

开始之前

- 您必须配置 Cisco Unified Communications Manager 才能使用语音留言。有关配置 Cisco Unified Communications Manager 以使用 Cisco Unity Connection 的详细信息，请参阅《*Cisco Unified Communications Manager* 系统配置指南》，位于：

  http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

- 您必须将设备和主分机号码与最终用户关联。
- 您可以使用 Cisco Unity Connection 中提供的导入功能，而不是执行本节中所述的程序。有关如何使用导入功能的信息，请参阅《*Cisco Unity Connection* 用户移动、添加和更改指南》。

过程

步骤 1 在 Cisco Unified Communications Manager 管理中，选择**用户管理** > **最终用户**。
此时将出现**查找并列出用户**窗口。

步骤 2 要选择现有用户，请在**查找用户位置**字段中指定合适的过滤器，并单击**查找**以检索用户列表，然后从列表中选择用户。
随即会显示**最终用户配置**窗口。

步骤 3 验证主分机号码与该用户关联。

注释 您必须定义主分机；否则创建 Cisco Unity 用户链接不会在**相关链接**下拉列表中显示。

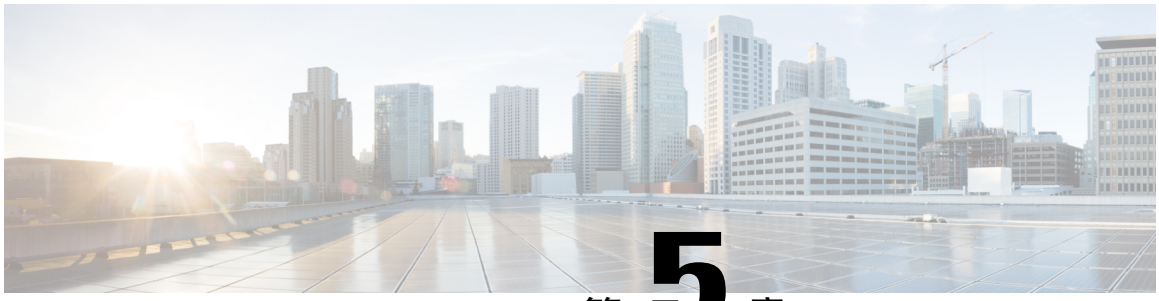
步骤 4 从**相关链接**下拉列表中，选择创建 Cisco Unity 用户链接，然后单击**转至**。
此时将显示“添加 Cisco Unity 用户”对话框。

步骤 5 从**应用服务器**下拉列表中，选择您要在其上创建 Cisco Unity Connection 用户的 Cisco Unity Connection 服务器，然后单击**下一步**。

步骤 6 从**订户模板**下拉列表中，选择您要使用的订户模板。

步骤 7 单击**保存**。
此时将创建信箱。**相关链接**下拉列表中的链接会更改为**最终用户配置**窗口中的编辑 Cisco Unity 用户。现在，您可以在 Cisco Unity Connection 管理中查看所创建的用户。

注释 将 Cisco Unity Connection 用户与 Cisco Unified Communications Manager 最终用户集成后，您无法编辑 Cisco Unity Connection 管理中的字段，例如“别名”（Cisco Unified CM 管理中的“用户 ID”）、“名字”、“姓氏”，以及“分机”（Cisco Unified CM 管理中的“主分机”）。您只能在“Cisco Unified CM 管理”中更新这些字段。



第 5 章

管理应用程序用户

应用程序用户概述

管理员可以使用“Cisco Unified CM 管理”中的**应用程序用户配置**窗口添加、搜索、显示和维护 Cisco Unified Communications Manager 应用程序用户的相关信息。

默认情况下，“Cisco Unified CM 管理”包括以下应用程序用户：

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

注释 “标准 CCM 超级用户”组中的管理员用户可以访问 Cisco Unified Communications Manager 管理、Cisco Unified 功能配置，以及 Cisco Unified 报告（单点登录到应用程序之一）。

应用程序用户任务流程

过程

	命令或操作	目的
步骤 1	添加新的应用程序用户， 第 48 页	添加新的应用程序用户。
步骤 2	将设备与应用程序用户关联， 第 49 页	分配设备以与应用程序用户关联。
步骤 3	添加管理员用户到 Cisco Unity 或 Cisco Unity Connection， 第 49 页	将用户作为管理员用户添加到Cisco Unity或Cisco Unity Connection。您可在“Cisco Unified CM 管理”中配置应用程序用户；然后，配置任何其他设置用于 Cisco Unity 或 Cisco Unity Connection 管理中的用户。
步骤 4	更改应用程序用户密码， 第 50 页	更改应用程序用户密码。
步骤 5	管理应用程序用户密码凭证信息， 第 50 页	更改或查看凭证信息，例如关联的验证规则、关联的凭证策略或应用程序用户上次更改密码的时间。

添加新的应用程序用户

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **应用程序用户**。

步骤 2 单击**新增**。

步骤 3 配置**应用程序用户配置**窗口中的字段。请参阅联机帮助，了解有关字段及其配置选项的信息。

步骤 4 单击**保存**。

接下来的操作

将设备与应用程序用户关联， 第 49 页

将设备与应用程序用户关联

过程

步骤 1 从 Cisco Unified CM 管理中，选择**用户管理** > **应用程序用户**。
此时将出现**查找并列出用户**窗口。

步骤 2 要选择现有用户，请在**查找用户位置**字段中指定合适的过滤器，并选择**查找**以检索用户列表，然后从列表中选择用户。

步骤 3 在**可用设备**列表中，选择要与应用程序用户关联的设备，然后单击列表下方的**向下箭头**。所选的设备会移至**受控设备**列表。

注释 要限制可用设备的列表，请单击**查找更多电话**或**查找更多路由点**按钮。

步骤 4 如果单击**查找更多电话**按钮，将显示**查找并列出电话**窗口。执行搜索，以查找要与此应用程序用户关联的电话。
对要分配给应用程序用户的每个设备重复上述操作。

步骤 5 如果单击**查找更多路由点**按钮，将显示**查找并列出 CTI 路由点**窗口。执行搜索，以查找要与此应用程序用户关联的 CTI 路由点。
对要分配给应用程序用户的每个设备重复上述操作。

步骤 6 单击**保存**。

添加管理员用户到 Cisco Unity 或 Cisco Unity Connection

如果您将 Cisco Unified Communications Manager 与 Cisco Unity Connection 7.x 或更新版本集成，您可以使用 Cisco Unity Connection 7.x 或更新版本中可用的导入功能，而不是执行本节中所述的程序。有关如何使用导入功能的信息，请参阅 Cisco Unity Connection 7.x 或更新版本的《用户移动、添加和更改指南》，位于：

http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html。

当 Cisco Unity 或 Cisco Unity Connection 用户与 Cisco Unified CM 应用程序用户集成时，您无法编辑字段。您只能在 Cisco Unified Communications Manager 管理中更新这些字段。

Cisco Unity 和 Cisco Unity Connection 监控从 Cisco Unified Communications Manager 进行的数据同步。您可以在工具菜单上的 Cisco Unity 管理或 Cisco Unity Connection 管理中配置同步时间。

开始之前

确保您已为打算推送到 Cisco Unity 或 Cisco Unity Connection 的用户定义相应的模板

仅当您安装并配置了相应的 Cisco Unity 或 Cisco Unity Connection 软件后，**创建 Cisco Unity 用户**链接才会显示。请参阅适用的用于 Cisco Unity 的《*Cisco Unified Communications Manager* 集成指南》

或适用的用于 Cisco Unity Connection 的《*Cisco Unified Communications Manager SCCP* 集成指南》，位于：

http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-and-configuration-guides-list.html。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**用户管理** > **应用程序用户**。

步骤 2 要选择现有用户，请在**查找用户位置**字段中指定合适的过滤器，并选择**查找**以检索用户列表，然后从列表中选择用户。

步骤 3 从**相关链接**下拉列表中，选择**创建 Cisco Unity 应用程序用户**链接并单击**转至**。
此时将显示**添加 Cisco Unity 用户**对话框。

步骤 4 从**应用服务器**下拉列表中，选择您要在其上创建 Cisco Unity 或 Cisco Unity Connection 用户的 Cisco Unity 或 Cisco Unity Connection 服务器，然后单击**下一步**。

步骤 5 从**应用程序用户模板**下拉列表中，选择您要使用的模板。

步骤 6 单击**保存**。
此时将在 Cisco Unity 或 Cisco Unity Connection 中创建管理员帐户。“相关链接”中的链接更改为**应用程序用户配置**窗口中的**编辑 Cisco Unity 用户**。现在，您可以查看您在 Cisco Unity 管理或 Cisco Unity Connection 管理中创建的用户。

更改应用程序用户密码

过程

步骤 1 从 Cisco Unified CM 管理中，选择**用户管理** > **应用程序用户**。
此时将出现**查找并列出用户**窗口。

步骤 2 要选择现有用户，请在**查找用户位置**字段中指定合适的过滤器，并选择**查找**以检索用户列表，然后从列表中选择用户。
应用程序用户配置窗口将显示关于所选应用程序用户的信息。

步骤 3 在**密码**字段中，双击已加密的现有密码，然后输入新密码。

步骤 4 在**确认密码**字段中，双击已加密的现有密码，然后再次输入新密码。

步骤 5 单击**保存**。

管理应用程序用户密码凭证信息

执行以下程序管理应用程序用户密码的凭证信息。这可让您执行管理任务，例如锁定密码、将凭证策略应用到密码，或查看信息，例如上次失败的登录尝试的时间。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**用户管理** > **应用程序用户**。
此时将出现**查找并列出用户**窗口。

步骤 2 要选择现有用户，请在**查找用户位置**字段中指定合适的过滤器，并选择**查找**以检索用户列表，然后从列表中选择用户。
应用程序用户配置窗口将显示关于所选应用程序用户的信息。

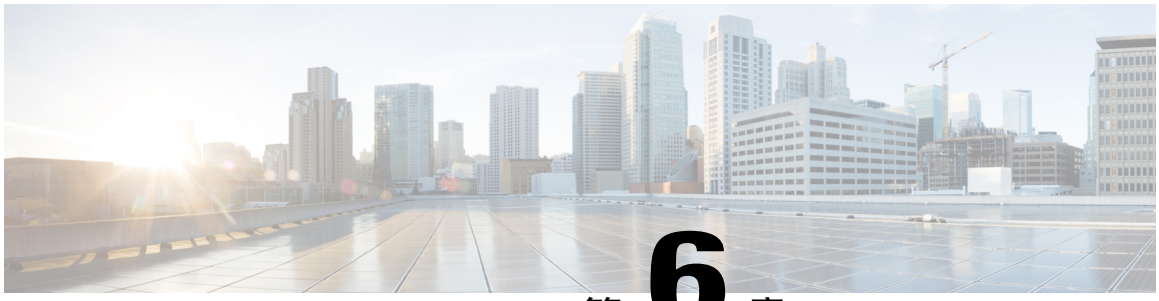
步骤 3 要更改或查看密码信息，请单击**密码**字段旁边的**编辑凭证**按钮。
随即会显示用户**凭证配置**。

步骤 4 配置**凭证配置**窗口中的字段。请参阅联机帮助，了解有关字段及其配置选项的更多信息。

步骤 5 如果更改了任何设置，请单击**保存**。

第 III 部分

管理设备



第 6 章

管理电话

电话管理概述

本章介绍如何管理您网络中的电话。各个主题介绍添加新电话、将现有电话移至另一个用户、锁定电话和重置电话等任务。

电话管理任务

过程

	命令或操作	目的
步骤 1	使用设备模板添加新电话， 第 56 页	为最终用户添加新电话并分配通用设备模板。
步骤 2	移动现有电话， 第 57 页	将已配置的电话移至不同的最终用户。
步骤 3	查找主动登录设备， 第 57 页	搜索特定的设备，或列出用户主动登录的所有设备。
步骤 4	查找远程登录设备， 第 58 页	搜索特定的设备，或列出用户远程登录的所有设备。
步骤 5	远程锁定电话， 第 58 页	某些电话可以远程锁定。当远程锁定电话时，电话将无法使用，直到您解锁。
步骤 6	将电话重置为出厂默认设置， 第 59 页	将电话重置为出厂设置。

	命令或操作	目的
步骤 7	搜索锁定或重置的设备，第 59 页	搜索已被远程锁定和/或远程重置为出厂默认设置的设备。
步骤 8	查看 LSC 状态并为电话生成 CAPF 报告，第 60 页	在电话上搜索 LSC 过期状态，同时生成 CAPF 报告。

使用设备模板添加新电话

执行以下程序为最终用户添加新电话。

开始之前

要为其添加电话的最终用户拥有包含通用设备模板的用户配置文件设置。Cisco Unified Communications Manager 会使用通用设备模板的设置配置电话。

- 最终用户管理任务，第 37 页

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户/电话添加** > **快速用户/电话添加**。

步骤 2 单击**查找**并选择您要为其添加新电话的最终用户。

步骤 3 单击**管理设备**按钮。
将出现“管理设备”窗口。

步骤 4 单击**添加新电话**。
此时将显示“添加电话至用户”弹出窗口。

步骤 5 从**产品类型**下拉列表中，选择电话型号。

步骤 6 从**设备协议**下拉列表中，选择 SIP 或 SCCP 作为协议。

步骤 7 在**设备名称**文本框中，输入设备的 MAC 地址。

步骤 8 从**通用设备模板**下拉列表中，选择一个通用设备模板。

步骤 9 如果电话支持扩展模块，输入您要部署的扩展模块数量。

步骤 10 如果您想使用分机移动访问电话，选中**在分机移动中**复选框。

步骤 11 单击**添加电话**。
此时“添加新电话”弹出窗口会关闭。Cisco Unified Communications Manager 会将电话添加至用户，并使用通用设备模板配置电话。

步骤 12 如果您想对电话配置进行其他编辑，单击对应的铅笔图标以在“电话配置”窗口中打开电话。

移动现有电话

执行以下程序将已配置的电话移至最终用户。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户/电话添加** > **快速用户/电话添加**。

步骤 2 单击**查找**并选择您要向其移动现有电话的用户。

步骤 3 单击**管理设备**按钮。

步骤 4 单击**查找要移至此用户的电话**按钮。

步骤 5 选择您想要移至此用户的电话。

步骤 6 单击**移动选定项**。

查找主动登录设备

Cisco 分机移动和 Cisco 跨群集分机移动功能记录用户主动登录的设备。对于 Cisco 分机移动功能，主动登录的设备报告跟踪本地用户主动登录的本地电话；对于 Cisco 跨群集分机移动功能，主动登录设备报告跟踪远程用户主动登录的本地电话。

Cisco Unified Communications Manager 提供特定的搜索窗口用于搜索用户登录的设备。按照这些步骤搜索特定的设备，或列出用户主动登录的所有设备。

过程

步骤 1 选择**设备** > **电话**。

步骤 2 从右上角的**相关链接**下拉列表中选择**主动登录设备报告**，并单击**转至**。

步骤 3 要查找数据库中所有主动登录设备记录，请确保对话框为空，并转至步骤 4。
要过滤或搜索记录：

a) 从第一个下拉列表框中选择搜索参数。
b) 从第二个下拉列表框中选择搜索模式。
c) 如果适用，指定适当的搜索文本。

注释 要添加其他搜索条件，请单击 + 按键。添加条件时，系统将搜索与您指定的所有条件匹配的记录。要删除条件，请单击 - 按键删除最后添加的条件，或单击“清除过滤器”按键删除所有已添加的搜索条件。

步骤 4 单击**查找**。
此时将显示所有相匹配的记录。通过在“每页行数”下拉列表框中选择不同的值，可以更改每个页面中显示的项目数量。

步骤 5 从显示的记录列表中，单击要查看的记录的链接。

注释　要反转排序顺序，请单击列表标题中的向上或向下箭头（如果可用）。

窗口中将显示您选择的项目。

查找远程登录设备

Cisco跨群集分机移动功能记录用户远程登录的设备。远程登录设备报告跟踪其他群集所拥有但通过使用 EMCC 功能的本地用户主动登录的电话。

Cisco Unified Communications Manager 提供特定的搜索窗口，用于搜索用户远程登录的设备。按照以下步骤搜索特定设备，或列出用户远程登录的所有设备。

过程

步骤 1　选择**设备** > **电话**。

步骤 2　从右上角的**相关链接**下拉列表中选择**远程登录设备**，并单击**转至**。

步骤 3　要查找数据库中所有远程登录设备记录，请确保对话框为空，并转至步骤 4。
要过滤或搜索记录：

a) 从第一个下拉列表框中选择搜索参数。
b) 从第二个下拉列表框中选择搜索模式。
c) 如果适用，指定适当的搜索文本。

注释　要添加其他搜索条件，请单击 + 按键。添加条件时，系统将搜索与您指定的所有条件匹配的记录。要删除条件，请单击 - 按键删除最后添加的条件，或单击“清除过滤器”按键删除所有已添加的搜索条件。

步骤 4　单击“查找”。
此时将显示所有相匹配的记录。通过在“每页行数”下拉列表框中选择不同的值，可以更改每个页面中显示的项目数量。

步骤 5　从显示的记录列表中，单击要查看的记录的链接。

注释　要反转排序顺序，请单击列表标题中的向上或向下箭头（如果可用）。

窗口中将显示您选择的项目。

远程锁定电话

某些电话可以远程锁定。当远程锁定电话时，电话将无法使用，直到您解锁。

如果电话支持远程锁定功能，右上角会显示**锁定**按钮。

过程

步骤 1 选择**设备** > **电话**。

步骤 2 从**查找并列出电话**窗口中，输入搜索条件并单击**查找**以查找特定电话。
此时将显示与搜索条件匹配的电话列表。

步骤 3 选择您要远程锁定的电话。

步骤 4 在**电话配置**窗口中，单击**锁定**。
如果电话未注册，将会显示一个弹出窗口，通知您下次注册电话之后将会锁定该电话。单击**锁定**。
此时将显示**设备锁定/擦除状态**部分，其中包含有关最新请求、它是否挂起以及最新确认的信息。

将电话重置为出厂默认设置

有些电话支持远程擦除功能。当您远程擦除电话时，该操作会将电话重置为出厂设置。电话上以前存储的所有内容均被擦除。

如果电话支持远程擦除功能，右上角会显示**擦除**按钮。

注意 此操作无法撤消。只有当您确定要将电话重置为出厂设置时，才应执行此操作。

过程

步骤 1 选择**设备** > **电话**。

步骤 2 在**查找并列出电话**窗口中，输入搜索条件并单击**查找**以查找特定电话。
此时将显示与搜索条件匹配的电话列表。

步骤 3 选择您要远程擦除的电话。

步骤 4 在**电话配置**窗口中，单击**擦除**。
如果电话未注册，将会显示一个弹出窗口，通知您下次注册电话之后将会擦除该电话。单击**擦除**。
此时将显示**设备锁定/擦除状态**部分，其中包含有关最新请求、它是否挂起以及最新确认的信息。

搜索锁定或重置的设备

您可以搜索已被远程锁定和/或远程重置为出厂默认设置的设备。按照以下步骤搜索某个特定设备或列出已被远程锁定和/或远程擦除的所有设备。

过程

步骤 1 选择**设备** > **电话**。
此时将显示“查找并列出电话”窗口。窗口中可能还会显示当前（之前）查询的记录。

步骤 2 从窗口右上角的**相关链接**下拉列表中选择**电话锁定/擦除报告**，然后单击**转至**。

步骤 3 要在数据库中查找所有远程锁定或远程擦除的设备记录，请确保该文本框为空；转至步骤 4。
要过滤或搜索特定设备的记录：

a) 从第一个下拉列表框中选择要搜索的操作类型。
b) 从第二个下拉列表框中选择搜索参数。
c) 从第三个下拉列表框中选择搜索模式。
d) 如果适用，指定适当的搜索文本。

注释 要添加其他搜索条件，请单击 + 按键。添加条件时，系统将搜索与您指定的所有条件匹配的记录。要删除条件，请单击 - 按键删除最后添加的条件，或单击“清除过滤器”按键删除所有已添加的搜索条件。

步骤 4 单击**查找**。
此时将显示所有相匹配的记录。通过在“每页行数”下拉列表框中选择不同的值，可以更改每个页面中显示的项目数量。

步骤 5 从显示的记录列表中，单击要查看的记录的链接。

注释 要反转排序顺序，请单击列表标题中的向上或向下箭头（如果可用）。

窗口中将显示您选择的项目。

查看 LSC 状态并为电话生成 CAPF 报告

使用此程序以从 Cisco Unified Communications Manager 界面监控当地有效证书 (LSC) 到期信息。以下搜索过滤器显示 LSC 信息：

- LSC 过期 — 在电话上显示 LSC 到期日期。
- LSC 颁发者 — 显示颁发机构的名称，可以是 CAPF 或第三方。
- LSC 颁发机构过期日期 — 显示颁发机构的到期日期。

注释 当新设备上没有颁发的 LSC 时，**LSC 过期**和 **LSC 颁发机构过期日期**字段的状态设置为 “不可用”。

当 LSC 在升级到 Cisco Unified Communications Manager 11.5(1) 之前颁发给设备时，**LSC 过期**和 **LSC 颁发机构过期日期**字段的状态设置为“未知”。

过程

步骤 1 选择**设备** > **电话**。

步骤 2 从第一个**查找电话条件**下拉列表中，选择以下条件之一：

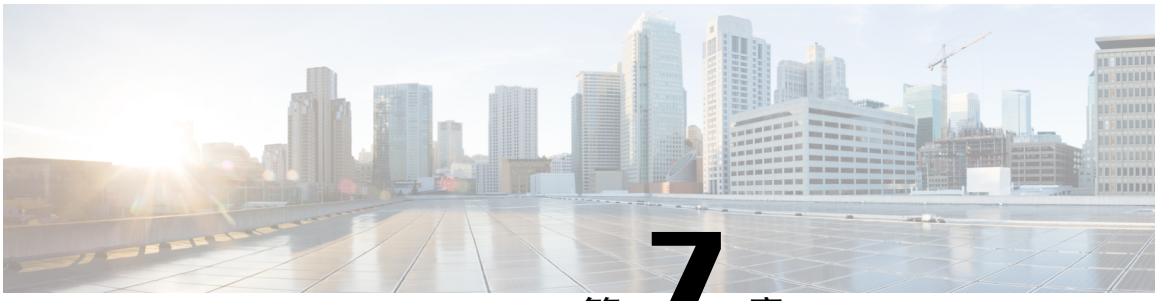
- LSC 过期
- LSC 颁发者
- LSC 颁发机构过期日期

从第二个**查找电话条件**下拉列表中，选择以下条件之一：

- 之前
- 精确等于
- 之后
- 开头为
- 包含
- 结尾为
- 精确等于
- 空白
- 非空白

步骤 3 单击**查找**。
此时将显示发现的电话列表。

步骤 4 在**相关链接**下拉列表中，选择**文件中的 CAPF 报告**，然后单击**转至**。
随即会下载报告。



第 7 章

管理设备固件

设备固件更新概述

设备加载是设备的软件和固件，例如 IP 电话、telepresence 系统，以及其他由 Cisco Unified Communications Manager 部署并注册到 Cisco Unified Communications Manager 的设备。安装或升级期间，Cisco Unified Communications Manager 包括基于 Cisco Unified Communications Manager 版本的发布时间可用的最新加载。思科会定期发布更新的固件，以引入新功能和软件修补程序。您可能希望将电话更新到较新的加载，而无需等待包含该加载的 Cisco Unified Communications Manager 升级。

在端点可以升级到新版本的软件之前，新加载所需的文件必须位于端点可以访问的位置以供下载。最常用的位置是已激活 Cisco TFTP 服务的 Cisco UCM 节点，称为“TFTP 服务器”。某些电话也支持使用备用下载位置，称为“负载服务器”。

如果您想在任何服务器上获得列表、查看或下载已经在 tftp 目录中的文件，可以使用 CLI 命令 file list tftp 查看 TFTP 目录中的文件，使用 file view tftp 查看文件，以及使用 file get tftp 获取 TFTP 目录中文件的副本。有关详细信息，请参阅《*Cisco Unified Communications* 解决方案的命令行界面参考指南》。您也可以使用 Web 浏览器，转到 URL “http://<tftp_server>:6970/<filename>” 下载任何 TFTP 文件。

提示 您可以在将新的加载配置为系统范围默认设置之前，将其应用到一台设备。此方法对于测试用途十分有用。但是，请记住，该类型的所有其他设备使用旧加载，直至您使用新加载更新系统范围默认设置。

安装设备包或单独的设备固件

安装设备包以引入新的电话类型，并为多个电话型号升级固件。现有设备的个别固件可以使用以下选项安装或升级：

- Cisco Options Package (COP) 文件 — COP 文件包含固件文件和数据库更新，因此当安装在发布方上时，除了安装固件文件以外，还会更新默认固件。
- 仅固件文件 — 它在一个 zip 文件中提供，包含应手动提取并上载到 TFTP 服务器上相应目录的单独的设备固件文件。

注释 请参阅有关 COP 或固件文件包安装程序的 Readme 文件。

将设备包应用到所有 Cisco Unified Communications Manager 服务器，从发布方服务器开始，然后是 TFTP 服务器。系统只能上传和处理思科认可的软件。您无法安装或使用与以前版本的 Cisco Unified Communications Manager 一起使用的第三方或基于 Windows 的软件应用程序。

开始之前

注释 重启发布方节点，在运行这些服务的所有节点上重新启动 TFTP 服务和 Tomcat 服务。

过程

步骤 1 从 Cisco Unified 操作系统管理，选择**软件升级** > **安装/升级**。

步骤 2 在“软件位置”部分中填写适当的值，然后单击**下一步**。

步骤 3 在**可用软件**下拉列表中，选择设备包文件，然后单击**下一步**。

步骤 4 验证 MD5 值正确，然后单击**下一步**。

步骤 5 在警告框中，验证您已选择正确的固件，然后单击**安装**。

步骤 6 检查您是否收到一条成功消息。

注释 如果要重新启动群集，则跳过步骤 8。

步骤 7 停止然后重新启动 TFTP 服务器。

步骤 8 重置受影响的设备以将设备升级到新加载。

步骤 9 从 Cisco Unified CM 管理中，选择**设备** > **设备设置** > **设备默认值**，然后将加载文件（或特定设备）的名称手动更改为新加载。

步骤 10 单击**保存**，然后重置设备。

从系统中删除未使用的固件

设备加载管理窗口允许您从系统中删除未使用的固件（设备加载）和关联的文件以增加磁盘空间。例如，您可以在升级之前删除未使用的加载，以防升级因磁盘空间不足而失败。某些固件文件可能有**设备加载管理**窗口中未列出的从属文件。当您删除一个固件时，从属文件也会被删除。但是，如果从属文件与其他固件相关联，则不会被删除。

注释 您必须为群集中的每台服务器分别删除未使用的固件。

开始之前

注意 删除未使用的固件之前，确保您正在删除正确的加载。如果不执行整个群集的 DRS 恢复，则无法恢复已删除的加载。我们建议您在删除固件之前进行备份。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**软件升级** > **设备加载管理**。

步骤 2 指定搜索条件，然后单击**查找**。

步骤 3 选择要删除的设备加载。如果需要，您可以选择多个加载。

步骤 4 单击**删除选定加载**。

步骤 5 单击**确定**。

为电话型号设置默认固件

使用此程序为特定电话型号设置默认固件加载。当一部新电话注册时，Cisco Unified Communications Manager 会尝试将默认固件发送到电话，除非电话配置具有在**电话配置**窗口中指定的覆盖固件加载。

注释 对于单独的电话，**电话配置**窗口中**电话负载名称**字段的设置会覆盖该特定电话的默认固件加载。

开始之前

确保固件加载到了 TFTP 服务器上。

过程

步骤 1 在“Cisco Unified CM 管理”中，选择**设备** > **设备设置** > **设备默认值**。

随即会出现**设备默认值配置**窗口，其中显示 Cisco Unified Communications Manager 支持的各种电话型号的默认固件加载。固件显示在**加载信息**列。

步骤 2 在**设备类型**下方，找到您要为其分配默认固件的电话型号。

步骤 3 在随同的**加载信息**字段中，输入固件负载。

步骤 4 （可选）输入该电话型号的默认**设备池**和默认**电话模板**。

步骤 5 单击**保存**。

为电话设置固件加载

使用此程序为特定电话分配固件加载。如果您想使用与**设备默认值配置**窗口中指定的默认设置不同的固件加载，不妨执行此操作。

注释 如果想要为许多电话分配一个版本，可以利用批量管理工具，使用 CSV 文件或查询配置**电话负载名称**字段。有关详细信息，请参阅《*Cisco Unified Communications Manager* 批量管理指南》。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**设备** > **电话**。

步骤 2 单击**查找**并选择单部电话。

步骤 3 在**电话负载名称**字段中，输入固件组的名称。对于此电话，在这里指定的固件加载会覆盖在**设备默认值配置**窗口中指定的默认固件加载。

步骤 4 在**电话配置**窗口填写其余的任何字段。有关这些字段及其设置的帮助，请参阅联机帮助。

步骤 5 单击**保存**。

步骤 6 单击**应用配置**以将更改后的字段推送到电话。

使用负载服务器

如果您希望电话从非TFTP服务器的一台服务器下载固件更新，可以在电话的**电话配置**页面配置“负载服务器”。负载服务器可能是另一台 Cisco Unified Communications Manager 或第三方服务器。第三方服务器必须能够通过 TCP 端口 6970（推荐）上的 HTTP 或基于 UDP 的 TFTP 协议提供电话请求的任何文件。某些电话型号，例如 DX 系列 Cisco TelePresence 设备，仅支持使用 HTTP 进行固件更新。

注释 如果想要为许多电话分配负载服务器，可以利用批量管理工具，使用 CSV 文件或查询配置**负载服务器**字段。有关详细信息，请参阅《*Cisco Unified Communications Manager* 批量管理指南》。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**设备** > **电话**。

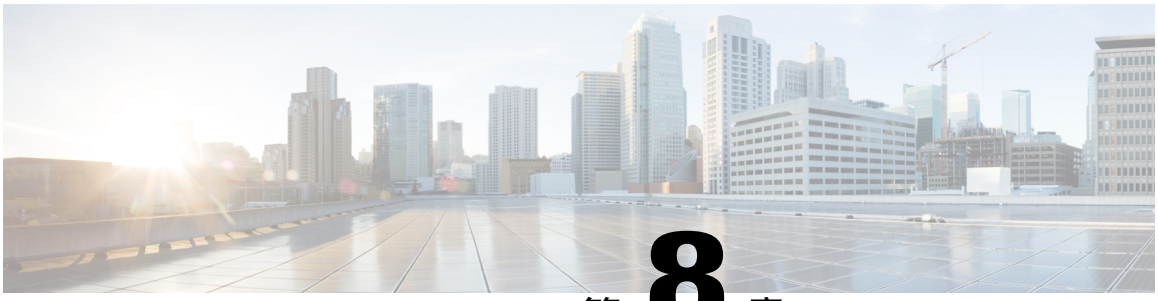
步骤 2 单击**查找**并选择单部电话。

步骤 3 在**负载服务器**字段中，输入备用服务器的 IP 地址或主机名。

步骤 4 在**电话配置**窗口填写其余的任何字段。有关这些字段及其设置的帮助，请参阅联机帮助。

步骤 5 单击**保存**。

步骤 6 单击**应用配置**以将更改后的字段推送到电话。



第 8 章

管理基础设施设备

管理基础设施概述

本章提供任务以管理网络基础设施设备，例如作为位置感知功能一部分的交换机和无线访问点。当启用位置感知时，Cisco Unified Communications Manager 数据库会保存您网络中交换机和访问点的状态信息，包括目前关联到每个交换机或访问点的端点的列表。

端点到基础设施设备的映射可帮助 Cisco Unified Communications Manager 和 Cisco Emergency Responder 确定主叫方的物理位置。例如，如果一个移动客户端在漫游情况下发出紧急呼叫，Cisco Emergency Responder 会使用映射来确定要将紧急服务发送到何处。

存储在数据库中的基础设施信息也有助于您监控基础设施使用情况。从 Cisco Unified Communications Manager 界面，您可以查看网络基础设施设备，例如交换机和无线访问点。您还可以查看当前关联至特定访问点或交换机的端点的列表。如果基础设施设备未在使用，您可以停用对基础设施设备的跟踪。

管理基础设施前提条件

您必须先配置“位置感知”功能，才能在 Cisco Unified Communications Manager 界面内管理无线基础设施。对于您的有线基础设施，该功能默认启用。有关配置的详细信息，请参阅以下章节：

"位置感知"，Cisco Unified Communications Manager 系统配置指南。

您还必须安装您的网络基础设施。有关详细信息，请参阅您的基础设施设备（例如无线 LAN 控制器、访问点和交换机）随附的硬件文档。

管理基础设施任务流程

完成以下任务以监控和管理您的网络基础设施设备。

过程

	命令或操作	目的
步骤 1	查看基础设施设备的状态，第 70 页	获取无线访问点或以太网交换机的当前状态，包括关联端点的列表。
步骤 2	禁用对基础设施设备的跟踪，第 70 页	如果您有未使用的交换机或访问点，将设备标记为非活动。系统将停止更新基础设施设备的状态或关联端点的列表。
步骤 3	激活对已禁用基础设施设备的跟踪，第 71 页	启动对非活动基础设施设备的跟踪。Cisco Unified Communications Manager 会开始使用基础设施设备的状态和关联端点的列表更新数据库。

查看基础设施设备的状态

使用此程序获取基础设施设备（例如无线访问点或以太网交换机）的当前状态。在 Cisco Unified Communications Manager 界面中，您可以查看访问点或交换机的状态，并可看到关联端点的当前列表。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**高级功能** > **设备位置跟踪服务** > **交换机和访问点**。

步骤 2 单击**查找**。

步骤 3 单击您要查看状态的交换机或访问点。
交换机和访问点配置窗口会显示当前状态，包括当前关联到该访问点或交换机的端点的列表。

禁用对基础设施设备的跟踪

使用此程序删除对特定基础设施设备（例如交换机或访问点）的跟踪。您可能希望对未使用的交换机或访问点执行此操作。

注释 如果删除对基础设施设备的跟踪，设备将保留在数据库中，但会变为非活动状态。Cisco Unified Communications Manager 将不会再更新设备的状态，包括关联到基础设施设备的端点的列表。您可以从**交换机和访问点**窗口的**相关链接**下拉列表中查看非活动的交换机和访问点。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**高级功能** > **设备位置跟踪服务** > **交换机和访问点**。

步骤 2 单击**查找**并选择您想要停止跟踪的交换机或访问点。

步骤 3 单击**禁用选定项**。

激活对已禁用基础设施设备的跟踪

使用此程序启动对已被禁用的非活动基础设施设备的跟踪。一旦交换机或访问点变为活动状态，Cisco Unified Communications Manager 将开始动态跟踪状态，包括关联至交换机或访问点的端点列表。

开始之前

必须配置位置感知。有关详细信息，请参阅 *Cisco Unified Communications Manager* 系统配置指南的"位置感知"一章。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**高级功能** > **设备位置跟踪服务** > **交换机和访问点**。

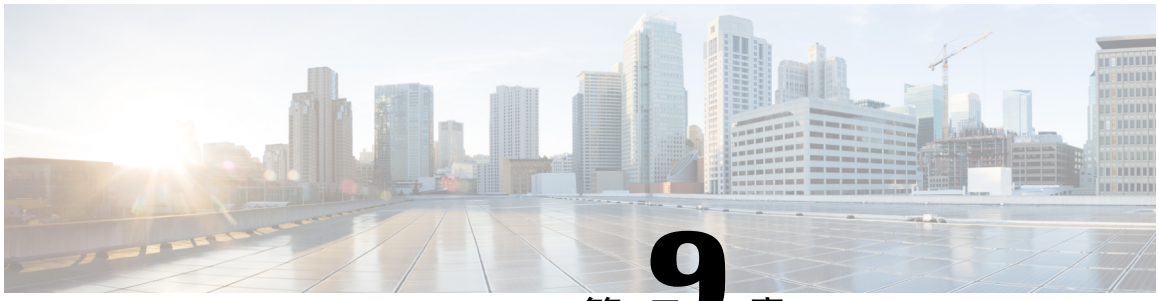
步骤 2 从**相关链接**中，选择**非活动交换机和访问点**，然后单击**转至**。
查找并列出非活动交换机和访问点窗口中将显示未被跟踪的基础设施设备。

步骤 3 选择您要为其启动跟踪的交换机或访问点。

步骤 4 单击**重新激活选定项**。

第 IV 部分

管理系统



第 9 章

监控系统状态

查看群集节点状态

使用此程序显示群集中节点的信息。

过程

步骤 1 从“Cisco Unified 操作系统管理”中，选择**显示** > **群集**。

步骤 2 查看**群集**窗口中的字段。请参阅联机帮助，获取有关字段的详细信息。

查看硬件状态

使用此程序可显示硬件状态和有关您系统中的硬件资源的信息。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**显示** > **硬件**。

步骤 2 查看**硬件状态**窗口中的字段。请参阅联机帮助，获取有关字段的详细信息。

查看网络状态

使用此程序显示您系统的网络状态，例如以太网和 DNS 信息。

显示的网络状态信息取决于是否已启用“网络容错”：

- 如果启用了“网络容错”，则当以太网端口 0 失败时，以太网端口 1 将自动管理网络通信。
- 如果启用了“网络容错”，将会显示网络端口以太网 0、以太网 1 和绑定 0 的网络状态信息。
- 如果未启用“网络容错”，仅会显示以太网 0 的状态信息。

过程

步骤 1 从“Cisco Unified 操作系统管理”中，选择**显示** > **网络**。

步骤 2 查看**网络配置**窗口中的字段。请参阅联机帮助，获取有关字段的详细信息。

查看已安装的软件

使用此程序显示有关软件版本和已安装软件包的信息。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**显示** > **软件**。

步骤 2 查看**软件包**窗口中的字段。请参阅联机帮助，获取有关字段的详细信息。

查看系统状态

使用此程序显示整体系统状态，例如区域设置、运行时间、CPU 使用率和内存使用量的相关信息。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**显示** > **系统**。

步骤 2 查看**系统状态**窗口中的字段。请参阅联机帮助，获取有关字段的详细信息。

查看 IP 首选项

使用此程序显示系统可用的注册端口列表。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**显示** > **IP 首选项**。

步骤 2 （可选） 要过滤或搜索记录，请执行以下任务之一：

- 从第一个列表中，选择搜索参数。
- 从第二个列表中，选择搜索模式。
- 如果适用，指定适当的搜索文本。

步骤 3 单击**查找**。

步骤 4 查看显示在**系统状态**窗口中的字段。请参阅联机帮助，获取有关字段的详细信息。

查看最后一次登录的详细信息

当最终用户（利用本地或 LDAP 凭证）和管理员登录到 Cisco Unified Communications Manager 或 IM and Presence 服务 的 Web 应用程序时，主应用程序窗口会显示最后一次成功和失败登录的详细信息。

使用 SAML SSO 功能登录的用户只能查看最后一次成功的系统登录信息。用户可以参考身份提供程序 (IdP) 应用程序以跟踪不成功的 SAML SSO 登录信息。

以下 Web 应用程序会显示登录尝试信息：

- Cisco Unified Communications Manager：

  Cisco Unified CM 管理

  Cisco Unified 报告

  Cisco Unified 功能配置

- IM and Presence 服务

Cisco Unified CM IM and Presence 管理

Cisco Unified IM and Presence 报告

Cisco Unified IM and Presence 功能配置

只有管理员可以在 Cisco Unified Communications Manager 中登录并查看以下 Web 应用程序的最后一次登录详细信息：

- 灾难恢复系统
- Cisco Unified OS 管理

Ping 节点

使用 Ping 实用程序来 ping 网络中的另一个节点。这些结果可帮助您检验或排查设备连接性故障。

过程

步骤 1 从“Cisco Unified 操作系统管理”中，选择**服务** > **Ping**。

步骤 2 配置 **Ping 配置**窗口中的字段。请参阅联机帮助，了解有关字段及其配置选项的更多信息。

步骤 3 选择 **Ping**。
屏幕上会显示 ping 结果。

显示服务参数

您可能需要比较属于群集中所有服务器上某一特定服务的所有服务参数。您可能还需要仅显示不同步参数（也就是说，一个服务器与另一个服务器值不同的服务参数）或从建议的值进行修改的参数。

使用以下程序以显示群集中所有服务器上特定服务的服务参数。

过程

步骤 1 选择**系统** > **服务参数**。

步骤 2 从“服务器”下拉列表框中选择服务器。

步骤 3 从“服务”下拉列表框中，选择您要在群集中所有服务器上显示服务参数的服务。

注释 “服务参数配置”窗口显示所有服务（活动或不活动）。

步骤 4 在显示的“服务参数配置”窗口中，在“相关链接”下拉列表框中选择“所有服务器的参数”；然后单击“转至”。

此时将显示“所有服务器的参数”窗口。对于当前服务，该列表按字母顺序显示所有参数。对于每个参数，建议的值在参数名称旁边显示。在每个参数名称下，显示包含此参数的服务器列表。在每个服务器名称旁边，显示此参数在此服务器上的当前值。

对于指定的参数，单击服务器名称或当前参数值，链接至相应的服务参数窗口更改该值。单击“上一个”和“下一个”在“所有服务器的参数”窗口之间导航。

步骤 5 如果您需要显示不同步的服务参数，在“相关链接”下拉列表框中选择“所有服务器的不同步参数”，然后单击“转至”。

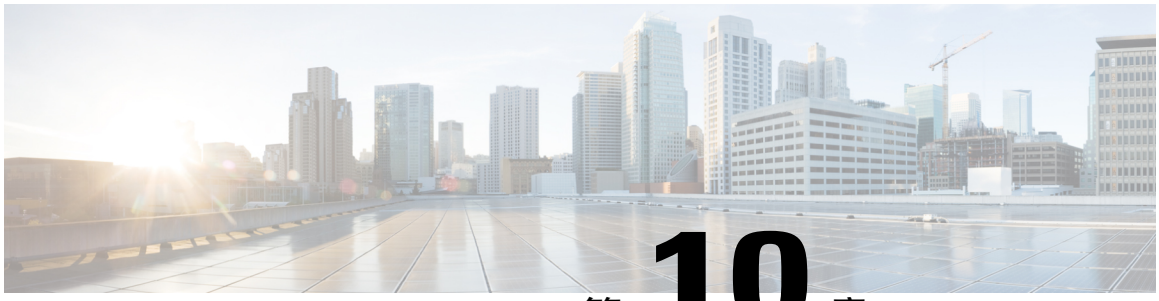
此时将显示“所有服务器的不同步参数”窗口。对于当前服务，在不同服务器上有不同值的服务参数将按字母顺序显示。对于每个参数，建议的值在参数名称旁边显示。在每个参数名称下，显示包含此参数的服务器列表。在每个服务器名称旁边，显示此参数在此服务器上的当前值。

对于指定的参数，单击服务器名称或当前参数值，链接至相应的服务参数窗口更改该值。单击“上一个”和“下一个”在“所有服务器的不同步参数”窗口之间导航。

步骤 6 如果您需要显示从建议值进行修改的服务参数，在“相关链接”下拉列表框中选择“所有服务器的已修改参数”；然后单击“转至”。

此时将显示“所有服务器的已修改参数”窗口。对于当前服务，与建议值有不同值的服务参数将按字母顺序显示。对于每个参数，建议的值在参数名称旁边显示。在每个参数名称下，显示与建议值有不同值的服务器列表。在每个服务器名称旁边，显示此参数在此服务器上的当前值。

对于指定的参数，单击服务器名称或当前参数值，链接至相应的服务参数窗口更改该值。单击“上一个”和“下一个”在“所有服务器的已修改参数”窗口之间导航。



第 10 章

查看使用记录

使用记录概述

Cisco Unified Communications Manager 提供各种记录，您可以查看配置的项目如何在您的系统中使用。配置的项目包括设备，以及系统级设置，例如设备池、日期和时间组，以及路由计划。

从属关系记录

使用从属关系记录用于以下用途：

- 查找关于系统级设置的信息，例如服务器、设备池以及日期和时间组。
- 确定数据库中使用其他记录的记录。例如，您可以确定哪些设备（例如 CTI 路由点或电话）使用特定的呼叫搜索空间。
- 在删除任何记录之前显示记录之间的从属关系。例如，删除分区之前，使用从属关系记录可查看哪些呼叫搜索空间 (CSS) 和设备与之关联。然后，您可以重新配置设置以删除从属关系。

路由计划报告

使用路由计划报告，您可以查看在系统中配置的号码、路由以及模式的部分或完整列表。当生成报告时，您可以通过单击报告中“模式/目录号码”、“分区”或“路由详细信息”列中的条目，访问每个项目的配置窗口。

此外，路由计划报告还可让您将报告数据保存到 .CSV 文件，以导入其他应用程序。.CSV 文件包含的信息比网页更详细，其中包括电话的目录号码、路由模式、模式的使用、设备名称以及设备说明。

Cisco Unified Communications Manager 使用路由计划来路由内部呼叫和外部公共交换电话网 (PSTN) 呼叫。由于在您的网络中可能有多个记录，借助 Cisco Unified Communications Manager 管理，您可以根据特定的条件查找特定的路由计划记录。

使用报告任务

过程

	命令或操作	目的
步骤 1	要查看路由计划记录并使用它们管理未分配的目录号码，请参阅以下程序： • 查看路由计划记录， 第 83 页 • 保存路由计划报告， 第 83 页 • 删除未分配的目录号码， 第 84 页 • 更新未分配的目录号码， 第 84 页	使用这些程序查找特定的路由计划记录，将记录保存在 .CSV 文件中，并管理未分配的目录号码。
步骤 2	要使用从属关系记录，请参阅以下程序： • • 查看从属关系记录， 第 86 页	使用这些程序查找关于系统级设置的信息并显示数据库中记录之间的从属关系。

路由计划报告任务流程

过程

	命令或操作	目的
步骤 1	查看路由计划记录， 第 83 页.	查看路由计划记录并生成自定义的路由计划报告。
步骤 2	保存路由计划报告， 第 83 页。	查看 .csv 文件格式的路由计划报告。
步骤 3	删除未分配的目录号码， 第 84 页。	从路由计划报告中删除未分配的目录号码。
步骤 4	更新未分配的目录号码， 第 84 页。	从路由计划报告中更新未分配的目录号码的设置。

查看路由计划记录

本节介绍如何查看路由计划记录。由于在您的网络中可能有多个记录，借助 Cisco Unified Communications Manager 管理，您可以根据特定的条件查找特定的路由计划记录。按照以下程序生成自定义的路由计划报告。

过程

步骤 1 选择**呼叫路由** > **路由计划报告**。

步骤 2 要查找数据库中的所有记录，请确保对话框为空，并转至第 3 步。
要过滤或搜索记录

a) 从第一个下拉列表框中选择搜索参数。
b) 从第二个下拉列表框中选择搜索模式。
c) 如果适用，指定适当的搜索文本。

步骤 3 单击**查找**。
此时将显示所有相匹配的记录。通过在“每页行数”下拉列表框中选择不同的值，可以更改每个页面中显示的项目数量。

步骤 4 从显示的记录列表中，单击要查看的记录的链接。
窗口中将显示您选择的项目。

保存路由计划报告

本节包含有关如何以 .csv 文件查看路由计划报告的信息。

过程

步骤 1 选择**呼叫路由** > **路由计划报告**。

步骤 2 从**路由计划报告**窗口的**相关链接**下拉列表中，选择**以文件查看**，然后单击**转至**。
在出现的对话框中，可以保存文件或将其导入到另一个应用程序。

步骤 3 单击**保存**。
另一个窗口将会显示，可让您将此文件保存到选择的位置。

注释 您也可以将文件保存为另一个名称，但文件名必须包含 .CSV 扩展名。

步骤 4 选择文件保存位置，然后单击**保存**。此操作应会将该文件保存到您指定的位置。

步骤 5 找到您刚才保存的 .CSV 文件，双击其图标即可查看。

删除未分配的目录号码

本节介绍如何从路由计划报告删除未分配的目录号码。目录号码在 Cisco Unified Communications Manager 管理的“目录号码配置”窗口中配置和删除。从删除的设备或电话中删除目录号码时，该目录号码在 Cisco Unified Communications Manager 数据库中仍然存在。要从数据库中删除目录号码，请使用“路由计划报告”窗口。

过程

步骤 1 选择呼叫**呼叫路由** > **路由计划报告**。

步骤 2 在“路由计划报告”窗口中，使用三个下拉列表指定列出所有未分配目录号码的路由计划报告。

步骤 3 存在三种方式可删除目录号码：

a) 单击您要删除的目录号码。显示“目录号码配置”窗口时，单击“删除”。

b) 选中您要删除的目录号码旁边的复选框。单击“删除选定项”。

c) 要删除所有找到的未分配的目录号码，请单击“删除所有已找到的项”。
此时将显示警告消息，确认您要删除目录号码。

步骤 4 要删除目录号码，请单击“确定”。要取消删除请求，请单击“取消”。

更新未分配的目录号码

本节介绍如何从路由计划报告更新未分配的目录号码的设置。目录号码在 Cisco Unified Communications Manager 管理的“目录号码配置”窗口中配置和删除。目录号码从设备删除后，在 Cisco Unified Communications Manager 数据库中仍然存在。要更新该目录号码的设置，请使用“路由计划报告”窗口。

过程

步骤 1 选择**呼叫路由** > **路由计划报告**。

步骤 2 在**路由计划报告**窗口中，使用三个下拉列表指定列出所有未分配目录号码的路由计划报告。

步骤 3 单击您要更新的目录号码。

注释 除了目录号码和分区之外，目录号码的所有其他设置都可以更新。

步骤 4 进行所需的更新，例如呼叫搜索空间或前转选项。

步骤 5 单击**保存**。
“目录号码配置”窗口将会重新显示，并且目录号码字段为空。

从属关系记录任务流程

过程

	命令或操作	目的
步骤 1	配置从属关系记录，第 85 页.	使用此程序启用或禁用从属关系记录。此程序以低于正常的优先级运行，并且由于拨号方案的大小和复杂程度、CPU 速度以及其他应用程序的 CPU 要求可能需要一段时间来完成。
步骤 2	查看从属关系记录，第 86 页。	启用从属关系记录后，您可以从界面上的配置窗口访问它们。

配置从属关系记录

使用从属关系记录查看 Cisco Unified Communications Manager 数据库中记录之间的关系。例如，删除分区之前，使用从属关系记录可查看哪些呼叫搜索空间 (CSS) 和设备与之关联。

⚠

注意 从属关系记录会导致高 CPU 使用率。此程序以低于正常的优先级运行，并且由于拨号方案的大小和复杂程度、CPU 速度以及其他应用程序的 CPU 要求可能需要一段时间来完成。

如果您启用了从属关系记录并且您的系统遇到 CPU 使用率问题，您可以禁用从属关系记录。

过程

步骤 1 从Cisco Unified CM 管理中，选择**系统** > **企业参数**。

步骤 2 滚动至 **CCMAdmin 参数**部分，并从**启用从属关系记录**下拉列表中，选择以下选项之一：

- **真** — 启用从属关系记录。
- **假** — 禁用从属关系记录。

根据您选择的选项，将显示一个对话框及关于启用或禁用从属关系记录后果的消息。请阅读该消息，然后再单击此对话框中的**确定**。

步骤 3 单击**确定**。

步骤 4 单击**保存**。

随即会出现更新成功消息，确认所作更改。

查看从属关系记录

启用从属关系记录后，您可以从界面上的配置窗口访问它们。

开始之前

配置从属关系记录，第 85 页

过程

步骤 1 从 Cisco Unified CM 管理中，导航到您要查看的记录的配置窗口。

示例：
要查看一个设备池的从属关系记录，请选择**系统** > **设备池**。

注释 无法从**设备默认值**和**企业参数配置**窗口中查看从属关系记录。

步骤 2 单击**查找**。

步骤 3 单击记录之一。
随即会出现配置窗口。

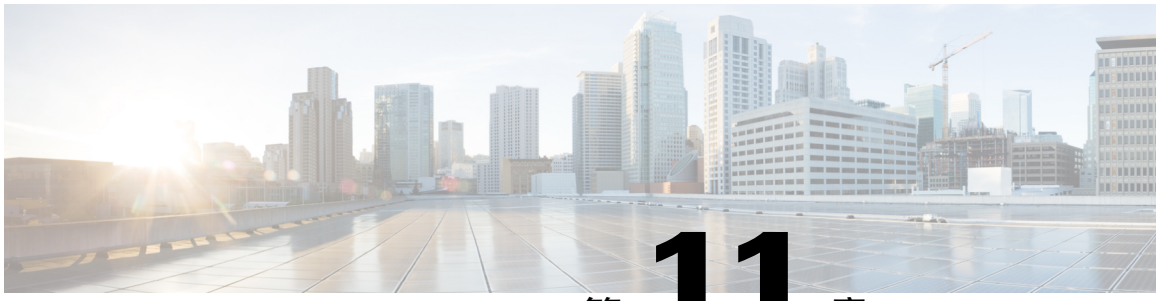
步骤 4 从**相关链接**列表框中，选择**从属关系记录**框，然后单击**转至**。

注释 如果您尚未启用从属关系记录，**从属关系记录摘要**窗口将显示一条消息，而不是关于记录的信息。

从属关系记录摘要窗口将出现，显示被数据库中其他记录使用的记录。

步骤 5 在此窗口中选择以下从属关系记录按钮之一：

- **刷新** — 以当前信息更新窗口。
- **关闭** — 关闭窗口而不返回您在其中点击“从属关系记录”链接的配置窗口。
- **关闭并返回** — 关闭窗口并返回您在其中点击“从属关系记录”链接的配置窗口。



第 11 章

备份系统

备份概述

思科建议定期执行备份。您可以使用灾难恢复系统(DRS)为群集中的所有服务器执行完整数据备份。您可以设置自动备份或随时调用备份。

灾难恢复系统执行群集层级备份，这意味着它会将一个 Cisco Unified Communications Manager 群集中所有服务器的备份收集到中心位置，并将备份数据存档到物理存储设备。备份文件已加密，并且只能由系统软件打开。

DRS 恢复其自己的设置（备份设备设置和计划设置）作为平台备份/恢复的一部分。DRS 备份和恢复 drfDevice.xml 和 drfSchedule.xml 文件。使用这些文件恢复服务器时，您无需重新配置 DRS 备份设备和计划。

当您执行系统数据恢复时，可以选择要恢复群集中的哪些节点。

灾难恢复系统包括以下功能：

- 用于执行备份和恢复任务的用户界面。
- 用于执行备份功能的分布式系统架构。
- 计划的备份或手动（用户调用）备份。
- 它会将备份存档到远程 sftp 服务器。

备份前提条件

- 确保您符合版本要求：

  所有 Cisco Unified Communications Manager 群集节点都必须运行相同版本的 Cisco Unified Communications Manager 应用程序。

  所有 IM and Presence 服务群集节点都必须运行相同版本的 IM and Presence 服务应用程序。

  备份文件中保存的软件版本必须与群集节点上运行的版本匹配。

  整个版本字符串必须匹配。例如，如果 IM and Presence 数据库发布方节点上的版本为 11.5.1.10000-1，则所有 IM and Presence 订阅方节点都必须是 11.5.1.10000-1，并且备份文件也必须是 11.5.1.10000-1。如果您尝试从与当前版本不匹配的备份文件恢复系统，恢复将失败。无论何时升级软件版本，都请确保备份系统，以使备份文件中保存的版本与群集节点上运行的版本匹配。

- 请注意，DRS 加密取决于群集安全密码。运行备份时，DRS 会生成一个随机密码用于加密，然后使用群集安全密码对随机密码进行加密。如果在备份与此次恢复之间，群集安全密码发生了更改，那么您需要知道备份时的密码是什么，才能使用该备份文件恢复系统，或者，在安全密码更改/重置后立即进行备份。
- 如果想要备份到远程设备，请确保您拥有 SFTP 服务器设置。有关可用 SFTP 服务器的详细信息，请参阅 用于远程备份的 SFTP 服务器，第 94 页

备份任务流程

完成这些任务以配置和运行备份。备份正在运行时，不要执行任何操作系统管理任务。这是因为灾难恢复系统会通过锁定平台 API 来阻止所有操作系统管理请求。但是，灾难恢复系统不会阻止大多数 CLI 命令，因为只有基于 CLI 的升级命令使用平台 API 锁定软件包。

过程

	命令或操作	目的
步骤 1	配置备份设备，第 89 页	指定要在其上备份数据的设备。
步骤 2	估算备份文件的大小，第 90 页	估计在SFTP设备上创建的备份文件的大小。
步骤 3	选择下列选项之一： • 配置计划的备份，第 90 页 • 开始手动备份，第 92 页	创建一个备份计划以按计划备份数据。 或者，也可以运行手动备份。

	命令或操作	目的
步骤 4	查看当前备份状态，第 92 页	可选。检查备份的状态。备份运行时，您可以检查当前备份作业的状态。
步骤 5	查看备份历史记录，第 93 页	可选。查看备份历史记录

配置备份设备

最多可以配置 10 个备份设备。执行以下步骤以配置要存储备份文件的位置。

开始之前

- 确保您对 SFTP 服务器中的目录路径拥有写入访问权限，以存储备份文件。
- 确保用户名、密码、服务器名称和目录路径有效，因为 DRS Master Agent 会验证备份设备的配置。

注释 计划在预期网络通信量较少的时段期间进行备份。

过程

步骤 1 从灾难恢复系统中，选择**备份** > **备份设备**。

步骤 2 在**备份设备列表**窗口中，执行下列操作之一：

- 要配置新设备，请单击**新增**。
- 要编辑现有的备份设备，请输入搜索条件，单击“查找”，然后单击**选定编辑**。
- 要删除备份设备，请在**备份设备**列表中将其选中，然后单击**删除选定项**。

您无法删除配置为备份计划中备份设备的备份设备。

步骤 3 在**备份设备名称**字段中输入备份名称。
备份设备名称只能包含字母数字字符、空格 ( )、连字符 (-) 和下划线 (_)。请勿使用任何其他字符。

步骤 4 在**网络目录**下方的**选择目标**区域中，执行以下操作：

- 在**主机名/IP 地址**字段中，输入网络服务器的主机名或 IP 地址。
- 在**路径名**字段中，输入您要存储备份文件的目录路径。
- 在**用户名**字段，输入有效的用户名。

- 在**密码**字段中，输入有效的密码。
- 从**要存储在网络目录上的备份数量**下拉列表中，选择所需的备份数量。

步骤 5 单击**保存**。

接下来的操作

估算备份文件的大小，第 90 页

估算备份文件的大小

只有当存在一个或多个选定功能的备份历史记录时，Cisco Unified Communications Manager 才会估算备份 tar 的大小。

计算出的大小并非精确值，而是备份 tar 的估计大小。系统会根据上一次成功备份的实际备份大小来计算，如果自上次备份后配置发生了更改，则大小可能会有所变化。

仅当存在先前的备份时，您才能使用此程序。若是第一次备份系统，则不可使用此程序。

按照此程序来估计保存到 SFTP 设备的备份 tar 的大小。

过程

步骤 1 从灾难恢复系统中，选择**备份** > **手动备份**。

步骤 2 在**选择功能**区域中，选择要备份的功能。

步骤 3 单击**估计大小**以查看所选功能备份的估计大小。

接下来的操作

执行以下程序之一以备份您的系统：

- 配置计划的备份，第 90 页
- 开始手动备份，第 92 页

配置计划的备份

最多可以创建 10 个备份计划。每个备份计划都有自己的一组属性，包括自动备份计划、要备份的功能集和存储位置。

请注意，您的备份 .tar 文件已使用随机生成的密码加密。然后会使用群集安全密码对此密码进行加密，并随备份 .tar 文件一起保存。您必须记住此安全密码，或在安全密码更改或重置后立即进行备份。

注意 计划在非高峰时段备份以避免呼叫处理中断和影响服务。

开始之前

配置备份设备，第 89 页

过程

步骤 1 从灾难恢复系统中，选择**备份计划程序**。

步骤 2 在**计划列表**窗口中，执行以下步骤之一以添加新的计划或编辑一个现有的计划。

- 要创建新的计划，单击**新增**。
- 要配置现有的计划，单击“计划列表”列中的名称。

步骤 3 在**计划程序**窗口中，在**计划名称**字段中输入计划名称。

注释 您无法更改默认计划的名称。

步骤 4 在**选择备份设备**区域选择备份设备。

步骤 5 在**选择功能**区域选择要备份的功能。必须至少选择一项功能。

步骤 6 在**开始备份时间**区域选择您希望开始备份的日期和时间。

步骤 7 在**频率**区域选择您希望进行备份的频率。频率可以设置为“每天一次”、“每周”和“每月"。如果选择**每周**，您还可以选择一周内哪几天进行备份。

提示 要将备份频率设置为**每周**，从星期二到星期六进行备份，可单击**设置默认值**。

步骤 8 要更新这些设置，单击**保存**。

步骤 9 选择下列选项之一：

- 要启用所选的计划，单击**启用所选计划**。
- 要禁用所选的计划，单击**禁用所选计划**。
- 要删除所选的计划，单击**删除选定项**。

步骤 10 要启用计划，单击**启用计划**。

下次备份将在您设置的时间自动进行。

注释 确保群集中的所有服务器都运行相同版本的 Cisco Unified Communications Manager 或 Cisco IM and Presence 服务，并可通过网络接通。在计划的备份时间无法接通的服务器将不会备份。

接下来的操作

执行以下程序：

- 估算备份文件的大小，第 90 页
- （可选） 查看当前备份状态，第 92 页

开始手动备份

开始之前

- 确保使用网络设备作为备份文件的存储位置。Unified Communications Manager 的虚拟化部署不支持使用磁带驱动器存储备份文件。
- 确保所有群集节点都安装有相同的 Cisco Unified Communications Manager 版本或 IM and Presence 服务。
- 备份过程可能会由于远程服务器上没有可用空间或由于网络连接中断而失败。在解决导致备份失败的问题后，您需要开始一个全新备份。
- 确保没有网络中断。
- 配置备份设备，第 89 页
- 估算备份文件的大小，第 90 页
- 确保您有群集安全密码记录。如果在完成此备份之后，群集安全密码发生了更改，您需要知道密码，否则将无法使用备份文件来恢复您的系统。

注释 备份运行时，您无法在“Cisco Unified 操作系统管理”或“Cisco Unified IM and Presence 操作系统管理”中执行任何任务，因为灾难恢复系统会锁定平台 API 来阻止所有请求。但是，灾难恢复系统不会阻止大多数 CLI 命令，因为只有基于 CLI 的升级命令使用平台 API 锁定软件包。

过程

步骤 1 从灾难恢复系统中，选择**备份** > **手动备份**。

步骤 2 在**手动备份**窗口中，从**备份设备名称**区域选择备份设备。

步骤 3 从**选择功能**区域选择一项功能。

步骤 4 单击**开始备份**。

接下来的操作

（可选） 查看当前备份状态，第 92 页

查看当前备份状态

执行以下步骤以检查当前备份作业的状态。

注意 请注意，如果备份到远程服务器没有在 20 小时内完成，备份会话将超时，您必须开始一个全新备份。

过程

步骤 1 从灾难恢复系统中，选择**备份** > **当前状态**。

步骤 2 要查看备份日志文件，请单击日志文件名链接。

步骤 3 要取消当前备份，请单击**取消备份**。

注释 备份将在当前组件完成其备份操作后取消。

接下来的操作

查看备份历史记录，第 93 页

查看备份历史记录

如要查看备份历史记录，请执行以下步骤。

过程

步骤 1 从灾难恢复系统中，选择**备份** > **历史记录**。

步骤 2 从**备份历史记录**窗口中，您可以查看已执行的备份，包括文件名、备份设备、完成日期、结果、版本、已备份的功能，以及失败的功能。

注释 **备份历史记录**窗口只显示最近 20 次备份作业。

备份相互作用和限制

备份限制

以下限制适用于备份：

表 2： 备份限制

限制	说明
群集安全密码	我们建议您每当更改群集安全密码时都运行备份。 备份加密使用群集安全密码加密备份文件上的数据。如果在创建备份文件后编辑群集安全密码，您将无法使用该备份文件恢复数据，除非您记得旧密码。
证书管理	灾难恢复系统 (DRS) 使用 Master Agent 与 Local Agent 之间基于 SSL 的通信，验证和加密 Cisco Unified Communications Manager群集节点之间的数据。DRS 使用 IPsec 证书进行其公钥/私钥加密。请注意，如果您从“证书管理”页面删除 IPSEC 信任存储库 (hostname.pem) 文件，DRS 将不会按预期工作。如果您手动删除 IPSEC-信任文件，必须确保将 IPSEC 证书上载到 IPSEC-信任。有关详细信息，请参阅《*Cisco Unified Communications Manager* 安全指南》中的“证书管理”部分，该文档位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

用于远程备份的 SFTP 服务器

要在网络上将数据备份到远程设备，您必须有经过配置的 SFTP 服务器。您可以使用任何 SFTP 服务器产品，但我们建议使用“思科技术合作伙伴”认证的产品。有关哪些供应商已使用您的 Cisco Unified Communications Manager 版本认证其产品的信息，请参阅思科开发商网络（网址为 https://marketplace.cisco.com）上的解决方案目录。

使用下表中的信息来确定要在您的系统中使用哪种 SFTP 服务器解决方案。

表 3： *SFTP* 服务器信息

SFTP 服务器	信息
Cisco Prime Collaboration 部署上的 SFTP 服务器	此服务器由思科提供和测试，并由思科 TAC 提供支持。 版本兼容性取决于您的 Unified Communications Manager 版本和 Cisco Prime Collaboration 部署。在升级其版本 (SFTP) 或 Unified Communications Manager 之前，请参阅《*Cisco Prime Collaboration* 部署管理指南》，以确保版本兼容。

SFTP 服务器	信息
来自技术合作伙伴的 SFTP 服务器	这些服务器由第三方提供，第三方测试，并由 TAC 和思科供应商联合提供支持。 版本兼容性取决于第三方测试。如果升级其 SFTP 产品和/或升级版本兼容的 Unified Communications Manager，请参阅“技术合作伙伴”页面： https://marketplace.cisco.com
来自其他第三方的 SFTP 服务器	这些服务器由第三方提供、经过有限的思科测试，不受思科 TAC 官方支持。 版本兼容性乃尽力提供，以建立兼容的 SFTP 版本和 Unified Communications Manager 版本。 要获取经过全面测试且受支持的 SFTP 解决方案，请使用 Cisco Prime Collaboration 部署或技术合作伙伴。

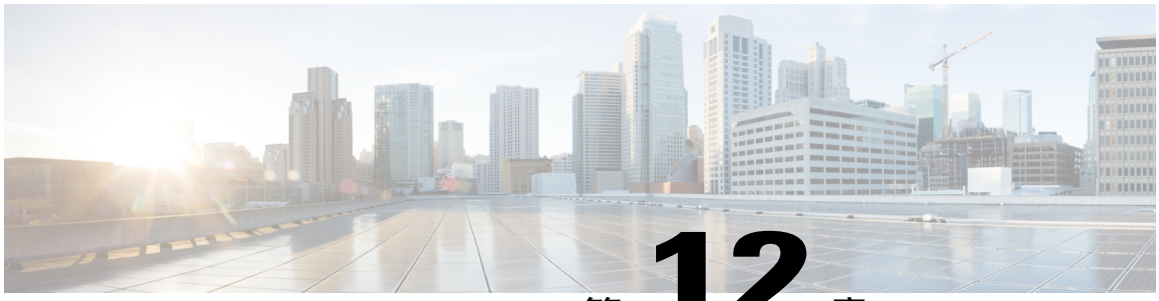
思科使用下列服务器来进行内部测试。您可以使用下列服务器之一，但必须与供应商联系以获得支持：

- 开放式 SSH
- Titan

思科不支持使用 SFTP 产品 freeFTPd。这是因为此 SFTP 产品有 1 GB 文件大小限制。

有关如何设置第三方 SFTP 产品的详细信息，请与第三方供应商联系以获得支持。有关尚未通过思科技术开发者计划 (Cisco Technology Developer Program) 流程认证的第三方产品的问题，请与第三方供应商联系以获得支持。有关将 GlobalSCAPE 与支持的 Cisco Unified Communications Manager 版本配合使用的信息，请与 GlobalSCAPE 联系。

注释 我们建议您在升级 Unified Communications Manager、升级 SFTP 服务器，或改用不同的 SFTP 服务器之后，重新测试 DRS 与您的 SFTP 服务器。执行此步骤以确保这些组件能一起正常运行。最好的做法是，在备用或备份服务器上执行备份和恢复。



第 12 章

恢复系统

恢复概述

灾难恢复系统 (DRS) 提供了一个向导，可带您了解恢复系统的过程。

备份文件是加密的，只有 DRS 系统可以打开它们以恢复数据。灾难恢复系统包括以下功能：

- 用于执行恢复任务的用户界面。
- 用于执行恢复功能的分布式系统架构。

Master Agent

系统会自动在群集中的每个节点上启动 Master Agent 服务，但 Master Agent 仅在发布方节点上工作。订阅方节点上的 Master Agent 不执行任何功能。

Local Agent

服务器利用 Local Agent 执行备份和恢复功能。

Cisco Unified Communications Manager 群集中的每个节点，包括包含 Master Agent 的节点，必须有自己的 Local Agent 来执行备份和恢复功能。

注释 默认情况下，Local Agent 会在群集的每个节点自动启动，包括 IM and Presence 节点。

恢复前提条件

- 确保您符合版本要求：

  所有 Cisco Unified Communications Manager 群集节点都必须运行相同版本的 Cisco Unified Communications Manager 应用程序。

  所有 IM and Presence 服务群集节点都必须运行相同版本的 IM and Presence 服务应用程序。

  备份文件中保存的版本必须与群集节点上运行的版本匹配。

  整个版本字符串必须匹配。例如，如果 IM and Presence 数据库发布方节点上的版本为 11.5.1.10000-1，则所有 IM and Presence 订阅方节点都必须是 11.5.1.10000-1，并且备份文件也必须是 11.5.1.10000-1。如果您尝试从与当前版本不匹配的备份文件恢复系统，恢复将失败。

- 确保服务器的 IP 地址、主机名、DNS 配置和部署类型与备份文件上存储的 IP 地址、主机名、DNS 配置和部署类型匹配。
- 如果您自运行备份后更改了群集安全密码，请确保您有旧密码的记录，否则恢复将失败。

恢复任务流程

在恢复过程中，不要使用 Cisco Unified Communications Manager 操作系统管理或 Cisco Unified IM and Presence 操作系统管理执行任何任务。

过程

	命令或操作	目的
步骤 1	仅恢复第一个节点，第 99 页	（可选）使用此程序仅恢复群集中的第一个发布方节点。
步骤 2	恢复后续群集节点，第 100 页	（可选）使用此程序恢复群集中的订阅方节点。
步骤 3	发布方重建后在一个步骤中恢复群集，第 101 页	（可选）如果发布方已重建，按照此程序在一个步骤中恢复整个群集。
步骤 4	恢复整个群集，第 103 页	（可选）使用此程序恢复群集中的所有节点，包括发布方节点。如果发生重大硬盘驱动器故障或升级，或如果硬盘驱动器迁移，您可能需要重建群集中的所有节点。

	命令或操作	目的
步骤 5	将节点或群集恢复到上次已知的良好配置，第 104 页	（可选）仅当将节点恢复到上次已知的良好配置时，才使用此程序。硬盘驱动器故障或其他硬件故障后不要使用此程序。
步骤 6	重新启动节点，第 104 页	使用此程序重新启动节点。
步骤 7	检查恢复作业状态，第 105 页	（可选）使用此程序检查恢复作业状态。
步骤 8	查看恢复历史记录，第 105 页	（可选）使用此程序查看恢复历史记录。

仅恢复第一个节点

若要在重建后恢复第一个节点，您必须配置备份设备。

此程序适用于 Cisco Unified Communications Manager 第一个节点，也称为发布方节点。其他 Cisco Unified Communications Manager 节点和所有 IM and Presence 服务节点均被视为辅助节点或订阅方。

开始之前

如果群集中有 IM and Presence 服务节点，确保当您恢复第一个节点时该节点正在运行并且可以访问。这是必需的，以便在执行程序期间可以找到有效的备份文件。

过程

步骤 1 从灾难恢复系统中，选择**恢复** > **恢复向导**。

步骤 2 在**恢复向导第 1 步**窗口中，**选择备份设备**区域，选择要恢复的适当的备份设备。

步骤 3 单击**下一步**。

步骤 4 在**恢复向导第 2 步**窗口中，选择要恢复的备份文件。

注释 备份文件名会指示系统创建备份文件的日期和时间。

步骤 5 单击**下一步**。

步骤 6 在**恢复向导第 3 步**窗口中，单击**下一步**。

步骤 7 选择要恢复的功能。

注释 随即将显示您为备份选择的功能。

步骤 8 选择要恢复的节点。

步骤 9 单击**恢复**以恢复数据。

步骤 10 单击**下一步**。

步骤 11 当系统提示您选择要恢复的节点时，仅选择第一个节点（发布方）。

注意　在此情况下，不要选择后续（订阅方）节点，因为这将导致恢复尝试失败。

步骤 12　（可选）从**选择服务器名称**下拉列表中，选择要从其中恢复发布方数据库的订阅方节点。确保您选择的订阅方节点正在运行并连接到群集。

灾难恢复系统会从备份文件恢复所有非数据库信息，并从所选的订阅方节点拉取最新的数据库。

注释　仅当您选择的备份文件包含 CCMDB 数据库组件，此选项才会出现。最初，仅发布方节点会完全恢复，但当您执行第 14 步并重新启动后续群集节点时，灾难恢复系统将执行数据库复制，并完全同步所有群集节点数据库。这可确保所有群集节点都使用当前数据。

步骤 13　单击**恢复**。

步骤 14　您的数据会在发布方节点上恢复。视您的数据库大小和选择要恢复的组件，系统可能需要几个小时才能恢复。

注释　恢复第一个节点，会将整个 Cisco Unified Communications Manager 数据库恢复到群集。这可能需要几个小时，具体取决于节点的数量和正在恢复的数据库的大小。视您的数据库大小和选择要恢复的组件，系统可能需要几个小时才能恢复。

步骤 15　当**恢复状态**窗口上的**完成百分比**字段显示 100% 时，重新启动服务器。如果仅恢复到第一个节点，需要重新启动群集中的所有节点。确保先重启第一个节点，然后再重启后续节点。有关如何重启服务器的信息，请参阅“下一步操作”部分。

注释　如果您要仅恢复 Cisco Unified Communications Manager 节点，必须重新启动 Cisco Unified Communications Manager 和 IM and Presence 服务群集。

如果您要仅恢复 IM and Presence 服务发布方节点，必须重新启动 IM and Presence 服务群集。

接下来的操作

- （可选）要查看恢复状态，请参阅 检查恢复作业状态，第 105 页
- 要重新启动节点，请参阅 重新启动节点，第 104 页

恢复后续群集节点

此程序仅适用于 Cisco Unified Communications Manager 订阅方（后续）节点。安装的第一个 Cisco Unified Communications Manager 节点是发布方节点。所有其他 Cisco Unified Communications Manager 节点和所有 IM and Presence 服务节点都是订阅方节点。

按照此程序恢复群集中的一个或多个 Cisco Unified Communications Manager 订阅方节点。

开始之前

在执行恢复操作之前，确保恢复的主机名、IP 地址、DNS 配置和部署类型与您要恢复的备份文件的主机名、IP 地址、DNS 配置和部署类型匹配。灾难恢复系统不会跨不同的主机名、IP 地址、DNS 配置和部署类型恢复。

确保服务器上安装的软件版本与您要恢复的备份文件的版本匹配。灾难恢复系统只支持匹配的软件版本进行恢复操作。若要在重建后恢复后续节点，您必须配置备份设备。

过程

步骤 1 从灾难恢复系统中，选择**恢复** > **恢复向导**。

步骤 2 在**恢复向导第 1 步**窗口中，**选择备份设备**区域，选择要从其中恢复的备份设备。

步骤 3 单击**下一步**。

步骤 4 在**恢复向导第 2 步**窗口中，选择要恢复的备份文件。

步骤 5 单击**下一步**。

步骤 6 在**恢复向导第 3 步**窗口中，选择要恢复的功能。

注释 只会显示那些备份到您所选文件的功能。

步骤 7 单击**下一步**。此时将显示“恢复向导第 4 步”窗口。

步骤 8 在**恢复向导第 4 步**窗口中，当系统提示您选择要恢复的节点时，请只选择后续节点。

步骤 9 单击**恢复**。

步骤 10 您的数据会在后续节点上恢复。有关如何查看恢复状态的详细信息，请参阅“下一步操作”部分。

注释 在恢复过程中，不要使用“Cisco Unified Communications Manager 管理”或“用户选项”执行任何任务。

步骤 11 当**恢复状态**窗口上的**完成百分比**字段显示 100% 时，重新启动刚刚恢复的辅助服务器。如果仅恢复到第一个节点，需要重新启动群集中的所有节点。确保先重启第一个节点，然后再重启后续节点。有关如何重启服务器的信息，请参阅“下一步操作”部分。

注释 如果恢复了 IM and Presence 服务第一个节点，确保在重新启动 IM and Presence 服务后续节点之前，重新启动 IM and Presence 服务第一个节点。

接下来的操作

- （可选）要查看恢复状态，请参阅 检查恢复作业状态，第 105 页
- 要重新启动节点，请参阅 重新启动节点，第 104 页

发布方重建后在一个步骤中恢复群集

视您的数据库大小和选择要恢复的组件，系统可能需要几个小时才能恢复。（可选）如果发布方已重建或新装，按照此程序在一个步骤中恢复整个群集。

过程

步骤 1 从灾难恢复系统中，选择**恢复** > **恢复向导**。

步骤 2 在**恢复向导第 1 步**窗口中，**选择备份设备**区域，选择要从其中恢复的备份设备。

步骤 3 单击**下一步**。

步骤 4 在**恢复向导第 2 步**窗口中，选择要恢复的备份文件。

备份文件名会指示系统创建备份文件的日期和时间。

仅选择您要从其中恢复整个群集的那一个群集的备份文件。

步骤 5 单击**下一步**。

步骤 6 在**恢复向导第 3 步**窗口中，选择要恢复的功能。
屏幕仅会显示那些被保存到备份文件中的功能。

步骤 7 单击**下一步**。

步骤 8 在**恢复向导第 4 步**窗口中，单击**一步恢复**。
仅当选择进行恢复的备份文件为群集的备份文件，且选择进行恢复的功能包括在发布方和订阅方节点都进行了注册的功能时，此选项才会出现在**恢复向导第 4 步**窗口中。有关详细信息，请参阅仅恢复第一个节点，第 99 页和恢复后续群集节点，第 100 页。

注释 如果状态消息指示“发布方未能变成群集感知。无法开始一步恢复“，则您需要恢复发布方节点，然后再恢复订阅方节点。有关详细信息，请参阅相关主题。

此选项允许发布方变成群集感知，将需要五分钟来执行此操作。单击此选项后，即会显示一条状态消息：“请等待 5 分钟，直到发布方变成群集感知，在此期间请不要开始任何备份或恢复活动”。

延迟后，如果发布方变成群集感知，则会一条状态消息：“发布方已变成群集感知。请选择服务器，然后单击“恢复”以开始恢复整个群集”。

延迟后，如果发布方未变成群集感知，则会一条状态消息：“发布方未能变成群集感知。无法开始一步恢复。请继续并执行正常的两步恢复。"要以两步（先发布方，然后订阅方）恢复整个群集，请执行仅恢复第一个节点，第 99 页和恢复后续群集节点，第 100 页中所述的步骤。

步骤 9 当系统提示您选择要恢复的节点时，选择群集中的所有节点。
当恢复第一个节点后，灾难恢复系统会自动在后续节点上恢复 Cisco Unified Communications Manager 数据库 (CCMDB)。这可能需要几个小时，具体取决于节点的数量和正在恢复的数据库的大小。

步骤 10 单击**恢复**。
您的数据会在群集中的所有节点上恢复。

步骤 11 当**恢复状态**窗口上的**完成百分比**字段显示 100% 时，重新启动服务器。如果仅恢复到第一个节点，需要重新启动群集中的所有节点。确保先重启第一个节点，然后再重启后续节点。有关如何重启服务器的信息，请参阅“下一步操作”部分。

接下来的操作

- （可选）要查看恢复状态，请参阅 检查恢复作业状态，第 105 页
- 要重新启动节点，请参阅 重新启动节点，第 104 页

相关主题

仅恢复第一个节点，第 99 页
恢复后续群集节点，第 100 页

恢复整个群集

如果发生重大硬盘驱动器故障或升级，或如果硬盘驱动器迁移，您得重建群集中的所有节点。执行这些步骤以恢复整个群集。

如果您正在做大多数其他类型的硬件升级，例如更换网卡或添加内存，则您不需要执行此程序。

过程

步骤 1 从灾难恢复系统中，选择**恢复** > **恢复向导**。

步骤 2 在**选择备份设备**区域，选择要恢复的适当的备份设备。

步骤 3 单击**下一步**。

步骤 4 在**恢复向导第 2 步**窗口中，选择要恢复的备份文件。

注释 备份文件名会指示系统创建备份文件的日期和时间。

步骤 5 单击**下一步**。

步骤 6 在**恢复向导第 3 步**窗口中，单击**下一步**。

步骤 7 在**恢复向导第 4 步**窗口中，当提示选择恢复节点时，选择所有节点。

步骤 8 单击**恢复**以恢复数据。

当恢复第一个节点后，灾难恢复系统会自动在后续节点上恢复 Cisco Unified Communications Manager 数据库 (CCMDB)。这可能需要几个小时，具体取决于节点的数量和数据库的大小。

数据会恢复到所有节点上。

注释 在恢复过程中，不要使用“Cisco Unified Communications Manager 管理”或“用户选项”执行任何任务。

视您的数据库大小和选择要恢复的组件，系统可能需要几个小时才能恢复。

步骤 9 在恢复过程完成后，重新启动服务器。请参阅“下一步操作”部分，了解有关如何重启服务器的详细信息。

注释 确保先重启第一个节点，然后再重启后续节点。

在第一个节点重新启动并运行恢复的 Cisco Unified Communications Manager 版本后，重新启动后续节点。

步骤 10 群集重启后，将会自动设置复制。通过使用《*Cisco Unified Communications* 解决方案的命令行界面参考指南》中所述的 “utils dbreplication runtimestate” CLI 命令，检查所有节点上的“复制状态”值。每个节点上的值应等于 2。

注释 后续节点重新启动后，在后续节点上的数据库复制可能需要足够的时间才能完成，具体视群集的大小而定。

提示 如果复制未正确设置，使用如《*Cisco Unified Communications* 解决方案的命令行界面参考指南》中所述的 "utils dbreplication rebuild" CLI 命令。

接下来的操作

- （可选）要查看恢复状态，请参阅 检查恢复作业状态，第 105 页

- 要重新启动节点，请参阅 重新启动节点 ，第 104 页

将节点或群集恢复到上次已知的良好配置

按照此程序将节点或群集恢复到上次已知的良好配置。

开始之前

- 确保恢复文件包含主机名、IP 地址、DNS 配置，以及在备份文件中配置的部署类型。
- 确保服务器上安装的 Cisco Unified Communications Manager 版本与您要恢复的备份文件的版本匹配。
- 确保仅将此程序用于将节点恢复到上次已知的良好配置。

过程

步骤 1 从灾难恢复系统中，选择**恢复** > **恢复向导**。

步骤 2 在**选择备份设备**区域，选择要恢复的适当的备份设备。

步骤 3 单击**下一步**。

步骤 4 在**恢复向导第 2 步**窗口中，选择要恢复的备份文件。

注释 备份文件名会指示系统创建备份文件的日期和时间。

步骤 5 单击**下一步**。

步骤 6 在**恢复向导第 3 步**窗口中，单击**下一步**。

步骤 7 当系统提示选择恢复节点时，选择适当的节点。
数据会恢复到所选的节点上。

步骤 8 重新启动群集中的所有节点。重新启动第一个 Cisco Unified Communications Manager 节点，然后再重启后续 Cisco Unified Communications Manager 节点。如果群集还有 Cisco IM and Presence 节点，则重新启动第一个 Cisco IM and Presence 节点，然后再重启后续 IM and Presence 节点。请参阅“下一步操作”部分，了解详细信息。

重新启动节点

恢复数据之后，您必须重新启动节点。

如果要恢复发布方节点（第一个节点），您必须先重新启动发布方节点。仅在发布方节点已重新启动并成功运行恢复的软件版本后，才重新启动订阅方节点。

注意 此程序将导致系统重新启动，并且临时停止服务。

在需要重新启动的群集中的每个节点上执行此程序。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**设置** > **版本**。

步骤 2 要重新启动节点，单击**重新启动**。

步骤 3 群集重启后，将会自动设置复制。通过使用 **utils dbreplication runtimestate** CLI 命令，检查所有节点上的“复制状态”值。每个节点上的值应等于2。请参阅下方的“相关主题”部分，查找有关CLI命令的信息。
如果复制未正确设置，使用如《*Cisco Unified Communications* 解决方案的命令行界面参考指南》中所述的 **utils dbreplication reset** CLI 命令。请参阅下方的“相关主题”部分，查找有关 CLI 命令的信息。

注释 后续节点重新启动后，在后续节点上的数据库复制可能需要几个小时才能完成，具体视群集的大小而定。

接下来的操作

（可选）要查看恢复状态，请参阅 检查恢复作业状态，第 105 页。

相关主题

Cisco Unified Communications Manager(CallManager)命令参考

检查恢复作业状态

按照此程序检查恢复作业状态。

过程

步骤 1 从灾难恢复系统中，选择**恢复** > **当前状态**。

步骤 2 在**恢复状态**窗口中，单击日志文件名链接以查看恢复状态。

查看恢复历史记录

如要查看恢复历史记录，请执行以下步骤。

过程

步骤 1 从灾难恢复系统中，选择**恢复** > **历史记录**。

步骤 2 从**恢复历史记录**窗口中，您可以查看已执行的恢复，包括文件名、备份设备、完成日期、结果、版本、已恢复的功能，以及失败的功能。
恢复历史记录窗口只显示最近 20 次恢复作业。

数据验证

跟踪文件

在故障排除或收集日志期间使用以下跟踪文件位置。

Master Agent、GUI、每个 Local Agent 和 JSch 库的跟踪文件将写入到以下位置：

- 对于 Master Agent，查找位于 platform/drf/trace/drfMA0* 的跟踪文件
- 对于每个 Local Agent，查找位于 platform/drf/trace/drfLA0* 的跟踪文件
- 对于 GUI，查找位于 platform/drf/trace/drfConfLib0* 的跟踪文件
- 对于 JSch，查找位于 platform/drf/trace/drfJSch* 的跟踪文件

有关详细信息，请参阅位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html 的《*Cisco Unified Communications* 解决方案的命令行界面参考指南》。

命令行界面

灾难恢复系统还提供对备份和恢复功能子集的命令行访问，如下表中所示。有关这些命令和使用命令行界面的详细信息，请参阅《*Cisco Unified Communications* 解决方案的命令行界面参考指南》，位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html。

表 *4*：灾难恢复系统命令行界面

命令	说明
utils disaster_recovery estimate_tar_size	显示来自 SFTP /本地设备的备份 tar 的估计大小，需要一个功能列表的参数
utils disaster_recovery backup	通过使用在灾难恢复系统界面中配置的功能开始手动备份

命令	说明
utils disaster_recovery jschLogs	启用或禁用 JSch 库日志记录
utils disaster_recovery restore	开始恢复，需要备份位置、文件名、功能以及要恢复的节点的参数
utils disaster_recovery status	显示正在进行的备份或恢复作业的状态
utils disaster_recovery show_backupfiles	显示现有备份文件
utils disaster_recovery cancel_backup	取消正在进行的备份作业
utils disaster_recovery show_registration	显示当前配置的注册
utils disaster_recovery device add	添加网络设备
utils disaster_recovery device delete	删除设备
utils disaster_recovery device list	列出所有设备
utils disaster_recovery schedule add	添加计划
utils disaster_recovery schedule delete	删除计划
utils disaster_recovery schedule disable	禁用计划
utils disaster_recovery schedule enable	启用计划
utils disaster_recovery schedule list	列出所有计划
utils disaster_recovery backup	通过使用在灾难恢复系统界面中配置的功能开始手动备份。
utils disaster_recovery restore	开始恢复，需要备份位置、文件名、功能以及要恢复的节点的参数。
utils disaster_recovery status	显示正在进行的备份或恢复作业的状态。
utils disaster_recovery show_backupfiles	显示现有备份文件。

命令	说明
utils disaster_recovery cancel_backup	取消正在进行的备份作业。
utils disaster_recovery show_registration	显示当前配置的注册。

警报和消息

警报和消息

灾难恢复系统会发出备份或恢复程序期间可能发生的各种错误的警报。下表提供了 Cisco 灾难恢复系统警报的列表。

表 *5*：灾难恢复系统警报和消息

警报名称	说明	说明
DRFBackupDeviceError	DRF 备份过程在访问设备时出现问题。	DRS 备份过程在访问设备时遇到问题。
DRFBackupFailure	Cisco DRF 备份过程失败。	DRS 备份过程遇到错误。
DRFBackupInProgress	其他备份仍在运行时，新备份无法启动	DRS 在其他备份仍在运行时无法启动新备份。
DRFInternalProcessFailure	DRF 内部过程遇到错误。	DRS 内部过程遇到错误。
DRFLA2MAFailure	DRF Local Agent 无法连接到 Master Agent。	DRS Local Agent 无法连接到 Master Agent。
DRFLocalAgentStartFailure	DRF Local Agent 未启动。	DRS Local Agent 可能已关闭。
DRFMA2LAFailure	DRF Master Agent 没有连接到 Local Agent。	DRS Master Agent 无法连接到 Local Agent。
DRFMABackupComponentFailure	DRF 无法备份至少一个组件。	DRS 请求组件备份其数据；但备份过程中发生错误，该组件没有得到备份。

警报名称	说明	说明
DRFMABackupNodeDisconnect	进行备份的节点在完全备份之前即从 Master Agent 断开连接。	DRS Master Agent 在 Cisco Unified Communications Manager 节点上运行备份操作时，节点在备份操作完成之前断开连接。
DRFMARestoreComponentFailure	DRF 无法恢复至少一个组件。	DRS 请求组件恢复其数据；但恢复过程中发生错误，该组件没有得到恢复。
DRFMARestoreNodeDisconnect	进行恢复的节点在完全恢复之前即从 Master Agent 断开连接。	DRS Master Agent 在 Cisco Unified Communications Manager 节点上运行恢复操作时，节点在恢复操作完成之前断开连接。
DRFMasterAgentStartFailure	DRF Master Agent 未启动。	DRS Master Agent 可能出现故障。
DRFNoRegisteredComponent	没有可用的注册组件，因此备份失败。	由于没有可用的注册组件，因此 DRS 备份失败。
DRFNoRegisteredFeature	没有为备份选择任何功能。	没有为备份选择任何功能。
DRFRestoreDeviceError	DRF 恢复过程在访问设备时出现问题。	DRS恢复过程无法从设备读取。
DRFRestoreFailure	DRF 恢复过程失败。	DRS 恢复过程遇到错误。
DRFSftpFailure	DRF SFTP 操作有错误。	DRS SFTP 操作中存在错误。
DRFSecurityViolation	DRF 系统检测到可导致安全违规的恶意模式。	DRF 网络消息包含可导致安全违规的恶意模式，如代码注入或目录遍历。DRF 网络消息已被阻止。
DRFTruststoreMissing	节点上缺少 IPsec 信任库。	节点上缺少 IPsec 信任库。DRF Local Agent 无法连接到 Master Agent。
DRFUnknownClient	公共网络上的 DRF Master Agent 收到来自群集外部未知服务器的客户端连接请求。该请求已被拒绝。	公共网络上的 DRF Master Agent 收到来自群集外部未知服务器的客户端连接请求。该请求已被拒绝。
DRFBackupCompleted	DRF 备份成功完成。	DRF 备份成功完成。

警报名称	说明	说明
DRFRestoreCompleted	DRF 恢复成功完成。	DRF 恢复成功完成。
DRFNoBackupTaken	DRF 找不到当前系统的有效备份。	DRF 在升级/迁移或全新安装后找不到当前系统的有效备份。
DRFComponentRegistered	DRF 成功注册所请求的组件。	DRF 成功注册所请求的组件。
DRFRegistrationFailure	DRF 注册操作失败。	DRF 对组件的注册操作由于某种内部错误而失败。
DRFComponentDeRegistered	DRF 成功注销所请求的组件。	DRF 成功注销所请求的组件。
DRFDeRegistrationFailure	DRF 对组件的注销请求失败。	DRF 对组件的注销请求失败。
DRFFailure	DRF 备份或恢复过程失败。	DRF 备份或恢复过程遇到错误。
DRFRestoreInternalError	DRF 恢复操作遇到错误。恢复已内部取消。	DRF 恢复操作遇到错误。恢复已内部取消。
DRFLogDirAccessFailure	DRF 无法访问日志目录。	DRF 无法访问日志目录。
DRFDeRegisteredServer	DRF 自动注销服务器的所有组件。	服务器可能已从 Unified Communications Manager 群集断开连接。
DRFSchedulerDisabled	DRF 计划程序被禁用，因为没有配置的功能可用于备份。	DRF 计划程序被禁用，因为没有配置的功能可用于备份
DRFSchedulerUpdated	DRF 计划的备份配置由于功能注销而自动更新。	DRF 计划的备份配置由于功能注销而自动更新

恢复相互作用和限制

恢复限制

以下限制适用于使用灾难恢复系统恢复 Cisco Unified Communications Manager 或 IM and Presence 服务

表 6: 恢复限制

限制	说明
出口受限	来自受限版本的 DRS 备份只能恢复到受限版本，而来自不受限版本的备份只能恢复到不受限版本。请注意，如果您升级到美国出口不受限版本的 Cisco Unified Communications Manager，日后您将无法升级到该软件的美国出口受限版本，或无法执行受限版本的全新安装
平台迁移	您不能使用灾难恢复系统在平台之间（例如，从 Windows 到 Linux 或从 Linux 到 Windows）迁移数据。恢复必须运行在与备份相同的产品版本上。有关从基于 Windows 的平台将数据迁移到基于 Linux 的平台的信息，请参阅数据迁移助手用户手册。
硬件更换和迁移	当您执行 DRS 恢复将数据迁移到新服务器时，必须为新服务器分配与旧服务器所使用的完全相同的 IP 地址和主机名。此外，如果进行备份时配置了 DNS，则在执行恢复之前，必须进行相同的 DNS 配置。 有关更换服务器的详细信息，请参阅《为 *Cisco Unified Communications Manager* 更换单个服务器或群集指南》。 此外，更换硬件后，您必须运行证书信任列表(CTL)客户端。如果不恢复后续节点（订阅方）服务器，您必须运行 CTL 客户端。在其他情况下，DRS 会备份您需要的证书。有关详细信息，请参阅《*Cisco Unified Communications Manager* 安全指南》中的“安装 CTL 客户端”和“配置 CTL 客户端”程序。
跨群集分机移动	备份时登录到远程群集的跨群集分机移动用户，恢复后应会保持登录。

注释 成功恢复 Cisco Unified Communications 服务器组件后，向 Cisco Smart Software Manager 或 Cisco Smart Software Manager 卫星注册 Cisco Unified Communications Manager。如果执行备份之前产品已注册，那么重新注册产品以更新许可证信息。

有关如何向 Cisco Smart Software Manager 或 Cisco Smart Software Manager 卫星注册产品的详细信息，请参阅《*Cisco Unified Communications Manager* 系统配置指南》，版本 12.0(1)，位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html。

故障排除

DRS 恢复到较小的虚拟机失败

问题

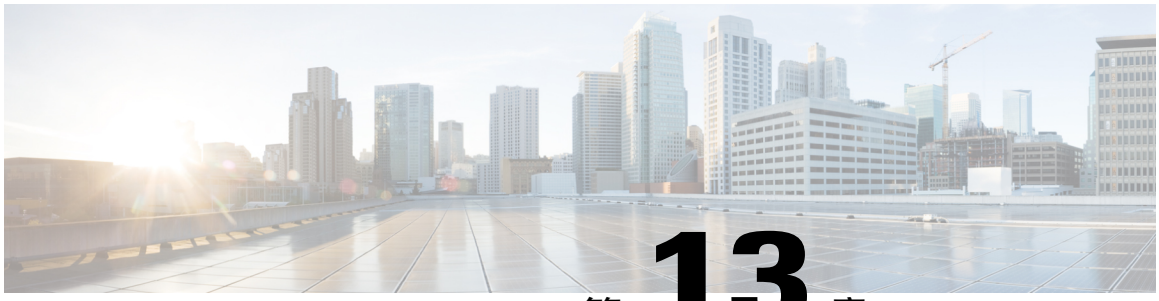
如果您将 IM and Presence 服务节点恢复到磁盘较小的 VM 上，数据库恢复可能会失败。

原因

当从较大的磁盘迁移到较小的磁盘时会发生此故障。

解决办法

部署 VM 以从具有 2 个虚拟磁盘的 OVA 模板恢复。



第 13 章

管理企业参数

企业参数概述

企业参数提供适用于跨整个群集中所有设备和服务的默认设置。例如，您的系统使用企业参数来设置其设备默认值的初始值。

您无法添加或删除企业参数，但可以更新现有的企业参数。配置窗口会将企业参数列于类别下；例如，CCMAdmin 参数、CCMUser 参数和 CDR 参数。

您可以在**企业参数配置**窗口中查看企业参数的详细的说明。

注意 许多企业参数并不需要更改。但是，除非您完全了解要更改的功能，或者思科技术支持中心(TAC)建议您更改，否则请勿更改企业参数。

查看企业参数信息

通过**企业参数配置**窗口中的嵌入内容，访问有关企业参数的信息。

过程

步骤 1 从“Cisco Unified CM 管理”中，选择**系统** > **企业参数**。

步骤 2 请执行以下任务之一：

- 要查看特定企业参数的说明，请单击该参数的名称。
- 要查看所有企业参数的说明，请单击 **?**。

更新企业参数

使用此程序打开**企业参数配置**窗口并配置系统级设置。

注意 许多企业参数并不需要更改。但是，除非您完全了解要更改的功能，或者思科技术支持中心(TAC)建议您更改，否则请勿更改企业参数。

过程

步骤 1 从“Cisco Unified CM 管理”中，选择**系统** > **企业参数**。

步骤 2 为您想要更改的企业参数选择所需的值。

步骤 3 单击**保存**。

接下来的操作

将配置应用到设备，第 114 页

将配置应用到设备

使用此程序以利用您配置的设置更新群集中所有受影响的设备。

开始之前

更新企业参数，第 114 页

过程

步骤 1 从“Cisco Unified CM 管理”中，选择**系统** > **企业参数**。

步骤 2 检验您的更改，然后单击**保存**。

步骤 3 选择下列选项之一：

- 如果您希望系统确定要重新启动哪些设备，请单击**应用配置**。在某些情况下，设备可能无需重新启动。正在进行的呼叫可能会掉线，但已接通的呼叫将被保留，除非设备池包含 SIP 干线。
- 如果想要重新启动群集中的所有设备，请单击**重置**。我们建议您在非高峰时段执行此步骤。

步骤 4 阅读确认对话框后，单击**确定**。

恢复默认企业参数

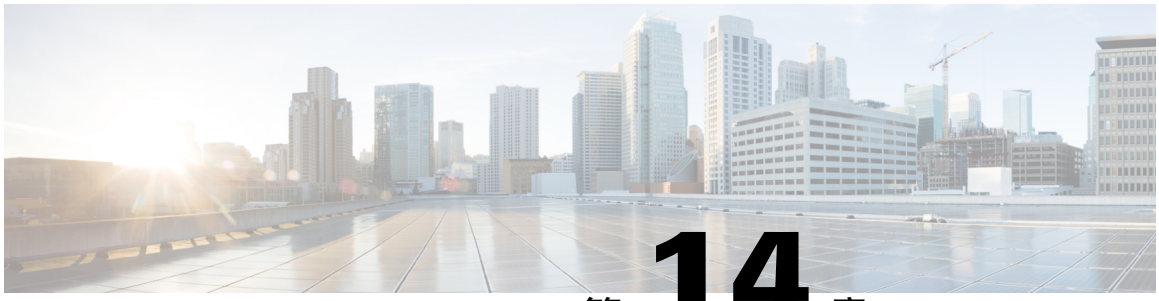
如果您要将企业参数重置为默认设置，请使用此程序。某些企业参数包含建议的值，如配置窗口的列中所示；此程序使用这些值作为默认设置。

过程

步骤 1 从“Cisco Unified CM 管理”中，选择**系统** > **企业参数**。

步骤 2 单击**设置为默认值**。

步骤 3 阅读确认提示后，单击**确定**。



第 14 章

管理服务器

管理服务器概述

本章介绍如何管理 Cisco Unified Communications Manager 节点的属性、查看 Presence 服务器状态，以及为 Unified Communications Manager 服务器配置主机名。

从群集中删除节点

如果您需要安全地将 IM and Presence 服务节点从其 Presence 冗余组中删除，请按照以下过程执行操作。

注意 删除节点会对 Presence 冗余组中其余节点上的用户造成服务中断。只有在维护期间才能执行此过程。

过程

步骤 1 在 **Cisco Unified CM 管理 > 系统 > Presence 冗余组**页面上，禁用高可用性（如果已启用）。

步骤 2 在 **Cisco Unified CM 管理 > 用户管理 > 分配 Presence 用户**页面上，取消分配所有用户，或者将所有用户移离您要删除的节点。

步骤 3 要将节点从其 Presence 冗余组中删除，请从该 Presence 冗余组的“Presence 冗余组配置”页面上的“Presence 服务器”下拉列表中选择**未选定**。当出现警告对话框，表明由于取消分配该节点而将要重新启动 Presence 冗余组时，选择**确定**。

步骤 4 从 **Cisco Unified CM 管理 > 系统 > 服务器**页面删除取消分配的节点。当出现警告对话框，表明无法撤消此操作时，选择**确定**。

步骤 5 为您已取消分配的节点关闭主机 VM 或服务器。

将已删除的服务器重新添加到群集

如果从 Cisco Unified Communications Manager 管理中删除了某个后续节点（订阅方），又想将其重新添加到群集中，请执行以下步骤。

过程

步骤 1 在 Cisco Unified Communications Manager 管理中，选择**系统** > **服务器**来添加服务器。

步骤 2 将后续节点添加到 Cisco Unified Communications Manager 管理后，使用软件包中思科提供的磁盘在服务器上执行安装。

提示 例如，如果您有 8.5(1) 版的磁盘，则在该节点上安装 8.5(1)。如果您有兼容版 6.1(3) 的磁盘，则使用该磁盘在后续节点上安装 Cisco Unified CM；在安装期间，当安装显示选项时，选择“在安装期间升级”(Upgrade During Install) 选项。

确保您在后续节点上安装的版本与群集中第一个节点（发布方）上运行的版本相匹配。

如果群集中的第一个节点运行 Cisco Unified Communications Manager 8.5(1) 版和服务更新（或工程专用），则在安装显示安装选项时，必须选择“在安装期间升级”(Upgrade During Install) 选项；在选择此选项前，确保您可以访问 DVD 或远程服务器上的服务更新（或工程专用）图像。有关如何执行安装的详细信息，请参阅支持您的 Cisco Unified Communications Manager 版本的安装文档。

步骤 3 安装 Cisco Unified CM 后，按照支持您的 Cisco Unified CM 版本的安装文档配置后续节点。

步骤 4 访问 Cisco Unified Reporting、RTMT 或 CLI，以确认现有节点之间发生了数据库复制；如有必要，可以修复节点之间的数据库复制。

安装前将节点添加到群集

在安装节点之前，使用 Cisco Unified Communications Manager 管理将新节点添加到群集。添加节点时您选择的服务器类型必须匹配您安装的服务器类型。

安装新节点之前，您必须使用 Cisco Unified Communications Manager 管理在第一个节点中配置新节点。要在群集上安装节点，请参阅《*Cisco Unified Communications Manager* 安装指南》。

对于 Cisco Unified Communications Manager 视频/语音服务器，您在 Cisco Unified Communications Manager 软件初始安装期间添加的第一台服务器指定为发布方节点。所有后续服务器安装或添加都指定为订阅方节点。您添加到群集的第一个 Cisco Unified Communications Manager IM and Presence 节点指定为 IM and Presence 服务数据库发布方节点。

注释 您无法使用 Cisco Unified Communications Manager 管理在服务器添加后更改服务器类型。您必须删除现有的服务器实例，然后再次添加新服务器并选择正确的服务器类型设置。

过程

步骤 1 选择**系统** > **服务器**。
此时将显示**查找并列出服务器**窗口。

步骤 2 单击**新增**。
此时将显示**服务器配置 - 添加服务器**窗口。

步骤 3 从**服务器类型**下拉列表框中，选择您要添加的服务器类型，然后单击**下一步**。

- CUCM 视频/语音
- CUCM IM and Presence

步骤 4 在**服务器配置**窗口中，输入相应的服务器设置。
有关服务器配置字段说明，请参阅服务器设置。

步骤 5 单击**保存**。

查看 Presence 服务器状态

使用 Cisco Unified CM 管理查看 IM and Presence 服务节点的关键服务的状态以及自我诊断测试结果。

过程

步骤 1 选择**系统** > **服务器**。

此时将显示**查找并列出服务器**窗口。

步骤 2 选择服务器搜索参数，然后单击**查找**。
屏幕上将显示相匹配的记录。

步骤 3 选择**查找并列出服务器**窗口中列出的 IM and Presence 服务器。
此时将显示**服务器配置**窗口。

步骤 4 单击**服务器配置**窗口的“IM and Presence 服务器信息”部分中的“Presence 服务器状态”链接。
此时将显示服务器的**节点详细信息**窗口。

主机名配置

下表列出您可以为 Unified Communications Manager 服务器配置主机名的地方，允许主机名使用的字符数量以及建议主机名使用的第一个和最后一个字符。请注意，如果您没有正确配置主机名，Unified Communications Manager 中的部分组件，例如操作系统、数据库、安装等组件可能无法按预期工作。

注意 为下表所列的任何位置更改主机名或 IP 地址之前，请参阅文档《更改 *Cisco Unified Communications Manager* 的 *IP* 地址和主机名》。在配置主机名或 IP 地址后未能正确更新这些信息可能导致 Unified Communications Manager 出现问题。

表 7：*Cisco Unified Communications Manager* 中的主机名配置

主机名位置	允许的配置	允许的字符数	建议主机名使用的第一个字符	建议主机名使用的最后一个字符
主机名/IP 地址字段 **Cisco Unified Communications Manager 管理中的系统 > 服务器**	您可以添加或更改群集中服务器的主机名	2-63	字母	字母数字
主机名字段 Cisco Unified Communications Manager 安装向导	您可以添加群集中服务器的主机名	1-63	字母	字母数字
主机名字段 **Cisco Unified Communications 操作系统中的设置 > IP > 以太网**	您可以更改，但不能添加群集中服务器的主机名。	1-63	字母	字母数字

主机名位置	允许的配置	允许的字符数	建议主机名使用的第一个字符	建议主机名使用的最后一个字符
设置网络主机名 主机名 命令行界面	您可以更改，但不能添加群集中服务器的主机名。	1-63	字母	字母数字

提示 主机名必须遵循ARPANET主机名的规则。在主机名的第一个和最后一个字符之间，您可以输入字母数字字符和连字符。

在任何位置配置主机名之前，请回顾以下信息：

- “服务器配置”窗口中的“主机名/IP字段”支持设备到服务器、应用程序到服务器和服务器到服务器通信，允许您输入点分十进制格式的 IPv4 地址或主机名。
  您在安装Unified Communications Manager发布方节点后，发布方的主机名将自动显示在此字段中。您在安装 Unified Communications Manager 订户节点之前，在 Unified Communications Manager 发布方节点上的此字段中输入订户节点的 IP 地址或主机名。

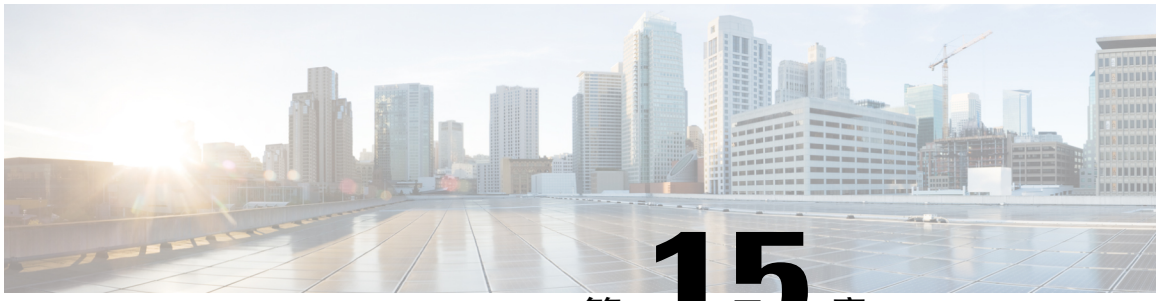
  在此字段中，只有 Unified Communications Manager 可以访问 DNS 服务器以将主机名解析为 IP 地址时，才可配置主机名，确保您在 DNS 服务器上配置 Cisco Unified Communications Manager 名称和地址信息。

提示 除了在 DNS 服务器上配置 Unified Communications Manager 信息外，您可以在 Cisco Unified Communications Manager 安装期间输入 DNS 信息。

- 在安装Unified Communications Manager发布方节点期间，您输入发布方节点的主机名（必填）和 IP 地址，以配置网络信息，假如您想使用静态网络。
  安装 Unified Communications Manager 订户节点期间，您输入 Unified Communications Manager 发布方节点的主机名和 IP 地址，以便 Unified Communications Manager 可以验证网络连通性和发布方-订户验证。此外，您必须输入订户节点的主机名和 IP 地址。当 Unified Communications Manager 安装提示您输入订户服务器的主机名时，输入显示在 Cisco Unified Communications Manager管理中的“服务器配置”窗口中的值，假如您在“主机名/IP地址”字段配置订户服务器的主机名。

第 V 部分

管理安全性



第 15 章

管理 SAML 单点登录

SAML 单点登录概述

使用 SAML 单点登录 (SSO) 登录到其中一个应用程序后，访问一组定义的 Cisco 应用程序。SAML 描述了受信任的业务合作伙伴之间安全相关信息的交换。它是服务提供程序（例如 Cisco Unified Communications Manager）用来验证用户的一种验证协议。利用 SAML，安全验证信息可在身份提供程序 (IdP) 与服务提供程序之间交换。该功能提供安全机制来跨各种应用程序使用通用凭证和相关信息。

SAML SSO 在部署过程中通过在 IdP 和服务提供程序之间交换元数据和证书建立信任圈 (CoT)。服务提供程序信任 IdP 的用户信息，提供对各种服务或应用的访问权限。

客户端根据 IdP 进行验证，IdP 则向客户端授予断言。客户端将断言提供给服务提供程序。由于建立了 CoT，服务提供程序信任断言，并授予访问客户端的权限。

Cisco Jabber on iOS 基于证书的 SSO 验证的选择加入控制

此版本的 Cisco Unified Communications Manager 引入了选择加入配置选项，以使用身份提供程序 (IdP) 控制 Cisco Jabber on iOS SSO 登录行为。使用此选项以允许 Cisco Jabber 在受控的移动设备管理 (MDM) 部署中使用 IdP 执行基于证书的验证。

您可以在 Cisco Unified Communications Manager 中通过 **iOS 的 SSO 登录行为** (SSO Login Behavior for iOS) 企业参数配置选择加入控制。

注释 在更改此参数的默认值之前，请参阅位于 http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/tsd-products-support-series-home.html 的 Cisco Jabber 功能支持和文档，以确保 Cisco Jabber on iOS 支持 SSO 登录行为和基于证书的验证。

要启用此功能，请参阅 为 Cisco Jabber on iOS 配置 SSO 登录行为，第 128 页 程序。

SAML 单点登录前提条件

- 为 Cisco Unified Communications Manager 群集配置了 DNS
- 一台身份提供程序 (IdP) 服务器
- 一台受 IdP 服务器信任且受您的系统支持的 LDAP 服务器

以下使用 SAML 2.0 的 Idp 针对 SAML SSO 功能进行了测试：

- OpenAM 10.0.1
- Microsoft® Active Directory® Federation Services 2.0 (AD FS 2.0)
- PingFederate® 6.10.0.4
- F5 BIP-IP 11.6.0

这些第三方应用程序必须满足以下配置要求：

- 必须在 IdP 上配置必需属性 “uid”。此属性必须与 Cisco Unified Communications Manager 中用于 LDAP 同步用户 ID 匹配。

  注释 Cisco Unified Communications Manager 目前只支持 sAMAccountName 选项作为用户 ID 设置的 LDAP 属性。

  有关配置必需属性映射的详细信息，请参阅 IdP 产品文档。

- 必须同步所有参与 SAML SSO 的实体的时钟。有关同步时钟的信息，请参阅《*Cisco Unified Communications Manager* 系统配置指南》中的 “NTP 设置”，该文档位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html。

管理 SAML 单点登录

启用 SAML 单点登录

注释 直到验证同步代理测试成功后，才能启用 SAML SSO。

开始之前

- 确保最终用户数据与 Unified Communications Manager 数据库同步。有关详细信息，请参阅《*Cisco Unified Communications Manager* 系统配置指南》，位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html。
- 验证 Cisco Unified CM IM and Presence 服务 Cisco 同步代理服务是否已成功完成数据同步。通过选择 **Cisco Unified CM IM and Presence 管理** > **诊断** > **系统故障排除程序**，检查此测试的状态。如果数据同步已成功完成，“验证同步代理是否已同步相关数据（例如设备、用户、许可信息）”测试显示“测试通过”结果。
- 确保至少一个 LDAP 同步用户添加到“标准 CCM 超级用户”组以允许访问“Cisco Unified CM 管理”。有关详细信息，请参阅《*Cisco Unified Communications Manager* 系统配置指南》，位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html。
- 要配置 IdP 与服务器之间的信任关系，必须从 IdP 获取信任元数据文件，并将该文件导入到所有服务器中。

过程

步骤 1 从“Cisco Unified CM 管理”中，选择**系统** > **SAML 单点登录**。

步骤 2 单击**启用 SAML SSO**。

步骤 3 看到通知您所有服务器连接都将重新启动的警告消息后，单击**继续**。

步骤 4 单击**浏览**查找并上载 IdP 元数据文件。

步骤 5 单击**导入 IdP 元数据**。

步骤 6 单击**下一步**。

步骤 7 单击**下载信任元数据文件集**将服务器元数据下载到系统。

步骤 8 将服务器元数据上载到 IdP 服务器。

步骤 9 单击**下一步**继续操作。

步骤 10 从有效管理员 ID 列表中选择具有管理权限的 LDAP 同步用户。

步骤 11 单击**运行测试**。

步骤 12 输入有效的用户名和密码。

步骤 13 看到成功消息之后，关闭浏览器窗口。

步骤 14 单击**完成**，等待 1 到 2 分钟，让 Web 应用程序重新启动。

为 Cisco Jabber on iOS 配置 SSO 登录行为

过程

步骤 1 从“Cisco Unified CM 管理”中，选择**系统** > **企业参数**。

步骤 2 要配置选择加入控制，在 SSO 配置部分，为 **iOS 的 SSO 登录行为** (SSO Login Behavior for iOS) 参数选择**使用本机浏览器**选项：

注释 **iOS 的 SSO 登录行为** (SSO Login Behavior for iOS) 参数包括以下选项：

- **使用嵌入式浏览器** — 如果启用此选项，Cisco Jabber 会使用嵌入式浏览器进行 SSO 验证。使用此选项可允许版本 9 之前的 iOS 设备使用 SSO 而无需交叉启动进入本机 Apple Safari 浏览器。默认情况下会启用此选项。
- **使用本机浏览器** — 如果启用此选项，Cisco Jabber 会在 iOS 设备上使用 Apple Safari 框架，在 MDM 部署中使用身份提供程序 (IdP) 执行基于证书的验证。

  注释 除了在受控的 MDM 部署中，不建议配置此选项，因为使用本机浏览器不如使用嵌入式浏览器安全。

步骤 3 单击**保存**。

升级后在 WebDialer 上启用 SAML 单点登录

执行这些任务以在升级后在 Cisco WebDialer 上重新激活 SAML 单点登录。如果在启用 SAML 单点登录之前 Cisco WebDialer 已激活，则默认情况下 SAML 单点登录未在 Cisco WebDialer 上启用。

过程

	命令或操作	目的
步骤 1	禁用 Cisco WebDialer 服务，第 129 页	如果 Cisco WebDialer Web 服务已激活，请将其停用。
步骤 2	禁用 SAML 单点登录，第 129 页	如果 SAML 单点登录已启用，请将其禁用。
步骤 3	激活 Cisco WebDialer 服务，第 130 页	
步骤 4	启用 SAML 单点登录，第 127 页	

禁用 Cisco WebDialer 服务

如果 Cisco WebDialer Web 服务已激活，请将其停用。

过程

步骤 1 从 Cisco Unified 功能配置中，选择**工具** > **服务启动**。

步骤 2 从**服务器**下拉列表中，选择列出的 Cisco Unified Communications Manager 服务器。

步骤 3 从 **CTI 服务**中，取消选中 **Cisco WebDialer Web 服务**复选框。

步骤 4 单击**保存**。

接下来的操作

禁用 SAML 单点登录，第 129 页

禁用 SAML 单点登录

如果 SAML 单点登录已启用，请将其禁用。

开始之前

禁用 Cisco WebDialer 服务，第 129 页

过程

从 CLI，运行命令 **utils sso disable**。

接下来的操作

激活 Cisco WebDialer 服务 ， 第 130 页

激活 Cisco WebDialer 服务

开始之前

禁用 SAML 单点登录 ， 第 129 页

过程

步骤 1 从 Cisco Unified 功能配置中，选择**工具** > **服务启动**。

步骤 2 从**服务器**下拉列表中，选择列出的 Cisco Unified Communications Manager 服务器。

步骤 3 从 **CTI 服务**中，选中 **Cisco WebDialer Web 服务**复选框。

步骤 4 单击**保存**。

步骤 5 从 Cisco Unified 功能配置中，选择**工具** > **控制中心 - 功能服务**，以确认 CTI Manager 服务为活动状态且处于启动模式。
要使 WebDialer 正常运行，CTI Manager 服务必须为活动状态且处于启动模式。

接下来的操作

启用 SAML 单点登录 ， 第 127 页

访问恢复 URL

使用恢复 URL 以绕过 SAML 单点登录并登录到“Cisco Unified Communications Manager 管理”和“Cisco Unified CM IM and Presence 服务”界面进行故障排除。例如，在更改服务器的域或主机名之前启用恢复 URL。登录恢复 URL 便于更新服务器元数据。

开始之前

- 只有具有管理权限的应用程序用户才能访问恢复 URL。
- 如果启用 SAML SSO，默认情况下启用恢复 URL。您可以从 CLI 启用或禁用恢复 URL。有关用于启用和禁用恢复 URL 的 CLI 命令的详细信息，请参阅《*Cisco Unified Communications* 解决方案的命令行界面指南》。

过程

在浏览器中，输入 `https://hostname:8443/ssosp/local/login`。

在域或主机名更改之后更新服务器元数据

域或主机名更改之后，SAML 单点登录将不起作用，直到您执行此程序。

注释 如果即使在执行此程序之后，仍然无法登录 **SAML 单点登录**窗口，请清除浏览器缓存，然后再次尝试登录。

开始之前

如果禁用恢复URL，则它不会出现以让您绕过单点登录链接。要启用恢复URL，请登录CLI并执行以下命令：**utils sso recovery-url enable**。

过程

步骤 1 在您的 Web 浏览器的地址栏中，输入以下 URL：
`https://<Unified CM-server-name>`

其中 `<Unified CM-server-name>` 是服务器的主机名或 IP 地址。

步骤 2 单击**恢复 URL 以绕过单点登录 (SSO)**。

步骤 3 输入具有管理员角色的应用程序用户的凭证，然后单击**登录**。

步骤 4 从“Cisco Unified CM 管理”中，选择**系统** > **SAML 单点登录**。

步骤 5 单击**导出元数据**，下载服务器元数据。

步骤 6 将服务器元数据文件上载到 IdP。

步骤 7 单击**运行测试**。

步骤 8 输入有效的用户 ID 和密码。

步骤 9 看到此成功消息之后，关闭浏览器窗口。

手动配置服务器元数据

要在身份提供程序中为多个 UC 应用程序配置一个连接，您必须手动配置服务器元数据，同时配置身份提供程序与服务提供程序之间的信任圈。有关配置信任圈的详细信息，请参阅 IdP 产品文档。

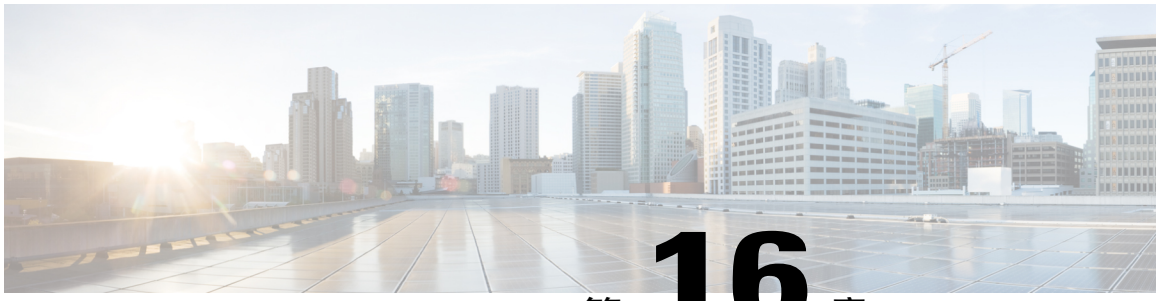
一般 URL 语法如下：

`https://<SP FQDN>:8443/ssosp/saml/SSO/alias/<SP FQDN>`

过程

要手动配置服务器元数据，请使用 Assertion Customer Service (ACS) URL。

示例：
ACS URL 示例：<md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://cucm.ucsso.cisco.com:8443/ssosp/saml/SSO/alias/cucm.ucsso.cisco.com"
index="0"/>



第 16 章

管理证书

证书概述

您的系统使用自签证书和第三方签名证书。证书在您系统中的设备之间使用，以安全地验证设备、加密数据，并对数据进行散列，以确保其从源到目的地的完整性。证书允许安全传输带宽、通信以及操作。

证书最重要的部分在于您知道并定义您的数据如何加密，并与诸如预期网站、电话或 FTP 服务器等实体共享。

当您的系统信任一个证书时，意味着您的系统上有一个预安装的证书，该证书声明它完全相信它与正确的目的地共享信息。否则，它会终止这些点之间的通信。

为了信任证书，必须已经与第三方证书颁发机构 (CA) 建立信任。

您的设备必须知道，它们可以首先信任 CA 和中间证书，然后才能信任由称为安全套接字层 (SSL) 握手的消息交换提供的服务器证书。

注释 支持基于 EC 的 Tomcat 证书。此新证书称为 tomcat-ECDSA。有关详细信息，请参阅在 *Cisco Unified Communications Manager* 上的 *IM and Presence* 服务配置和管理“IM and Presence 服务部分”的增强型 TLS 加密。

默认情况下，Tomcat 接口上的 EC 密码处于禁用状态。您可以使用 Cisco Unified Communications Manager 或 IM and Presence 服务上的 **HTTPS 密码**企业参数启用它们。如果您更改此参数，必须在所有节点上重新启动 Cisco Tomcat 服务。

有关基于 EC 的证书的详细信息，请参阅 Cisco Unified Communications Manager 和 IM and Presence 服务发行说明中的“对认证解决方案通用标准的 ECDSA 支持”。

第三方签名证书或证书链

上载为应用程序证书签名的证书颁发机构的证书颁发机构根证书。如果次级证书颁发机构为应用程序证书签名，您必须上载次级证书颁发机构的证书颁发机构根证书。您还可以上载所有证书颁发机构证书的 PKCS#7 格式的证书链。

您可以使用相同的**上载证书**对话框上载证书颁发机构根证书和应用程序证书。当上载证书颁发机构根证书或仅包含证书颁发机构证书的证书链时，选择格式为“证书类型-信任”的证书名称。当上载应用程序证书或包含应用程序证书和证书颁发机构证书的证书链时，选择仅包含证书类型的证书名称。

例如，当上载 Tomcat 证书颁发机构证书或证书颁发机构证书链时，选择 **tomcat-信任**；当上载 Tomcat 应用程序证书或包含一个应用程序证书和证书颁发机构证书的证书链时，选择 **tomcat** 或 **tomcat-ECDSA**。

当上载 CAPF 证书颁发机构根证书时，该证书会被复制到 CallManager-信任存储库中，因此您无需单独为 CallManager 上载证书颁发机构根证书。

注释 成功上载第三方证书颁发机构签名的证书，会删除最近生成的用于获取签名证书的 CSR，并且会覆盖现有证书，包括第三方签名证书（如果已上载）。

注释 系统会自动将“tomcat-信任”、“CallManager-信任”和“电话-SAST-信任”证书复制到群集中的每个节点。

注释 您可以将目录信任证书上载到 tomcat-信任，这是 DirSync 服务在安全模式下工作所必需的。

第三方证书颁发机构的证书

若要使用第三方证书颁发机构颁发的应用程序证书，您必须向证书颁发机构或 PKCS#7 证书链（可辨别编码规则 [DER]，其中包含应用程序证书和证书颁发机构的证书）获取签署的应用程序证书和证书颁发机构根证书。请检索有关向您的证书颁发机构获取这些证书的信息。证书颁发机构之间的流程各不相同。签名算法必须使用 RSA 加密。

Cisco Unified Communications 操作系统以隐私增强邮件 (PEM) 编码格式生成 CSR。系统接受 DER 和 PEM 编码格式的证书和 PEM 格式的 PKCS#7 证书链。对于除证书权限代理功能 (CAPF) 之外的所有证书类型，您必须获取和上载证书颁发机构根证书和每个节点上的应用程序证书。

对于 CAPF，获取并上载证书颁发机构根证书和仅在第一个节点上的应用程序证书。CAPF 和 Cisco Unified Communications ManagerCSR 中包含的扩展必须包括在向证书颁发机构申请应用程序证书的请求中。如果您的证书颁发机构不支持扩展请求机制，则您必须启用 X.509 扩展，如下所述：

- CAPF CSR 使用以下扩展：

```
X509v3 Extended Key Usage:
TLS Web Server Authentication, IPSec End System
X509v3 Key Usage:
Digital Signature, Certificate Sign
```

- 适用于 Tomcat 的 CSR 和 Tomcat-ECDSA 使用以下扩展：

注释 Tomcat 或 Tomcat-ECDSA 不要求密钥协议或 IPsec 终端系统密钥用法。

```
X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web
Client Authentication, IPSec End System X509v3 Key Usage: Digital
Signature, Key Encipherment, Data Encipherment, Key Agreement
```

- 适用于 IPsec 的 CSR 使用以下扩展：

```
 X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication, IPSec
End System
X509v3 Key Usage:
Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
```

- 适用于 Cisco Unified Communications Manager 的 CSR 使用以下扩展：

```
 X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Key Usage:
Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
```

注释 您可以为您的证书生成CSR并让具有SHA256签名的第三方证书颁发机构对其进行签名。然后，您可以将该签名证书上载回 Cisco Unified Communications Manager，允许 Tomcat 和其他证书支持 SHA256。

显示证书

查看属于您系统的证书和信任存储库的详细信息。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**安全** > **证书管理**。

步骤 2 使用**查找**控件过滤证书列表。

步骤 3 要查看证书或信任存储库的详细信息，请单击证书的 .PEM 或 .DER 文件名。

步骤 4 要返回到**证书列表**窗口，请单击**相关链接**列表中的**返回到查找/列出**，然后单击**转至**。

下载证书

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**安全** > **证书管理**。

步骤 2 指定搜索条件，然后单击**查找**。

步骤 3 选择证书或证书信任列表 (CTL) 的文件名称。

步骤 4 单击**下载**。

安装中间证书

要安装中间证书，您必须首先安装根证书，然后上载签名证书。仅当证书颁发机构在证书链中提供了签名证书及多个证书时，才需要执行此步骤。

提示 根证书名称为 .pem，这是上载根证书时生成的文件名。

过程

步骤 1 从 Cisco Unified 操作系统管理中，单击**安全** > **证书管理**。

步骤 2 单击**上载证书**。

步骤 3 从**证书目的**下拉列表中选择 **intelligenceCenter-srvr-trust** 以安装根证书。

步骤 4 单击**浏览**，导航至文件，然后单击**打开**。

步骤 5 单击**上传文件**。

步骤 6 从 Cisco Unified 操作系统管理中，选择**安全** > **证书管理**。

步骤 7 单击**上载证书**。

步骤 8 在**上载证书**弹出窗口中，从**证书名称**下拉列表中选择 **IntelligenceCenter-srvr**，然后输入根证书名称。

步骤 9 通过执行以下操作之一选择要上传的文件：

- 在**上载文件**文本框中，输入文件的路径。
- 单击**浏览**并导航至文件，然后单击**打开**。

步骤 10 单击**上传文件**。

步骤 11 安装客户证书后，使用 FQDN 访问 Cisco Unified Intelligence Center URL。如果使用 IP 地址访问 Cisco Unified Intelligence Center，即使成功安装了自定义证书，您也会看到消息“单击此处以继续”。

注释 上载 Tomcat 证书后，TFTP 服务应会被禁用，稍后会再激活。此外，TFTP 将继续提供过去缓存的自签名 tomcat 证书。

删除信任证书

信任的证书是您可以删除的唯一一种证书类型。您无法删除由您的系统生成的自签证书。

注意 删除证书可能会影响您的系统操作。如果证书是现有证书链的一部分，则删除该证书可能会破坏证书链。您可以通过**证书列表**窗口中相关证书的用户名和主题名称来检验此关系。您无法撤销此操作。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**安全** > **证书管理**。

步骤 2 使用“查找”控件过滤证书列表。

步骤 3 选择证书的文件名。

步骤 4 单击**删除**。

步骤 5 单击**确定**。

注释 如果您删除的证书属于“tomcat-信任”、“CallManager-信任”或“电话-SAST-信任”类型，证书将跨群集中的所有服务器删除。

重新生成证书

如果证书已过期，请重新生成证书。在下班时间按照此程序操作，因为您必须重新启动电话并重启服务。您只能重新生成在“Cisco Unified 操作系统管理”中被列为 “cert” 类型的证书。

注意 重新生成证书可能影响您的系统操作。重新生成证书会覆盖现有证书，包括第三方签名证书（如果已上载）。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**安全** > **证书管理**。

步骤 2 配置**生成新的自签名证书**窗口中的字段。请参阅联机帮助，了解有关字段及其配置选项的更多信息。

步骤 3 点击**生成 (Generate)**。

步骤 4 重新启动受重新生成的证书影响的所有服务。请参阅“相关主题”部分，了解有关证书名称及其说明的更多信息。

步骤 5 重新生成 CAPF 或 CallManager 证书之后，重新运行 CTL 客户端（如配置有）。

注释 重新生成 Tomcat 证书后，TFTP 服务应会被禁用，稍后会再激活。此外，TFTP 将继续提供过去缓存的自签名 tomcat 证书。

接下来的操作

重新生成证书后，您必须执行系统备份，以使最新备份包含重新生成的证书。如果您的备份不包含重新生成的证书，而您要执行系统恢复任务，则您必须手动解锁系统中的每部电话，以使电话可以注册。请参阅备份任务流程，第 88 页。

相关主题

证书名称和说明，第 139 页

证书名称和说明

下表说明您可以重新生成的系统安全证书，以及必须重新启动的相关服务。有关重新生成 TFTP 证书的信息，请参阅《*Cisco Unified Communications Manager* 安全指南》，位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

表 *8*：证书名称和说明

名称	说明	相关服务
tomcat tomcat-ECDSA	此自签名根证书在安装 HTTPS 节点期间生成。	Tomcat 和 TFTP
ipsec	此自签名根证书在安装 IPsec 与 MGCP 和 H.323 网关的连接期间生成。	Cisco 灾难恢复系统 (DRS) Local 和 Cisco DRF Master
CallManager	此自签名根证书在安装 Cisco Unified Communications Manager 时自动安装。此证书提供节点标识，包括节点名称和全局唯一标识符 (GUID)。	CallManager、CAPF 和 CTI
CAPF	在您完成 Cisco 客户端配置后，系统会将此根证书复制到您的节点或群集中的所有节点。	CallManager 和 CAPF
TVS	这是一种自签名根证书。	TVS

重新生成 OAuth 刷新登录的密钥

使用此程序以使用命令行界面重新生成加密密钥和签名密钥。仅当 Cisco Jabber 用来在 Cisco Unified Communications Manager 中进行 OAuth 验证的加密密钥或签名密钥已经被入侵时，才完成此任务。签名密钥是一种不对称密钥，基于 RSA，而加密秘钥是一种对称密钥。

注释

- 完成此任务后，使用这些秘钥的当前访问和刷新令牌将失效。
- 我们建议您在非高峰时段完成此任务，以将对最终用户的影响降至最低。
- 加密密钥仅可通过下面的 CLI 重新生成，但您也可以使用 Cisco Unified 操作系统管理 GUI 重新生成签名密钥。选择**安全** > **证书管理**，然后选择 **AUTHZ** 证书，并单击**重新生成**。

过程

步骤 1 在 Cisco Unified Communications Manager publisher 节点上，登录到命令行界面。

步骤 2 如果想要重新生成加密密钥：

a) 运行 `set key regen authz encryption` 命令。

b) 输入 `yes`。

步骤 3 如果想要重新生成签名密钥：

a) 运行 `set key regen authz signing` 命令。

b) 输入 `yes`。

Cisco Unified Communications Manager publisher 节点会重新生成密钥并将新密钥复制到所有 Cisco Unified Communications Manager 群集节点，包括任何本地 IM and Presence 服务节点。

接下来的操作

您必须重新生成新密钥并在所有 UC 群集上同步：

- IM and Presence 中心群集 — 如果您有一个 IM and Presence 集中式部署，您的 IM and Presence 节点会运行在与您的电话分离的群集上。在这种情况下，在 IM and Presence 服务中心群集的 Cisco Unified Communications Manager publisher 节点上重复此程序。
- Cisco Expressway 或 Cisco Unity Connection — 同样在那些群集上重新生成秘钥。有关详细信息，请参阅您的 Cisco Expressway 和 Cisco Unity Connection 文档。

上载证书或证书链

上载您希望您的系统信任的任何新证书或证书链。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**安全** > **证书管理**。

步骤 2 单击**上载证书/证书链**。

步骤 3 从**证书目的**下拉列表中选择证书名称。

步骤 4 通过执行以下操作之一选择要上传的文件：

- 在**上载文件**文本框中，输入文件的路径。
- 单击**浏览**，导航至文件，然后单击**打开**。

步骤 5 要将文件上载到服务器，请单击**上载文件**。

注释 上载证书后，重新启动受影响的服务。当服务器恢复时，您可以访问 CCMAdmin 或 CCMUser GUI，检验是否在使用您新添加的证书。

管理第三方证书颁发机构的证书

此任务流程提供第三方证书流程的概述，以及对序列中每个步骤的参考。您的系统支持由第三方证书颁发机构使用 PKCS # 10 证书签名请求 (CSR) 签发的证书。

过程

	命令或操作	目的
步骤 1	生成证书签名请求， 第 142 页	生成证书签名请求 (CSR) 是一块加密的文本，其中包含证书应用程序信息，包括您的公钥、组织名称、通用名称、所在地，以及国家/地区。证书颁发机构使用此 CSR 为您的系统生成信任证书。
步骤 2	下载证书签名请求， 第 142 页	将CSR下载到您的计算机，以便准备好提交给您的证书颁发机构。
步骤 3	请参阅您的证书颁发机构文档。	向您的证书颁发机构获取应用程序证书。
步骤 4	请参阅您的证书颁发机构文档。	向您的证书颁发机构获取根证书。
步骤 5	将证书颁发机构签名的 CAPF 根证书添加到信任存储库， 第 142 页	将根证书添加到信任存储库中。当使用证书颁发机构签名的 CAPF 证书时，请执行此步骤。
步骤 6	上载证书或证书链， 第 140 页	将证书颁发机构根证书上载到节点。
步骤 7	如果您更新了 CAPF 或 Cisco Unified Communications Manager 的证书，请生成新的CTL 文件。	请参阅《*Cisco Unified Communications Manager* 安全指南》，位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。 上载第三方签名的 CAPF 或 CallManager 证书之后，重新运行 CTL 客户端（如配置有）。
步骤 8	重新启动服务， 第 143 页	重新启动受新证书影响的服务。对于所有证书类型，重新启动相应的服务（例如，如果您更新了 Tomcat 或 Tomcat-ECDSA 证书，则重新启动 Cisco Tomcat 服务）。

生成证书签名请求

生成证书签名请求 (CSR) 是一块加密的文本，其中包含证书应用程序信息，包括您的公钥、组织名称、通用名称、所在地，以及国家/地区。证书颁发机构使用此 CSR 为您的系统生成信任证书。

注释 如果您生成新的 CSR，将覆盖任何现有的 CSR。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**安全** > **证书管理**。

步骤 2 单击**生成 CSR**。

步骤 3 配置**生成证书签名请求**窗口中的字段。请参阅联机帮助，了解有关字段及其配置选项的更多信息。

步骤 4 单击**生成 CSR**。

下载证书签名请求

将 CSR 下载到您的计算机，以便准备好提交给您的证书颁发机构。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**安全** > **证书管理**。

步骤 2 点击 **Download CSR**（**下载 CSR**）。

步骤 3 从**证书目的**下拉列表中选择证书名称。

步骤 4 点击 **Download CSR**（**下载 CSR**）。

步骤 5 （可选） 如果收到提示，请单击**保存**。

将证书颁发机构签名的 CAPF 根证书添加到信任存储库

当使用证书颁发机构签名的 CAPF 证书时，请执行这些步骤将根证书添加到 CallManager 信任存储库。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**安全** > **证书管理**。

步骤 2 单击**上载证书/证书链**。

步骤 3 在**上载证书/证书链**弹出窗口中，从**证书目的**下拉列表中选择**CallManager-信任**并浏览至证书颁发机构签名的 CAPF 根证书。

步骤 4 证书出现在**上载文件**字段中后，单击**上载**。

重新启动服务

如果您的系统需要您在群集中的特定节点上重新启动任何功能或网络服务，请使用此程序。

过程

步骤 1 根据您要重新启动的服务类型，执行以下任务之一：

- 选择**工具** > **控制中心 - 功能服务**。
- 选择**工具** > **控制中心 - 网络服务**。

步骤 2 从**服务器**下拉列表中选择您的系统节点，然后单击**转至**。

步骤 3 单击要重新启动的服务旁边的单选按钮，然后单击**重新启动**。

步骤 4 看到重新启动需要一些时间的消息之后，单击**确定**。

监控证书过期

使用此程序配置您的系统，当证书接近过期时间时自动向您发送电子邮件。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**安全** > **证书监控**。

步骤 2 在**通知开始时间**中，输入一个数值。此值是您通过电子邮件收到通知之前的天数。

步骤 3 在**通知频率**中，输入一个数值，然后选择**天**或**小时**。

步骤 4 （可选） 选中**启用电子邮件通知**，然后在**电子邮件 ID** 字段中输入电子邮件地址。

步骤 5 单击**保存**。

注释　默认情况下，证书监控服务每 12 小时运行一次。当重新启动证书监控服务时，它将启动服务，然后计算下一个计划，仅在 12 个小时后运行。即使证书接近七天的到期日期，间隔也不会改变。当证书已经过期或将在一天内过期时，服务会每 1 小时运行一次。

配置在线证书状态协议

使用在线证书状态协议 (OCSP) 获取证书的撤销状态。

注释　证书撤销状态检查仅会在证书或证书链上载期间执行。如果证书被撤销，会发出适用的警报。

开始之前

注意　启用 OSCP 之前，您必须将 OCSP 响应者证书上载到 tomcat-信任。

过程

步骤 1　从 Cisco Unified 操作系统管理中，选择**安全** > **证书撤销**。

步骤 2　选中**启用 OCSP** 复选框，然后执行以下任务之一：

- 如果使用外部或配置的 URI 联系 OCSP 响应者，选择**使用配置的 OCSP URI**。在 **OCSP 配置的 URI** 字段中，输入检验了证书撤销状态的 OCSP 响应者的 URI。
- 如果证书配置有将用于联系 OCSP 响应者的 OCSP URI，选择**从证书使用 OCSP URI**。

步骤 3　选中**启用撤销检查**复选框以执行撤销检查。

注释　当撤销和过期检查企业参数设置为启用时，证书撤销服务对于 LDAP 和 IPsec 连接为活动状态。

步骤 4　输入**检查间隔**值以配置证书撤销状态检查的频率。

a) 单击**小时**或**天**以按小时或按天检查撤销状态。

步骤 5　单击**保存**。

对证书错误进行故障排除

如果您在尝试从 IM and Presence 服务节点或来自 Cisco Unified Communications Manager 节点的 IM and Presence 服务功能访问 Cisco Unified Communications Manager 服务时遇到错误，问题的根源在于 tomcat-信任证书。错误消息 `Connection to the Server cannot be established (unable`

to connect to Remote Node)（无法建立与服务器的连接（无法连接到远程节点））出现在以下功能配置界面窗口中：

- **服务激活**
- **控制中心 - 功能服务**
- **控制中心 - 网络服务**

使用此程序帮助您解决证书错误。从第一个步骤开始，如有必要，继续后面的步骤。在某些情况下，您可能只需要完成第一个步骤便可解决错误。在其他情况下，则必须完成所有步骤。

过程

步骤 1 从 Cisco Unified 操作系统管理中，确认存在必需的 tomcat-信任证书：**安全** > **证书管理**。
如果所需的证书不存在，请等待 30 分钟，然后再次检查。

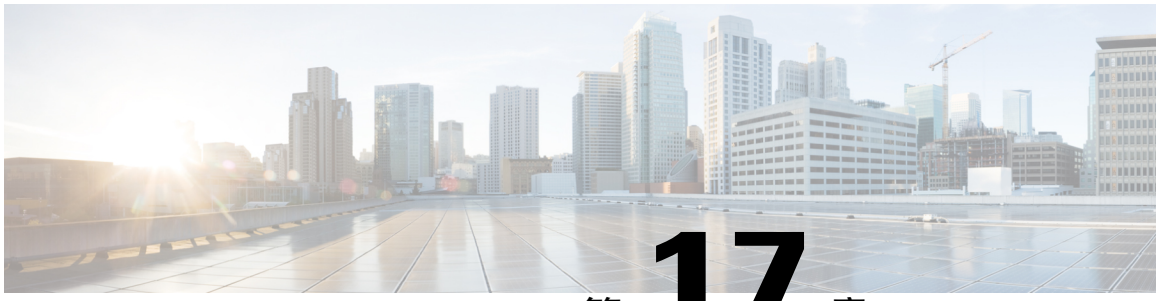
步骤 2 选择要查看其信息的证书。确认内容与远程节点上的相应证书匹配。

步骤 3 从 CLI 中，重新启动 Cisco 群集间同步代理服务：**utils service restart Cisco Intercluster Sync Agent**。

步骤 4 Cisco 群集间同步代理服务重新启动后，重新启动 Cisco Tomcat 服务：**utils service restart Cisco Tomcat**。

步骤 5 等待 30 分钟。如果前面的步骤不能解决证书错误，而 tomcat-信任证书存在，请删除该证书。删除证书后，您必须通过此方法手动交换证书：下载用于每个节点的 Tomcat 和 Tomcat-ECDSA 证书并将其作为 tomcat-信任证书上载到其对等机。

步骤 6 证书交换完成后，重新启动每台受影响服务器上的 Cisco Tomcat：**utils service restart Cisco Tomcat**。



第 17 章

管理批量证书

管理批量证书

如果您想在群集之间共享一组证书，可以使用批量证书管理。对于需要在群集之间建立信任的系统功能，例如跨群集分机移动，此步骤是必需的。

过程

	命令或操作	目的
步骤 1	导出证书，第 147 页	此程序为群集中的所有节点创建包含证书的 PKCS12 文件。 **注释** • 每个参与群集必须将证书导出到相同的 SFTP 服务器和 SFTP 目录。 • 每当 Tomcat、Tomcat-ECDSA、TFTP 或 CAPF 证书在任何群集节点上重新生成，您都必须将群集上的证书导出。
步骤 2	导入证书，第 148 页	将证书导回到主群集和远程（访问）群集中。 **注释** 在升级后，这些证书会保留。您无需重新导入或重新合并证书。

导出证书

此程序为群集中的所有节点创建包含证书的 PKCS12 文件。

注释
- 每个参与群集必须将证书导出到相同的 SFTP 服务器和 SFTP 目录。
- 每当 Tomcat、Tomcat-ECDSA、TFTP 或 CAPF 证书在任何群集节点上重新生成，您都必须将群集上的证书导出。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**安全** > **批量证书管理**。

步骤 2 配置主群集和远程群集都可以到达的 TFTP 服务器的设置。请参阅联机帮助，了解有关字段及其配置选项的信息。

步骤 3 单击**保存**。

步骤 4 单击**导出**。

步骤 5 在**批量证书导出**窗口中，为**证书类型**字段选择**全部**。

步骤 6 单击**导出**。

步骤 7 单击**关闭**。

导入证书

将证书导回到主群集和远程（访问）群集中。

注释 在升级后，这些证书会保留。您无需重新导入或重新合并证书。

注释 使用批量证书管理导入证书会导致电话重置。

开始之前

“导入”按钮出现之前，您必须完成以下活动：

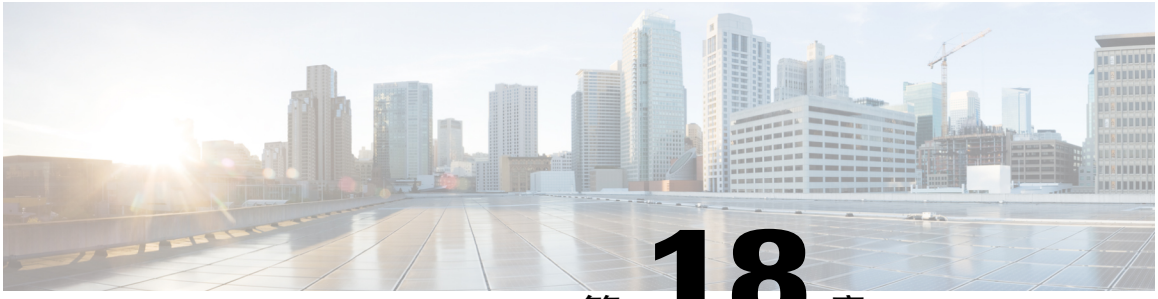
- 将证书从至少两个群集导出到 SFTP 服务器。
- 合并导出的证书。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**安全** > **批量证书管理** > **导入** > **批量证书导入**。

步骤 2 从**证书类型**下拉列表中，选择**全部**。

步骤 3 选择**导入**。



第 18 章

管理 IPSec 策略

IPsec 策略概述

IPsec 是一个框架，它通过使用加密安全服务确保私人、安全的 IP 网络通信。IPsec 策略用于配置 IPsec 安全服务。策略为您网络中的大多数流量类型提供不同级别的保护。您可以配置 IPsec 策略，以满足计算机、组织单位 (OU)、域、站点或全球企业的安全需求。

配置 IPsec 策略

注释

- 由于在系统升级过程中对 IPsec 策略所做的任何更改都会丢失，所以在升级期间不要修改或创建 IPsec 策略。
- IPsec 需要双向部署，或每个主机（或网关）一个对等机。
- 当您在两个节点上部署 IPSec 策略时，Cisco Unified Communications Manager一个 IPsec 策略协议设置为 “ANY”，另一个 IPsec 策略协议设置为 “UDP” 或 “TCP”，如果从使用 “ANY” 协议的节点运行验证，可能会导致漏报。
- IPsec，尤其是使用加密时，会影响系统性能。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**安全** > **IPSec 配置**。

步骤 2 单击**新增**。

步骤 3 配置 **IPSEC 策略配置**窗口中的字段。请参阅联机帮助，了解有关字段及其配置选项的更多信息。

步骤 4 单击**保存**。

步骤 5 （可选） 要验证 IPsec，选择**服务** > **Ping**，选中**验证 IPsec** 复选框，然后单击 **Ping**。

管理 IPsec 策略

由于在系统升级过程中对IPsec策略所做的任何更改都会丢失，所以在升级期间不要修改或创建IPsec策略。

注意 若您由于主机名、域或 IP 地址更改而对现有 IPsec 证书作出任何更改，将需要删除 IPsec 策略并重新创建（如果证书名称发生了更改）。如果证书名称未改变，则在导入远程节点上重新生成的证书后，必须禁用然后再启用 IPsec 策略。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**安全** > **IPSEC 配置**。

步骤 2 要显示、启用或禁用策略，请执行这些步骤：

a) 单击策略名称。

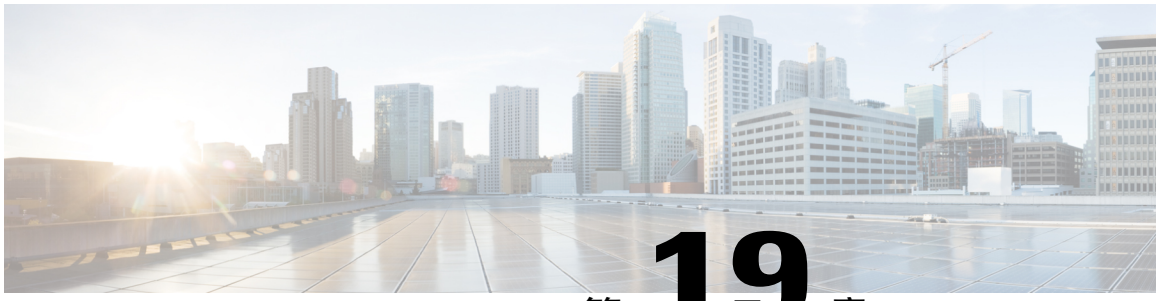
b) 要启用或禁用策略，请选中或取消选中**启用策略**复选框。

c) 单击**保存**。

步骤 3 要删除一项或多项策略，请执行这些步骤：

a) 选中您要删除的各项策略旁边的复选框。
您可以单击**全部选择**以选择所有策略，或单击**全部清除**以清除所有复选框。

b) 单击**删除选定项**。



第 19 章

管理凭证策略

凭证策略和验证

验证功能会验证用户、更新凭证信息、跟踪和记录用户事件和错误、记录凭证更改历史记录，以及加密或解密数据存储的用户凭证。

系统始终根据 Cisco Unified Communications Manager 数据库验证应用程序用户密码和最终用户个人识别码。系统可以根据公司目录或数据库验证最终用户密码。

如果系统与公司目录同步，Cisco Unified Communications Manager或轻量级目录访问协议 (LDAP) 中的验证功能可以验证密码：

- 启用 LDAP 验证时，用户密码和凭证策略不适用。这些默认值会应用于通过目录同步（DirSync 服务）创建的用户。
- 禁用 LDAP 验证后，系统根据数据库验证用户凭证。通过此选项，您可以分配凭证策略、管理验证事件和管理密码。最终用户可以通过电话用户界面更改密码和个人识别码。

凭证策略不适用于操作系统用户或 CLI 用户。这些管理员使用操作系统支持的标准密码验证程序。

在数据库中配置用户后，系统将在数据库中存储用户凭证的历史记录，以防用户在收到提示其更改其凭证的消息时输入之前用过的信息。

凭证策略的 JTAPI 和 TAPI 支持

由于 Cisco Unified Communications Manager Java 电话应用程序编程接口 (JTAPI) 和电话应用程序编程接口 (TAPI) 支持分配给应用程序用户的凭证策略，所以开发者必须创建应用程序以应对凭证策略执行时的密码过期、个人识别码过期以及锁定返回码。

应用程序使用 API 验证数据库或公司目录，而不管应用程序使用何种验证模型。

有关开发人员 JTAPI 和 TAPI 的详细信息，请参阅开发人员手册，位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html。

配置凭证策略

凭证策略适用于应用程序用户和最终用户。可将密码策略分配给最终用户和应用程序用户，将个人识别码策略分配给最终用户。“凭证策略默认值配置”列出这些组的策略分配。向数据库添加新用户时，系统会分配默认策略。您可以更改分配的策略并管理用户验证事件。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**用户管理** > **凭证策略**。

步骤 2 请执行以下步骤之一：

- 单击**查找**并选择一个现有的凭证策略。
- 单击**新增**以创建新的凭证策略。

步骤 3 填写**凭证策略配置**窗口中的字段。请参阅联机帮助，了解有关字段及其配置设置的更多信息。

步骤 4 单击**保存**。

配置凭证策略默认设置

安装时，Cisco Unified Communications Manager 将静态默认凭证策略分配给用户组。它不提供默认凭证。您的系统提供了一些选项来分配新的默认策略，以及为用户配置新的默认凭证和凭证要求。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **凭证策略默认设置**。

步骤 2 从**凭证策略**下拉列表框中，选择此组的凭证策略。

步骤 3 在**更改凭证**和**确认凭证**配置窗口中输入密码。

步骤 4 如果您不希望用户可以更改此凭证，请选中**用户无法更改**复选框。

步骤 5 如果您想将此凭证用作临时凭证，最终用户必须在下次登录时更改，请选中**用户必须在下次登录时更改**复选框。

步骤 6 如果您不希望凭证过期，请选中**没有过期**复选框。

步骤 7 单击**保存**。

监控验证活动

系统显示最近的验证结果，例如上次黑客尝试时间以及登录尝试失败计数。

系统将为以下凭证策略事件生成日志文件条目：

- 验证成功
- 验证失败（密码错误或未知）
- 由于以下原因验证失败：

  管理锁定

  黑客行为锁定（登录失败锁定）

  过期软锁定（过期的凭证）

  非活动锁定（凭证有一段时间未使用）

  用户必须更改（凭证设置为“用户必须更改”）

  LDAP 非活动（切换到 LDAP 验证且 LDAP 非活动）

- 用户凭证更新成功
- 用户凭证更新失败

注释 如果对最终用户密码使用 LDAP 验证，LDAP 仅跟踪验证成功和失败。

所有事件消息都包含字符串 “ims-auth” 和尝试验证的用户 ID。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **最终用户**。

步骤 2 输入搜索条件，单击**查找**，然后从结果列表中选择用户。

步骤 3 单击**编辑凭证**以查看用户的验证活动。

接下来的操作

您可以通过 Cisco Unified 实时监控工具 (Unified RTMT) 查看日志文件。还可以将捕获的事件收集到报告中。有关如何使用 Unified RTMT 的详细步骤，请参阅《*Cisco Unified* 实时监控工具管理指南》，位于http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

配置凭证缓存

启用凭证缓存以提高系统效率。您的系统不必为每一个单点登录请求执行数据库查找或调用存储的程序。关联的凭证策略不会执行，直至缓存时间到期。

此设置适用于所有调用用户验证的 Java 应用程序。

过程

步骤 1 从“Cisco Unified CM 管理”中，选择**系统** > **企业参数**。

步骤 2 根据需要执行以下任务：

- 将**启用缓存**企业参数设置为**真**。启用此参数后，Cisco Unified Communications Manager 会使用缓存的凭证最多 2 分钟。
- 将**启用缓存**企业参数设为**假**以禁用缓存，这样系统就不会使用缓存的凭证进行验证。对于LDAP验证，系统会忽略此设置。凭证缓存要求每位用户具备最小额外内存量。

步骤 3 单击**保存**。