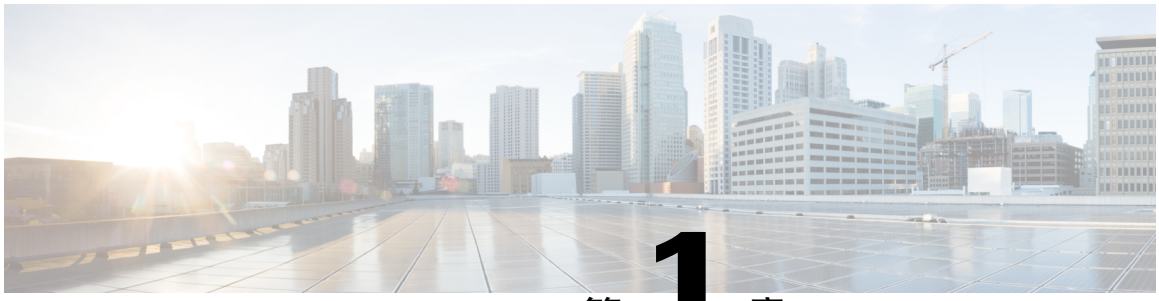
Cisco WebEx Meetings Server 2.5 版管理指南

首次发布日期: 2014 年 07 月 30 日

上次修改日期: 2014 年 10 月 14 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



第 1 章

系统概述

- 产品许可信息，第 1 页
- 关于产品文档，第 1 页
- 术语，第 2 页

产品许可信息

本产品的许可信息链接：

- http://www.webex.com/license.html
- http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html
- http://www.webex.com/CiscoWebExMeetingsServerSEULA.html

关于产品文档

Cisco WebEx Meetings Server 指南提供有关规划、部署和管理系统的详细过程：

这些过程包括安装和联网核对表，使您能够在实际部署之前收集信息和制定决策。

此外，还涵盖了部署后的系统改动过程，例如：

- 添加高可用性 (HA)
- 将系统扩展为更大容量
- 将系统更新或升级至最新版本

Cisco WebEx Meetings Server Administration Guide 介绍了在管理站点上使用可用功能的方法，包括以下部分：

- 控制板 — 控制板显示系统监控器并包括指向警告设置、**会议趋势**页、**资源历史记录**页、系统页和设置页的链接。 请参阅关于控制板以获取更多信息。

- 用户管理 — 使用这些功能可添加、导入、激活和停用用户，配置跟踪代码，以及向系统上的用户发送电子邮件。 请参阅管理用户，第 105 页以获取更多信息。
- 系统 — 使用这些功能可配置系统属性、站点及管理站点URL、服务器、SNMP 设置和许可证。请参阅配置系统，第 127 页以获取更多信息。
- 设置 — 使用这些功能可配置您的设置，包括公司信息、定制功能、会议设置、音频、视频、移动性、服务质量、密码、电子邮件设置、下载和安全性设置。 请参阅配置设置，第 151 页以获取更多信息。
- 报告管理 — 配置和查看月度报告。 请参阅管理报告，第 225 页以获取更多信息。
- 支持访问和信息 — 使用这些功能可开设和查看支持案例、配置调试功能以及执行系统资源和会议测试。 请参阅使用支持功能，第 253 页以获取更多信息。

术语

说明本产品时使用的术语。

数据中心 - 该物理硬件至少包括一个内含系统实例的设备。

高可用性 - 与主系统本地并行存在的冗余系统。 如果主系统发生故障，高可用性系统会取代发生故障的功能并发出警告。 故障转移对于用户而言是透明的。

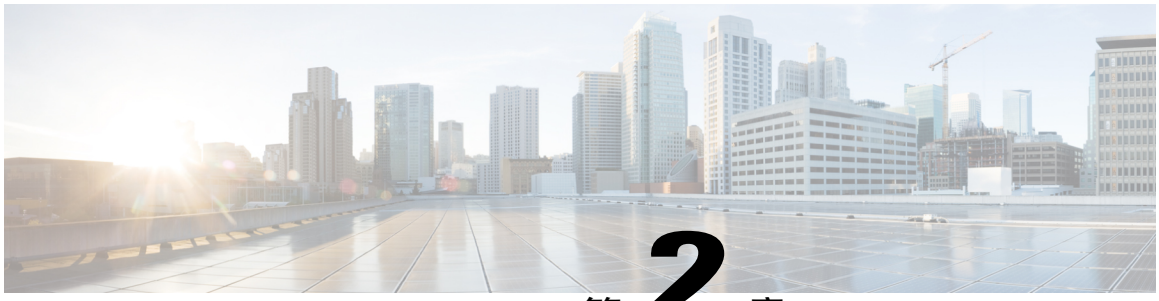
服务器 — Cisco WebEx Server 的单个实例。 可以加入多数据中心，并以单个系统的形式工作。

系统 - 该 Cisco WebEx Server 系统应用程序包括一个或多个物理数据中心。

第 I 部分

Cisco WebEx Meetings Server 部署指南

- 将 VMware vSphere 与系统配合使用， 第 5 页
- 自动部署系统， 第 11 页
- 手动部署系统， 第 31 页
- 配置邮件服务器、时区和区域设置， 第 47 页
- 在部署后改动系统， 第 53 页
- 添加高可用性系统， 第 55 页
- 扩大系统规模， 第 61 页
- 更新系统， 第 67 页
- 升级系统， 第 73 页
- 测试系统， 第 81 页



第 2 章

将 VMware vSphere 与系统配合使用

- 使用 VMware vSphere， 第 5 页
- 将 ESXi 主机配置为使用 NTP 服务器， 第 6 页
- 通过使用 VMware vCenter 创建备份， 第 6 页
- 通过使用 VMware vCenter 拍摄快照， 第 7 页
- 将现有 VMDK 文件附加到新虚拟机， 第 8 页

使用 VMware vSphere

系统的虚拟机是通过 VMware vSphere 部署的。 Cisco WebEx Meetings Server 必须安装在 VMware 虚拟机上，并受到下列限制的制约：

- 请使用 VMware vSphere 5.0、5.0 Update 1、5.0 Update 2、5.1、5.1 Update 1 或 5.5。

  不支持早期发行版的 vSphere。
- 请使用 VMware ESXi 5.0、5.0 Update 1、5.0 Update 2、5.1、5.1 Update 1 或 5.5。

  使用早期 ESXi 版本会出现难以理解的错误消息，这些消息有关**不受支持的硬件**，但不会明确列出问题。
- 请验证使用 ESXi 主机配置的 DNS 服务器可以解析在该 ESXi 主机上部署的虚拟机的主机名。
- 您必须使用 VMware vCenter 来管理在其中部署 Cisco WebEx Meetings Server 系统的 ESXi 主机。
- 关闭虚拟机时，请始终为每个虚拟机选择**电源** > **关闭客户机**。 （请勿使用**关闭**选项。）

注释 有关受支持的 VMware 配置的详细信息，请参阅《*Cisco WebEx Meetings Server* 规划指南》和《*Cisco WebEx Meetings Server* 系统要求》。

将 ESXi 主机配置为使用 NTP 服务器

将 ESXi 主机配置为使用网络时间协议 (NTP) 进行设备时钟同步，并验证 NTP 服务器可以被访问。在多数据中心环境中，数据中心时钟同步对于在数据中心之间保持数据共享至关重要。 有关详细说明，请参阅 VMware ESXi 文档。

步骤 1 使用 vSphere 客户端，在清单面板中选择 ESXi 主机。

步骤 2 在“软件”部分中选择**配置** > **时间配置**。

步骤 3 选择**属性**。

步骤 4 选择**已启用的 NTP 客户端**。

步骤 5 选择**选项**以配置 NTP 服务器设置。
我们建议您选择**与主机一起开始和停止**，以降低 ESXi 主机时间不正确的可能性。

通过使用 VMware vCenter 创建备份

备份是传统的文件系统，主要利用 VMware 技术和基于 SAN 的数据传输。 VMware® 数据恢复可为虚拟机创建备份，而不会中断虚拟机的使用或它们提供的数据和服务。 数据恢复使用虚拟机设备和客户端插件来管理和恢复备份。 将以开放虚拟化格式 (OVF) 提供备份设备。 数据恢复插件需要 VMware vSphere 客户端。

数据恢复管理现有备份，并删除过时备份。它还支持重复数据删除以删除冗余数据。在执行任何系统改动过程之前，我们建议您通过使用 VMware 数据恢复（VMware vSphere 发行版 5.0 可用）或 vSphere 数据保护（vSphere 发行版 5.1 可用）来为每个虚拟机创建备份。（VMware 数据恢复/vSphere 数据保护是 VMware vSphere 中自带的，vSphere Essentials 工具包中除外。 有关更多信息，请参阅 http://www.vmware.com/pdf/vdr_11_admin.pdf。）

您也可以通过使用存储服务器来创建备份。 请参阅配置存储服务器， 第 136 页以获取更多信息。

虚拟机快照是系统在特定时间点的照片，与备份不同。 由于性能原因，我们建议您使用备份，并且不要将虚拟机备份存储在包含虚拟机的物理驱动器上。 有关快照以及已知性能问题的更多信息，请参阅通过使用 VMware vCenter 拍摄快照， 第 7 页。

步骤 1 开启维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
我们建议您给每个虚拟机拍摄快照。（请参阅通过使用 VMware vCenter 拍摄快照， 第 7 页。）

在所有活动数据中心开启维护模式会关闭会议活动，并会使用户无法登录 WebEx 站点、安排会议、加入会议，或播放会议录制文件。 如果此数据中心属于多数据中心 (MDC) 系统，并且另一个数据中心是活动的，那么进

行中的会议将故障转移到活动的数据中心。 这可能会导致活动的会议暂时中断。 有关要求开启维护模式的系统任务的信息，请参阅关于维护模式。

步骤 2 遵照 VMware vSphere 文档中的指示并使用 VMware 数据恢复（从 vSphere 发行版 5.1 开始称为 VMware vSphere 数据保护）以创建系统及每个虚拟机的备份。
有关此备份的详细信息，请参阅 *VMware Data Recovery Administration Guide* 或 *vSphere Data Protection Administration Guide*。

注释 我们建议您在完成系统改动过程、已经测试过系统并且对结果感到满意后删除备份。 从旧的备份或快照还原数据中心可能导致意外的动作。

通过使用 VMware vCenter 拍摄快照

虚拟机快照用于在系统改动过程之后快速恢复虚拟机。 快照是系统在特定时间点的照片，与备份不同（请参阅通过使用 VMware vCenter 创建备份，第 6 页）。 我们建议您除截取快照之外，还要对系统进行备份。

注释 因为如果原始虚拟机磁盘文件丢失，您不能使用快照来恢复虚拟机。

快照存储在包含虚拟机的物理驱动器上。 如果不及时删除这些快照，最终用户可能会因为影响虚拟机性能的已知问题而体验到较差的音频和视频。 因此，我们建议您使用备份，并且不要将虚拟机备份存储在包含虚拟机的物理驱动器上。 此外，快照可用于更新，但对于系统升级，我们建议您在执行升级之前删除所有快照并对原始系统进行备份。

有关 VMware 快照的该已知问题的更多信息，请转至 VMware 网站并参阅白皮书在网络附加存储上运行 *VMware vSphere* 的最佳实践。 您还可以在 VMware 知识库中搜索**快照影响性能**以获取其他信息。

在执行多数系统改动过程之前，我们建议您备份系统（尤其是在执行升级或扩展时）或者截取每个虚拟机的快照（在执行更新时）。 您可以使用 VMware 数据恢复（从 vSphere 发行版 5.1 开始称为 VMware vSphere 数据保护）来备份系统，也可以截取每个虚拟机的快照。（VMware 数据恢复/vSphere 数据保护是 VMware vSphere 中自带的，vSphere Essentials 工具包中除外。）

确保阅读准备部分以了解具体过程。 我们列出了每个过程的具体注意事项。

记住 如果系统包含多个虚拟机，请选择**电源**>**关闭客户系统**，然后为系统中的每个虚拟机拍摄快照。请使用相同的前缀标注每台虚拟机的快照，例如，8 月 20 日，这样您就知道这些快照是在同一时间完成的。

我们建议您保留快照的时间不超过 24 小时。 如果您想保留更长时间，我们建议您创建备份。 有关 VMware 数据恢复（从 vSphere 发行版 5.1 开始称为 VMware vSphere 数据保护）的更多信息，请参阅通过使用 VMware vCenter 创建备份，第 6 页。

步骤 1 使系统处于维护模式。 有关完整的详细信息，请参阅关于维护模式，第 101 页。
请确保不存在活动的会议且选定的时间是对用户影响最小的时间。

步骤 2 在 VMware vCenter 上，为每个虚拟机选择**电源** > **关闭客户系统**。

步骤 3 为每个虚拟机选择**快照** > **拍摄快照**。

步骤 4 输入快照的名称并选择**确定**。

接下来的操作

- 完成过程并测试系统以确认过程成功。
- 如果必须恢复到快照，请确保每个虚拟机的快照是在同一时间拍摄的。 启动快照不匹配的系统可能导致数据库损坏。

将现有 VMDK 文件附加到新虚拟机

本节描述了如何使用 VMware vCenter 将虚拟机磁盘 (VMDK) 文件从现有管理虚拟机附加到新的管理虚拟机。 在扩展或升级系统时会使用此过程。 （我们再次使用存储在管理虚拟机的硬盘 4 中的系统数据。）

注意 制作硬盘 4 中基本 VMDK 文件的副本，并将该文件复制到升级或扩展系统上管理虚拟机的虚拟机文件夹中。 如果仅仅附加硬盘 4，数据仍将存储在旧管理虚拟机的虚拟机文件夹中。 如果不小心删除了 vCenter 清单中的现有管理虚拟机，当前系统将无法访问硬盘 4。

重要事项 确保复制硬盘 4 的原始基本 VMDK 文件，而不是此 VMDK 文件的快照。

注释 如果您使用的是直连存储 (DAS)，必须将 VMDK 迁移至新管理虚拟机可访问的逻辑单元号 (LUN)。

注释 在系统改动过程之前，我们将管理虚拟机称为当前管理虚拟机。 在扩展或升级后，将管理虚拟机称为升级管理虚拟机。

步骤 1 浏览 VMware vCenter 中的清单并查找系统的现有管理虚拟机。

步骤 2 右键单击虚拟机名称并选择**编辑设置...**。
系统将显示**虚拟机属性**窗口。

步骤 3 选择**硬件**标签页，然后选择**硬盘 4**。

步骤 4 复制**磁盘文件**位置并将其粘贴至另一个文档以备将来参考。
这指定了 VMDK 在 VMware vCenter 中的位置。

该字符串类似于 `[EMC-LUN10-RAID5] webex-sysA-admin/webex-sysA-admin_3.vmdk`。 如果之前已经升级系统，文件名将不会遵照现有虚拟机的命名约定。

步骤 5 写下硬盘 4 的存储位置和虚拟机文件夹名称。
文件夹名称字符串类似于 `[EMC-LUN8-RAID5] webex-sysB-admin`。

步骤 6 请不作任何更改地关闭**编辑设置...**窗口。

步骤 7 将 vCenter 视图更改为数据存储和数据存储群集视图。 选择**视图** > **清单** > **数据存储和数据存储群集**。

步骤 8 选择现有管理虚拟机所在的存储位置（步骤 5），然后选择**浏览此数据存储**。

步骤 9 选择（为扩展或升级系统）新部署的管理虚拟机所在的存储位置，然后选择**浏览此数据存储**。

步骤 10 将（现有和扩展或升级管理虚拟机的）两个数据存储浏览器窗口并列排列，以便您可以同时看到两个管理虚拟机文件夹。

步骤 11 打开两个虚拟机文件夹并将 VMDK 从现有管理虚拟机文件夹复制到扩展或更新管理虚拟机文件夹中。

a) 在现有管理虚拟机文件夹中，确定与硬盘 4 相关联的 VMDK。 请参考第 4 步中写下的文件位置，以确认准确度。
b) 右键单击该文件，然后选择**复制**。
c) 右键单击扩展或升级管理虚拟机文件夹内部，然后选择**粘贴**。完成粘贴操作后，关闭这两个数据存储器窗口。
d) 通过选择**视图** > **清单** > **主机和群集**来将 vCenter 视图还原为主机和群集的列表。

步骤 12 浏览 VMware vCenter 中的清单并查找系统扩展或升级的管理虚拟机。

步骤 13 右键单击扩展或更新的虚拟机名称并选择**编辑设置...**。
系统将显示**虚拟机属性**窗口。

步骤 14 选择**硬件**标签页，然后选择**硬盘 4**。

步骤 15 选择**删除**。
此操作不会立即删除虚拟磁盘。 而是预定删除现有虚拟磁盘。

步骤 16 选择**添加**。

系统将显示**添加硬件**向导。

步骤 17 选择**硬盘**，然后选择**下一步**。

步骤 18 选择**使用现有虚拟磁盘**，然后选择**下一步**。

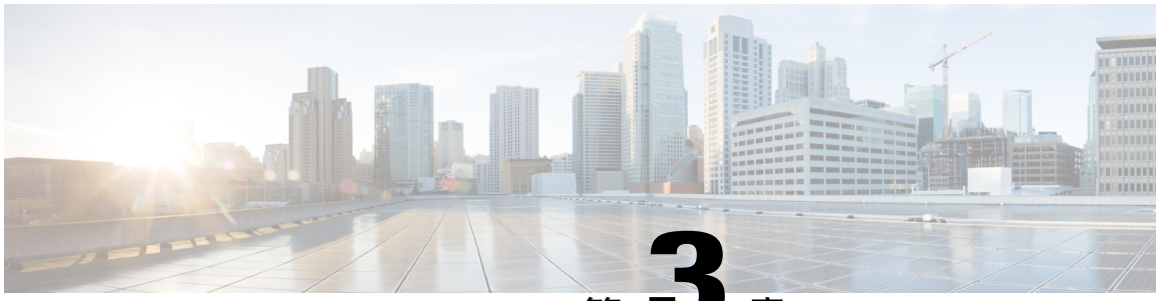
步骤 19 选择**浏览**，然后导航至扩展或升级的管理虚拟机所在的数据存储器。 导航至新管理虚拟机文件夹。 双击此文件夹，然后选择在第 11 步中复制的虚拟磁盘。 选择**确定**。

步骤 20 在**虚拟设备节点**下拉列表中，选择 **SCSI (0:3)**，然后选择**下一步**。

步骤 21 复查所做的更改，如果更改正确，请选择**完成**。 否则，选择 **上一步** 并修复所有错误。
向导完成之后，“硬件”标签页中将显示标记为添加的新磁盘。

步骤 22 通过选择**确定**来落实添加和删除操作。

步骤 23 在 VMware vCenter **最近任务**窗格中查看此虚拟机重新配置任务以确保没有错误。



第 3 章

自动部署系统

- 系统部署的一般概念， 第 12 页
- 安装核对表， 第 14 页
- 自动部署所需的信息， 第 15 页
- 从 VMware vSphere 客户端部署 OVA 文件， 第 18 页
- 选择安装向导语言， 第 20 页
- 确认部署， 第 21 页
- 选择要安装的系统， 第 21 页
- 选择部署类型， 第 22 页
- 提供 VMware vCenter 凭证， 第 22 页
- 选择媒体虚拟机的 vCenter 设置， 第 23 页
- 输入媒体虚拟机的联网信息， 第 23 页
- 添加公开访问， 第 23 页
- 输入公共 VIP 地址， 第 25 页
- 输入专用 VIP 地址， 第 26 页
- WebEx 站点和 WebEx 管理 URL， 第 26 页
- 确认网络配置正确， 第 28 页
- 部署虚拟机， 第 28 页
- 检查系统， 第 28 页

系统部署的一般概念

系统容量

系统由支持的并发用户数识别：

- 50 个并发用户（又称为微型系统）

  通常支持员工数为 500-1000 的公司

  主系统 [（不带高可用性 (HA)）] 拥有一个管理虚拟机和一个可选的互联网反向代理（用于公开访问）

- 250 个并发用户（又称为小型系统）

  通常支持员工数为 2500-5000 的公司

  主系统（无HA）拥有一个管理虚拟机、一个媒体虚拟机和一个可选的互联网反向代理（用于公开访问）

- 800 个并发用户（又称为中型系统）

  通常支持员工数为 8000-16000 的公司

  主系统（无HA）拥有一个管理虚拟机、一个媒体虚拟机和一个可选的互联网反向代理（用于公开访问）

- 2000 个并发用户（又称为大型系统）

  通常支持员工数为 20000-40000 的公司

  主系统（无 HA）拥有 1 个管理虚拟机、3 个媒体虚拟机、2 个 Web 虚拟机和 1 个可选的互联网反向代理（用于公开访问）

部署期间使用的术语

WebEx 站点 URL — 供用户在单数据中心环境中主持和出席会议的安全 http URL。

WebEx 管理 URL — 供管理员在单数据中心环境中配置、监控和管理系统的安全 http URL。

公共 VIP - 用于 WebEx 站点 URL 的虚拟 IP 地址。

专用 VIP — 用于管理站点 URL 的虚拟 IP 地址或用于 WebEx 站点 URL 的虚拟 IP 地址（仅适用于内部用户，如有水平分割 DNS）。

WebEx 公共 URL — 由 DNS 用于将用户重定向至数据中心，用户在该处执行会议相关任务，例如安排或主持会议。 DNS 选择哪个数据中心对用户而言是透明的。 WebEx 公共 URL 只是用户进入系统的一个便利位置。 如果数据中心停机，对用户而言没有变化，包括对用于访问会议的 URL 也没有变化，因为 DNS 会将用户重定向至续存数据中心。

管理公共 URL — 通常简称为管理 *URL*。 DNS 将其用于把管理员重定向至管理数据中心，管理员在其中登录系统。 DNS 选择哪个数据中心对管理员而言是透明的（但是，URL 栏中的字符串会根据管理员用来访问系统的数据中心而变化）。 管理公共 URL 只是管理员用于进入系统的一个便利目标。

管理本地 URL — 特定于多数据中心 (MDC) 系统中的各个数据中心。 通过管理公共 URL 登录时，DNS 将管理员重定向至管理数据中心的管理本地 URL。 向用户分配许可证之类的任意系统修改都将在管理数据中心中执行，并复制到 MDC 系统的所有数据中心中。

管理员可以从CWMS应用程序中选择具体的数据中心进行修改，但是选择其他数据中心进行修改不会更改管理本地URL，因为管理员对系统的访问保持为管理员登录系统时DNS所选择的数据中心。管理员在 MDC 系统中对其他数据中心所作的修改将由 DNS 所选择的管理数据中心传递至目标数据中心。

MDC 系统将至少有两个管理本地 URL，系统中的每个数据中心各一个。

本地 URL 特定于每个数据中心。

系统配置文件信息

请针对您的系统填写下表。

公共站点 URL		
公共管理 URL		
DC1 和 DC2 虚拟 IP 地址		
	数据中心 1	**数据中心 2**
本地站点 URL		
本地管理员 URL		
公共虚拟 IP 地址		
专用虚拟 IP 地址		
DNS 服务器		
管理虚拟机 IP 地址		
媒体虚拟机 IP 地址 1		
媒体虚拟机 IP 地址 2		
媒体虚拟机 IP 地址 3		
Web 虚拟机 IP 地址 1		

Web 虚拟机 IP 地址 2		
DMZ 虚拟机 IP 地址（可选）		
CWMS 管理员电子邮件地址		
密码		
Remote Access[1]		
密码		
Call Manager IP 地址		
Cisco Call Manager 管理员标识		
Cisco Call Manager 密码		
CWMS 拨入号码		
电话号码		

1 远程访问帐户未启用，直到帐户激活。

安装核对表

限制 您必须使用 VMware vCenter 来管理在其中部署 Cisco WebEx Meetings Server 系统的 ESXi 主机。

网络更改

请参阅与部署相应的网络核对表。 考虑以下因素：

- 公开访问： 防火墙以外的用户是否能从互联网或移动设备主持和访问会议

  Cisco 建议公开访问，因为这会给移动办公的员工带来更好的用户体验。
- 贵公司的 DNS 设置类型： 水平分割 DNS 或非水平分割 DNS（最常见的 DNS 配置）。 有关 DNS 设置的更多信息，请参阅《*Cisco WebEx Meetings Server* 规划指南》。
- 从管理虚拟机的管理员桌面打开端口 10200。 Web 浏览器在部署过程中使用端口 10200。

选择与部署相应的核对表：

- 启用公开访问和具有非水平分割 DNS 的系统的联网清单
- 禁止公开访问的系统的联网清单
- 启用公开访问和具有水平分割 DNS 的系统的联网清单

必填信息

如果使用自动部署（支持 50 个并发用户、250 个并发用户和 800 个并发用户）系统或手动部署（支持所有系统容量），所需信息会有所不同。 我们建议选择自动部署，除非部署的是始终需要手动部署的 2000 个用户的系统。

选择与部署类型相应的核对表：

- 自动部署所需的信息，第 15 页
- 手动部署所需的信息，第 35 页

自动部署所需的信息

以下依次为系统所需的信息。

注释 确保在开始系统部署之前将虚拟机 FQDN、IP 地址、WebEx 和管理站点 URL 以及 VIP 地址添加至 DNS 服务器。 我们将在部署过程中使用此信息来查找您的 IP 地址。

为避免任何 DNS 问题，您可能要在开始 OVA 部署之前测试这些 URL 和 IP 地址。 否则，部署将失败，直至您更正这些错误。

字段名	描述	您的系统的值
vCenter URL	系统中虚拟机的 vCenter 服务器的 http 地址。	
vCenter 用户名	用于为系统部署虚拟机的用户名。此用户必须有管理员权限：用于部署、配置、启动、关闭和删除虚拟机。	
vCenter 密码	vCenter 用户的密码。	
（仅限 250 个和 800 个并发用户的系统） ESXi 主机	媒体虚拟机的 ESXi 主机。 **注释** 此 ESXi 主机必须位于与上述 vCenter URL 相同的 vCenter 上。	
（仅限 250 个和 800 个并发用户的系统） 数据存储	媒体虚拟机的数据存储。	

字段名	描述	您的系统的值
（仅限 250 个和 800 个并发用户的系统） 虚拟机端口组	媒体虚拟机的端口组。 **注释** Cisco 建议您选择与为管理虚拟机所选端口组相同的端口组。	
（仅限 250 个和 800 个并发用户的系统） 媒体虚拟机的 FQDN。	媒体虚拟机的标准域名（全小写字符）。	
（仅限 250 个和 800 个并发用户的系统） 媒体虚拟机的 IPv4 地址	媒体虚拟机的 IPv4 地址。 我们将自动查找此媒体虚拟机的相应 IPv4 地址。	
（仅限公开访问） ESXi 主机	互联网反向代理虚拟机的 ESXi 主机。 **注释** Cisco 建议您选择与为管理和其他内部虚拟机选择的 ESXi 主机不同的主机。 为启用到互联网反向代理的传输，请确保该 ESXi 主机配置有一个可以路由至互联网反向代理使用其 IP 地址的 VLAN 的端口组。	
（仅限公开访问） 数据存储	互联网反向代理虚拟机的数据存储。	
（仅限公开访问） 虚拟机端口组	互联网反向代理虚拟机的端口组。 **注释** 出于安全性考虑，Cisco 建议选择与为管理虚拟机选择的端口组不同的组。	
（仅限公开访问） 互联网反向代理的 FQDN	互联网反向代理虚拟机的标准域名（全小写字符）。	
（仅限公开访问） 互联网反向代理 IPv4 地址	互联网反向代理虚拟机的 IPv4 地址。 我们将自动查找此互联网反向代理虚拟机的相应 IPv4 地址。	

字段名	描述	您的系统的值
（仅限公开访问） IPv4 网关	互联网反向代理虚拟机的 IPv4 网关。	
（仅限公开访问） IPv4 子网掩码	互联网反向代理虚拟机的子网掩码。	
（仅限公开访问） 首选 DNS 服务器 IPv4 地址	互联网反向代理虚拟机的 DNS 服务器。	
（仅限公开访问） 备用 DNS 服务器 IPv4 地址	（可选）互联网反向代理虚拟机的附加 DNS 服务器。	
公共 VIP	WebEx 站点 URL 的 IP 地址（站点用户访问该地址以主持和出席会议）	
专用 VIP	• 管理站点 URL 的 IP 地址（供管理员配置、监控和管理系统） • WebEx 站点 URL 的 IP 地址（仅供内部用户使用，前提是您有水平分割 DNS）。	
WebEx 站点 URL	供用户主持和参加会议的安全 http URL（全小写字符）。	
WebEx 管理 URL	供管理员配置、监控和管理系统的安全 http URL（全小写字符）。	

后续步骤

按照此信息在浏览器窗口输入部署 URL 开始部署系统。（管理虚拟机的控制台窗口中会显示部署 URL。）

注释 如果在配置完成之前重新启动系统，会生成新的密码，您必须搭配新的密码使用部署 URL。

从 VMware vSphere 客户端部署 OVA 文件

OVA 模板为每个虚拟机创建两个虚拟 NIC。 但是，只有管理虚拟机会同时使用这两个虚拟 NIC。 对于所有其他 Cisco WebEx Meetings Server (CWMS) 虚拟机，只使用一个虚拟 NIC，而另一个会断开连接。

此步骤提供作为一般指导。 在部署 OVA 过程中看到的屏幕取决于您的 vCenter、存储空间以及网络配置，可能与此步骤中所述的不一样。 查看 VMware vSphere 文档，获取有关 OVA 向导的完整信息。

开始之前

获取 Cisco WebEx Meetings Server 系统 OVA 文件并将其置于可从 VMware vSphere 进行访问的位置。 使用 VMware vSphere 客户端部署用于您系统的管理虚拟机。

您必须使用 VMware vCenter 来管理在其中部署 Cisco WebEx Meetings Server 系统的 ESXi 主机。 使用 vSphere 客户端登录 vCenter 并部署管理虚拟机的 OVA 文件。

步骤 1 登录 VMware vSphere 客户端。
确保以拥有管理员权限的用户身份登录： 用于部署、配置、启动、关闭和删除虚拟机。

步骤 2 选择**文件** > **部署 OVF 模板...**

步骤 3 选择**浏览**以导航到保存 OVA 文件的位置。 选择**下一步**。
您可以选择 **Cisco WebEx Meetings Server** 链接，转至含有此系统详细信息的网页。

步骤 4 阅读最终用户许可协议并选择**接受**，然后选择**下一步**。

步骤 5 导航至 vCenter 目录并选择要放置管理虚拟机的位置。

步骤 6 根据系统容量输入虚拟机的名称，然后选择**下一步**。 关于为系统选择正确大小的更多信息，请参阅系统容量，第 12 页。
必须先部署管理虚拟机，然后才能部署任何其他虚拟机。 如果您选择自动部署（推荐使用），我们将为您部署其他虚拟机。 如果您选择手动部署（支持 2000 个并发用户的系统需要使用此方式），那么在完成对管理虚拟机的部署后，您必须使用同一向导部署其他虚拟机。

Cisco 建议您将类型包含在虚拟机名称中；例如，将“管理”包含在管理虚拟机名称中，以便在 vCenter 清单中轻松找到管理虚拟机。

系统所有的内部虚拟机必须和管理虚拟机位于同一子网。 （根据您选择的系统容量，可能需要一个或多个媒体和 Web 内部虚拟机。）

步骤 7 根据系统容量从下拉列表中选择虚拟机，并选择**下一步**。
在系统中部署任何其他虚拟机前，确保先部署管理虚拟机。

步骤 8 浏览 vCenter 清单并选择要部署系统虚拟机的 ESXi 主机或群集。 选择**下一步**。

步骤 9 如果群集包含资源池，则选择要在其中部署 OVA 模板的资源池，然后选择**下一步**。
资源池共享 CPU 和内存资源，或与 VMware 功能（例如 DRS 或 vMotion）配合使用。 资源池必须专供单个 ESXi 主机使用。 不建议 VMware 资源池用于 Cisco WebEx Meetings Server。

步骤 10 选择虚拟机数据存储和配置类型。
必须选择**密集配置**，并创建系统所需的最大虚拟磁盘空间。 如果选择精简配置，VMware 将根据需要分配文件系统空间，从而导致性能低下。 延迟置零已足够，也可使用积极置零，但积极置零需要更多时间来完成。

步骤 11 设置网络映射。 从**目标网络**列中的下拉列表中，为各个资源网络选择目标网络。 选择**下一步**。

注释 “VM Network”和“VIP Network”必须映射到“目标网络”列中的同一个值。 您可以忽略关于多源网络映射到同一主机网络的警告消息。

步骤 12 输入以下虚拟机信息，然后选择**下一步**：

- 虚拟机的主机名（这里不包括域）
- 虚拟机的域名
- 虚拟机的 IPv4 地址 (Eth0)
- 虚拟机的子网掩码
- 网关 IP 地址
- 包含此虚拟机的主机名和 IP 地址条目的首选 DNS 服务器
- 包含此虚拟机的主机名和 IP 地址条目的备用 DNS 服务器（仅配置一个 DNS 服务器的系统有风险，因为它产生了单点故障。 我们建议您配置一个备用 DNS 服务器，以产生网络冗余。）
- 此虚拟机开机后，安装过程中显示的语言

注释 为避免出现 DNS 问题，您可以在开始 OVA 部署之前测试 URL 和 IP 地址。 如有错误，部署将失败。

步骤 13 确认您输入的信息。 如有任何错误，请选择**上一步**，然后更改值。

步骤 14 如果要手动升级系统，选择**完成**，忽略此步骤的平衡，在手动升级系统，第 77 页中继续下一步。 （在部署升级系统之后，但是尚未启动时，应通过使用手动部署将原始系统的数据复制到升级系统中。） 否则，勾选**部署后启动**，然后选择**完成**。

步骤 15 如果您正在部署管理虚拟机，请转至 vCenter 并打开虚拟机控制台窗口。 开机后，我们将检查您在部署 OVA 的过程中输入的网络信息。
如果我们能够确认连通性，系统将显示绿色勾选标记。

如有问题，系统将显示红叉。 修复错误，然后重新尝试部署 OVA。

步骤 16 记下控制台窗口中显示的 URL（区分大小写）。
管理员使用此 URL 继续系统部署。

如果系统在配置完成之前重新启动，则将生成新密码，您必须通过该新密码使用 URL。

接下来的操作

如果您是手动执行部署，我们建议此时为系统部署剩余的虚拟机。 这样可避免诸如启动虚拟机时超时等问题。

如果部署成功，请继续在浏览器窗口中部署系统。

如果部署失败，请参阅OVA 部署失败后请检查联网配置 ， 第 20 页。

OVA 部署失败后请检查联网配置

确认虚拟机的联网条目。

重要事项 请勿对系统中的任何虚拟机使用**编辑设置...**（除非在部署失败后使用）。一旦系统开始运行，必须通过 WebEx 管理站点才能对虚拟机设置进行任何进一步的编辑。如果您使用 vSphere 客户端，那么系统将不会接受所做的修改。

注释 更多详细步骤，请参阅 VMware vSphere 文档。

步骤 1 在 vSphere 客户端中，在虚拟机上选择**电源** > **关闭客户系统**。

步骤 2 在清单中查找虚拟机，然后右键单击**编辑设置...**。

步骤 3 选择**选项**标签页。

步骤 4 选择**属性**并确认已正确输入所有的联网信息。若需要更改，请按正确的设置重新部署 OVA。
一个可能出现的网络问题是为 ESXi 主机设置的 VLAN 路由不正确。由于虚拟机位于该 VLAN，无法进行网络连接。通过 ESXi 主机所在的网络，您可以 Ping 将用于系统虚拟机的 VLAN 的缺省网关 IP 地址。

选择安装向导语言

确定用于安装系统的首选语言。

注释 切勿关闭浏览器窗口，直到系统部署完成。如果提前关闭浏览器，可能需要重新开始部署。

升级至版本 2.5 之后，CWMS System是数据中心的缺省名称；它没有从英语翻译为任何其他语言。

开始之前

请确保已从 VMware vCenter 部署管理虚拟机。 请参阅 从 VMware vSphere 客户端部署 OVA 文件，第 18 页

步骤 1 从该下拉菜单中选择一个语言。

步骤 2 选择**下一步**。

确认部署

要确认部署新系统或者扩展现有系统，选择**下一步**。

确认系统容量

在使用 OVA 文件部署管理虚拟机时，您已选择系统容量。

- 确认在 OVA 部署过程中选中的系统容量是否正确。

  如果选中的系统容量是正确的，则选择**下一步**。

  如果选中的系统容量是错误的，则选择**我想更改系统容量**。

  a) 使用 VMware vSphere 客户端，对系统容量错误的管理虚拟机选择**电源** > **关闭客户系统**。
  b) 右键单击虚拟机，然后选择**从磁盘中删除**。
  c) 重新部署 OVA 文件，然后选择正确系统容量的管理虚拟机。

选择要安装的系统

步骤 1 确定安装类型。

- 如果您是首次安装此系统，请选择**安装主系统**。
- 如果您已安装主系统并且要添加冗余的高可用性 (HA) 系统，请选择**创建高可用性 (HA) 冗余系统**。

请勿尝试在安装主系统之前安装 HA 系统，因为只有在安装了主系统后才能使用 HA 系统。

步骤 2 选择**下一步**。

选择部署类型

您可以选择自动或手动部署系统虚拟机。 您可根据以下情形选择自动部署或手动部署：

- 如果时间有限，自动部署要比手动部署快。
- 如需逐步指导，自动部署期间提供此指导。
- 如果您对 VMware vCenter 很熟悉，并且不想提供 vCenter 凭证，请选择手动部署。

我们建议您选择**自动**，除非您部署的是始终需要手动部署的 2000 个用户的系统。

步骤 1 选择自动或手动部署：

- **自动**： 我们会部署系统所需的所有虚拟机。
- **手动**： 通过使用 VMware vCenter 可手动部署各个虚拟机。 回答几个有关系统的问题之后，会为您提供系统所需虚拟机的列表。

步骤 2 选择**下一步**。

提供 VMware vCenter 凭证

如果选择了自动部署，那么 Cisco WebEx Meetings Server 需要 vCenter 凭证才能为您部署虚拟机。

开始之前

系统所有的 ESXi 主机必须属于同一 VMware vCenter。

步骤 1 输入将要部署系统的 vCenter 的安全 https URL。

步骤 2 输入用于部署虚拟机的用户名。 vCenter 用户必须包含管理员权限，以便允许管理员部署、配置、启动和关闭以及删除虚拟机。

步骤 3 输入此用户名的密码。

步骤 4 选择**下一步**。

选择媒体虚拟机的 vCenter 设置

部署 250 个和 800 个用户系统需要媒体虚拟机。

步骤 1 从下拉列表中选择媒体虚拟机的 ESXi 主机。

步骤 2 选择媒体虚拟机的数据存储。

步骤 3 选择媒体虚拟机的虚拟机端口组。
Cisco 建议您选择与为管理虚拟机所选端口组相同的端口组。

步骤 4 选择**下一步**。

输入媒体虚拟机的联网信息

Cisco WebEx Meetings Server 通过输入媒体虚拟机的标准域名来尝试填充联网信息。

注释 媒体虚拟机必须和管理虚拟机位于相同的子网。 请勿编辑媒体虚拟机的域名、IPv4 网关、子网掩码或 DNS 服务器。

步骤 1 输入媒体虚拟机的 FQDN。
您应该已经输入 DNS 服务器中的媒体虚拟机的主机名和 IP 地址。 Cisco WebEx Meetings Server 将查找并填充 **IPv4 地址**。

步骤 2 选择**下一步**。

添加公开访问

如果您通过使用 IRP 添加了公开访问，防火墙外面的用户可以通过互联网或移动设备主持或出席会议。 IRP 虚拟机可以基于每数据中心随时添加至系统中。 在多数据中心 (MDC) 环境中添加 IRP 至一个数据中心中可以使防火墙外的用户访问整个系统。 要阻止外部访问，必须从系统中删除所有 IRP 虚拟机。

出于安全性原因，我们建议您将互联网反向代理与管理虚拟机置于不同的子网中。 这将确保在互联网反向代理与内部虚拟机（管理虚拟机和媒体虚拟机，如适用）之间的网络级别隔离。

在多数据中心 (MDC) 环境中，数据中心无法扩展、升级或更新。 备用数据中心必须从 MDC 中删除，使其成为单数据中心 (SDC) 环境。 修改数据中心并且验证数据中心大小和版本匹配之后，可以还原 MDC 环境。

开始之前

不必将存储服务器连接到互联网反向代理 (IRP) 服务器。

如果管理虚拟机和 IRP 虚拟机之间存在防火墙，必须允许临时 IP 地址穿越防火墙。

步骤 1 选择外部用户是否可以主持或出席会议。

- 如果您想要添加公开访问，确认已选择**创建互联网反向代理虚拟机**。
- 如果您只想让内部用户（公司防火墙内的用户）主持或出席会议，请取消选中**创建互联网反向代理虚拟机**。

步骤 2 选择**下一步**。

接下来的操作

- 有公开访问： 选择互联网反向代理 (IRP) 的 vCenter 设置，第 24 页
- 没有公开访问： 输入专用 VIP 地址，第 26 页
- 对于 IPv6 客户端连接： 配置 IPv6 客户端连接，第 132 页

选择互联网反向代理 (IRP) 的 vCenter 设置

开始之前

验证 VMware vCenter 所需的防火墙端口处于打开状态，以便 vCenter 可以部署互联网反向代理 (IRP) 虚拟机。 有关所需防火墙端口的更多信息，请参阅《*Cisco WebEx Meetings Server* 规划指南》。

步骤 1 从下拉列表中选择 IRP 虚拟机的 ESXi 主机。

步骤 2 选择用于 IRP 的数据存储。

步骤 3 选择虚拟机端口组。

步骤 4 选择**下一步**。

输入互联网反向代理 (IRP) 的联网信息

步骤 1 在 DNS 中输入互联网反向代理 (IRP) 服务器的主机名和 IP 地址，以启用从外部网络查找功能。
如果拥有启用从外部网络查找功能的 DNS 服务器，同样也将 IRP 服务器的主机名和 IP 地址添加到这些 DNS 服务器中。 这样即可在内部虚拟机与 IRP 服务器之间建立安全连接。

步骤 2 输入以下内容：
如果在 DNS 服务器中输入了互联网反向代理虚拟机的主机名和 IP 地址，那么我们就会查找并填充 **IPv4 地址**字段。

- 标准域名（FQDN）
- IPv4 网关
- IPv4 子网掩码
- 首选 DNS 服务器 IPv4 地址
- （可选）备用 DNS 服务器 IPv4 地址

步骤 3 选择**下一步**。

输入公共 VIP 地址

- 该公共 VIP 地址必须从互联网和内部网络（仅限水平分割 DNS）都可见。
- 此公共 VIP 地址必须和互联网反向代理位于相同的子网。
- 如果没有水平分割 DNS，那么所有用户均使用公共 VIP 地址来主持和出席会议。
- 如果有水平分割 DNS 并且已添加公开访问，那么外部用户将使用公共 VIP 地址来主持和出席会议。

有关非水平分割与水平分割 DNS 以及公开访问的更多信息，请参阅《*Cisco WebEx Meetings Server* 规划指南》。

注释 如果您正在创建高可用性 (HA) 系统，则无需重新输入此信息（我们会使用您输入的主系统信息）。

- 输入公共 VIP IPv4 地址并选择**下一步**。

输入专用 VIP 地址

管理员从映射至专用 VIP 地址的管理站点 URL 对系统进行配置、监控和维护。

如果拥有水平分割 DNS，那么内部用户也使用专用 VIP 地址来主持和出席会议。

如果要添加高可用性 (HA) 系统，则无需重新输入此信息；我们会使用您输入的主系统信息。

开始之前

专用虚拟 IP (VIP) 地址必须与内部虚拟机（管理虚拟机和媒体虚拟机，如适用）在相同的子网上。

- 输入 IPv4 专用 VIP 地址，然后选择**下一步**。

WebEx 站点和 WebEx 管理 URL

WebEx 站点 URL

用户可访问 WebEx 站点 URL 以安排、主持或出席会议。 根据您是否使用水平分割 DNS，此 URL 将解析为专用 VIP 地址或公用 VIP 地址。

- 如果您没有水平分割 DNS，它会为所有用户解析为公共 VIP 地址。
- 如果您有水平分割 DNS，则对外部用户将解析为公用 VIP 地址。
- 如果您有水平分割 DNS，则对内部用户会解析为专用 VIP 地址。

注释 必须对 WebEx 站点 URL 打开端口 80 和 443。

WebEx 管理 URL

管理员可访问 WebEx 管理 URL 以配置、管理和监控系统。 该 URL 将解析到专用 VIP 地址。

注释 必须对 WebEx 管理 URL 打开端口 80 和 443。

WebEx 站点和 WebEx 管理 URL 的名称

几乎可以为这些 URL 选择任何由全小写字符组成的名称。 但是，不能使用下列名称作为 URL 中的主机名：

- 与系统中任何虚拟机的主机名相同的名称
- authentication
- client

- companylogo
- dispatcher
- docs
- elm-admin
- elm-client-services
- emails
- maintenance
- Manager
- orion
- oriondata
- oriontemp
- NBR
- npp
- probe
- reminder
- ROOT
- solr
- TomcatROOT
- upgradeserver
- url0107ld
- version
- WBXService
- WebEx

输入 WebEx 公共站点和管理站点 URL

公共站点 URL 允许用户安排和主持会议，以及访问会议录制文件。 管理站点 URL 用于管理系统。 如果是添加高可用性 (HA) 系统，则无需重新输入此信息；主系统 URL 应与 HA 系统 URL 匹配。（有关 URL 的说明，请参阅系统部署的一般概念，第 12 页。）

步骤 1 输入 WebEx 公共站点和 WebEx 管理站点的安全 (http) URL。
WebEx 公共站点 URL 必须不同于 WebEx 管理 URL。

请勿在 WebEx URL 的主机名部分重复使用虚拟机的主机名。

步骤 2 选择**下一步**。

确认网络配置正确

此屏幕提供系统所需网络更改的在线帮助链接。 在线帮助提供有关 DNS 服务器更改和防火墙设置的详细信息。

您必须更改 DNS 服务器和防火墙，以允许我们测试网络连接。

如果您尚未进行此设置，请完成网络配置，然后选择**下一步**。

如果要测试自动部署，当您选择**下一步**时，我们部署您系统所需的虚拟机。

如果要测试手动部署，则输入虚拟机的主机名并部署它们（如果您尚未部署它们）。

部署完成后，通过启动并验证所有虚拟机启动开机对其进行测试。

部署虚拟机

我们根据您之前输入的信息部署系统所需的虚拟机。

只需几分钟即可完成部署。 请勿离开此页面，直到所有虚拟机已部署和启动（或者系统显示错误消息指示部署失败）。

状态栏全部显示绿色勾选标记时，部署成功完成。 选择**下一步**。

如指示错误，请修复错误，然后选择**下一步**以重新部署系统。 您可以选择**下载日志文件**，以获取此部署的日志文件。 此日志提供了部署记录，可用于对失败的部署进行诊断。

注释 重新部署系统之前，请确保关闭并删除错误所涉及的任意虚拟机；否则，重新部署期间，您可能会看到有关现有虚拟机的错误消息。

检查系统

系统检查会验证系统的配置参数。 这包括确认虚拟机是否具备所需的最低配置，并验证 WebEx 站点和 WebEx 管理 URL。

只需几分钟即可完成系统检查。 在所有检查成功完成前，切勿离开此页面，否者系统检查会失败，并显示指示该问题的错误消息。

如果在检查完成前重新加载该页，您会返回至此次系统部署的第一页。 检查成功完成后，系统会显示配置实用工具的第一页。

部署过程中使用的管理站点 URL 是管理虚拟机的主机名。 在基本配置期间，主机名会替换为管理站点 URL。 因此，首次登录管理站点时，系统可能提示您接受证书例外。

- 完成以下任一操作：

  如果没有错误，并且状态全部显示绿色复选标记，则选择**下一步**并参阅配置电子邮件 (SMTP) 服务器，第 47 页。 在极少数情况下，系统会显示**未测试**。 这并不意味着虚拟机存在问题。它只是指示系统检查未完成；例如，因为网络连接临时丢失，可能会显示该条目。 完成部署后，您可以登录管理站点并检查这些资源。

  如果存在网络连接问题，请验证正确输入了 WebEx 站点 URL、管理 URL 和 IP 地址。 验证这些站点位于同一子网中，以及在 DNS 服务器中正确输入了参数。

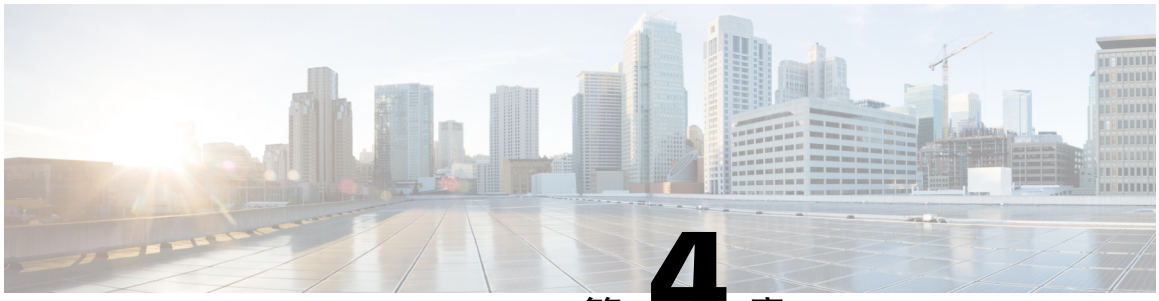
  如果系统会议最低系统容量存在问题，那么您有两个选择：

  从 VMware vCenter 关闭所有虚拟机，然后手动进行删除。 然后在系统上使用符合或超过最低要求的资源重新尝试部署系统。

  继续进行当前安装。 如果选择这样做，您必须确认放弃请求 Cisco 提供技术支持的权利。 通过选中错误消息复选框进行确认，然后选择**下一步**。

  如果一个或多个虚拟机存在任何问题，请使用 VMware vCenter 关闭有错误的虚拟机，然后手动删除这些虚拟机。 修复问题，然后重试系统部署。

- 选择**继续**以转至基本配置，在该处开始设置邮件服务器（配置电子邮件 (SMTP) 服务器，第 47 页）并标识管理员（创建管理员帐户，第 49 页）。 如果其他管理员将完成基本配置，请将此 URL 发送给该管理员。



第 4 章

手动部署系统

- 系统部署的一般概念， 第 31 页
- 安装核对表， 第 34 页
- 手动部署所需的信息， 第 35 页
- 从 VMware vSphere 客户端部署 OVA 文件， 第 36 页
- 选择安装向导语言， 第 38 页
- 确认部署， 第 39 页
- 确认系统容量， 第 39 页
- 选择要安装的系统， 第 39 页
- 选择部署类型， 第 40 页
- 添加公开访问， 第 40 页
- 输入公共 VIP 地址， 第 42 页
- 输入专用 VIP 地址， 第 42 页
- WebEx 站点和 WebEx 管理 URL， 第 43 页
- 输入 WebEx 公共站点和管理站点 URL， 第 44 页
- 确认网络配置正确， 第 44 页
- 部署虚拟机， 第 45 页
- 检查系统， 第 45 页

系统部署的一般概念

系统容量

系统由支持的并发用户数识别：

- 50 个并发用户（又称为微型系统）

  通常支持员工数为 500-1000 的公司

  主系统 [（不带高可用性 (HA)）] 拥有一个管理虚拟机和一个可选的互联网反向代理（用于公开访问）

- 250 个并发用户（又称为小型系统）

  通常支持员工数为 2500-5000 的公司

  主系统（无HA）拥有一个管理虚拟机、一个媒体虚拟机和一个可选的互联网反向代理（用于公开访问）

- 800 个并发用户（又称为中型系统）

  通常支持员工数为 8000-16000 的公司

  主系统（无HA）拥有一个管理虚拟机、一个媒体虚拟机和一个可选的互联网反向代理（用于公开访问）

- 2000 个并发用户（又称为大型系统）

  通常支持员工数为 20000-40000 的公司

  主系统（无 HA）拥有 1 个管理虚拟机、3 个媒体虚拟机、2 个 Web 虚拟机和 1 个可选的互联网反向代理（用于公开访问）

部署期间使用的术语

WebEx 站点 URL — 供用户在单数据中心环境中主持和出席会议的安全 http URL。

WebEx 管理 URL — 供管理员在单数据中心环境中配置、监控和管理系统的安全 http URL。

公共 VIP - 用于 WebEx 站点 URL 的虚拟 IP 地址。

专用 VIP — 用于管理站点 URL 的虚拟 IP 地址或用于 WebEx 站点 URL 的虚拟 IP 地址（仅适用于内部用户，如有水平分割 DNS）。

WebEx 公共 URL — 由 DNS 用于将用户重定向至数据中心，用户在该处执行会议相关任务，例如安排或主持会议。 DNS 选择哪个数据中心对用户而言是透明的。 WebEx 公共 URL 只是用户进入系统的一个便利位置。 如果数据中心停机，对用户而言没有变化，包括对用于访问会议的 URL 也没有变化，因为 DNS 会将用户重定向至续存数据中心。

管理公共 URL — 通常简称为管理 *URL*。 DNS 将其用于把管理员重定向至管理数据中心，管理员在其中登录系统。 DNS 选择哪个数据中心对管理员而言是透明的（但是，URL 栏中的字符串会根据管理员用来访问系统的数据中心而变化）。 管理公共 URL 只是管理员用于进入系统的一个便利目标。

管理本地 URL — 特定于多数据中心 (MDC) 系统中的各个数据中心。 通过管理公共 URL 登录时，DNS 将管理员重定向至管理数据中心的管理本地 URL。 向用户分配许可证之类的任意系统修改都将在管理数据中心中执行，并复制到 MDC 系统的所有数据中心中。

管理员可以从CWMS应用程序中选择具体的数据中心进行修改，但是选择其他数据中心进行修改不会更改管理本地URL，因为管理员对系统的访问保持为管理员登录系统时DNS所选择的数据中心。管理员在 MDC 系统中对其他数据中心所作的修改将由 DNS 所选择的管理数据中心传递至目标数据中心。

MDC 系统将至少有两个管理本地 URL，系统中的每个数据中心各一个。

本地 URL 特定于每个数据中心。

系统配置文件信息

请针对您的系统填写下表。

公共站点 URL		
公共管理 URL		
DC1 和 DC2 虚拟 IP 地址		
	数据中心 1	**数据中心 2**
本地站点 URL		
本地管理员 URL		
公共虚拟 IP 地址		
专用虚拟 IP 地址		
DNS 服务器		
管理虚拟机 IP 地址		
媒体虚拟机 IP 地址 1		
媒体虚拟机 IP 地址 2		
媒体虚拟机 IP 地址 3		
Web 虚拟机 IP 地址 1		
Web 虚拟机 IP 地址 2		
DMZ 虚拟机 IP 地址（可选）		
CWMS 管理员电子邮件地址		
密码		

Remote Access[2]		
密码		
Call Manager IP 地址		
Cisco Call Manager 管理员标识		
Cisco Call Manager 密码		
CWMS 拨入号码		
电话号码		

2 远程访问帐户未启用，直到帐户激活。

安装核对表

限制 您必须使用 VMware vCenter 来管理在其中部署 Cisco WebEx Meetings Server 系统的 ESXi 主机。

网络更改

请参阅与部署相应的网络核对表。 考虑以下因素：

- 公开访问： 防火墙以外的用户是否能从互联网或移动设备主持和访问会议

  Cisco 建议公开访问，因为这会给移动办公的员工带来更好的用户体验。
- 贵公司的 DNS 设置类型： 水平分割 DNS 或非水平分割 DNS（最常见的 DNS 配置）。 有关 DNS 设置的更多信息，请参阅《*Cisco WebEx Meetings Server* 规划指南》。
- 从管理虚拟机的管理员桌面打开端口 10200。 Web 浏览器在部署过程中使用端口 10200。

选择与部署相应的核对表：

- 启用公开访问和具有非水平分割 DNS 的系统的联网清单
- 禁止公开访问的系统的联网清单
- 启用公开访问和具有水平分割 DNS 的系统的联网清单

必填信息

如果使用自动部署（支持 50 个并发用户、250 个并发用户和 800 个并发用户）系统或手动部署（支持所有系统容量），所需信息会有所不同。 我们建议选择自动部署，除非部署的是始终需要手动部署的 2000 个用户的系统。

选择与部署类型相应的核对表：

- 自动部署所需的信息，第 15 页
- 手动部署所需的信息，第 35 页

手动部署所需的信息

在手动部署过程中，您可以从 vSphere 客户端使用 OVA 向导来为系统创建所有虚拟机。 然后可以通过手动部署安装系统。

如果您准备部署 2000 个用户的系统，则必须选择手动部署。

注释 确保在开始系统部署之前将虚拟机 FQDN、IP 地址、WebEx 和管理站点 URL 以及 VIP 地址添加至 DNS 服务器。 我们将在部署结束后使用此信息来检查网络连接。

为避免任何 DNS 问题，您可能要在开始 OVA 部署之前测试这些 URL 和 IP 地址。 否则，部署将失败，直至您更正这些错误。

以下依次为系统所需的信息。

字段名	描述	您的系统的值
公共 VIP	WebEx 站点 URL 的 IP 地址（站点用户访问该地址以主持和出席会议）	
专用 VIP	• 管理站点 URL 的 IP 地址（供管理员配置、监控和管理系统） • WebEx 站点 URL 的 IP 地址（仅供内部用户使用，前提是您有水平分割 DNS）。	
WebEx 站点 URL	供用户主持和参加会议的安全 http URL（全小写字符）。	
WebEx 管理 URL	供管理员配置、监控和管理系统的安全 http URL（全小写字符）。	
内部虚拟机的 FQDN	根据您选择的系统容量，输入媒体和 Web 虚拟机的标准域名（全小写字符）。	
（仅限公开访问） 互联网反向代理的 FQDN	如果您计划添加公开访问，那么需要输入互联网反向代理虚拟机的标准域名（全小写字符）。	

后续步骤

按照此信息在浏览器窗口输入部署 URL 开始部署系统。（管理虚拟机的控制台窗口中会写入部署 URL。）

注释 如果在配置完成之前重新启动系统，会生成新的密码，您必须搭配新的密码使用部署 URL。

从 VMware vSphere 客户端部署 OVA 文件

OVA 模板为每个虚拟机创建两个虚拟 NIC。 但是，只有管理虚拟机会同时使用这两个虚拟 NIC。 对于所有其他 Cisco WebEx Meetings Server (CWMS) 虚拟机，只使用一个虚拟 NIC，而另一个会断开连接。

此步骤提供作为一般指导。 在部署 OVA 过程中看到的屏幕取决于您的 vCenter、存储空间以及网络配置，可能与此步骤中所述的不一样。 查看 VMware vSphere 文档，获取有关 OVA 向导的完整信息。

开始之前

获取 Cisco WebEx Meetings Server 系统 OVA 文件并将其置于可从 VMware vSphere 进行访问的位置。 使用 VMware vSphere 客户端部署用于您系统的管理虚拟机。

您必须使用 VMware vCenter 来管理在其中部署 Cisco WebEx Meetings Server 系统的 ESXi 主机。 使用 vSphere 客户端登录 vCenter 并部署管理虚拟机的 OVA 文件。

步骤 1 登录 VMware vSphere 客户端。
确保以拥有管理员权限的用户身份登录： 用于部署、配置、启动、关闭和删除虚拟机。

步骤 2 选择**文件** > **部署 OVF 模板...**

步骤 3 选择**浏览**以导航到保存 OVA 文件的位置。 选择**下一步**。
您可以选择 **Cisco WebEx Meetings Server** 链接，转至含有此系统详细信息的网页。

步骤 4 阅读最终用户许可协议并选择**接受**，然后选择**下一步**。

步骤 5 导航至 vCenter 目录并选择要放置管理虚拟机的位置。

步骤 6 根据系统容量输入虚拟机的名称，然后选择**下一步**。 关于为系统选择正确大小的更多信息，请参阅系统容量，第 12 页。
必须先部署管理虚拟机，然后才能部署任何其他虚拟机。 如果您选择自动部署（推荐使用），我们将为您部署其他虚拟机。 如果您选择手动部署（支持 2000 个并发用户的系统需要使用此方式），那么在完成对管理虚拟机的部署后，您必须使用同一向导部署其他虚拟机。

Cisco 建议您将类型包含在虚拟机名称中；例如，将“管理”包含在管理虚拟机名称中，以便在 vCenter 清单中轻松找到管理虚拟机。

系统所有的内部虚拟机必须和管理虚拟机位于同一子网。（根据您选择的系统容量，可能需要一个或多个媒体和 Web 内部虚拟机。）

步骤 7 根据系统容量从下拉列表中选择虚拟机，并选择**下一步**。
在系统中部署任何其他虚拟机前，确保先部署管理虚拟机。

步骤 8 浏览 vCenter 清单并选择要部署系统虚拟机的 ESXi 主机或群集。 选择**下一步**。

步骤 9 如果群集包含资源池，则选择要在其中部署 OVA 模板的资源池，然后选择**下一步**。
资源池共享 CPU 和内存资源，或与 VMware 功能（例如 DRS 或 vMotion）配合使用。 资源池必须专供单个 ESXi 主机使用。 不建议 VMware 资源池用于 Cisco WebEx Meetings Server。

步骤 10 选择虚拟机数据存储和配置类型。
必须选择**密集配置**，并创建系统所需的最大虚拟磁盘空间。 如果选择精简配置，VMware 将根据需要分配文件系统空间，从而导致性能低下。 延迟置零已足够，也可使用积极置零，但积极置零需要更多时间来完成。

步骤 11 设置网络映射。 从**目标网络**列中的下拉列表中，为各个资源网络选择目标网络。 选择**下一步**。

注释 “VM Network”和“VIP Network”必须映射到“目标网络”列中的同一个值。 您可以忽略关于多源网络映射到同一主机网络的警告消息。

步骤 12 输入以下虚拟机信息，然后选择**下一步**：

- 虚拟机的主机名（这里不包括域）
- 虚拟机的域名
- 虚拟机的 IPv4 地址 (Eth0)
- 虚拟机的子网掩码
- 网关 IP 地址
- 包含此虚拟机的主机名和 IP 地址条目的首选 DNS 服务器
- 包含此虚拟机的主机名和 IP 地址条目的备用 DNS 服务器（仅配置一个 DNS 服务器的系统有风险，因为它产生了单点故障。 我们建议您配置一个备用 DNS 服务器，以产生网络冗余。）
- 此虚拟机开机后，安装过程中显示的语言

注释 为避免出现 DNS 问题，您可以在开始 OVA 部署之前测试 URL 和 IP 地址。 如有错误，部署将失败。

步骤 13 确认您输入的信息。 如有任何错误，请选择**上一步**，然后更改值。

步骤 14 如果要手动升级系统，选择**完成**，忽略此步骤的平衡，在手动升级系统，第 77 页中继续下一步。 （在部署升级系统之后，但是尚未启动时，应通过使用手动部署将原始系统的数据复制到升级系统中。） 否则，勾选**部署后启动**，然后选择**完成**。

步骤 15 如果您正在部署管理虚拟机，请转至 vCenter 并打开虚拟机控制台窗口。 开机后，我们将检查您在部署 OVA 的过程中输入的网络信息。
如果我们能够确认连通性，系统将显示绿色勾选标记。

如有问题，系统将显示红叉。 修复错误，然后重新尝试部署 OVA。

步骤 16 记下控制台窗口中显示的 URL（区分大小写）。
管理员使用此 URL 继续系统部署。

如果系统在配置完成之前重新启动，则将生成新密码，您必须通过该新密码使用 URL。

接下来的操作

如果您是手动执行部署，我们建议此时为系统部署剩余的虚拟机。 这样可避免诸如启动虚拟机时超时等问题。

如果部署成功，请继续在浏览器窗口中部署系统。

如果部署失败，请参阅OVA 部署失败后请检查联网配置，第 20 页。

OVA 部署失败后请检查联网配置

确认虚拟机的联网条目。

重要事项 请勿对系统中的任何虚拟机使用**编辑设置...**（除非在部署失败后使用）。 一旦系统开始运行，必须通过 WebEx 管理站点才能对虚拟机设置进行任何进一步的编辑。 如果您使用 vSphere 客户端，那么系统将不会接受所做的修改。

注释 更多详细步骤，请参阅 VMware vSphere 文档。

步骤 1 在 vSphere 客户端中，在虚拟机上选择**电源** > **关闭客户系统**。

步骤 2 在清单中查找虚拟机，然后右键单击**编辑设置...**。

步骤 3 选择**选项**标签页。

步骤 4 选择**属性**并确认已正确输入所有的联网信息。 若需要更改，请按正确的设置重新部署 OVA。
一个可能出现的网络问题是为 ESXi 主机设置的 VLAN 路由不正确。 由于虚拟机位于该 VLAN，无法进行网络连接。 通过 ESXi 主机所在的网络，您可以 Ping 将用于系统虚拟机的 VLAN 的缺省网关 IP 地址。

选择安装向导语言

确定用于安装系统的首选语言。

注释 切勿关闭浏览器窗口，直到系统部署完成。 如果提前关闭浏览器，可能需要重新开始部署。

升级至版本 2.5 之后，CWMS System是数据中心的缺省名称；它没有从英语翻译为任何其他语言。

开始之前

请确保已从 VMware vCenter 部署管理虚拟机。 请参阅 从 VMware vSphere 客户端部署 OVA 文件，第 18 页

步骤 1 从该下拉菜单中选择一个语言。

步骤 2 选择**下一步**。

确认部署

要确认部署新系统或者扩展现有系统，选择**下一步**。

确认系统容量

在使用 OVA 文件部署管理虚拟机时，您已选择系统容量。

- 确认在 OVA 部署过程中选中的系统容量是否正确。

  如果选中的系统容量是正确的，则选择**下一步**。

  如果选中的系统容量是错误的，则选择**我想更改系统容量**。

  a) 使用 VMware vSphere 客户端，对系统容量错误的管理虚拟机选择**电源** > **关闭客户系统**。
  b) 右键单击虚拟机，然后选择**从磁盘中删除**。
  c) 重新部署 OVA 文件，然后选择正确系统容量的管理虚拟机。

选择要安装的系统

步骤 1 确定安装类型。

- 如果您是首次安装此系统，请选择**安装主系统**。
- 如果您已安装主系统并且要添加冗余的高可用性 (HA) 系统，请选择**创建高可用性 (HA) 冗余系统**。

请勿尝试在安装主系统之前安装 HA 系统，因为只有在安装了主系统后才能使用 HA 系统。

步骤 2 选择**下一步**。

选择部署类型

您可以选择自动或手动部署系统虚拟机。 您可根据以下情形选择自动部署或手动部署：

- 如果时间有限，自动部署要比手动部署快。
- 如需逐步指导，自动部署期间提供此指导。
- 如果您对 VMware vCenter 很熟悉，并且不想提供 vCenter 凭证，请选择手动部署。

我们建议您选择**自动**，除非您部署的是始终需要手动部署的 2000 个用户的系统。

步骤 1 选择自动或手动部署：

- **自动**： 我们会部署系统所需的所有虚拟机。
- **手动**： 通过使用 VMware vCenter 可手动部署各个虚拟机。 回答几个有关系统的问题之后，会为您提供系统所需虚拟机的列表。

步骤 2 选择**下一步**。

添加公开访问

如果您通过使用 IRP 添加了公开访问，防火墙外面的用户可以通过互联网或移动设备主持或出席会议。 IRP 虚拟机可以基于每数据中心随时添加至系统中。 在多数据中心 (MDC) 环境中添加 IRP 至一个数据中心中可以使防火墙外的用户访问整个系统。 要阻止外部访问，必须从系统中删除所有 IRP 虚拟机。

出于安全性原因，我们建议您将互联网反向代理与管理虚拟机置于不同的子网中。 这将确保在互联网反向代理与内部虚拟机（管理虚拟机和媒体虚拟机，如适用）之间的网络级别隔离。

在多数据中心 (MDC) 环境中，数据中心无法扩展、升级或更新。 备用数据中心必须从 MDC 中删除，使其成为单数据中心 (SDC) 环境。 修改数据中心并且验证数据中心大小和版本匹配之后，可以还原 MDC 环境。

开始之前

不必将存储服务器连接到互联网反向代理 (IRP) 服务器。

如果管理虚拟机和 IRP 虚拟机之间存在防火墙，必须允许临时 IP 地址穿越防火墙。

步骤 1 选择外部用户是否可以主持或出席会议。

- 如果您想要添加公开访问，确认已选择**创建互联网反向代理虚拟机**。

- 如果您只想让内部用户（公司防火墙内的用户）主持或出席会议，请取消选中**创建互联网反向代理虚拟机**。

步骤 2 选择**下一步**。

接下来的操作

- 有公开访问： 选择互联网反向代理 (IRP) 的 vCenter 设置，第 24 页
- 没有公开访问： 输入专用 VIP 地址，第 26 页
- 对于 IPv6 客户端连接： 配置 IPv6 客户端连接，第 132 页

选择互联网反向代理 (IRP) 的 vCenter 设置

开始之前

验证 VMware vCenter 所需的防火墙端口处于打开状态，以便 vCenter 可以部署互联网反向代理 (IRP) 虚拟机。 有关所需防火墙端口的更多信息，请参阅《*Cisco WebEx Meetings Server* 规划指南》。

步骤 1 从下拉列表中选择 IRP 虚拟机的 ESXi 主机。

步骤 2 选择用于 IRP 的数据存储。

步骤 3 选择虚拟机端口组。

步骤 4 选择**下一步**。

输入互联网反向代理 (IRP) 的联网信息

步骤 1 在 DNS 中输入互联网反向代理 (IRP) 服务器的主机名和 IP 地址，以启用从外部网络查找功能。
如果拥有启用从外部网络查找功能的 DNS 服务器，同样也将 IRP 服务器的主机名和 IP 地址添加到这些 DNS 服务器中。 这样即可在内部虚拟机与 IRP 服务器之间建立安全连接。

步骤 2 输入以下内容：
如果在 DNS 服务器中输入了互联网反向代理虚拟机的主机名和 IP 地址，那么我们就会查找并填充 **IPv4 地址**字段。

- 标准域名（FQDN）
- IPv4 网关
- IPv4 子网掩码

- 首选 DNS 服务器 IPv4 地址
- （可选）备用 DNS 服务器 IPv4 地址

步骤 3 选择**下一步**。

输入公共 VIP 地址

- 该公共 VIP 地址必须从互联网和内部网络（仅限水平分割 DNS）都可见。
- 此公共 VIP 地址必须和互联网反向代理位于相同的子网。
- 如果没有水平分割 DNS，那么所有用户均使用公共 VIP 地址来主持和出席会议。
- 如果有水平分割 DNS 并且已添加公开访问，那么外部用户将使用公共 VIP 地址来主持和出席会议。

有关非水平分割与水平分割 DNS 以及公开访问的更多信息，请参阅《*Cisco WebEx Meetings Server* 规划指南》。

注释 如果您正在创建高可用性 (HA) 系统，则无需重新输入此信息（我们会使用您输入的主系统信息）。

- 输入公共 VIP IPv4 地址并选择**下一步**。

输入专用 VIP 地址

管理员从映射至专用 VIP 地址的管理站点 URL 对系统进行配置、监控和维护。

如果拥有水平分割 DNS，那么内部用户也使用专用 VIP 地址来主持和出席会议。

如果要添加高可用性 (HA) 系统，则无需重新输入此信息；我们会使用您输入的主系统信息。

开始之前

专用虚拟 IP (VIP) 地址必须与内部虚拟机（管理虚拟机和媒体虚拟机，如适用）在相同的子网上。

- 输入 IPv4 专用 VIP 地址，然后选择**下一步**。

WebEx 站点和 WebEx 管理 URL

WebEx 站点 URL

用户可访问 WebEx 站点 URL 以安排、主持或出席会议。 根据您是否使用水平分割 DNS，此 URL 将解析为专用 VIP 地址或公用 VIP 地址。

- 如果您没有水平分割 DNS，它会为所有用户解析为公共 VIP 地址。
- 如果您有水平分割 DNS，则对外部用户将解析为公用 VIP 地址。
- 如果您有水平分割 DNS，则对内部用户会解析为专用 VIP 地址。

注释 必须对 WebEx 站点 URL 打开端口 80 和 443。

WebEx 管理 URL

管理员可访问 WebEx 管理 URL 以配置、管理和监控系统。 该 URL 将解析到专用 VIP 地址。

注释 必须对 WebEx 管理 URL 打开端口 80 和 443。

WebEx 站点和 WebEx 管理 URL 的名称

几乎可以为这些 URL 选择任何由全小写字符组成的名称。 但是，不能使用下列名称作为 URL 中的主机名：

- 与系统中任何虚拟机的主机名相同的名称
- authentication
- client
- companylogo
- dispatcher
- docs
- elm-admin
- elm-client-services
- emails
- maintenance
- Manager
- orion

- oriondata
- oriontemp
- NBR
- npp
- probe
- reminder
- ROOT
- solr
- TomcatROOT
- upgradeserver
- url0107ld
- version
- WBXService
- WebEx

输入 WebEx 公共站点和管理站点 URL

公共站点 URL 允许用户安排和主持会议，以及访问会议录制文件。 管理站点 URL 用于管理系统。如果是添加高可用性 (HA) 系统，则无需重新输入此信息；主系统 URL 应与 HA 系统 URL 匹配。（有关 URL 的说明，请参阅系统部署的一般概念，第 12 页。）

步骤 1 输入 WebEx 公共站点和 WebEx 管理站点的安全 (http) URL。
WebEx 公共站点 URL 必须不同于 WebEx 管理 URL。

请勿在 WebEx URL 的主机名部分重复使用虚拟机的主机名。

步骤 2 选择**下一步**。

确认网络配置正确

此屏幕提供系统所需网络更改的在线帮助链接。 在线帮助提供有关 DNS 服务器更改和防火墙设置的详细信息。

您必须更改 DNS 服务器和防火墙，以允许我们测试网络连接。

如果您尚未进行此设置，请完成网络配置，然后选择**下一步**。

如果要测试自动部署，当您选择**下一步**时，我们部署您系统所需的虚拟机。

如果要测试手动部署，则输入虚拟机的主机名并部署它们（如果您尚未部署它们）。

部署完成后，通过启动并验证所有虚拟机启动开机对其进行测试。

部署虚拟机

提供有关系统中的虚拟机信息后，我们将尝试连接到各个已部署的系统虚拟机。

注释 在系统连接到所有虚拟机前，切勿离开此页。如果连接失败将出现表示问题的错误消息。

步骤 1 输入系统需要的其他任何虚拟机的标准域名 (FQDN)。（您之前在从 OVA 文件进行部署时输入了管理虚拟机 FQDN。）

步骤 2 如果尚未执行该操作，请使用 VMware vCenter 部署系统所需的所有其他虚拟机。

步骤 3 将这些虚拟机全部启动，并验证它们已成功启动。 然后选择**检测虚拟机**。
我们会建立这些虚拟机的连接。 这可能需要几分钟时间。

步骤 4 请稍等，直到每个虚拟机的状态均显示为**已连接**，然后完成以下操作之一：

- 如果没有错误，状态将全部显示绿色勾选标记。 如果您到目前为止对配置感到满意，请选择**下一步**。 否则，您可以通过再次选择**检测虚拟机**，更改虚拟机的 FQDN。
- 如有错误，请修复错误，然后选择**下一步**以继续操作。
  注释 您可以选择**下载日志文件**，以获取此部署的日志文件。此日志提供了记录，可用于对失败的部署进行诊断。
- 如果一个或多个虚拟机存在其他问题，请从 VMware vCenter 关闭这些有错误的虚拟机，然后手动删除这些虚拟机。（如果您未删除它们，可能会看到有关这些虚拟机的错误消息。） 在问题修复后，从 OVA 文件重新部署虚拟机，然后选择**检测虚拟机**。

检查系统

系统检查会验证系统的配置参数。 这包括确认虚拟机是否具备所需的最低配置，并验证 WebEx 站点和 WebEx 管理 URL。

只需几分钟即可完成系统检查。 在所有检查成功完成前，切勿离开此页面，否者系统检查会失败，并显示指示该问题的错误消息。

如果在检查完成前重新加载该页，您会返回至此次系统部署的第一页。 检查成功完成后，系统会显示配置实用工具的第一页。

部署过程中使用的管理站点 URL 是管理虚拟机的主机名。 在基本配置期间，主机名会替换为管理站点 URL。 因此，首次登录管理站点时，系统可能提示您接受证书例外。

- 完成以下任一操作：

  如果没有错误，并且状态全部显示绿色复选标记，则选择**下一步**并参阅配置电子邮件 (SMTP) 服务器，第 47 页。 在极少数情况下，系统会显示**未测试**。 这并不意味着虚拟机存在问题。它只是指示系统检查未完成；例如，因为网络连接临时丢失，可能会显示该条目。 完成部署后，您可以登录管理站点并检查这些资源。

  如果存在网络连接问题，请验证正确输入了 WebEx 站点 URL、管理 URL 和 IP 地址。 验证这些站点位于同一子网中，以及在 DNS 服务器中正确输入了参数。

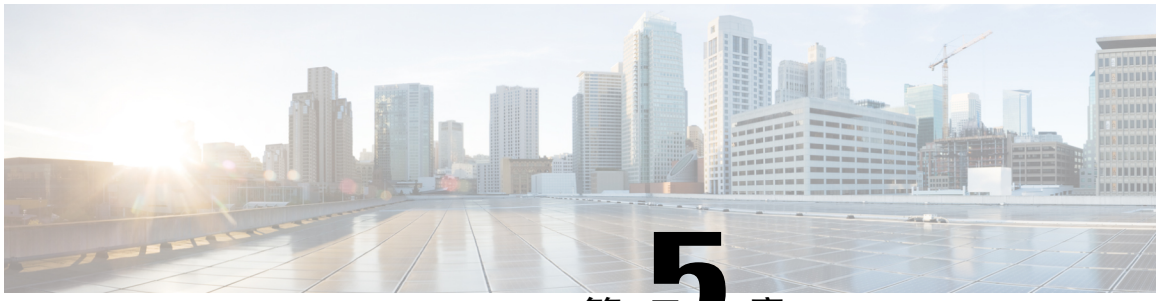
  如果系统会议最低系统容量存在问题，那么您有两个选择：

  从 VMware vCenter 关闭所有虚拟机，然后手动进行删除。 然后在系统上使用符合或超过最低要求的资源重新尝试部署系统。

  继续进行当前安装。 如果选择这样做，您必须确认放弃请求 Cisco 提供技术支持的权利。 通过选中错误消息复选框进行确认，然后选择**下一步**。

  如果一个或多个虚拟机存在任何问题，请使用 VMware vCenter 关闭有错误的虚拟机，然后手动删除这些虚拟机。 修复问题，然后重试系统部署。

- 选择**继续**以转至基本配置，在该处开始设置邮件服务器（配置电子邮件 (SMTP) 服务器，第 47 页）并标识管理员（创建管理员帐户，第 49 页）。 如果其他管理员将完成基本配置，请将此 URL 发送给该管理员。



第 5 章

配置邮件服务器、时区和区域设置

- 配置电子邮件 (SMTP) 服务器， 第 47 页
- 设置时区、语言和区域设置， 第 48 页
- 创建管理员帐户， 第 49 页
- 关于系统测试， 第 50 页

配置电子邮件 (SMTP) 服务器

配置电子邮件服务器可使系统能向用户发送会议邀请和其他通信。

务必要保证电子邮件服务器始终可运行。 电子邮件是与用户通信的主要方式，这些通信包括录制文件通知、会议信息更改、帐户状态和许多其他重要公告。 （另请参阅添加用户， 第 115 页。）

重要事项 用户在系统中由电子邮件地址进行识别。 如果用户电子邮件地址被更改并且用户保持活动，则 CWMS 上的电子邮件地址也必须更改，否则该用户将无法接收通知。

注释 更改这些属性不需要开启维护模式。

步骤 1 登录管理网站。

步骤 2 选择**系统**，然后在服务器部分选择**查看更多内容**。

步骤 3 在**SMTP 服务器**部分，选择**编辑**。

步骤 4 输入系统将用于发送电子邮件的邮件服务器的标准域名（FQDN）。

步骤 5 （可选） 选择**启用 TLS** 以启用传输层安全性 (TLS)。（缺省情况下已启用基本验证。）

步骤 6 （可选） 编辑**端口**字段以更改缺省值。
SMTP 缺省端口号为 25 或 465（安全 SMTP 端口）。

注释 Web 节点和管理节点会将 SMTP 请求发送到已配置的电子邮件服务器。 如果在内部 Web 及管理虚拟机与电子邮件服务器之间有防火墙，则SMTP通信可能被拦截。要确保电子邮件服务器配置和电子邮件通知正常工作，必须在电子邮件服务器与 Web 及管理虚拟机之间打开端口 25 或 465（安全 SMTP 端口号）。

步骤 7 （可选） 要启用邮件服务器验证，选择**启用服务器验证**。 如果您启用了验证，输入系统访问公司邮件服务器所需的**用户名**和**密码**凭证。
系统电子邮件的发件人为 admin@<WebEx-site-URL>。 请确保邮件服务器能够识别出该用户。

对于微型、小型或中型系统，电子邮件通知来自管理虚拟机（主系统或高可用性系统）。

对于大型系统，电子邮件通知来自 Web 虚拟机（主系统或高可用性系统上）。 在大型系统中，主系统上存在三个 Web 虚拟机，高可用性系统上存在一个 Web 虚拟机。

步骤 8 选择**保存**。

接下来的操作

另请参阅从用户页面激活或停用用户和管理员，第 117 页、添加用户，第 115 页和编辑用户，第 115 页。

设置时区、语言和区域设置

开始之前

如果您运行 Windows 7 并且在 Internet Explorer 10 浏览器中打开 Cisco WebEx 站点，那么您可能要选择文档 Internet Explorer 10 标准，以确保应用程序中的所有按钮正常工作。

- 选择**工具** > **开发者工具**。
- 在“开发者工具”窗口的顶部，选择**文档模式： IE7 标准** > **Internet Explorer 10 标准**。

步骤 1 从管理网站，导航至**设置** > **公司信息**

步骤 2 从下拉列表中选择此系统的本地**时区**。

步骤 3 选择**语言**。

步骤 4 选择国家/地区的**区域设置**。

步骤 5 选择**保存**。

创建管理员帐户

系统创建首个管理员帐户。此管理员必须登录系统，创建密码并添加其他管理员。在此之前，其他管理员均将无法访问系统。 在此过程中，首个管理员可以创建审核员帐户，将管理员和审核员分开。 这可以在部署过程中完成，或者首个管理员可以创建审核员（**用户** > **编辑用户**）。（请参阅添加审核员角色，第 49 页。）

开始之前

必须配置系统用于向管理员发送电子邮件的邮件服务器。 有关说明，请参阅配置电子邮件 (SMTP) 服务器，第 47 页。

步骤 1 输入该管理员的姓名。

步骤 2 输入管理员的完整电子邮件地址，然后再次输入以进行确认。

步骤 3 （可选） 选择**创建审核员帐户**以向系统中添加审核员。

步骤 4 选择**下一步**以创建初始密码。

步骤 5 输入密码，然后再次输入以进行确认。

步骤 6 选择**提交**以登录 WebEx 管理站点。

步骤 7 登录系统中并添加管理员和用户。 创建每个新帐户时，系统会向此人发送一封欢迎电子邮件，请该用户登录并更改初始密码。
首次登录时，每个管理员都提供有一个系统教程。 管理员可以立即查看教程或随需查看教程。

添加审核员角色

首个管理员缺省具有审核员角色，并且是唯一可以为其他用户激活审核员角色的人。 如果这样做，审核员权限会从首个管理员那里分离。 如果审核员也是系统管理员，则这个人具有系统审核角色。

审核员角色将下列管理操作与系统监控分开：

- 打开或关闭审核。
- 将 CWMS 配置为与远程系统日志服务器同步。
- 执行日志清除。
- 为日志分区配置警告。
- 生成日志捕获。
- 如果管理员和审核员角色未分开，仅管理员和主持人角色存在；管理员拥有全部权限。

- 如果管理员和审核员角色在系统部署时分开，会创建首个管理员角色（被称为应急帐户）。 系统部署之后，仅首个管理员应急帐户可以创建审核员，将审核员权限从管理员那里分离。 部署系统之后，首个管理员可以根据需要创建多个审核员。
- 审核员仅为本地的；它无法来自与任何外部用户群的同步。
- 审核员参数（例如姓名）可以修改，但是创建之后，审核员角色无法停用或重新分配给另一个用户标识。
- 审核员无法修改用户参数。
- 审核员没有主持人权限，无法通过使用审核员帐户安排会议。 审核员可以作为参加者出席会议。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**用户**。

步骤 3 选择用户。
系统将弹出**编辑用户**窗口。

步骤 4 选择**审核员**帐户类型。

步骤 5 选择**保存**。
系统会向审核员发送一封欢迎电子邮件。

关于系统测试

通过使用 CWMS 系统完成大多数系统测试，例如通过使用会议测试，第 82 页和使用系统资源测试，第 82 页。

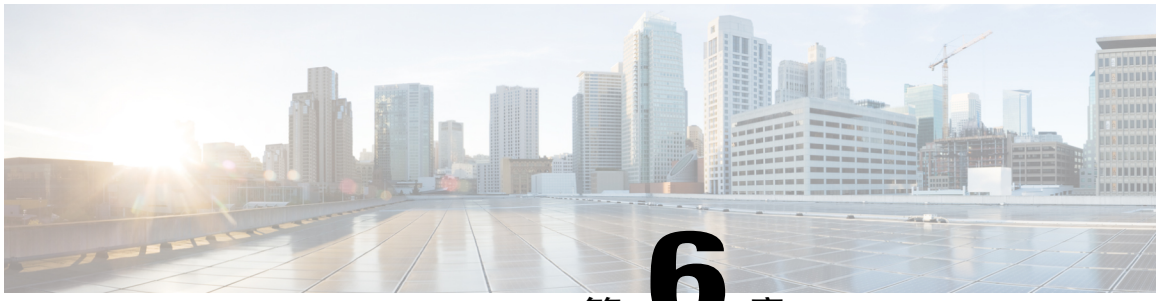
测试升级系统时，可以保留原始系统，直到已完成测试升级系统为止（但是由于它们共用 IP 地址之类的一些参数，因此不能同时启动两个系统）。 在对升级系统测试结果感到满意之后，可（永久）删除原始系统。 确保删除原始系统时升级系统已在运行。 这可以防止意外删除基本虚拟机磁盘 (VMDK) 文件，升级系统必须访问该文件。

建议在系统上运行一些测试：

- 添加、编辑、激活和停用用户。 （请参阅管理用户，第 105 页。）
- 安排和举行会议。
- 重新安排现有会议。
- 删除一系列安排的会议。
- 从会议邀请中添加和打开会议附件。
- 录制会议和播放录制文件。

系统也可以通过以下方式进行测试：

- 确认网络配置正确， 第 28 页
- 检查系统， 第 28 页
- 验证主系统和 HA 系统是同一版本
- 通过删除主系统物理连接确认主系统将故障转移至 HA 系统，并验证 Cisco WebEx 在 HA 系统上运行。



第 6 章

在部署后改动系统

本章概述了执行系统改动过程之前必要的准备工作：

- 更新系统， 第 67 页
- 升级系统， 第 73 页
- 扩大系统规模， 第 61 页

- 做好改动系统的过程的准备， 第 53 页

做好改动系统的过程的准备

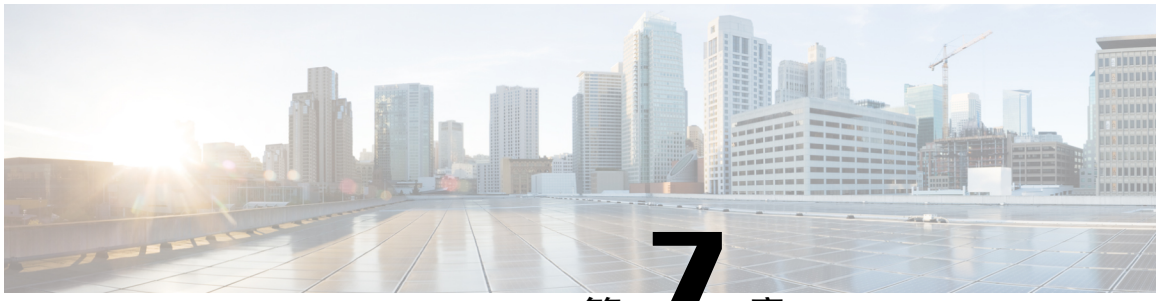
改动系统且需要由管理员进行事先准备的事件包括：

- 添加或删除高可用性 (HA) 系统。（请参阅添加高可用性系统， 第 55 页。）
- 将系统更新为较新的版本（使用 ISO 更新文件）。（请参阅准备更新现有系统。）
- 通过部署一个并行系统并将原系统数据传输到升级系统来升级系统（使用 ISO 更新文件）。（请参阅准备升级数据中心， 第 73 页。）
- 扩展系统容量。（请参阅准备系统扩展， 第 61 页。）

注释 由于这些过程需要对系统进行独占访问，因此用户无法访问系统以进行会议。 确保将此过程安排在对用户影响最小的时间段内。

在开始系统改动过程之前，必须与其他系统管理员进行协调。 其他系统管理员不应在此过程中访问系统。 如果他们这样做，则他们所作的更改不会得到保存，且可能造成不可预测的结果。

上述操作均无需进行备份。如果您不需要为虚拟机创建备份，则不需要完成该过程。但是，我们建议您创建备份，这是最佳的做法。 有关此备份的详细信息，请参阅通过使用 VMware vCenter 创建备份， 第 6 页、*VMware Data Recovery Administration Guide* 或 *vSphere Data Protection Administration Guide*。



第 7 章

添加高可用性系统

- 准备向系统中添加高可用性 (HA)，第 55 页
- 部署高可用性 (HA) 系统，第 56 页
- 将高可用性系统链接到主系统，第 57 页
- 发生组件故障后的高可用性系统行为，第 58 页
- 从系统中删除高可用性系统，第 59 页

准备向系统中添加高可用性 (HA)

高可用性 (HA) 系统是一个被创建然后添加到主系统中的本地冗余系统。 如果虚拟机发生故障，系统会故障转移至 HA 系统。

如果计划向系统中添加 HA，并且也计划更新系统，我们建议您在更新系统之前添加 HA，然后更新组合（主和 HA）系统；当主系统更新时，HA 系统会自动更新。 如果先更新主系统，然后添加 HA，则需要先单独部署然后更新 HA 系统（使主系统和 HA 系统的版本相同）。

HA 系统具有以下限制：

- 运行 HA 的系统无法加入多数据中心 (MDC)。（要删除 HA，请参阅从系统中删除高可用性系统，第 59 页。）
- HA 系统和主系统的容量必须相同。
- HA 系统的发行版本必须与主系统相同。

  如果您更新主系统，则必须更新 HA 系统。
- 如果主系统当前带有 HA 并且您要部署新的 HA 系统，那么您可能无法重用原始 HA 系统中的虚拟机。 请先删除旧的 HA 虚拟机，然后才能为新的 HA 系统部署新的虚拟机。
- 由于此过程会向系统中添加新虚拟机，所以您的当前安全证书会失效并需要更新的证书，除非您使用的是自签名证书。

- HA 系统必须使用与主系统相同的 OVA 和修补程序进行配置。 如果主系统和高可用性系统的版本不匹配，系统将指示您将两者升级到更高版本。
- HA 系统和主系统的内部虚拟机必须在同一子网上。
- 如果您已在主系统上添加了公开访问，则必须将其添加到 HA 系统上。 此外，HA 系统和主系统的互联网反向代理虚拟机必须处于同一子网上。

注释 HA 系统上的大多数功能会被禁用。 例如，您无权访问 HA 系统进行升级、配置 SNMP、访问存储，或配置电子邮件服务器。 您可以查看系统属性，但不能修改 HA 系统。

此外，负载平衡不可配置；它是自动的和系统内置的。

准备工作

将 HA 添加到主系统之前，应满足以下条件：

- 验证：

  目标主系统已部署并且不属于 MDC。

  虚拟机之间存在冗余网络。

  网络是 10gbps 高带宽网络。

  主系统和 HA 系统上已配置网络时间协议 (NTP)，并且时钟已同步。

- 创建主系统的备份。 请参阅通过使用 VMware vCenter 创建备份，第 6 页。
- 验证所有虚拟机都在正常运行。 如 关于控制板 中所述，通过查看系统监控器来确定虚拟机状态。
- 我们建议您在执行此过程前制作高可用性虚拟机的快照。 万一发生错误可以从快照重做该过程。
- 记录高可用性虚拟机的标准域名 (FQDN)；您必须知道 FQDN 才能向主系统添加高可用性。

部署高可用性 (HA) 系统

高可用性 (HA) 系统与主系统的部署类似，只是系统在部署期间将其标识为 HA 系统。 然后，HA 系统链接到主系统中，主系统会在发生故障的情况下使用 HA 系统进行恢复。 主系统故障对用户透明。

要向系统添加 HA，请执行以下操作：

步骤 1 使用自动部署系统，第 11 页或手动部署系统，第 31 页部署一个并行的系统。 该过程询问要部署主系统还是要部署 HA 时，选择 HA。

我们建议您使用与用于部署主系统的过程相同的过程部署 HA 系统。 如果您不知道使用了哪个过程部署主系统，则使用自动部署系统，第 11 页过程，除非要部署大型（2000 个并发用户）系统。 所有大型系统都需要手动部署系统，第 31 页。

步骤 2 验证 HA 和主系统版本匹配：

1. 在单独的浏览器窗口中，登录主系统 WebEx 管理站点。
2. 在**控制板**标签页上，验证**系统**窗格中的主系统版本号与 HA 的版本匹配。
   如果版本匹配，则继续操作。

   如果主系统的版本比 HA 系统的版本新，那么必须使用具有匹配软件版本的 OVA 文件重新部署 HA 系统，或者更新 HA 系统。

接下来的操作

通过使用将高可用性系统链接到主系统将 HA 系统链接到主系统中。

當您升級高可用性系統時，在重新啟動系統且重新啟動程序看似完成之後，建議您再等候15分鐘，然後再開始執行新增高可用性系統的程序。

将高可用性系统链接到主系统

要将主系统链接到已部署的 HA 系统，以完成 HA 向主系统的集成：

开始之前

验证此系统不是多数据中心 (MDC) 系统的一部分。 （MDC 环境中不支持 HA。）

使用与创建主系统相同的过程创建高可用性 (HA) 系统，如部署高可用性 (HA) 系统，第 56 页中所述。

步骤 1 通知用户和管理员系统已被转入维护模式。
请注意，如果安排维护时段来执行该任务，关闭维护模式后系统会进行重新引导。 根据系统容量，系统重新引导约需 30 分钟。

步骤 2 登录主系统管理站点。

步骤 3 选择**开启维护模式**。

步骤 4 在系统部分，选择**查看更多内容**链接。

步骤 5 选择**添加高可用性系统**。

步骤 6 遵循**系统属性**页面上的指示说明来添加 HA 系统。

步骤 7 输入高可用性系统的管理站点虚拟机的标准域名 (FQDN)，然后选择**继续**。

我们会验证主系统和HA系统是否准备就绪。 如果两个系统都已准备就绪，则会看到一个绿色**添加**按钮。（如果您的系统不是维护模式，请勿选中此按钮。） 如果有一个系统尚未准备就绪，系统将显示错误消息。 请修复错误，并再次尝试此过程。

步骤 8 选择**添加**。

注释 如果显示“错误代码： Database-64”，请使用高可用性虚拟机的快照重复此过程。

会添加高可用性系统并自动配置为发生主系统故障时的备份。

步骤 9 选择**关闭维护模式**，然后选择**继续**以确定。

系统重新启动。 完成重启后，您可以再次登录管理站点。 （要删除 HA，请参阅从系统中删除高可用性系统，第 59 页。）

发生组件故障后的高可用性系统行为

当虚拟机上的特定媒体和平台组件停止运行时，系统将自动重启这些组件。 发生故障时，受到影响的会议会转移到系统中同一虚拟机或不同虚拟机上的其他可用资源（适用于50个用户的独立版系统之外的系统）。

高可用性系统

当在高可用性 (HA) 系统上有单个组件故障时，Cisco WebEx Meetings Server 将对以下组件进行恢复：

- 一个虚拟机上的单个服务。
- 虚拟机。
- 拥有多达两个虚拟机的单个物理服务器或刀片服务器（只要虚拟机布局符合《*Cisco WebEx Meetings Server* 规划指南》中列出的规范）。
- 单个网络链接（假设以完全冗余方式配置网络）。
- 单个 Cisco Unified Communications Manager (CUCM) 节点（假设以冗余方式配置 CUCM）。

在单个组件发生故障后，Cisco WebEx Meetings Server 系统将作出以下行为：

- 应用程序共享、使用计算机的音频语音连接和视频可能会被中断，最多持续三分钟。 Cisco WebEx Meetings Server 可在三分钟内检测到故障并自动重新连接所有受影响的会议客户端。 用户不需要关闭客户端并重新加入会议。
- 某些故障可能引起电话会议音频连接断开。 如果发生这种情况，用户将需要手动重新连接。 重新连接应在 2 分钟内顺利完成。
- 对于某些故障，并非所有客户端和会议都会受到影响。 会议连接通常重新分发至多个虚拟机和主机。

包含 2000 个用户的系统的其他信息

2000 个用户的系统不添加 HA 系统即可提供一些高可用性功能。 对于不带有高可用性功能的包含 2000 个用户的系统：

- 失去任何一个 Web 或媒体虚拟机，系统仍将工作，不过容量将会变少。
- 失去管理虚拟机将导致系统无法使用。

对于带有高可用性功能的包含 2000 个用户的系统：

- 失去任何虚拟机（管理、媒体或 Web）都不会影响系统。即使失去任何承载主虚拟机（管理和媒体，或 Web 和媒体）或 HA 虚拟机（管理和媒体或 Web）的物理服务器，系统也将继续运行并保持容量不变。
- 发生故障的虚拟机重启后，它将重新加入系统，系统将返回至正常工作状态。
- 当媒体虚拟机发生故障时，该服务器上的会议会暂时中断，但会议会转移到备用媒体虚拟机上。 用户必须手动重新加入桌面音频和视频会话。
- 当 Web 虚拟机发生故障时，该虚拟机上承载的现有 Web 会话也会失败。 用户必须重新登录至 Cisco WebEx 站点并建立将托管在备用 Web 虚拟机上的新浏览器会话。
- 当管理虚拟机发生故障时，任何现有的管理会话都会失败。管理员必须重新登录至管理站点并建立将托管在备用管理虚拟机上的新浏览器会话。同样，任何现有管理员或最终用户会议会话都可能会暂时中断。

从系统中删除高可用性系统

步骤 1 登录管理站点。

步骤 2 选择**开启维护模式**。

步骤 3 在“系统”部分选择**查看更多内容**。

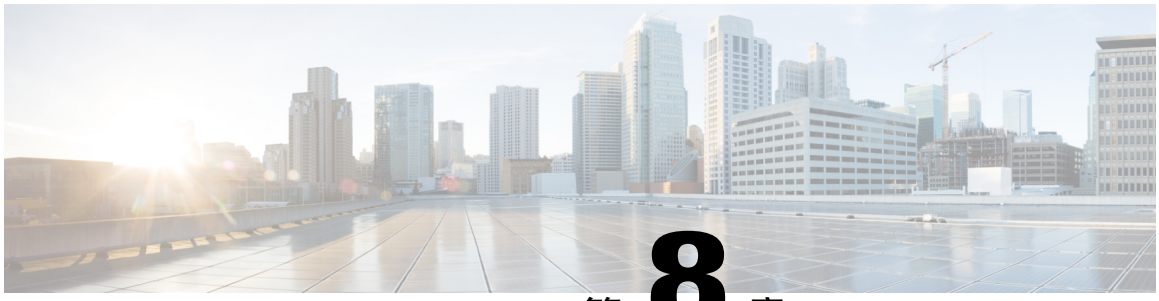
步骤 4 选择**删除高可用性系统**。
会出现**删除高可用性系统**页，其中将显示高可用性系统的标准域名 (FQDN)。

步骤 5 选择**继续**。
在删除高可用性系统后，您无法重新将相同的高可用性系统添加到此系统中。 要重新配置高可用性，必须从 OVA 文件中重新部署高可用性系统以重新开始。 请参阅添加高可用性系统，第 55 页以获取更多信息。

将会删除高可用性系统。

步骤 6 打开 VMware vCenter 并使用**从磁盘中删除**命令删除高可用性系统。

步骤 7 选择**关闭维护模式**，然后选择**继续**以确定。
系统重新启动。



第 8 章

扩大系统规模

- 准备系统扩展，第 61 页
- 扩展系统容量，第 62 页

准备系统扩展

系统扩展要求部署新的主系统，以及将原始系统中的系统数据转移到扩展系统。 系统扩展要求在扩展系统上对现有的主持人许可证进行重新托管。（请参阅执行重大系统修改之后重新托管许可证，第 240 页。）

多数据中心 (MDC) 系统无法扩展。 要扩展 MDC 系统：

- 删除备用数据中心（请参阅删除数据中心，第 250 页）。
- 扩展主要的单数据中心系统。
- 获取用于扩展后系统的 MDC 许可证，并将这些许可证加载到主系统中。
- 新建与主数据中心大小相同的备用数据中心。
- 加入数据中心（请参阅将数据中心加入 MDC 系统，第 247 页）。

扩展系统的注意事项

考虑以下因素：

- 任何附加硬件的预算。
- 在接下来的几个月内同时进行的会议的预计数量及其平均大小。
- 升级或扩展原始系统时，一个并行的系统会被创建。 如果原始系统的试用期有剩余时间，该时间会转移到升级或扩展系统中。 可以通过重新托管许可证将原始系统上有效的永久主持人许可证转移到升级或扩展系统中。

获取系统扩展所需的信息

获取用于安装现有系统版本的 OVA 文件并完成扩展核对表：

字段名	您系统的当前值
WebEx 站点 URL	
管理站点 URL	
专用 VIP 地址	
公共 VIP 地址	

扩展系统容量

开始之前

扩展多数据中心 (MDC) 系统时，需要先删除所有备用数据中心。 （请参阅删除数据中心， 第 250 页。）

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 如果是扩展主系统，请删除除主数据中心之外的所有数据中心。
请参阅删除数据中心， 第 250 页。

步骤 3 如果是扩展 MDC 系统，请新建一个运行 Cisco WebEx Meeting Server 的数据中心，用于在主系统扩展后加入。
请参阅加入数据中心以创建多数据中心 (MDC) 系统， 第 243 页。

步骤 4 创建原始系统的备份。 （请参阅通过使用 VMware vCenter 创建备份， 第 6 页。）

步骤 5 开启维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
我们建议您给每个虚拟机拍摄快照。 （请参阅通过使用 VMware vCenter 拍摄快照， 第 7 页。）

在所有活动数据中心开启维护模式会关闭会议活动，并会使用户无法登录 WebEx 站点、安排会议、加入会议，或播放会议录制文件。 如果此数据中心属于多数据中心 (MDC) 系统，并且另一个数据中心是活动的，那么进行中的会议将故障转移到活动的数据中心。 这可能会导致活动的会议暂时中断。 有关要求开启维护模式的系统任务的信息，请参阅关于维护模式。

步骤 6 选择**继续**。

步骤 7 选择**系统** > **查看更多内容**。

步骤 8 选择**扩展系统容量**。

步骤 9 选择**继续**。

系统将检查到虚拟机的连接。 如果一个或多个虚拟机存在连接问题，则必须修复问题，然后才能继续。 如果没有连接问题，系统将执行自动备份。 在备份完成后，将通知您可以继续进行扩展。

步骤 10 使用 VMware vSphere 客户端，在原始系统的虚拟机上选择**电源** > **关闭客户系统**。（请参阅从 VMware vSphere 客户端部署 OVA 文件，第 18 页。）

步骤 11 使用 vSphere 客户端，部署针对新系统容量的管理虚拟机。
如果是自动执行扩展，我们将为您的系统创建其他虚拟机。 如果是手动执行扩展，您可以为您的系统创建其他虚拟机。

步骤 12 将**硬盘 4** 从原始系统的管理虚拟机连接到扩展系统的管理虚拟机。（请参阅将现有 VMDK 文件附加到新虚拟机，第 8 页。）

步骤 13 启动扩展系统的管理虚拟机，并写下部署 URL。
如果是自动执行扩展，我们将为您的系统启动其他虚拟机。 如果是手动执行扩展，您可以为您的系统启动其他虚拟机。

步骤 14 将部署 URL 输入 Web 浏览器中，然后继续部署扩展系统。

步骤 15 选择扩展系统部署的喜好语言。（请参阅选择安装向导语言，第 20 页。）

步骤 16 选择**扩展现有系统的容量** > **下一步**。

步骤 17 确认系统容量。（请参阅确认系统容量，第 21 页。）
此系统容量必须大于等于原始系统容量。

步骤 18 选择**安装主系统**。

步骤 19 选择自动或手动部署。（请参阅选择部署类型，第 22 页。）
如果选择手动部署，请执行下一步。 如果选择自动部署：

a) 输入 vCenter 凭证以便可以部署虚拟机。（请参阅提供 VMware vCenter 凭证，第 22 页。）
b) 选择媒体虚拟机的 ESXi 主机、数据存储和虚拟机端口组。（请参阅选择媒体虚拟机的 vCenter 设置，第 23 页。）
c) 输入媒体虚拟机的标准域名。
如果已经用扩展系统的条目更新了 DNS 服务器，那么将查找 IP 地址。（请参阅输入媒体虚拟机的联网信息，第 23 页。）

使用用于部署原始系统的同一 OVA 文件，根据新的系统容量部署管理虚拟机。

扩展完成后系统将通知您。

步骤 20 如果希望为扩展系统添加公开访问，则应确保选中**创建互联网反向代理虚拟机**复选框。 否则，取消选中此复选框。（请参阅通过使用 IRP 向系统中添加公开访问，第 130 页。）
如果已选择添加公开访问权限:

a) 选择互联网反向代理 (IRP) 虚拟机的 ESXi 主机、数据存储和虚拟机端口组。
b) 输入 IRP 虚拟机的主机名和联网信息。

步骤 21 输入 WebEx 站点 URL 的公共 VIP 地址。（请参阅输入公共 VIP 地址，第 25 页。）
可以输入用于原始系统的同一公共 VIP 地址，或更改为新的 IP 地址。 如果做了更改，请在 DNS 服务器中进行必要更新。

步骤 22 输入 WebEx 站点 URL 的专用 VIP 地址。（请参阅输入专用 VIP 地址，第 26 页。）

您可以输入用于原始系统的同一个专用 VIP 地址，或更改为新的 IP 地址。 如果做了更改，请在 DNS 服务器中进行必要更新。

步骤 23 输入 WebEx 公共站点 URL。（请参阅输入 WebEx 公共站点和管理站点 URL ， 第 27 页。）
参加者可访问此 URL 以主持和出席会议。 根据是否使用水平分割 DNS，此 URL 将解析为专用 VIP 地址或公共 VIP 地址。

可以输入用于原始系统的同一 WebEx 站点 URL，或更改为新的 URL。 如果确实要进行更改，请在 DNS 服务器中进行必要更新。

在 DNS 服务器上保留原始站点 URL。 将原始站点 URL 重定向到新的站点 URL。 如果用户尝试使用原始 URL 并且您尚未将其重新定向到新的 URL，那么这些用户将无法主持或加入会议。

步骤 24 输入管理员用于访问 Cisco WebEx 管理站点的 WebEx 管理站点 URL。（请参阅输入 WebEx 公共站点和管理站点 URL ， 第 27 页。）
该 URL 将解析到专用 VIP 地址。

可以输入用于原始系统的同一 WebEx 站点 URL，或更改为新的 URL。 如果确实要进行更改，请在 DNS 服务器中进行必要更新。

在 DNS 服务器上保留原始站点 URL。 将原始站点 URL 重定向到新的站点 URL。 如果用户尝试使用原始 URL 并且您尚未将其重新定向到新的 URL，那么这些用户将无法主持或加入会议。

步骤 25 验证已对系统进行了所有必需的网络、DNS 服务器和防火墙配置更改。 （请参阅确认网络配置正确 ， 第 28 页。）

步骤 26 成功部署虚拟机后，选择**下一步**以继续系统检查。 （请参阅部署虚拟机 ， 第 45 页。）
在系统检查中，我们还将用所有必需的更新来更新扩展系统，使软件版本与扩展前的原始系统相符。 （这些更新可能最多需要一个小时。） 完成后，系统将重启。 （请参阅检查系统 ， 第 28 页。）

步骤 27 选择**重新启动**。

步骤 28 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 29 如果是扩展 MDC 系统，请将其加入 MDC 系统。 （请参阅将数据中心加入 MDC 系统 ， 第 247 页。）

步骤 30 关闭维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。 如果此数据中心属于多数据中心 (MDC) 系统，那么管理员会被重定向至全局管理 URL。 管理员所看到的数据中心由 DNS 解析策略确定。 如果启用密钥再生，让一个数据中心退出维护模式会自动让系统中的所有数据中心退出维护模式。

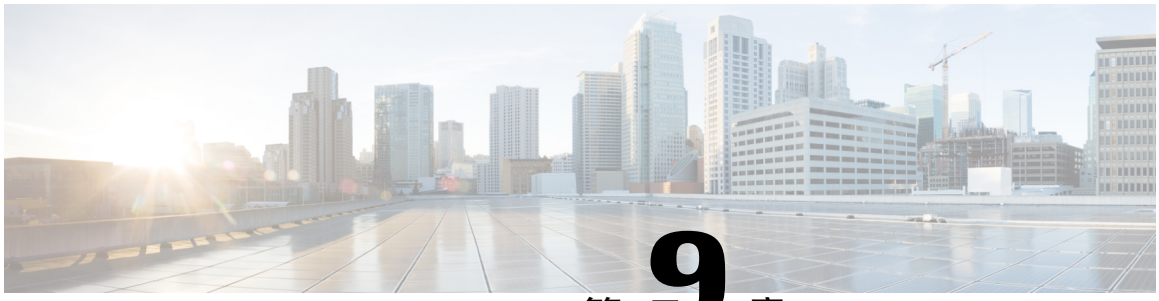
此数据中心上用户的会议服务将被还原。

步骤 31 选择**继续**。
系统将重新启动。 完成重启后，您可以登录管理站点。

注释 如果您最初是使用 Cisco WebEx Meetings Server 2.0 OVA 文件创建的虚拟机，就可能会看到“无法访问服务器”的错误消息。 在这种情况下，请使用 VMware vSphere 客户端并为系统中的所有虚拟机“重新启动客户机”。

步骤 32 测试扩展系统。 （请参阅关于系统测试 ， 第 50 页。）
如果扩展失败，则关闭扩展系统，再打开原始系统。 如有必要，请联系 Cisco TAC 以获取更多帮助。

步骤 33 必要时，为扩展系统重新托管主持人许可证或 MDC 许可证。（请参阅执行重大系统修改之后重新托管许可证，第 240 页。）



第 9 章

更新系统

- 关于更新系统， 第 67 页
- 从 CD/DVD 驱动器连接 ISO 映像， 第 68 页
- 在系统停机情况下更新数据中心 2.5 版及更高版本， 第 69 页
- 以零系统停机更新多数据中心系统， 第 71 页

关于更新系统

在单数据中心 (SDC) 系统中，数据中心必须转入维护模式。 在多数据中心 (MDC) 系统中，可以加入全部数据中心以进行更新，或者在有些情况下，也可以逐个加入数据中心。 逐个加入数据中心并保持为用户提供服务的过程称为零停机更新。 请查看发行说明以了解哪个 Cisco WebEx Meeting Server 版本适合于零停机更新。 如果您要执行零停机更新，在更新首个数据中心之后，我们建议您尽快更新系统中的所有其他数据中心。

升级的定义是更换系统以部署我们对系统所作的重大修改。 例如把当前运行版本 1.5 的系统更换为运行包含新操作系统支持的版本 2.0 的系统。 更新的定义是覆盖现有的（原始的）系统，以利用我们为改进系统所作的修改。扩展的定义是扩大现有系统，而不更改应用程序版本。例如，您可以将系统从版本 1.5 更新至 1.5MR，也可以将系统从 1.5 升级至 2.0，还可以将系统从 800 个用户扩展至 2000 个用户。在所有情况下，这些过程包括将原始系统的所有数据传输给更新、升级或扩展系统。

使用下表确定是否应该对数据中心执行系统升级或更新，以运行具体发行版的 Cisco WebEx Meetings Server。

已安装的发行版	目标发行版	升级	更新
1.5MR3 或更高版本	2.0 或 2.5[3]	X	
1.0MR、1.1MR 或 1.5MR	2.5	X	
2.0MR3 或更高版本	2.5		X

已安装的发行版	目标发行版	升级	更新
2.5 单数据中心 (SDC)	任意 2.5MR		X
2.5 多数据中心 (MDC)	任意 2.5MR		X

[3] 我们建议在升级至版本 2.5 之前，应将任意版本的 1.0、1.1 或 1.5 升级至 1.5MR3 版本的 OVA 和 ISO 文件。

整个更新过程（包括备份虚拟机）最多可能需要一个小时，具体取决于以下因素：

- 系统容量
- 数据库大小
- vCenter 的速度和负载

注释 **升级至版本 2.5 之后，CWMS System** 是数据中心的缺省名称；它没有从英语翻译为任何其他语言。

从 CD/DVD 驱动器连接 ISO 映像

要达到最快的更新速度，我们建议您在 vCenter 数据存储器中装入 ISO 映像。 但是，如果您将其放在 vSphere 客户端可访问的本地磁盘上，请确保 vSphere 客户端具备与公司内部网进行连接的硬连线（而不是通过 VPN 进行连接）。

要将 ISO 映像放在 vCenter 数据存储器中并连接到 CD/DVD，请完成以下步骤：

步骤 1 从 Cisco 获取所需的 ISO 映像：http://www.cisco.com/cisco/software/navigator.html。

步骤 2 验证您有相应的权限。

步骤 3 对于要更新的数据中心的管理虚拟机，选择 ESXi 主机。 选择**摘要**标签页，然后双击**存储空间**下的 **datastore1** 名称。

步骤 4 在**数据存储和数据存储器群集**窗口中，选择**浏览此数据存储**。

步骤 5 选择绿色向上箭头图标（上传文件），然后载入更新的 ISO 文件。

步骤 6 在 VMware vCenter 目录中选择管理虚拟机。

步骤 7 为管理虚拟机选择 **CD/DVD** 图标。

步骤 8 在本地磁盘或数据存储器中选择 **CD/DVD 驱动器 1** > **连接到 ISO 映像**。

步骤 9 确认已连接 CD/DVD 驱动器。

a) 在 vCenter 目录中右键单击管理虚拟机的名称，然后选择**编辑设置...**。

b) 在**硬件**标签页中选择 **CD/DVD 驱动器 1**。
c) 如果未选中，请选中**已连接**复选框。
d) 选择**确定**。

接下来的操作

要更新数据中心，请参阅 在系统停机情况下更新数据中心 2.5 版及更高版本，第 69 页。

要在零停机时间的情况下更新数据中心，请参阅 以零系统停机更新多数据中心系统，第 71 页。

在系统停机情况下更新数据中心 2.5 版及更高版本

此过程描述在通过将所有数据中心置于维护模式而令系统脱机的情况下，如何更新单数据中心 (SDC) 系统或多数据中心（MDC) 系统。

开始之前

您已完成：

- 查看发行说明，确定此 Cisco WebEx Meeting Server 版本是否适合进行零停机更新。 如果它适合进行零停机更新，请按照以零系统停机更新多数据中心系统，第 71 页中的步骤操作。
- 将 ISO 映像放在 vCenter 数据存储器中并连接到 CD/DVD，如从 CD/DVD 驱动器连接 ISO 映像，第 68 页中所述。

步骤 1 从 Cisco 获取最新的更新文件，位置是：http://www.cisco.com/cisco/software/navigator.html。
系统的更新包含有 ISO 映像。 不能跳过该软件的某些版本。 例如，在应用 1.5MR3 之前，您必须安装 Cisco WebEx Meetings Server V1.1（内部版本号 1.1.1.9.A）。 请查看发行说明以获取要使用的正确版本。 请参阅关于更新系统，第 67 页。

步骤 2 通知其他系统管理员，在此过程中不要访问任何正在更新的数据中心。 如果他们这样做，则他们所作的更改不会得到保存，且可能造成不可预测的结果。

步骤 3 清除浏览器缓存。
静态资源会被缓存，以提高网页的性能；但是缓存的数据可能不正确。 因此，我们建议您清除浏览器缓存。

步骤 4 登录管理站点。
在数据中心重新启动或重新引导之前，请勿关闭浏览器窗口，否则将可能无法重新登录管理站点。

步骤 5 为所有数据中心开启维修模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
在所有活动的数据中心上开启维护模式会关闭会议活动，并使用户无法登录 WebEx 站点、安排会议、加入会议或播放会议录制文件。

步骤 6 备份此系统中所有数据中心的所有虚拟机（除非正在从失败的更新恢复）。

（请参阅通过使用 VMware vCenter 创建备份，第 6 页。）

步骤 7 选择**系统**。

步骤 8 选择要更新的数据中心。

步骤 9 选择**升级**。
系统将显示**升级系统**页面。

步骤 10 选择**更新** > **继续**。
系统将显示**验证 ISO 映像**页面。

步骤 11 选择**选中我已连接 ISO 文件并已做好继续操作的准备** > **继续**。
此时读取 ISO 映像，以了解停机时间要求之类的条件。

系统将显示**更新系统**页面。

步骤 12 选择**我已备份所有数据中心上的所有虚拟机** > **继续**。 切勿关闭浏览器窗口；否则，您将无法返回此页。
完成更新最多可能要一小时的时间。 如果尚未显示重新启动按钮，请验证主数据中心的更新状态，确保更新过程没有任何错误且正在进行更新。

重要事项 当另一个数据中心正在更新时，请勿关闭或重新启动任何数据中心；否则，将会导致更新失败。

当完成所有数据中心的更新后，将显示**重新启动**按钮，用于确认更新成功。

步骤 13 选择**继续**。

注意 一旦选择**继续**，将无法停止更新过程。如果在此过程中发生问题，并且更新过程没有成功完成，那么您必须使用备份来恢复系统中的所有数据中心。

切勿关闭浏览器窗口；否则，您将无法返回此页。 如果出于某种原因而导致浏览器会话被关闭或失去连接，您必须检查虚拟机的启动界面，验证已成功完成更新，然后手动重新启动系统。

重要事项 当另一个数据中心正在更新时，请勿关闭或重新启动任何数据中心；否则，将会导致更新失败。

更新完成后，会显示新页面，确认更新成功。

当系统中的所有数据中心均已更新时，重新启动将变为活动状态。

步骤 14 选择**重新启动**以重启系统。
系统将显示 Cisco WebEx 管理站点登录页面。

步骤 15 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 16 检查此次更新的发行说明，然后确定是否需要任何更新后任务。 如果需要其他任务，请在将系统切换出维护模式前完成这些任务。

步骤 17 关闭维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。 如果此数据中心属于多数据中心 (MDC) 系统，那么管理员会被重定向至全局管理 URL。 管理员所看到的数据中心由 DNS 解析策略确定。 如果启用密钥再生，让一个数据中心退出维护模式会自动让系统中的所有数据中心退出维护模式。

此数据中心上用户的会议服务将被还原。

步骤 18 测试系统。 有关推荐的测试，请参阅关于系统测试，第 50 页。

接下来的操作

当对操作感到满意时，建议您删除所有备份。

以零系统停机更新多数据中心系统

此过程描述在更新此数据中心并同时利用另一个数据中心继续服务用户的情况下，如何更新多数据中心（MDC) 系统。 在零停机更新期间，请勿重新启动或关闭任何数据中心。

开始之前

您已完成：

- 查看发行说明，确定此 Cisco WebEx Meeting Server 版本是否适合进行零停机更新。 如果它不适合进行零停机更新，请按照在系统停机情况下更新数据中心 2.5 版及更高版本，第 69 页中的步骤操作。
- 将 ISO 映像放在 vCenter 数据存储器中并连接到 CD/DVD，如从 CD/DVD 驱动器连接 ISO 映像，第 68 页中所述。

步骤 1 从 Cisco 获取最新的更新文件，位置是：http://www.cisco.com/cisco/software/navigator.html。
系统的更新包含有 ISO 映像。 不能跳过该软件的某些版本。 例如，在应用 1.5MR3 之前，您必须安装 Cisco WebEx Meetings Server V1.1（内部版本号 1.1.1.9.A）。 请查看发行说明以获取要使用的正确版本。 请参阅关于更新系统，第 67 页。

步骤 2 通知其他系统管理员，在此过程中不要访问任何正在更新的数据中心。 如果他们这样做，则他们所作的更改不会得到保存，且可能造成不可预测的结果。

步骤 3 清除浏览器缓存。
静态资源会被缓存，以提高网页的性能；但是缓存的数据可能不正确。 因此，我们建议您清除浏览器缓存。

步骤 4 登录管理站点。
在数据中心重新启动或重新引导之前，请勿关闭浏览器窗口，否则将可能无法重新登录管理站点。

步骤 5 选择**系统**。

步骤 6 选择要更新的数据中心。

步骤 7 选择**升级**。
系统将显示**升级系统**页面。

步骤 8 选择**更新** > **继续**。
系统将显示**验证 ISO 映像**页面。

步骤 9 选择**选中我已连接 ISO 文件并已做好继续操作的准备** > **继续**。
此时读取 ISO 映像，以了解停机时间要求之类的条件。

系统将显示**更新系统**页面。

步骤 10 备份所有虚拟机（除非正在从失败的更新恢复）。（请参阅通过使用 VMware vCenter 创建备份，第 6 页。）

重要事项 这里创建的备份可用于重试失败的零停机更新。 如果试图通过其他任何备份来恢复失败的零停机更新，则可能会丢失数据或损坏系统。 只有在您要从最近失败的零停机更新尝试恢复时，才能跳过本步骤。

步骤 11 启动所有虚拟机并重复步骤 2 至步骤 9，重新登录数据中心。
如果因备份操作而导致您失去与 ISO 映像的连接，请重新建立连接。（请参阅从 CD/DVD 驱动器连接 ISO 映像，第 68 页。）

步骤 12 选择**我已备份此数据中心上的所有虚拟机** > **继续**。 切勿关闭浏览器窗口；否则，您将无法返回此页。
完成更新最多可能要一小时的时间。 如果尚未显示重新启动按钮，请验证主数据中心的更新状态，确保更新过程没有任何错误且正在进行更新。

重要事项 当另一个数据中心正在更新时，请勿关闭或重新启动任何数据中心；否则，将会导致更新失败。

当完成此数据中心的更新后，将显示**重新启动**按钮，用于确认更新成功。
对于恢复操作而言，在此过程中所做的备份将不再有效。 如果出于某种原因而导致更新失败，您可以利用在此过程中创建的备份来恢复此数据中心。

步骤 13 选择**重新启动**。
系统将显示登录屏幕。

步骤 14 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 15 导航到刚刚更新的数据中心的控制板。
更新的版本将显示在控制板上。

步骤 16 检查此次更新的发行说明，然后确定是否需要任何更新后任务。 如果需要其他任务，请在将系统切换出维护模式前完成这些任务。

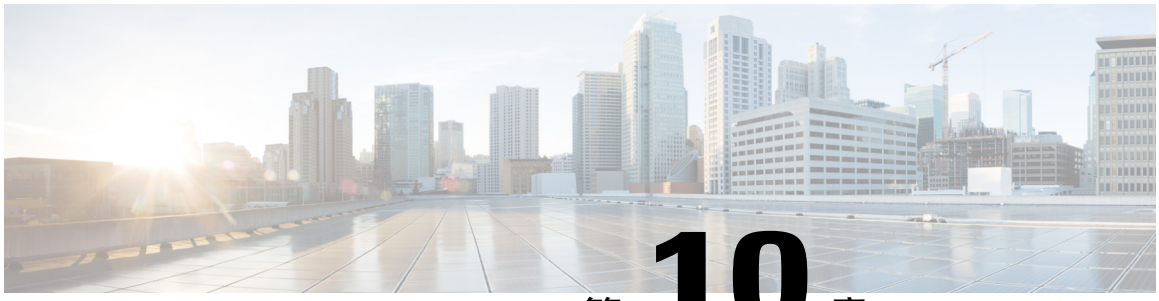
步骤 17 关闭维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。 如果此数据中心是多数据中心（MDC) 系统的一部分，管理员就会被重定向到全局管理 URL。 管理员所看到的数据中心由 DNS 解析策略确定。

此数据中心上用户的会议服务将被还原。

接下来的操作

当对操作感到满意时，建议您删除所有备份。

待此数据中心能正常运行且状态良好之后，应尽快通过重复此过程来更新另一个数据中心。



第 10 章

升级系统

- 准备升级数据中心，第 73 页
- 自动升级系统，第 75 页
- 手动升级系统，第 77 页

准备升级数据中心

可以通过使用升级的OVA（虚拟服务器模板）文件重新部署系统来升级系统。升级过程会创建一个并行的系统，并且原始系统的数据会在升级过程中转移到升级系统中。 如果升级系统无法进行测试，您可以重新启动原始系统，以还原服务、修复任意错误，以及重新部署升级系统。

升级的定义是更换系统以部署我们对系统所作的重大修改。 例如把当前运行版本 1.5 的系统更换为运行包含新操作系统支持的版本 2.0 的系统。 更新的定义是覆盖现有的（原始的）系统，以利用我们为改进系统所作的修改。扩展的定义是扩大现有系统，而不更改应用程序版本。例如，您可以将系统从版本 1.5 更新至 1.5MR，也可以将系统从 1.5 升级至 2.0，还可以将系统从 800 个用户扩展至 2000 个用户。在所有情况下，这些过程包括将原始系统的所有数据传输给更新、升级或扩展系统。

使用下表确定是否应该对数据中心执行系统升级或更新，以运行具体发行版的 Cisco WebEx Meetings Server。

已安装的发行版	目标发行版	升级	更新
1.5MR3 或更高版本	2.0 或 2.5[4]	X	
1.0MR、1.1MR 或 1.5MR	2.5	X	
2.0MR3 或更高版本	2.5		X
2.5 单数据中心 (SDC)	任意 2.5MR		X

已安装的发行版	目标发行版	升级	更新
2.5 多数据中心 (MDC)	任意 2.5MR		X

4 我们建议在升级至版本 2.5 之前，应将任意版本的 1.0、1.1 或 1.5 升级至 1.5MR3 版本的 OVA 和 ISO 文件。

系统可以自动升级或手动升级。 **我们建议您使用自动过程升级系统。**

进行升级时：

- 请勿尝试将系统升级为增量版本；升级为下一个完整版本的应用程序。 例如，将系统从 1.5 升级到 2.0。 将系统从 1.1 更新为 1.5。
- 验证所有 VM 的时间设置匹配：

  确保时间正确，并且网络时间协议 (NTP) 正在运行。 （请参阅配置 NTP 服务器。）

  确认每个 ESXi 主机上的 NTP 配置已配置为通过主机开始和停止。

  如果必须修改配置以更正任意这些问题，请验证主机上的所有 VM 已正常关机。

- 如果升级 Cisco WebEx Meeting Server，在原始系统上保存的日志捕获不会转移到更新后的 Cisco WebEx Meeting Server 系统。 因此，在开始升级前应该从原始系统捕获和下载您需要的所有日志和日志捕获。
- “更新管理 VM”和“原始管理 VM”必须位于相同的 ESXi 主机上。
- 升级或扩展原始系统时，一个并行的系统会被创建。 如果原始系统的试用期有剩余时间，该时间会转移到升级或扩展系统中。 可以通过重新托管许可证将原始系统上有效的永久主持人许可证转移到升级或扩展系统中。
-

注释 我们将启动升级前的系统称为原始系统。 升级后存在的系统称为升级系统。

开始自动或手动升级前

自动或手动升级系统前，应该处理下列问题：

- 获取升级所需的 OVA 文件。
- 删除原始（现有）系统的所有 VMware 快照。 升级过程中请勿拍摄任何快照。
- 为原始（现有）系统中的每个虚拟机创建备份。 （请参阅通过使用 VMware vCenter 创建备份，第 6 页。）
- 安排维护中断。 升级过程中，原始系统会进入维护模式，并且要求对系统进行独占访问；此时用户无法访问系统召开会议。 把此部分升级安排在对用户影响最小的时间。

- 请规划增加的数据存储空间大小，因为原始系统和升级系统将共用数据存储空间，直到升级系统的测试完成并删除原始系统为止。
- 验证原始系统的主机名和 IP 地址在升级系统中重用。 另外，验证两个系统的内部虚拟机位于同一子网。 如果已添加公开访问，原始系统和升级系统的互联网反向代理虚拟机应位于同一子网。
- 验证 vCenter 主机名可以由 DNS 服务器进行解析。 通过 Ping 主机名测试该链接。

注释 **升级至版本 2.5 之后，CWMS System**是数据中心的缺省名称；它没有从英语翻译为任何其他语言。

自动升级系统

此过程列出了完成自动升级所需的高级任务。 它包含的链接指向《*Cisco WebEx Meetings Server* 管理指南》(http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html) 中的章节，其中提供了完成每个任务所需的详细步骤。

开始之前

在使用自动升级过程对系统进行升级之前：

- 在多数据中心 (MDC) 环境中，数据中心无法扩展、升级或更新。 备用数据中心必须从 MDC 中删除，使其成为单数据中心 (SDC) 环境。 修改数据中心并且验证数据中心大小和版本匹配之后，可以还原 MDC 环境。
- 通知其他系统管理员：不应该在升级期间访问或更改原始系统，因为他们的更改可能产生无法预测的结果。
- 通知其他系统管理员：不应该在升级期间访问或更改原始系统，因为他们的更改可能产生无法预测的结果。
- 提供和配置一个将临时用于升级系统管理虚拟机的附加 IP 地址和主机名。 这可以是 VLAN 中的任意可用 IP 地址。 主机名可以为任意名称，因为此 IP 地址和主机名将在升级过程结束之后释放掉。

  原始系统和升级系统在此过程中同时启动。 在该过程的此部分中，临时 IP 地址和主机名可防止 IP 冲突。 将原始系统的数据传输给修改后的系统之后，原始系统关闭。 在该过程结束时，修改后的系统退出维护模式并重新启动。

  重新启动过程中，临时 IP 地址和主机名被释放，修改后的系统使用原始管理虚拟机 IP 地址和主机名。

  如果管理虚拟机和 IRP 虚拟机之间存在防火墙，必须允许临时 IP 地址穿越防火墙。
- 切勿手动启动或关闭任一系统。

- 验证 vSwitch 未在 ESXi 主机上用作分布式交换机。 在 CWMS ESXi 主机上，自动过程不支持 vSwitch 分布式交换机。 更改为标准交换机或使用手动过程。 （请参阅手动升级系统，第 77 页、在系统停机情况下更新数据中心 2.5 版及更高版本，第 69 页或扩展系统容量，第 62 页。）

步骤 1 清除浏览器缓存。
静态资源会被缓存，以提高网页的性能；但是缓存的数据可能不正确。 因此，我们建议您清除浏览器缓存。

步骤 2 在原始系统上转至许可证管理器，并通过选择**系统** > **查看更多内容** > **管理许可证**生成一个许可证请求。
在新的标签页中打开许可证管理器。

步骤 3 选择**生成许可证请求**。
此时将出现含有许可证请求文本的弹出框。 复制文本，并将许可证请求保存在一个方便的位置，因为以手动方式重新托管过程时可能需要它来收回许可证。 此信息还可以帮助 Cisco 找回您的许可证。 （请参阅通过使用许可证管理器完成许可证，第 236 页。）

步骤 4 使用 vSphere 客户端，部署升级系统的管理虚拟机（利用临时 IP 地址），方法是：选择带有**自动升级**后缀的配置（例如250 用户管理自动升级）。 使用同一主机作为原始系统的管理虚拟机。

步骤 5 验证升级管理虚拟机可以连接原始系统磁盘。
管理虚拟机位于同一 ESXi 主机上并能访问相同的数据存储，因此它们应该能够看到这两组磁盘。 通过 vCenter 应能看到管理虚拟机数据存储 (vmdk) 文件所用的数据存储（使用与自动升级过程相同的 vCenter 凭证）。

步骤 6 启动升级系统的管理虚拟机并记下虚拟机控制台上显示的部署 URL。

步骤 7 将部署 URL 输入 Web 浏览器 URL 字段中。

步骤 8 输入管理和 vCenter URL 和凭证，这样我们就可为您部署虚拟机。（请参阅提供 VMware vCenter 凭证，第 22 页。）

步骤 9 要部署更多虚拟机，请选择**继续**。
在开始设置升级系统并且原始系统进入维护模式以前，用户可以召开会议，但是管理员不应修改原始系统虚拟机。

步骤 10 记下 vCenter 中列出的自动创建的虚拟机的名称。
虚拟机名称的格式为：`CWMS_hostname_MMDDHHmm`，其中 `mm`= 分钟

完成升级后，系统不会显示虚拟机。 要找到在 CWMS 升级过程中创建的虚拟机，可以基于此格式进行搜索。

升级过程显示在升级系统的部署 URL 上以及连接到主系统管理虚拟机的 VMware 控制台上。 VMware 控制台提供可使用的部署 URL，以防在升级过程中浏览器窗口不小心关闭。

步骤 11 要将系统自动置入维护模式并开始设置升级系统，请选择**继续**。
启用维护模式最多可能需要 30 分钟，完成后会显示消息。

步骤 12 要启动升级 Cisco WebEx 管理站点，请选择**登录管理站点**并登入。

步骤 13 等待系统状态良好，然后关闭升级系统的维护模式并选择**继续**。
可能要过几分钟才能使用会议服务。 当**系统属性**页面上列出的所有虚拟机都显示状态良好（绿色）时，表示您的系统已经就绪，可以让用户开始会议了。 请参阅开启或关闭 2.0 版及以前版本的维护模式，第 104 页以获取更多信息。

系统重新启动。

步骤 14 测试升级系统。（请参阅关于系统测试，第 50 页。）
对升级系统运行感到满意后，可以删除原始系统以释放原始系统资源。 删除原始系统时确保升级系统保持运行状态，以防止意外删除升级系统可能会访问的硬盘 4 基础 VMDK 文件。

如果升级失败，请关闭升级系统，启动原始系统，并联系 Cisco TAC。

步骤 15 重新托管并更新适用于升级系统的许可证。（请参阅关于主持人许可证，第 234 页和执行重大系统修改之后重新托管许可证，第 240 页。）
如果先前部署的 Cisco WebEx Meetings 应用程序或快捷会议工具的版本或内部版本号与新部署的应用程序不同，且升级未被阻止，那么就会显示升级警告对话框来通知您。 此时可能需要将 Cisco WebEx Meetings 应用程序或快捷会议工具推送给用户。 请参阅《Cisco WebEx Meetings Server 规划指南》中的 *Cisco WebEx Meetings* 应用程序和快捷会议工具兼容性矩阵一节：http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html。

免许可证宽限期应该在 180 天内到期。 如果原始系统具有有效的许可证，那么必须在 180 天内重新托管这些许可证。 如果运行原始系统时处于免许可证宽限期内，那么免许可证的剩余天数将转到升级系统中。

接下来的操作

如果先前部署的 Cisco WebEx Meetings 应用程序或快捷会议工具的版本或内部版本号与新部署的应用程序不同，且升级未被阻止，那么就会显示升级警告对话框来通知您。 此时可能需要将 Cisco WebEx Meetings 应用程序或快捷会议工具推送给用户。 请参阅《Cisco WebEx Meetings Server 规划指南》中的 *Cisco WebEx Meetings* 应用程序和快捷会议工具兼容性矩阵一节及《Cisco WebEx Meetings Server 系统要求》：http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html。

手动升级系统

此过程列出了完成手动升级所需的高级任务。 它包含的链接指向《*Cisco WebEx Meetings Server* 管理指南》(http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html) 中的章节，其中提供了完成每个任务所需的详细步骤。

开始之前

在多数据中心 (MDC) 环境中，数据中心无法扩展、升级或更新。 备用数据中心必须从 MDC 中删除，使其成为单数据中心 (SDC) 环境。 修改数据中心并且验证数据中心大小和版本匹配之后，可以还原 MDC 环境。

验证升级系统可以访问原始系统中管理虚拟机的磁盘。（硬盘 4 将从原始系统复制到升级系统中。）

切勿同时启动和运行两个系统，因为原始虚拟机的主机名和 IP 地址会用在升级系统中。

步骤 1 清除浏览器缓存。

静态资源会被缓存，以提高网页的性能；但是缓存的数据可能不正确。 因此，我们建议您清除浏览器缓存。

步骤 2 在原始系统上转至许可证管理器，并通过选择**系统** > **查看更多内容** > **管理许可证**生成一个许可证请求。
在新的标签页中打开许可证管理器。

步骤 3 选择**生成许可证请求**。
此时将出现含有许可证请求文本的弹出框。 复制文本，并将许可证请求保存在一个方便的位置，因为以手动方式重新托管过程时可能需要它来收回许可证。 此信息还可以帮助 Cisco 找回您的许可证。 （请参阅通过使用许可证管理器完成许可证，第 236 页。）

步骤 4 登录原始系统的管理站点。

步骤 5 转至“系统”标签页，然后选择**升级**。

步骤 6 选择**重要升级**。

步骤 7 选择**继续**以归档原始系统数据并将系统置入维护模式。

步骤 8 使用 VMware vSphere 客户端，在原始系统的虚拟机上选择**电源** > **关闭客户系统**。

步骤 9 部署所有升级系统虚拟机，包括高可用性 (HA) 虚拟机和互联网反向代理 (IRP) 虚拟机。
如果是部署多数据中心 (MDC)，请勿部署 HA 虚拟机；MDC 不支持 HA。

在部署过程中，有一个**部署后启动 VM** 选项。 验证该选项未被选中，且在完成下一步之前已手动启动 VM；否则，将导致 VM 作为新的系统进行部署，并由此新建部署，而非迁移数据。 如果已启动 VM，则在继续操作之前必须将其删除并重新部署。

步骤 10 将数据从原始系统复制到升级系统的管理虚拟机。（请参阅将现有 VMDK 文件附加到新虚拟机，第 8 页。）

步骤 11 启动升级的管理虚拟机，然后记下虚拟机控制台上显示的部署 URL。（请参阅配置高可用性系统。）
如果系统中包含 HA，请勿通过 HA 管理部署来设置 HA 虚拟机；让升级脚本去发现 HA 虚拟机。

步骤 12 启动其他升级虚拟机。

步骤 13 将部署 URL 输入 Web 浏览器中。

步骤 14 选择**继续**以启动系统设置。
升级过程显示在升级系统的部署 URL 上以及连接到主系统管理虚拟机的 VMware 控制台上。

VMware 控制台提供可使用的部署 URL，以防在升级过程中浏览器窗口不小心关闭。

步骤 15 等待系统状态良好，然后关闭维护模式并选择**继续**。
可能要过几分钟才能使用会议服务。 当**系统属性**页面上列出的所有虚拟机都显示状态良好（绿色）时，表示您的系统已经就绪，可以让用户开始会议了。 请参阅开启或关闭2.0版及以前版本的维护模式，第104页以获取更多信息。

步骤 16 测试升级系统。（请参阅关于系统测试，第 50 页。）
对升级系统运行感到满意后，可以删除原始系统以释放原始系统资源。 删除原始系统时确保升级系统保持运行状态，以防止意外删除升级系统可能会访问的硬盘 4 基础 VMDK 文件。

如果升级失败，请关闭升级系统，启动原始系统，并联系 Cisco TAC。

步骤 17 重新托管并更新适用于升级系统的许可证。（请参阅关于主持人许可证，第 234 页和执行重大系统修改之后重新托管许可证，第 240 页。）
如果先前部署的 Cisco WebEx Meetings 应用程序或快捷会议工具的版本或内部版本号与新部署的应用程序不同，且升级未被阻止，那么就会显示升级警告对话框来通知您。 此时可能需要将 Cisco WebEx Meetings 应用

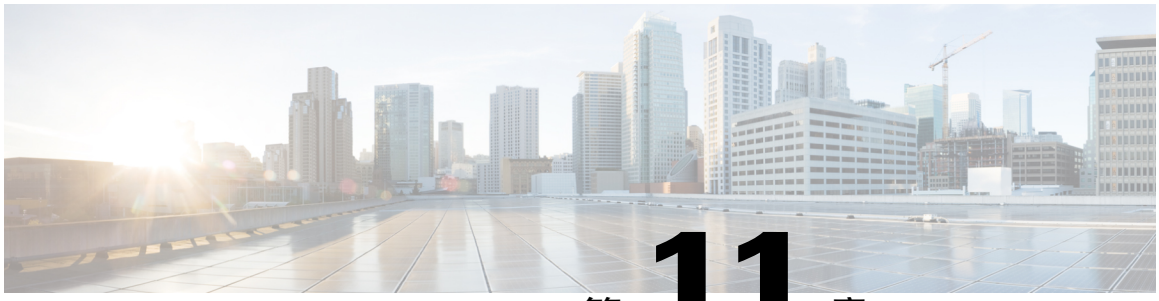
程序或快捷会议工具推送给用户。 请参阅《Cisco WebEx Meetings Server 规划指南》中的 *Cisco WebEx Meetings* 应用程序和快捷会议工具兼容性矩阵一节：http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html。

免许可证宽限期应该在 180 天内到期。 如果原始系统具有有效的许可证，那么必须在 180 天内重新托管这些许可证。 如果运行原始系统时处于免许可证宽限期内，那么免许可证的剩余天数将转到升级系统中。

步骤 18

接下来的操作

如果先前部署的 Cisco WebEx Meetings 应用程序或快捷会议工具的版本或内部版本号与新部署的应用程序不同，且升级未被阻止，那么就会显示升级警告对话框来通知您。 此时可能需要将 Cisco WebEx Meetings 应用程序或快捷会议工具推送给用户。 请参阅《Cisco WebEx Meetings Server 规划指南》中的 *Cisco WebEx Meetings* 应用程序和快捷会议工具兼容性矩阵一节及《Cisco WebEx Meetings Server 系统要求》：http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html。



第 11 章

测试系统

- 关于系统测试，第 81 页
- 使用会议测试，第 82 页
- 使用系统资源测试，第 82 页

关于系统测试

通过使用 CWMS 系统完成大多数系统测试，例如通过使用会议测试，第 82 页和使用系统资源测试，第 82 页。

测试升级系统时，可以保留原始系统，直到已完成测试升级系统为止（但是由于它们共用 IP 地址之类的一些参数，因此不能同时启动两个系统）。 在对升级系统测试结果感到满意之后，可（永久）删除原始系统。 确保删除原始系统时升级系统已在运行。 这可以防止意外删除基本虚拟机磁盘 (VMDK) 文件，升级系统必须访问该文件。

建议在系统上运行一些测试：

- 添加、编辑、激活和停用用户。 （请参阅管理用户，第 105 页。）
- 安排和举行会议。
- 重新安排现有会议。
- 删除一系列安排的会议。
- 从会议邀请中添加和打开会议附件。
- 录制会议和播放录制文件。

系统也可以通过以下方式进行测试：

- 确认网络配置正确，第 28 页
- 检查系统，第 28 页
- 验证主系统和 HA 系统是同一版本

- 通过删除主系统物理连接确认主系统将故障转移至 HA 系统，并验证 Cisco WebEx 在 HA 系统上运行。

使用会议测试

步骤 1 登录管理站点。

步骤 2 选择**支持** > **会议测试**。

步骤 3 选择**下一步**。
系统将运行会议测试，验证自身安排、开始和加入会议的功能。 将在几分钟内显示测试结果。

使用系统资源测试

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 开启维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
我们建议您给每个虚拟机拍摄快照。 （请参阅通过使用 VMware vCenter 拍摄快照，第 7 页。）

在所有活动数据中心开启维护模式会关闭会议活动，并会使用户无法登录 WebEx 站点、安排会议、加入会议，或播放会议录制文件。 如果此数据中心属于多数据中心 (MDC) 系统，并且另一个数据中心是活动的，那么进行中的会议将故障转移到活动的数据中心。 这可能会导致活动的会议暂时中断。 有关要求开启维护模式的系统任务的信息，请参阅关于维护模式。

步骤 3 选择**支持** > **系统资源测试**。

步骤 4 选择**下一步**。
将为以下各项张贴测试的结果：

- 您系统上每个主机的 CPU、内存、网络和存储
- 您的站点和管理 URL 的内部和外部连接检查

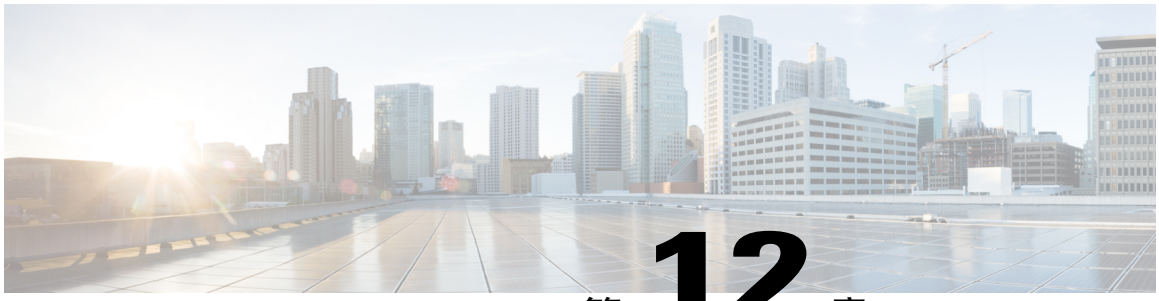
步骤 5 关闭维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。 如果此数据中心属于多数据中心 (MDC) 系统，那么管理员会被重定向至全局管理 URL。 管理员所看到的数据中心由 DNS 解析策略确定。 如果启用密钥再生，让一个数据中心退出维护模式会自动让系统中的所有数据中心退出维护模式。

此数据中心上用户的会议服务将被还原。

第 II 部分

《Cisco WebEx Meetings Server 配置指南》

- 使用控制板， 第 87 页
- 管理用户， 第 105 页
- 配置系统， 第 127 页
- 配置设置， 第 151 页
- 管理报告， 第 225 页
- 管理许可证， 第 233 页
- 加入数据中心以创建多数据中心 (MDC) 系统， 第 243 页
- 使用支持功能， 第 253 页



第 12 章

使用控制板

本模块描绘 Cisco WebEx 服务器控制板上的功能和使用方法。

- 关于控制板， 第 87 页
- 查看和编辑警告， 第 90 页
- 查看会议趋势， 第 92 页
- 安排维护时段， 第 100 页
- 关于维护模式， 第 101 页

关于控制板

控制板是管理站点的主页，可提供重要监控功能的多个参数和图表。

控制板包括以下部分：

- 系统监控器 — 用于显示系统状态和时间标记，包括下列子部分：

  会议和用户 - 正在进行的会议的状态以及使用情况。 显示当前正在进行的会议数以及不同的参加者数（使用情况）。 LED 状态表示正在进行的会议以及使用情况是低于还是超过配置的警告阈值。 绿色 LED 状态表示低于配置的阈值，而红色 LED 状态表示超过配置的阈值。 有关配置警告的更多信息，请参阅查看和编辑警告， 第 90 页。

  警告图标 - 选择“警告”图标可查看并编辑已配置的警告阈值设置。 警告阈值以数字形式显示在**警告**页面上。 缺省情况下，警告阈值显示为百分比。 有关配置警告的更多信息，请参阅查看和编辑警告， 第 90 页。

  您可以为以下各项配置警告：

  正在进行的会议 - 在当前会议发生问题时发出提示。

  使用情况 - 使用系统的不同用户的总数。 有时参加者同时进行多个会话，但是参加者数仅计一次。

  存储空间 - 使用的录制文件和数据库备份存储空间。

注释 仅当配置了存储服务器时才出现存储警告。 请参阅配置存储服务器，第 136 页以获取更多信息。

如果存储空间使用量超过阈值，将禁用会议录制。

日志分区 - 用于存储应用程序审核日志的空间量。

注释 如果系统配置了审核员，此警告仅对审核员可见。

许可证使用量 - 分配给主持人用户的永久许可证的百分比。

宽限期许可证 - 指示是否给主持人用户分配宽限期许可证。

- 数据中心信息 - 此部分列出各个数据中心的名称、维护模式处于开启或关闭状态、各个数据中心的存储空间量，以及数据复制的状态。 请参阅关于控制板上显示的数据中心信息，第 89 页以获取更多详细信息。
- 会议趋势图和会议列表 - 指定时间段内在系统中举行的会议数的图表。 使用**开始时间**和**结束时间**字段为会议趋势信息以及“会议”列表中显示的会议设置时间段。 您可以在“会议趋势”图表上选择某个点，“会议”列表中将会列出图表上指定时间段内举行的会议。 要查看在一天的特定时间段内举行的会议，请将鼠标悬停在图表上，然后选择所需的时间。 “会议”列表将显示选定时间段内举行的会议总数、会议主题、主持人、参加者人数以及会议状态。 您可以在“会议”列表中对每列的信息进行分类，会议将按以下状态显示：“正在进行”、“已结束”和“未开始”。
- 会议搜索 - 按照输入的具体搜索条件（例如会议号、会议主题或日期范围）查找会议。
- 维护 - 安排维护时段，通知何时开启或关闭维护模式。 请参阅 安排维护时段，第 100 页 和 关于维护模式，第 101 页 以获取更多信息。
- 上次系统备份时间 - 上次进行备份的时间和日期；备份的文件名、大小和位置；以及下次备份的日期和时间。 如果获取备份失败，系统会通知您，如果尚未创建备份，系统会告知您首次备份尝试的日期。 各个数据中心都有单独的备份链接。

  注释 仅当配置了存储服务器时才出现。
- 系统 - 显示可同时参加会议的最大用户数、版本号、产品 URL、是否允许公开访问、是否为高可用性系统以及用户许可证数。 选择**查看更多内容**可转到 配置系统，第 127 页。
- 用户 - 显示活动用户数、是否已配置“目录集成”、下次进行同步的时间（若已配置）以及所选的验证类型。 选择**查看更多内容**可转到 编辑用户，第 115 页。
- 设置 - 显示每个会议所允许的最大参加者人数、音频类型以及是否启用 WebEx HQ 视频。 选择**查看更多内容**可转到 配置设置，第 151 页。

相关主题

查看资源历史记录
使用正在进行的会议图表解决会议问题
安排维护时段，第 100 页
开启或关闭 2.0 版及以前版本的维护模式，第 104 页

关于控制板上显示的数据中心信息

控制板的“系统监控器”部分显示系统中的数据中心的状态信息。 在单数据中心系统中，系统自动分配的数据中心名称为 **CWMS System**，但是单数据中心的状态信息会动态更新。 在多数据中心系统中，各个数据中心按加入数据中心过程中输入的名称在单独的行中列出，并且每个数据中心的状态信息单独动态更新和显示。

- 状态 - 此列显示各数据中心的状态。 状态可以为良好、部分服务、已冻结或停止。

  良好 - 数据中心的所有组件均工作正常。 不向管理员发送系统生成的电子邮件。

  部分服务 - 数据中心的一些组件工作不正常，但是数据中心仍在提供服务。 系统向管理员发送一封电子邮件，指示此数据中心需要引起注意。

  已冻结 - 数据中心的一些组件长期工作不正常。 系统已冻结此数据中心的服务，并且将所有活动重定向至另一个数据中心。 系统向管理员发送一封电子邮件，指示服务已停止，数据被重定向至另一个数据中心，并且此数据中心需要引起注意。

  停止 - 数据中心的运行已降级至无法再提供可靠服务的程度，并且故障转移至运行正常的数据中心。 系统向管理员发送一封电子邮件，指示服务已停止，数据被重定向至另一个数据中心，并且此数据中心需要引起注意。

  在多数据中心 (MDC) 环境中，一些组件能够级联，因此在此数据中心上禁用的服务可能由另一个数据中心提供。 这并不表明总体系统状态，仅适用于此数据中心的状态。

  已冻结或停止并且维护模式开启 - 数据中心状态不断显示数据中心已冻结。 当维护模式关闭并且所有组件再次启动和运行时，状态会发生更改。

  无法访问 - 其他数据中心无法与此数据中心通信。 系统向管理员发送一封电子邮件，要求管理员检查数据中心之间的网络连接。

- 维护 - 指示数据中心是否已开启或关闭维护模式。
- 存储 - 各数据中心连接的存储服务器上所使用的存储空间量。 **未配置**显示存储服务器是否未连接到系统。
- 数据复制 - 指示在 MDC 系统的数据中心之间是否出现数据复制。

数据中心处于冻结或停止状态时，用户可能遇到以下情形：

- 正在进行的会议几分钟之后自动移至运行正常的数据中心；类似于在故障转移情况下出现的状况。 对 PCN 或群拨会议不存在影响。
- 未开始的之前安排的会议移至运行正常的数据中心。 主持人或参加者不需要采取其他措施。

- 用户按通常的方式登录 WebEx 站点 URL，但是系统将登录重定向至运行正常的数据中心。
- 管理员可以登录冻结的数据中心，以及运行正常的数据中心。
- 管理员收到一封系统生成的电子邮件，指示哪个数据中心处于冻结状态，并告知一些可能的原因。

查看和编辑警告

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择警告**图标**。
系统会显示**警告**页面，显示当前警告阈值。

步骤 3 选择**编辑**。
系统将显示**编辑警告**页面。 选择**百分比%** 按百分比查看警告阈值，或选择**数值**按数字查看警告阈值。 缺省设置是**百分比%**。

步骤 4 选择想要启用的警告复选框，然后选择各个已启用警告的时间间隔。

选项	描述
正在进行的会议	将显示进行中的会议阈值。 • 如果设置为**百分比 %**，请移动选择栏以设置为 2% 至 99%。 • 如果设置为**数值**，请输入 2% 至 99% 中的一个数。 **缺省**： 选择时间间隔为 **1 小时**。
使用情况	显示当前系统阈值。 • 如果设置为**百分比 %**，请移动选择栏以设置为 2% 至 99%。 • 如果设置为**数值**，请输入用户数。 **缺省**： 选择时间间隔为 **12 小时**。

选项	描述
存储空间	将显示当前存储阈值 (GB)。 最大存储阈值计算方法为（总空间 - 录制文件缓冲区大小）。 录制文件缓冲区的大小取决于用户系统容量 [50 用户 (1 GB)、250 用户 (5 GB)、800 用户 (16 GB) 或 2000 用户 (40 GB)]、召开的 Cisco WebEx 会议数以及录制会议的长度。 大的用户系统（800 个和 2000 个用户的系统）需要更多的存储空间来容纳更大的数据库备份。 一般情况下，应计划为三个备份文件提供足够的存储空间。 有关详细信息，请访问 备份文件的建议存储空间。 • 如果设置为**百分比 %**，请移动选择栏以设置为 2% 至 99%。 • 如果设置为**数值**，请以千兆字节 (GB) 为单位输入数字。 **缺省**： 未选择。 时间间隔为 **1 小时**。 **注释** 只有在已经配置了存储服务器时才显示此部分。 如果存储空间使用量超过配置的阈值，将禁用录制。 请参阅配置存储服务器，第 136 页以获取更多信息。
日志内存使用情况	显示用于日志的磁盘空间量。 如果在系统部署过程中将某个用户配置为审核员，则只有审核员能在**审核**标签页上查看和配置此警告。 如果您的系统中没有拥有审核员角色的用户，则管理员、SSO 管理员或 LDAP 管理员可以查看和配置此警告。 • 如果设置为**百分比 %**，请移动选择栏以设置为 2% 至 99%。 • 如果设置为**数值**，请以千兆字节 (GB) 为单位输入数字。 设置**间隔**，指定系统检查日志内存使用情况的频率。
许可证使用情况	显示永久许可证使用情况。 • 如果设置为**百分比 %**，请移动选择栏以设置为 2% 至 99%。 • 如果设置为**数值**，请以千兆字节 (GB) 为单位输入数字。 设置**间隔**，指定系统检查分配的许可证数的频率。
宽限期许可证	显示处于宽限期的许可证使用情况。 选中**发送电子邮件通知**复选框将在满足下列选定条件之一时向用户发送通知： • 为用户分配了宽限期许可证 • 分配给用户的宽限期许可证过期 • 分配了所有宽限期许可证

警告超过阈值时，将给管理员发送一封电子邮件。 时间间隔用来抑制特定时间内的多个警告以避免对同一问题发送过多的电子邮件。

步骤 5 选择**保存**。
会保存警告设置，**警告**页将根据更改更新。

查看会议趋势

步骤 1 登录管理站点。

步骤 2 在**会议趋势**图表上设置趋势时间段，方法是选择**开始时间**和**结束时间**日期和时间。

- 您可以查看前四个月、本月以及未来一个月的会议趋势数据。
- 会议开始当天的图表上会显示午夜前安排的会议以及延续至第二天的会议。
- 如果会议因系统问题中断后又重新连接，会议趋势图表上将计为两次会议。
- 一个月和六个月会议趋势数据视图基于格林尼治标准时间 (GMT)，因此无法准确显示 24 小时时间段内的数据。 例如，如果您的系统在某一天托管 200 场会议，数据库将根据 GMT 而非当地时间记录这些召开的会议。 一天和一周会议趋势数据视图基于用户时区。
- 绿色标记表示正在进行或已结束的会议。 尚未进行的会议显示为黄色。
- 如果所选时间范围是 24 小时，已过去或正在进行的会议的数据点时间间隔为 5 分钟，而尚未进行的会议的数据点时间间隔为 1 小时。
- 如果所选时间范围大于一天而小于或等于一周，那么已过去、正在进行或尚未进行的会议的数据点时间间隔将以 1 小时为单位。
- 如果所选时间范围大于一周，那么已过去、正在进行或尚未进行的会议的数据点时间间隔将以 1 天为单位。

会议趋势图表将显示所选时间段内召开的会议总数。图表下的**会议**列表将列出所选趋势时间段内所有的会议。

注释 部分会议趋势项可能是重复的，因为这些项的名称相同。 每召开一个会议就会创建一项。 因此，如果召开、停止，然后再重新召开某个会议，则会显示多个含有相同会议名称的项。

步骤 3 要查看特定时间召开的会议的列表，请执行以下操作：

a) 单击**会议趋势**图表上的特定位置可列出该图表下**会议**列表中所选时间的 5 分钟内召开的会议。 请参阅查看会议列表，第 93 页以获取更多信息。

b) 选择**开始时间**和**结束时间**字段下的图表符号可显示在“开始时间”和“结束时间”之间召开的会议的日期和时间列表。 然后，从下拉列表中选择日期。
下拉菜单中显示的数据点与图表上显示的相同。提供对它们的访问主要是为了方便使用键盘和屏幕朗读器的用户。

将鼠标悬停在图表上可查看在该时间召开的会议总数。

接下来的操作

- 要查看有关会议的更多信息，请参阅查看会议列表，第 93 页。
- 有关使用查找会议，第 95 页会议搜索**标签页的更多信息，请参阅**。

查看会议列表

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 通过选择**开始时间**和**结束时间**日期和时间，在“会议趋势”图表上设置趋势时间段。
缺省情况下，“会议”列表将显示当前 24 小时内的会议。 请参阅查看会议趋势，第 92 页以获取更多信息。

缺省情况下，会议列表将按预定开始时间显示会议。会议按如下状态顺序显示：“正在进行”、“已结束”和“未开始”。 显示在“会议”列表中的信息包括：

- 趋势图表中所选的时间范围
- 会议主题
- 主持人姓名
- 参加者人数
- 会议状态：“正在进行”、“已结束”和“未开始”

注释　第一列中显示状态图标，以指示正在进行的或已结束的会议的状态为良好（绿色）、一般（黄色）或差（红色）。

- 一般（黄色）表示会议期间发生的音频/视频延迟或抖动情况已达到次要阈值，应该予以监控并调查以确定原因。
- 差（红色）指示会议达到严重阈值时出现的音频/视频延迟或抖动。
- 如果会议列表中大部分会议指示“差”状态，请联系 Cisco 技术支持中心 (TAC) 以获取帮助。
- 下表提供不同会议状态指示器的更多详细信息。

类别	良好	一般	差
数据往返时间	小于 3000 毫秒	3000 – 5999 毫秒	大于等于 6000 毫秒
音频往返时间	小于 100 毫秒	100 – 299 毫秒	大于等于 300 毫秒
音频数据包丢失	小于 5%	5% – 9%	大于等于 10%
音频抖动	小于 100 毫秒	100-499 毫秒	大于等于 500 毫秒
视频往返时间	小于 100 毫秒	100-499 毫秒	大于等于 500 毫秒
视频包丢失	小于 20%	20% – 49%	大于等于 50%
视频抖动	小于 100 毫秒	100-499 毫秒	大于等于 500 毫秒

步骤 3　（可选） 选择列标题对会议进行排序。

步骤 4　使用分页功能可查看下一页或上一页。

- 每页最多显示 10 个会议。
- 您可能会在“会议”列表中看到重复的会议项。 每召开一个会议就会创建一个会议项。 因此，如果召开、停止，然后再重新召开某个会议，列表中会显示多个含有相同名称的会议项。

步骤 5　在“会议”列表中选择**会议主题**，以显示更多会议信息。
展开该列表可显示会议详细信息，例如参加者姓名、开始和结束时间，以及会议状态

- 选择**时间标记**以转至**会议分析报告**页面。
- 选择**下载日志**以将系统信息捕捉 (Infocap) 日志下载到本地驱动器中。

步骤 6　（可选） 要缩小搜索范围，请选择**会议搜索**标签页。
系统将显示其他搜索字段。

接下来的操作

- 有关更详细的会议信息，请参阅查看会议分析报告 ， 第 96 页。
- 要下载含有多个会议日志的压缩文件，请参阅下载 Cisco WebEx Meeting 日志 ， 第 97 页。 使用这些日志可以对参加者在会议期间遇到的问题进行诊断。
- 要优化搜索结果或查找特定的会议，请参阅查找会议 ， 第 95 页。

查找会议

步骤 1 登录管理站点。

步骤 2 在“会议趋势”部分，选择**会议搜索**标签页。

步骤 3 输入搜索条件。
利用以下部分或全部字段搜索会议：

- 会议号或主持人姓名
- 状态 - 从下拉菜单中选择“全部”、“良好”、“一般”或“差”。
- 会议主题 - 可以输入会议主题的前几个字母，查找具有类似主题的所有会议。
- 开始日期和时间 - 利用日历图标和下拉菜单选择日期和时间。
- 结束日期和时间 - 利用日历图标和下拉菜单选择日期和时间。

步骤 4 选择**搜索**。
搜索结果中列出与搜索条件匹配的会议。

步骤 5 要开始另一次搜索，请选择**清除**。
系统将清除搜索字段，但上一次搜索的结果仍将保留在**搜索结果**中。

步骤 6 在“会议”列表中选择**会议主题**，以显示更多会议信息。
展开该列表可显示会议详细信息，例如参加者姓名、开始和结束时间，以及会议状态

- 选择**时间标记**以转至**会议分析报告**页面。
- 选择**下载日志**以将系统信息捕捉 (Infocap) 日志下载到本地驱动器中。

接下来的操作

要查看会议详细信息，请参阅查看会议分析报告 ， 第 96 页。

要下载包含会议日志的压缩文件，请参阅下载 Cisco WebEx Meeting 日志 ， 第 97 页。

查看会议分析报告

有关 Cisco WebEx 会议及其参加者的其他信息在**会议分析报告**页上提供。

开始之前

一个或多个会议显示在**会议趋势**标签页的会议列表中。 有关详细信息，请访问 查看会议列表，第 93 页。

步骤 1 选择“会议趋势”标签页上的会议列表中显示的**会议主题**。

步骤 2 在会议列表中，选择**分析会议详细信息**。
在系统处理信息时，将显示系统开始生成信息的日期和时间，状态为“暂挂”。 系统生成完信息后，日期和时间将变为活动链接，“暂挂”状态也更改为“下载日志”活动链接。

步骤 3 选择**日期和时间**链接以查看**会议分析报告**页面。
系统将显示以下信息:

- 会议主题
- 主持人的电子邮件地址
- 状态 - 会议的当前状态。 值可以是“未开始”、“正在进行”或“已结束”。
- 开始时间 - 会议开始的日期和时间。
- 结束时间 - 会议结束的日期和时间。
- 在线会议标识 - 分配给会议网络部分的会议标识。
- 在主持人之前加入 - 指示是否允许参加者先于会议主持人加入会议。
- 数据中心 - 显示用于会议的数据中心的名称。 在单数据中心环境中，该名称始终为 CWMS System。
- 会议号 - 分配给会议的一个 9 位数编号。
- 状态 - 会议的一般状态。 值可以是“正常”、“一般”或“差”。
- 预定开始时间 - 会议安排开始的日期和时间。
- 预定结束时间 - 会议安排结束的日期和时间。
- 音频会议标识 - 分配给会议音频部分的会议标识。
- 首先开始音频会议 - 指示会议的音频部分是否先于会议的网络部分开始。

注释 系统刷新窗口后，会议详细信息将关闭。 再次选择会议主题，显示日期和时间或下载日志链接。

步骤 4 选择**会议消息**标签页以显示功能、时间和会议期间生成的消息。

步骤 5 选择**参加者**标签页以显示每个会议参加者的下列信息：

- 参加者姓名

- 加入时间
- 浏览器
- 客户端 IP 地址 - WebEx 站点的 IP 地址。
- 离开时间 - 参加者离开会场的时间。
- 离开原因 - 离开会场的原因。 值为“正常”或“超时”。
- 电话号码 - 参加者用于出席本次会议的电话号码。
- 网络语音延迟
- 音频 QoS - 会议过程中的音频质量。 值为“正常”或“不佳”。
- 视频 QoS - 会议过程中的视频质量。 值可以是“正常”或“不佳”。
- 客户端延迟 - 从会议客户端到数据会议服务器之间的延迟。 值可以是“正常”或“不佳”。
- 托管服务器 - 托管会议的虚拟机的名称。 这是托管会议的虚拟机的标准域名 (FQDN)。 例如，如果一个微型 VM 的 FQDN 是 `susmicro-vm.orionqa.com`，则系统将显示 `susmicro-vm`。

接下来的操作

要下载含有多个会议日志的压缩文件，请参阅下载 Cisco WebEx Meeting 日志， 第 97 页。

下载 Cisco WebEx Meeting 日志

Cisco WebEx 会议正在进行或者会议结束时，您可以下载系统生成的会议日志，该日志提供了对用户在会议期间遇到的问题进行诊断的信息。

步骤 1 登录管理站点。

步骤 2 选择“会议趋势”标签页，然后选择**开始时间**和**结束时间**，以显示所选时间期间举行的会议图表。

步骤 3 单击**会议趋势**图表上的特定位置可列出该图表下**会议**列表中所选时间的 5 分钟内召开的会议。

步骤 4 在**会议**列表中选择**会议主题**。
会议主题下面显示有关所选会议的信息。

步骤 5 选择**下载日志**。

接下来的操作

有关下载的会议日志的更多信息，请参阅关于会议日志， 第 98 页。

关于会议日志

您下载的会议日志压缩文件包含以下日志：

数据会议日志

此日志包含有关会议网络部分的信息。

- 会议标识
- 会议标识
- 预定开始时间
- 开始时间
- 结束时间
- 主持人电子邮件地址
- 站点 URL
- 会议类型 - 会议客户端
- 会议名称 - 会议主题。
- 主要呼入号码
- 备用呼入号码
- 结束时删除会议 - 指示会议结束时是否从会议详细页面中删除此会议。
- 会议状态
- 应用程序共享 - 指示会议期间是否使用应用程序共享功能。
- 一般电话 - 指示参加者是否使用电话呼叫会议。
- 混合电话
- Eureka 视频
- Eureka 网络语音
- MMP 网络语音
- 混合网络语音
- MMP 视频
- NBR2
- 移动设备
- 音频广播
- 移动设备音频广播

多媒体日志

此日志提供有关音频流、音频切换和 SVC 流自适应的信息给会议客户端，因为它与 MMP 相关。

- 会议名称
- 会议标识
- 会话类型
- 参加者
- 加入总数
- MCS 服务器
- 开始时间
- 结束时间
- 持续时间

电话会议日志

此日志包含有关电话会议的信息。

- 电话会议标识
- 应用程序服务器
- 呼叫者
- 回呼
- 呼入
- 开始时间
- 结束时间
- 持续时间
- 描述
- 帐户类型

网络加入事件日志

此日志包含有关网络加入事件的信息。

- 会议名称 - 显示会议主题。
- 会议标识 - 数据会议实例标识。
- 站点标识 — Cisco WebEx 站点的名称。
- 参加者 — 从 Web 浏览器加入会议的参加者总数。

注释 此总数不含开始会议的主持人。

- 加入总数 - 加入会议的人员总数。
- 开始时间 - 会议开始的日期和时间。
- 结束时间 - 会议结束的日期和时间。
- 持续时间 - 会议持续的时间（分钟）。
- 结束原因 - 会议结束的原因。

安排维护时段

在执行系统维护之前，应安排维护时段。 在维护时段生效后的唯一限制是用户无法安排处于维护时段中或与维护时段重叠的会议。 例如，管理员想要对系统进行大约一个小时的维护（如 5:00 a.m. 到 6:00 a.m.），即这段时间不能安排会议。 如果安排了会议，管理员必须联系每个会议主持人，告诉他们在其会议期间已安排了维护时段。维护时段设定完成后，用户将无法在该时段内安排会议。但是，用户可以使用**即时会议**功能开始即时会议。

开启维护模式后，所有当前正在进行的会议都会结束，即时会议功能也不再可用。 假设您确定进行必要的系统更改需要两个小时左右。 您需要执行的任务之一是上传新的证书中心 (CA) 证书，因此在关闭维护模式后您可能需要进行系统重新引导。 您计划在凌晨 4:00 前后开始系统维护。 您指定了开始时间为 04/15/2014 3:30，持续时间为 3 小时30 分钟的维护时段。 这意味着维护时段将从凌晨 3:30 开始生效（允许所有会议结束，并且禁止在管理员计划开始系统维护的 30 分钟前安排会议），持续到上午 7 点。 这一时段使系统在开启维护模式后可能发生的重新引导结束后仍能运转一段时间，而且给管理员留出了一定时间，使其可以先开始一个或多个即时会议来测试修改的设置，再允许用户安排和主持会议。

虽然有些系统维护任务不需要您开启维护模式，但请注意，那些需要系统处于维护模式的任务会在您关闭维护模式之后耗用额外时间来完成重新启动或重新引导。 重新启动系统仅需几分钟（约 3 至 5 分钟），但是重新引导约需 30 分钟。 在安排维护时段时，别忘了系统需要经过这段额外时间才能全面运转。 请参阅开启或关闭 2.0 版及以前版本的维护模式，第 104 页以获取更多详细信息。

步骤 1 登录管理站点。

步骤 2 选择**安排维护**。
系统将显示**安排维护时段**。

步骤 3 使用日历工具和时间下拉菜单选择维护时段的日期和开始时间。

步骤 4 通过指定小时数和分钟数来输入维护时段的持续时间。

步骤 5 选择**安排**。
维护时段开始后，如果用户尝试在预定维护时段内安排会议，将会收到错误消息。

此时将在维护窗格中显示预定的维护时段日期、开始时间和持续时间。

接下来的操作

- 有关让用户了解系统维护情况的详细信息，请参阅向用户发送电子邮件，第 126 页。
- 有关开启维护模式的信息，请参阅开启或关闭 2.5 版及更高版本的维护模式或开启或关闭 2.0 版及以前版本的维护模式，第 104 页。

更改已安排的维护时段

在安排了维护时段之后，您可以重新安排日期和时间或将其删除。

步骤 1 登录管理站点。

步骤 2 选择**控制板**。

步骤 3 选择显示的系统维护日期和时间。

步骤 4 在**安排维护时段**中，您可以：

- 输入其他开始日期和时间。
- 修改持续小时和分钟数。
- 选择**删除**可删除维护时段。

注释 如果您提早完成了系统维护，您可以在**安排维护时段**中减少持续时间或选择**删除**。

接下来的操作

修改系统属性前别忘了开启维护模式。 请参阅关于维护模式，第 101 页获取需要开启维护模式的系统属性的相关信息。

关于维护模式

许多配置更改要求将系统转入维护模式。 维护模式会关闭数据中心上的所有会议活动，因此您应该通过安排维护时段向用户发出提示（请参阅安排维护时段，第 100 页）。

单击此处以显示开启或关闭 2.5 版及更高版本的维护模式。 单击此处以显示开启或关闭 2.0 版及以前版本的维护模式，第 104 页。

将数据中心转入维护模式会产生下列结果：

- 断开用户并关闭所有会议。 如果您将属于多数据中心 (MDC) 系统一部分的数据中心转入维护模式，正在进行的会议将故障转移至活动的数据中心。
- 禁止用户从网页、Outlook 插件和移动应用程序登录。 电子邮件将在系统退出维护模式时自动发送。
- 停止对会议录制文件的访问。
- 用户无法安排或主持新会议。
- 系统将继续向用户和管理员发送自动通知电子邮件。

根据系统容量，系统重新引导可能约需 30 分钟。 重新启动可能要花 3 至 5 分钟。 系统会监控修改并自动做出决定。

使用下表帮助确定要求您开启维护模式的任务，以及在关闭维护模式后系统执行的操作，以便您可以计划停机。 需要转入维护模式时，如果您尝试在不开启维护模式的情况下执行任务，系统会发出提醒消息。

任务	参考	需要维护模式	重新引导或重新启动
添加或删除高可用性	配置高可用性系统	是	重启
添加或删除公开访问	通过使用 IRP 向系统中添加公开访问，第 130 页 或 删除公开访问功能，第 131 页	是	重新开始
更改系统缺省语言	配置公司信息，第 151 页	是	重新开始
更改主持人或管理员帐户 URL	更改站点设置，第 133 页	是	重新开始
更改邮件服务器	配置电子邮件 (SMTP) 服务器，第 47 页	否	不适用
更改虚拟 IP 地址	更改虚拟 IP 地址，第 129 页	是	重启
配置和更改定制设置	配置定制设置，第 153 页	否	不适用
配置和更改众多音频设置	关于配置音频设置，第 157 页	是	重新开始
配置和更改呼入接入号码、显示名称和呼入者标识音频设置。	配置音频设置，第 159 页	否	不适用
配置和更改服务质量设置	配置服务质量 (QoS)，第 172 页	否	不适用
配置和更改 SNMP 设置	配置 SNMP 设置，第 141 页	是	重新开始

任务	参考	需要维护模式	重新引导或重新启动
配置证书	管理证书，第 205 页	是	重新启动或重新引导
配置灾难恢复设置	通过使用存储服务器进行灾难恢复，第 139 页	是	重新开始
配置 FIPS 兼容加密	启用符合 FIPS 的加密，第 221 页	是	重新开始
配置存储服务器	配置存储服务器，第 136 页	是	重新开始
配置虚拟机安全性	配置虚拟机安全性，第 220 页	是	重启
扩展系统容量	准备系统扩展，第 61 页	是	重新开始
执行更新或升级	准备更新现有系统或准备升级数据中心，第 73 页	是	重新开始
更新共享密钥	管理证书，第 205 页	是	重新开始
使用系统资源测试	使用系统资源测试，第 82 页	是	重新开始

每台虚拟机都有一个控制台窗口，指示它何时处于维护模式。 可以在 vCenter 目录栏中打开控制台窗口（用于导航）。控制台窗口提供系统的URL、系统的类型（主系统、高可用性系统或公开访问系统）、部署的类型（50 个、250 个、800 个或 2000 个用户的系统）和当前系统状态，包括维护模式是否打开和状态变化的日期及时间。显示的时间在“公司信息”设置中配置。请参阅配置公司信息，第 151 页以获取更多信息。

完成系统维护任务

修改完系统配置后您可以关闭维护模式。 根据执行的任务，您的系统会：

- 快速运行，因为更新不需要启用维护模式。
- 显示一条消息，表明所作更改需要重新启动系统，过程只需几分钟。
- 显示一条消息，表明所作更改需要重新引导系统，根据系统容量，过程约需 30 分钟。 在此期间，无法进行会议活动。

关闭维护模式时，**控制板**页面会刷新。 当**系统属性**页面上列出的所有虚拟机都显示状态良好（绿色）并且维护模式关闭时，表示您的系统已经就绪，可以让用户成功开始会议了。 请参阅开启或关闭 2.0 版及以前版本的维护模式，第 104 页以获取更多信息。

如果维护模式已关闭，而已安排的维护时段仍然处于活动状态，那么用户能够主持并参加之前已安排的会议，但在维护时段结束之前不能安排新的会议。

相关主题

安排维护时段，第 100 页
开启或关闭 2.0 版及以前版本的维护模式，第 104 页

开启或关闭 2.0 版及以前版本的维护模式

开启维护模式会关闭会议活动，并使用户无法登录 WebEx 站点、安排会议、加入会议和播放会议录制文件。 正在进行的会议将结束。 有关要求开启维护模式的系统任务的信息，请参阅关于维护模式。

开始之前

安排维护时段并告知用户预定的系统维护时间。 有关详细信息，请访问 安排维护时段，第 100 页。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**开启维护模式**。
系统将弹出**开启维护模式**对话框。 维护模式开启时，请务必阅览系统的情况。

步骤 3 如果准备开启系统维护或配置，请选择**继续**。
系统将显示表明系统处于维护模式的消息。 系统将显示**关闭维护模式**按钮。

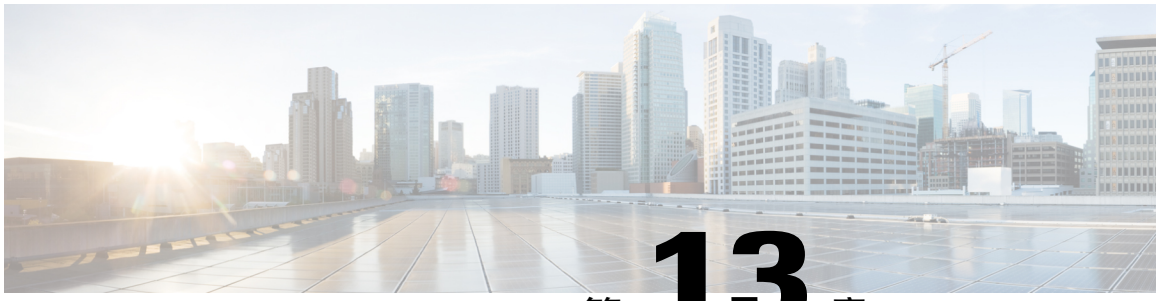
步骤 4 （可选）备份虚拟机。

步骤 5 完成配置系统后，请选择**关闭维护模式**。
当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。

步骤 6 （可选）要确定系统是否完全可用，选择**控制板** > **系统** > **查看更多内容**（在“系统”部分中）。
如果列出的所有虚拟机的**状态**均为**良好**（绿色），则会议活动可继续。

相关主题

安排维护时段，第 100 页
开启或关闭 2.0 版及以前版本的维护模式，第 104 页



第 13 章

管理用户

本节描述如何管理系统上的用户。

- 关于管理用户，第 105 页
- 创建逗号分隔或制表符分隔的文件，第 107 页
- 将用户帐户导出到 CSV 文件，第 113 页
- 从 CSV 文件导入用户帐户，第 113 页
- 利用 CSV 文件在系统之间传输用户帐户，第 114 页
- 添加用户，第 115 页
- 编辑用户，第 115 页
- 解锁管理员帐户，第 117 页
- 从用户页面激活或停用用户和管理员，第 117 页
- 查找用户，第 118 页
- 配置跟踪代码，第 118 页
- 配置目录集成，第 120 页
- 同步用户组，第 124 页
- 使用 CUCM 配置 AXL Web 服务和目录同步，第 124 页
- 使用 CUCM 配置 LDAP 集成和验证，第 125 页
- 向用户发送电子邮件，第 126 页

关于管理用户

您可以使用 GUI 逐个添加用户，也可以导入逗号分隔或制表符分隔 (CSV) 文件中存储的用户帐户。请参阅创建逗号分隔或制表符分隔的文件，第 107 页。

系统在使用期内支持最多 400,000 个用户帐户，该数字为活动和停用的用户帐户的总和。（此使用期最大用户帐户数非常大，足以适应任意组织用户数据库的预期增长。）

您可以添加和停用用户帐户，但不能进行删除。停用的用户可以在必要时重新激活。重新激活的用户帐户会重新获得其在被停用前能访问的会议、录制文件和其他数据的访问权。

用户帐户基于用户的电子邮件地址。如果用户的电子邮件地址在系统以外更改，用户可能无法使用系统，直到电子邮件地址重新一致。

为防止有人未经授权登录系统，请停用所有已离开组织的用户。可以通过以下方式停用用户：

- 如果系统不使用集成 SSO，您可以使用 GUI 逐个停用用户，也可以在 CSV 文件中将您要停用的所有用户的 ACTIVE 字段设置为 N，然后导入该文件。请参阅从用户页面激活或停用用户和管理员，第 117 页以获取更多信息。
- 如果系统使用集成 SSO，必须通过在 SAML 2.0 iDP 中将用户从企业目录中删除来停用用户。此过程无法在此产品中执行。
- 使用密码配置功能可在一段指定的时间后停用用户。请参阅配置常规密码设置，第 174 页以获取更多信息。

Cisco WebEx Meetings Server 发行版 2.5 有更多用户角色： SSO 管理员、LDAP 管理员和审核员。

审核员角色

审核员角色是创建用于需要审核登录以及由管理员执行的配置更改的情况的专用角色。审核员可以配置日志设置，生成应用程序审核日志，以满足公司安全性和 JITC 兼容性要求。审核员角色是具有以下特性的唯一角色：

- 在系统部署过程中可以创建单个审核员用户。系统部署之后，首个管理员可以创建任意多个审核员。（请参阅添加审核员角色，第 49 页。）
- 审核员只能登录管理站点 URL。
- 审核员只能查看和配置“审核员”标签页上的设置。
- 审核员只能作为访客用户出席会议。
- 审核员无法安排会议。

注释 如果未配置审核员，所有管理员都可以访问和配置“应用程序审核日志”设置（位于**设置**>**安全性**>**应用程序审核日志**页）和“日志内存使用情况”警告（位于**控制板**>**警告**>**编辑警告**页。如果配置了审核员，则管理员可以查看这些页面，但是无法对其进行修改。

创建逗号分隔或制表符分隔的文件

系统可以导入和导出包含在逗号分隔或制表符分隔(CSV)文件中的用户帐户值。（可以使用Microsoft Excel之类的电子表格应用程序来管理CSV文件。） 如果导入的CSV文件中的帐户不存在，系统将添加该帐户。 如果帐户存在，导入的CSV帐户值会替换当前值。

系统可以导出包含用户帐户值的CSV文件，用户可以对该文件进行修改，然后导回系统或新系统。

要成功导入CSV文件，必须满足以下条件：

- 表中列出的所有字段都是必填字段，不过字段值可以为空。如果漏填字段，系统会发出错误消息。 例如，
  文档格式不正确。 Custom10为必填项。
- CSV文件中的有效字符限于8位UCS转换格式(UTF-8)中包含的字符。
- 添加新用户帐户时，**用户标识**字段可以为空白，前提是**电子邮件**字段中的电子邮件地址未被其他用户帐户使用。 如果该电子邮件地址与另一用户帐户中的电子邮件地址匹配，系统就不会添加CSV文件中的用户帐户。
- 编辑用户帐户时，**用户标识**和**电子邮件**值必须匹配现有的用户帐户。 如果它们与用户帐户不匹配，当前值不会被更改为CSV值。
- 可以定义最多十个**跟踪代码组**。 跟踪代码组的名称应该是唯一的。 请勿将预定义的字段名称（USERID、ACTIVE、FIRSTNAME、LASTNAME、EMAIL、LANGUAGE、HOSTPRIVILEGE、TIMEZONE等）用作跟踪代码。

下表列出必填字段的名称、说明和可接受的值。

字段名	描述	值的大小和类型
USERID	用户标识。 **注释** 该字段由系统自动生成，必须在导入CSV文件时留空。	1到19个字母数字字符
ACTIVE	指示此用户是否活动。	Y或N
FIRSTNAME	用户的名。	1到32个字符的字符串
LASTNAME	用户的姓。	1到32个字符的字符串
EMAIL	用户的电子邮件地址。	1到192个字母数字字符的字符串
LANGUAGE	用户的语言。 请参阅CSV文件字段值，第109页以获取更多信息。	1到64个字符的字符串

字段名	描述	值的大小和类型
HOSTPRIVILEGE	主持人权限。	ADMN 或 HOST
TIMEZONE	用户所在的时区。 请参阅CSV 文件字段值，第 109 页以获取更多信息。	时区名称
DIVISION	用户的分部。 用于跟踪代码组 1。 此字段可在“跟踪代码”页面上配置。 请参阅配置跟踪代码，第 118 页以获取更多信息。	1 到 128 个字符的字符串
DEPARTMENT	用户的部门。 用于跟踪代码组 2。 此字段可在“跟踪代码”页面上配置。 请参阅配置跟踪代码，第 118 页以获取更多信息。	1 到 128 个字符的字符串
PROJECT	用户的项目。 用于跟踪代码组 3。 此字段可在“跟踪代码”页面上配置。 请参阅配置跟踪代码，第 118 页以获取更多信息。	1 到 128 个字符的字符串
OTHER	其他信息。 用于跟踪代码组 4。 此字段可在“跟踪代码”页面上配置。 请参阅配置跟踪代码，第 118 页以获取更多信息。	1 到 128 个字符的字符串
CUSTOM5	自定义字段 5。 请参阅配置跟踪代码，第 118 页以获取更多信息。	1 到 128 个字符的字符串
CUSTOM6	自定义字段 6。	1 到 128 个字符的字符串
CUSTOM7	自定义字段 7。	1 到 128 个字符的字符串
CUSTOM8	自定义字段 8。	1 到 128 个字符的字符串
CUSTOM9	自定义字段 9。	1 到 128 个字符的字符串
CUSTOM10	自定义字段 10。	1 到 128 个字符的字符串

有关其他信息，请参阅下列主题：

- 将用户帐户导出到 CSV 文件，第 113 页
- 从 CSV 文件导入用户帐户，第 113 页
- 利用 CSV 文件在系统之间传输用户帐户，第 114 页
- 配置跟踪代码，第 118 页

CSV 文件字段值

语言字段值

以下是可以在 CSV 文件中使用的国家/地区代码值示例。

字段值	语言
en-us	美国 英语
zh-cn	簡體中文
zh-tw	繁體中文
jp	JAPANESE
ko	韩文
fr	法語
de	德語
it	義大利語
es-me	卡斯提爾西班牙語
es	西班牙語（拉丁美洲）
nl	荷蘭語
pt-br	葡萄牙語
ru	俄語

时区字段值

以下是可在 CSV 文件中设置的时区 (TIMEZONE) 字段值。

字段值	GMT
马歇尔群岛	-12 小时
萨摩亚	-11 小时
檀香山	-10 小时

字段值	GMT
安克雷奇	-9 小时
旧金山	-8 小时
提华纳	-8 小时
亚利桑那	-7 小时
丹佛	-7 小时
奇瓦瓦	-7 小时
芝加哥	-6 小时
墨西哥	-6 小时
萨斯喀彻温	-6 小时
特古西加尔巴	-6 小时
波哥大	-5 小时
巴拿马	-5 小时
纽约	-5 小时
印地安那	-5 小时
加拉加斯	-4.5 小时
圣地亚哥	-4 小时
哈利法克斯	-4 小时
纽芬兰	-3.5 小时
巴西利亚	-3 小时
布宜诺斯艾利斯	-3 小时
累西腓	-3 小时
努克	-3 小时
中大西洋	-2 小时

字段值	GMT
亚述尔群岛	-1 小时
雷克雅维克	0 小时
伦敦	0 小时
卡萨布兰卡	0 小时
西非	1 小时
阿姆斯特丹	1 小时
柏林	1 小时
马德里	1 小时
巴黎	1 小时
罗马	1 小时
斯德哥尔摩	1 小时
雅典	2 小时
开罗	2 小时
比勒陀利亚	2 小时
赫尔辛基	2 小时
特拉维夫	2 小时
阿曼	2 小时
伊斯坦布尔	2 小时
利雅得	3 小时
内罗毕	3 小时
德黑兰	3.5 小时
莫斯科	4 小时
阿布扎比	4 小时

字段值	GMT
巴库	4 小时
喀布尔	4.5 小时
伊斯兰堡	5 小时
孟买	5.5 小时
科伦坡	5.5 小时
叶卡捷琳堡	6 小时
阿拉木图	6 小时
加德满都	6.75 小时
曼谷	7 小时
北京	8 小时
珀斯	8 小时
新加坡	8 小时
台北	8 小时
吉隆坡	8 小时
东京	9 小时
首尔	9 小时
阿得莱德	9.5 小时
达尔文	9.5 小时
雅库茨克	10 小时
布里斯班	10 小时
悉尼	10 小时
关岛	10 小时
霍巴特	10 小时

字段值	GMT
符拉迪沃斯托克	11 小时
所罗门群岛	11 小时
惠灵顿	12 小时
斐济	12 小时

将用户帐户导出到 CSV 文件

要导出 CSV 文件：

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**用户** > **导入/导出用户**。

步骤 3 选择**导出**。
用户数据将导出为 CSV 文件。 系统将向管理员发送电子邮件，其中包含可下载已导出文件的链接。

从 CSV 文件导入用户帐户

要将 CSV 文件导入系统：

开始之前

准备好含有用户帐户信息的逗号分隔或制表符分隔 (CSV) 的文件。 您可以将当前的系统用户帐户值导出到 CSV 文件，修改该文件，然后重新导入以添加或更改用户帐户。 请参阅 将用户帐户导出到 CSV 文件，第 113 页 和 创建逗号分隔或制表符分隔的文件，第 107 页 以获取更多信息。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**用户** > **导入/导出用户**。
系统将显示**导入/导出用户**页面。

步骤 3 选择**导入**。

系统将显示**导入用户**页面。

步骤 4 选择**浏览**，然后选择要导入的 CSV 文件。

步骤 5 选择**逗号**或**制表符**以指定要导入的 CSV 文件的类型：逗号分隔或制表符分隔。

步骤 6 选择**导入**。
将会导入文件，同时系统发送一封电子邮件，指示成功导入的用户帐户数以及未能添加或修改的帐户数。

接下来的操作

选择**用户**查看用户帐户，并验证这些值已被正确导入。

利用 CSV 文件在系统之间传输用户帐户

要利用 CSV 文件将一个系统的用户帐户复制到另一个系统，请执行以下操作：

步骤 1 在包含要传输的源用户帐户的系统上，登录管理站点。

步骤 2 选择**用户** > **导入/导出用户**。

步骤 3 选择**导出**。
用户数据将导出为 CSV 文件。 系统将向管理员发送电子邮件，其中包含可下载已导出文件的链接。

步骤 4 （可选）打开导出的CSV文件，根据需要修改用户帐户值，然后保存CSV文件。（有关更多信息，请参阅创建逗号分隔或制表符分隔的文件，第 107 页。）

步骤 5 登录目标系统管理站点。

步骤 6 选择**用户** > **导入/导出用户**。
系统将显示**导入/导出用户**页面。

步骤 7 选择**导入**。
系统将显示**导入用户**页面。

步骤 8 选择**浏览**，然后选择要导入的 CSV 文件。

步骤 9 选择**逗号**或**制表符**以指定要导入的 CSV 文件的类型：逗号分隔或制表符分隔。

步骤 10 选择**导入**。
将会导入文件，同时系统发送一封电子邮件，指示成功导入的用户帐户数以及未能添加或修改的帐户数。

接下来的操作

选择**用户**查看用户帐户，并验证这些值已被正确导入。

添加用户

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**用户** > **添加用户**。

步骤 3 选择帐户类型（**审核员**、**主持人**或**管理员**）。
尽管您可以看到审核员选项，但是该选项仅适用于首个管理员。

步骤 4 在字段中填写用户信息。 标有星号的字段是必填字段。

重要事项 用户在系统中由电子邮件地址进行识别。 如果用户电子邮件地址被更改并且用户保持活动，则 CWMS 上的电子邮件地址也必须更改，否则该用户将无法接收通知。

步骤 5 选择**保存**。
Cisco WebEx Meetings Server 会向用户发送包含**创建密码**链接的电子邮件。 用户必须先创建密码才能登录 WebEx 公共站点。

“创建密码”链接会在 72 小时后过期。 如果链接已过期，用户可以选择**忘记密码**链接，以接收一封新电子邮件以创建密码。

用户将被添加到系统中。

编辑用户

您可以用编辑用户功能来更改用户信息，以及激活或停用用户帐户。

注释 如果由于多次登录失败而导致管理员帐户被锁定，该管理员的**编辑用户**页上就会显示一条消息。另一个管理员可利用消息（显示在页面顶端）中的链接来解锁该管理员帐户。 有关详细信息，请访问 解锁管理员帐户，第 117 页。

简要步骤

1. 登录管理站点。
2. 选择**用户**。
3. 选择要编辑的用户。
4. 对可编辑的字段进行更改。 标有星号的字段是必填的。
5. （可选） 如果该用户为主持人，且需要永久许可证来定期召开会议，请选中**保留许可证**复选框。
6. （可选） 或者选中**要求用户在下次登录时更改密码**复选框。
7. 可选择激活或停用帐户：
   - 选择**激活**可重新激活非活动状态的帐户。
   - 选择**停用**可停用帐户。
8. 选择**保存**。 这将保存更改而不会变更帐户的状态。

详细步骤

步骤 1 登录管理站点。

步骤 2 选择**用户**。
系统将显示用户列表。 每个页面上出现的缺省用户数为 50 个。 或者您可以选择**每页用户数**下拉菜单，并将设置更改为 **50** 或 **100**。

步骤 3 选择要编辑的用户。

步骤 4 对可编辑的字段进行更改。 标有星号的字段是必填的。

步骤 5 （可选） 如果该用户为主持人，且需要永久许可证来定期召开会议，请选中**保留许可证**复选框。
请参阅关于主持人许可证，第 234 页以获取更多详细信息。

步骤 6 （可选） 或者选中**要求用户在下次登录时更改密码**复选框。

注释 如果您的系统上启用了 SSO 或 LDAP，将禁用此功能。

步骤 7 可选择激活或停用帐户：
   - 选择**激活**可重新激活非活动状态的帐户。
   - 选择**停用**可停用帐户。

注释 激活或停用帐户不会保存您已对该帐户所做的任何其他更改。 您必须选择**保存**来保存更改。

步骤 8 选择**保存**。 这将保存更改而不会变更帐户的状态。

解锁管理员帐户

为防止未经授权访问管理站点，系统可以自动锁定管理员帐户。此功能在缺省情况下关闭。可配置某一时间段（分钟）内的失败次数以及锁定持续时间等参数。（请参阅配置常规密码设置，第 174 页。）

以下小节介绍如何解锁帐户。

管理员通过电子邮件解锁自己的帐户

系统会向被锁定的管理员发送一封自动生成的电子邮件，指示其帐户已被锁定。在该电子邮件中，管理员可以点击**解锁帐户**按钮以解锁帐户。此选项在缺省情况下关闭。

管理员通过电子邮件解锁其他管理员的帐户

如果存在多个管理员帐户，那么每个管理员都会收到一封自动生成的电子邮件，指示某个帐户已被锁定。要解锁帐户，请在电子邮件中点击**用户配置文件**链接，以转至该管理员的**编辑用户**页面。然后在页面顶部显示的消息中点击**解锁管理员**链接，并通知该管理员帐户已解锁。此选项始终开启。

管理员在编辑用户页面上解锁其他管理员的帐户

某管理员的帐户被锁定后，被锁定管理员的**编辑用户**页面顶部会出现一条消息。尽管该管理员无法自己的**编辑用户**页面，但是其他管理员可以访问该页面，在显示的消息中点击**解锁管理员**链接，然后通知该管理员帐户已解锁。

等到定时器到期

当某管理员帐户被锁定时，如果设置了定时器，则被锁定管理员的**编辑用户**页面顶部会出现一条消息。定时器到期后，管理员可以再次尝试登录。

从用户页面激活或停用用户和管理员

使用此功能可激活停用的帐户或重新激活非活动状态的帐户。只有审核员帐户是您无法停用的帐户。或者，您可以通过在 CSV 文件中设置参数并将其导入来激活帐户。请参阅编辑用户，第 115 页以获取更多信息。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。所有数据中心都可以从此控制板进行管理。

步骤 2 选择**用户**。

步骤 3 选择要激活的任何非活动用户的复选框。或者选择要停用的任何活动用户的复选框。

步骤 4 选择**操作** > **激活**或**停用**。
所选帐户被修改并且每个帐户的状态反映了更新状态。

查找用户

您可以按类型（如处于活动状态或主持人）或按分配给主持人的许可证类型对用户进行排序。 除了对用户排序外，您还可以按名字、姓氏或全名以及按电子邮件地址来搜索用户。 搜索结果中将显示用户档案和许可证信息。

步骤 1 登录管理站点。

步骤 2 选择**用户**。

步骤 3 从下拉菜单中选择一个类别对用户进行排序。

步骤 4 （可选） 使用**到期时间**下拉列表可按许可证到期时间（已到期、1 个月、3 个月、6 个月）对拥有临时许可证的用户进行排序。

步骤 5 在搜索字段中输入用户的名称（名字、姓氏或全名）或电子邮件地址，然后选择**搜索**。

配置跟踪代码

您可以配置跟踪代码来跟踪指定组中的主机使用情况。 例如：您可以配置项目或部门的跟踪代码。 在添加或编辑用户时，配置的跟踪代码会显示为选项。

必须对每个跟踪代码进行以下配置：

- 跟踪代码组 - 配置跟踪代码组。 在添加和编辑用户时会使用跟踪代码组。 缺省值为部门、科室、项目、其他和自定义 5 至自定义 10。

  注释 跟踪代码组名称应该是唯一的，而且不应该使用预定义的字段名称（USERID、ACTIVE、FIRSTNAME、LASTNAME、EMAIL、LANGUAGE、HOSTPRIVILEGE、TIMEZONE）。

- 输入模式 - 选择**文本字段**或**下拉菜单**。
- 使用情况 - 选择**不使用**、**可选**或**必填**。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**用户** > **跟踪代码**。

步骤 3 在**跟踪代码组**栏中输入要配置的各个跟踪组的名称。

步骤 4 为每个跟踪代码选择**文本输入**或**下拉菜单**（**输入模式**栏）。

- 选择**文本输入**，并在文本字段中输入跟踪代码名称。
- 选择**下拉菜单**。 **编辑列表**链接显示在**输入模式**字段旁边。 选择**编辑列表**链接，以配置此跟踪代码的值。 请参阅编辑跟踪代码， 第 119 页以获取更多信息。

步骤 5 在**使用情况**栏中为每个跟踪代码选择**不使用**、**可选**或**必填**。
配置了下拉菜单列表后，应仅将使用情况更改为**必填**或**可选**。

步骤 6 选择**保存**。
会保存跟踪代码设置。

编辑跟踪代码

缺省情况下，跟踪代码将会作为文本框显示。 您也可通过创建跟踪代码列表的方式，在下拉菜单中显示跟踪代码选项。（另请参见配置跟踪代码， 第 118 页。)

开始之前

要编辑跟踪代码，必须先配置跟踪代码。 请参阅配置跟踪代码， 第 118 页。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 为每个跟踪代码选择**文本输入**或**下拉菜单**（**输入模式**栏）。

- 如果选择了**文本输入**，请在文本字段中输入跟踪代码名称。
- 如果选择了**下拉菜单**，**输入模式**字段旁就会出现**编辑列表**链接。 选择**编辑列表**链接，以配置此跟踪代码的值。

步骤 3 选择**编辑列表**链接。
系统将弹出**编辑跟踪代码列表**对话框。

步骤 4 配置**编辑跟踪代码列表**中的字段：

- 要在打开此对话框时只显示活动跟踪代码，请选择**仅显示激活的代码**。 取消选中此选项以显示所有跟踪代码。 第一次配置跟踪代码时，不能选择此选项。
- 在**代码**文本框中输入下拉菜单项名称。 限制： 128 个字符。 如果未显示空的跟踪代码，请选择**增加 20 行**来添加 20 个可配置的跟踪代码。 限制： 500 行（25 页）。
- 选择**缺省**来使此菜单项成为下拉菜单的缺省选项。

活动在缺省情况下已选中。 取消选中**活动**将使跟踪代码成为非活动状态。 非活动状态的跟踪代码不会出现在此跟踪代码组的下拉菜单中。

步骤 5 选择**更新**以保存设置。
将保存设置，并关闭**编辑跟踪代码列表**页面。

配置目录集成

目录集成使您的系统能用 Cisco Unified Communications Manager (CUCM) 用户数据库填充和同步 Cisco WebEx Meetings Server 用户数据库，然后与 LDAP 目录集成。

目录集成通过下列方式简化用户档案管理：

- 将用户档案从 CUCM 导入 Cisco WebEx Meetings Server 中。
- 定期用 CUCM 数据库中新的或修改过的用户属性更新 Cisco WebEx Meetings Server 数据库，例如每个用户的名、姓和电子邮件地址。 Cisco WebEx Meetings Server 通过用户的电子邮件地址区分用户，因此如果用户同名同姓但电子邮件地址不同，Cisco WebEx Meetings Server 会将其作为不同用户对待。
- 定期检查 CUCM 数据库中的非活动用户条目，并从 Cisco WebEx Meetings Server 数据库停用其用户档案。
- 允许系统使用 LDAP 验证来对照外部目录验证 Cisco WebEx Meetings Server 目录集成用户。
- 在 CUCM 和 LDAP 服务器上启用安全 LDAP (SLDAP) 的情况下支持完全加密的 LDAP 集成。
- 所有在 CUCM 中配置的用户都会同步到 Cisco WebEx Meetings Server，其帐户都会被激活。 在同步完成后，您可以有选择地停用帐户。 所有 CUCM 中的活动用户都会同步到 Cisco WebEx Meetings Server 中。 非活动用户不会被导入 Cisco WebEx Meetings Server 中。 （LDAP/AD 在 CUCM 中不可用或未配置的情况下，可以手动将用户添加到 CUCM 中。）

开始之前

在进行目录集成前，确保已满足下列前提条件：

- 把同步安排在非高峰时间或周末，以尽量减少对用户的影响。
- 验证您拥有受支持版本的 Cisco Unified Communications Manager (CUCM)。 有关更多信息，请访问 http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html。
- 获取 CUCM 管理用户凭证（有它才能添加用于目录集成的 CUCM 服务器）。
- 在 CUCM 上配置 AXL 和 LDAP 目录服务。 需要有 CUCM 才能将用户导入 Cisco WebEx Meetings Server 系统中。 请使用 CUCM 执行下列操作：

  启用 Cisco AXL Web 服务

  启用 Cisco 目录同步

  配置 LDAP 集成

配置 LDAP 验证

请参阅使用 CUCM 配置 AXL Web 服务和目录同步，第 124 页和使用 CUCM 配置 LDAP 集成和验证，第 125 页。 有关更多信息，请访问 http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html。

- 确保所有需要主持人权限的用户都在 CUCM 中可用。 所有不在 CUCM 中的用户都不能主持会议（所有用户都可作为访客加入）。 如有必要，创建仅由要从 CUCM 中导入的用户组成的 CUCM 组或过滤器。

注释 如果您不使用 CUCM 组，则所有活动的 CUCM 用户都会在您第一次目录同步期间导入到 Cisco WebEx Meetings Server 中。 不会导入非活动 CUCM 用户。 在随后的同步中只会导入活动的新用户和修改后用户。 必须在 Cisco WebEx Meetings Server 中停用您不想授予主持人访问权的用户。 请注意，只有在用户实际主持会议时，才会在 Cisco WebEx Meetings Server 中耗用主持人许可证。 不主持会议的帐户不耗用许可证。 请参见g_managingYourSystem.xml#topic_1213FB8D4C674F899219DF951AD6990B中的“管理许可证”了解更多关于许可证消耗的信息。

- 不会导入没有电子邮件地址的用户。
- 如果用户有多个同名同姓的帐户，但在 CUCM 上指定了不同的电子邮件地址，那么这些用户导入到 Cisco WebEx Meetings Server 时将被视为不同的用户。 CUCM 用户的用户名是唯一的，这样管理员就可以使用相同的电子邮件地址创建多个用户帐户。 但是，Cisco WebEx Meeting Server 上帐户的电子邮件地址是唯一的。 因此，如果多个 CUCM 用户帐户使用相同的电子邮件地址，CUCM 的管理员应该手动编辑这些用户帐户，以便在向 Cisco WebEx Meetings Server 导入这些帐户之前确保电子邮件地址唯一。
- 启用 LDAP 身份验证后，如果您选择**立即同步**或查看**下次同步**选项并输入日期和时间，Cisco WebEx Meetings Server 会使用端口 8443 与 CUCM 连接。
- Cisco WebEx Meetings Server 支持最多 64 个字符的密码。 在 CUCM 上创建用户时，请确保用户密码不超过 64 个字符。 密码超过 64 个字符的用户将无法登录 Cisco WebEx。

步骤 1 登录 Cisco WebEx Meetings Server 管理站点。

步骤 2 （可选） **开启维护模式**。
执行目录集成不需要维护模式，但大规模同步可能影响系统性能。 可以通过将系统转入维护模式来防止用户在同步期间使用系统。

步骤 3 选择**用户** > **目录集成**。

步骤 4 （可选） 选择服务器 (CUCM) 以输入 CUCM 服务器信息（如果尚未这么做）：

- IP 地址或标准域名 (FQDN)
- 用户名

- 密码

用户名密码可以是您的 CUCM 管理员或 AXL 用户名和密码。 配置 CUCM 信息后，CUCM 服务器的 IP 地址或 FQDN 会出现在 CUCM 图标下面。

注释 在配置 CUCM 信息后，若要更改它，过程会很复杂，可能引发用户同步问题，建议不要这样做。

步骤 5 选择**要过滤的 CUCM 用户组**以便仅将选定的 CUCM 用户组中的用户添加至 Cisco WebEx Meeting Server。

步骤 6 （可选） 选中**完全同步**可同步所有用户，取消选中此选项则仅同步新用户。（选择同步整个数据库时，根据用户数据库的大小，系统性能可能受影响。）

步骤 7 将 Cisco WebEx Meetings Server 系统与 LDAP 目录服务同步。 可以通过以下方式执行同步：

- 选择**立即同步**以立即执行同步。同步开始后不能取消。同步完成后，系统会向您发送一封电子邮件。系统上的其他管理员不会在**立即同步**后收到通知。
- 选择**下次同步**并输入步日期和时间来安排同步。 您可以选择定期**重复**同步。

如果选择**立即同步**，系统会立即执行同步。 如果您安排同步，它会发生在指定的日期和时间。 在安排的同步完成后，所有管理员都会收到电子邮件。 如果要阻止今后的同步，可以取消选中**下次同步**。

在同步过程中会映射下列属性：

CUCM 属性	**Cisco WebEx Meetings Server 属性**
名	名
姓	姓
邮件标识	电子邮件地址

注释 Cisco WebEx Meetings Server 中的名和姓是对用户显示的完整姓名的组成部分。

最终用户无法更新 Cisco WebEx Meetings Server 中映射的属性。

如果同步失败，页面上会显示一条错误消息，管理员还会收到包含关于错误的详细信息的电子邮件。 选择**查看日志**可查看错误的详细说明。 提供的日志包括停用用户报告、失败用户报告和摘要。

在您至少执行过一次同步后，系统会显示最近一次同步的摘要，其中表明同步是否完成，完成的时间及日期（使用在“公司信息”设置中配置的时间及日期）以及用户更改清单，包括：

- 已添加 — 添加的新用户数。
- 已停用 — 停用的用户数。

步骤 8 如果您配置或更改了同步安排或管理员通知设置，请选择**保存**。

步骤 9 选择**用户**标签页并确保同步了正确的用户。

a) 在下拉菜单上选择**远程用户**以过滤用户列表。 确保您要同步的用户在列表中。 远程用户将通过目录同步被导入 Cisco WebEx Meetings Server 中。 如果用户最初是在本地创建的，后来被目录同步覆盖，则该用户将成为远程用户，而非本地用户。

b) 选择**本地用户**以查看不包括在同步中的用户。 本地用户是 Cisco WebEx Meetings Server 管理员在本地创建的。 可以手动添加或使用 CSV 文件导入本地用户。

步骤 10 确保 CUCM 和 Cisco WebEx Meetings Server 同步安排是依次进行的。 必须先进行 CUCM 同步，紧接着进行 Cisco WebEx Meetings Server 同步。

步骤 11 （可选） 选中或取消选中**同步完成时通知管理员**，然后选择**保存**。 缺省情况下已选中此选项，系统仅在安排的同步完成后通知管理员。

步骤 12 选择**启用 LDAP 验证**。

注释 如果系统配置为使用 SSO，您必须先禁用 SSO。 请参阅禁用 SSO，第 219 页以获取更多信息。 如果系统未配置为使用 SSO，它会使用其缺省验证，直到您启用 LDAP 验证为止。

启用 LDAP 后，我们建议管理员使用 Active Directory 服务器进行用户管理，包括添加、禁用和修改用户。 在启用 LDAP 验证后，所有参加者都必须使用其 LDAP 凭证来登录 WebEx 站点。 但是，管理员仍可使用其 Cisco WebEx Meetings Server 凭证登录管理站点。

步骤 13 请确保用户能使用其 AD 域凭证登录系统。

步骤 14 （可选） 如果您使系统转入了维护模式，请选择**关闭维护模式**。

步骤 15 （可选） 如果您执行了同步，可以选择**立即通知**以通过电子邮件通知用户：已经在 Cisco WebEx Meetings Server 系统上为其创建了帐户或更改其帐户的时间。 您还可以选择**自动发送通知**，该选项在每次同步后自动向新添加的用户发送电子邮件。对验证设置进行任何更改（例如启用LDAP）后，系统会向有关用户发送“用户 - 密码已更改”电子邮件。

如果您选择**立即通知**

- 所有用户在其存在期间只会收到一次通知。 后续同步不会导致系统发送其他电子邮件。
- “需要通知的用户”指的是所有处于活动状态且尚未收到通知的用户。
- 不会对非活动用户或本地用户发送任何通知。
- 在 Cisco WebEx Meetings Server 上添加本地用户会使系统向该用户发送电子邮件。 但是，必须先在 CUCM Active Directory 服务器上添加该用户，他才能登录 WebEx 站点。
- 您只能向使用同步功能添加的用户发送通知。
- 电子邮件通知可能要过几分钟才会送到用户手中。 这一延迟是 Cisco WebEx Meetings Server 系统以外的多种因素造成的，包括电子邮件服务器、网络连接问题和个别电子邮件帐户上的垃圾邮件过滤器。

您的系统会发送下列电子邮件：

- “AD 激活”电子邮件发送给每个在同步中第一次被导入系统中的用户。 用户在后续同步时不会受到此电子邮件。
- “用户密码已更改”电子邮件发送给在系统上本地创建的用户。

有关自定义这些电子邮件模板的信息，请参阅关于电子邮件模板，第 178 页。

注释　如果您正在使用目录集成进行 LDAP 验证，那么 CUCM 中配置的用户将同步为 Cisco WebEx Meeting Server 的主持人，并使用其 LDAP 凭证来登录 WebEx 站点。 但是，如果您将导入用户的帐户类型从**主持人**更改为**管理员**，用户将收到带有“创建密码”链接的电子邮件。 用户将选择此链接并为 Cisco WebEx Meetings Server 输入新密码。 用户将使用这个新创建的密码登录管理站点，但也将继续使用 LDAP 凭证来登录他们的 WebEx 站点。

同步用户组

管理员可以在CUCM中创建用户组。 例如，管理员可以创建一个用户组，该用户组由允许使用Cisco WebEx Meetings Server 的用户组成。 从 CWMS 中，管理员可以通过选择特定的用户组过滤和导入特定的用户。

开始之前

使用 CUCM 创建用户组。 有关更多信息，请参阅*Cisco Unified Communications Manager* 管理指南 http://www.cisco.com/en/us/products/sw/voicesw/ps556/prod_maintenance_guides_list.html中的“用户管理配置”部分。

步骤 1　登录 Cisco WebEx Meetings Server 管理站点。

步骤 2　选择**用户** > **目录集成**。

步骤 3　选择**用于过滤的 CUCM 组**链接。

步骤 4　勾选要同步的用户组。

注释　如果没有选择组，那么目录集成会同步所有用户组。

步骤 5　选择**保存**。

步骤 6　选择“立即同步”以执行同步。 此过程所需时间取决于要同步的用户数。

注释　系统记得哪些用户组之前已同步。 如果您没有选择之前已同步的用户组，那么未选择的用户组中的用户将在同步期间被停用。

完成同步后，系统会显示添加和停用的用户数。

步骤 7　选择**查看日志**以了解有关在同步过程中导入或停用的用户的摘要信息。

使用 CUCM 配置 AXL Web 服务和目录同步

使用 CUCM 配置 AXL Web 服务和目录同步。

开始之前

请在使用目录集成功能前执行此过程。 请参阅配置目录集成， 第 120 页以获取更多信息。

步骤 1 登录 CUCM 帐户。

步骤 2 从右上角下拉菜单选择 **Cisco Unified 可服务性**，然后选择**执行**。

步骤 3 选择**工具** > **服务激活**。

步骤 4 选择 **Cisco AXL Web 服务**和 **Cisco DirSync**，然后选择**保存**。

注释 如果在作为多数据中心（MDC） 系统组成部分的数据中心上发生 Cisco Unified Call Manager (CUCM) 故障转移，则 CUCM 管理员凭证应对该数据中心中的所有 CUCM 都有效。

接下来的操作

如果尚未使用 CUCM 配置 LDAP 集成和验证，请执行该操作。 请参阅使用 CUCM 配置 LDAP 集成和验证， 第 125 页以获取更多信息。

使用 CUCM 配置 LDAP 集成和验证

使用 CUCM 配置 LDAP 集成和验证。

重要事项 用户在系统中由电子邮件地址进行识别。 如果用户电子邮件地址被更改并且用户保持活动，则 CWMS 上的电子邮件地址也必须更改，否则该用户将无法接收通知。

注释 如果将 CUCM 配置为目录集成，您就可以选择使用 SSO、LDAP 或本地身份验证。

开始之前

请在使用目录集成功能前执行此过程。 请参阅配置目录集成，第 120 页以获取更多信息。

步骤 1 登录 Cisco Unified Call Manager (CUCM) 帐户。

步骤 2 从右上角下拉菜单选择 **Cisco Unified CM 管理**，然后选择**执行**。

步骤 3 选择**文件** > **LDAP** > **LDAP 系统**。

步骤 4 选择**允许从 LDAP 服务器同步**，选择 **Microsoft Active Directory** 作为 LDAP 服务器类型，选择 **sAMAccountName** 作为 LDAP 的用户标识属性，并选择**保存**。

步骤 5 选择您的 LDAP 服务器的复选框，然后选择**新增**。

步骤 6 将“LDAP 目录”页面上的字段填写完整，然后选择**保存**。

步骤 7 在“LDAP 验证”页面上，选择**对最终用户使用 LDAP 验证**复选框，填写页面上的字段，然后选择**保存**。

接下来的操作

如果您尚未使用 CUCM 配置 Cisco AXL Web 服务和 Cisco 目录同步，请执行该操作。 请参阅使用 CUCM 配置 AXL Web 服务和目录同步，第 124 页以获取更多信息。

向用户发送电子邮件

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 要向用户发送电子邮件通知，请选择**用户** > **向用户发送电子邮件**。

步骤 3 在**收件人**字段中输入目标用户的电子邮件地址或电子邮件别名，或保留该字段为空，从而向所有用户发送电子邮件。

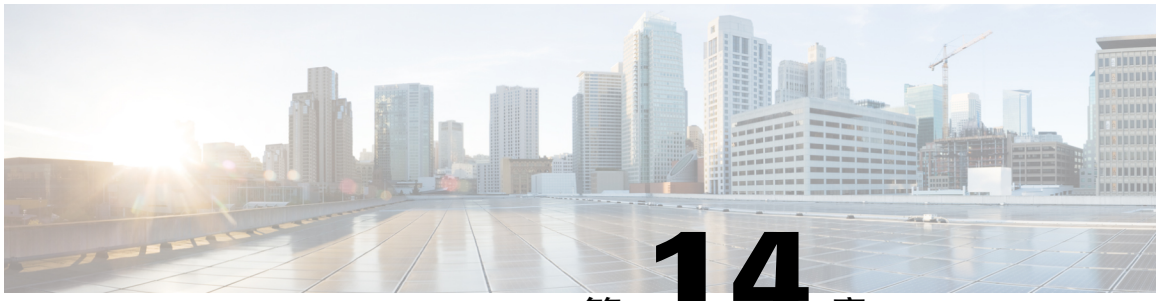
步骤 4 （可选） 在**密件抄送**字段中输入电子邮件地址或电子邮件别名。

步骤 5 在**主题**字段中输入主题。

步骤 6 在**消息**字段中输入消息。

步骤 7 选择**发送**。
用户可能要过几分钟才会收到电子邮件。 这一延迟可能是 Cisco WebEx Meetings Server 系统以外的多种因素造成的，包括电子邮件服务器、网络连接速度和个别电子邮件帐户上的垃圾邮件过滤器。

您的电子邮件已发送。



第 14 章

配置系统

本模块描述如何使用管理员页配置系统。

- 配置系统属性，第 127 页
- 配置常规设置，第 133 页
- 配置服务器，第 135 页
- 配置 SNMP 设置，第 141 页

配置系统属性

选择系统，然后在系统部分中选择查看更多内容来配置系统属性。

更改虚拟机设置

使用此功能可更改虚拟机设置。 请勿使用 VMware vCenter 更改虚拟机设置。

部署期间，您只能配置 IPv4 设置。 部署之后，如果您在 DMZ 网络的互联网反向代理和内部虚拟机之间有 IPv6 连接，则可以配置 IPv6 设置。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 开启维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
我们建议您给每个虚拟机拍摄快照。（请参阅通过使用 VMware vCenter 拍摄快照，第 7 页。）

在所有活动数据中心开启维护模式会关闭会议活动，并会使用户无法登录 WebEx 站点、安排会议、加入会议，或播放会议录制文件。 如果此数据中心属于多数据中心 (MDC) 系统，并且另一个数据中心是活动的，那么进

行中的会议将故障转移到活动的数据中心。 这可能会导致活动的会议暂时中断。 有关要求开启维护模式的系统任务的信息，请参阅关于维护模式。

步骤 3 选择**系统**，然后在系统部分选择**查看更多内容**。

步骤 4 要修改虚拟机的设置，请在主系统或高可用性系统部分选择虚拟机名称。

步骤 5 您可修改虚拟机的以下设置：

- 标准域名 (FQDN)（小写字符）
- 主 DNS 服务器
- 备用 DNS 服务器
- 子网掩码/前缀
- 网关

虚拟机字段变为灰色。 系统通过在 DNS 服务器中将主机名解析为虚拟机的 IP 地址自动获取 IP 地址。 有关更改虚拟机 IP 地址的更多信息，请参阅更改虚拟机的 IP 地址，第 128 页。

步骤 6 选择**保存**。
您所做的修改将会被保存，然后会重新启动虚拟机。

步骤 7 关闭维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。 如果此数据中心属于多数据中心 (MDC) 系统，那么管理员会被重定向至全局管理 URL。 管理员所看到的数据中心由 DNS 解析策略确定。 如果启用密钥再生，让一个数据中心退出维护模式会自动让系统中的所有数据中心退出维护模式。

此数据中心上用户的会议服务将被还原。

接下来的操作

如果要对任何虚拟机做出更改，您必须在每个数据中心的所有虚拟机上部署新证书，除非您正在使用同一域上的系统通配符证书。 有关更多信息，请参阅管理证书，第 205 页。

更改虚拟机的 IP 地址

如果更改部署中的虚拟机的主机名，将自动从 DNS 中选取相应的 IP 地址。 此过程说明如何更改虚拟机的 IP 地址并保持相同的主机名。

步骤 1 在 DNS 服务器中配置临时主机名。

步骤 2 完成更改虚拟机设置，第 127 页过程，以将虚拟机的主机名更改为在 DNS 服务器中输入的临时主机名。
系统退出维护模式后，新的临时主机名将生效。

作出此更改之后，部署中将不再包含原始主机名。

步骤 3 在 DNS 中将原始主機名稱的 IP 位址變更為新 IP 位址。

步骤 4 使用更改虚拟机设置，第 127 页过程将虚拟机的临时主机名更改为原始主机名。
系统退出维护模式后，原始主机名将生效。

这就配置了带新 IP 地址的原始主机名。

更改虚拟 IP 地址

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 开启维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
我们建议您给每个虚拟机拍摄快照。（请参阅通过使用 VMware vCenter 拍摄快照，第 7 页。）

在所有活动数据中心开启维护模式会关闭会议活动，并会使用户无法登录 WebEx 站点、安排会议、加入会议，或播放会议录制文件。 如果此数据中心属于多数据中心 (MDC) 系统，并且另一个数据中心是活动的，那么进行中的会议将故障转移到活动的数据中心。 这可能会导致活动的会议暂时中断。 有关要求开启维护模式的系统任务的信息，请参阅关于维护模式。

步骤 3 选择**系统**，选择数据中心，并在“系统”部分中选择**查看更多内容**。
系统将显示**属性**页面。

步骤 4 要修改 IP 地址，在“虚拟 IP 地址”部分选择“类型”列中的链接。

步骤 5 输入虚拟 IP 地址。

步骤 6 如果您已启用用于客户端连接的 IPv6，在 IPv6 地址列中输入虚拟 IP 地址、子网掩码和网关。
公共和专用虚拟 IP 地址必须在不同的 IPv6 子网上。

步骤 7 选择**保存**。

步骤 8 关闭维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。 如果此数据中心属于多数据中心 (MDC) 系统，那么管理员会被重定向至全局管理 URL。 管理员所看到的数据中心由 DNS 解析策略确定。 如果启用密钥再生，让一个数据中心退出维护模式会自动让系统中的所有数据中心退出维护模式。

此数据中心上用户的会议服务将被还原。

配置公开访问

公开访问功能允许外网的人员通过互联网或移动设备主持或出席在线会议。 删除公开访问功能将会删除 WebEx 站点 URL 的公共虚拟 IP 地址设置，并终止站点的外部访问功能。

通过使用 IRP 向系统中添加公开访问

互联网反向代理 (IRP) 的要求为：

- 对于单数据中心系统而言，用于添加或删除 IRP 的流程与 MDC 系统的流程相同。
- 添加数据中心至 MDC 系统时，所有数据中心都应配置为使用 IRP 或都不配置为使用 IRP。
- 每个数据中心使用一个 IRP 节点。
- 修改 IRP 要求系统处于维护模式。 在 MDC 系统中，可以逐个系统添加或删除 IRP，以避免服务中断。
- 在 MDC 环境中，在一个数据中心添加或删除本地公共 VIP 不会影响其他的数据中心。

有关内部互联网反向代理拓扑的说明，请参阅内部互联网反向代理 (IRP) 网络拓扑。

开始之前

要启用公开访问，必须先配置互联网反向代理虚拟机作为公开访问系统。 启动 VMware vCenter 并执行以下操作：

- 使用 VMware 数据恢复 (vSphere 5.0) 或 VMware vSphere 数据保护 (vSphere 5.1) 备份系统。 这使您可以在必要时恢复更改。 请参阅通过使用 VMware vCenter 创建备份，第 6 页以获取更多信息。
- 使用与部署管理虚拟机时相同的 OVA 文件来部署互联网反向代理虚拟机。 互联网反向代理虚拟机必须和公共虚拟 IP 地址位于同一子网上。

注释 如果您具有高可用性系统，则还必须针对高可用性系统部署互联网反向代理虚拟机。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 开启维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
我们建议您给每个虚拟机拍摄快照。（请参阅通过使用 VMware vCenter 拍摄快照，第 7 页。）

在所有活动数据中心开启维护模式会关闭会议活动，并会使用户无法登录 WebEx 站点、安排会议、加入会议，或播放会议录制文件。 如果此数据中心属于多数据中心 (MDC) 系统，并且另一个数据中心是活动的，那么进行中的会议将故障转移到活动的数据中心。 这可能会导致活动的会议暂时中断。 有关要求开启维护模式的系统任务的信息，请参阅关于维护模式。

步骤 3 选择**系统** > **查看更多内容**。

步骤 4 选择**添加公开访问**。

步骤 5 在 **FQDN** 字段中输入互联网反向代理虚拟机。
如果将系统配置为高可用性，那么会有两个标准域名 (FQDN) 字段。 在第二个字段中输入高可用性 FQDN。

步骤 6 选择**检测虚拟机**。
如果系统未被配置为高可用性，则会出现一个表格，显示互联网反向代理虚拟机。

如果系统被配置为高可用性，则会出现一个表格，显示主系统互联网反向代理虚拟机和高可用性互联网反向代理虚拟机。

如果您的系统有任何更新与用于创建互联网反向代理虚拟机的 OVA 版本不兼容，您会收到一条错误消息，并且无法继续进行，直到用相应 OVA 文件重新部署互联网反向代理虚拟机。

步骤 7 选择**继续**。

步骤 8 在**公共 (VIP) 虚拟 IPv4 地址**字段中输入用来配置互联网反向代理虚拟机的同一子网中的 IP 地址，然后选择**保存**。
将更新系统并配置公开访问。 在整个过程中不要关闭浏览器窗口。

如果您的系统需要进行微小更新（与用于创建互联网反向代理虚拟机的 OVA 版本兼容），这些更新会自动应用到您的互联网反向代理虚拟机。

步骤 9 如果您的系统需要进行微小更新，在更新完成后会提示您选择**重新启动**。
系统重启后，您将收到说明已添加公开访问的确认消息。

步骤 10 验证您的配置。 如果您感到满意，则可以删除在执行此过程之前配置的虚拟机备份。

步骤 11 选择**完成**。

步骤 12 验证您的安全证书仍有效。
由于此过程更改了虚拟机，可能会影响到您的证书。 必要时，系统将提供自签名证书以保持运作，直到您重新配置证书。 请参阅管理证书，第 205 页以获取更多信息。

步骤 13 对 DNS 服务器进行任何必要的更改。

步骤 14 关闭维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。 如果此数据中心属于多数据中心 (MDC) 系统，那么管理员会被重定向至全局管理 URL。 管理员所看到的数据中心由 DNS 解析策略确定。 如果启用密钥再生，让一个数据中心退出维护模式会自动让系统中的所有数据中心退出维护模式。

此数据中心上用户的会议服务将被还原。

删除公开访问功能

开始之前

使用 VMware 数据恢复或 VMware vSphere 数据保护来备份虚拟机。 请参阅通过使用 VMware vCenter 创建备份，第 6 页以获取更多信息。 确保在备份完成后启动虚拟机。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 开启维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
我们建议您给每个虚拟机拍摄快照。 （请参阅通过使用 VMware vCenter 拍摄快照， 第 7 页。）

在所有活动数据中心开启维护模式会关闭会议活动，并会使用户无法登录 WebEx 站点、安排会议、加入会议，或播放会议录制文件。 如果此数据中心属于多数据中心 (MDC) 系统，并且另一个数据中心是活动的，那么进行中的会议将故障转移到活动的数据中心。 这可能会导致活动的会议暂时中断。 有关要求开启维护模式的系统任务的信息，请参阅关于维护模式。

步骤 3 选择**系统**，然后选择系统部分中的**查看更多内容**链接。
系统将显示**属性**页面。

步骤 4 选择所需站点，选择**删除公开访问功能**，然后选择**继续**。
从您的站点中删除公开访问功能后，无法将相同的互联网代理虚拟机添加到该站点。 要重新配置公开访问功能，必须从 OVA 文件中重新部署互联网反向代理虚拟机以重新开始。 请参阅通过使用 IRP 向系统中添加公开访问， 第 130 页以获取更多信息。

会删除此站点的公开访问功能。

步骤 5 选择**完成**。

步骤 6 打开 VMware vCenter。 关闭互联网反向代理机和高可用性互联网反向代理机（如果已部署）并将其从系统中删除。

步骤 7 关闭维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。 如果此数据中心属于多数据中心 (MDC) 系统，那么管理员会被重定向至全局管理 URL。 管理员所看到的数据中心由 DNS 解析策略确定。 如果启用密钥再生，让一个数据中心退出维护模式会自动让系统中的所有数据中心退出维护模式。

此数据中心上用户的会议服务将被还原。

配置 IPv6 客户端连接

具有非水平分割网络拓扑时，具有 IPv6 客户端连接的所有用户（内部和外部）可以访问 WebEx 站点，使用公共 VIP 地址主持和访问网络会议。 已配置专用 IPv6 虚拟 IP 地址信息时，带 IPv6 客户端连接的管理员可以登录管理站点。

注释
- IPv6 专用虚拟 IP 地址必须与管理虚拟机处于相同的 IPv6 子网。
- IPv6 公共虚拟 IP 地址必须与互联网反向代理虚拟机处于相同的 IPv6 子网。

开始之前

配置 IPv6 客户端连接时，请考虑以下事项：

- 仅为非水平分割网络拓扑配置 IPv6 连接。

- 应已配置内部虚拟机和互联网反向代理的 IPv4 地址信息。
- 配置 IPv6 公共虚拟 IP 地址之前，应已配置 IPv4 专用和公共虚拟 IP 地址。
- 用于 IPv6 客户端连接的专用和公共虚拟 IP 地址位于不同的子网上。
- 配置 DNS 服务器，使管理站点 URL 指向专用 IPv6 和专用 IPv4 虚拟 IP 地址。
- 配置 DNS 服务器，使 WebEx 站点 URL 指向公共 IPv6 和公共 IPv4 虚拟 IP 地址。

步骤 1 登录管理站点。

步骤 2 选择**开启维护模式** > **继续**。

步骤 3 选择**系统**，然后选择系统部分中的**查看更多内容**链接。

步骤 4 在“虚拟 IP 地址”部分，选择**类型**栏中的某个链接。

- 选择公共链接以配置用于访问 WebEx 站点 URL 的 IPv6 地址。
- 选择专用链接以配置用于访问管理 URL 的 IPv6 地址。

“专用或公共虚拟 IP 地址”页面显示之前输入的 WebEx 站点 URL 和管理 URL 的 IPv4 IP 地址、子网掩码和网关 IP 地址。

步骤 5 在 IPv6 **地址**栏中，输入 WebEx 站点 URL 和管理 URL 的 IPv6 IP 地址、子网掩码和网关 IP 地址。

步骤 6 选择**保存**。

步骤 7 选择**关闭维护模式** > **继续**。
关闭维护模式后系统将重启。 完成重启后，您可以再次登录管理站点。

配置常规设置

常规设置包括下列参数：

- 站点设置 - 对站点 URL 进行管理
- 管理站点设置 - 对管理站点 URL 进行管理

虚拟 IP 地址显示在信息块中，并且可以通过以下菜单管理：**系统** > **属性**。

更改站点设置

使用此功能配置或更改管理站点 URL，以及本地管理站点 URL（如果您有多数据中心 (MDC) 系统）。 您可以在部署期间配置原始站点 URL。 在 MDC 系统中，您可以在加入数据中心过程中配置本地站点 URL。 有关站点 URL 配置及命名约定的更多信息，请参阅WebEx 站点和 WebEx 管理 URL，第 26 页。

开始之前

确保您在 DNS 服务器上保留原始站点 URL，并将原始站点 URL 重定向至更新的站点 URL。 如果用户尝试使用尚未重定向到新 URL 的原始 URL，那么他们将无法从网页、快捷会议工具和移动应用程序主持或加入会议或者进行登录。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 开启维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
我们建议您给每个虚拟机拍摄快照。 （请参阅通过使用 VMware vCenter 拍摄快照，第 7 页。）

在所有活动数据中心开启维护模式会关闭会议活动，并会使用户无法登录 WebEx 站点、安排会议、加入会议，或播放会议录制文件。 如果此数据中心属于多数据中心 (MDC) 系统，并且另一个数据中心是活动的，那么进行中的会议将故障转移到活动的数据中心。 这可能会导致活动的会议暂时中断。 有关要求开启维护模式的系统任务的信息，请参阅关于维护模式。

步骤 3 选择**系统** > （**配置/常规设置**）**查看更多内容**。
系统将弹出“常规设置”窗口。

步骤 4 选择数据中心（如果此为 MDC 系统）。

步骤 5 在要修改的“站点设置”部分，选择**编辑**。

步骤 6 输入 URL，然后选择**保存**。

步骤 7 关闭维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。 如果此数据中心属于多数据中心 (MDC) 系统，那么管理员会被重定向至全局管理 URL。 管理员所看到的数据中心由 DNS 解析策略确定。 如果启用密钥再生，让一个数据中心退出维护模式会自动让系统中的所有数据中心退出维护模式。

此数据中心上用户的会议服务将被还原。

接下来的操作

更新站点证书以确保安全访问。 请参阅管理证书，第 205 页以获取更多信息。

更改管理设置

您可以在部署期间配置原始管理站点 URL 设置。 在 MDC 系统中，您可以在加入数据中心过程中配置本地管理站点 URL。 有关管理站点配置及命名约定的更多信息，请参阅WebEx 站点和 WebEx 管理 URL，第 26 页。

开始之前

确保在 DNS 服务器上保留原始管理站点 URL。 将原始管理站点 URL 重定向到更新后的管理站点 URL。 如果用户尝试使用尚未重定向到新 URL 的原始 URL，那么他们将无法从网页、快捷会议工具和移动应用程序主持或加入会议或者进行登录。

步骤 1 登录管理站点。

步骤 2 开启维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
我们建议您给每个虚拟机拍摄快照。 （请参阅通过使用 VMware vCenter 拍摄快照， 第 7 页。）

在所有活动数据中心开启维护模式会关闭会议活动，并会使用户无法登录 WebEx 站点、安排会议、加入会议，或播放会议录制文件。 如果此数据中心属于多数据中心 (MDC) 系统，并且另一个数据中心是活动的，那么进行中的会议将故障转移到活动的数据中心。 这可能会导致活动的会议暂时中断。 有关要求开启维护模式的系统任务的信息，请参阅关于维护模式。

步骤 3 选择**系统**。

步骤 4 在“配置”部分，选择**查看更多内容**。

步骤 5 在管理设置部分选择**编辑**。

步骤 6 在对话框中输入新的管理站点 URL，然后选择**保存**。

步骤 7 关闭维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。 如果此数据中心属于多数据中心 (MDC) 系统，那么管理员会被重定向至全局管理 URL。 管理员所看到的数据中心由 DNS 解析策略确定。 如果启用密钥再生，让一个数据中心退出维护模式会自动让系统中的所有数据中心退出维护模式。

此数据中心上用户的会议服务将被还原。

接下来的操作

更新站点证书以确保安全访问。 请参阅管理证书， 第 205 页以获取更多信息。

配置服务器

使用这些功能来配置服务器：

- SMTP 服务器 - SMTP 服务器将处理从 Cisco WebEx Meeting Server 向目标发送电子邮件的任务。
- 存储服务器 - NFS 服务器是存储所有会议录制文件的存储服务器。

配置电子邮件 (SMTP) 服务器

配置电子邮件服务器可使系统能向用户发送会议邀请和其他通信。

务必要保证电子邮件服务器始终可运行。 电子邮件是与用户通信的主要方式，这些通信包括录制文件通知、会议信息更改、帐户状态和许多其他重要公告。 （另请参阅添加用户，第 115 页。）

重要事项 用户在系统中由电子邮件地址进行识别。 如果用户电子邮件地址被更改并且用户保持活动，则 CWMS 上的电子邮件地址也必须更改，否则该用户将无法接收通知。

注释 更改这些属性不需要开启维护模式。

步骤 1 登录管理网站。

步骤 2 选择**系统**，然后在服务器部分选择**查看更多内容**。

步骤 3 在**SMTP 服务器**部分，选择**编辑**。

步骤 4 输入系统将用于发送电子邮件的邮件服务器的标准域名（FQDN）。

步骤 5 （可选） 选择**启用 TLS** 以启用传输层安全性 (TLS)。（缺省情况下已启用基本验证。）

步骤 6 （可选） 编辑**端口**字段以更改缺省值。
SMTP 缺省端口号为 25 或 465（安全 SMTP 端口）。

注释 Web 节点和管理节点会将 SMTP 请求发送到已配置的电子邮件服务器。 如果在内部 Web 及管理虚拟机与电子邮件服务器之间有防火墙，则SMTP通信可能被拦截。要确保电子邮件服务器配置和电子邮件通知正常工作，必须在电子邮件服务器与 Web 及管理虚拟机之间打开端口 25 或 465（安全 SMTP 端口号）。

步骤 7 （可选） 要启用邮件服务器验证，选择**启用服务器验证**。 如果您启用了验证，输入系统访问公司邮件服务器所需的**用户名**和**密码**凭证。
系统电子邮件的发件人为 admin@<WebEx-site-URL>。 请确保邮件服务器能够识别出该用户。

对于微型、小型或中型系统，电子邮件通知来自管理虚拟机（主系统或高可用性系统）。

对于大型系统，电子邮件通知来自 Web 虚拟机（主系统或高可用性系统上）。 在大型系统中，主系统上存在三个 Web 虚拟机，高可用性系统上存在一个 Web 虚拟机。

步骤 8 选择**保存**。

接下来的操作

另请参阅从用户页面激活或停用用户和管理员，第 117 页、添加用户，第 115 页和编辑用户，第 115 页。

配置存储服务器

使用存储服务器备份您的系统以及会议录制文件。 在灾难恢复（请参阅通过使用存储服务器进行灾难恢复，第 139 页）期间，可以使用这些备份来还原系统。 （支持的存储方法为网络文件系统 (NFS)）。 验证存储服务器可从所有内部虚拟机访问。 （另外还可使用 VMware 提供的 VMware 数

据恢复功能，以便为虚拟机备份。 有关更多信息，请参阅http://www.vmware.com/pdf/vdr_11_admin.pdf。）

不必将存储服务器连接到外部虚拟机，例如外部互联网反向代理 (IRP) 服务器。

限制

请勿在 Cisco WebEx Meetings Server 使用的 NFS 共享中手动创建文件或目录，因为它会在 NFS 文件和目录上运行各种脚本。 NFS 存储服务器必须为 Cisco WebEx Meetings Server 专用。

存储服务器每日备份以下内容：

- 某些系统设置
- 用户信息
- 会议信息
- 上传到系统中的 SSL 证书
- 站点 URL

备份每日执行，并且设置为当地时间早上 4:20 启动。 Cisco WebEx Meetings Server 在备份过程中保持运行，不会中断任何会议、录制文件或其他功能。 系统不删除之前的备份，直到接下来的每日备份完成，以确保备份可用。

系统备份 500 MB 要花大约五分钟。 备份系统所花的时间取决于存储速度、NFS 速度和其他因素。 70 GB 数据库大约花一小时进行备份，花 10 分钟将其传输到 NFS 中。 传输率为 12 MB/秒，以便其他网络通信能够正常工作，并确保产品持续运行。

开始之前

确保配置 Unix 访问权限以使系统可存储用户生成的内容和系统备份。

在基于 Linux 的存储系统上，这取决于您为要用于网络文件系统 (NFS) 的特定目录配置的匿名用户读/写权限。

在基于 Windows 的存储系统上，这取决于**网络访问： 让 Everyone 权限应用于匿名用户**设置。 此外，您必须为 Everyone 用户组提供对 NFS 的读和写权限。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 开启维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
我们建议您给每个虚拟机拍摄快照。 （请参阅通过使用 VMware vCenter 拍摄快照，第 7 页。）

在所有活动数据中心开启维护模式会关闭会议活动，并会使用户无法登录 WebEx 站点、安排会议、加入会议，或播放会议录制文件。 如果此数据中心属于多数据中心 (MDC) 系统，并且另一个数据中心是活动的，那么进行中的会议将故障转移到活动的数据中心。 这可能会导致活动的会议暂时中断。 有关要求开启维护模式的系统任务的信息，请参阅关于维护模式。

步骤 3 在“服务器”部分，选择**服务器** > （**服务器**）**查看更多内容**。

如果系统中存在存储服务器，则会显示在此页上。 如果系统中没有存储服务器，那么您可以配置一个存储服务器。

步骤 4 在存储服务器部分，选择**立即添加存储服务器**。

步骤 5 输入 NFS 装入点并选择**保存**。
系统确认 NFS 装入点。

步骤 6 选择**继续**。
您会收到一条确认消息，确认已添加存储服务器。

步骤 7 选择**完成**。

步骤 8 （可选） 您可以更改每日备份的缺省时间。 在“存储服务器”部分，单击系统备份安排**时间**，然后从下拉菜单选择其他时间。 然后选择**保存**。
系统会在您所选的时刻执行每日备份。

步骤 9 关闭维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。 如果此数据中心属于多数据中心 (MDC) 系统，那么管理员会被重定向至全局管理 URL。 管理员所看到的数据中心由 DNS 解析策略确定。 如果启用密钥再生，让一个数据中心退出维护模式会自动让系统中的所有数据中心退出维护模式。

此数据中心上用户的会议服务将被还原。

接下来的操作

配置系统以将存储服务器用于下列项：

- 会议录制文件。
- 灾难恢复。 请参阅通过使用存储服务器进行灾难恢复， 第 139 页以获取更多信息。

为了确保存储服务器正确运行，请确保

- 可以从 Cisco WebEx Meetings Server 之外访问存储服务器。
- 存储服务器已启动。
- 存储服务器有网络连接。
- 从非 Cisco WebEx Meetings Server 计算机进行装入/访问。
- 存储服务器未满。

注释 如果用户不小心从 **Cisco WebEx Meeting 录制文件**页面删除了录制文件，但该录制文件保存在网络文件系统 (NFS) 存储服务器上，可联系 Cisco 技术支持中心 (TAC) 获取恢复录制文件的帮助。

通过使用存储服务器进行灾难恢复

灾难可能是网络崩溃、服务器故障、数据中心断电或其他使系统无法使用的活动。 有以下两种灾难恢复：

- 单数据中心 (SDC) 灾难恢复 — 您可以在相同的数据中心重新安装 SDC 系统，并通过使用存储服务器备份将其还原到相同的状态。
- 多数据中心 (MDC) 灾难恢复 — 如果一个数据中心出现故障，您可以通过备份数据中心访问 MDC 系统，还原损坏的数据中心，并加入数据中心以还原 MDC 系统。

在配置存储服务器后，系统将每天进行备份。 控制板上将出现系统备份通知，包含与最近备份有关的信息。 存储中一次仅保留一个备份系统。 执行升级或更新之后，保留前一个 Cisco WebEx Meetings Server 版本的备份。 建议不同的 Cisco WebEx Meetings Server 安装不要使用同一个存储目录。

请注意，灾难恢复将：

- 花费至少 30 分钟时间
- 用最近备份中的设置覆盖您的设置
- 需要您执行额外步骤来还原用户的服务（在本节的后续步骤中有详细描述）

此过程备份某些系统设置、用户信息、会议信息、上传到系统中的 SSL 证书，以及站点 URL。 备份过程不存储各个虚拟机的 VMware 凭证或 IP 地址信息。（另外还可使用 VMware 提供的 VMware 数据恢复功能，以便为虚拟机备份。 有关更多信息，请参阅http://www.vmware.com/pdf/vdr_11_admin.pdf。） 如果执行灾难恢复，必须手动再次应用某些设置，包括：

- 到某些外部组件的连接，例如 Cisco Unified Communications Manager (CUCM)。
- SSL 证书（如果灾难恢复系统的主机名不同于原始系统的主机名）。
- 在单数据中心系统上，您可以选择使用相同的 IP 地址或主机名。 在多数据中心系统上，您可以选择使用主系统的原始 IP 地址或主机名。

在因灾难发生而使您无法使用系统后执行此过程。

开始之前

要执行灾难恢复过程：

- 必须配置存储服务器。 如果不配置存储服务器，**灾难恢复**选项将不可用并且不创建备份。 请参阅配置存储服务器，第 136 页以获取更多信息。
- 您必须能够访问可在其中恢复部署的系统。 请参阅下面有关单数据中心 (SDC) 和多数据中心 (MDC) 灾难恢复的信息。
- 恢复系统的部署大小和软件版本必须与原系统保持一致。

对于高可用性 (HA) 系统，必须先配置灾难恢复，然后在该系统上配置 HA。 如果 HA 系统需要进行灾难恢复，那么必须先还原系统，然后在还原的系统上配置HA。 有关HA的更多信息，请参阅添加高可用性系统，第 55 页。

步骤 1 在可以恢复部署的系统上登录管理站点。

步骤 2 开启维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
我们建议您给每个虚拟机拍摄快照。 （请参阅通过使用 VMware vCenter 拍摄快照，第 7 页。）

在所有活动数据中心开启维护模式会关闭会议活动，并会使用户无法登录WebEx站点、安排会议、加入会议，或播放会议录制文件。 如果此数据中心属于多数据中心 (MDC) 系统，并且另一个数据中心是活动的，那么进行中的会议将故障转移到活动的数据中心。 这可能会导致活动的会议暂时中断。 有关要求开启维护模式的系统任务的信息，请参阅关于维护模式。

步骤 3 选择**系统** > > > **服务器** > **添加存储服务器**。

步骤 4 在 **NFS 装入点**字段中输入存储服务器的名称，然后选择**保存**。

示例：
192.168.10.10:/CWMS/backup。

步骤 5 选择**继续**以继续进行灾难恢复。
如果恢复系统的部署大小和软件版本与原系统相匹配，则可以继续进行灾难恢复。 如果系统具有不同的部署大小或软件版本，那么您无法继续进行下去，直到将应用程序重新部署到恢复系统中，使部署大小和软件版本与原始部署相符。 IP 地址或主机名不一定要与您的原始部署匹配。

步骤 6 选择以下措施之一继续：

- **取消** - 在添加存储服务器之前备份已有的系统。 备份系统之后，将返回到该页面，然后选择**继续**来继续进行。
- **继续** - 覆盖已有的系统并继续进行灾难恢复。

灾难恢复过程开始。 如果关闭浏览器，将无法重新登录系统，直到过程完成。

步骤 7 关闭维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。 如果此数据中心属于多数据中心 (MDC) 系统，那么管理员会被重定向至全局管理 URL。 管理员所看到的数据中心由 DNS 解析策略确定。 如果启用密钥再生，让一个数据中心退出维护模式会自动让系统中的所有数据中心退出维护模式。

此数据中心上用户的会议服务将被还原。

接下来的操作

必须执行以下过程来恢复用户的服务：

- 重新配置电话会议设置。 有关更多信息，请参阅《规划指南》中的“配置 CUCM”。

- 重新配置 SSO 设置。 请参阅配置联合单点登录 (SSO) 设置，第 216 页以获取更多信息。
- 重新配置 SNMP 设置。 请参阅配置 SNMP 设置，第 141 页以获取更多信息。
- 重新配置证书。 如果 SSL 证书与恢复系统上配置的 SSL 证书不匹配，可能需要重新加载 SSL 证书。 请参阅还原 SSL 证书，第 211 页以获取更多信息。
- 已恢复系统最初配置为免许可证模式，有效期将为 180 天。 将先前系统许可证重新托管在已恢复系统上。 请参阅执行重大系统修改之后重新托管许可证，第 240 页 和 关于许可证 以获取更多信息。
- 配置 DNS 设置以使站点 URL 指向当前 VIP。 已还原的系统上的 VIP 可能与原系统上的 VIP 不同。 必须完成 DNS 配置以使最终用户能使用他们的原始链接在已还原的系统上进行登录或加入会议。 请参阅更改虚拟 IP 地址，第 129 页以获取更多信息。
- 如果为系统配置了目录集成并启用了 LDAP 验证，请验证 CUCM 凭证有效。 使系统退出维护模式并完成系统重启后，登录管理站点，选择**用户** > **目录集成**，然后选择**保存**。 如果您的 CUCM 凭证不正确，您会收到**无效的凭证**错误消息。 如果收到此错误消息，输入正确的凭证并再次选择**保存**。 请参阅配置目录集成，第 120 页以获取更多信息。

配置 SNMP 设置

您可以配置以下 SNMP 设置：

- 团体字符串 - SNMP 团体字符串验证对 MIB 对象的访问并且起到嵌入密码的作用。
- USM 用户 - 配置基于用户的安全性 (USM) 以提供附加的消息级别安全性。 可以选择现有 USM 配置进行编辑或添加其他 USM 配置。 除了对 MIB 信息有读写权限的缺省 USM 用户 serveradmin 外，配置的所有新 USM 用户对 MIB 信息只有只读权限。
- 通知目标 - 使用此功能可配置陷阱/通知接收者。

配置团体字符串

可以添加和编辑团体字符串以及团体字符串访问权限。

添加团体字符串

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 开启维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
我们建议您给每个虚拟机拍摄快照。 （请参阅通过使用 VMware vCenter 拍摄快照，第 7 页。）

在所有活动数据中心开启维护模式会关闭会议活动，并会使用户无法登录 WebEx 站点、安排会议、加入会议，或播放会议录制文件。 如果此数据中心属于多数据中心 (MDC) 系统，并且另一个数据中心是活动的，那么进

行中的会议将故障转移到活动的数据中心。 这可能会导致活动的会议暂时中断。 有关要求开启维护模式的系统任务的信息，请参阅关于维护模式。

步骤 3 选择**系统**，然后选择 SNMP 部分中的**查看更多内容**链接。

步骤 4 在团体字符串部分选择**添加**。

步骤 5 在**团体字符串**页面上填写以下字段。

选项	描述
团体字符串名称	请输入团体字符串名称。 最大长度： 256 个字符。
访问权限	设置团体字符串的访问权限。 选项包括： • 只读 • 读写 • 读写通知 • 仅通知 • 无 **缺省：** 只读
主机 IP 地址信息	选择主机 IP 地址信息类型。（缺省： **接受任何主机发送的 SNMP 包**） 如果选择**接受来自这些主机的 SNMP 数据包**，那么选项下方将出现对话框。输入主机名和 IP 地址，以逗号分隔。

选择**添加**。

团体字符串将添加到系统。

步骤 6 关闭维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。 如果此数据中心属于多数据中心 (MDC) 系统，那么管理员会被重定向至全局管理 URL。 管理员所看到的数据中心由 DNS 解析策略确定。 如果启用密钥再生，让一个数据中心退出维护模式会自动让系统中的所有数据中心退出维护模式。

此数据中心上用户的会议服务将被还原。

编辑团体字符串

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 开启维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
我们建议您给每个虚拟机拍摄快照。 （请参阅通过使用 VMware vCenter 拍摄快照，第 7 页。）

在所有活动数据中心开启维护模式会关闭会议活动，并会使用户无法登录 WebEx 站点、安排会议、加入会议，或播放会议录制文件。 如果此数据中心属于多数据中心 (MDC) 系统，并且另一个数据中心是活动的，那么进行中的会议将故障转移到活动的数据中心。 这可能会导致活动的会议暂时中断。 有关要求开启维护模式的系统任务的信息，请参阅关于维护模式。

步骤 3 选择**系统**，然后选择 SNMP 部分中的**查看更多内容**链接。

步骤 4 在团体字符串部分选择团体字符串名称链接。

步骤 5 在**编辑团体字符串**页面上更改需要的字段。

选项	描述
团体字符串名称	更改团体字符串名称。 最大长度： 256 个字符。
访问权限	设置团体字符串的访问权限： • 只读 • 读写 • 读写通知 • 仅通知 • 无 **缺省：** 只读
主机 IP 地址信息	选择主机 IP 地址信息类型。 **缺省：** 接受任何主机发送的 SNMP 包 **接受这些主机发送的 SNMP 包：** 选择下面出现一个对话框。 输入主机名和 IP 地址，以逗号分隔。

选择**编辑**。

团体字符串信息已更改。

步骤 6 关闭维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。 如果此数据中心属于多数据中心 (MDC) 系统，那么管理员会被重定向至全局管理 URL。 管理员所看到的数据中心由 DNS 解析策略确定。 如果启用密钥再生，让一个数据中心退出维护模式会自动让系统中的所有数据中心退出维护模式。

此数据中心上用户的会议服务将被还原。

配置 USM 用户

可以添加和编辑 USM 用户。

添加 USM 用户

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 开启维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
我们建议您给每个虚拟机拍摄快照。 （请参阅通过使用 VMware vCenter 拍摄快照，第 7 页。）

在所有活动数据中心开启维护模式会关闭会议活动，并会使用户无法登录 WebEx 站点、安排会议、加入会议，或播放会议录制文件。 如果此数据中心属于多数据中心 (MDC) 系统，并且另一个数据中心是活动的，那么进行中的会议将故障转移到活动的数据中心。 这可能会导致活动的会议暂时中断。 有关要求开启维护模式的系统任务的信息，请参阅关于维护模式。

步骤 3 选择**系统**，然后选择 SNMP 部分中的**查看更多内容**。

步骤 4 在USM 用户部分选择**添加**。

步骤 5 填写**添加 USM 用户**页面上的字段。

选项	描述
USM 用户名	输入要配置的 USM 用户名。 最多 256 个字符。
安全级别	选择安全级别。 所选的安全级别确定可以为用户设置的算法和密码。 选项包括： • noAuthNoPriv - 既不为用户设置验证算法和密码，也不设置保密算法和密码。 • authPriv - 使您能够为用户配置验证算法和密码以及保密算法和密码。 • authNoPriv — 使您能够为用户配置验证算法和密码。 **缺省：** noAuthNoPriv
身份验证算法	为用户选择验证算法。 **注释** 仅当安全级别设置为 **authPriv** 或 **authNoPriv** 时，才出现此选项。 **缺省：** SHA
验证密码	为用户输入验证密码。 **注释** 仅当安全级别设置为 **authPriv** 或 **authNoPriv** 时，才出现此选项。

选项	描述
隐私算法	为用户选择保密算法。 **注释** 仅当安全级别设置为 **authPriv** 时，才出现此选项。 **缺省：** AES128
保密密码	为用户输入保密密码。 **注释** 仅当安全级别设置为 **authPriv** 时，才出现此选项。

步骤 6 选择**添加**。
USM 用户将添加到系统。

步骤 7 关闭维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。 如果此数据中心属于多数据中心 (MDC) 系统，那么管理员会被重定向至全局管理 URL。 管理员所看到的数据中心由 DNS 解析策略确定。 如果启用密钥再生，让一个数据中心退出维护模式会自动让系统中的所有数据中心退出维护模式。

此数据中心上用户的会议服务将被还原。

编辑 USM 用户

注释 缺省 USM 用户 serveradmin 供内部使用。 管理员可以更改 serveradmin 用户的 USM 用户名和保密密码，但无法更改该用户的安全性级别、验证算法或保密算法。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 开启维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
我们建议您给每个虚拟机拍摄快照。 （请参阅通过使用 VMware vCenter 拍摄快照，第 7 页。）

在所有活动数据中心开启维护模式会关闭会议活动，并会使用户无法登录 WebEx 站点、安排会议、加入会议，或播放会议录制文件。 如果此数据中心属于多数据中心 (MDC) 系统，并且另一个数据中心是活动的，那么进

行中的会议将故障转移到活动的数据中心。 这可能会导致活动的会议暂时中断。 有关要求开启维护模式的系统任务的信息，请参阅关于维护模式。

步骤 3 选择**系统**，然后选择 SNMP 部分中的**查看更多内容**。

步骤 4 在USM 用户部分选择 USM 用户。

步骤 5 在**编辑 USM 用户**页面上更改需要的字段。

选项	描述
USM 用户名	更改 USM 用户名。 最多 256 个字符。
安全级别	选择安全级别。 所选的安全级别确定可以为用户设置的算法和密码。 选项包括： • noAuthNoPriv - 既不为用户设置验证算法和密码，也不设置保密算法和密码。 • authPriv - 使您能够为用户配置验证算法和密码以及保密算法和密码。 • authNoPriv — 使您能够为用户配置验证算法和密码。 **缺省：** noAuthNoPriv
身份验证算法	为用户选择验证算法。 **注释** 仅当安全级别设置为 **authPriv** 或 **authNoPriv** 时，才出现此选项。 **缺省：** SHA
验证密码	更改用户的验证密码。 **注释** 仅当安全级别设置为 **authPriv** 或 **authNoPriv** 时，才出现此选项。
隐私算法	为用户选择保密算法。 **注释** 仅当安全级别设置为 **authPriv** 时，才出现此选项。 **缺省：** AES128
保密密码	更改用户的保密密码。 **注释** 仅当安全级别设置为 **authPriv** 时，才出现此选项。

步骤 6 选择**编辑**。
已更改 USM 用户信息。

步骤 7 关闭维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。 如果此数据中心属于多数据中心 (MDC) 系统，那么管理员会被重定向至全局管理 URL。 管理员

所看到的数据中心由 DNS 解析策略确定。 如果启用密钥再生，让一个数据中心退出维护模式会自动让系统中的所有数据中心退出维护模式。

此数据中心上用户的会议服务将被还原。

配置通知目标

您可以在系统上配置虚拟机以便为下列事件生成 SNMP 通知或陷阱：

- 虚拟机启动（冷启动陷阱）
- 所有警告条件

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 开启维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
我们建议您给每个虚拟机拍摄快照。 （请参阅通过使用 VMware vCenter 拍摄快照，第 7 页。）

在所有活动数据中心开启维护模式会关闭会议活动，并会使用户无法登录 WebEx 站点、安排会议、加入会议，或播放会议录制文件。 如果此数据中心属于多数据中心 (MDC) 系统，并且另一个数据中心是活动的，那么进行中的会议将故障转移到活动的数据中心。 这可能会导致活动的会议暂时中断。 有关要求开启维护模式的系统任务的信息，请参阅关于维护模式。

步骤 3 选择**系统**，然后选择 SNMP 部分中的**查看更多内容**链接。

步骤 4 选择**添加新的通知目标**（在**通知目标**下）。

步骤 5 为通知目标配置以下字段：

选项	描述
目标主机名称/IP 地址	要设置为通知目标的虚拟机的主机名或 IP 地址。
端口号	虚拟机的端口号。 **缺省：** 162
SNMP 版本	您的 SNMP 版本。 **缺省：** V3
通知类型	选择**通知**或**陷阱**。 **缺省：** 陷阱

选项	描述
USM 用户 注释 只有在 SNMP 版本设置为 V3 时才会出现此选项。	选择 USM 用户。 请参阅配置 USM 用户，第 144 页以获取更多信息。
团体字符串 注释 只有在 SNMP 版本没有设置为 V3 时才会出现此选项。	选择团体字符串。 请参阅配置团体字符串，第 141 页以获取更多信息。

步骤 6 选择**添加**。
会添加通知目标。

步骤 7 关闭维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。 如果此数据中心属于多数据中心 (MDC) 系统，那么管理员会被重定向至全局管理 URL。 管理员所看到的数据中心由 DNS 解析策略确定。 如果启用密钥再生，让一个数据中心退出维护模式会自动让系统中的所有数据中心退出维护模式。

此数据中心上用户的会议服务将被还原。

编辑通知目标

配置通知目标

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 开启维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
我们建议您给每个虚拟机拍摄快照。（请参阅通过使用 VMware vCenter 拍摄快照 à la page 7。）

在所有活动数据中心开启维护模式会关闭会议活动，并会使用户无法登录 WebEx 站点、安排会议、加入会议，或播放会议录制文件。 如果此数据中心属于多数据中心 (MDC) 系统，并且另一个数据中心是活动的，那么进行中的会议将故障转移到活动的数据中心。 这可能会导致活动的会议暂时中断。 有关要求开启维护模式的系统任务的信息，请参阅关于维护模式。

步骤 3 选择**系统**，然后选择 SNMP 部分中的**查看更多内容**链接。

步骤 4 从**通知目标**列表中选择通知目标链接。

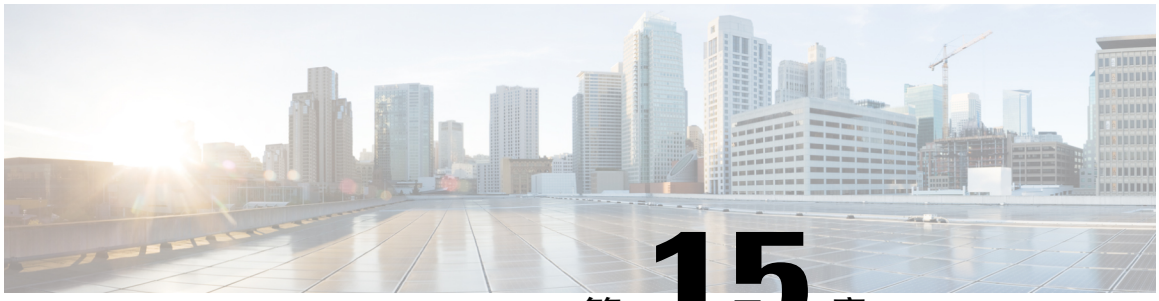
步骤 5 您可以为通知目标编辑以下字段：

选项	描述
目标主机名称/IP 地址	要设置为通知目标的虚拟机的主机名或 IP 地址。
端口号	虚拟机的端口号。 **缺省：** 162
SNMP 版本	您的 SNMP 版本。 **缺省：** V3
通知类型	选择**通知**或**陷阱**。 **缺省：** 通知
USM 用户 **注释** 只有在 SNMP 版本设置为 V3 时才会出现此选项。	选择 USM 用户。 请参阅配置 USM 用户，第 144页以获取更多信息。
团体字符串 **注释** 只有在 SNMP 版本没有设置为 V3 时才会出现此选项。	选择团体字符串。 请参阅配置团体字符串，第141页以获取更多信息。

步骤 6 选择**保存**。
将保存对通知目标的更改。

步骤 7 关闭维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。 如果此数据中心属于多数据中心 (MDC) 系统，那么管理员会被重定向至全局管理 URL。 管理员所看到的数据中心由 DNS 解析策略确定。 如果启用密钥再生，让一个数据中心退出维护模式会自动让系统中的所有数据中心退出维护模式。

此数据中心上用户的会议服务将被还原。



第 15 章

配置设置

本模块描述如何配置设置。

- 配置公司信息，第 151 页
- 配置定制设置，第 153 页
- 配置会议设置，第 154 页
- 关于配置音频设置，第 157 页
- 配置视频设置，第 171 页
- 配置移动设备设置，第 171 页
- 配置服务质量 (QoS)，第 172 页
- 配置密码，第 173 页
- 配置电子邮件设置，第 177 页
- 关于应用程序下载，第 203 页
- 管理证书，第 205 页
- 上传安全登录警告消息，第 222 页
- 配置应用程序审核日志，第 223 页
- 配置安全登录警告，第 224 页

配置公司信息

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 （可选） 要更改语言设置，选择**开启维护模式**。

修改**公司信息**页面上的其他设置时不必开启维护模式。

在所有活动数据中心开启维护模式会关闭会议活动，并会使用户无法登录 WebEx 站点、安排会议、加入会议，或播放会议录制文件。 如果此数据中心属于多数据中心 (MDC) 系统，并且另一个数据中心是活动的，那么进行中的会议将故障转移到活动的数据中心。 这可能会导致活动的会议暂时中断。 有关要求开启维护模式的系统任务的信息，请参阅关于维护模式。

步骤 3 选择**设置**。 如果正在查看其他设置页面，还可以选择设置部分下的**公司信息**。

步骤 4 将页面上的字段填写完整，然后选择**保存**。

选项	描述
公司名称	公司或组织名称。
地址 1	地址行 1。
地址 2	地址行 2。
县/市	您所在的城市。
省/自治区	所在的省/市/自治区的名称。
邮政编码	邮政编码。
国家□地区	所在的国家/地区名称。
业务电话	含有国家/地区代码的下拉菜单和业务电话（含区号）的字段。
时区	所在时区。
语言	所用语言。 语言设置影响： • 管理员首次激活其管理员帐户时看到的登录页面 • 报告语言。 （请参阅 管理报告 ， 第 225 页
区域设置	区域设置。区域设置会影响时间、日期、货币及数字的显示。

步骤 5 （可选） 如果您更改了语言，请选择**关闭维护模式**，然后选择**继续**以确认。
当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。 如果此数据中心属于多数据中心 (MDC) 系统，那么管理员会被重定向至全局管理 URL。 管理员所看到的数据中心由 DNS 解析策略确定。 如果启用密钥再生，让一个数据中心退出维护模式会自动让系统中的所有数据中心退出维护模式。

配置定制设置

开始之前

在配置定制设置之前请准备好下列内容：

- 一张含有公司徽标的图像（大小为 120x32，格式为 PNG、GIF 或 JPEG）
- 公司的隐私权声明 URL
- 公司的服务条款声明 URL
- 公司的支持 URL

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**设置** > **定制**。

步骤 3 将页面上的字段填写完整，然后选择**保存**。

选项	描述
公司徽标	徽标文件。 徽标必须为 PNG、JPEG 或 GIF 格式。 最大尺寸为 120x32 像素，最大文件大小为 5 MB。
隐私权声明	公司的隐私权声明 URL。
服务条款	公司的服务条款 URL。
自定义页脚文本	您输入的文本显示在系统发送的所有最终用户和管理员网页和电子邮件的页脚中。
标题背景颜色	选择此选项以关闭缺省的背景色，包括所有的浏览器工具条和电子邮件。
在线帮助	选择适用于您的环境的在线帮助选项。 如果用户被阻止访问互联网，选择自定义的帮助选项，并输入公司视频、用户指南和常见问题解答的 URL。
支持联系人 URL	公司支持网页的 URL。

删除公司徽标

开始之前

创建尺寸为 120x32 的透明 PNG 文件或 GIF 文件。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**设置** > **定制**。

步骤 3 为公司徽标字段选择**浏览**并选择尺寸为 120x32 的透明 PNG 文件或 GIF 文件。

步骤 4 选择**保存**。
先前的公司徽标会替换为空白 PNG 文件或 GIF 文件。 确认已删除原先的徽标。

配置会议设置

配置会议设置以控制参加者可以使用哪些功能：

- 加入会议设置
- 每个会议的最大参加者人数（会议规模）
- 参加者权限

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**设置** > **会议**。

步骤 3 在加入会议设置部分，选择选项。
缺省设置为**允许参加者在主持人之前加入会议**、**允许参加者在主持人之前加入电话会议**以及**第一个与会者将成为主讲者**。

如果您取消选中**允许参加者在主持人之前加入会议**，则将自动取消选中**第一个参加者将成为主讲者**功能。

如果选中了**允许参加者在主持人之前加入会议**和**允许参加者在主持人之前加入电话会议**，参加者最多可以提前 15 分钟加入会议。 或者，选择**任何人都可在会议中演示**。

步骤 4 拖动滑块来选择每个会议的最大参加者人数：

参加者人数设置	系统容量
50	带或不带 HA 的 50 个用户的系统（单数据中心）

参加者人数设置	系统容量
250	带或不带 HA 的 250 个用户的系统（单数据中心） 不带 HA 的 250 个用户的系统（多数据中心）
500	带或不带 HA 的 800 个或 2000 个用户的系统（单数据中心） 不带 HA 的 800 个或 2000 个用户的系统（多数据中心） [5]

此设置会受到在部署期间配置的系统容量的限制。 请参阅确认系统容量，第 21 页以获取更多信息。

步骤 5 在**参加者权限**部分，选择选项。
聊天、**投票**、**文档审阅与演示**和**共享与远程控制**在缺省情况下被选中。 在用户控制中会出现选中的参加者权限。

步骤 6 选择**录制**以在存储服务器上录制和存储会议。

a) 选择**当会议录制文件准备就绪时向主持人和与会者发送通知电子邮件**，以允许系统向主持人以及收到会议邀请的所有用户发送电子邮件通知。

b) 选择**仅限登录用户查看和下载录制文件**，以仅允许系统用户，而不是访客，查看或下载会议录制文件。

缺省情况下，禁用录制。

必须配置存储服务器以启用录制。 请参阅配置存储服务器，第 136 页以获取更多信息。

步骤 7 选择**文件传输**以允许用户在会议期间共享文件。

步骤 8 选择**保存**。

关于会议录制文件

Cisco WebEx Meetings Server 根据以下因素启用不同的会议安全功能：

- 用户类型： 主持人、候补主持人、用户（已登录）和嘉宾。
- 会议有无密码。
- 密码在会议邀请中隐藏或可见。
- 密码在会议邀请电子邮件中隐藏或可见。
- 会议加入页上显示的动作（请参阅以下表格）。

表 *1*：安排会议时已排除密码

用户类型	密码显示在邀请和提醒电子邮件中	会议详细信息页
主持人	是	是
候补主持人	是	是
受邀者	否	否
转发的受邀者	否	否

表 *2*：安排会议时已包含密码

用户类型	密码显示在邀请和提醒电子邮件中	会议详细信息页
主持人	是	是
候补主持人	是	是
受邀者	是	是
转发的受邀者	是	是

- “在主持人之前加入”功能开启或关闭：

  开启： 受邀者或访客可以在会议开始前 15 分钟至会议结束时加入会议。

  关闭。受邀者或访客不能在主持人之前加入会议。 主持人或候补主持人可以先开始会议，然后受邀者可以加入。

- “在主持人之前加入电话会议”功能开启或关闭：

  开启：即使主持人未在会议客户端开始电话会议，受邀者也可以在主持人之前加入电话会议。

  关闭。 如果主持人未在会议客户端开始电话会议，则受邀者无法在主持人之前加入电话会议。

- “首个参加者可以演示”功能开启或关闭：

  开启： 已配置“在主持人之前加入”功能时，首个参加者为主讲者。

  关闭。 主持人始终为主讲者。

关于配置音频设置

第一次配置音频设置时，向导会引导您完成整个过程，帮助您设置CUCM SIP配置和呼入接入号码。完成向导操作并配置初始音频设置后，您可以配置所有其他音频设置。

在继续进行音频配置前必须先启用电话会议，并配置CUCM。如果您计划提供电话会议高可用性，那么必须在两个系统上配置CUCM。请参阅《规划指南》以获取更多信息。要继续进行，必须获取以下信息：

- 参加者用于进入会议的呼入接入号码清单
- CUCM IP 地址
- （可选）有效的安全会议证书（如果您打算使用 TLS/SRTP 电话会议加密） 请参阅导入安全电话会议证书，第 214 页以获取更多信息。

注释 此功能在俄罗斯或土耳其不可用。

首次配置音频设置

首次配置音频设置时，向导会指导您完成安装过程。 您必须在此过程中配置 Cisco Unified Communications Manager (CUCM)。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 开启维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
我们建议您给每个虚拟机拍摄快照。 （请参阅通过使用 VMware vCenter 拍摄快照，第 7 页。）

在所有活动数据中心开启维护模式会关闭会议活动，并会使用户无法登录WebEx站点、安排会议、加入会议，或播放会议录制文件。 如果此数据中心属于多数据中心 (MDC) 系统，并且另一个数据中心是活动的，那么进行中的会议将故障转移到活动的数据中心。 这可能会导致活动的会议暂时中断。 有关要求开启维护模式的系统任务的信息，请参阅关于维护模式。

步骤 3 选择**设置** > **音频**。
系统将显示**音频**页面，其中包括“当前音频功能”。

步骤 4 选择**下一步**。
系统将显示 **SIP 配置**页面。 此页面显示配置 CUCM 所需的 SIP 配置参数，包括每个服务器类型的 IP 地址和端口号。

步骤 5 选择**下一步**。
启用电话会议： CUCM 设置页面出现，显示当前设置。

步骤 6 选择**编辑**以更改设置。

系统将弹出 **CUCM (Cisco Unified Communications Manager)** 对话框。

步骤 7 按以下所示填写 **CUCM (Cisco Unified Communications Manager)** 对话框中的字段：

a) 为 CUCM 1 IP 地址（或 CUCM 2 IP 地址）输入 IP 地址。
这些 IP 地址需要与主 CUCM 节点以及可选的备用 CUCM 节点相符，这些节点属于在设备池中设置的 Cisco Unified Communications Manager 组，而设备池在 CUCM 的应用程序服务器 SIP 中继上进行配置。 有关更多详细信息，请参阅《规划指南》中的“为应用程序服务器配置 SIP 中继”：http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html。

注释 CUCM 2 不是必需的，但是建议用它实现电话会议高可用性。

b) 输入系统的端口号。 端口号必须与 CUCM 中分配的端口号相匹配。（**缺省值**： 5062)

c) 使用**传输**下拉菜单来选择系统的传输类型。 （**缺省值**： TCP)
如果您选择 TLS 作为传输类型，则必须为每个 CUCM 服务器导入有效的安全会议证书，导出 SSL 证书并将其上传到 CUCM，然后将系统的标准域名 (FQDN) 配置为每个 CUCM 服务器上的 SIP 域名。 有关导入证书的更多信息，请参阅导入安全电话会议证书，第 214 页。有关在 CUCM 上管理呼叫控制的更多信息，请参阅《规划指南》中的“配置 Cisco Unified Communications Manager (CUCM)”。

d) 选择**继续**。

新的或已更新的 CUCM 设置将显示在**启用电话会议： CUCM 设置**页面。

步骤 8 选择**下一步**。
启用电话会议： 系统将显示接入号码设置页面。

步骤 9 选择**编辑**。
系统将弹出**呼入接入号码**对话框。

步骤 10 选择**添加**以添加呼入接入号码。
对话框中将添加一行，用于输入电话标签和号码。 每次选择**添加**，都会在对话框中新增一行。

步骤 11 在添加完号码后，为添加的每个接入号码输入**电话标签**和**电话号码**，然后选择**继续**。
确保仅添加在 CUCM 中配置过的号码。 添加的号码会显示在电子邮件邀请中和 Cisco WebEx Meetings 客户端中。

示例：
输入“Headquarters”至**电话标签**中，输入 `888-555-1212` 至**电话号码**中。
输入的接入号码将添加到系统中，并返回到**启用电话会议： 接入号码设置**页面。 现在，页面显示已配置的接入号码的数量。

步骤 12 选择**保存**。
向导会通知您已经成功配置了电话会议功能。

步骤 13 （可选）在**显示名称**对话框中输入显示名称。

步骤 14 （可选）在**呼叫者标识**对话框中输入有效的呼叫者标识。
呼叫者标识仅限于数字字符和破折号 (-)，并且最长为 32 个字符。

步骤 15 （可选） 配置WebEx 呼叫我设置（**缺省：** 按 1 以连接到会议）。 选择此选项来忽略按下 **1** 以连接到会议的要求。

注释 除非您的电话系统无法发送数字 **1**，否则建议您不要选择此选项。

步骤 16 （可选） 选择**电话的进入与退出声音**。

- 嘀嘀声（缺省值）
- 无声音
- 播放姓名

步骤 17 （可选） 如果系统支持且已配置 IPv6，请将 **IPv6 电话会议**设置设定为**开**或**关**。（**缺省值：** 关闭。 设定为**关闭**表示该设置为 IPv4。）

步骤 18 选择用户在拨入 WebEx 会议的音频部分或使用“呼叫我”服务时听到的**系统音频语言**。

步骤 19 选择**保存**。

步骤 20 关闭维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。 如果此数据中心属于多数据中心 (MDC) 系统，那么管理员会被重定向至全局管理 URL。 管理员所看到的数据中心由 DNS 解析策略确定。 如果启用密钥再生，让一个数据中心退出维护模式会自动让系统中的所有数据中心退出维护模式。

此数据中心上用户的会议服务将被还原。

配置音频设置

开始之前

首次配置音频设置时，请参阅首次配置音频设置，第 157 页。

注释 不需要开启“维护模式”即可以配置或更改“群拨”、“呼入服务语言”、“显示名称”或“呼入者标识”音频设置。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 开启维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
我们建议您给每个虚拟机拍摄快照。（请参阅通过使用 VMware vCenter 拍摄快照，第 7 页。）

在所有活动数据中心开启维护模式会关闭会议活动，并会使用户无法登录 WebEx 站点、安排会议、加入会议，或播放会议录制文件。 如果此数据中心属于多数据中心 (MDC) 系统，并且另一个数据中心是活动的，那么进

行中的会议将故障转移到活动的数据中心。 这可能会导致活动的会议暂时中断。 有关要求开启维护模式的系统任务的信息，请参阅关于维护模式。

步骤 3 选择**设置** > **音频**。

步骤 4 选择**全局设置**。 配置音频功能设置。

音频配置有全局设置，并且每个数据中心都有本地设置。 全局设置适用于所有数据中心。 本地设置适用于单个数据中心。

选项	描述
WebEx 音频	• 用户呼入和呼叫我服务 - 能够使用户通过拨打指定的电话号码或接听来自系统的呼叫我电话来参加电话会议。 • 呼入 - 能够使用户通过拨打指定的电话号码来参加电话会议。 会议主持人无法开始群拨会议。 • 关闭 - 禁用所有呼叫功能。 会议主持人无法开始 WebEx 音频会议、群拨会议，或个人会议。
个人会议	• 选中**启用个人会议**复选框，以允许用户开始和拨入个人会议。 • 选择**允许参加者先于主持人加入个人会议**，以允许参加者通过仅输入参加者访问码开始个人会议的音频部分；无需主持人 PIN。
使用计算机连接语音	• **开** 允许计算机语音连接。 • **关** 拒绝计算机语音连接。

步骤 5 配置群拨（请参阅关于 WebEx 群拨，第 163 页）。

步骤 6 在编辑电话会议设置部分，选择 CUCM (Cisco Unified Communications Manager) 下的**编辑**链接来更改设置。

在 MDC 系统中，每个数据中心都必须连接至 Cisco Unified Call Manager (CUCM)。 多数据中心可以共享一个 CUCM 或者每个数据中心都与一个 CUCM 相关联。 CUCM 在 MDC 系统中的配置与在单数据中心 (SDC) 系统中的配置相同。

选项	描述
CUCM 1 IP 地址	输入 CUCM 1 系统的主机名或 IP 地址。
CUCM 2 IP 地址	（可选）输入 CUCM 2（负载平衡）系统的主机名或 IP 地址。 **注释** CUCM 2 不是必需的，但是建议用它实现电话会议高可用性。
端口号	请输入有效的端口号。 确保端口号与 CUCM 中的设置相匹配。 **缺省：** 5062

选项	描述
传输	选择传输类型。 如果您选择 TLS 作为传输类型，则必须为每个 CUCM 服务器导入有效的安全会议证书，导出 SSL 证书，将 SSL 证书上传到 CUCM 中，然后将系统的标准域名 (FQDN) 配置为每个 CUCM 服务器上的 SIP 域名。 有关导入证书的更多信息，请参阅导入安全电话会议证书，第 214 页。有关 CUCM 的更多信息，请参阅《*Cisco WebEx Meetings Server* 规划指南》中的“配置 CUCM”。 **缺省：** TCP

系统将弹出 **CUCM (Cisco Unified Communications Manager)** 对话框。 将字段填写完整，然后选择**继续**。

步骤 7 在“呼入接入号码”部分中选择**编辑**，以添加、更改或删除接入号码。

a) 选择**添加**，然后输入您想添加的每个新接入号码的电话标签和电话号码。要删除号码，请选择位于行末的**删除**链接。
b) 在想更改的任何接入号码的电话标签和电话号码字段中输入更新的信息。
c) 选择**继续**。
在主页上选择**保存**后，您的更改才会被保存。

确保仅添加在 CUCM 中配置过的号码。 添加的号码会显示在电子邮件邀请中和 Cisco WebEx Meetings 客户端中。

步骤 8 在“呼入服务语言”部分选择**编辑**，以添加、更改或删除用户可用于呼入会议音频部分的语言。

a) 选择**添加**并输入与每个呼入号码相关联的所需路由模式，以便为呼入会议音频部分的用户提供语言选择。呼叫与路由模式相关联的呼入号码的所有用户都可以从配置的语言选择中进行选择。 例如，如果您将英语、西班牙语和法语配置为语言选择，当用户呼叫与该路由模式相关联的呼入号码时，呼叫者听到英语致辞，但是也可以选择西班牙语或法语。 如果用户选择西班牙语，初始音频提示则为西班牙语。

注释 缺省语言可以通过以下菜单设置：**设置** > **音频** > **全局设置** > **系统音频语言**。

b) 要删除条目，选择位于行末的 **X**。
c) 要更改条目，键入不同的路由模式，并选择不同的语言设置。
d) 选择**继续**。
在页面底部选择**保存**后，您的更改才会被保存。

确保仅添加在 CUCM 中配置过的路由模式。

步骤 9 使用**传输**下拉菜单，选择系统的传输类型和各个服务器的端口。（**缺省值：** TCP)
如果您选择 TLS 作为传输类型，则必须为每个 CUCM 服务器导入有效的安全会议证书，导出 SSL 证书并将其上传到 CUCM，然后将系统的标准域名 (FQDN) 配置为每个 CUCM 服务器上的 SIP 域名。 有关导入证书的更多信息，请参阅导入安全电话会议证书，第 214 页。有关在 CUCM 上管理呼叫控制的更多信息，请参阅《规划指南》中的“配置 Cisco Unified Communications Manager (CUCM)”。

确保端口号与 CUCM 中的设置相匹配。

步骤 10 在**显示名称**对话框中输入显示名称。

使用“呼叫我”服务或呼入 Cisco WebEx Meeting Server (CWMS) 时，该名称会显示在会议参加者的 IP 电话上。

步骤 11 在**呼叫者标识**对话框中输入有效的呼叫者标识。
呼叫者标识仅限于数字字符和破折号 (-)，并且最长为 32 个字符。

步骤 12 配置WebEx 呼叫我设置（**缺省：** 按 1 以连接到会议）。 或者，选择此选项来忽略按 **1** 以连接到会议的要求。
除非您的电话系统无法发送数字 **1**，否则建议您不要选择此选项。

步骤 13 选择**电话的进入与退出声音**。

- 嘀嘀声（缺省值）
- 无声音
- 播放姓名

步骤 14 如果系统支持且已配置 IPv6，请将 **IPv6 电话会议**设置设定为**开**或**关**。（**缺省值：** **关**表示设置为 IPv4。）

步骤 15 选择用户在拨入 Cisco WebEx 会议的音频部分或使用“呼叫我”服务时听到的**系统音频语言**。
此设置显示为呼入服务语言的缺省语言。

步骤 16 选择**保存**。

步骤 17 关闭维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。 如果此数据中心属于多数据中心 (MDC) 系统，那么管理员会被重定向至全局管理 URL。 管理员所看到的数据中心由 DNS 解析策略确定。 如果启用密钥再生，让一个数据中心退出维护模式会自动让系统中的所有数据中心退出维护模式。

此数据中心上用户的会议服务将被还原。

配置音频 CUCM

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 开启维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
我们建议您给每个虚拟机拍摄快照。（请参阅通过使用 VMware vCenter 拍摄快照，第 7 页。）

在所有活动数据中心开启维护模式会关闭会议活动，并会使用户无法登录 WebEx 站点、安排会议、加入会议，或播放会议录制文件。 如果此数据中心属于多数据中心 (MDC) 系统，并且另一个数据中心是活动的，那么进

行中的会议将故障转移到活动的数据中心。 这可能会导致活动的会议暂时中断。 有关要求开启维护模式的系统任务的信息，请参阅关于维护模式。

步骤 3 选择**设置** > **音频** > **CUCM 数据中心**。

步骤 4 选择**编辑** CUCM (Cisco Unified Communications Manager) 以更改这些设置。

a) 在 **CUCM 1 IP 地址**中，输入 CUCM 1 系统的主机名或 IP 地址。

b) （可选）输入 CUCM 2（负载平衡）系统的主机名或 IP 地址。
CUCM 2 不是必需的，但是建议用它实现电话会议高可用性。

步骤 5 关闭维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。 如果此数据中心属于多数据中心 (MDC) 系统，那么管理员会被重定向至全局管理 URL。 管理员所看到的数据中心由 DNS 解析策略确定。 如果启用密钥再生，让一个数据中心退出维护模式会自动让系统中的所有数据中心退出维护模式。

此数据中心上用户的会议服务将被还原。

关于 WebEx 群拨

WebEx 群拨功能允许指定为会议主持人的用户呼叫电话号码并输入主持人 PIN（如果需要），以立即开始会议的音频部分。 同时，系统自动呼叫群拨组中定义的参加者列表。 几分钟之内，主持人可以开始与拥有批准权限或者经过紧急状况培训的人员讨论紧急问题或提供处理重要问题所需的详细说明。 除了开始会议的音频部分，主持人还可以访问自动生成的电子邮件，以开始会议的网络部分，与会议参加者共享图片、视频或电子信息。

系统呼叫参加者列表中的人员后，此人接听呼叫并输入参加者 PIN（如果需要），即可加入会议的音频部分。 会议的音频部分开始进行后，主持人按下 *# 可接听已加入会议的人员的姓名，在会议的网络部分中也可查看参加者列表。 所有参加者都可以选择不接听呼叫，或者从群拨组中删除自己。 管理员可以随时删除群拨组中的人员。

每个群拨组可拥有每个大小用户系统支持的最大参加者数（请参阅《*Cisco WebEx Meetings Server* 规划指南》和《*Cisco WebEx Meetings Server* 系统要求》中的“系统容量矩阵”一节以获取详细信息）。管理员负责配置群拨组及其参加者，但是组设置及参加者列表信息由会议主持人提供。 管理员可以通过在“群拨”页面手动输入参加者或者导入由主持人完成的“参加者模板”文件向群拨组添加参加者。

下载组模板

使用提供的链接下载组模板，以发送给将为群拨组主持会议的人员。

步骤 1 登录管理站点。

步骤 2 选择**设置** > **音频**。

步骤 3 选择**组模板**链接以下载模板，主持人用该模板为新的群拨组提供常规设置，例如组名称和主持人 PIN。

步骤 4 用电子邮件将组模板发送给群拨组的主持人。 请主持人完成模板并将其返回给您。

接下来的操作

如果您有新建组的信息，请转至添加群拨组，第 164 页。

要导入参加者，在参加者模板文件中删除带示例文本的说明和行，然后转至导入参加者列表，第 170 页。

要手动添加组的参加者，请转至添加群拨参加者，第 167 页。

添加群拨组

对于每个群拨组，指定组名称、路由模式和呼入号码。 路由模式和呼入号码必须在 CUCM 中定义并复制到群拨页面中。 为提供会议安全性级别，请配置主持人 PIN 和参加者 PIN。 对于每个组，至少选择一个内部参加者的**主持人**复选框，使该用户成为主持人。 每个群拨组必须至少有一个主持人。 您可以将多个内部参加者指定为群拨组的主持人，并且所有主持人都可以开始群拨会议的音频部分。 但是，会议主持人需要许可证才能开始群拨会议的网络部分。

配置群拨组时，系统会向主持人发送一封包含主持人 PIN 和呼入号码的电子邮件。 所有参加者都会收到一封包含参加者 PIN 和呼入号码的电子邮件。 主持人呼叫呼入号码并输入主持人 PIN 以开始会议。 参加者接听群拨呼叫（或者如果未接到呼叫，则呼叫呼入号码），并输入参加者 PIN（如果需要）。 不同于其他类型 Cisco WebEx 会议（24 小时之后自动结束），群拨会议会持续举行，直到最后一个人结束通话或者离开会议的网络部分。

注释 主持人开始群拨会议的网络部分后，DTMF 声音被禁用。

开始之前

在 Cisco Unified Communications Manager 中为每个群拨组配置路由模式及相应的呼入号码。 每个群拨组都需要自己的专用呼入号码。 有关路由模式的详细信息，请参阅《*Cisco Unified Communications Manager* 管理指南》中的“呼叫路由设置”。

下载**组模板**文件并将其发送给群拨组的主持人。 主持人应填写模板然后将其返回。 使用模板中的信息创建群拨组。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**设置** > **音频** > **全局设置**。

步骤 3 在“群拨”部分，选择**添加组**。

步骤 4 输入**组名称**。

步骤 5 键入**路由模式**。
必须在 Cisco Unified Communications Manager 中为每个群拨组配置一个路由模式。

步骤 6 键入与此群拨组配置的路由模式相关联的**呼入号码**。
每个群拨组都需要专用的呼入号码。 主持人拨打呼入号码可启动群拨会议。

注释 此呼入号码必须重定向至在 Cisco Unified Communications Manager 中为此组选择的路由模式。 有关详细信息，请访问 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

步骤 7 （可选） 在**会议密码**字段中键入字母数字密码。
如果已配置，参加者输入此密码即可加入群拨会议的网络部分。

注释 会议密码的规则可以通过以下菜单设置：**设置** > **密码管理** > **会议密码**。 有关详细信息，请访问 配置会议设置，第 154 页。

步骤 8 选择**主持人 PIN** 选项：

- （缺省）选择**自动生成主持人 PIN** 并将滑块移动至所需的安全级别。 随着您移动滑块，PIN 和安全级别将随之改变。 选择**刷新**以生成另一个数字。
- 选择**键入主持人 PIN** 并键入数字 PIN。 选择此选项时，PIN 是必填项。

  3 位 PIN 安全级别较低，4 位至 7 位 PIN 安全级别中等，8 位至 10 位 PIN 安全级别较高。

  注释 主持人 PIN 不能为单个数字或顺序数字序列，例如 11111 或 1234567。

- 如果您不想要求主持人输入 PIN 来开始群拨会议，则选择**无**。

  注释 选择此选项时，任何知道呼入号码的用户都可以启动群拨会议。

步骤 9 选择**参加者 PIN** 选项：

- （缺省）如果您不想要求参加者输入 PIN 来加入群拨会议，则选择**无**。
- 选择**键入参加者 PIN** 并键入数字 PIN。 选择此选项时，PIN 是必填项。

  3 位 PIN 安全级别较低，4 位至 7 位 PIN 安全级别中等，8 位至 10 位 PIN 安全级别较高。

注释　参加者 PIN 不能为单个数字或顺序数字序列，例如 11111 或 1234567。

步骤 10　选择系统呼叫参加者应进行的**呼叫尝试**次数。
系统按照“呼叫尝试”所选的次数呼叫每个参加者。 如果用户在**我的帐户**页面上列出四个电话号码（对于内部用户）或者管理员在导入系统的 CSV 文件中输入四个电话号码，系统会按“呼叫尝试”所选的次数拨打第一个号码，然后按“呼叫尝试”所选的次数呼叫第二个号码，以此类推。 系统按“呼叫尝试”所选的次数拨打各个电话号码之后，将停止呼叫参加者。 如果为此字段选择**无限制**，则系统会不断呼叫参加者，直到他们接听呼叫或者直到群拨会议结束。

- 1（系统呼叫每个参加者一次。）
- 3（缺省）
- 5日
- 10日
- 无限制（如果公司政策要求系统不断呼叫参加者直到其加入会议，则选择此选项。）

步骤 11　选择**添加参加者**链接（**内部列表**部分）。

步骤 12　在**内部列表**中，输入至少一个主持人的电子邮件地址，并选择 + 以添加每个人至参加者列表中。

步骤 13　选择**主持人**复选框，以将该内部用户指定为会议主持人。

步骤 14　（可选） 选择**添加参加者**链接（**外部列表**部分）。

步骤 15　（可选） 对于外部用户，输入姓名、电子邮件地址，以及电话号码，然后选择**添加**以添加此人到参加者列表中。 有关外部用户的详细信息，请参阅添加群拨参加者，第 167 页。

步骤 16　选择**保存**以保存更改。
群拨组会添加到系统中。

接下来的操作

要导入参加者列表，请导出包含预先配置列标题的CSV文件。 有关详细信息，请参阅导出参加者列表，第 169 页和导入参加者列表，第 170 页。

要创建小型群拨列表或添加新人到现有列表中，请参阅添加群拨参加者，第 167 页。

要删除群拨组，请参阅删除群拨组，第 167 页。

编辑群拨组设置

您可以更改群拨组设置，包括参加者列表。

步骤 1 登录管理站点。

步骤 2 选择**设置** > **音频**。

步骤 3 在“群拨”部分，选择**组名称**链接。

步骤 4 对可编辑的字段进行更改。 标有星号的字段是必填的。

步骤 5 要更改参加者列表中的条目，选择 **X** 以删除条目，然后用更新数据再次添加该条目。

步骤 6 选择**更新**以保存更改。

删除群拨组

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**设置** > **音频**。

步骤 3 在“群拨”部分，选择要删除的组旁边的**X**。

步骤 4 单击**确定**进行确认。
群拨组以及相关的参加者列表将从系统中删除。

添加群拨参加者

配置群拨组的设置之后，您可以创建内部和外部参加者列表。 主持人启动 WebEx 群拨会议后，系统会呼叫内部和外部参加者列表的成员，先拨打内部列表的成员，接着拨打外部列表的成员。

内部参加者具有公司电子邮件地址。 管理员仅输入内部用户的电子邮件地址，系统就会在**我的帐户**页面上找到用户名和电话号码。 系统按顺序呼叫**我的帐户**页面上列出的内部参加者电话号码，这意味着如果用户输入办公室号码，则系统拨打该号码，但是如果用户输入移动号码，而不是办公室号码，则系统先拨打移动号码。 有关详细信息，请参阅《*Cisco WebEx Meetings Server* 用户指南》中的“更新帐户信息”。

外部参加者可以作为访客参加 WebEx 群拨会议，但是他们不具有公司电子邮件地址。 管理员在**群拨**对话框为外部参加者输入名称、电子邮件地址和电话号码。 系统按顺序拨打电话号码。

要添加参加者，有两种方法：

- 在“内部列表”或“外部列表”部分的字段中输入参加者信息。

- 请将主持群拨会议的人员在**我的帐户**页面上选择**参加者模板**链接以下载模板文件。 主持人应输入参加者信息，并向管理员发送完整的模板，以导入到系统中。
- 导出参加者列表 CSV 文件，输入必填信息，然后导入更新的 CSV 文件。

注释 外部参加者无法主持 WebEx 群拨会议。

如果外部参加者列表中输入了内部用户电子邮件地址，或者系统无法在数据库的内部参加者列表中找到条目的电子邮件地址，系统将检查所有参加者条目并自动在参加者列表之间移动条目。 如果内部参加者条目被移动到外部列表中，则输入用户名和电话号码以使条目有效。

开始之前

联系将主持群拨会议的人员并请其在**我的帐户**页面上选择**参加者模板**链接以下载模板文件。 主持人应输入参加者信息，并向管理员发送完整的模板。 请参阅《*Cisco WebEx Meetings Server* 用户指南发行版 *2.5*》中的“下载组和参加者模板”一节。

步骤 1 登录管理站点。

步骤 2 选择**设置** > **音频**。

步骤 3 在“群拨”部分，选择**组名称**链接。

步骤 4 您可以导出现有的参加者列表，修改 CSV 文件，并导入文件以添加或更改参加者信息。

注释 首次选择**导出列表**时，系统会导出具有相应列标题的空 CSV 文件。

步骤 5 要导入参加者，请执行以下操作：

- 选择**制表符**或**逗号**以指示要导入的 CSV 文件类型：制表符分隔或逗号分隔。
- 选择**浏览**，然后选择要导入的 CSV 文件。
- 选择**导入**。

步骤 6 要在提供的字段中添加单个条目，请执行以下操作：

- 对于内部参加者，键入电子邮件地址，然后选择 + 以添加该条目。
- 对于外部参加者，键入参加者姓名、电子邮件地址，以及电话号码（包括国家代码）。 然后选择**添加**。

新添加的参加者会出现在“内部列表”或“外部列表”中。

步骤 7 （可选） 选择**主持人**复选框，以将某人指定为主持人。

注释 系统要求为每个群拨组至少指定一个内部参加者为主持人。

步骤 8 选择**保存**以保存群拨组设置以及参加者列表中的新添加条目。

指定为主持人的人员会收到一封通知电子邮件，里面包括主持人PIN、参加者PIN、会议密码（如已配置），以及群拨呼入号码。 所有其他参加者会收到一封通知电子邮件，里面包括参加者 PIN 和会议密码（如已配置）。

接下来的操作

要修改参加者列表中的条目，请参阅编辑群拨组设置，第 167 页。

要导入参加者列表，请参阅导入参加者列表，第 170 页。

要导出参加者列表，请参阅导出参加者列表，第 169 页。

导出参加者列表

在创建参加者列表之前，请选择**导出列表**以导出带有相应列标题的空CSV文件。 否则，系统会导出此群拨组的所有参加者信息。 导出的列表中，同时包含内部和外部参加者的列表有： NAME、EMAIL、PHONENUMBER1、PHONENUMBER2、PHONENUMBER3、PHONENUMBER4 和 ISHOST。

步骤 1 登录管理站点。

步骤 2 选择**设置** > **音频**。

步骤 3 在“群拨”部分选择**组名称**。

步骤 4 在“参加者”部分选择**导出列表**。
参加者数据将导出为 CSV 文件。

步骤 5 在导出对话框中，选择用特定的应用程序打开文件，或选择保存文件并下载。

步骤 6 访问导出的 CSV 文件并添加、更改或删除参加者数据。
对于外部参加者，系统要求提供**姓名**、**电子邮件地址**和一个**电话号码**。 对于内部参加者，系统只要求提供用户的公司**电子邮件地址**。 必须至少为一个内部用户分配主持人角色。

注释 如果输入了不需要的参加者信息，如内部用户的用户名，则在导入 CSV 文件时系统将不会保存此信息。 但如果信息不完整，例如您忘记了输入外部参加者的名称，系统就会导入信息，但同时会显示一条错误消息。 不正确的输入将被视为无效，不会保存到数据库中。

- **姓名**（外部参加者必填）- 以规定的格式输入一个人的名字和姓氏。 可以使用任何符号，但不建议使用 < and >。 此名称显示在“外部列表”及系统发送给参加者的电子邮件中，邮件中含有有关加入群拨会议的信息。 如果该名称对于“外部列表”而言太长，就会被截断。（电子邮件中的名称始终不会被截断。）对于内部用户，系统将从用户的 WebEx **我的帐户**页中检索相应的名称。
- **电子邮件**（所有参加者必填）- 系统利用该地址发送PIN和呼入信息、向群拨会议的网络部分发送链接，以及确定某个人是内部参加者还是外部参加者。 如果电子邮件地址存放在 Cisco WebEx Meetings Server 上，则说明此人为内在参加者，系统将自动从用户的WebEx **我的帐户**页中检测名称和电话信息。 如果电子邮件地址为外部地址，系统将使用 CSV 文件中输入的名称和电话号码。

- **电话号码**（外部参加者必填）- 输入外部参加者的最多四个电话号码，包括国家/地区代码。 系统将按顺序拨打这些电话号码，即 Phonenumber1、Phonenumber2，等等。 为每位外部参加者至少输入一个电话号码。 可以使用的字符： 0~9、(、)、-。 CWMS 系统无法识别、验证格式，也无法转换电话号码；它只是将输入内容转发到 CUCM。
- **角色**（仅适用于内部参加者）- 为所有将担任会议主持人的内部用户输入**主持人**。 主持人会收到一封电子邮件，上面包含主持人 PIN、参加者 PIN 及呼入号码。 可以将多个用户指定为主持人。

接下来的操作

转至 导入参加者列表，第 170 页.

导入参加者列表

开始之前

准备好含有参加者信息的逗号分隔或制表符分隔 (CSV) 的文件。 您可以将当前的参加者列表值导出到 CSV 文件，修改该文件，然后重新导入以添加或更改参加者信息。

步骤 1 登录管理站点。

步骤 2 选择**设置** > **音频**。

步骤 3 在“群拨”部分选择**组名称**。

步骤 4 选择**制表符**或**逗号**以指定要导入的 CSV 文件的类型。

步骤 5 选择**浏览**，然后选择要导入的 CSV 文件。

步骤 6 选择**导入**。
文件将被导入系统。

步骤 7 选择**更新**以保存参加者信息。
导入的参加者信息将存入数据库中。

接下来的操作

滚动参加者列表，查看参加者信息，并验证这些值已正确导入。

要导出参加者列表，请参阅导出参加者列表，第 169 页。

配置视频设置

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**设置** > **视频**。

步骤 3 选择 **360p**、**180p** 或**关闭**，然后选择**保存**。
有关近似的存储空间要求，请参阅《CWMS 规划指南》中的“关于会议录制文件”一节。

配置移动设备设置

如果您的系统配置为允许多个呼入接入号码，则系统假设第一个号码是免费接入号码，并且会先尝试此号码。如果从移动网络无法接通此号码，应用程序将不会连接。请确保可从移动网络接通此号码。

使用 iOS 移动设备并且数据中心证书不是来自已知的证书颁发机构时，必须将两个数据中心 SSL 证书导入 iOS 移动设备中。 否则，iOS 移动设备在尝试启动会议时会显示错误。

我们建议 Android 移动设备用户在尝试启动会议之前导入两个数据中心证书。将证书导入到 Android 设备中之后，设备将信任 WebEx 站点，并且从此站点开始会议时不会显示警告消息。

注释 Cisco WebEx Meetings Server 2.0 及更高版本支持 Android。 缺省情况下，已启用 iOS 和 Android WebEx 应用程序。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**设置** > **移动设备**。

步骤 3 通过选择系统所支持的移动平台来配置移动设备设置，然后选择**保存**。
缺省： iOS WebEx 应用程序和 Android WebEx 应用程序。

iOS 和 Android WebEx 应用程序与通过内部网或外部互联网运行的 Cisco WebEx 桌面应用程序相同。

接下来的操作

对于 Cisco WebEx Meetings Server 发行版 2.0 及更高版本，请参阅 导出移动设备的 SSL 证书，第 209 页 以获取有关导出证书以向您的移动设备用户发送电子邮件的信息。

配置服务质量 (QoS)

如 RFC 2475 中所定义的，差分服务 (DiffServ) 代码点 (DSCP) 设置确定音频和视频媒体信号的 QoS。Cisco 建议您保留缺省值。 在少数情况下，当网络需要不同的 DSCP 设置时，可以使用其他值。 有关更多信息，请参阅以下网址中相应 Cisco Unified Communications Manager 版本的 Cisco Unified Communications Solution Reference Network Design (SRND) 文档的“Network Infrastructure”一章：http://www.cisco.com/en/us/products/sw/voicesw/ps556/products_implementation_design_guides_list.html。

以下为缺省值：

- WebEx 音频（媒体）

  IPv4 QoS 标记： **EF DSCP 101110**

  IPv6 QoS 标记： **EF DSCP 101110**

- WebEx 音频（信号）

  IPv4 QoS 标记： **CS3 (优先级 3) DSCP 011000**

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**设置** > **服务质量**。

步骤 3 使用相应的下拉菜单选择 QoS 标记设置，然后选择**保存**。

关于 QoS 标记

请参见下表，比较有流量经过互联网反向代理服务器的部署的 QoS 标记信息和没有流量经过互联网反向代理服务器的部署的 QoS 标记信息。

有流量经过互联网反向代理服务器的 Cisco WebEx Meetings Server 系统上的 QoS 标记

流量	QoS 标记
SIP 音频 — 媒体 — CWMS 到端点	是
SIP 音频 — 信号 — CWMS 到端点	是
PC 音频 — 媒体 — CWMS 到客户端	否
PC 音频 — 信号 — CWMS 到客户端	否
PC 音频 — 媒体 — 客户端到 CWMS	否

流量	**QoS** 标记
PC 音频 — 信号 — 客户端到 CWMS	否
PC 视频 — 媒体 — CWMS 到客户端	否
PC 视频 — 信号 — CWMS 到客户端	否
PC 视频 — 媒体 — 客户端到 CWMS	否
PC 视频 — 信号 — 客户端到 CWMS	否

没有流量经过互联网反向代理服务器的 Cisco WebEx Meetings Server 系统上的 QoS 标记

流量	**QoS** 标记
SIP 音频 — 媒体 — CWMS 到端点	是
SIP 音频 — 信号 — CWMS 到端点	是
PC 音频 — 媒体 — CWMS 到客户端	是
PC 音频 — 信号 — CWMS 到客户端	是
PC 音频 — 媒体 — 客户端到 CWMS	否
PC 音频 — 信号 — 客户端到 CWMS	否
PC 视频 — 媒体 — CWMS 到客户端	是
PC 视频 — 信号 — CWMS 到客户端	是
PC 视频 — 媒体 — 客户端到 CWMS	否
PC 视频 — 信号 — 客户端到 CWMS	否

配置密码

您可以配置下列密码设置：

- 一般设置 - 控制密码有效期并让您能强制规定用户立即更改密码或按指定间隔更改密码。
- 用户密码 - 让您能配置用户帐户的密码强度，包括大小写混合、长度、字符类型和用法、动态网页文本控制，并设置不可接受的密码列表。
- 会议密码 - 让您能强制规定会议的密码用法和配置会议的密码强度，包括大小写混合、长度、字符类型和用法、动态网页文本控制，并设置不可接受的密码列表。

注释 如果在系统上启用了 SSO，**一般设置**和**用户密码**页面上的设置以及**编辑用户**页面上的密码更改控制就不再应用于主持人帐户。

配置常规密码设置

此页面上的所有密码设置都是可选的，并且可以切换为开启（选中）或关闭（取消选中）。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**设置** > **密码管理** > **一般设置**。

步骤 3 （可选） 选中**在停止活动 [*X*] 天后停用主持人帐户**，并在文本字段中输入天数。 （**缺省值：** 不勾选（禁用）并设置为 90 天。）
启用缺省设置时，如果用户连续 90 天未主持或安排会议，那么该用户将被停用。

此功能仅应用于主持人帐户。 无法用此功能停用管理员帐户。 要停用管理员帐户，请参阅从用户页面激活或停用用户和管理员，第 117 页。

步骤 4 （可选） 选中**强制所有用户每隔 X 天更改一次密码**，并在文本字段中输入天数。 （**缺省值：** 未选中）

步骤 5 （可选） 选中**强制所有用户在下次登录时更改密码**。 （**缺省值：** 未选中）

步骤 6 （可选） 选中**启用用户帐户锁定**。 （**缺省值：** 未选中）
管理员可以解锁帐户（请参阅解锁管理员帐户，第 117 页）。

附加参数显示：

- [*X*] 次连续登录失败。
- [*X*] 分钟之后忘记失败的登录尝试。
- [*X*] 分钟之后清除用户帐户锁定。
- 向锁定用户发送电子邮件通知。

步骤 7 选择**保存**。

配置用户密码要求和限制

系统使用缺省验证时，这些设置同时适用于管理员和最终用户。系统使用轻量级目录访问协议(LDAP)验证或单点登录 (SSO) 验证时，这些设置仅适用于管理员；最终用户密码由 AD 服务器或 IdP 服务器管理。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**设置** > **密码管理** > **用户密码**。

步骤 3 通过配置页面上的字段来更改用户密码设置。

选项	描述
必须为用户帐户设置强密码	选择此选项以启用剩余的选项。 **缺省：** 选中
最小字符长度	最少字符要求。 **缺省：** 选中，**6** 个字符
最少字母字符数	最少字母数（非数字、非特殊字符）。 **缺省：** 选中，**1** 个字符
最少数字字符数	最少数字数（非字母、非特殊字符）。 **缺省：** 选中，**1** 个数字
最少特殊字符数	最少特殊字符数（非字母、非数字字符）。 **缺省：** 未选中，**1** 个字符
必须包含大小写混合字母	密码必须含有大写和小写的字母字符。 **缺省：** 选中
不允许任何字符重复 3 次以上	一个字符（字母、数字或特殊字符）不能重复超过三次。 **缺省：** 选中
禁止使用的密码列表	管理员指定的不可用的密码列表。 **缺省：** 未选择
不允许使用公司名称、站点名称、用户电子邮件地址和主持人姓名	请勿使用这些特定名称。 **缺省：** 选中

选项	描述
不得包含先前的 *n* 个密码。	请勿使用以前用过的密码。 从下拉菜单选择一个数字，以指定不能使用的先前密码的数。 **缺省：** 选中 **缺省数目：** 5日

步骤 4 选择**保存**。

配置会议密码

使用此功能配置会议密码参数。 下表说明用户必须输入密码以出席会议的情况。

已配置密码	电子邮件邀请中不包含密码	已登录的会议创建者	已登录的主持人	已登录的受邀者	已登录的访客	未登录的访客
否	不适用	不需要密码。	不需要密码。	不需要密码。	不需要密码。	不需要密码。
是	是	不需要密码。	不需要密码。	不需要密码。	需要密码。	需要密码。
是	否	不需要密码。	不需要密码。	不需要密码。	需要密码。密码已预填。	需要密码。密码已预填。

步骤 1 登录管理站点。

步骤 2 选择**设置** > **密码管理** > **会议密码**。

步骤 3 通过配置页面上的字段更改会议密码设置。

选项	描述
所有会议都必须设置密码	所有会议都要求有密码。
必须为会议设置强密码	启用剩余选项。
最小字符长度	最少字符数。 **缺省：** 6日

选项	描述
最少字母字符数	最少字母数（非数字、非特殊字符）。 **缺省：** 1
最少数字字符数	最少数字数（非字母、非特殊字符）。 **缺省：** 1
最少特殊字符数	最少特殊字符数（非字母、非数字字符）。 **缺省：** 1
不得含有以下特殊字符（空格、\、'、"、/、&、<,>、=、[、]）	选择此选项以禁止使用这些字符。
必须包含大小写混合字母	密码必须含有大写和小写的字母字符。
禁止使用的密码列表	管理员指定的非法密码列表。
不允许使用公司名称、站点名称、用户电子邮件地址、主持人姓名和会议主题	选择此选项以禁止使用这些词或字符串。

步骤 4 选择**保存**。

配置电子邮件设置

您可以配置电子邮件设置和模板。 电子邮件模板有缺省设置（可选择性地更改）。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**设置** > **电子邮件**。
将打开**变量**页面。

步骤 3 输入**发件人姓名**、**发件人电子邮件地址**、**答复**电子邮件地址，然后选择**保存**。
您可以在“变量”页上的“发件人姓名”中输入某个人员的姓名，但是会议邀请将体现主持人的电子邮件地址。

步骤 4 选择**模板**。 有关每个模板类型的描述，请参阅关于电子邮件模板，第 178 页。

系统将显示**模板**页面。 选择**通用**或**会议**标签页。 **通用**为缺省值。

步骤 5 要配置电子邮件模板，请在**通用**和**会议**标签页上选择想要的模板链接。

步骤 6 对所选的电子邮件模板进行更改（若有），然后选择**保存**。

示例：
在**通用**标签页上选择**已重新激活帐户**模板链接。对**已重新激活帐户**对话框中的字段进行更改，然后选择**保存**。**发件人姓名**、**发件人电子邮件地址**和**答复**的缺省值来源于**变量**页面上所配置的设置。

注释 如果在**发件人姓名**（**变量**页）中输入某个人员的姓名，系统会自动将该人员的姓名替换为所有会议邀请的 WebEx 站点 URL。

关于电子邮件模板

使用电子邮件模板向用户传达重要事件。每个电子邮件模板都有必须配置的变量。有关每个模板中变量的说明，请参阅下表。

有两种电子邮件模板：

- 通用 – 包括丢失密码、主持人和受邀者通知、录制文件可用性和其他一般通知。
- 会议 – 包括会议邀请、取消、更新、提醒和信息通知。

表 *3*：普通电子邮件模板

标题	描述	变量
AD 激活	启用 AD 帐户之后发送到用户。	• %SiteURL% • DISPLAYNAME • %SSOSignINLink% • %OrgLogo% • %Participants% • %Support% • %CustomFooterText%： • %Year%

标题	描述	变量
AD 同步失败	同步失败后发送给管理员。	• %FullName% • %Failure_Reason% • %DownloadLogURL% • %Sync_Start_Time% • %Sync_Completion_Time% • %Users_Added% • %Users_Deactivated% • %Users_Failed_to_Sync% • %SiteURL% • %Support% • %CustomFooterText%： • %Year%
AD 同步成功	同步成功后发送给管理员。	• %FullName% • %DownloadLogURL% • %Sync_Start_Time% • %Sync_Completion_Time% • %Users_Added% • %Users_Deactivated% • %Users_Failed_to_Sync% • %SiteURL% • %Support% • %CustomFooterText%： • %Year%
已重新激活帐户	在管理员重新激活用户的帐户后发送给用户。	• DISPLAYNAME • %SiteURL% • %Support% • %CustomFooterText%： • %Year%

标题	描述	变量
忘记密码 - 密码已更改	用户在最终用户站点上重设密码后发送给用户。	• %SiteURL% • DISPLAYNAME • %OrgLogo% • %SiteURL% • %Support% • %CustomFooterText%： • %Year%
忘记密码 - 重设密码	用户在最终用户站点上重设密码后发送给用户。 此电子邮件会请求用户创建新密码。	• %SiteURL% • DISPLAYNAME • %OrgLogo% • %SiteURL% • %Support% • %CustomFooterText%： • %Year%
PT 会议邀请 - 受邀者	使用个人会议帐户通过快捷会议工具安排会议后发送给会议受邀者。	• %HostName% • %Topic% • %TeleconferencingInfo% • %Meeting Link% • %MeetingNumber% • %Meeting Password% • 会议空间 • %SiteURL% • %Support% • %CustomFooterText%： • %Year%

标题	描述	变量
PT 会议通知 - 主持人	使用个人会议帐户通过快捷会议工具安排会议后发送给会议主持人。	• %HostName% • %Topic% • %TeleconferencingInfo% • %Meeting Link% • %MeetingNumber% • %Meeting Password% • 会议空间 • %SiteURL% • %Support% • %CustomFooterText%： • %Year%
PT 会议邀请 - 主持人	在使用快捷会议工具安排会议后发送给会议主持人。	• %Topic% • %HostName% • %Meeting Link% • %MeetingNumber% • %Meeting Password% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText%：
PT 会议邀请 - 受邀者	在使用快捷会议工具安排会议后发送给会议受邀者。	• %Topic% • %HostName% • %Meeting Link% • %MeetingNumber% • %Meeting Password% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText%：

标题	描述	变量
主持人可使用录制文件	向主持人发送会议录制文件的链接。	• %SiteURL% • %OrgLogo% • DISPLAYNAME • %Topic Name% • %Duration% • %Recording Time% • %SiteURL% • %Support% • %CustomFooterText%： • %Year%
SSO 激活电子邮件	启用单点登录 (SSO) 后发送。	• %SiteURL% • DISPLAYNAME • %OrgLogo% • %SiteURL% • %Support% • %CustomFooterText%： • %Year%
向所有用户发送电子邮件	向系统上所有用户发送电子邮件。	• %SiteURL% • %Subject% • %OrgLogo% • %AttendeeName% • %Body% • %SiteURL% • %Support% • %CustomFooterText%： • %Year%

标题	描述	变量
设置 Cisco WebEx - 移动设备	通知用户关于移动设备版 Cisco WebEx 应用程序的信息，并提供该应用程序的下载链接。	• %SiteURL% • %Subject% • %OrgLogo% • DISPLAYNAME • %SiteURL% • %Support% • %CustomFooterText%： • %Year%
共享录制文件	向选定的会议受邀者发送会议录制文件的链接。	• %HostName% • %HostEmail% • %OrgLogo% • %AttendeeName% • %HostName% • %Topic Name% • %Duration% • %Recording Time% • %Personalized Message% • %SiteURL% • %Support% • %CustomFooterText%： • %Year%

标题	描述	变量
从 MC 共享录制文件	向选定的会议受邀者发送会议录制文件的链接。 主持人选择**离开会议**后在 Meeting Center 中选择的参加者。	• %HostName% • %HostEmail% • %OrgLogo% • %AttendeeName% • %Topic Name% • %Duration% • %Recording Time% • %SiteURL% • %Support% • %CustomFooterText%： • %Year%
用户密码已更改	用户密码已更改时给用户发送电子邮件。	• %SiteURL% • %OrgLogo% • DISPLAYNAME • %SiteURL% • %Support% • %CustomFooterText%： • %Year%
欢迎电子邮件	在新管理员的帐户创建后发送给该管理员。	• %SiteURL% • DISPLAYNAME • %SiteURL% • %Support% • %participants% • %CustomFooterText%： • %Year%

表 *4*：会议电子邮件模板

标题	描述	变量
群拨会议邀请（针对主持人）	主持人拨打群拨呼入号码以开始会议时发送给主持人。	• %SiteURL% • %BlastDialGroupName% • %HostName% • %AccessNumber% • %HostPin% • %NeedInfo_InternalUse% • %Support% • %CustomFooterText%： • %Year%
群拨会议邀请（针对与会者）	主持人拨打群拨呼入号码以开始会议时发送给参加者。	• %SiteURL% • %BlastDialGroupName% • %HostName% • %AccessNumber% • %ParticipantPin% • %NeedInfo_InternalUse% • %Support% • %CustomFooterText%： • %Year%
群拨会议组已删除	管理员删除组时发送给群拨组的成员。	• %SiteURL% • %BlastDialGroupName% • %Support% • %CustomFooterText%： • %Year%

标题	描述	变量
正在进行的群拨会议邀请（针对主持人）	主持人在会议进行中邀请其他主持人参加会议时发送给他们。	• %SiteURL% • %BlastDialGroupName% • %HostName% • %MeetingInfoURL% • %AccessNumber% • %HostPin% • %MeetingPassword% • %NeedInfo_InternalUse% • %Support% • %CustomFooterText%： • %Year%
正在进行的群拨会议邀请（针对与会者）	如果主持人在会议进行中邀请用户参加会议，则发送给这些用户。	• %SiteURL% • %BlastDialGroupName% • %HostName% • %AccessNumber% • %ParticipantPin% • %MeetingPassword% • %NeedInfo_InternalUse% • %Support% • %CustomFooterText%： • %Year%

标题	描述	变量
群拨会议信息已更新（针对主持人）	会议设置更改后向主持人提供会议信息。	• %SiteURL% • %BlastDialGroupName% • %HostName% • %AccessNumber% • %HostPin% • %NeedInfo_InternalUse% • %Support% • %CustomFooterText%： • %Year%
群拨会议信息已更新（针对与会者）	会议设置更改后向参加者提供会议信息。	• %SiteURL% • %BlastDialGroupName% • %HostName% • %AccessNumber% • %ParticipantPin% • %NeedInfo_InternalUse% • %Support% • %CustomFooterText%： • %Year%

标题	描述	变量
进行中的会议邀请（针对与会者）	如果主持人在会议进行中邀请用户参加会议，则发送给这些用户。	• %HostName% • %HostEmail% • %Topic% • %AttendeeName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText%： • %Year%
即时会议邀请（针对主持人）	当主持人选择**即时会议**时发送给主持人和受邀者。	• %SiteURL% • %Topic% • %HostName% • %Topic_HTML% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText%： • %Year%

标题	描述	变量
会议已取消（针对与会者）	通知用户安排的会议已被取消。	• %HostName% • %HostEmail% • %Topic% • %AttendeeName% • %HostName% • %Topic_HTML% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %Write% • %SiteURL% • %CustomFooterText%： • %Year%
会议已取消（针对主持人）	发送给会议主持人，用于确认取消会议。	• %SiteURL% • %Topic% • %HostName% • %Topic_HTML% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %Write% • %SiteURL% • %CustomFooterText%： • %Year%

标题	描述	变量
会议信息已更新（针对候补主持人）	会议设置更改后向候补主持人提供会议信息。	• %HostName% • %HostEmail% • %Topic% • %OrgLogo% • %AlternateHostName% • %MeetingTime% • %HostName% • %Duration% • %MeetingNumber% • %MeetingPassword% • %HostNumberDes% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText%： • %Year%

标题	描述	变量
会议信息已更新（针对与会者）	会议设置更改后向会议受邀者提供会议信息。	• %HostName% • %HostEmail% • %Topic% • %AttendeeName% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText%： • %Year%
会议信息已更新（针对主持人）	会议设置更改后向主持人提供会议信息。	• %SiteURL% • %Topic% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %HostNumberDes% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText%： • %Year%

标题	描述	变量
候补主持人的会议提醒	向会议候补主持人发送会议提醒。	• %HostName% • %HostEmail% • %Topic% • %OrgLogo% • %AlternateHostName% • %MeetingTime% • %HostName% • %Duration% • %MeetingNumber% • %MeetingPassword% • %HostNumberDes% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText%： • %Year%

标题	描述	变量
主持人的会议提醒	向会议主持人发送会议提醒。	• %SiteURL% • %Topic% • %OrgLogo% • %HostName% • %MeetingTime% • %HostName% • %Duration% • %MeetingNumber% • %MeetingPassword% • %HostNumberDes% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText%： • %Year%

标题	描述	变量
会议已重新安排（针对候补主持人）	向候补主持人发送更新的会议信息。	• %HostName% • %HostEmail% • %Topic% • %AlternateHostName% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %HostNumberDes% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText%： • %Year%

标题	描述	变量
会议已重新安排（针对与会者）	向受邀者发送更新的会议信息。	• %HostName% • %HostEmail% • %Topic% • %AttendeeName% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText%： • %Year%

标题	描述	变量
候补主持人的会议信息	向候补主持人发送会议确认。	• %HostName% • %HostEmail% • %Topic% • %AlternateHostName% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %HostNumberDes% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText%： • %Year%

标题	描述	变量
与会者的会议信息	向受邀者发送会议邀请。	• %HostName% • %HostEmail% • %Topic% • %AttendeeName% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText%： • %Year%
主持人的会议信息	向主持人发送会议确认。	• %SiteURL% • %Topic% • %HostName% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %MeetingNumber% • %MeetingPassword% • %HostNumberDes% • %TeleconferencingInfo% • %SiteURL% • %Support% • %CustomFooterText%： • %Year%

标题	描述	变量
PCN 会议自动提醒-主持人	向会议主持人发送自动会议提醒（仅限个人会议帐户）。	• %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %HostNumberDes% • %SiteURL% • %Support%
PCN 会议邀请-受邀者	给受邀者发送会议邀请（仅限个人会议帐户）。	• %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %SiteURL% • %Support%

标题	描述	变量
PCN 会议手动提醒-主持人	向会议主持人发送手动会议提醒（仅 PCN 帐户）。	• %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %HostNumberDes% • %SiteURL% • %Support%
PCN 会议手动提醒-受邀者	给受邀者发送手动会议提醒（仅限个人会议帐户）。	• %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %SiteURL% • %Support%

标题	描述	变量
PCN 会议通知-主持人	向主持人发送会议通知（仅限个人会议帐户）。	• %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %HostNumberDes% • %SiteURL% • %Support%
PCN 会议即时邀请 — 主持人	向主持人发送即时会议通知（仅限个人会议帐户）。	• %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %SiteURL% • %Support%

标题	描述	变量
PCN 会议进行中邀请 — 受邀者	向受邀者发送即时会议通知（仅限个人会议帐户）。	• %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %SiteURL% • %Support%
PCN 会议安排更改 — 主持人	向主持人发送安排更改通知（仅限个人会议帐户）。	• %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %HostNumberDes% • %SiteURL% • %Support%

标题	描述	变量
PCN 会议安排更改 — 受邀者	向受邀者发送安排更改通知（仅限个人会议帐户）。	• %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %SiteURL% • %Support%
PCN 会议已重新安排 — 受邀者	向受邀者发送会议重新安排通知（仅限个人会议帐户）。	• %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %TeleconferencingInfo% • %MeetingInfoURL% • %MeetingNumber% • %MeetingPassword% • %SiteURL% • %Support%

标题	描述	变量
PCN 会议已取消 — 主持人	向主持人发送会议取消通知（仅限个人会议帐户）。	• %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %Write% • %SiteURL%
PCN 会议已取消 — 受邀者	向受邀者发送会议取消通知（仅限个人会议帐户）。	• %AttendeeName% • %HostName% • %Topic% • %MeetingDateOrRecurrence% • %MeetingTime% • %TimeZone% • %Write% • %SiteURL%

关于应用程序下载

您可以使用管理站点上提供的工具大规模部署 CWMS 应用程序。 可供下载的应用程序包括：

- WebEx Meetings 应用程序

  注释 不支持在虚拟操作系统上运行 WebEx Meetings 应用程序。

- WebEx 快捷会议工具

  更新或升级系统之后，用户必须卸载所有旧版本的 WebEx 快捷会议工具。 更新或升级之后，您可以使用管理站点向用户推送 WebEx 快捷会议工具，也可以请用户从最终用户**下载**页面下载 WebEx 快捷会议工具。

- WebEx 网络录制文件播放器

您可以使用管理站点允许用户自行下载应用程序，也可以向用户计算机推送应用程序，还可以下载安装文件并请用户自行手动安装应用程序。

您可从**管理员** > **设置** > **下载**页分别获取 .MSI 安装程序。 有关更多信息，请参阅从管理站点下载应用程序。

如果用户对计算机拥有管理员权限，您可以通过使用自动下载、支持用户的下载和安装，也可以向用户计算机推送应用程序来分发应用程序。 如果您的公司没有赋予用户管理员权限，则您必须使用其他方法来将应用程序安装到用户计算机上。

我们建议您先向用户计算机脱机推送应用程序，然后再通知这些最终用户已为其创建帐户。 这将确保用户首次登录时可以开始和加入会议，以及播放网络录制文件。

如果用户没有安装应用程序，那么用户首次加入会议时，WebEx Meetings 应用程序会下载到 PC 中。这可以配置为随需或以无提示方式完成。 用户可以在会议期间使用 Cisco WebEx Meetings 应用程序然后在会议结束时删除它，也可以安装应用程序以加快今后开始或加入会议的速度。 该操作可能发生故障，原因是用户没有管理员权限。

在用户拥有管理员权限的 PC 上，用户可以从最终用户下载页面下载并安装 Cisco WebEx Meetings 应用程序、快捷会议工具和网络录制文件播放器。 无需其他管理员操作。

在用户对 PC 没有管理员权限的锁定环境中，**升级**至 Cisco WebEx Meetings Server 发行版 1.5MR3 或更高版本时，请先向所有用户 PC 推送新版本的 WebEx Meetings 应用程序，然后再开始升级过程。在用户 PC 上存储新版和旧版的 Meetings 应用程序，使其能够出席由运行最新版本或先前版本的 Meetings 应用程序的用户主持的会议。 用户可以在 PC 上存储多个版本的 WebEx Meetings 应用程序，只要将文件存储在正确的文件夹中即可。

注释 对于已部署 Cisco WebEx Meetings Server 发行版 1.5 MR3（内部版本号 1.5.1.386）或更低版本并使用云模式 WebEx 会议服务的站点，请先卸载 WebEx Meetings Server 和 WebEx 会议服务的 Meetings 应用程序，然后再将 Meetings 应用程序重新安装到用户 PC 的正确文件夹中。 否则，用户无法加入由云模式的 WebEx 用户主持的会议。 请参阅《*Cisco WebEx Meeting Server* 疑难解答指南》中的“没有管理员权限的 PC 用户无法加入由云模式 WebEx 用户主持的会议”以获取更多详细信息。

配置下载设置

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**设置** > **下载**。

步骤 3 选中**自动更新“WebEx 快捷会议工具”**复选框以配置定期自动更新。 （**缺省值：** 选中。）

注释 如果计划将“WebEx 快捷会议工具”手动推送给用户，建议取消选中此复选框。

注释 选择此选项时，用户安装更新版本的“Cisco WebEx 快捷会议工具”之后，Windows 控制面板的**程序和功能**中显示的“WebEx 快捷会议工具”版本显示更旧的版本号。 但是，WebEx 助手的**关于 WebEx 快捷会议工具**中显示的版本显示正确的版本。这是已知问题，将在以后的发行版中修复。

步骤 4 选择下载方法：

- 允许用户下载 WebEx 桌面应用程序
- 手动将 Cisco WebEx Meetings 和快捷会议工具推送到用户的桌面

如果选择**允许用户下载 WebEx 桌面应用程序**，则可以选择**保存**以完成下载配置。 不需要进一步的操作。

如果选择**手动将 Cisco WebEx Meetings 和快捷会议工具推送到用户的桌面**，那么页面上会出现“WebEx Meetings 应用程序”、“快捷会议工具”和“WebEx 网络录制文件播放器”部分。 继续下一个步骤。

步骤 5 对于要下载和安装的每个应用程序，选择**下载**，然后选择**保存**将 ZIP 文件保存到包含相应应用程序安装程序的系统。
每个 ZIP 文件包含所有受支持语言和平台的应用程序安装程序。

步骤 6 选择**保存**以保存下载设置。

管理证书

证书确保系统各组件之间的安全通信。 部署系统时，系统会配置有一个自签名证书。 虽然自签名证书可保持长达五年，但我们建议您配置证书中心验证的证书。 证书中心确保虚拟机之间的通信得到验证。 系统可以拥有多个虚拟机。 一个数据中心只需要一个证书。 除了 IRP 虚拟机以外，系统证书包括用于所有其他虚拟机的标准域名 (FQDN)、站点 URL 和管理 URL。

支持以下证书类型：

- SSL - 在所有系统上都需要。 （请参阅导入 SSO IdP 证书，第 213 页。）
- SSO IdP - 用于有身份提供程序 (IdP) 证书的 SSO。
- 安全电话会议 - TLS 电话会议需要。 您最多可以配置两个安全电话会议证书，您选择要配置的每个 CUCM 系统中对应配置一个证书。
- SMTP - 在电子邮件服务器启用 TLS 功能的情况下需要。

本产品支持下列 SSL 证书：

- 自签名
- 证书中心签署
- 外部证书中心签署

您无法更新证书或证书签名请求 (CSR)，但是可以随时生成证书或 CSR。 如果向系统添加虚拟机，或更改任何现有的虚拟机，必须为系统上的每个虚拟机生成新证书。

SSL 证书会因以下原因而无效：

- 数据中心已加入系统中。
- 系统容量已扩展，且导致了新虚拟机的部署。 原始SSL 证书中不存在这些新虚拟机的FQDN。

- 高可用性系统已添加，且导致了新虚拟机的部署。 原始 SSL 证书中不存在这些新虚拟机的 FQDN。
- 已更改 Cisco WebEx Meetings 站点 URL。 原始 SSL 证书中不存在此 URL。
- 已更改管理站点 URL。 原始 SSL 证书中不存在此 URL。
- 已更改管理虚拟机的 FQDN。 原始 SSL 证书中不存在此 FQDN。
- 当前的 SSL 证书已过期。

如果您的 SSL 证书因任何原因而无效，那么您的系统会自动生成新的自签名证书，并通过管理站点页面顶部的表示 SSL 已无效的全局警告消息来通知您此次更改。

生成 SSL 证书

必须为系统配置 SSL 证书。 本产品支持下列类型的 SSL 证书：

- 自签名
- 证书中心签署
- 外部证书中心签署

生成证书签名请求（CSR）

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**设置** > **安全性** > **证书** > **数据中心** > **生成 CSR**。

步骤 3 在**生成 CSR**（**证书签名请求**）页面中将字段填写完整。

选项	描述
公用名	选择**本地站点 URL** 证书、**全球站点 URL** 证书或**通配符**证书。
使用者备用名称 只有在为公用名类型选择了**使用者备用名称**时才会出现此选项。	管理站点和虚拟机名称。 如果选择了通配符公用名，则不需要使用者备用名称。
组织	输入组织名称。
部门	输入部门名称。
县/市	输入城市。
省/自治区	输入省或自治区。

选项	描述
国家/地区	选择国家。
密钥大小	选择密钥大小。 **缺省：** 2048（推荐）

步骤 4 选择**生成 CSR**。
系统将弹出**下载 CSR** 对话框。

步骤 5 选择**下载**。
您将收到ZIP 文件，其中包含CSR 和关联的私钥。 CSR 文件名为 `csr.pem`，私钥文件名为 `csr_private_key.pem`。

步骤 6 使用 VMware 数据恢复或 VMware vSphere 数据保护来备份系统。 请参阅通过使用 VMware vCenter 创建备份，第 6 页。
备份系统将保留私钥以防需要对其进行恢复。

导入 SSL 证书

Cisco WebEx Meetings Server 支持带 PEM 和 DER 编码及 PKCS12 档案的 X.509 证书。

如果用户的系统中使用的是自签名证书，则在加入会议时可能会有问题。 为避免此情况，请配置客户端使用自签名证书。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 开启维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
我们建议您给每个虚拟机拍摄快照。 （请参阅通过使用 VMware vCenter 拍摄快照，第 7 页。）

在所有活动数据中心开启维护模式会关闭会议活动，并会使用户无法登录WebEx站点、安排会议、加入会议，或播放会议录制文件。 如果此数据中心属于多数据中心 (MDC) 系统，并且另一个数据中心是活动的，那么进行中的会议将故障转移到活动的数据中心。 这可能会导致活动的会议暂时中断。 有关要求开启维护模式的系统任务的信息，请参阅关于维护模式。

步骤 3 选择**设置** > **安全性** > **数据中心** > **证书** > **更多选项** > **导入 SSL 证书/私钥**。
如果您已安装证书，系统会警告您导入新证书将覆盖已安装的证书。

步骤 4 选择**继续**。

步骤 5 选择**浏览**，然后选择证书。
必须选择符合 X.509 的证书或证书链。 有效类型包括：

- PEM/DER 编码证书： .CER / .CRT / .PEM / .KEY
- PKCS12 加密证书： .P12 / .PFX

您可以用 PKCS#12 文件或 PEM 块的单个文件导入证书链。 如果使用 PEM 文件，必须按如下所述进行格式化：

- （可选）如果想上传私钥，那么私钥必须是文件中的第一个块。 可以对其进行加密或解密。 它必须为 PKCS#8 格式，以 PEM 编码。 如果已加密，则必须输入密码对其进行解密。
- 下一个元素必须是中间证书中心的证书，该证书中心颁发的证书为 PEM 编码 X.509 格式。
- 您可以在基础结构中列入您所使用的所有中间证书。 根证书中心的证书不包括在内。 如果您使用的是专用证书中心，请确保已经将根证书分发给所有客户端。

所有证书都必须放在一个文件中上传； 不能先上传一个证书，然后再添加中间证书。 如果您使用的是采用中间证书的证书中心，并且在其客户端中没有分发中间证书，则可以上传中间证书来防止出现证书警告。

如果证书带有证书链，则必须将中间证书和最终用户证书合并到一个文件中。 其顺序如下：先是中间证书，然后是最终用户证书。 这两个证书首尾相连，中间没有空格。

PKCS#12 文件必须含有 .p12 扩展名。 它们只能包含证书和私钥（可选）。

步骤 6 选择**上传**。
系统会确定证书是否有效。 证书无效可能有以下原因：

- 证书文件不是有效的证书文件。
- 证书文件已过期。
- 公钥小于 2048 位。
- 证书中的服务器域名与站点 URL 不匹配。
- 系统自动生成的私钥与证书不兼容。
- 证书中未包含系统中的所有主机名（DMZ 主机名除外），或未包含站点和管理 URL。 在 MDC 系统中，证书中必须包含全球站点、本地站点及管理 URL。

步骤 7 （可选） 输入**密码**。
需要密码来解密 PKCS12 档案或加密的私钥（如果上传的 PEM 文件包含私钥）。

步骤 8 选择**继续**。
系统将导入 SSL 证书并将其显示在滚动式证书文件对话框中。

步骤 9 选择**完成**。

步骤 10 关闭维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。 如果此数据中心属于多数据中心 (MDC) 系统，那么管理员会被重定向至全局管理 URL。 管理员所看到的数据中心由 DNS 解析策略确定。 如果启用密钥再生，让一个数据中心退出维护模式会自动让系统中的所有数据中心退出维护模式。

此数据中心上用户的会议服务将被还原。

导出 SSL 证书

下载安全套接字层 (SSL) 证书：

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**设置** > **安全性** > **证书** > **数据中心** > **更多选项** > **导出 SSL 证书**。
系统将显示用于打开或保存证书的选项。

步骤 3 保存证书文件。
这仅提供 Cisco WebEx Meeting Server CWMS 最终实体证书。 如果您上传了其他中间证书，这里并不包括这些证书。

接下来的操作

验证管理员和最终用户都可以登录管理站点或公共网页，而不会看到任何站点不可信警告。

导出移动设备的 SSL 证书

运行 Apple iOS 5.0 或更高版本的 Apple iPhone 或 iPad 具有内置的可信根证书。 如果您的公司使用自签名证书，或者安装在 Cisco WebEx Meetings Server 上的根证书不在 Apple 可信的证书颁发机构列表上，您必须导出 SSL 证书，并使用电子邮件将证书发送给您的用户，以便这些用户加入 WebEx 会议前先在移动设备上安装该证书。

仅当使用自签名证书时才需要导出 SSL 证书。 如果您使用可信的证书中心签署的证书，则不需要导出 SSL 证书。

开始之前

验证预安装在用户的 Apple iPhone 或 iPad 上的可信根证书在 Apple 可信的证书颁发机构列表中。 有关详细信息，请访问 http://support.apple.com/kb/ht5012。

验证用户的移动设备能够与有效的高速互联网连接。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**设置** > **安全性** > **证书** > **数据中心** > **更多选项** > **导出 SSL 证书**。

步骤 3 将证书文件保存到本地硬盘。

步骤 4 将保存的证书文件附加到电子邮件中，并将其发送到每个授权用户的 iOS 电子邮件帐户。

步骤 5 用户在移动设备上打开电子邮件，保存该文件，然后在移动设备上安装证书文件：

a) 在**安装档案**页面上点击**安装**。

b) 在“未签名的档案”对话框上点击**立即安装**。
c) 输入 iOS 密码。
d) 点击**下一步**。
e) 点击**完成**。

下载 CSR 和私钥

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**设置** > **安全性** > **证书** > **数据中心** > **更多选项** > **下载 CSR**。
系统将弹出对话框，要求您保存含有 CSR 和私钥的 CSR.zip 文件。

步骤 3 在系统上选择要保存文件的位置，然后选择**确定**。

步骤 4 备份私钥文件 csr-private-key.pem，以备需要时使用。

生成自签名证书

自签名证书将在部署系统后自动生成。建议安装由证书颁发机构签名的证书。使用此功能可随时生成新的自签名证书。

注释 如果用户的系统使用自签名证书，他们在加入会议时可能遇到问题，除非客户端的管理员已配置其系统使用自签名证书。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**设置** > **安全性** > **证书** > **数据中心** > **更多选项** > **生成自签名证书**。

步骤 3 填写**生成自签名证书**页上的字段。

选项	描述
证书名称	输入自签名证书的名称。（必填）
X.509 使用者名称	系统的主机名为站点 URL。 在 MDC 系统上，您可以选择本地站点 URL 或全球站点 URL。

选项	描述
组织	输入组织名称。
部门	输入部门名称。
县/市	输入城市名称。
省/自治区	输入省、市或自治区名称。
国家/地区	选择国家/地区名称。

步骤 4 选择**生成证书和私钥**。
如果在重大升级后需要使用相同的 SSL 证书，那么必须上传生成的私钥以及用于获取证书的 CSR。 私钥必须为证书文件中的第一个数据块。

会生成并显示您的证书文件。

步骤 5 选择**完成**。

还原 SSL 证书

如果证书失效或您已经在系统上执行了灾难恢复，您可以使用此功能还原 SSL 证书。 Cisco WebEx Meetings Server 支持带 PEM 和 DER 编码及 PKCS12 档案的 X.509 证书。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 开启维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
我们建议您给每个虚拟机拍摄快照。 （请参阅通过使用 VMware vCenter 拍摄快照，第 7 页。）

在所有活动数据中心开启维护模式会关闭会议活动，并会使用户无法登录 WebEx 站点、安排会议、加入会议，或播放会议录制文件。 如果此数据中心属于多数据中心 (MDC) 系统，并且另一个数据中心是活动的，那么进行中的会议将故障转移到活动的数据中心。 这可能会导致活动的会议暂时中断。 有关要求开启维护模式的系统任务的信息，请参阅关于维护模式。

步骤 3 选择**设置** > **安全性** > **证书** > **数据中心** > **更多选项** > **导入 SSL 证书/私钥**。
如果您已安装证书，系统会警告您导入新证书将覆盖已安装的证书。

步骤 4 选择**继续**。

步骤 5 选择**浏览**，然后选择证书文件。
必须选择符合 X.509 的证书或证书链。 有效类型包括：

- PEM/DER 编码证书： .CER / .CRT / .PEM / .KEY

- PKCS12 加密证书： .P12 / .PFX

您可以用 PKCS#12 文件或 PEM 块的单个文件导入证书链。 如果使用 PEM 文件，必须按如下所述进行格式化：

- （可选）如果要再次应用之前的私/公钥对进行灾难恢复，请将公钥文件 (csr_private_key.pem) 和从证书中心 (CA) 收到的证书合并到一个文件中。 私钥必须为文件中的第一个数据块，紧跟其后的是公钥。 可以对其进行加密或解密。 它应该为 PKCS#8 格式，以 PEM 编码。 如果已加密，必须在密码字段中输入密码来对其进行解密。
- 下一个元素必须是中间证书中心的证书，该证书中心颁发的证书为 PEM 编码 X.509 格式。
- 您可以在基础结构中列入您所使用的所有中间证书。 根证书中心的证书不包括在内。 如果您正在使用专用证书中心，您必须确保已经将根证书分发给所有客户端。

必须将所有的证书合并在一个文件中上传。 不能先上传一个证书，然后又添加中间证书。 如果您使用的是采用中间证书的证书中心，并且在其客户端中没有分发中间证书，则可能需要上传中间证书。 上传中间证书将防止出现证书警告。

PKCS#12 文件必须含有 .p12 扩展名。 它们只能包含证书和私钥（可选）。

步骤 6 选择**上传**。
选择**上传**后，系统将确定您的证书是否有效。 证书无效可能有以下原因：

- 证书文件不是有效的证书文件。
- 您选择的证书文件已到期。
- 您的公钥必须至少为 2048 位。
- 证书中的服务器域名与站点 URL 不匹配。
- 系统自动生成的私钥与证书不兼容。

如果证书有效，请继续下一步。 如果证书无效，您将无法上传。 您必须选择有效的证书才能继续。

步骤 7 （可选） 输入**密码**。
需要密码来解密 PKCS12 档案或加密的私钥（如果上传的 .pem 文件包含私钥）。

步骤 8 选择**继续**。
系统将导入 SSL 证书并将其显示在滚动式证书文件对话框中。

步骤 9 在 **SSL 证书**页面上，选择**继续**以完成导入。

步骤 10 选择**完成**。

步骤 11 关闭维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。 如果此数据中心属于多数据中心 (MDC) 系统，那么管理员会被重定向至全局管理 URL。 管理员所看到的数据中心由 DNS 解析策略确定。 如果启用密钥再生，让一个数据中心退出维护模式会自动让系统中的所有数据中心退出维护模式。

此数据中心上用户的会议服务将被还原。

导入 SSO IdP 证书

对于由服务提供商启动的单点登录 (SSO)，如果在多数据中心 (MDC) 系统中有签名的验证请求，则必须将证书从每个数据中心导入到身份提供程序 (IdP)。（Cisco WebEx Meeting Server 无法使用其私钥来解密声明。）

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**设置** > **安全性** > **SSO IdP 证书**。

步骤 3 选择**浏览**，然后选择 SSO IdP 证书。

步骤 4 选择**上传**。
系统将显示您的证书文件。

步骤 5 选择**完成**以提交证书。

导入 SMTP 证书

将 SMTP 证书从本地计算机导入 CWMS 系统。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**设置** > **安全性** > **证书** > **数据中心** > **SMTP 证书** > **导入证书**。

步骤 3 选择**浏览**，然后选择 SMTP 证书。

步骤 4 选择**上传**。
系统将显示您的证书文件。

步骤 5 如果您的系统未在维护模式下，请选择**继续**以进入维护模式。

步骤 6 选择**完成**以提交证书。

步骤 7 关闭维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。 如果此数据中心属于多数据中心 (MDC) 系统，那么管理员会被重定向至全局管理 URL。 管理员所看到的数据中心由 DNS 解析策略确定。 如果启用密钥再生，让一个数据中心退出维护模式会自动让系统中的所有数据中心退出维护模式。

此数据中心上用户的会议服务将被还原。

步骤 8 选择**继续**。
系统将重新启动。

导入安全电话会议证书

只有在启用了 TLS 会议的情况下才需要安全电话会议证书。 如果未启用 TLS 会议，则该选项不可用。

开始之前

当在音频设置中选择了 TLS 作为传输类型时，CUCM 服务器需要安全电话会议证书。 请参阅关于配置音频设置，第 157 页以获取更多信息。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 开启维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
我们建议您给每个虚拟机拍摄快照。（请参阅通过使用 VMware vCenter 拍摄快照，第 7 页。）

在所有活动数据中心开启维护模式会关闭会议活动，并会使用户无法登录 WebEx 站点、安排会议、加入会议，或播放会议录制文件。 如果此数据中心属于多数据中心 (MDC) 系统，并且另一个数据中心是活动的，那么进行中的会议将故障转移到活动的数据中心。 这可能会导致活动的会议暂时中断。 有关要求开启维护模式的系统任务的信息，请参阅关于维护模式。

步骤 3 选择**设置** > **安全性** > **证书**。
安全电话会议证书部分将显示以下两条消息中的一条：

- 没有启用 TLS 电话会议，因此该系统不要求安全电话会议证书。
- 该系统上启用的 TLS 电话会议需要使用 CUCM 安全电话会议证书。

如果需要安全电话会议证书，则将为必须配置的每个 CUCM 服务器显示**导入证书**按钮。

步骤 4 选择**导入证书**（针对 CUCM *n*）。
系统将显示**安全电话会议证书**页面。

步骤 5 输入证书名称。

步骤 6 选择**浏览**，然后选择证书文件。

注释 如果 CUCM 使用自签名证书，那么请使用 CallManager.pem 文件。 如果 CUCM 使用第三方证书，那么请使用根证书颁发机构 (CA) 证书。 有关如何将 CUCM 证书下载到本地硬盘的详细信息，请参阅《规划指南》中的“下载 CUCM 证书”。

步骤 7 选择**上传**。
选择**上传**后，系统将确定您的证书是否有效。

如果证书有效，请继续下一步。 如果证书无效，您将无法上传。 您必须选择有效的证书才能继续。

步骤 8 选择**继续**。
系统将导入 SSL 证书并将其显示在滚动式证书文件对话框中。 将通知您已导入 SSL 证书。

步骤 9 选择**完成**。

步骤 10 返回到步骤 4 并为下一个 CUCM 服务器重复上述过程。

步骤 11 选择**关闭维护模式** > **继续**。
关闭维护模式后系统将重启。 完成重启后，您可以再次登录管理站点。

配置用户会话安全

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**设置** > **安全性** > **用户会话**。

步骤 3 将**用户会话**页面上的字段填写完整以设定网页过期时间。

选项	描述
网页过期时间	配置用户自动退出前的天、小时和分钟数。 **缺省：** 一小时三十分钟。
移动设备或快捷会议工具过期日（SSO）	配置用户自动退出前的天、小时和分钟数。 **缺省：** 14 天 ） **注释** 仅当配置了 SSO 时，才会出现此字段。
同时进行的用户会话数	配置用户在任意给定时间可以开始的（同一种类的）用户会话数或选择**无限制**。
同时进行的管理员会话数	配置用户在任意给定时间可以打开的管理员会话最大数目或选择**无限制**。
显示重要的登录信息	选择此选项以显示用户已登录的IP地址，以及登录尝试失败的次数。 **缺省：** 已选择。

步骤 4 选择**保存**。

配置联合单点登录 (SSO) 设置

CWMS 系统支持基于行业标准安全声明标记语言（SAML）2.0 协议的单点登录 (SSO) 系统。

SSO 允许客户端使用内建的 SSO 系统简化 CWMS 系统的管理。 通过 SSO，用户能够使用其公司的登录凭证安全地登录系统。 用户尝试登录时，您也可以配置 SSO 来联机创建或管理用户帐户。 为保护公司的登录信息，用户登录凭证不会发送给 Cisco。

注释 启用 SSO 将覆盖用户的 SSO 设置。 确保您启用 SSO 之前已告知用户。

配置 SSO 的操作十分复杂，我们强烈建议您在继续操作前联系 Cisco 渠道合作伙伴或 Cisco 高级服务。

开始之前

- 生成一组公钥和私钥，以及包含公钥的 X.509 证书，并将其上传（请参阅管理证书，第 205 页）。

  注释 启用 SSO 后，用户凭证由企业验证系统来管理。 某些密码管理功能对用户不再适用。 请参阅 配置密码，第 173 页 和 编辑用户，第 115 页 以获取更多信息。 尽管管理员也是最终用户，但是他们不使用 SSO 来登录；他们使用本产品的管理员凭证登录。

- 配置 SSO IdP 证书以使用此功能。 请参阅导入 SSO IdP 证书，第 213 页以获取更多信息。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**设置** > **安全性** > **证书** > **联合 SSO**。

步骤 3 生成了前提条件中所述的公钥和私钥以及 X.509 证书后，请选择**继续**。

步骤 4 选择启动方法：

- 从 SP（服务提供程序）起始 - 用户选择到服务提供程序的链接后会临时重定向到身份提供程序以进行验证。 然后用户返回到初始请求的链接。
- 从 IdP（身份提供程序）起始 - 用户从身份提供程序开始登录，然后重定向到服务提供程序的登录页面。

步骤 5 填写这些字段并在 **SSO 配置** 页面上选择选项：
注释 请参考 IdP 配置文件以填写 IdP 字段。 选择 **IdP 证书**链接。

字段	描述
从 SP（服务提供程序）起始	选择该选项以通过服务提供程序启动的方式进行登录。
已签署 AuthnRequest	选择该选项以要求必须由服务提供程序的私钥来标记 AuthnRequest 消息。 **注释** 如果希望在导出的 SAML 元数据文件中包含站点的 SSL 证书，那么必须选择该选项。
目标位置	IdP（接收验证请求以进行处理）的 SAML 2.0 实现 URL。 **注释** 仅当选中**已签署 AuthnRequest**时才显示此字段。
从 IdP（标识提供程序）起始	选择该选项以通过身份提供程序启动的方式进行登录。
目标页 URL 参数名	当 SSO 成功时，系统重定向到此 URL。 **缺省：** 目标物 **注释** 在从 IdP 起始的系统上，URL 必须是合并的 URL 且以下列格式表示： 服务登录 URL，“?”或“&”，目标页URL参数，“=”（如果没有出现的话），以及目标 URL。
SAML 颁发者（SP 标识）	输入为 IdP 配置的同一 SP 标识。 引用 SAML 2 协议。
SAML 颁发者（IdP 标识）	输入为 IdP 配置的同一标识。 引用 SAML 2 协议。
客户 SSO 服务登录 URL	IdP 中的 SAML 2 的声明占用 URL。
NameID 格式	选择在 IdP 中设置的同一 NameID 格式。 NameID 是发送声明中的用户标识以及来自 Cisco WebEx Meetings 的单点注销请求所用的格式。 请参阅 SAML 协议获取指导。 我们建议您将电子邮件地址设置为您的 NameID。 这样做将为已经基于系统上的电子邮件地址设置了其帐户的用户简化使用 SSO 的过程。 我们支持但不建议使用其他 NameID 格式。 如果使用非电子邮件地址的格式，而且禁用了 SSO，则用户将再也无法登录 WebEx 站点。 **缺省：** 未指定

字段	描述
AuthnContextClassRef	输入在 IdP 中配置的值。 AuthnContextClassRef 是在 AuthnRequest 消息中出现的值。 **缺省：** urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified
缺省 WebEx 目标页面 URL	当 SSO 成功时，系统重定向到此 URL。 缺省页为 Cisco WebEx Meetings 会议页（与正常登录的页面相同）。
客户 SSO 错误 URL	当SSO失败时，系统重定向到此URL。 缺省情况下，错误页是公共 Cisco WebEx Meetings 错误页。
单点注销	该选项启用由 SAML 2 协议定义的单点注销。 如果已选择SSO选项但未选择单点注销选项，那么在最终用户的页面上不会出现注销选项。 删除 ADFS 2.0 的该选项。 **注释** 此版本不支持从 IdP 起始的 SLO。
客户 SSO 服务注销 URL **注释** 仅当选中单点注销时才显示此选项。	输入在 IdP 中的 SAML 2 的声明占用 URL。
自动创建帐户	没有 Cisco WebEx 帐户的用户无法登录。 如果您选择此选项，当新用户尝试登录时，系统会为其自动创建一个帐户。
自动更新帐户	如果选择该选项，那么在 SAML 2 声明中出现“updateTimeStamp”时，用户信息会得到更新，用户信息将比 Cisco WebEx 中的当前数据更新。
删除 Active Directory UPN 的 UID 域后缀	选择该选项可验证不包含域后缀的用户。 **删除 Active Directory UPN 的 UID 域后缀**选项在下列情况中有效： • NameId 格式是电子邮件，而 UID 格式是 X509 使用者名称或用户主要名称 (UPN)。 • NameId 格式是 X509 使用者名称或 UPN。

步骤 6 选择**启用 SSO**。

系统将显示**复查 SSO 设置**页面。 复查设置并选择**保存**。

禁用 SSO

开始之前

禁用SSO将会使用户无法用其公司凭证进行登录。确保通知了您的用户将要禁用SSO，而他们仍将可以用其 Cisco WebEx Meetings 凭证进行登录。

步骤 1 登录管理站点。

步骤 2 选择**设置** > **安全性** > **联合 SSO**。

步骤 3 找到句子“如果您要禁用 SSO，请单击此处。” 选择**单击此处**链接。

步骤 4 选择**禁用 SSO** 以确认。
出现**联合 SSO** 页面，同时会出现一条确认您已禁用 SSO 的横幅。

配置云功能

您可以对系统进行配置以使用户使用单个版本的 Cisco WebEx Meetings 快捷会议工具，该会议工具可与 Cisco WebEx Meetings Server 及 SaaS WebEx 帐户一同使用，也可以用来查看由 Cisco WebEx Meetings 在线主持的培训视频。

注释 您的系统支持 Cisco WebEx SaaS 发行版 WBS27 及更高版本 和 Cisco WebEx Meetings 1.2。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**设置** > **安全性** > **云功能**。

步骤 3 （可选） 选择**允许用户从 WebEx 快捷会议工具登录 SaaS WebEx 帐户**。

步骤 4 选择**保存**。

配置虚拟机安全性

您的虚拟机安全功能包括更新加密密钥和启用或禁用 FIPS 兼容加密的功能。

更新您的加密密钥

Cisco WebEx Meetings Server 使用内部生成的加密密钥来保护位于系统上的虚拟机之间的所有通信安全。 使用该功能定期更新加密密钥。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 开启维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
我们建议您给每个虚拟机拍摄快照。 （请参阅通过使用 VMware vCenter 拍摄快照，第 7 页。）

在所有活动数据中心开启维护模式会关闭会议活动，并会使用户无法登录 WebEx 站点、安排会议、加入会议，或播放会议录制文件。 如果此数据中心属于多数据中心 (MDC) 系统，并且另一个数据中心是活动的，那么进行中的会议将故障转移到活动的数据中心。 这可能会导致活动的会议暂时中断。 有关要求开启维护模式的系统任务的信息，请参阅关于维护模式。

步骤 3 选择**设置** > **安全性** > **虚拟机**。

步骤 4 选择**更新加密密钥**。

步骤 5 关闭维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。 如果此数据中心属于多数据中心 (MDC) 系统，那么管理员会被重定向至全局管理 URL。 管理员所看到的数据中心由 DNS 解析策略确定。 如果启用密钥再生，让一个数据中心退出维护模式会自动让系统中的所有数据中心退出维护模式。

此数据中心上用户的会议服务将被还原。

关于 FIPS

联邦信息处理标准 (FIPS) 140 是美国和加拿大政府标准，指定了密码模块的安全性要求。 密码模块是“在密码范畴内实现经认可的安全性功能（包括密码算法和密钥生成）的一套硬件、软件和/或固件”。 密码模块是被验证的对象。

FIPS 140 要求

在非常高的级别上，FIPS 140 要求适用于下列模块特征：

- FIPS 认可的算法的实现
- 密钥生命周期的具体管理
- 认可的随机数生成

- 密码算法、图像完整性和随机数生成器 (RNG) 的自测试

Cisco WebEx Meetings Server 使用 CiscoSSL 2.0 达到 FIPS 140-2 2 级要求。

启用 FIPS

启用 FIPS 可能导致与流行 Web 浏览器和操作系统的兼容性下降。 症状可能包括（但不限于）登录系统时的问题、404 错误，以及开始和加入会议时的问题。

Cisco 建议采取下列操作：

- 请确保 Windows PC 运行的当前版本是 Windows XP SP3 或更高版本。
- 无论用户期望的浏览器是 Internet Explorer、Mozilla Firefox 还是 Google Chrome，请将所有 Windows 计算机更新到 Microsoft Internet Explorer 8 或更高版本。 用户必须在所有计算机上提供 Internet Explorer 8，因为我们启用 FIPS 的客户端（Cisco WebEx Meetings、快捷会议工具以及 WebEx 录制文件播放器）使用仅在 Internet Explorer 8 及更高版本上可用的启用 FIPS 的系统库。
- 在所有用户计算机上将**互联网设置**配置为 TLS 加密。 在 PC 桌面上，选择**控制面板** > **Internet 选项** > **高级** > **安全** > **使用 TLS 1.0** 和**使用 TLS 1.2**。 我们建议同时选择两者以实现最高的兼容性，但必须至少选择**使用 TLS 1.0**。
- 如果您的用户计划为访客（例如非公司员工）主持会议，您必须在他们加入会议之前，按上文所述通知访客用户手动更新操作系统和浏览器。 如果不执行上述步骤，就可能遇到兼容性问题。 我们建议在会议邀请中包含上述说明。 可以通过在管理站点上编辑相应的会议邀请来完成此操作，选择**设置** > **电子邮件** > **模板**。

启用符合 FIPS 的加密

使用此功能可启用符合联邦信息处理标准 (FIPS) 的加密设置。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 开启维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
我们建议您给每个虚拟机拍摄快照。 （请参阅通过使用 VMware vCenter 拍摄快照，第 7 页。）

在所有活动数据中心开启维护模式会关闭会议活动，并会使用户无法登录 WebEx 站点、安排会议、加入会议，或播放会议录制文件。 如果此数据中心属于多数据中心 (MDC) 系统，并且另一个数据中心是活动的，那么进行中的会议将故障转移到活动的数据中心。 这可能会导致活动的会议暂时中断。 有关要求开启维护模式的系统任务的信息，请参阅关于维护模式。

步骤 3 选择**设置** > **安全性** > **虚拟机**。

步骤 4 选择**启用**以启用符合 FIPS 的加密，然后选择**继续**进行确认。
系统上将配置符合 FIPS 的加密。

步骤 5 关闭维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。

当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。 如果此数据中心属于多数据中心 (MDC) 系统，那么管理员会被重定向至全局管理 URL。 管理员所看到的数据中心由 DNS 解析策略确定。 如果启用密钥再生，让一个数据中心退出维护模式会自动让系统中的所有数据中心退出维护模式。

此数据中心上用户的会议服务将被还原。

禁用符合 FIPS 的加密

使用此功能可在系统上禁用符合联邦信息处理标准 (FIPS) 的加密。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 开启维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
我们建议您给每个虚拟机拍摄快照。 （请参阅通过使用 VMware vCenter 拍摄快照，第 7 页。）

在所有活动数据中心开启维护模式会关闭会议活动，并会使用户无法登录 WebEx 站点、安排会议、加入会议，或播放会议录制文件。 如果此数据中心属于多数据中心 (MDC) 系统，并且另一个数据中心是活动的，那么进行中的会议将故障转移到活动的数据中心。 这可能会导致活动的会议暂时中断。 有关要求开启维护模式的系统任务的信息，请参阅关于维护模式。

步骤 3 选择**设置** > **安全性** > **虚拟机**。

步骤 4 选择**禁用**以禁用符合 FIPS 的加密，然后选择**继续**进行确认。
系统上将禁用符合 FIPS 的加密。

步骤 5 关闭维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。 如果此数据中心属于多数据中心 (MDC) 系统，那么管理员会被重定向至全局管理 URL。 管理员所看到的数据中心由 DNS 解析策略确定。 如果启用密钥再生，让一个数据中心退出维护模式会自动让系统中的所有数据中心退出维护模式。

此数据中心上用户的会议服务将被还原。

上传安全登录警告消息

对于要求用户在登录前阅读安全消息并接受协议的安全站点，请上传包含警告消息的文件。

要删除登录警告消息，请参阅配置安全登录警告，第 224 页。

开始之前

在用户登录 WebEx 公共站点或管理站点之前，创建一个带有所要显示的警告消息的文本文件 (.txt)。该文本文件必须使用 UTF-8 字符及编码方式。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**设置** > **安全性** > **登录警告**。

步骤 3 选择**浏览**并选中要上传的文本文件。

步骤 4 选择**上传**。
文件随即上传并显示在所有登录页面上。

配置应用程序审核日志

如果站点要求存储有关系统更改的审核信息，请配置“应用程序审核日志”设置。

如果用户配置为审核员，那么**应用程序审核日志**选项仅由该审核员可见和配置。 如果系统没有具有审核员角色的用户，那么**应用程序审核日志**选项仅由管理员、SSO 管理员或 LDAP 管理员可见和配置。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**设置** > **安全性** > **应用程序审核日志**。

步骤 3 选择**启用审核日志**以生成日志。

步骤 4 要将应用程序审核信息记录到远程系统日志服务器上，输入**主远程系统日志服务器**的参数。
“远程系统日志审核事件级别”菜单中的事件按重要性的顺序进行组织。

a) 如果您希望系统将应用程序审核信息记录到远程系统日志服务器上，输入**IPv4 地址**和**端口号**。

b) 选择协议。

c) 选择**远程系统日志审核事件级别**。
选择事件级别时，高于所选级别的级别也会被选中。 例如，选择**错误**事件级别后，系统会捕捉错误、重要、警告和紧急事件。

级别仅对操作系统日志以及这些消息的严重性产生影响。

缺省为紧急事件级别。 在“审核员”视图中，还显示日志分区的警告。

步骤 5 （可选） 要将应用程序审核信息记录到备用远程系统日志服务器上，请输入“备用远程系统日志服务器”的参数。

步骤 6 （可选） 要删除旧的日志文件，请在**日志清除设置**中选择要清除先前日志归档的日期并选择**清除日志归档**。

步骤 7 通过移动滑块设置**日志分区上空闲空间的最低百分比**。
日志服务参数确保日志分区上有所选的空闲空间百分比可用。 缺省设置为 20%。

审核员从“审核员”标签页访问此窗口时，系统将显示“日志分区警告”的配置。

步骤 8 设置**保留不超过所选天数的日志归档**。
缺省设置为 40 天。

步骤 9 选择**保存**。

接下来的操作

有关设置警告阈值的详细信息，请参阅查看和编辑警告， 第 90 页。

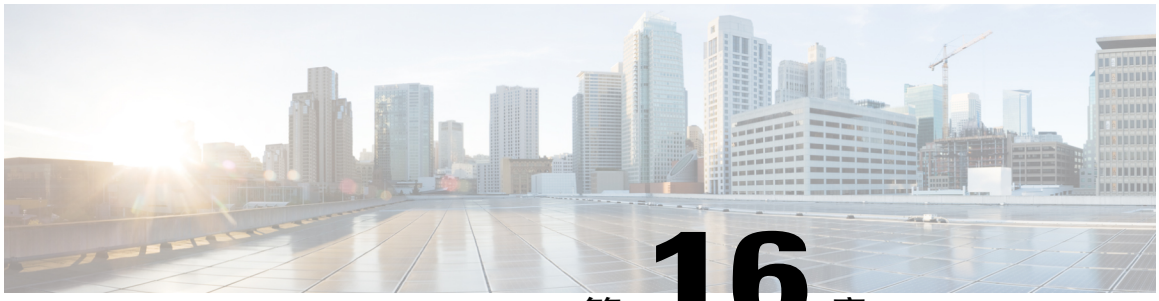
配置安全登录警告

安全登录警告在公共 WebEx 站点、管理 WebEx 站点和 CLI 登录页面上显示警告消息。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**设置** > **安全性** > **登录警告**。

步骤 3 浏览消息，并选择**上传**或**删除消息**。
选择“上传”可将消息添加到系统中，并在登录页面上显示，选择“删除消息”可将文件从系统中删除，并且不再出现在登录页面上。



第 16 章

管理报告

可以查看月度报告并为特定日期范围自定义报告。 报告使用**公司信息**页上配置的语言、区域设置和时区设置。 请参阅配置公司信息，第 151 页以获取更多信息。

重要事项

部署或升级系统时，直到首月月底，将不存在任何报告（自定义详细信息报告除外）的数据。在这种情况下，直到首月月底，**下载**链接以及本节中描述的所有其他报告将不可用。

- 下载月报，第 225 页
- 关于月度报告，第 226 页
- 生成自定义详细信息报告，第 227 页
- 关于自定义详细信息报告，第 228 页

下载月报

您可以查看和下载 PDF 格式的月报。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**报告**。

步骤 3 选择想要查看的月报的**下载**链接。

关于月度报告

您的月度报告包含以下部分：

系统摘要报告

您的系统摘要报告包含以下报告：

- 服务采用率 - 此报告显示的图表描述前三个月中的唯一主机数和与会者数以及在接下来三个月中预期的增长率。
- 用户许可证 - 此报告显示正在使用的已购买许可证的百分比和描述在过去三个月中使用的许可证数及在接下来三个月中的预期增长率的图表。 您可以使用这些数字来预测未来许可证的使用量并相应调整您的许可证购买数。 请参阅通过使用许可证管理器完成许可证以获取更多信息。
- 系统容量 - 此报告显示会议参加者高峰和该高峰使用量消耗的系统容量的百分比。 该图表描述在过去三个月中的会议参加者高峰及在接下来三个月中的预期增长率。
- 存储空间 - 此报告以占总存储空间的百分比和总千兆字节 (GB) 的形式显示您的数据存档和录制文件的存储使用量。 该图表描述在过去三个月中的总存储量及在接下来三个月中的预期增长率。 使用此报告可监视存储使用量。 如果您需要添加更多存储空间，必须在激活新的存储服务器之前将现有存储数据存档和录制文件手动复制到该存储服务器上。

  注释 只有在已经配置了存储服务器时才显示此报告。 请参阅配置存储服务器，第 136 页以获取更多信息。

- 网络 - 此报告显示以下内容：
  - 高峰网络带宽消耗量 (Mbps)。
  - 描述在过去三个月中的高峰网络带宽消耗量 (Mbps) 及在接下来三个月中的预期增长率（红色栏表示最大网络带宽）的图表。
  - 指示每个系统资源所消耗的带宽百分比的饼图。

  报告从数据库中抽取数据。 如果带宽消耗小于 1 Mbps，监控模块在数据库中写入 0。 因此，报告中的 0 表示该功能未占用很多的网络带宽。
- 系统计划停机时间和意外故障 - 此报告显示以下内容：
  - 在过去三个月中的系统平均运行时间。
  - 在过去三个月中系统非计划中断的平均时间。
  - 在过去三个月中由于这些中断而干扰的平均会议数。
  - 描述在过去三个月中的计划停机时间和非计划中断及在接下来三个月中的预期增长率的图表。

注释 有时停机时间增加反映了使用量增加。 确保将停机时间的统计信息与在其他报告中显示的使用量统计信息进行对比。

会议摘要报告

您的会议摘要报告包含以下报告：

- 会议状态 - 此报告显示的图表描述上个月的会议状态、遭遇问题的会议百分比和该月举行会议的总数。 有关实时会议状态，请参见“控制板”。 请参阅关于控制板以获取更多信息。 有关会议状态的更多信息，请参阅查看会议列表，第 93 页。
- 会议容量 - 此报告显示的图表描述系统在上个月举行的会议的大小、会议容量的细目和该月举行的最大会议的详细信息。
- 会议功能使用情况 - 此报告显示以下内容：

  上个月中使用最多的功能，包括使用该功能的总分钟数。

  上个月中系统上使用量增加最快的功能，包括增长率。

  描述系统上每个功能的使用情况（以分钟计）的图表。

  描述系统上增加最快的功能的增长率的图表。

- 活动中的参加者电子邮件域排名 - 此报告显示以下内容：

  描述最活跃参加者电子邮件域的图表。

  参加者电子邮件域的细目。

  系统上的会议参加者使用最多的三个电子邮件域列表。

- 高峰日和高峰时段 - 此报告显示两个图表。 第一个图表描述上个月中一周最忙的一天。 第二个图表描述上个月中系统一天最忙的时间。

生成自定义详细信息报告

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**报告** > **自定义您的报告**。

步骤 3 选择要查看的报告日期范围，然后选择**提交**。
缺省为最近月份。 您可以选择过去的日期范围（最多为过去六个月）。

出现**已提交自定义报告请求**页，显示自定义报告的日期。 会向您发送电子邮件，其中含有 CSV 格式自定义报告的链接。

步骤 4 选择**完成**。

关于自定义详细信息报告

在生成自定义详细信息报告后，您会收到一个电子邮件，包含带有 CSV 格式的下列报告的存档：

- **欺诈尝试报告** — 显示所有失败的电话访问尝试，在这些尝试中呼叫者尝试开始或加入个人会议时三次输入了错误的主持人或参加者访问码或主持人 PIN：
  - 呼叫的访问号码 — 为了开始或加入个人会议而拨打的 Cisco WebEx 呼入号码。
  - 呼叫方号码 — 用于发出呼叫的电话的电话号码。
  - 呼叫开始时间 — 呼叫的日期和时间。
  - 尝试的第 1 个访问码 — 呼叫者输入的第一个无效访问码。
  - 第 1 个访问码所有者的电子邮件（如果可用）— 与第一个无效访问码关联的用户的电子邮件地址，前提是该访问码与有效的 Cisco WebEx Meetings Server 帐户关联。
  - 尝试的第 2 个访问码 — 呼叫者输入的第二个无效访问码。
  - 第 2 个访问码所有者的电子邮件（如果可用）— 与第二个无效访问码关联的用户的电子邮件地址，前提是该访问码与有效的 Cisco WebEx Meetings Server 帐户关联。
  - 尝试的第 3 个访问码 — 呼叫者输入的第三个无效访问码。
  - 第 3 个访问码所有者的电子邮件（如果可用）— 与第三个无效访问码关联的用户的电子邮件地址，前提是该访问码与有效的 Cisco WebEx Meetings Server 帐户关联。
- **会议报告** — 包含指定时间段内召开的所有会议的信息：
  - 会议标识 - 安排会议时系统生成的唯一会议标识。
  - 会议号 — Cisco WebEx 会议号。
  - 主题 - 主持人配置的会议名称。
  - 主持人姓名 - 会议主持人的姓名。
  - 开始时间 - 会议开始的时间和日期。
  - 持续时间 - 会议持续的时间（分钟）。
  - 参加者人数 — 包括主持人在内的参加者人数。

注释 如果访客或主持人加入会议两次，系统会把访客的加入次数重复加到参加者计数，但主持人只算加入一次。

- 每个会议的状态。
- 呼入音频分钟数
- 回呼音频分钟数
- 网络语音分钟数
- 视频分钟数
- 录制文件分钟数
- 录制时间间隔 - 会议期间创建的每个录制文件的开始和结束时间。
- “Web 共享”分钟数 — 所有参加者用于网络会议的总分钟数（例如，如果有三个参加者出席一个会议的网络会议部分，该会议持续了 10 分钟，则“Web 共享”分钟数为 30）。
- 参加者 - 会议参加者列表。
- 主持人平台/浏览器 - 主持人召开 Cisco WebEx 会议时所使用的操作系统和浏览器版本。
- 主持人 IP 地址 - 主持人召开 Cisco WebEx 会议时所使用的 IP 地址。
- 跟踪代码 - 安排会议时主机应用的跟踪代码。

- **网络带宽使用量报告** - 指定时间段内下列每项功能每天的网络带宽消耗量：
  - 音频的带宽消耗上限（mbps）
  - 音频网络语音的最大带宽消耗量 (mbps)
  - 视频的带宽消耗上限（mbps）
  - Web 共享的带宽消耗上限（mbps）

  消耗量为 0（零）表示该日期未使用此功能。 如果指定日期的消耗量小于 1 Mbps，那么会显示消耗量小于 1。

  视频的网络带宽消耗包括摄像头视频和网络会议的视频文件共享。 如果站点禁用视频，则无法打开摄像头获得视频，但是仍可以共享视频文件。 这导致报告中包含的视频会消耗一些网络带宽。 这是站点禁用视频时导致产生视频网络带宽消耗的唯一情形。

- 存储空间使用量报告 - 显示截至所列日期使用的总磁盘空间，以及每个日期发生的录制会议数。

注释 只有在已经配置了存储服务器时才包含此报告。 请参阅配置存储服务器，第 136 页以获取更多信息。

- **参加者报告** - 显示了会议的历史记录、各个会议的开始时间以及各个会议所应用的跟踪代码。

会议标识 - 安排会议时系统生成的唯一会议标识。

会议名称 - 安排会议时主持人在**内容**字段中输入的会议名称。

用户名 - 主持人的用户名。

加入时间 - 用户加入 Cisco WebEx 会议的时间和日期。

离开时间 - 用户离开 Cisco WebEx 会议的时间和日期。

持续时间 - 用户参加 Cisco WebEx 会议的时间（分钟）。

平台/浏览器 - 主持人召开 Cisco WebEx 会议时所使用的操作系统和浏览器版本。

客户端 IP 地址 - 主持人召开 Cisco WebEx 会议或参加者出席 Cisco WebEx 会议所使用的 WebEx 客户端 IP 地址。

会话开始时间 - 会话开始时间。

会话结束时间 - 会话结束时间。

会话类型 - 会话类型可以是视频（Web 共享）、网络语音（电话连接）、呼入或回呼。

会话持续时间 - 会话持续的时间。

电话号码 - 呼入 WebEx 会议所用的电话号码。

电话服务器 - 电话服务器。

- **系统停机报告** - 指定时间段内的系统停机信息，包括下列字段：

  类别 - 停止使用或维护。 停止使用表示断电。 维护表示计划的维护时段。

  服务 - 受影响的功能。

  停机开始 - 停机开始的日期和时间。

  停机结束 - 停机结束的日期和时间。

  中断的会议数 - 中断的会议数目。 此字段对于维护停机为空，因为已经计划维护停机。 如果在停止使用停机期间没有安排任何会议，那么该数为 0。

- **用户许可证使用量报告** - 此报告有两种版本。 一个版本显示过去 30 天的许可证使用量，标题为 UserLicenseUtilizationReportForLastMonth.csv，另一个版本显示当前月的许可证使用量（从该月的第一天到当前日），标题为 UserLicenseUtilizationForThisMonth.csv。 每个这类报告都包含以下字段：

  用户名 - 会议主持人的用户名。

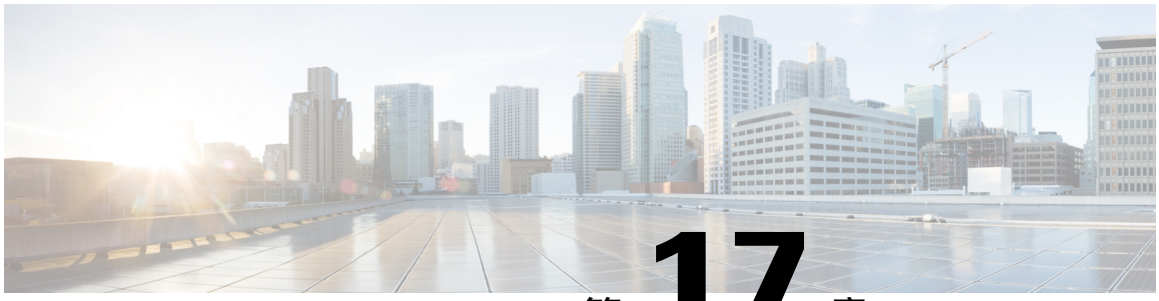
  电子邮件地址 - 会议主持人的电子邮件地址。

  会议标识 - 安排会议时系统生成的唯一会议标识。

  会议号 — Cisco WebEx 会议号。

  开始时间 - 会议开始的日期和时间。

同时进行的会议 - 同一用户安排的同时进行的会议数。 每个录制的同时进行的会议会为安排同时进行的会议的用户在此报告中新增一行。



第 17 章

管理许可证

- 管理许可证， 第 233 页
- 主持人许可证重新托管， 第 240 页

管理许可证

由单数据中心支持的系统不需要系统许可证。 首次部署本产品时，您将获得 180 天试用期，并可以使用无数的主持人许可证。 免费试用期到期之后，您需要为主持会议的所有用户购买永久主持人许可证。 安排或参加会议但是不主持任何会议的用户不需要许可证。

如果部署的系统由多数据中心支持，您必须购买“多数据中心 (MDC)”功能许可证。 MDC 许可证不存在宽限期或试用期。 在尝试加入 MDC 系统中的数据中心之前，必须在主数据中心托管 MDC 许可证。 要部署 MDC 系统，请参阅加入数据中心以创建多数据中心 (MDC) 系统， 第 243 页。

关于 MDC 许可证

新的多数据中心 (MDC) 不存在试用期。 在加入数据中心之前，请先购买适合系统容量的 MDC 功能许可证。 MDC 许可证托管在主数据中心上；接受另一个数据中心加入以构成系统的数据中心，通常为正在运行许可证管理器的数据中心。 如果您升级或扩展现有的 MDC 系统，必须在 90 天或更短时间内购买正确版本和容量的许可证。

- 永久 MDC 许可证 - 购买以允许数据中心加入单个 MDC 系统。
- 宽限 MDC 许可证 - 在购买必要的许可证之前的 90 天期限内，您可以在 MDC 系统中升级或扩展数据中心。 此系统修改之后，您有 90 天时间解决任意许可证问题，例如购买 MDC 许可证用于更大的系统。 如果在宽限 MDC 许可证到期之前未安装相应容量和版本的许可证，未托管许可证管理器的数据中心将被禁用。
- 演示 MDC 许可证 - MDC 系统的临时许可证支持。 颁发演示 MDC 许可证由供应商按具体案例确定，许可证的有效期在许可证颁发时确定。

要部署 MDC 系统，请参阅加入数据中心以创建多数据中心 (MDC) 系统， 第 243 页。

关于主持人许可证

本产品的**许可方式基于主持人**，要求您为每个**主持**会议的用户购买许可证，或者为这些用户手动分配许可证。用户代表他人出席或安排会议时，不会耗用主持人许可证。出于报告目的，每月计算一次许可证使用量，例如，从 1 月 1 日至 31 日计算一次，从 2 月 1 日至 28 日计算一次，以此类推。

注释 从先前版本升级至版本 2.5 或更高版本时，原始系统上的所有许可证会从用户分配中释放出来。用户可以通过主持会议或者手动分配许可证的方式重新获取许可证。 安装多数据中心 (MDC) 系统时，也可以这样做。加入MDC 系统的数据中心将丢失主持人许可证。加入之后，可以在MDC 系统上重新托管这些许可证。

可以从**报告**页面请求提供许可证消耗总数的报告。 此外，我们建议您查看显示许可证消耗趋势的 PDF 摘要报告。 通过查看许可证的总体趋势，您可以更有效地计划未来许可证的购买，以适应公司内对此系统日益增加的使用。

主持人许可证类型

主持会议需要主持人许可证。 安排或出席会议不需要许可证。 主持人许可证的类型为：

- **永久主持人许可证** — 已安装的主持人许可证，购买用于允许用户主持会议，在该用户首次主持会议时分配给他。 主持人许可证可由管理员手动分配给用户；用户不必等到主持会议时就可以分配到许可证。 如果有一个用户拥有宽限期许可证，并且永久主持人许可证通过删除主持人或购买更多永久主持人许可证变得可用，则永久许可证被分配给拥有宽限期许可证的主持人。

  在版本 2.5 中，用户不会消耗多个永久主持人许可证，并且可以同时主持最多两个会议。 此外，永久主持人许可证仅在该许可证的用户停用时才被释放供另一主持人使用（与版本 2.0 不同，后者为一段时间内未主持会议的主持人的许可证会被释放）。 如果有人尝试主持会议，并且：

  无可用的许可证。

  由于会议已安排或会议主持人已停用，主持人的许可证已过期。

  系统会显示错误消息，会议无法开始。 （请参阅超过可用的许可证数 ， 第 235 页。）

- **试用期主持人许可证** — 系统中自动分配的临时主持人许可证，具有试用期。

- **宽限期主持人许可证** — 在所有永久许可证已消耗的永久许可证环境中会议主持人消耗的临时许可证。 如果暂时超出安装的许可证数，可临时为具有永久主持人许可证的系统（系统不处于试用期）提供数目受限的宽限期主持人许可证。 系统会向管理员显示有关许可证过多的警告。在这种情况下，临时宽限期主持人许可证与用户的关联期限为 180 天。 当永久主持人许可证变得可用时，永久主持人许可证会与用户关联，并且宽限期许可证被释放。 如果 180 天之后用户没有获得永久主持人许可证，用户将无法主持会议。 （有关永久主持人许可证超额时的系统行为的更多信息，请参阅超过可用的许可证数 ， 第 235 页。）

- **演示许可证** — 临时主持人许可证，具有各种有效期限（由供应商根据具体案例提供）。（它们主要用于测试。） 这些许可证过期后，系统将恢复到其之前的许可证状态。 主持人演示许可证会过期，无论是否已分配给用户。
- **本地主持人许可证** — 在本地数据中心上管理的许可证。
- **远程主持人许可证** — 通过使用 Active Directory 管理的许可证。
- **过期主持人许可证** — 由于超过分配的时间而无效的临时主持人许可证。 拥有过期主持人许可证的用户仍然可以出席会议，也可以替他人安排会议。

用户的许可证状态

本节说明用户状态与主持人许可证计算方法之间的关系：

- 参加者 - 出席会议但不主持会议，且无法控制主持人功能（例如，除非主持人将参加者指定为主讲者，否则其无法提供内容）的人员。 会议参加者不消耗主持人许可证。 此用户也可以代表他人安排会议，而不消耗主持人许可证。
- 会议主持人 - 以会议主持人身份安排和出席会议，并可控制所选功能，例如确定主讲者或将其他参加者静音。 主持会议将消耗许可证，并且该许可证在保留给该用户，直到用户被停用。 主持人许可证有多种类型。（有关主持人许可证类型的更多信息，请参阅主持人许可证类型，第 234 页。）
- 候补主持人 - 安排会议时确定为会议主持人缺席时可担任主持人角色的人员。 如果安排会议的会议主持人未出席，候补主持人可控制会议主持人所具有的大多数功能。 主持会议所需的许可证会根据安排会议的用户的状态进行验证。 也就是说，安排会议的用户在会议召开时必须拥有有效的许可证，即使用户不出席该会议。
- 在主持人之前加入 (JBH) - 允许参加者在主持人或候补主持人到达之前加入会议。
- 重叠会议 - 由同一个主持人在一天的同一时间内安排的两个或两个以上的会议。 从版本 2.5 开始，用户可以主持最多两个同时进行的会议，仅消耗一个许可证；用户不能同时主持两个以上会议。

超过可用的许可证数

免费试用期内，任何容量的系统上都有无数的可用许可证数。 购买许可证并在系统上安装后，必须确保安装有足够的许可证来用于系统上的所有主机。

如果暂时超出安装的许可证数，新主持人可以获取宽限期许可证。（有关宽限期许可证的信息，请参阅主持人许可证类型，第 234 页。）

如果系统上的活动主持人数经常超出安装的许可证数，系统会发送一封电子邮件给管理员，指示已超过安装的许可证数，建议购买更多许可证。 您必须在系统上减少许可证使用量或增加许可证数，以使许可证数大于等于活动主持人数。

审核管理器每天运行一次 (凌晨 2:00)，必要时会调整使用的许可证数。 如果主持人数降到少于安装的许可证数，则许可证超额的状况结束。 如果活动主持人数仍然超过许可证数，系统每个月会发送一封电子邮件给管理员，指示仍然存在许可证超额的状况。

从版本 2.5 开始，拥有许可证的用户可以继续使用系统，但是没有许可证的用户无法主持会议。 如果未获得许可的用户安排会议时不存在可用的许可证，用户将收到通知，告知他们由于许可证不足无法主持该会议。

在所有版本中，管理站点继续可用，因此管理员可以登录、添加许可证，以及恢复用户主持会议和访问录制文件的功能。

获取许可证

系统试用期间，可以使用控制板查看使用情况、资源历史记录和会议趋势，以确定系统上主持和出席会议的用户数。 使用本产品数月后，可以使用每月摘要报告和自定义详细信息报告帮助确定需要的永久主持人许可证数。每月摘要报告显示服务采用情况和用户许可证使用情况的统计信息。服务采用情况统计信息显示新用户采用系统的比率，它会显示之前三个月的采用率，并预测接下来三个月的增长率。 主持人许可证统计信息显示之前三个月的主持人许可证使用情况和接下来三个月的预期增长。

多数据中心 (MDC) 许可证不存在试用期；必须先获得 MDC 许可证，然后才能创建 MDC 系统。 您必须购买至少两个 MDC 许可证，系统中的每个数据中心一个。 （所有许可证都安装于托管许可证管理器的数据中心。）

通过以下方式获得主持人或 MDC 许可证：

- 使用 eFulfillment（请参阅通过使用 eFulfilment 完成许可证，第 238 页）。
- 使用基于文件的完成（请参阅通过使用许可证管理器完成许可证，第 236 页）。
- 联系 TAC 开设订购许可证案例（请参阅通过联系 TAC 完成许可证，第 239 页）。

有关管理许可证的更多信息，请参阅管理许可证，第 233 页一节（《*Cisco WebEx Meetings Server* 管理指南》）。

许可证管理器连接

购买许可证时，可使用内嵌的许可证管理器工具输入 PAK 并注册许可证。 许可证管理器每 12 小时执行一次同步，更新许可证状态和上次符合时间。 如果未连接到许可证管理器的状态持续了两天，管理员将收到一封电子邮件，通知他许可证管理器无法与系统同步。 系统将提供 180 天的宽限期供您重新连接许可证管理器。

在每个月结束时，管理员都会收到一封新电子邮件，告知系统无法与许可证管理器连接以及系统将被禁用的日期。 如果在六个月宽限期结束前系统重新连接到许可证管理器，则这种状况结束。

如果系统在 180 天之内未重新连接许可证管理器，系统将设置为维护模式并且无法启用，直到该问题得到解决。管理员将收到电子邮件，通知发生这种情况的日期。 系统处于维护模式后，用户将无法在系统上安排、主持或出席会议，也无法访问录制文件。 管理站点正常工作，因此管理员可以登录系统，但系统必须重新连接许可证管理器才能结束这种状况，用户才能恢复安排、主持和参加会议以及访问录制文件的能力。

通过使用许可证管理器完成许可证

通过内嵌的 Cisco Enterprise License Manager 来获得主持人和多数据中心 (MDC) 许可证：

开始之前

要为您的系统定购主持人和多数据中心 (MDC) 许可证，请与您的销售代表联系。 销售代表将向您发送电子邮件，其中包含您的产品授权密钥 (PAK)。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**系统**，然后在**许可证**部分选择**查看更多内容**链接。

步骤 3 选择**管理许可证**
浏览器将打开包含许可证管理器的新标签页或新窗口。（许可证管理器内嵌于 Cisco WebEx Meetings Server；它不是外部网站。）

步骤 4 选择**许可证管理** > **许可证**。

步骤 5 选择**生成许可证请求**。
系统将弹出**许可证请求及后续步骤**对话框。

步骤 6 复制字段中突出显示的文本，然后选择 **Cisco 许可证注册**。

步骤 7 登录 Cisco 帐户并显示**产品许可证注册**。

步骤 8 在**产品授权密钥**字段中输入从 Cisco 销售代表处获得的产品授权密钥 (PAK)，然后选择**下一步**。
系统将显示**完成 PAK** 页面或**为设备分配 SKU** 标签页。

步骤 9 在**分配数量**字段中输入从激活的各个 PAK 中获取的许可证数量。

步骤 10 将您所生成并复制的许可证请求的内容粘贴到**粘贴内容....** 字段中，然后选择**下一步**。
系统将显示**复查**标签页。

步骤 11 请确保联系人电子邮件地址正确。 可在**发送至**字段中更改联系人电子邮件地址。

步骤 12 复查页面并选择**我同意许可证中的条款**。

步骤 13 选择**获取许可证**
系统将弹出**许可证请求状态**对话框。

步骤 14 通过以下方式之一获得许可证文件：

- 选择**下载**以下载许可证文件 (.bin)。
- 从通过电子邮件发送给您的 ZIP 档案中提取许可证文件 (.bin)。

步骤 15 返回到管理站点并选择**系统**，然后在**许可证**部分选择**查看更多内容**链接。

步骤 16 选择**管理许可证**。
浏览器将打开**许可证**窗口。

步骤 17 从“其他完成选项”菜单中选择**从文件完成许可证**。

步骤 18 选择**浏览**，然后选择从电子邮件中的 ZIP 文件下载或提取的许可证文件 (.bin)。

步骤 19 选择**安装**。

将会安装许可证文件。 检查显示的许可证信息，确保其正确。

步骤 20 在完成日期列中选择**当前**。
系统将显示**许可证完成**页面。 验证**已完成许可证**部分中显示的信息正确。

通过使用 eFulfilment 完成许可证

通过在许可证管理器中输入产品授权密钥 (PAK) 来完成许可证订购，而不必使用网站。

开始之前

要为您的系统定购主持人和多数据中心 (MDC) 许可证，请与 Cisco 销售代表联系。 销售代表将向您发送电子邮件，其中包含您的产品授权密钥 (PAK)。

eFulfillment 要求，可以建立系统与 Cisco Systems, Inc. 之间的网络连接。 验证您的系统位于不允许访问的防火墙后。 如果不允许访问，请使用基于文件的实践（请参阅通过使用许可证管理器完成许可证，第 236 页）或联系 TAC 开设订购许可证案例（请参阅通过联系 TAC 完成许可证，第 239 页）。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**系统**，然后在许可证部分选择**查看更多内容**链接。

步骤 3 选择**管理许可证**
浏览器将打开包含许可证管理器（内嵌于 Cisco WebEx Meetings Server）的新标签页或新窗口。（许可证管理器站点不是外部网站。）

步骤 4 选择**从 PAK 完成许可证**。
系统将显示**从 PAK 完成许可证**向导。

步骤 5 在**产品授权密钥**字段中输入从 Cisco 销售代表处获得的 PAK，然后选择**下一步**。
系统将显示**完成 PAK** 页面。

步骤 6 选择**从新的 PAK 添加许可证**。

步骤 7 在 *** PAK 代码**框中输入 PAK 代码并选择**下一步**。

步骤 8 通过使用 cisco.com 用户标识和密码登录。

出现**完成许可证**窗口，其中显示可用的许可证数。

步骤 9 在**操作**列中选择**完成**。

步骤 10 单击**安装**列以编辑值。

步骤 11 输入您想完成的系统许可证数量。 如果 PAK 支持一部分一部分地完成，则输入范围为 1 至 PAK 中剩余的许可证数量。

步骤 12 选择**保存**。

步骤 13 选择**确定**。
系统将弹出**完成许可证**窗口。 **安装**列中的值显示您选定要完成的许可证数。

步骤 14 选择**下一步**。
系统将弹出**查看内容**窗口。 **当前值**列显示活动的许可证数。 **完成后**列显示完成 eFulfillment 后您拥有的许可证的数量。

步骤 15 选择**下一步**。

步骤 16 选择**通过勾选此框，我承认我已阅读、理解并同意遵守最终用户许可协议的条款和条件**。

步骤 17 选择**完成**。
许可证管理器连接到 Cisco 以完成许可证的同时将显示**连接许可证服务器**进度条。 完成 eFulfillment 后，将在**许可证**窗口添加新行。 **完成日期**列显示当前日期，后接**-当前**。 您可以选择此链接来显示许可证的详细信息，包括安装在此系统上的许可证的类型和数量。

通过联系 TAC 完成许可证

开始之前

获取注册标识号。 通过打开“企业许可证管理”工具并选择**关于**可找到注册标识号。

步骤 1 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 2 选择**支持**并通过所列号码呼叫 TAC。

步骤 3 提交案例，并按想要的数目请求主持人和多数据中心 (MDC) 许可证。
我们会处理您的请求并在您的系统上启用额外的许可证。

步骤 4 选择**系统**。

步骤 5 检查“许可证”部分以确认是否已添加许可证。

主持人许可证重新托管

重新托管是指在有限的时间期限内，将正在加入到 MDC 系统或正在升级、扩展或更换的系统上的主持人许可证移到续存系统中。如果许可证未进行重新托管，那么无法将其升级。例如，当系统从版本 1.5MR3 升级至版本 2.0 时，在必须将原先在 1.5MR3 系统上托管的主持人许可证更换为对 2.0 版本有效的许可证之前，可以在 2.0 系统上将它们重新托管 180 天。 如果运行于 2.0 版系统的 1.5 版主持人许可证在 180 天之内未更换，系统将关闭，直到许可证问题得到解决。 （唯一允许的任务就是在系统中添加主持人许可证。 请参阅执行重大系统修改之后重新托管许可证，第 240 页。）

如果原始系统在无许可证的情况下运行并且处于试用许可期之内，那么免主持人许可证的剩余天数将转到修改后的系统中。

访问 GLO 申请表

要显示全球许可运营 (GLO) 申请表，请在产品许可注册页面选择**联系我们**，该页面网址是：https://tools.cisco.com/SWIFT/LicensingUI/Quickstart。 在 GLO 支持联系信息页面上选择**申请**。

开始之前

准备提供以下信息：

- 联系信息
- 问题描述
- 产品名称和许可活动（例如重新发送许可证信息或升级许可证）
- 授权信息（例如产品序列号）

执行重大系统修改之后重新托管许可证

采取措施（例如升级或扩展）修改系统并完成测试之后，下一步就是重新托管许可证。

如果您有多数据中心 (MDC) 系统，并且系统已扩展，您必须购买更大的 MDC 许可证。 如果系统已升级，您有 90 天时间来升级 MDC 许可证。 重新托管的许可证在原始系统上自动失效。 开始重新托管之前，保留原始系统的许可证请求，以备由于修改该系统时出现错误，需要用它在原始系统上重新托管许可证。

重新托管许可证时，可以重新托管的许可证数上限为原始系统上的许可证数。 重新托管许可证的首选方式是通过产品许可证注册门户。

如果原始系统有主持人许可证，则在要求提供升级的主持人许可证之前，修改后的系统将给您 180 天的宽限期，您可以利用这段时间对升级系统进行测试，然后在升级系统上重新托管原始许可证。重新托管许可证之后，试用期结束。 重新托管可以通过使用产品许可证注册门户 (http://tools.cisco.com/SWIFT/LicensingUI/Home) 来完成。 （请参阅访问 GLO 申请表，第 240 页。）

生成许可证请求

要获取原始系统的许可证请求，请执行以下操作：

步骤 1 从原始系统管理窗口中选择**系统**。

步骤 2 选择（**许可证**）**查看更多内容** > **管理许可证**。

步骤 3 选择**其他完成选项** > **生成许可证请求**。

步骤 4 复制内容并将许可证请求保存到 PC 上的文件中。

接下来的操作

注册许可证。 有关说明，请参阅注册要重新托管的许可证 ， 第 241 页。

注册要重新托管的许可证

要使用产品许可证注册门户，请登录 https://tools.cisco.com/SWIFT/LicensingUI/Quickstart。 发送含有已重新托管的许可证的电子邮件。 请注意，如果您要在软件升级时进行重新托管，则必须在升级系统上重新托管（请参阅执行重大系统修改之后重新托管许可证，第240页）并升级旧版本的许可证。 类似于**您使用的许可证文件对当前部署无效**的错误消息可能会显示在升级系统的管理站点上。 这是预料之中的。 消息中包含到期日期，指示如果您在此日期之前不升级主持人许可证，那么您的系统将在这一天被关闭。 在此日期之后您唯一可以执行的任务是安装许可证。

接下来的操作

在重新托管许可证之后，请在显示日期之前完成许可证升级，从而确保能够不间断地使用系统。 请参阅通过使用许可证管理器完成许可证 ， 第 236 页以获取更多信息。

软件修改之后升级许可证

软件修改之后，在升级系统上重新托管原始系统的已安装许可证。 （有关更多信息，请参阅执行重大系统修改之后重新托管许可证 ， 第 240 页。） 重新托管许可证之后，可对其进行升级以供升级系统使用。

用户与许可证的关联会被删除。 用户首次主持会议时会与许可证关联。

要使用 eFulfilment 升级已安装的许可证，请执行以下操作：

1. 从供应商处获取产品授权密钥 (PAK) 代码。
2. 从**系统**窗口中，选择（**许可证**）**查看更多**>**管理许可证**>**许可证**>**从 PAK 履行许可证**。 系统将弹出**从 PAK 履行许可证**窗口。
3. 输入 PAK 代码并选择**下一步**。
4. 使用 cisco.com 帐户凭证登录。 系统将弹出**从 PAK 完成许可证**窗口。
5. 单击安装栏以选择要安装的许可证数。

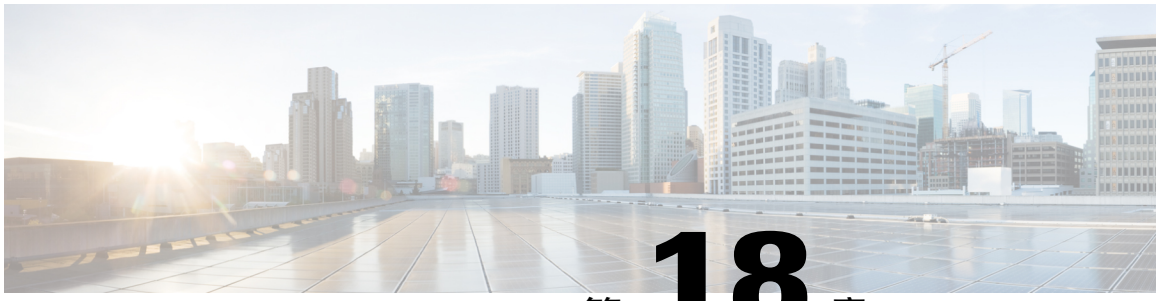
6 指定要安装的许可证数并选择**保存**。 通过 PAK 将作为 eFulfillment 一部分的许可证安装在系统上。

注释 可安装的许可证数受升级 PAK 中可用许可证数的限制，并且不能超过原始系统中已重新托管的许可证数。

要从许可证文件升级已安装的许可证版本：

1 从供应商处获取许可证文件 **(cisco.com/go/license)**。
2 从**系统**窗口中，选择（**许可证**）**查看更多**>**管理许可证**>**许可证**>**从文件履行许可证**。 系统将弹出**安装许可证文件**窗口。
3 浏览许可证文件。 文件显示在**许可证**窗口上。

许可证会被更新。



第 18 章

加入数据中心以创建多数据中心 (MDC) 系统

- 加入数据中心以创建多数据中心 (MDC) 系统，第 243 页

加入数据中心以创建多数据中心 (MDC) 系统

关于多数据中心

版本 2.5 及更高版本提供多数据中心 (MDC) 许可功能。 版本 2.5 允许两个 CWMS 系统加入单个 MDC 系统。 在 MDC 系统中，每个 CWMS 数据中心必须购买一个许可证。 尝试部署 MDC 之前，应购买 MDC 许可证。 具有单数据中心的系统不需要功能许可证。 有关 MDC 许可证的进一步说明，请参阅关于 MDC 许可证，第 233 页。

多数据中心系统的优势包括：

- 最终用户可通过使用一个 URL 和一组电话号码访问所有的数据中心；MDC 的存在性对最终用户而言是透明的。
- 主持人许可证、录制文件，以及相关的管理数据可在加入的数据中心之间自由迁移。
- 用户可以拨入会议，没有地理上的限制；通过拨打本地电话号码可出席会议。
- 数据中心可以（可选地）位于不同的地理区域。
- 当数据中心可以运行于不同的 CWMS 2.5 更新版本时，在一些计划的维护活动中实现零停机。请参阅发行说明 (http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-release-notes-list.html)，以确定哪些 CWMS 版本可以同时运行。

  有时 MDC 系统中的数据中心可以运行于不同的更新版本中。 请参阅发行说明 (http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-release-notes-list.html)，以确定哪些 CWMS 版本可以同时运行。
- 灾难恢复环境对用户而言是透明的。 如果一个数据中心出于任何原因发生故障，其他数据中心可以支持用户。

尽管在 MDC 环境中，数据中心全部运行 CWMS 并且被视为对等的，出于将数据中心加入系统的目的，数据中心之间的关系被视为主和备用。加入之前，主数据中心支持要保留的系统。备用数据中心成为 MDC 系统的一部分。如果您加入已在为用户提供有效支持的数据中心，区别尤为明显。

注释 数据中心添加到 MDC 系统中后，容量不会增加。如果一个拥有 2000 个端口的数据中心添加到由一个拥有 2000 个端口的数据中心支持的 MDC 系统中，最终系统为一个拥有 2000 个端口的 MDC。

要将一个没有用户数据的新建备用 CWMS 系统数据中心加入到 MDC 系统中，请参阅准备 MDC 系统来接收数据中心加入请求，第 246 页。

要将一个包含用户数据的活动备用 CWMS 系统数据中心加入到 MDC 系统中，请参阅准备将活动 CWMS 数据中心加入 MDC 系统中，第 244 页。

准备将活动 CWMS 数据中心加入 MDC 系统中

当您加入已为用户提供服务的备用CWMS 系统数据中心时，它已获取或配置用户数据，这些数据在它加入到多数据中心 (MDC) 时可能会丢失。在单数据中心环境中，有一个 CWMS 数据中心为用户社区提供服务。需要 MDC 系统时，一般会先创建新的 CWMS 数据中心，然后将其加入到 MDC 系统中，接着将该数据中心投入使用，因此，不需要为加入期间的备用数据中心保留用户信息、许可证或者配置信息。但是，如果要加入两个活动的数据中心，用户内容会被覆盖或不可访问：

- 所有全局数据都会被覆盖。（数据中心本地的配置参数会被保留。）
- 备用数据中心上的用户信息、安排的会议、报告，以及相关电子邮件会被删除。
- 会议录制文件对用户不可访问。录制文件在 NAS 上保留完好，但是它们无法由用户访问或恢复。（请参阅在加入 MDC 系统之前保留录制文件，第 245 页。）
- 主持人许可证丢失，但是托管在备用数据中心的永久主持人许可证可通过将其重新托管到MDC 系统中进行恢复。（如果主数据中心从系统中删除，那么必须在另一个数据中心上重新托管许可证。

  如果主数据中心出于任意原因脱机，必须先将其恢复联机，然后才能修改主持人许可证。如果管理数据中心无法恢复，那么续存数据中心进入 180 天的宽限模式。要进行恢复，必须在宽限期结束之前重新托管永久主持人许可证。（请参阅主持人许可证重新托管，第 240 页。）如果在宽限期结束之前未重新托管许可证，系统将转入维护模式，直到重新托管许可证。
- 加入数据中心时，活动备用数据中心上的用户至主持人的许可证关联丢失。如果用户在活动备用数据中心上为主持人，那么只需在加入的系统上主持会议就可以恢复他们的许可证，或者管理员可以从管理许可证的数据中心手动分配主持人许可证。

备用数据中心上的以下信息在加入之后保留：

- 系统特定的配置，例如 Cisco Unified Call Manager (CUCM)。
- 语言设置，例如 IVR 语言设置
- 音频设置

- 群拨信息

加入之前保留备用数据中心上的 CWMS 数据

要加入到 MDC 系统的备用数据中心上的 CWMS 数据将被覆盖或变得不可访问。 如果要加入未投入使用的 CWMS 数据中心，则不需要保留数据，请参阅准备 MDC 系统来接收数据中心加入请求，第 246 页。 否则，请考虑保留重要数据。

当备用数据中心加入 MDC 系统时，该数据中心将丢失：

- 用户-主持人许可证关联
- 主持人许可证（可以通过将许可证重新托管到 MDC 系统来恢复它们执行重大系统修改之后重新托管许可证，第 240 页）
- 安排的会议（必须在 MDC 系统中手动重新安排）
- 会议录制文件，可以通过以下方式保留：

  要求用户下载和本地保留录制文件。

  由系统管理员归档供检索。

  以上两种方式。（推荐）

会议录制文件“驻留”于 NFS，因此它们不会丢失；CWMS 的用户不可以访问它们。

在加入 *MDC* 系统之前保留录制文件

在 `NFS:/nbr` 目录的下面是 `Recording`、`nfskeepalive` 和 `Snapshot` 目录。 要存档文件，请将 `NFS1:/nbr/1/*` 复制到 `NFS2:/nbr/1`。

注释 以下步骤仅作为示例。 具体到您的系统可能会有所不同。

对于以下步骤示例，我们假定 NFS 位于 DC1 上，名为 `sanjose-nfs:/cisco/cwms`，而 DC2 上的 NFS 则命名为 `rtp-nfs:/cisco/cwms`。

开始之前

- 以 NFS 的根访问权限访问 Linux 机器。（任何版本均可，如 Redhat、CentOS 等等。）

• 如果 NFS 有基于 IP 的过滤功能或对安装有访问控制，则将 Linux 主机 IP 添加到访问列表中。

步骤 1 cd/tmp

步骤 2 新建 DC1 NFS 临时安装目录：`mkdir nfs-dc1`。

步骤 3 新建 DC2 NFS 临时安装目录：`mkdir nfs-dc2`。

步骤 4 将 DC1 NFS 安装至 `/tmp/nfs-dc1`：`mount -t nfs -o vers=3,rw,soft,timeo=400 sanjose-nfs:/cisco/cwms/tmp/nfs-dc1/`

步骤 5 将 DC2 NFS 安装至 `/tmp/nfs-dc2`：`mount -t nfs -o vers=3,rw,soft,timeo=400 rtp-nfs:/cisco/cwms/tmp/nfs-dc2/`。

步骤 6 同步录制文件：`rsync -av --exclude='*Snapshot*/' nfs-dc1/ nfs-dc2`。

步骤 7 卸载 DC1 NFS：`umount nfs-dc1`。

步骤 8 卸载 DC2 NFS：`umount nfs-dc2`。

步骤 9 删除 DC1 NFS 临时安装目录：`rm -r nfs-dc1`。

步骤 10 删除 DC2 NFS 临时安装目录：`rm -r nfs-dc2`。

准备 MDC 系统来接收数据中心加入请求

可以加入数据中心并作为一个系统来管理。 此过程描述如何准备主数据中心（已向系统提供服务）以接收备用数据中心的加入请求：

开始之前

下面是为确保将数据中心成功加入系统，系统管理员必须完成的任务列表。

1. 验证所有数据中心都运行相同的 CWMS 软件版本。
2. 验证所有数据中心都运行相同类型的软件。 例如，验证所有数据中心均为音频加密 -AE 或音频非加密 -AU。
3. 验证所有数据中心的系统容量均相同。
4. 所有数据中心都必须设置网络时间协议 (NTP)，且所有数据中心的 NTP 时间必须相同。
5. 所有虚拟机主机都必须配置 NTP 服务器。
6. 虚拟机主机必须能访问 NTP 服务器。 （如果 DNS 或防火墙未通过 NTP，或者未正确配置 NTP 服务器，就可能会出现错误。）
7. 在运行许可证管理器的主数据中心上安装多数据中心 (MDC) 许可证（至少两个）。
8. 所有数据中心要同步启用或禁用互联网反向代理 (IRP)。 务必要遵守此规则，但在加入后可以从数据中心增删 IRP。
9. 没有任何数据中心运行高可用性 (HA) 系统。（请参阅从系统中删除高可用性系统，第 59 页。）
10. 验证两个数据中心均已配置存储空间，或者两者均未配置存储空间。 如果配置了存储空间，数据中心应使用不同服务器上的存储空间（至少应位于不同的文件夹上）。
11. 验证所有数据中心均使用相同的验证模式。 验证模式可以是 LDAP、SSO 或缺省模式。

12 验证 DNS 已输入所有本地 URL、所有公共 URL 及所有主机名。 执行加入操作时，管理公共 URL 只能与一个 IP 地址关联。 执行加入操作时，WebEx 公共 URL 只能与一个 IP 地址关联。 在数据中心加入系统后，公共 URL 应返回两个 IP 地址。

13 验证两个数据中心的 CUCM 使用相同的传输协议。 传输协议可以是 TCP、UDP 或 TLS。

步骤 1 通知辅助系统上的用户有加入请求。 如果备用数据中心还不是任何活动系统的一部分，请跳过此步骤。 如果此数据中心支持活动的系统，请参阅准备将活动 CWMS 数据中心加入 MDC 系统中，第 244 页。
加入的结果，便是用户数据、预约会议以及对备用数据中心上会议录制文件的访问权丢失。 从备用数据中心发送加入请求前，建议您向用户发送通知，提示他们要想保留任何会议录制文件，应将其下载到本地 PC 上。

步骤 2 选择**数据中心** > **添加数据中心** > **准备加入系统**

步骤 3 请输入：

- 本地站点 URL - 允许用户安排、出席或主持会议的用户站点 URL。
- 公共管理 URL - 此系统管理 URL 将解析到系统的专用 VIP 地址。
- 远程管理电子邮件 - 接收系统发出的信息和警告的目标电子邮件地址。
- 本地数据中心名称 - 标识本地系统上的备用数据中心。

步骤 4 下载用于加入系统的证书。
加入前，必须将主数据中心的证书上传到备用数据中心。 证书由系统修改，因此最好不要试图通过重用旧证书的方式来实现加入。

注释 使用 Safari 时，下载的证书另存为 `CAcert.pem.txt`。 这是 Safari 浏览器的缺省行为。 要还原 `.pem` 扩展名（在上传证书前），请删除 `.txt` 字符串。

步骤 5 选择**完成**。

步骤 6 登录备用数据中心并从该数据中心发送加入请求。 有关说明，请参阅将数据中心加入 MDC 系统，第 247 页。

将数据中心加入 MDC 系统

加入请求从备用数据中心发送到主数据中心（即支持 CWMS 多数据中心 (MDC) 系统，且在加入后保留其数据以及对会议录制文件访问权的数据中心）。 MDC 功能许可证和永久主持人许可证通常在主数据中心上进行托管和管理。 MDC 系统没有试用期；必须在加入之前在主数据中心上加载 MDC 许可证。 如果主数据中心上没有可用的 MDC 许可证，备用数据中心将无法加入系统。

注释 加入数据中心时，将更新主数据中心证书。 新的证书为自签名证书，它将自动予以重新生成，以便从备用数据中心领取新的 URL。 当您访问主数据中心或 MDC 管理站点时，这将导致浏览器中显示证书警告。 请接受警告并按照标准流程来更新系统证书。 （请参阅管理证书，第 205 页。）

注释 加入非英语的数据中心时，在加入过程中，**始终**会有一段时间，任务列表是以英文显示的。 加入过程中，还可能会出现多语言混杂的错误消息。（页面中的其余文本以原始语言显示。）

启动**数据库表同步**任务时，预期的任务列表语言行为是：

- 如果管理员帐户托管在采用相同语言设置的主数据中心和备用数据中心上，则在**数据库表同步**任务期间，任务列表将以英文显示。完成表同步后，任务名称将恢复为管理员的语言。
- 如果管理员帐户托管在加入后将保持不变的主数据中心上，而在加入系统的备用数据中心上还有另一个管理员帐户被设置为与主数据中心管理员帐户使用不同的语言，则在数据库表同步时，任务列表将以英文显示。 完成同步后，任务列表将切换为主数据中心管理员的语言。
- 如果管理员帐户唯一托管在加入系统的备用数据中心上，且在加入后将保持不变的主数据中心上管理员没有相应的帐户，则在数据库表同步时，任务列表将以英文显示。 一旦系统完成同步，语言便不再改变，也不会出现**完成**按钮。 要继续操作，管理员必须先关闭当前浏览器窗口并使用备用数据中心的本地管理 URL 打开一个新窗口，之后使用主数据中心上的管理员帐户登录，然后选择**数据中心** > **添加数据中心**，并验证状态。

开始之前

网络时间协议 (NTP) 必须配置如下：

- 所有数据中心都必须设置 NTP，且所有数据中心的 NTP 时间必须相同。
- 所有虚拟机主机都必须配置 NTP 服务器。
- 虚拟机主机必须能访问 NTP 服务器。（如果 DNS 或防火墙未通过 NTP，或者未正确配置 NTP 服务器，就可能会出现错误。）

如果此数据中心支持活动的系统，就会删除此数据中心上支持的主持人许可证。 这些主持人许可证可在托管许可证管理器的数据中心上进行重新托管。（请参阅主持人许可证重新托管，第240页。）建议您在开始加入之前先保存此数据中心的许可证请求，以防以后需要 TAC 来帮助您查找许可证。

步骤 1 要发送一个从备用数据中心加入 MDC 系统的请求，请选择**数据中心** > **添加数据中心** > **加入系统**。

步骤 2 请输入：

- **远程系统证书** - 匹配主数据中心证书的证书。

  注释 使用 Safari 时，下载的证书另存为 `CAcert.pem.txt`。 这是 Safari 浏览器的缺省行为。 要还原 `.pem` 扩展名（在上传证书前），请删除 `.txt` 字符串。

- **远程公共管理 URL** - 此系统管理 URL 将解析到辅助系统的专用 VIP 地址。
- **远程管理电子邮件** - 接收系统发出的信息和警告的目标电子邮件地址。
- **远程管理员密码** - 供管理员访问辅助系统的密码。

- **本地数据中心名称** - 用于标识本地系统上的备用数据中心的字符串。

步骤 3 选择**继续**。

系统将显示“加入数据中心”任务列表。

注释 在**数据库表同步**任务过程中，将删除备用数据中心中的所有用户，而主数据中心上所列的用户则被复制到备用数据中心。 系统无法获得管理员的语言（因为 DC2 中没有用户），界面缺省以英文显示。

如果备用数据中心的管理员也同样存在于主数据中心上，则在管理员登入备用数据中心后，系统将显示管理员的语言（除非主数据中心上为管理员配置的语言与备用数据中心上配置的语言不同）。

如果备用数据中心的管理员也同样存在于主数据中心上（或存在数据库同步错误），则系统将以英文显示。

步骤 4 令 MDC 系统中的所有数据中心退出维护模式。

接下来的操作

向 DNS 服务器添加指针

- **公共站点 URL** - 每个数据中心的公共 VIP 地址。
- **公共管理 URL** - 两个数据中心的专用 VIP 地址。
- **本地站点 URL**（归属某个数据中心）- 此数据中心的公共 VIP 地址。
- **本地站点 URL**（归属另一个数据中心）- 此数据中心的公共 VIP 地址。
- **本地管理 URL**（归属某个数据中心）- 此数据中心的专用 VIP 地址。
- **本地管理 URL**（归属另一个数据中心）- 此数据中心的专用 VIP 地址。

修改音频访问码和服务语言

在主数据中心上配置的音频访问码和服务语言将被配置为全局访问码和服务语言，替换原来的访问码和服务语言配置。如有必要，请转至全局配置并适当调整访问码和服务语言。（请参阅配置音频设置，第 159 页。）

多数据中心环境中的灾难恢复

在多数据中心 (MDC) 环境中，如果一个数据中心由于硬件或数据中心错误发生故障，我们建议通过创建新数据中心并将该数据中心加入到系统中更换数据中心。（另请参阅通过使用存储服务器进行灾难恢复，第 139 页）。

步骤 1 登录续存数据中心的管理站点。

步骤 2 从系统中删除故障数据中心。

（请参阅删除数据中心，第 250 页。）

步骤 3 新建数据中心以更换故障数据中心。
更换数据中心的版本应与续存数据中心的版本匹配。

步骤 4 完成本地配置，例如 CUCM、SNMP 等，匹配故障数据中心。

步骤 5 准备系统中的续存数据中心，以接收“加入”请求。
（请参阅准备 MDC 系统来接收数据中心加入请求，第 246 页。）

步骤 6 将新数据中心加入系统中。
（请参阅将数据中心加入 MDC 系统，第 247 页。）

续存数据中心中的数据被复制到新数据中心中。

步骤 7 用新的 URL 和 IP 地址信息更新 DNS。

删除数据中心

从多数据中心 (MDC) 系统中删除数据中心时，将删除所有 CWMS 设置。 应用于所删除的数据中心的参数也将从续存数据中心中予以删除。

注释 在多数据中心（MDC)环境中，许可证管理器只能在一个数据中心上运行，而不能在多个数据中心上运行。 如果删除了托管许可证管理器的数据中心，那么您将有 90 天的时间在另一个数据中心上配置许可证管理器并重新托管许可证。（请参阅注册要重新托管的许可证，第 241 页。）

开始之前

制作要删除的系统和数据中心的备份。

删除所有 DNS 和 Communications Manager 条目。

步骤 1 关闭所要删除的数据中心的虚拟机。

步骤 2 登录管理站点。
在多数据中心系统中，DNS 确定显示哪个数据中心控制板。 所有数据中心都可以从此控制板进行管理。

步骤 3 选择**数据中心**.
系统将弹出**数据中心**窗口。

步骤 4 （可选） 验证数据中心无法访问。
您可以手动进行验证，也可以立即着手删除数据中心的过程，并让 CWMS 检查其可用性。 如果可以 Ping 到数据中心，删除过程将无法继续并显示错误消息。

步骤 5 要发送一个从 MDC 系统中删除数据中心的请求，请选择**删除**（**操作**）列。
如果所删除的数据中心在托管许可证管理器，则系统将显示警告。 此外，还会警告需要进行 DNS 更改。

主数据中心将进入维护模式，同时出现**删除数据中心**窗口，显示操作进度。

步骤 6 选择**继续**

步骤 7 当所有任务均为绿色时，选择**完成**.
数据中心将被删除，您将返回**数据中心**窗口。

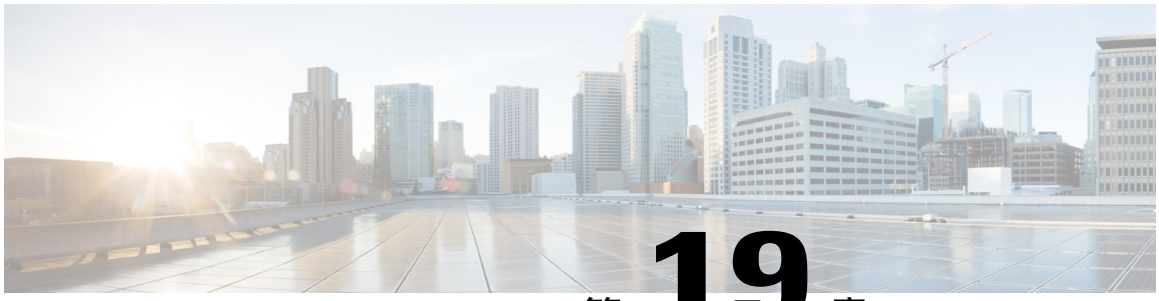
步骤 8 验证数据中心已被删除。
用于系统访问的 URL 发生改变，系统将只保留全球 URL。

步骤 9 删除已删除的数据中心的所有 DNS 条目，并将续存数据中心的公共和专用虚拟 IP 地址映射至全球 URL。

步骤 10 关闭维护模式。 请参阅开启或关闭 2.5 版及更高版本的维护模式。
当您关闭维护模式时，系统会确定是需要重新启动（约需 3 - 5 分钟）还是重新引导（约需 30 分钟），并显示相应消息。 如果此数据中心属于多数据中心 (MDC) 系统，那么管理员会被重定向至全局管理 URL。 管理员所看到的数据中心由 DNS 解析策略确定。 如果启用密钥再生，让一个数据中心退出维护模式会自动让系统中的所有数据中心退出维护模式。

此数据中心上用户的会议服务将被还原。

步骤 11 （可选） 如果删除了托管许可证管理器的数据中心，请在续存数据中心上重新托管许可证管理器及许可证。



第 19 章

使用支持功能

- 自定义日志，第 253 页
- 设置 Remote Support 帐户，第 254 页
- 禁用 Remote Support 帐户，第 255 页

自定义日志

您可以生成显示整个系统上的活动或特定会议活动的日志文件。 使用日志文件来排除问题，或者当您需要帮助时将日志文件提交到 Cisco 技术支持中心 (TAC)。

注释 我们建议您在非工作时间生成日志文件。 日志文件的容量较大，会影响系统性能。

注释 日志数据会保留 40 天。 但是，如果将 Cisco WebEx Meetings Server 2.0 部署升级到发行版 2.5，则发行版 2.0 中的日志数据不会转移到 Cisco WebEx Meetings Server 2.5 系统，因此在升级到发行版 2.5 的过程完成后将不可用。

步骤 1 登录管理站点。

步骤 2 选择**支持** > **日志**。

步骤 3 将**自定义日志**页面上的字段填写完整，然后选择**提交**。

字段	描述
（可选）案例标识	输入 Cisco TAC 案例标识。 案例标识可从协助您解决案例的 Cisco TAC 处获得。 使用此功能可以将生成的日志与案例标识相关联。

字段	描述
类型	选择日志类型。您可以选择**整体系统日志**或**特定会议日志**。整体系统日志包含系统的所有指定日志信息，特定会议日志从数据库收集日志和数据以进行 MATS 处理。 **缺省：** 系统综合日志
范围	选择日志范围。必须指定日志的开始和结束日期以及时间。限定为 24 小时。日志数据只包含过去 40 天的数据。 **注释** 要生成超过 24 小时的日志，必须重复该操作并选择连续的日期范围。每次操作都会生成独立的日志文件。例如：要生成 1 月 1 日至 1 月 3 日的日志，请先选择 1 月 1 日至 1 月 2 日的日期范围，然后选择**提交**并下载创建的日志文件。接着选择 1 月 2 日至 3 日作为日期范围。选择**提交**并下载创建的日志文件。
包含	指定想要包括在日志中的数据。 **缺省：** 所有活动

将生成日志，并向您发送电子邮件，其中包含可下载日志的链接。

设置 Remote Support 帐户

如果您有技术问题并联系 Cisco TAC 寻求协助，则可以设置 Remote Support 帐户以授权 TAC 代表临时访问您的系统。本产品不向管理员提供 CLT 访问，因此需要 TAC 代表来对某些问题进行诊断。

步骤 1 登录管理站点。

步骤 2 选择**支持** > **Remote Support 帐户**。

步骤 3 选择**启用 Remote Support**。

步骤 4 填写**Remote Support 帐户**页上的字段，然后选择**创建帐户**。

字段	描述
Remote Support 帐户名称	输入 Remote Support 帐户的名称（6 – 30 个字符）。

字段	描述
帐户有效期	指定帐户的持续时间（小时）。 时间最长为 720 小时（30 天）。
解码器版本	选择 **2- Webex Meetings Server**。 **注释** 如果您有在 Cisco WebEx Meetings Server 版本 1.5 发行前活动的 Remote Support 帐户，则不必配置此设置。

系统将弹出**创建 Remote Support 帐户**对话框，并显示您的密码。 请联系 Cisco TAC，并提供 Remote Support 帐户名称和密码，以便 Cisco 支持人员访问您的系统。

禁用 Remote Support 帐户

步骤 1 登录管理站点。

步骤 2 选择**支持** > **Remote Support 帐户**。

步骤 3 在状态消息“Remote Support 已启用”旁边，选择**禁用它**链接。
将禁用您的 Remote Support 帐户。