



Cisco Unified Communications Manager 版本 14 和 SU 系统配置指南

首次发布日期: 2022 年 6 月 16 日

上次修改日期: 2023 年 5 月 18 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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 – 2023 Cisco Systems, Inc. 保留所有权利。



目 录

Full Cisco Trademarks with Software License ?

第 1 章	新增和变更内容 1
	新增和变更内容 1
第 2 章	简介 3
	系统配置概述 3
第 I 部分：	系统组件 5
第 3 章	智能软件许可 7
	智能软件许可概述 7
	许可证类型 9
	产品实例评估模式 9
	系统许可前提条件 10
	智能软件许可任务流程 10
	获取产品实例注册令牌 11
	配置与智能软件许可的连接 11
	向 Cisco Smart Software Manager 注册 12
	采用智能软件许可的附加任务 13
	续订授权 14
	续订注册 15
	注销 15
	重新向 Cisco Smart Software Manager 注册许可证 17

特定许可证预留	17
特定许可证预留任务流程	20
license smart reservation enable	20
license smart reservation request	20
license smart reservation install "<authorization-code>"	22
license smart reservation install-file<url>	22
特定许可证预留的其他任务	23
license smart reservation disable	23
update license reservation	23
license smart reservation cancel	26
license smart reservation return	26
license smart reservation return-authorization "<authorization-code>"	28
将已启用许可证预留的特定系统升级到版本 14	29
不受版本限制的许可证	30
智能许可导出合规	30
导出控制任务流程	30
license smart export request local <exportfeaturename>	30
license smart export return local <exportfeaturename>	31
license smart export cancel	31

第 4 章

配置企业参数和服务	33
企业参数概述	33
服务参数概述	33
系统参数任务流程	34
配置企业参数	34
通用企业参数	35
激活基本服务	39
针对发布方节点的建议服务	40
针对订阅方节点的建议服务	41
配置服务参数	42
查看群集范围的服务参数设置	42

第 5 章

配置 IPv6 堆栈 45

IPv6 堆栈概述 45

IPv6 前提条件 46

IPv6 配置任务流程 46

在操作系统中配置 IPv6 47

为 IPv6 配置服务器 47

启用 IPv6 48

配置群集的 IP 寻址首选项 48

配置设备的 IP 寻址首选项 49

重新启动服务 49

第 6 章

配置双堆栈（IPv4 和 IPv6） 51

双堆栈（IPv4 和 IPv6）概述 51

双堆栈（IPv4 和 IPv6）前提条件 51

双堆栈（IPv4 和 IPv6）配置任务流程 51

为 SIP 配置文件配置 ANAT 52

将 ANAT 应用于 SIP 电话 52

将 ANAT 应用到 SIP 干线 53

重新启动服务 53

第 7 章

配置基本的安全性 55

关于安全配置 55

安全配置任务 55

为群集启用混合模式 55

下载证书 56

生成证书签名请求 56

下载证书签名请求 56

上传第三方 CA 的根证书 57

TLS 前提条件 57

设置最低 TLS 版本 58

设置 TLS 密码 58

第 8 章

配置单点登录 61

关于 SAML SSO 解决方案 61

SAML SSO 配置任务流程 62

从 Cisco Unified Communications Manager 导出 UC 元数据 63

在 Cisco Unified Communications Manager 中启用 SAML SSO 63

重新启动 Cisco Tomcat 服务 65

验证 SAML SSO 配置 66

第 9 章

配置设备池的核心设置 67

设备池概述 67

网络时间协议概述 67

区域概述 68

Cisco Unified CM 组概述 70

呼叫处理冗余 70

分布式呼叫处理 71

设备池前提条件 74

设备池的核心设置配置任务流程 74

配置网络时间协议 75

添加 NTP 服务器 76

通过对称密钥配置 NTP 验证 76

通过自动密钥配置 NTP 验证 77

配置电话 NTP 首选项 77

添加日期/时间组 78

配置区域 79

自定义音频编解码器首选项 79

配置群集范围内的区域默认设置 80

配置区域关系 80

配置 Cisco Unified CM 组 81

配置设备池 82

基本设备池配置字段 83

呼叫保留 83

呼叫保留情景 84

第 10 章

配置干线 87

SIP 干线概述 87

SIP 干线前提条件 87

SIP 干线配置任务流程 88

配置 SIP 配置文件 88

配置 SIP 干线安全性配置文件 89

配置 SIP 干线 89

SIP 干线相互作用和限制 90

H.323 干线概述 91

H.323 干线前提条件 92

配置 H.323 干线 92

第 11 章

配置网关 93

网关概述 93

网关设置前提条件 94

网关配置任务流程 94

配置 MGCP 网关 95

配置 MGCP (IOS) 网关 96

配置网关端口接口 96

配置数字接入 PRI 端口 96

配置 MGCP 网关的数字接入 T1 端口 97

配置 FXS 端口 98

配置 FXO 端口 99

配置 BRI 端口 99

为 MGCP 网关添加数字接入 T1 端口 100

重置网关 101

MGCP 主叫方 ID 限制 101

配置 SCCP 网关	102
将 SCCP 配置为网关协议	102
为模拟电话启用自动注册	103
为未配置的模拟 FXS 端口启用自动注册	104
故障诊断提示	104
配置 SIP 网关	105
配置 SIP 配置文件	105
配置 SIP 干线安全性配置文件。	106
配置 SIP 网关的 SIP 干线	106
配置 H.323 网关	106
为网关配置群集范围的呼叫分类	107
阻止网外网关转移	108

第 12 章

配置 SRST	109
Survivable Remote Site Telephony 概述	109
Survivable Remote Site Telephony 配置任务流程	110
配置 SRST 参考	110
分配 SRST 参考给设备池	111
配置群集的连接监控持续时间	111
配置设备池的连接监控持续时间	112
在 SRST 网关上启用 SRST	112
SRST 限制	113

第 13 章

配置媒体资源	115
关于媒体资源	115
媒体终结点	115
SRTP DTMF 交互工作	117
媒体终结点相互作用和限制	118
转码器	118
Opus 编解码器转码器支持	119
具备 MTP 功能的转码器	119

转码器类型	120
转码器相互作用和限制	122
信任的中继点概述	123
信任的中继点相互作用和限制	124
TRP 资源不足的呼叫行为	125
报警器概述	126
默认报警器通知和提示音	126
交互式语音应答概述	128
默认 IVR 通知和提示音	128
交互式语音应答限制	129
通知概述	129
默认通知	129
媒体资源配置任务流程	130
激活软件媒体资源	131
配置媒体终结点	131
配置转码器	132
配置交互式语音应答 (IVR)	133
配置报警器	133
配置媒体资源组	133
配置媒体资源组列表	134
将媒体资源分配给设备或设备池	134
配置通知	135
上传自定义通知	135

第 14 章

配置会议桥	137
会议桥概述	137
会议桥类型	137
会议桥配置任务流程	142
配置会议桥	142
为会议桥配置服务参数	143
配置到会议桥的 SIP 干线连接	143

第 15 章

配置增强位置通话准入控制	145
增强位置通话准入控制概述	145
群集间 LBM 复制	146
增强位置 CAC 前提条件	147
增强位置 CAC 任务流程	147
激活位置带宽管理器	148
配置 LBM 组	148
配置位置和链路	149
配置 LBM 群集间复制组	149
配置 SIP 群集间干线	150
配置通话准入控制服务参数	150
增强位置 CAC 相互作用限制	151

第 16 章

配置资源预留协议	153
RSVP 通话准入控制概述	153
RSVP 通话准入控制前提条件	153
RSVP 配置任务流程	153
配置群集范围的默认 RSVP 策略	154
配置位置对 RSVP 策略	155
配置 RSVP 重试	155
配置呼叫中 RSVP 错误处理	156
配置 MLPP 到 RSVP 优先级映射	157
配置应用程序 ID	158
配置 DSCP 标记	158

第 17 章

配置推送通知	161
推送通知概述	161
推送通知配置	165

第 II 部分：

拨号方案	167
-------------	------------

第 18 章

配置分区 169

- 分区概述 169
- 呼叫搜索空间概述 169
- 服务级别 170
- 分区配置任务流程 171
 - 配置分区 171
 - 分区名称指导原则 172
 - 配置呼叫搜索空间 172
- 分区相互作用和限制 173

第 19 章

安装国家编号方案 175

- 国家编号方案概述 175
- 国家编号方案前提条件 175
- 国家编号方案安装任务流程 176
 - 安装 COP 文件 176
 - COP 文件安装字段 177
 - 安装国家编号方案 177
 - 重新启动 CallManager 服务 177

第 20 章

配置呼叫路由 179

- 呼叫路由概述 179
- 呼叫路由前提条件 180
- 呼叫路由配置任务流程 181
 - 配置转换模式 181
 - 配置主叫方转换模式 182
 - 配置被叫方转换模式 183
 - 配置本地路由组 183
 - 配置本地路由组名称 184
 - 将本地路由组关联到设备池 184
 - 将本地路由组添加到路由列表 184

配置路由组	185
配置路由列表	185
配置路由过滤器	186
路由过滤器设置	187
配置路由模式	189
路由模式设置	190
启用群集范围内的自动路由迂回	193
配置 AAR 组	193
配置每天定时路由时间	194
配置时段	194
配置时间表	195
将时间表与分区关联	195
呼叫路由限制	195
使用被叫号码分析器进行故障诊断	196
线路组设置	197
关于线路组设置	197
删除线路组	197
线路组设置	198
向线路组添加成员	201
从线路组中删除成员	202

第 21 章

配置寻线引导	203
寻线引导概述	203
寻线引导配置任务流程	203
配置线路组	204
配置寻线列表	204
配置寻线引导	205
寻线引导中的通配符和特殊字符	205
寻线引导的性能和可扩展性	207
寻线引导相互作用和限制	208
未分配的呼叫	209

第 22 章

配置群集间查询服务 211

ILS 概述 211

ILS 网络容量 212

ILS 配置任务流程 212

配置群集 ID 213

配置 ILS 213

验证 ILS 正在运行 214

配置远程群集视图 215

ILS 相互作用和限制 215

ILS 相互作用 215

ILS 限制 216

第 23 章

配置全球拨号方案复制 219

全局拨号方案复制概述 219

URI 拨号 220

目录 URI 格式 221

呼叫前转到 URI 222

全局拨号方案复制呼叫路由 222

全局拨号方案复制前提条件 223

全局拨号方案复制配置任务流程 223

启用 ILS 对全局拨号方案复制的支持 224

配置 SIP 配置文件 225

为 URI 拨号配置 SIP 干线 225

配置 SIP 路由模式 226

设置对学习的数据的数据库限制 227

分配学习号码和模式的分区 227

为备用号码设置通告的模式 228

阻止学习模式 229

预配置全局拨号方案数据 229

导入全局拨号方案数据 230

全局拨号方案复制相互作用和限制 232

第 24 章

主叫方标准化 235

主叫方标准化概述 235

主叫方标准化前提条件 236

主叫方标准化配置任务流程 236

 全球化主叫方号码 237

 设置呼叫搜索空间 238

 创建主叫方转换模式 238

 将主叫方转换模式应用到呼叫搜索空间 239

 主叫方标准化服务参数示例 239

主叫方标准化相互作用和限制 240

 主叫方标准化相互作用 240

 主叫方标准化限制 242

第 25 章

配置拨号规则 243

拨号规则概述 243

拨号规则前提条件 243

拨号规则配置任务流程 244

 配置应用程序拨号规则 244

 配置目录查找拨号规则 245

 配置 SIP 拨号规则 245

 模式格式 246

 设置 SIP 拨号规则 246

 重置 SIP 拨号规则 247

 与 SIP 电话同步 SIP 拨号规则设置 248

 重排拨号规则优先顺序 248

拨号规则相互作用和限制 249

 SIP 拨号规则相互作用 249

 目录查找拨号规则限制 249

第 III 部分：

集成应用程序 251

第 26 章

集成 Cisco 应用程序 253

Cisco Unity Connection 253

启用 PIN 同步 254

Cisco Expressway 255

Cisco Emergency Responder 256

Cisco Paging Server 256

Cisco Unified Contact Center Enterprise 257

Cisco Unified Contact Center Express 257

高级 QoS APIC-EM 控制器 257

配置 Cisco WebDialer 服务器 258

第 27 章

配置 CTI 应用程序 259

CTI 应用程序概述 259

CTI 路由点概述 260

Cisco Unified Communications Manager 上的 CTI 冗余 260

CTIManager 上的 CTI 冗余 260

应用程序故障的 CTI 冗余 260

CTI 应用程序前提条件 261

配置 CTI 应用程序任务流程 261

激活 CTIManager 服务 262

配置 CTIManager 和 Cisco Unified Communications Manager 服务参数 262

配置 CTI 路由点任务流程 263

配置 CTI 路由点 263

配置新呼叫接受计时器 263

配置并发活动呼叫 264

同步 CTI 路由点 264

配置 CTI 设备目录号码 264

将设备与组关联 265

添加最终用户和应用程序用户 265

访问控制组配置选项	266
配置 CTI 冗余以解决应用程序故障	266

第 IV 部分：

预配置最终用户 269

第 28 章

配置预配置配置文件 271

预配置配置文件概述	271
预配置配置文件任务流程	272
配置 SIP 配置文件	274
配置电话安全性配置文件	274
创建功能控制策略	275
创建通用电话配置文件	276
配置通用设备配置	277
配置通用设备模板	277
配置通用线路模板	278
配置用户配置文件	278
配置头戴式耳机模板	280
配置 UC 服务	280
配置服务配置文件	281
配置功能组模板	282
配置默认凭证策略	283

第 29 章

配置 LDAP 同步 285

LDAP 同步概述	285
LDAP 同步前提条件	286
LDAP 同步配置任务流程	286
激活 Cisco DirSync 服务	287
启用 LDAP 目录同步	287
创建 LDAP 过滤器	288
配置 LDAP 目录同步	288
配置企业目录用户搜索	291

配置 LDAP 验证	291
自定义 LDAP 协议服务参数	292

第 30 章

使用批量管理工具预配置用户和设备	293
批量管理工具概述	293
批量管理工具前提条件	294
批量管理工具任务流程	294
添加电话到数据库	295
创建新的 BAT 电话模板	295
在 BAT 模板中添加或更新电话线路	296
在 BAT 模板中添加或更新 IP 服务	296
在 BAT 模板中添加或更新快速拨号	297
在 BAT 模板中添加或更新忙灯字段	298
在 BAT 模板中添加或更新忙灯字段定向呼叫暂留	298
在 BAT 模板中添加或更新内部通信模板	299
使用 BAT 电子表格创建电话 CSV 数据文件	299
使用文本编辑器创建自定义电话文件格式	302
将电话插入到 Unified Communications Manager	303
添加用户	304
从 BAT 电子表格创建用户 CSV 数据文件	305
将用户插入到 Unified Communications Manager 数据库	306
使用 BAT 电子表格添加电话及用户	307
添加电话和用户文件格式	307
将电话和用户插入到 Unified Communications Manager	308

第 V 部分：

预配置终端	311
-------	-----

第 31 章

配置终端	313
终端预配置默认设置	313
终端预配置默认设置前提条件	313
终端预配置默认设置任务流程	314

配置设备默认设置	314
更新设备默认设置	314
配置默认设备配置文件	315
在默认设备配置文件中配置软键模板	315
配置设备配置文件	317
配置企业电话	317
配置企业电话设置	317
配置电话	318
Self Care 自助门户	318

第 32 章

配置 CAPF	321
证书权限代理功能 (CAPF) 概述	321
电话证书类型	322
通过 CAPF 生成 LSC	322
CAPF 前提条件	323
证书权限代理功能配置任务流程	324
上传第三方 CA 的根证书	325
上传证书颁发机构 (CA) 根证书	325
配置在线证书颁发机构设置	326
配置离线证书颁发机构设置	327
激活或重新启动 CAPF 服务	328
在通用设备模板中配置 CAPF 设置	328
通过批量管理更新 CAPF 设置	329
配置电话的 CAPF 设置	331
设置保持连接计时器	331
CAPF 管理任务	332
证书状态监控	332
运行过时的 LSC 报告	332
查看待处理的 CSR 列表	332
删除过时的 LSC 证书	333
CAPF 系统相互作用和限制	333

7942 和 7962 电话的 CAPF 示例 334

CAPF 与 IPv6 寻址的相互作用 335

第 33 章

配置 TFTP 服务器 337

代理 TFTP 部署概述 337

冗余和对等代理 TFTP 服务器 337

代理 TFTP 337

TFTP 对 IPv4 和 IPv6 设备的支持 339

TFTP 部署的终端和配置文件 339

代理 TFTP 的安全考虑事项 339

TFTP 服务器配置任务流程 340

动态配置 TFTP 服务器 341

手动配置 TFTP 服务器 341

更新 TFTP 服务器的 CTL 文件 342

修改 TFTP 服务器的非配置文件 343

停止和启动 TFTP 服务 343

第 34 章

通过激活码激活设备 345

激活代码概述 345

现场模式下的自行激活工作流程 346

移动和远程访问模式下的自行激活工作流程 347

激活代码前提条件 347

现场模式下使用激活代码自行激活设备任务流程 348

激活设备激活服务 348

设置注册方法以使用激活代码 349

使用激活代码添加电话的要求 349

通过批量管理使用激活代码添加电话 350

配置 BAT 预配置模板 351

创建包含新电话的 CSV 文件 352

嵌入电话 352

激活电话 353

导出激活代码	354
设备自行激活任务流程（移动和远程访问模式）	354
通过移动和远程访问启用思科云自行激活	355
移动和远程访问服务域配置（可选）	355
上传自定义证书（可选）	355
激活代码的其他任务	356
激活代码用例	357

第 35 章

配置自动注册	359
自动注册概述	359
配置自动注册任务流程	359
配置自动注册分区	360
配置用于自动注册的呼叫搜索空间	361
配置自动注册设备池	362
设置自动注册的设备协议类型	363
启用自动注册	363
禁用自动注册	365
重复使用自动注册号码	365

第 36 章

配置自我预配置	367
自我预配置概述	367
自我预配置前提条件	368
自我预配置配置任务流程	369
激活自我预配置服务	369
启用自我预配置自动注册	370
配置 CTI 路由点	370
将目录号码分配给 CTI 路由点	371
配置应用程序用户进行自我预配置	371
配置系统以进行自我预配置	372
在用户配置文件中启用自我预配置	372

第 VI 部分：

参考信息 375

第 37 章

Cisco Unified Communications Manager TCP 和 UDP 端口使用情况 377

Cisco Unified Communications Manager TCP 和 UDP 端口使用情况概述 377

端口说明 379

Cisco Unified Communications Manager 服务器之间的群集内端口 379

公共服务端口 381

Cisco Unified Communications Manager 与 LDAP 目录之间的端口 384

从 CCMAAdmin 或 CCMUser 到 Cisco Unified Communications Manager 的 Web 请求 384

从 Cisco Unified Communications Manager 到电话的 Web 请求 385

电话和 Cisco Unified Communications Manager 之间的信令、媒体和其他通信 385

网关和 Cisco Unified Communications Manager 之间的信令、媒体和其他通信 387

应用程序和 Cisco Unified Communications Manager 之间的通信 389

CTL 客户端和防火墙之间的通信 390

思科智能许可服务和思科智能软件管理器之间的通信 391

HP 服务器上的特殊端口 391

端口参考 391

防火墙应用程序检测指南 391

IETF TCP/UDP 端口分配列表 392

IP 电话配置和端口利用指南 392

VMware 端口分配列表 392

第 38 章

IM and Presence Service 的端口使用信息 393

IM and Presence Service 端口使用概述 393

表中列出的信息 393

IM and Presence Service 端口列表 394



第 1 章

新增和变更内容

- [新增和变更内容，第 1 页](#)

新增和变更内容

下表概述本指南中对此最新版本及之前版本的重大功能更改。下表未提供对此版本及之前版本的指南或新功能进行的所有更改的详尽列表。

表 1: *Unified Communications Manager* 和 *IM and Presence* 服务中的新增功能和更改的行为

功能或更改	说明	请参阅	日期
14 版的文档初始版本	—	—	2021 年 3 月 31 日
为 78xx 和 88xx 电话启用 SIP OAuth	SIP OAuth 提供端到端安全信令和媒体加密，无需 CAPF 内部部署和 MRA。默认情况下，启用 SIP OAuth 时，TFTP 对 SIP 电话而言是安全的。	<ul style="list-style-type: none">• 设置注册方法以使用激活代码，第 349 页• 激活代码用例，第 357 页	2021 年 3 月 31 日
不受版本限制的许可证	Unified Communications Manager 支持不受版本限制的用户许可证。许可证按年收费，并按订购期限签发。您可以通过 Flex EA（企业协议）或 Flex NU（指定用户—专业版、增强版、访问权限）订购这些 V14 许可证。	智能软件许可，第 7 页	2021 年 3 月 31 日
14SU1 版的文档初始版本	—	—	2021 年 10 月 27 日

功能或更改	说明	请参阅	日期
Opus 编解码器转码器支持	Unified Communications Manager 现在包括信令客户端控制协议 (SCCP) 控制的基于 iOS 的注册媒体资源，支持成功媒体协商所需的转码 Opus 音频编解码器。	Opus 编解码器转码器支持，第 119 页	2021 年 10 月 27 日
用于 OAuth 的 TFTP 代理支持	Unified Communications Manager 在 SIP OAuth 部署中支持 TFTP 代理。	<ul style="list-style-type: none"> • 动态配置 TFTP 服务器，第 341 页 • 手动配置 TFTP 服务器，第 341 页 	2021 年 10 月 27 日
14SU2 版的文档初始版本	—	—	2022 年 6 月 16 日
14SU3 版的文档初始版本	—	—	2023 年 5 月 18 日
DTMF SRTP 交互工作	<p>目前，Unified Communications Manager 会在安全和非安全呼叫中为 DTMF 不匹配插入 MTP。但是对于安全呼叫，虽然为 DTMF 不匹配插入了 MTP，但它只会通过媒体在双方之间传送。因此，DTMF 事件不会在各方之间发送。在 Unified CM Release 14SU3 之前，只有为 DTMF 不匹配分配了 MTP 时，DTMF 转换才会对非安全呼叫有效。</p> <p>在此版本中，Unified CM 可以为安全终端之间的 DTMF 不匹配调用硬件 MTP（使用 SRTP DTMF 互通支持）。</p>	SRTP DTMF 交互工作，第 117 页	2023 年 5 月 18 日
呼叫的 iOS 本地推送连接	<p>当 iOS 设备在没有 Internet 连接的 Wi-Fi 受约束网络（例如，医院、游轮、飞机等）中运行时，将不会向 Webex 应用发送 VoIP 来电通知。由于缺少 Internet 连接，设备无法访问 Apple 推送通知服务 (APNS)。用户希望没有任何延迟的情况下接收呼叫。但是，如果存在网络滞后，则使用 APNS 呼叫可能会延迟数秒。</p> <p>在此版本中，已在 Apple 设备上引入了呼叫的本地推送通知服务 (LPNS)。这有助于最大限度地减少推送消息通过永久连接发送到客户端时的任何延迟。</p>	<ul style="list-style-type: none"> • 公共服务端口，第 381 页 • 电话和 Cisco Unified Communications Manager 之间的信令、媒体和其他通信，第 385 页 	2023 年 5 月 18 日



第 2 章

简介

- [系统配置概述，第 3 页](#)

系统配置概述

本文档包含用于呼叫控制系统安装后设置的基本配置任务。此文档可让您配置系统参数、拨号方案和呼叫路由、媒体资源、集成应用程序以及预配置最终用户和终端。完成本文档中的配置，您应该拥有了基本配置，其中包含已配置的拨号方案、呼叫路由、媒体资源、带宽管理资源和基本安全。此外，还会预配置用户和终端。

本文档包含以下各节：

- 系统组件—配置系统许可、基本安全性、SSO、设备池、干线、网关、媒体资源和通话准入控制等项目。
- 拨号方案—配置拨号方案和呼叫路由元素。
- 集成应用程序—集成 Cisco Emergency Responder、Cisco Unity Connection 和 Cisco Expressway 等应用程序。
- 部署用户—将用户添加到您的系统。
- 部署设备—为您的用户注册设备。

完成本指南中的任务后，系统即完成了用户、设备、基本安全和SSO设置。然后，您可以继续配置 Cisco 解决方案。



第 I 部分

系统组件

- [智能软件许可，第 7 页](#)
- [配置企业参数和服务，第 33 页](#)
- [配置 IPv6 堆栈，第 45 页](#)
- [配置双堆栈（IPv4 和 IPv6），第 51 页](#)
- [配置基本的安全性，第 55 页](#)
- [配置单点登录，第 61 页](#)
- [配置设备池的核心设置，第 67 页](#)
- [配置干线，第 87 页](#)
- [配置网关，第 93 页](#)
- [配置 SRST，第 109 页](#)
- [配置媒体资源，第 115 页](#)
- [配置会议桥，第 137 页](#)
- [配置增强位置通话准入控制，第 145 页](#)
- [配置资源预留协议，第 153 页](#)
- [配置推送通知，第 161 页](#)



第 3 章

智能软件许可

- [智能软件许可概述，第 7 页](#)
- [系统许可前提条件，第 10 页](#)
- [智能软件许可任务流程，第 10 页](#)
- [采用智能软件许可的附加任务，第 13 页](#)
- [特定许可证预留，第 17 页](#)
- [不受版本限制的许可证，第 30 页](#)
- [智能许可导出合规，第 30 页](#)

智能软件许可概述

Cisco 智能软件许可是一种新的许可方式。它可提高您的许可灵活性，并在整个企业中简化许可过程。它还可用于查看您的许可证所有权和使用情况。

Cisco 智能软件许可可帮助您轻松地获取、部署和管理许可证，使设备可以自注册并报告许可证使用情况，从而无需产品激活密钥 (PAK)。它将许可证权利汇集在一个帐户中，并允许您根据需要跨网络自由转移许可证。Cisco 产品中都启用了该功能，并通过基于云或中介的直接部署模型进行管理。

Cisco Smart Software Licensing 服务可从 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 注册产品实例、报告许可使用并获取必要授权。

您可以使用智能许可执行以下操作：

- 查看许可使用和计数
- 显示各许可类型的状态
- 查看 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 上可用的产品许可证
- 与 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 续订产品授权
- 续订许可证注册
- 取消与 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 的注册



注释 许可证授权有效期为 90 天，至少 30 天续订一次。如果未连接到 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite，则授权将在 90 天后过期。

如果选择了 Cisco Smart Software Manager satellite 选项，则 satellite 必须与 Cisco Smart Software Manager 建立 Internet 连接才能进行授权。Cisco Smart Software Manager satellite 可以在两种模式下运行：连接模式（连接时间可配置）和断开模式（需要手动同步）。

有两种用于智能许可的主要部署选项：

- Cisco Smart Software Manager
- Cisco Smart Software Manager satellite

Cisco Smart Software Manager

Cisco Smart Software Manager 是一项基于云的服务，负责处理您的系统许可。如果 Unified Communications Manager 可直接或通过代理服务器连接到 cisco.com，使用此选项。Cisco Smart Software Manager 可用于：

- 管理和跟踪许可证
- 在虚拟帐户之间转移许可证
- 删除注册的产品实例

或者，如果 Unified Communications Manager 无法直接连接到 Cisco Smart Software Manager，您可以部署代理服务器来管理连接。

有关 Cisco Smart Software Manager 的其他信息，请转至<https://software.cisco.com>。

Cisco Smart Software Manager Satellite

Cisco Smart Software Manager satellite 是一种现场部署，可在 Unified Communications Manager 因安全或可用性原因而无法直接连接到 cisco.com 时，处理您的许可需求。部署此选项时，Unified Communications Manager 将注册并向 satellite 报告许可证使用情况，它会定期将其数据库与 cisco.com 上托管的后端 Cisco Smart Software Manager 同步。

Cisco Smart Software Manager satellite 可以在“连接”或“断开连接”的模式下使用，具体取决于 satellite 是否可以直接连接到 cisco.com。

- 连接—直接从 Smart Software Manager satellite 连接到 cisco.com 时使用。智能帐户会自动同步。
- 断开连接—当无法从 Smart Software Manager satellite 连接到 cisco.com 时使用。智能帐户同步必须手动上传和下载。



注释 在双堆栈模式下运行的 Unified CM 支持使用 IPv4 和 IPv6 地址配置的 satellite。

对于 Cisco Smart Software Manager satellite 信息和文档，请转至 <https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html>。

许可证类型

以下许可类型可用于满足您的需求：

Cisco Unified Workspace Licensing

Cisco Unified Workspace Licensing (UWL) 通过实惠方便的套餐，提供最常用思科协作应用和服务的捆绑包，包括软客户端、应用服务器软件和按用户提供的许可。

Cisco User Connect 许可

用户连接许可 (UCL) 是针对每个 Cisco Unified Communications 应用程序的基于用户的许可，其中包括应用服务器软件、用户许可和软客户端。根据所需的设备类型和设备数量，UCL 提供 Essential、Basic、Enhanced 和 Enhanced Plus 版本。

有关这些许可证类型及其可用版本的详细信息，请参阅 <http://www.cisco.com/c/en/us/products/unified-communications/unified-communications-licensing/index.html>。

会话管理版

会话管理版本可以注册到 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite。您可以使用与 Unified Communications Manager 相同的过程注册会话管理版本，注册到 Cisco Unified Communications Manager 已注册的虚拟帐户或单独的虚拟帐户，并满足一组最小的许可要求。



注释

在特定许可证预留 (SLR) 中注册的 SME 需要在 CSSM 中预留一组最低的许可证，同时生成 SLR 授权码。

产品实例评估模式

安装后，Unified Communications Manager 会在 90 天的评估期内运行。评估期结束时，Unified Communications Manager 会停止允许添加新用户或设备，除非先向 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 注册。



注释

评估期为产品注册之前。



注释

在 90 天评估期内运行时，您无法部署安全 SIP 干线。要部署安全的 SIP 干线，您的系统必须已注册到 Smart Software Manager 帐户，并且选择了允许导出受控的功能产品注册令牌。

系统许可前提条件

计划您的系统许可

查看并了解 Unified Communications (UC) 许可结构。有关详细信息，请参阅 <http://www.cisco.com/c/en/us/products/unified-communications/unified-communications-licensing/index.html>。

计划打算如何将 Unified Communications Manager 连接到 Smart Software Manager 服务：

- 至 [cisco.com](http://www.cisco.com) 上的 Cisco Smart Software Manager 的直接连接—Unified Communications Manager 直接连接到 [cisco.com](http://www.cisco.com) 上的 Smart Software Manager。使用此选项时，必须在解析 tools.cisco.com 的 Unified Communications Manager 上配置 DNS。
- 通过代理服务器至 Smart Software Manager 的连接—Unified Communications Manager 连接到代理服务器或传输网关，后者连接到 [cisco.com](http://www.cisco.com) 上的 Cisco Smart Software Manager。DNS 在 Unified Communications Manager 上并非必需，但您确实需要配置可以解析 tools.cisco.com 的代理服务器上的 DNS。
- 至现场 Cisco Smart Software Manager satellite 的连接—Unified Communications Manager 连接到现场 Smart Software Manager satellite。DNS 在 Unified Communications Manager 上并非必需。如果您部署已连接模式，则在 satellite 服务器上必需可以解析 tools.cisco.com 的 DNS。如果您部署断开连接模式，DNS 在 satellite 服务器上并非必需。

智能许可注册

设置智能帐户和虚拟帐户。有关详细信息，请参阅 <https://software.cisco.com/>。

可选。如果您想要部署 Cisco Smart Software Manager satellite，请安装并设置 satellite。请参阅文档，包括《*Smart Software Manager satellite 安装指南*》。您可以在 <https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html> 上查找文档。

智能软件许可任务流程

完成这些任务以设置 Unified Communications Manager 的系统许可。

过程

	命令或操作	目的
步骤 1	获取产品实例注册令牌，第 11 页。	使用此程序为您的虚拟帐户生成产品实例注册令牌。
步骤 2	配置与智能软件许可的连接，第 11 页	选择传输设置，Unified Communications Manager 将通过该设置连接到智能软件许可服务。 直接 选项默认为选中，其中产品直接与 Cisco 许可服务器通信。

	命令或操作	目的
步骤 3	向 Cisco Smart Software Manager 注册，第 12 页。	执行此步骤以向 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 注册 Cisco Unified Communications Manager。

获取产品实例注册令牌

开始之前

从 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 获取产品实例注册令牌以注册产品实例。令牌可以在启用或禁用导出控制功能的情况下生成。

过程

步骤 1 登录到 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 中的智能帐户。

步骤 2 导航到要与 Unified Communications Manager 群集关联的虚拟帐户。

步骤 3 生成“产品实例注册令牌”。

注释 选中允许使用此令牌注册的产品具备导出受控功能复选框，为要加入此智能帐户的产品实例启用导出受控功能。选中此复选框并接受条件时，即为使用此注册令牌注册的产品启用更高级别的加密。默认情况下，此复选框为选中状态。如果您希望不允许提供导出受控功能与此令牌一起使用，可以取消选中此复选框。

注意 仅当您符合导出受控功能时，才可使用此选项。

注释 允许使用此令牌注册的产品具备导出受控功能复选框不会对不允许使用导出受控功能的智能帐户显示。

步骤 4 复制该令牌或将其保存到另一位置。

有关详细信息，请参阅：<https://software.cisco.com/>。

配置与智能软件许可的连接

完成此任务以将 Unified Communications Manager 连接到智能软件许可服务。

过程

步骤 1 从 Cisco Unified CM 管理中，选择系统 > 许可 > 许可管理。
许可管理窗口将会显示。

步骤 2 从智能软件许可部分，单击查看/编辑许可 **Smart Call Home** 设置链接。
系统将显示传输设置对话框。

步骤 3 选择将 Unified Communications Manager 连接到智能许可服务的方法：

- **直接**—Unified Communications Manager 直接连接到 cisco.com 上的 Smart Software Manager。这是默认选项。使用此选项时，必须在可以解析 tools.cisco.com 的 Unified Communications Manager 上部署 DNS。
- **传输网关**—Unified Communications Manager 连接到现场 Cisco Smart Software Manager satellite 或传输网关以获取系统许可。在 URL 文本框中，输入 Smart Software Manager satellite 或传输网关的地址和端口。例如，fqdn_of_smart_software_manager:port_number。对于 HTTPS，使用端口 443。
- **HTTP/HTTPS 代理**—Unified Communications Manager 连接到代理服务器，后者连接 Cisco Smart Software Manager 服务和传输网关以及 cisco.com 上的 satellite。输入代理服务器的 IP 地址或主机名以及端口：
 - HTTP 或 HTTPS 上需要验证—如果想要使用基于身份验证的代理服务器注册到 Cisco Smart Software Manager，请启用此复选框。
 - IP 地址/主机名
 - 端口—适用于 HTTPS，使用端口 443。
 - 用户名
 - 密码

步骤 4 选中不要与 **Cisco** 共享我的主机名或 IP 地址 复选框，以限制 Unified Communications Manager 在智能许可注册期间共享其 IP 地址和主机名。

步骤 5 单击保存。

向 Cisco Smart Software Manager 注册

此程序用于向 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 注册您的产品。在注册完成之前，您的产品仍处于评估模式。

过程

步骤 1 从 Cisco Unified CM 管理中，选择系统 > 许可 > 许可管理。
许可管理窗口将会显示。

步骤 2 从智能软件许可部分，单击注册按钮。
注册窗口将会显示。

步骤 3 在产品实例注册令牌部分，粘贴复制或保存的“注册令牌密钥”，该密钥是您使用 Smart Software Manager 或 Smart Software Manager satellite 生成的。

步骤 4 单击注册完成注册过程。

步骤 5 单击关闭。有关详细信息，请参阅在线帮助。

步骤 6 在许可使用报告部分中，单击更新使用详细信息手动更新系统许可使用信息。

注释 使用信息每 24 小时自动更新一次。有关详细信息，请参阅在线帮助。

采用智能软件许可的附加任务

以下可选任务适用于 Unified Communications Manager 和智能软件许可：

过程

	命令或操作	目的
步骤 1	续订授权，第 14 页	<p>手动完成此任务可续订许可证类型下列出的所有许可证的许可授权状态。</p> <p>注释 许可证授权每 30 天自动续订一次。如果授权状态未连接到 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite，将在 90 天后过期。</p> <p>如果选择了 Cisco Smart Software Manager satellite 选项，则 satellite 必须与 Cisco Smart Software Manager 建立 Internet 连接才能进行授权。Cisco Smart Software Manager satellite 可以在两种模式下运行：连接模式（连接时间可配置）和断开模式（需要手动同步）。</p>
步骤 2	续订注册，第 15 页	<p>完成此任务以手动续订注册信息。</p> <p>注释 初始注册的有效期为一年。只要产品连接到 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite，注册续订每六个月自动进行。</p>
步骤 3	注销，第 15 页	<p>完成此任务会断开 Unified Communications Manager 群集与 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 的连</p>

	命令或操作	目的
		接。只要评估期末过期，产品可恢复为评估模式。用于产品的所有许可证权利将立即释放回虚拟帐户，可供其他产品实例使用。
步骤 4	重新向 Cisco Smart Software Manager 注册许可证，第 17 页	完成此任务会向 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 注册 Cisco Unified Communications Manager。 注释 通过使用令牌从新的虚拟帐户重新注册，产品可以迁移到其他虚拟帐户。

续订授权

使用此程序可手动为许可证类型下列的所有许可证续订许可授权状态。



注释 许可证授权每 30 天自动续订一次。如果授权状态未连接到 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite，将在 90 天后过期。

如果选择了 Cisco Smart Software Manager satellite 选项，则 satellite 必须与 Cisco Smart Software Manager 建立 Internet 连接才能进行授权。Cisco Smart Software Manager satellite 可以在两种模式下运行：连接模式（连接时间可配置）和断开模式（需要手动同步）。

开始之前

产品应注册到 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite。

过程

步骤 1 从 Cisco Unified CM 管理中，选择系统 > 许可 > 许可管理。

许可管理窗口将会显示。

步骤 2 从智能软件许可部分，单击操作下拉列表。

步骤 3 选择立即续订授权。

续订授权窗口将会显示。

步骤 4 单击确定。

Unified Communications Manager 将请求发送到 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 以检查“许可证授权状态”，然后，Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 会将状态报告回 Unified Communications Manager。有关详细信息，请参阅在线帮助。

步骤 5 在许可使用报告部分中，单击更新使用详细信息手动更新系统许可使用信息。

注释 使用信息每 24 小时自动更新一次。有关字段及其配置选项的更多信息，请参阅系统联机帮助。

续订注册

在产品注册到 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 期间，有一个用于识别产品并通过注册证书固定的安全关联，该关联的有效期限为一年（即注册期间）。这不同于注册令牌 ID 过期，后者对令牌激活有时间限制。此注册期间每六个月自动续订。但是，如果存在问题，您可以手动续订此注册期间。

开始之前

产品应注册到 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite。

过程

步骤 1 从 Cisco Unified CM 管理中，选择系统 > 许可 > 许可管理。

许可管理窗口将会显示。

步骤 2 从智能软件许可部分，单击操作下拉列表。

步骤 3 选择立即续订注册。

续订注册窗口即会显示。

步骤 4 单击确定。

Unified Communications Manager 将请求发送到 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 以检查“注册状态”，然后，Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 将状态报告回 Unified Communications Manager。

步骤 5 在许可使用报告部分中，单击更新使用详细信息手动更新系统许可使用信息。

注释 使用信息每 24 小时自动更新一次。有关字段及其配置选项的更多信息，请参阅系统联机帮助。

注销

使用此程序从 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 注销，然后释放当前虚拟帐户的所有许可证。此程序还会断开 Unified Communications Manager 群集与 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 的连接。用于产品的所有许可证权利将释放回虚拟帐户，可供其他产品实例使用。



注释 如果 Unified Communications Manager 无法与 Cisco Smart software Manager 或 Cisco Smart software manager satellite 连接，并且该产品仍在注销，则会显示一条警告消息。此消息会通知您手动从 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 中删除该产品以释放许可证。

开始之前

产品应注册到 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite。

过程

步骤 1 从 Cisco Unified CM 管理中，选择系统 > 许可 > 许可管理。

许可管理窗口将会显示。

步骤 2 从智能软件许可部分，单击操作下拉列表。

步骤 3 选择注销。

注销窗口将会显示。

步骤 4 单击确定。

步骤 5 在许可使用报告部分中，单击更新使用详细信息手动更新系统许可使用信息。

注释 使用信息每 6 小时自动更新一次。有关字段及其配置选项的更多信息，请参阅系统联机帮助。

注释

- 如果在使用 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 注册后，数据平面加密（混合模式下的 Unified Communications Manager 群集）已启用并且该产品会在以后注销，则混合模式将继续启用。

当从 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 注销该产品时，会将名称为 SmartLicenseExportControlNotAllowed 的警报发送到管理员，以将群集设置为非安全模式。混合模式即使在重新启动后仍将继续启用。

- 此行为在注销后，可能会在产品将来的版本中发生变化。有关设置 CTL 客户端的详细信息，请参阅《Cisco Unified Communications Manager 安全指南》的“设置 Cisco CTL 客户端”一章，位于 <http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-maintenance-guides-list.html>。

有关无令牌 CTL 的混合模式的详细信息，请参阅“无令牌 CTL 的 CUCM 混合模式”，位于 <http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-tech-notes-list.html>。

重新向 Cisco Smart Software Manager 注册许可证

使用此程序向 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 注册 Cisco Unified Communications Manager。

开始之前

[获取产品实例注册令牌，第 11 页。](#)

过程

步骤 1 从 Cisco Unified CM 管理中，选择系统 > 许可 > 许可管理。

许可管理窗口将会显示。

步骤 2 从智能软件许可部分，单击注册按钮。

注册窗口将会显示。

步骤 3 从智能软件许可部分，单击操作下拉列表。

步骤 4 选择重新注册。

重新注册窗口将会显示。

步骤 5 单击确定。

步骤 6 在产品实例注册令牌部分，粘贴您使用 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 生成的已复制或已保存“注册令牌密钥”。

步骤 7 单击注册完成注册过程。

步骤 8 单击关闭。有关详细信息，请参阅在线帮助。

步骤 9 在许可使用报告部分中，单击更新使用详细信息手动更新系统许可使用信息。

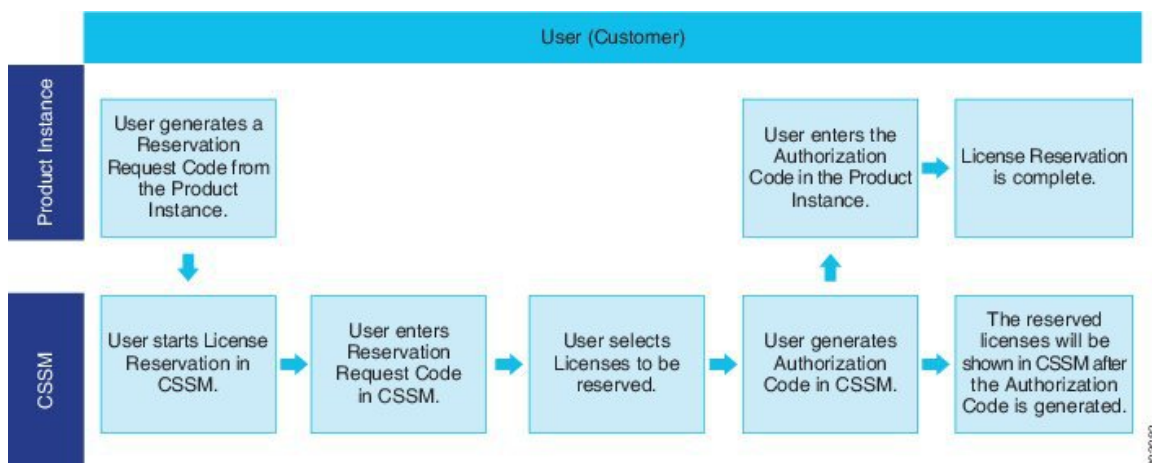
注释 使用信息每 24 小时自动更新一次。有关字段及其配置选项的更多信息，请参阅系统联机帮助。

特定许可证预留

特定许可证预留是高度安全的网络中使用的功能。它提供的方法让客户无需传输使用信息即可在设备（产品实例 - Unified Communications Manager）上部署软件许可证。

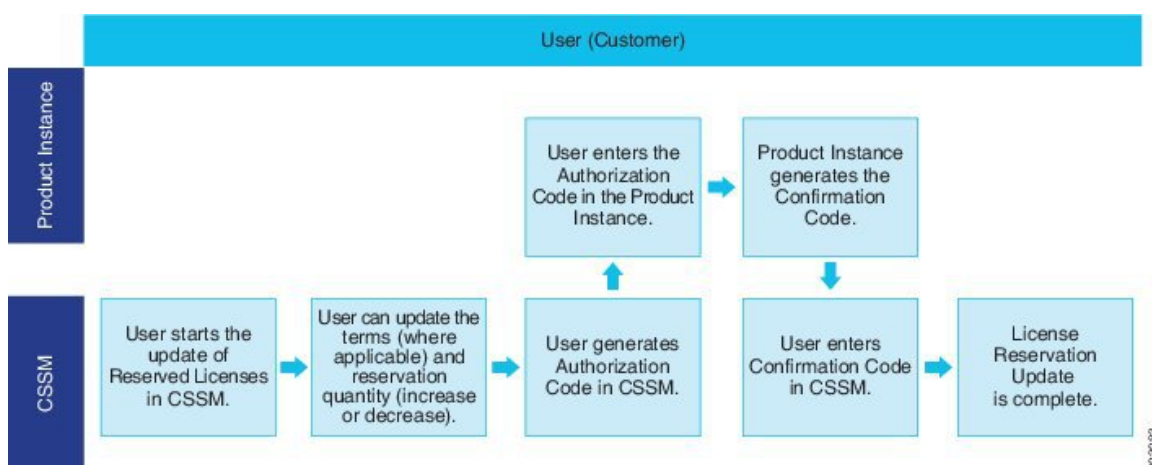
用户可以根据 Unified Communications Manager 产品指定和保留永久或基于字词的许可证。在交换授权码后，无需进行常规的产品同步，直到保留发生更改。预留的许可在 Cisco Smart Software Manager 中仍将被阻止，除非使用退回代码从产品发布。

图 1: 预留许可证



在 Cisco Smart Software Manager 中，可在以前预留的许可证上完成预留许可证（增加或减少）的更新或更改。新授权码可安装在产品上，并可获得确认码。除非在 Cisco Smart Software Manager 上安装了产品的确认码，否则新的更改将保持传输中状态。

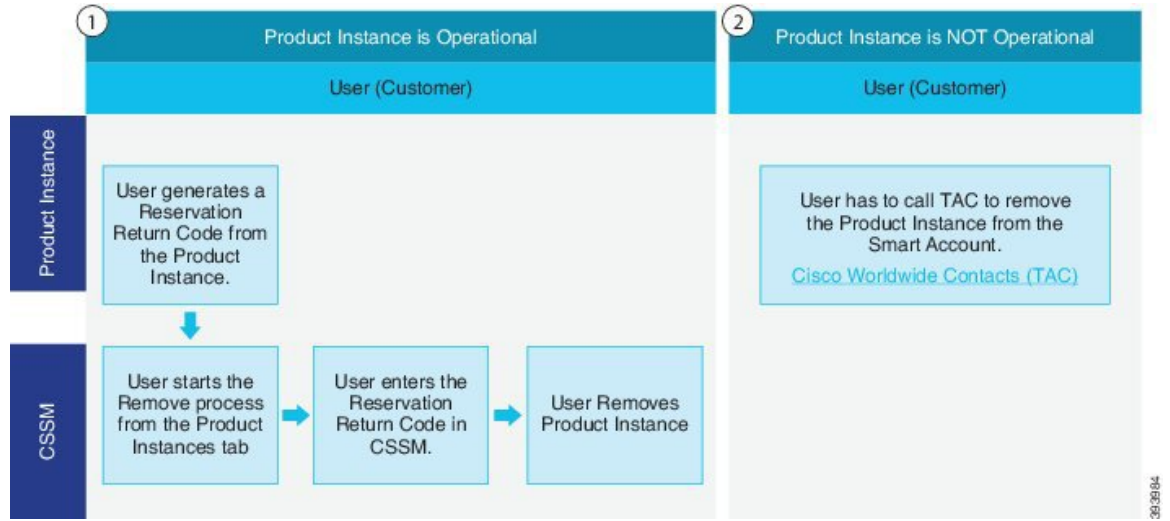
图 2: 更新预留许可证



在产品实例 (Unified Communications Manager) 上预留许可证时，有两种方法可以从智能账户中删除产品，并释放为该产品实例 (Unified Communications Manager) 预留的所有许可证：

产品实例正在工作（平稳删除）：用户通过在产品实例（它删除了授权代码）创建预留退回代码并在 Cisco Smart Software Manager 中输入预留退回代码，可以退回特定的许可证预留授权。

产品实例不工作（失败/RMA 或因销毁 VM/容器而导致）：用户必须联系 TAC，用户才能从其智能账户中删除产品实例。

图 3: 删除产品实例 - *Unified Communications Manager*

注释 用户只能使用 CLI 配置来启用特定的许可证预留。



注释 在 Unified Communications Manager 上启用特定的许可证预留时，将不支持适用于云自行激活的凭证生成。

有权在其智能账户上使用许可证预留功能的客户可以从其虚拟帐户预留许可证，将它们与设备 UDI 进行关联，并在断开连接模式下使用具有这些预留许可证的设备。客户从虚拟账户为 UDI 预留特定许可证和许可证计数。以下选项介绍用于特定许可预留的新功能和设计元素：

- license smart reservation enable
- license smart reservation disable
- license smart reservation request
- license smart reservation cancel
- update license reservation
- license smart reservation install "<authorization-code>"
- license smart reservation install-file<url>
- license smart reservation return
- license smart reservation return-authorization "<authorization-code>"

特定许可证预留任务流程

完成这些任务以为 Unified Communications Manager 保留特定的许可证。

license smart reservation enable

此程序用于启用特定许可证预留。

开始之前

Cisco Unified Communications Manager 取消与 Cisco Smart Software Manager 或 Satellite 的注册。

过程

从 Cisco Unified CM 管理控制台执行以下 CLI 命令。

- `license smart reservation enable`
-

license smart reservation request

此程序用于从 Unified Communications Manager 产品生成保留请求代码生成请求代码。

开始之前

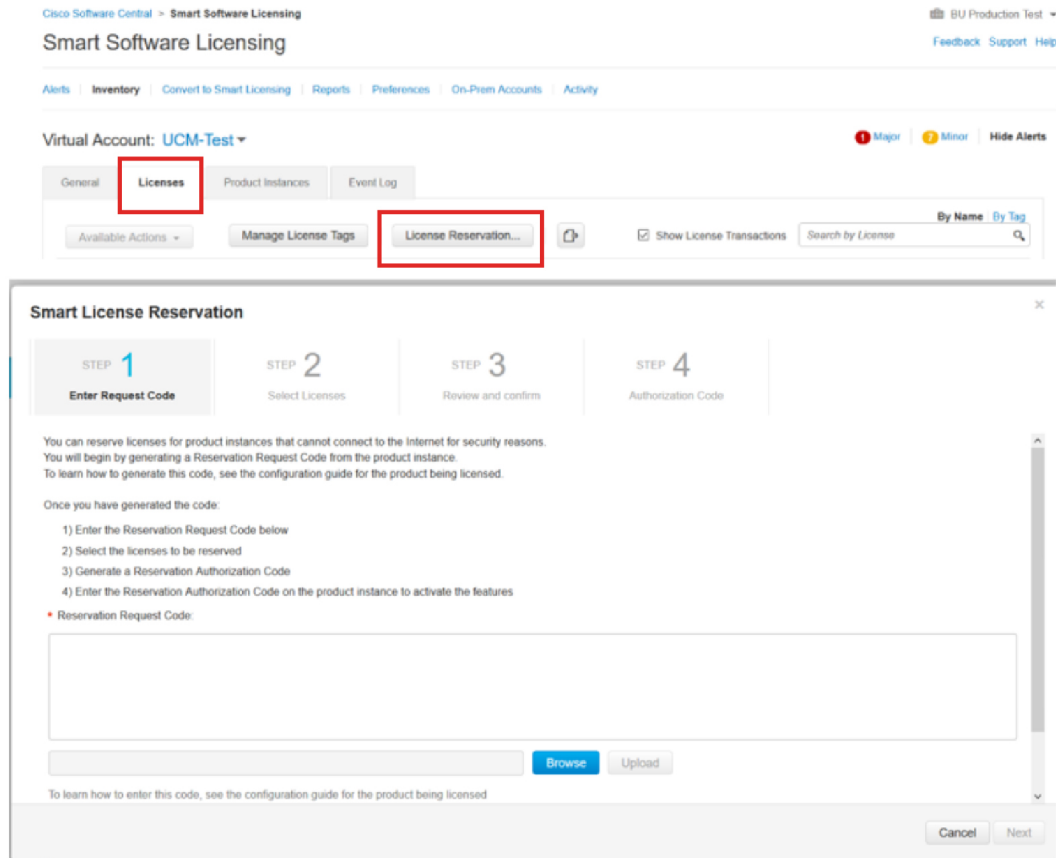
通过执行 **license smart reservation enable**，确保 Unified Communications Manager 注册状态为“正在预订”。

命令

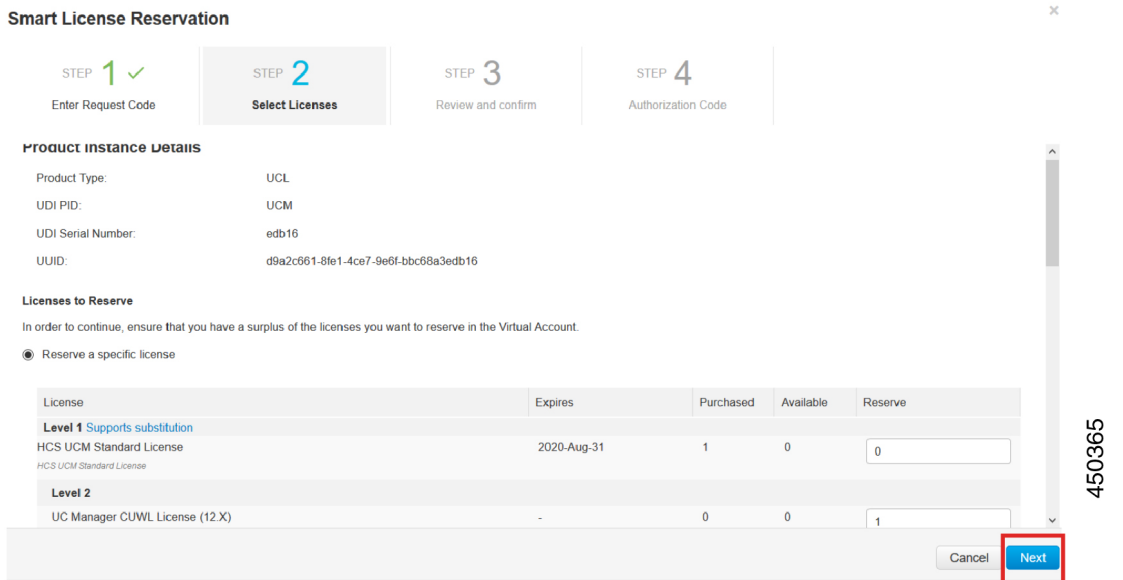
过程

步骤 1 从 Cisco Unified CM 管理控制台执行 *license smart reservation request* 命令。

步骤 2 登录到 CSSM [Cisco Smart Software Manager] 并输入预留请求代码。



步骤 3 选择必须为此设备预留的许可证，然后生成授权码。



[illegible]

450366

使用此程序安装从 Cisco Smart Software Manager 生成的许可证预留授权码。

按以下顺序执行命令，确保 Unified Communications Manager 注册状态为“正在预留”：

- **license smart reservation enable**
- **license smart reservation request**

从 Cisco Unified CM 管理控制台执行以下 CLI 命令。

- license smart reservation install "<authorization-code>"

使用此程序安装在 Cisco Smart Software Manager 上生成的许可证预留授权码文件。

按以下顺序执行命令，确保 Unified Communications Manager 注册状态为“正在预留”：

- **license smart reservation enable**
- **license smart reservation request**



sftp://<HostName/IP>:<port>/<Path to Authorization-Code file>

过程

从 Cisco Unified CM 管理控制台执行以下 CLI 命令。

- license smart reservation install-file<url>

特定许可证预留的其他任务

以下其他任务可在 Unified Communications Manager 上用于特定许可预留：

license smart reservation disable

使用此程序禁用特定许可证预留。

开始之前

在 Unified Communications Manager 上启用特定许可证预留

过程

从 Cisco Unified CM 管理控制台执行以下 CLI 命令。

- license smart reservation disable

update license reservation

使用此程序可更新您的产品实例的许可证预留并获取新的授权码。

开始之前

通过执行以下命令，确保 Unified Communications Manager 注册状态为“已注册- 特定的许可证预留”：

- license smart reservation enable
- license smart reservation request
- license smart reservation install "<authorization-code>"

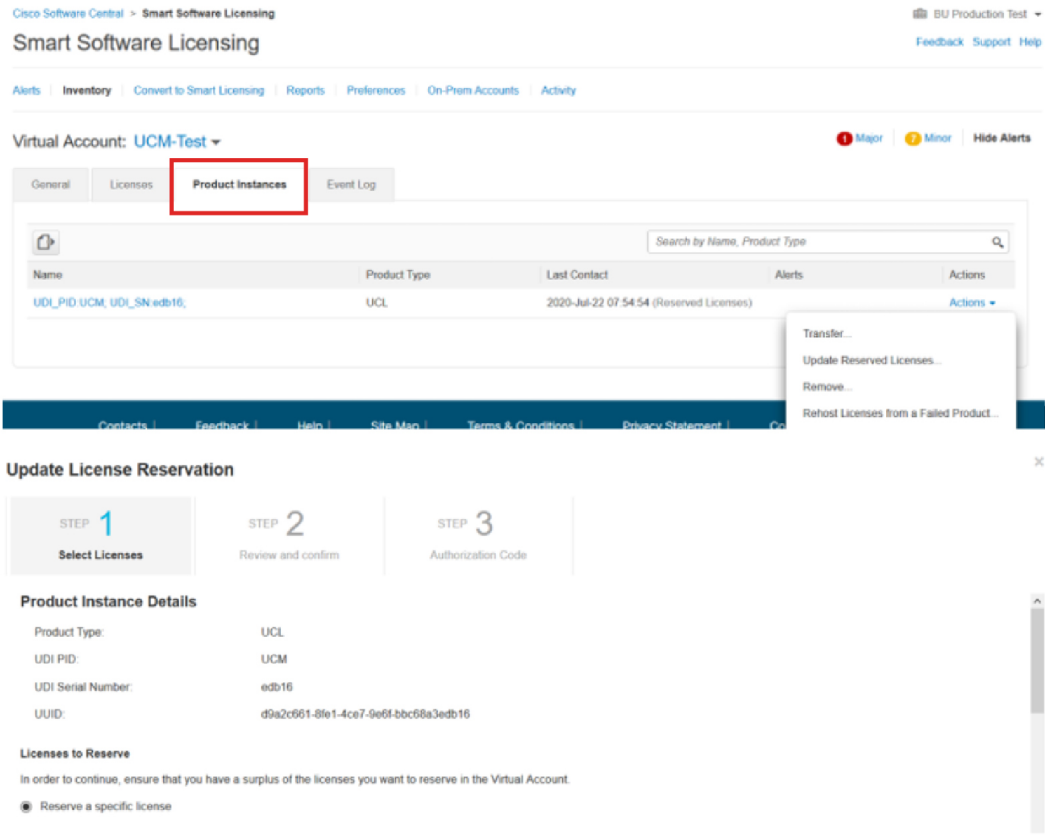


注释

当在 Unified Communications Manager 中启用特定许可证预留时，从较高层借用许可证不会自动发生。许可证预留必须手动更新 Unified Communications Manager 许可证消耗/使用。

过程

步骤 1 从您要在 CSSM 上更新预留的产品实例旁边的“操作”下拉列表中选择“更新预留许可证”。



450363

步骤 2 更新预留（为此产品实例的添加/删除/更新许可证）并生成授权码。

Update License Reservation

STEP 1
Select Licenses

STEP 2
Review and confirm

STEP 3
Authorization Code

Product Instance Details

Product Type: UCL
UDI PID: UCM
UDI Serial Number: edb16
UUID: d9a2c661-8fe1-4ce7-9e6f-bbc68a3edb16

Licenses to Reserve

In order to continue, ensure that you have a surplus of the licenses you want to reserve in the Virtual Account.

☒ Reserve a specific license

License	Expires	Purchased	Available	Reserve
Level 1 Supports substitution HCS UCM Standard License <small>HCS UCM Standard License</small>	2020-Aug-31	1	0	<input type="text" value="0"/>
Level 2 UC Manager CUWL License (12 X)	-	0	0	<input type="text" value="1"/>

Cancel

Next

450367

步骤 3 将授权码复制到产品实例，然后执行 **license smart reservation install "<authorization-code>"** 命令进行安装。

Update License Reservation

STEP 1 ✓
Select Licenses

STEP 2 ✓
Review and confirm

STEP 3
Authorization Code

☒ The Reservation Authorization Code below has been generated for this product instance. Several steps remain:

1. This code must be entered into the Product Instance's Smart Licensing settings to complete the reservation.
2. When the code has been entered, a Reservation Confirmation Code will be generated.
3. To release licenses in transition, enter confirmation code generated by device into CSSM.

Authorization Code:

```
<specificPLR><authorizationCode><flag>A<flag><version>C<version><pid>6191f5e5-319e-41ff-abba-be220ea4b2e1</pid><timestamp>1595405336190</timestamp><entitlements><entitlement><tag>regid.2017-02.com.cisco.UCM_CUWL.12.0_cc59375a-1cd8-4b36-8366-6f4d2abba965</tag><count>1</count><startDate>2020-Mar-04 UTC</startDate><endDate>2020-Aug-31 UTC</endDate><licenseType>TERM</licenseType><displayName>UC Manager CUWL License (12 X)</displayName><tagDescription>UC Manager CUWL License</tagDescription><subscriptionID></subscriptionID></entitlement><entitlement><tag>regid.2016-07.com.cisco.UCM_Enhanced.12.0_66d0d1cf-4863-4761-91d0-d01d3eb1949a</tag><count>1</count><startDate></startDate></endDate></endDate><licenseType>PERPETUAL</licenseType><displayName>UC Manager Enhanced License (12 X)</displayName><tagDescription>UC Manager Enhanced License</tagDescription><subscriptionID></subscriptionID></entitlement><entitlements></entitlements><authorizationCode><signature>MEQCIFDLpw4k+0O+Zr3bp/ucJ3KNyKVGdGumUVN0BuGyvi9JAIBcB60+c2GXA52FUIAIZdVhHz9xcVbbr/raWoavm9Hmw==</signature><udi>P-UCM,S.edb16,U.d9a2c661-8fe1-4ce7-9e6f-bbc68a3edb16</udi>
```

To learn how to enter this code, see the configuration guide for the product being licensed

Download as File

Copy to Clipboard

Enter Confirmation Code

Close

450362

步骤 4 授权码成功安装后，即会在产品上生成确认码。

```
admin:license smart reservation install "specificPLR-authorizationCode=<flag>A<flag><version>C<version><pid>6191f5e5-319e-41ff-abba-be220ea4b2e1</pid><timestamp>1595405336190</timestamp><entitlements><entitlement><tag>regid.2017-02.com.cisco.UCM_CUWL.12.0_cc59375a-1cd8-4b36-8366-6f4d2abba965</tag><count>1</count><startDate>2020-Mar-04 UTC</startDate><endDate>2020-Aug-31 UTC</endDate><licenseType>TERM</licenseType><displayName>UC Manager CUWL License (12 X)</displayName><tagDescription>UC Manager CUWL License</tagDescription><subscriptionID></subscriptionID></entitlement><entitlement><tag>regid.2016-07.com.cisco.UCM_Enhanced.12.0_66d0d1cf-4863-4761-91d0-d01d3eb1949a</tag><count>1</count><startDate></startDate></endDate></endDate><licenseType>PERPETUAL</licenseType><displayName>UC Manager Enhanced License (12 X)</displayName><tagDescription>UC Manager Enhanced License</tagDescription><subscriptionID></subscriptionID></entitlement><entitlements></entitlements><authorizationCode><signature>MEQCIFDLpw4k+0O+Zr3bp/ucJ3KNyKVGdGumUVN0BuGyvi9JAIBcB60+c2GXA52FUIAIZdVhHz9xcVbbr/raWoavm9Hmw==</signature><udi>P-UCM,S.edb16,U.d9a2c661-8fe1-4ce7-9e6f-bbc68a3edb16</udi>"
Please enter the confirmation code to CSSM account:6f6f2f2f
admin:
```

450368

步骤 5 将确认码复制到 CSSM 并输入以完成预留更新。

Update License Reservation

STEP 1 ✓

Select Licenses

STEP 2 ✓

Review and confirm

STEP 3

Authorization Code



The Reservation Authorization Code below has been generated for this product instance. Several steps remain:

1. This code must be entered into the Product Instance's Smart Licensing settings to complete the reservation.
2. When the code has been entered, a Reservation Confirmation Code will be generated.
3. To release licenses in transition, enter confirmation code generated by device into CSSM.

Authorization Code:

```
<specificPLR><authorizationCode><flag>A</flag><version>C</version><pid>6191f5e5-319e-41ff-abba-be220ea4b2e1</pid><timestamp>1595405336190</timestamp><entitlements>
<entitlement><tag>regid.2017-02.com.cisco.UCM_CUWL.12.0_cc59375a-1cd8-4b36-8366-6f4d2abba965</tag><count>1</count><startDate>2020-Mar-04 UTC</startDate><endDate>2020-
Aug-31 UTC</endDate><licenseType>TERM</licenseType><displayName>UC Manager CUWL License (12 X)</displayName><tagDescription>UC Manager CUWL License</tagDescription>
<subscriptionID></subscriptionID><entitlement><tag>regid.2016-07.com.cisco.UCM_Enhanced.12.0_66d0d1cf-4863-4761-91d0-d01d3eb1949a</tag><count>1</count>
<startDate></startDate><endDate></endDate><licenseType>PERPETUAL</licenseType><displayName>UC Manager Enhanced License (12 x)</displayName><tagDescription>UC Manager
Enhanced License</tagDescription><subscriptionID></subscriptionID><entitlement><entitlements><authorizationCode><signature>MEQCFIDLpw4k+0O+Zr3p
/ucJ3KNyKVGdGumUvN0BuGyv9JAiBcB6O+c2GxAS2FUIAZdVhHz9xcVbbr/raWoavm9Hnw==</signature><udi>P:UCM,S:edb16,U:d9a2c661-8fe1-4ce7-9e6f-bbc68a3edb16</udi>
```

To learn how to enter this code, see the configuration guide for the product being licensed

Download as File

Copy to Clipboard

Enter Confirmation Code

Close

450362

license smart reservation cancel

在根据 CUCM 请求代码安装 Cisco Smart Software Manager 授权码之前，使用此程序可取消预留过程。

开始之前

按以下顺序执行命令，确保 Unified Communications Manager 注册状态为“正在预留”：

- license smart reservation enable
- license smart reservation request

过程

从 Cisco Unified CM 管理控制台执行以下 CLI 命令。

- license smart reservation cancel

license smart reservation return

此程序用于生成必须输入到 Cisco Smart Software Manager 中的退回代码，以便将许可证退回到虚拟帐户池，并从 CSSM 中删除产品实例。

开始之前

按以下顺序执行命令，确保 Unified Communications Manager 注册状态为注册特定的许可证预留：

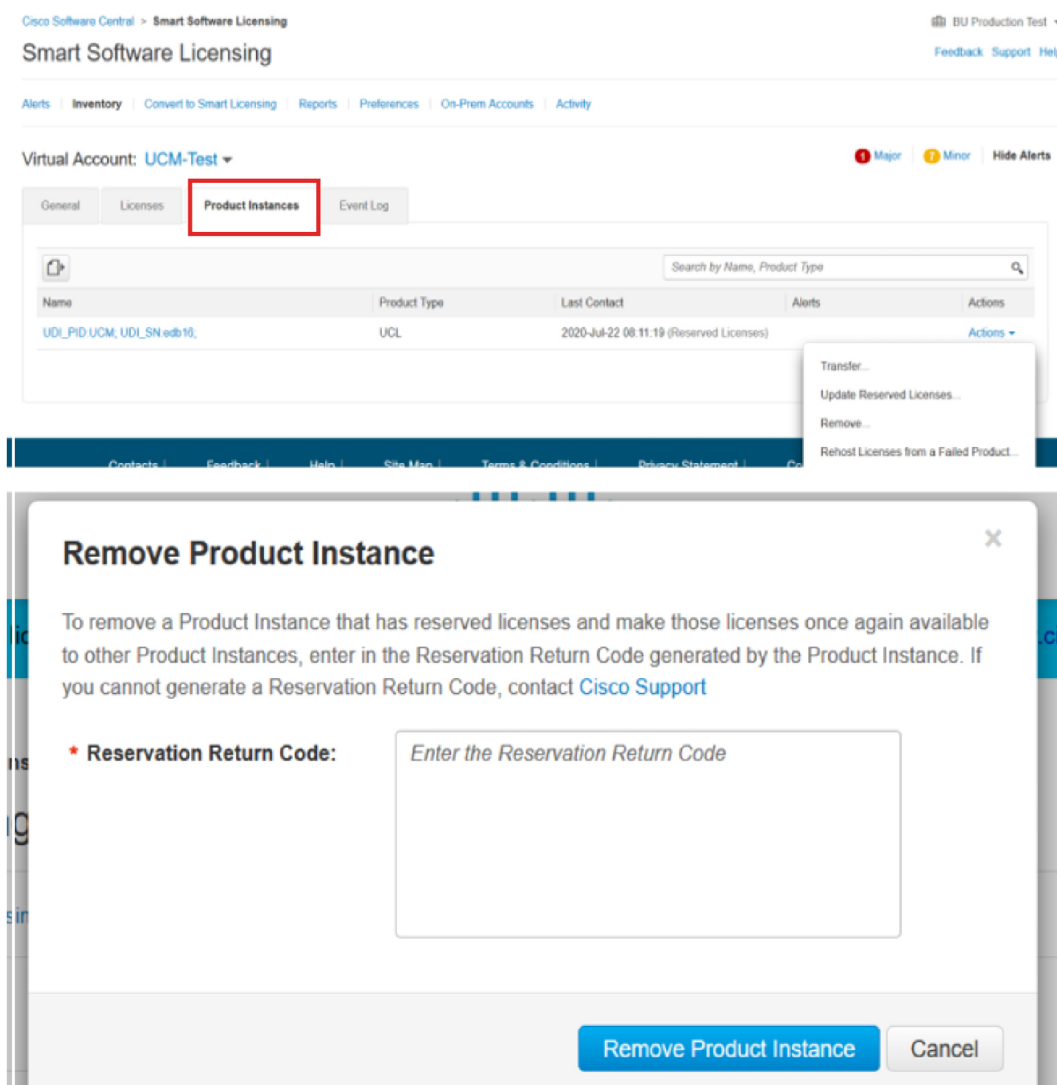
- **license smart reservation enable**
- **license smart reservation request**
- **license smart reservation install "<authorization-code>"**

过程

步骤 1 从 Cisco Unified CM 管理控制台执行许可证智能保留返回命令。

步骤 2 将保留返回代码复制到 CSSM 并删除产品实例。

license smart reservation return-authorization "<authorization-code>"



450360

license smart reservation return-authorization "<authorization-code>"

此程序用于为尚未安装的授权码生成返回代码。必须将返回代码输入到 Cisco Smart Software Manager 中，以将许可证退回到虚拟帐户池，并从 CSSM 中删除产品实例。

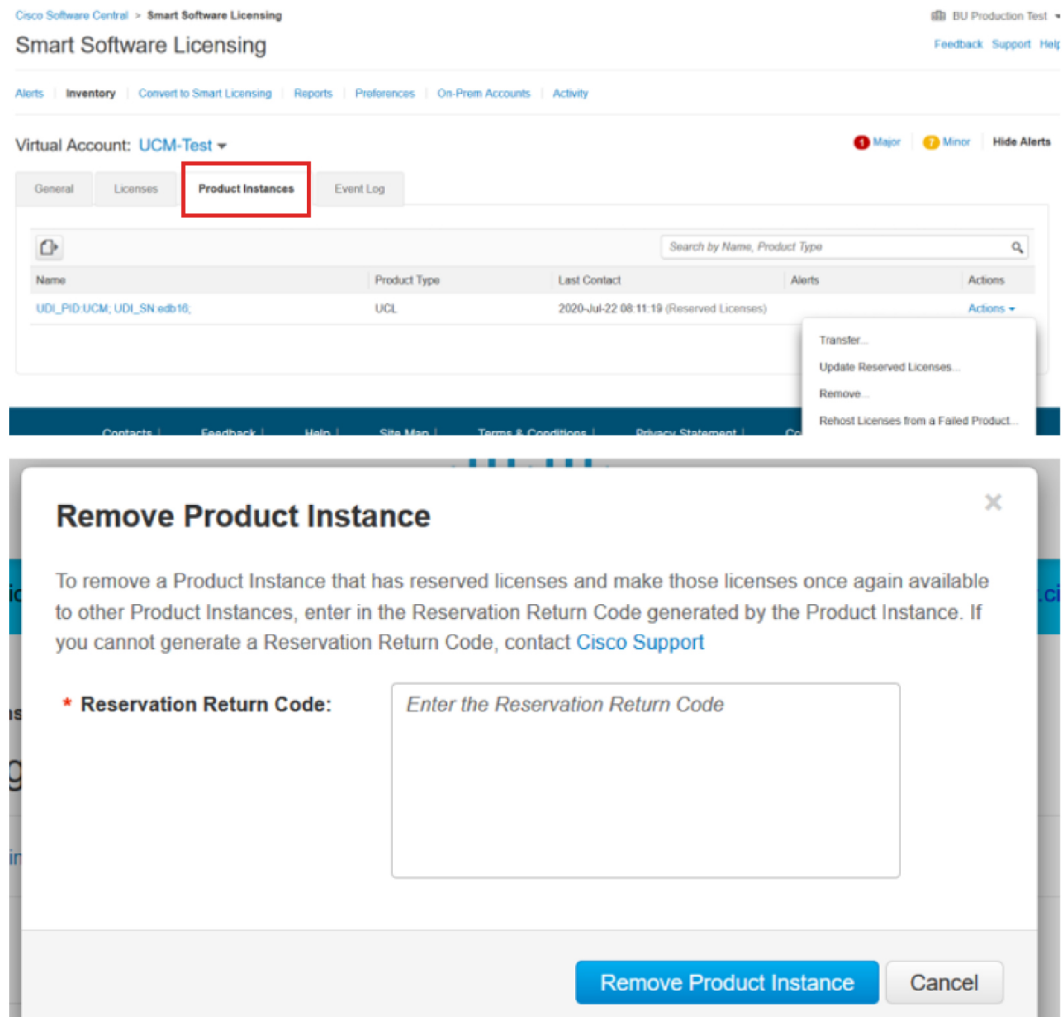
开始之前

按以下顺序执行命令，确保将 Unified Communications Manager 注册状态为“正在保留”：

- **license smart reservation enable**
- **license smart reservation request**

过程

- 步骤 1** 从 Cisco Unified CM 管理控制台执行 license smart reservation return-authorization "<authorization-code>" 命令。
- 步骤 2** 将保留返回代码复制到 CSSM 并删除产品实例。



450361

将已启用许可证预留的特定系统升级到版本 14

如果您将启用许可证预留的 12.5 Unified Communications Manager 系统升级到版本 14，则需要考虑以下情况：

1. 升级到版本 14 之前，使用 "license smart reservation return" 命令退回 12.x 许可证（推荐）。

或

升级到版本 14 之后，使用 "license smart reservation return" 命令退回 12.x 许可证。

2. 使用 "license smart reservation request" 命令创建请求代码。在 Cisco Smart Software Manager 中使用版本较少的许可证生成授权码。
3. 在 Cisco Unified Communications Manager 中使用 "license smart reservation install <auth-code>" 命令安装授权码。

不受版本限制的许可证

Unified Communications Manager 支持不受版本限制的用户许可证。许可证按年收费，并按订购期限签发。您可以通过 Flex EA（企业协议）或 Flex NU（指定用户—专业版、增强版、访问权限）订购这些 V14 许可证。有关详细信息，请参阅[订购指南](#)。

Unified Communications Manager 继续使用 12.X 版的许可证。

许可证在 CSSM (Cisco Smart Software Manager) 上管理。有关详细信息，请参阅[Cisco Unified Communications Manager 系统配置指南](#)中的“智能软件许可证”一章。

智能许可导出合规

“智能许可”提供一种方法，允许用户使用导出控制功能。在连接状态下，通过注册过程使用导出控制功能。在断开连接状态下，通过“智能许可证预订”使用导出控制功能。

此导出控制功能是面向具有智能帐户的客户的解决方案，对其应用了“导出限制”。此功能使得用户可以请求在 Cisco Smart Software Manager 或 satellite 中授予的监管导出许可证，并在 Cisco Unified Communications Manager 上启用导出受限功能。

以下选项介绍了导出控制功能的新增功能和设计元素：

- license smart export request local <exportfeaturename>
- license smart export return local <exportfeaturename>
- license smart export cancel

导出控制任务流程

完成以下任务可导出 Cisco Unified Communications Manager 的控制许可证。

license smart export request local <exportfeaturename>

此命令可让智能帐户受出口限制约束的用户从 Cisco Smart Software Manager 或 Satellite 申请监管出口许可证。

如果可在 Cisco Smart Software Manager 或 Satellite 上获得监管出口许可证，则命令将退回出口授权密钥，并在产品上启用出口受限功能。

开始之前

Cisco Unified Communications Manager 已在 Cisco Smart Software Manager 或 satellite 中注册。请确保 <CUCM Export Restricted Authorization Key> 许可证在 Cisco Smart Software Manager 上可用。

过程

从 Cisco Unified CM 管理控制台中，执行以下 CLI 命令：

- license smart export request local <exportfeaturename>
-

license smart export return local <exportfeaturename>

此命令允许将以前请求的导出限制许可证退回给 Cisco Smart Software Manager 或 satellite。导出限制功能的导出授权密钥将从系统中删除。

开始之前

系统会为此功能生成导出授权密钥。

过程

从 Cisco Unified CM 管理控制台中，执行以下 CLI 命令：

- license smart export return local <exportfeaturename>
-

license smart export cancel

此命令允许用户通过应用导出限制的智能帐户，取消之前失败的导出请求的自动重试，或从 Cisco Smart Software Manager 或 satellite 返回。

开始之前

Cisco Unified Communications Manager 已在 Cisco Smart Software Manager 或 satellite 中注册。

过程

从 Cisco Unified CM 管理控制台中，执行以下 CLI 命令：

- license smart export cancel
-



第 4 章

配置企业参数和服务

- [企业参数概述，第 33 页](#)
- [服务参数概述，第 33 页](#)
- [系统参数任务流程，第 34 页](#)

企业参数概述

企业参数提供适用于同一群集中所有设备和服务的默认设置。群集包含共享相同数据库的一组 Cisco Unified Communications Manager。安装新的 Cisco Unified Communications Manager 时，将使用企业参数设置其设备的初始默认值。

许多企业参数偶尔需要更改。但是，除非您完全了解要更改的功能，或者 Cisco 技术支持中心 (TAC) 指示更改，否则请勿更改企业参数。

建议的默认设置应该适用大多数情况。

- 设置 IP 电话的回退连接监听持续时间。
- 允许搜索所有用户的公司目录。
- 为组织的群集和顶级域设置完全限定目录号码 (FQDN)。
- 设置视频的 Cisco Jabber 启动条件。
- (可选) 如果网络使用 IPv6 则启用 IPv6。
- (可选) 输入远程系统日志服务器名称。
- (可选) 设置呼叫跟踪日志以对部署进行故障排除。
- (可选) 启用从属关系记录。

服务参数概述

服务参数可用于在所选的 Unified Communications Manager 服务器上配置不同的服务。与应用于所有服务的企业参数不同，每项服务都使用一组单独的服务参数配置。

服务参数可配置以下两种服务类型的设置，可以在 Cisco Unified 功能配置中激活这两种服务：

- **功能服务** - 这些服务用于运行某些系统功能。 您必须打开功能服务才可使用。
- **网络服务** - 网络服务默认是打开的，但您可以出于故障诊断目的停止和启动（或重新启动）网络服务。 这些服务包括让系统组件（例如数据库和平台）正常运行的服务。

单击**服务参数配置**窗口中的？图标，或者单击一个参数名称，可以查看服务参数的服务参数字段说明。



注释 如果您禁用服务，Unified Communications Manager 会保留所有更新的服务参数值。 如果再次启动服务，Unified Communications Manager 会将服务参数设置为更改的值。

系统参数任务流程

开始之前

设置您的 Unified Communications Manager 节点和端口设置。

过程

	命令或操作	目的
步骤 1	配置企业参数，第 34 页.	配置您的 Unified Communications Manager 节点初始设置所需的系统范围参数。
步骤 2	激活基本服务，第 39 页.	您可以使用 Cisco Unified 功能配置激活节点上的服务。
步骤 3	配置服务参数，第 42 页.	为群集中的发布方和订阅方节点配置服务参数。

配置企业参数

使用此程序可编辑您的部署的企业级参数。 您可以使用此功能设置企业级设置，例如组织顶级域或群集完全限定域名。



注释 如果在 Cisco Unified CM 管理中编辑参数，新设置也会在 Cisco Unified CM、IM and Presence 管理中反映。

过程

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

企业参数窗口将显示企业参数列表。

步骤 2 编辑任何参数设置。

有关参数说明，请单击 GUI 中的参数名称。有关通用企业参数列表的详细信息，请参阅 [通用企业参数，第 35 页](#)。

步骤 3 单击保存。

步骤 4 单击重置，然后单击确定重置所有设备。

注释 大多数参数要求您在保存设置后重置设备。如果您注册了设备，我们建议您在重置设备之前完成所有配置更改。

您可以在系统中重置每个设备池，以重置所有设备。

通用企业参数

下表列出了用于设置企业设置（例如组织顶层域或群集完全限定域名）的通用企业参数。有关详细列表，请使用 Cisco Unified CM 管理中的系统 > 企业参数菜单。

表 2: 初始 *Unified Communications Manager* 设置的通用企业参数

参数名称	说明
企业参数	
连接监视器持续时间	<p>如果群集中的 IP 电话注册在辅助节点上，则使用此参数设置时长，IP 电话将在主节点可用后等待所设定时间，然后回退并向主节点重新注册。此参数影响特定安全 Survivable Remote Site Telephony (SRST) 路由器的所有安全设备。</p> <p>有关详细信息，请参阅《<i>Cisco Unified Communications Manager</i> 安全指南》。</p> <p>默认值：120 秒</p> <p>重新启动所有服务以使更改生效。</p>
CCMAdmin 参数	

参数名称	说明
启用从属关系记录	<p>此参数用于显示故障排除所需的从属关系记录。在初始系统设置期间显示从属关系记录可能有益。</p> <p>显示从属关系记录可能会导致CPU使用达到高峰，可能会影响呼叫处理。为避免可能出现的性能问题，请在系统设置完成后禁用此参数。我们建议仅在非高峰时段或在维护期间显示从属关系记录。</p> <p>启用后，您可以从使用 Unified Communications Manager 的大多数配置窗口访问的相关链接下拉列表中选择从属关系记录。</p> <p>默认值：False</p>
用户数据服务参数	
启用所有用户搜索	<p>此参数可让您在未指定姓氏、名字或目录号码的情况下，在公司目录中搜索所有用户。此参数也适用于 Cisco CallManager 自助 (CCMUser) 窗口中的目录搜索。</p> <p>默认值：True</p>
集群范围内的域配置	
组织顶级域	<p>此参数定义组织的顶级域。例如 cisco.com。</p> <p>最大长度：255 个字符</p> <p>允许的值：使用大小写字母、数字 (0-9)、连字符和点（作为域标签分隔符）的有效域。域标签不得以连字符开头。最后一个标签不得以数字开头。例如，--cisco.lom 这个域无效。</p>
群集完全限定域名	<p>此参数定义群集的一个或多个完全限定域名 (FQDN)。多个 FQDN 必须用空格分隔。在 FQDN 中使用星号 (*) 指定通配符。示例： cluster-1.cisco.com *.cisco.com。</p> <p>SIP 呼叫等包含 URL 的请求，其主机部分与此参数中的任何 FQDN 相匹配，都将路由到该群集及所连接的设备。</p> <p>最大长度：255 个字符</p> <p>允许的值：FQDN 或使用 * 通配符的部分 FQDN。大小写字母、数字 (0-9)、连字符和点号（作为域标签分隔符）。域标签不得以连字符开头。最后一个标签不得以数字开头。例如，--cisco.lom 这个域无效。</p>
IPv6	

参数名称	说明
启用 IPv6	<p>此参数确定 Unified Communications Manager 是否可以协商 Internet 协议版本 6 (IPv6) 以及是否允许电话通告 IPv6 功能。</p> <p>必须先在所有其他网络组件（包括所有节点的平台）上启用 IPv6，然后才能启用此参数。否则，系统将继续在仅 IPv4 模式下运行。</p> <p>这是必填字段。</p> <p>默认值：假（禁用 IPv6）</p> <p>您必须重新启动以下服务以使 IPv6 参数更改生效，以及 IM and Presence Service 群集中受影响的服务。</p> <ul style="list-style-type: none"> • Cisco CallManager • Cisco IP 语音媒体流应用程序 • Cisco CTIManager • Cisco 证书权限代理功能
Cisco Syslog 代理	
远程系统日志服务器 1	<p>输入远程系统日志服务器的名称或 IP 地址。如果未指定服务器名称，Cisco Unified 功能配置不会发送系统日志消息。只有当您为日志使用系统日志服务器时，才需要此参数。</p> <p>最大长度：255 个字符</p> <p>允许的值：使用大小写字母、数字 (0-9)、连字符和点的有效远程系统日志服务器名称。</p> <p>不要将另一个 Unified Communications Manager 节点指定为目标。</p>
Cisco Jabber	
从不使用视频启动视频	<p>此参数确定视频呼叫启动时是否发送视频。选择真将启动视频呼叫而不立即发送视频。在视频呼叫期间的任何时候，您都可以选择开始发送视频。</p> <p>此参数将覆盖任何 IM and Presence Service 首选项。设置为“假”时，视频呼叫根据 IM and Presence Service 中设置的首选项启动。</p> <p>默认值：假。</p>
SSO 和 OAuth 配置	

参数名称	说明
适用于 iOS 的 SSO 登录行为	<p>必须设置此参数以允许 Cisco Jabber 在受控的移动设备管理 (MDM) 部署中使用 IdP 执行基于证书的验证。</p> <p>iOS 的 SSO 登录行为 (SSO Login Behavior for iOS) 参数包括以下选项：</p> <ul style="list-style-type: none"> • 使用嵌入式浏览器—如果启用此选项，Cisco Jabber 会使用嵌入式浏览器进行 SSO 验证。使用此选项可允许版本 9 之前的 iOS 设备使用 SSO 而无需交叉启动进入本机 Apple Safari 浏览器。 • 使用本机浏览器—如果启用此选项，Cisco Jabber 会在 iOS 设备上使用 Apple Safari 框架，在 MDM 部署中使用身份提供程序 (IdP) 执行基于证书的验证。 <p>注释 我们建议不要配置此选项，除了在受控的 MDM 部署中，因为使用本机浏览器不如使用嵌入式浏览器安全。</p> <p>这是必填字段。</p> <p>默认值：使用嵌入式浏览器 (WebView)。</p>
OAuth with Refresh Login Flow	<p>此参数控制 Cisco Jabber 等客户端在连接到 Unified Communications Manager 时使用的登录流程。</p> <ul style="list-style-type: none"> • 启用—如果启用此选项，客户端可以使用基于 OAuth 的快速登录流程提供更快、简化的登录体验，无需用户输入即可重新登录。例如，由于网络更改。此选项需要来自 Unified Communications 解决方案的其他组件的支持，例如 Expressway 和 Unity Connection（启用了刷新登录流程的兼容版本）。 • 禁用—如果您启用此选项，现有行为将被保留，并且与其他系统组件的旧版本兼容。 <p>注释 对于使用 Cisco Jabber 的移动和远程访问部署，我们建议仅对支持 OAuth with Refresh login flow 的 Expressway 兼容版本启用此参数。不兼容的版本可能会影响 Cisco Jabber 功能。有关受支持版本和配置要求的信息，请参阅具体的产品文档。</p> <p>重要事项 此功能适用于 12.5(1)SU7 和 14SU3 及更高版本。</p> <p>除了发布方之外，订阅方节点还可以访问请求方节点数据库上的更新刷新令牌，并且在整个群集中将重复相同的操作。</p> <p>这是必填字段。</p> <p>默认设置：禁用。</p>

参数名称	说明
为 RTMT 使用 SSO	<p>此参数配置为对实时监控工具 (RTMT) 启用 SAML SSO。</p> <p>为 RTMT 使用 SSO 参数包括以下选项：</p> <ul style="list-style-type: none"> • 真—如果选择此选项，RTMT 会显示基于 SAML SSO 的 IdP 登录窗口。 <p>注释 当您执行全新安装时，为 RTMT 使用 SSO 参数的默认值显示为真。</p> <ul style="list-style-type: none"> • 假—如果选择此选项，RTMT 会显示基本验证登录窗口。 <p>注释 当您从不存在为 RTMT 使用 SSO 参数的 Cisco Unified Communications Manager 版本执行升级时，在新版本中此参数的默认值显示为假。</p> <p>这是必填字段。</p> <p>默认值：真。</p>

激活基本服务

使用此程序可激活整个群集中的服务。

有关发布方节点和订阅方节点的建议服务列表，请参阅以下主题：

- [针对发布方节点的建议服务，第 40 页](#)
- [针对订阅方节点的建议服务，第 41 页](#)

过程

步骤 1 从 Cisco Unified 功能配置中，选择工具 > 服务激活。

步骤 2 从下拉菜单中选择一个**服务器**，然后单击前往。

服务及其当前状态将会显示。

步骤 3 激活和取消激活所需的服务：

- 要激活服务，请选中您要激活的服务旁边的复选框。
- 要停用服务，请取消选中要停用的服务旁边的复选框。

步骤 4 单击**保存**。

服务激活可能需要几分钟的时间才能完成。刷新页面以确认状态更改。

针对发布方节点的建议服务

下表列出了使用非专用 TFTP 服务器时为 Unified Communications Manager 发布方节点推荐的服务。

表 3: 针对非专用 TFTP 服务器部署的建议发布方节点服务

类型	服务名称
CM 服务	Cisco CallManager
	Cisco Unified 移动语音访问服务
	Cisco IP 语音媒体流应用程序
	Cisco CTIManager
	Cisco 扩展功能
	Cisco 群集间查询服务
	Cisco 位置带宽管理器
	Cisco TFTP
CTI 服务	Cisco IP Manager Assistant
	Cisco WebDialer Web 服务
CDR 服务	Cisco SOAP - CDRonDemand 服务
	Cisco CAR Web 服务
数据库和管理服务	Cisco 批量预配置服务
	AXL Web 服务
	Cisco URL Web 服务
性能和监控服务	Cisco 功能配置报告程序
	Cisco 证书权限代理功能
目录服务	Cisco DirSync



提示 如果您不打算使用以下服务，可以安全地将其禁用：

- Cisco Messaging 接口
- Cisco DHCP 监控器服务
- Cisco TAPS 服务
- 思科电话号码别名同步 (Cisco Directory Number Alias Sync)
- 思科拨号号码分析器服务器 (Cisco Dialed Number Analyzer Server)
- Cisco 被叫号码分析器
- 自行调配 IVR (Self Provisioning IVR)

针对订阅方节点的建议服务

下表列出了使用非专用 TFTP 服务器时为 Unified Communications Manager 订阅方节点推荐的服务。



提示 如果您不打算使用其他服务，可以安全地将其禁用。

表 4: 针对非专用 TFTP 服务器部署的建议订阅方节点服务

类型	服务名称
CM 服务	Cisco CallManager
	Cisco IP 语音媒体流应用程序
	Cisco CTIManager
	Cisco Extension Mobility
	Cisco 扩展功能
	Cisco TFTP

您必须在群集中的每个 IM and Presence Service 节点上激活以下服务。

- Cisco SIP Proxy
- Cisco Presence Engine
- Cisco XCP 连接管理器
- Cisco XCP 验证服务

配置服务参数

您可以使用 Cisco Unified Communications Manager 管理 在节点上配置服务参数。标记为群集范围的服务参数会影响群集中的所有节点。



注意 对服务参数的某些更改可能会导致系统失败。我们建议您不要对服务参数做任何更改，除非您完全了解要更改的功能，或者 Cisco 技术支持中心 (TAC) 指定更改。

开始之前

- 确保 Unified Communications Manager 节点已配置。
- 确保该服务处于活动状态。有关详细信息，请参阅[激活基本服务](#)，第 39 页。

过程

步骤 1 从 Cisco Unified CM 管理中，选择 **选择系统 > 服务参数**。

步骤 2 在 **服务器** 下拉列表中选择 一个节点。

步骤 3 在 **服务** 下拉列表中选择 一个服务。

提示 单击 **服务参数配置** 窗口中的 (?) 图标可查看服务参数列表及其说明。

步骤 4 单击 **高级** 以查看参数的完整列表。

步骤 5 修改服务参数，然后单击 **保存**。

窗口将会刷新，并且服务参数值将会更新。

您可以单击 **设为默认设置** 按钮将所有参数更新为 **参数值** 字段后显示的建议值。如果参数没有建议值，则当您单击 **设为默认设置** 按钮时，服务参数值不会变化。

查看群集范围的服务参数设置

您可以使用 Cisco Unified Communications Manager Assistant 和 Cisco Unified 功能配置查看群集中节点的服务状态。要查看服务参数设置和参数说明，请使用 Cisco Unified Communications Manager Assistant。

过程

步骤 1 要使用显示服务和查看节点的服务参数设置 Cisco Unified Communications Manager Assistant，请执行以下步骤。

- a) 选择 **系统 > 服务参数**。
- b) 在 **服务参数配置** 窗口中，从 **服务器** 下拉列表中选择 一个节点。

- c) 在**服务**下拉框中选择一项服务。

适用于所选节点的所有参数将会显示。在**群集范围参数（常规）**部分中显示的参数适用于群集中的所有节点。

- d) 单击**服务参数配置**窗口中的 (?) 图标可查看服务参数列表及其说明。

步骤 2 要在群集中的所有节点上显示特定服务的服务参数，请在**服务参数配置**窗口的**相关链接**下拉框中选择**所有服务器的参数**，然后单击前往。

所有服务器的参数窗口将会显示。您可以单击列出的服务器名称或参数值打开相关的**服务参数配置**窗口。

步骤 3 要在群集中的所有节点上显示特定服务的不同步服务参数，请在**所有服务器的参数**窗口的**相关链接**下拉框中选择**所有服务器的不同步参数**，然后单击前往。

所有服务器的不同步参数窗口将会显示。您可以单击列出的服务器名称或参数值打开相关的**服务参数配置**窗口。



第 5 章

配置 IPv6 堆栈

- [IPv6 堆栈概述，第 45 页](#)
- [IPv6 前提条件，第 46 页](#)
- [IPv6 配置任务流程，第 46 页](#)

IPv6 堆栈概述

IPv6 是一个扩展 IP 寻址协议，使用 128 位而不是 IPv4 地址使用的 32 位。IPv6 提供的 IP 地址范围比 IPv4 更广，这大大降低了 IP 地址耗尽的风险，而这是 IPv4 寻址的主要问题之一。

默认情况下，Cisco Unified Communications Manager 配置为使用 IPv4 寻址。不过，您也可以将系统配置为支持 IPv6 堆栈，从而允许您部署具有仅 IPv6 终端的 SIP 网络。除了降低 IP 地址耗尽风险之外，IPv6 还提供以下优点：

- 无状态地址自动配置
- 简化组播功能
- 简化路由，最大限度地减少对路由表的需求
- 服务交付优化
- 更好的移动处理
- 更强的隐私和安全性

系统级 IPv6

如果您部署 IPv6 网络，则 Cisco Unified Communications Manager 服务器仍对某些内部通信使用 IPv4。这是因为某些内部系统组件和应用程序仅支持 IPv4。因此，即使所有设备都在仅 IPv6 模式下运行，Cisco Unified Communications Manager 服务器仍将有 IPv4 和 IPv6 地址，因为对于某些内部通信，服务器必须使用 IPv4。



注释 如果您需要 SIP 设备在 IPv4 和 IPv6 网络中运行，您将需要配置双堆栈。在完成本章中的任务以在 Cisco Unified Communications Manager 中启用 IPv6 堆栈后，您还必须为两个堆栈启用 SIP 网络。请参阅 [双堆栈（IPv4 和 IPv6）概述，第 51 页](#)。

IPv6 前提条件

在使用 IPv6 支持配置 Cisco Unified Communications Manager 之前，必须将以下网络服务器和设备配置为支持 IPv6。有关详细信息，请参阅设备用户文档：

- 预配置支持 IPv6 的 DHCP 和 DNS 服务器。Cisco Network Registrar 服务器支持 DHCP 和 DNS 的 IPv6。
- 配置支持 IPv6 的网络设备（例如网关、路由器和 MTP）的 IOS。
- 配置您的 TFTP 服务器以运行 IPv6。

IPv6 配置任务流程

完成以下任务以配置适用于 IPv6 的系统。

过程

	命令或操作	目的
步骤 1	在操作系统中配置 IPv6，第 47 页	配置支持 IPv6 地址的操作系统。
步骤 2	为 IPv6 配置服务器，第 47 页	使用 IPv6 地址配置群集中的服务器。
步骤 3	启用 IPv6，第 48 页	配置为 IPv6 启用系统的企业参数。
步骤 4	执行以下任何操作： <ul style="list-style-type: none">• 配置群集的 IP 寻址首选项，第 48 页• 配置设备的 IP 寻址首选项，第 49 页	您可以配置企业参数以分配群集范围 IP 寻址首选项。 如果要为不同的终端组分配不同的首选项，请在通用设备配置中配置寻址首选项。 配置首选 IP 寻址方法的群集设置。
步骤 5	重新启动服务，第 49 页	重新启动以下网络服务： <ul style="list-style-type: none">• Cisco CallManager• Cisco CTIManager• Cisco IP 语音媒体流应用程序

命令或操作	目的
	• Cisco 证书权限代理功能

下一步做什么

要配置双堆栈干线，请参阅配置 SIP 干线的章节。

要配置 SIP 设备的双堆栈，请参阅您要配置的 SIP 设备部分。

在操作系统中配置 IPv6

使用此程序在 Cisco Unified 操作系统管理中设置以太网 IPv6。



注释 使用 Cisco IOS IPv6 DHCP 服务器，因为 Windows 上不支持 IPv6 DHCP 服务器配置。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**设置 > IPv6 > 以太网**。

步骤 2 选中**启用 IPv6**复选框。

步骤 3 从**地址来源**下拉列表框中，配置系统获取 IPv6 地址的方式：

- **路由器通告**—系统使用无状态自动配置来获取 IPv6 地址。
- **DHCP**—系统从 DHCP 服务器获取 IPv6 地址。
- **手动输入**—如果要手动输入 IPv6 地址，请选择此选项。

步骤 4 如果您已将手动输入配置为获取 IPv6 地址的方式，请填写以下字段：

- 输入 **IPv6 地址**。例如， **fd62:6:96:21e:bff:fecc:2e3a**。
- 输入 **IPv6 掩码**。例如， **64**。

步骤 5 选中**通过重新启动更新**复选框，以确保系统在您保存后重新启动。

步骤 6 单击**保存**。

为 IPv6 配置服务器

使用 IPv6 地址配置群集中的服务器。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**系统 > 服务器**。

步骤 2 在 **IPv6 地址**（适用于双 **IPv4/IPv6**）字段中，输入以下值之一：

- 如果您已配置了 DNS，并且 DNS 服务器支持 IPv6，请输入服务器主机名。
- 否则，请输入非链路本地 IPv6 地址。

步骤 3 单击保存。

步骤 4 为每个群集节点上重复这些步骤。

启用 IPv6

如果要在系统中设置 IPv6 支持，必须让系统支持 IPv6 设备。

过程

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

步骤 2 将启用 **IPv6** 企业参数的值设置为真。

步骤 3 单击保存。

下一步做什么

为群集中的设备配置 IP 寻址首选项。您可以通过群集范围企业参数应用设置，也可以使用通用设备配置将设置应用到使用该配置的设备组：

- [配置群集的 IP 寻址首选项，第 48 页](#)
- [配置设备的 IP 寻址首选项，第 49 页](#)

配置群集的 IP 寻址首选项

此程序用于使用企业参数配置群集范围内用于 IPv6 的 IP 寻址首选项。系统会将这些设置应用到所有 SIP 干线和设备，除非将覆盖的通用设备配置应用到特定的干线或设备。



注释 通用设备配置中的 IP 地址首选项将覆盖使用该通用设备配置的设备的群集范围企业参数设置。

过程

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

步骤 2 将媒体的 **IP 寻址模式**首选项企业参数的值设置为 **IPv4** 或 **IPv6**

步骤 3 将信令的 **IP 寻址模式**首选项企业参数的值设置为 **IPv4** 或 **IPv6**。

步骤 4 单击保存。

配置设备的 IP 寻址首选项

通过使用首选项设置配置通用设备配置，您可以配置各设备的 IP 寻址首选项。您可以将通用设备配置应用到支持 IPv6 寻址的 SIP 和 SCCP 设备，例如干线、电话、会议桥和转码器。



注释 通用设备配置中的 IP 地址首选项将覆盖使用该通用设备配置的设备的群集范围企业参数设置。

过程

步骤 1 从 Cisco Unified CM 管理中，选择设备 > 设备设置 > 通用设备配置。

步骤 2 单击新增。

步骤 3 对于 SIP 干线、SIP 电话或 SCCP 电话，从 **IP 寻址模式** 下拉列表中选择一个值：

- **仅 IPv4**—对于媒体和信令，设备仅使用 IPv4 地址。
- **仅 IPv6**—对于媒体和信令，设备仅使用 IPv6 地址。
- **IPv4 和 IPv6（默认）**—设备为双堆栈设备，并使用任何可用的 IP 地址类型。如果设备上配置了两种 IP 地址类型，则对于信令，设备使用用于信令的 **IP 寻址模式首选项** 设置，对于媒体，设备使用用于媒体的 **IP 寻址模式首选项** 企业参数。

步骤 4 如果您在上一步中配置 IPv6，则为用于信令的 **IP 寻址模式** 下拉列表配置 IP 寻址首选项：

- **IPv4**—双堆栈设备首选 IPv4 地址进行信令。
- **IPv6**—双堆栈设备首选 IPv6 地址进行信令。
- **使用系统的默认值**—设备将该设置用于用于信令的 **IP 寻址模式首选项** 企业参数。

步骤 5 配置通用设备配置窗口中的其余字段。有关字段及其配置选项的更多信息，请参阅系统联机帮助。

步骤 6 单击保存。

下一步做什么

如果您的 IPv6 配置已完成，则[重新启动服务](#)，第 49 页。

如果想要您的 SIP 设备同时支持 IPv4 和 IPv6 网络，则必须配置系统以在设备级别支持两个堆栈。有关详细信息，请参阅[双堆栈（IPv4 和 IPv6）概述](#)，第 51 页。

重新启动服务

为 IPv6 配置系统后，重新启动基本服务。

过程

步骤 1 登录到 Cisco Unified 功能配置并选择工具 > 控制中心 - 功能服务。

步骤 2 选中与以下每项服务对应的复选框：

- Cisco CallManager
- Cisco CTIManager
- Cisco 证书权限代理功能
- Cisco IP 语音媒体流应用程序

步骤 3 单击重新启动。

步骤 4 单击确定。



第 6 章

配置双堆栈（IPv4 和 IPv6）

- [双堆栈（IPv4 和 IPv6）概述，第 51 页](#)
- [双堆栈（IPv4 和 IPv6）前提条件，第 51 页](#)
- [双堆栈（IPv4 和 IPv6）配置任务流程，第 51 页](#)

双堆栈（IPv4 和 IPv6）概述

如果您的 SIP 网络同时配置了 IPv4 和 IPv6 堆栈，SIP 设备可以处理以下每种场景的呼叫：

- 呼叫中的所有设备仅支持 IPv4
- 呼叫中的所有设备仅支持 IPv6
- 呼叫中的所有设备同时支持 IPv4 和 IPv6 堆栈。在此场景中，系统依据适用于信令事件的用于信令的 **IP 寻址模式首选项** 设置和适用于媒体事件的用于媒体的 **IP 寻址模式首选项** 企业参数的配置，确定 IP 地址类型。
- 一个设备仅支持 IPv4，而另一个设备仅支持 IPv6。在此场景中，Unified Communications Manager 将 MTP 插入到呼叫路径中，以在两个寻址类型之间转换信令。

对于 SIP 设备和干线，您可以通过配置备用网络地址类型 (ANAT) 启用双堆栈支持。当 ANAT 应用到 SIP 设备或干线时，则设备或干线发送的 SIP 信令同时包含 IPv4 和 IPv6 地址（如果都可用）。ANAT 允许终端在仅 IPv4 和仅 IPv6 网络中无缝地互操作。

双堆栈（IPv4 和 IPv6）前提条件

您必须先配置 Cisco Unified Communications Manager 以支持 IPv6 堆栈（IPv4 默认为启用）。这包括设置媒体和信令的 IP 寻址首选项。有关配置详细信息，请参阅 [IPv6 配置任务流程，第 46 页](#)。

双堆栈（IPv4 和 IPv6）配置任务流程

完成以下任务以配置 SIP 设备和干线同时支持 IPv4 和 IPv6 寻址。

过程

	命令或操作	目的
步骤 1	为 SIP 配置文件配置 ANAT，第 52 页	配置同时支持 IPv4 和 IPv6 堆栈的 SIP 配置文件。
步骤 2	将 ANAT 应用于 SIP 电话，第 52 页	将启用 ANAT 的 SIP 配置文件应用到 SIP 电话。这将允许 SIP 电话同时支持 IPv4 和 IPv6 堆栈。
步骤 3	将 ANAT 应用到 SIP 干线，第 53 页	将启用 ANAT 的 SIP 配置文件应用到 SIP 干线。这将允许干线同时支持 IPv4 和 IPv6 堆栈。
步骤 4	重新启动服务，第 53 页	将系统配置为同时支持 IPv4 和 IPv6 堆栈后，重新启动基本服务。

为 SIP 配置文件配置 ANAT

此程序用于配置支持备用网络地址类型 (ANAT) 的 SIP 配置文件。使用此配置文件的 SIP 设备和干线可以在仅 IPv4 与仅 IPv6 网络之间进行无缝互操作。

过程

步骤 1 从“Cisco Unified CM 管理”中，选择设备 > 设备设置 > SIP 配置文件。

步骤 2 执行下列操作之一：

- 单击**新增**以创建新的 SIP 配置文件。
- 单击**查找**并选择现有的 SIP 配置文件。

步骤 3 选中启用 ANAT 复选框。

步骤 4 完成 SIP 配置文件配置窗口中其余字段的设置。有关字段及其配置选项的更多信息，请参阅系统联机帮助。

步骤 5 单击保存。

您必须将 SIP 配置文件应用到 SIP 电话或 SIP 干线，以使这些设备能够同时支持 IPv4 和 IPv6 堆栈。

将 ANAT 应用于 SIP 电话

使用此程序将备用网络地址类型 (ANAT) 配置应用到 SIP 电话。启用 ANAT 后，电话可以同时与仅 IPv4 和仅 IPv6 网络通信。

过程

步骤 1 从 Cisco Unified CM 管理中，选择设备 > 电话。

步骤 2 单击查找并选择现有电话。

步骤 3 从 **SIP 配置文件** 下拉列表框中选择您启用了 ANAT 的 SIP 配置文件。

步骤 4 完成电话配置窗口中其余字段的设置。有关字段及其配置选项的更多信息，请参阅系统联机帮助。

步骤 5 单击保存。

将 ANAT 应用到 SIP 干线

此程序用于将备用网络地址类型配置应用到现有的 SIP 干线。这将允许 SIP 干线同时支持 IPv4 和 IPv6 堆栈。



注释 有关 SIP 干线配置选项的详细信息，请参阅[配置 SIP 干线](#)，第 89 页。

过程

步骤 1 从 Cisco Unified CM 管理中，选择设备 > 干线。

步骤 2 单击查找并选择现有的 SIP 干线。

步骤 3 从 **SIP 配置文件** 下拉列表框中选择您启用了 ANAT 的 SIP 配置文件。

步骤 4 完成干线配置窗口中其余字段的设置。有关字段及其配置选项的更多信息，请参阅系统联机帮助。

步骤 5 单击保存。

重新启动服务

将系统配置为同时支持 IPv4 和 IPv6 堆栈后，重新启动基本服务。

过程

步骤 1 登录到 Cisco Unified 功能配置并选择工具 > 控制中心 - 功能服务。

步骤 2 选中与以下每项服务对应的复选框：

- Cisco CallManager
- Cisco CTIManager
- Cisco 证书权限代理功能
- Cisco IP 语音媒体流应用程序

步骤 3 单击重新启动。

步骤 4 单击确定。



第 7 章

配置基本的安全性

- [关于安全配置，第 55 页](#)
- [安全配置任务，第 55 页](#)

关于安全配置

本节提供设置 Cisco Unified Communications Manager 必须执行的基本安全配置任务的相关信息。

安全配置任务

执行以下任务以设置基本安全配置：

- [为群集启用混合模式，第 55 页](#)
- [下载证书，第 56 页](#)
- [生成证书签名请求，第 56 页](#)
- [下载证书签名请求，第 56 页](#)
- [上传第三方 CA 的根证书，第 57 页](#)
- [设置最低 TLS 版本，第 58 页](#)
- [设置 TLS 密码，第 58 页](#)

为群集启用混合模式

使用此程序可在群集中启用混合模式。

过程

步骤 1 登录到发布方节点上的命令行界面。

步骤 2 运行 `utils ctl set-cluster mixed-mode` CLI 命令。

注释 确保 Communications Manager 已注册到 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite，并且从智能帐户或虚拟帐户收到的注册令牌允许在注册此群集时启用导出受控功能。

下载证书

提交 CSR 请求时，使用下载证书任务复制证书或上传证书。

过程

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

步骤 2 指定搜索条件，然后单击查找。

步骤 3 选择所需的文件名，然后单击下载。

生成证书签名请求

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



注释 如果您生成新的 CSR，将覆盖任何现有的 CSR。

过程

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

步骤 2 单击生成 CSR。

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

步骤 4 单击生成。

下载证书签名请求

下载所生成的 CSR 并准备好将其提交给您的证书颁发机构。

过程

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

步骤 2 单击下载 CSR。

步骤 3 从证书目的下拉列表中选择证书名称。

步骤 4 单击下载 CSR。

步骤 5 （可选）如果收到提示，请单击保存。

上传第三方 CA 的根证书

将 CA 根证书上传到 CAPF-trust 存储区，Unified Communications Manager 信任存储区使用外部 CA 签名 LSC 证书。



注释 如果您不想使用第三方 CA 签名 LSC，请跳过此任务。

过程

步骤 1 从 Cisco Unified OS 管理中，选择安全 > 证书管理。

步骤 2 单击上传证书/证书链。

步骤 3 从证书用途下拉列表，选择 CAPF-trust。

步骤 4 输入证书说明。例如，适用于外部 LSC 签名 CA 的证书。

步骤 5 单击浏览，导航至文件，然后单击打开。

步骤 6 单击上传。

步骤 7 重复此任务，将证书上传到 callmanager-trust 证书用途。

TLS 前提条件

在配置最低 TLS 版本之前，请确保您的网络设备和应用程序都支持 TLS 版本。此外，请确保您启用了要使用 Unified Communications Manager 和 IM and Presence Service 配置的 TLS。如果您部署了以下任何产品，请确认它们符合最低 TLS 要求。如果它们不符合这一要求，请升级这些产品：

- 信令客户端控制协议 (SCCP) 会议桥
- 转码器
- 硬件媒体终结点 (MTP)
- SIP 网关

- Cisco Prime Collaboration Assurance
- Cisco Prime Collaboration Provisioning
- 思科 Prime 协作部署
- Cisco Unified 边界组件 (CUBE)
- Cisco Expressway
- Cisco TelePresence Conductor

您将无法升级会议桥、媒体终结点 (MTP)、Xcoder、Prime Collaboration Assurance 和 Prime Collaboration Provisioning。



注释 如果您是从较早版本的 Unified Communications Manager 升级，请确保所有设备和应用程序都支持较高版本的 TLS，然后再进行配置。例如，Unified Communications Manager 和 IM and Presence Service 版本 9.x 仅支持 TLS 1.0。

设置最低 TLS 版本

默认情况下，Unified Communications Manager 支持的最低 TLS 版本为 1.0。使用此程序可将 Unified Communications Manager 和 IM and Presence Service 支持的最低 TLS 版本重置为较高的版本，例如 1.1 或 1.2。

确保网络中的设备和应用程序支持您要配置的 TLS 版本。有关详细信息，请参阅[TLS 前提条件](#)，第 57 页。

过程

步骤 1 登录到命令行界面。

步骤 2 要确认现有 TLS 版本，请运行 **show tls min-version** CLI 命令。

步骤 3 运行 **set tls min-version<minimum>** CLI 命令，其中 *<minimum>* 代表 TLS 版本。

例如，运行 **set tls min-version 1.2** 将最低 TLS 版本设置为 1.2。

步骤 4 在所有 Unified Communications Manager 和 IM and Presence Service 服务群集节点上执行步骤 3。

设置 TLS 密码

您可以通过为 SIP 接口选择可用的最强密码来禁用弱密码。使用此程序配置 Unified Communications Manager 支持用于建立 TLS 连接的密码。

过程

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

步骤 2 在安全参数中，配置 **TLS 密码** 企业参数的值。有关可用选项的帮助，请参阅企业参数联机帮助。

步骤 3 单击保存。

注释 所有 TLS 密码将根据客户端密码首选项进行协商



第 8 章

配置单点登录

- [关于 SAML SSO 解决方案，第 61 页](#)
- [SAML SSO 配置任务流程，第 62 页](#)

关于 SAML SSO 解决方案



重要事项 如果 Cisco Jabber 部署为采用 Cisco Webex Meeting Server，则 Unified Communications Manager 和 Webex Meeting Server 必须位于相同的域中。

SAML 是基于 XML 的开放标准数据格式，可让管理员在登录到其中一个应用后能够无缝访问定义的一组 Cisco 协作应用。SAML 描述了受信任的业务合作伙伴之间安全相关信息的交换。它是服务提供程序（例如 Unified Communications Manager）用来验证用户的一种验证协议。SAML 实现了身份提供程序 (IdP) 和服务提供程序之间安全身份验证信息的交换。

SAML SSO 使用 SAML 2.0 协议为 Cisco 协作解决方案提供跨域和跨产品单点登录。SAML 2.0 实现了跨 Cisco 应用程序的 SSO 并实现了 Cisco 应用程序和 IdP 之间联盟。SAML 2.0 允许 Cisco 管理用户访问安全的 web 域，以便在维护高安全性级别的同时在 IdP 与服务提供程序之间交换用户身份验证和授权数据。该功能提供安全机制来跨各种应用程序使用通用凭证和相关信息。

SAML SSO 管理员访问授权基于在 Cisco 协作应用程序上本地配置的基于角色的访问控制 (RBAC)。

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



重要事项 服务提供程序不再参与身份验证。SAML 2.0 将身份验证从服务提供程序委托给 Idp。

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

SAML SSO 配置任务流程

完成这些任务以为 SAML SSO 配置 Unified Communications Manager。

开始之前

SAML SSO 配置要求您在配置 Unified Communications Manager 的同时配置身份提供程序 (IdP)。有关 IdP 特定的配置示例，请参阅：

- [Active Directory Federation Services](#)
- [Okta](#)
- [Open Access Manager](#)
- [PingFederate](#)



注释 上述链接仅提供一些示例。有关正式文档，请参阅您的 IdP 文档。

过程

	命令或操作	目的
步骤 1	从 Cisco Unified Communications Manager 导出 UC 元数据，第 63 页	要创建信任关系，必须在 Unified Communications Manager 和 IdP 之间交换元数据文件。
步骤 2	在身份提供程序 (IdP) 上配置 SAML SSO	完成以下任务： <ul style="list-style-type: none">• 上传从 Unified Communications Manager 导出的 UC 元数据文件，以便完成信任关系。• 在 IdP 上配置 SAML SSO• 导出 IdP 元数据文件。此文件将导入到 Unified Communications Manager
步骤 3	在 Cisco Unified Communications Manager 中启用 SAML SSO	导入 IdP 元数据并在 Unified Communications Manager 中启用 SAML SSO。
步骤 4	重新启动 Cisco Tomcat 服务，第 65 页	在启用 SSO 之前和之后，您必须在启用 SSO 的所有群集节点上重新启动 Cisco Tomcat 服务。
步骤 5	验证 SAML SSO 配置，第 66 页	验证 SAML SSO 已成功配置。

从 Cisco Unified Communications Manager 导出 UC 元数据

使用此程序可从服务提供程序 (Unified Communications Manager) 导出 UC 元数据文件。元数据文件将导入到身份提供程序 (IdP)，以便建立信任圈关系。

过程

步骤 1 从 Cisco Unified CM 管理中，选择系统 > **SAML 单点登录**

步骤 2 从 **SAML 单点登录** 窗口中，选择 **SSO 模式** 字段中的一个选项：

- **群集范围**—群集的单个 SAML 协议。

注释 如果选择此选项，请确保群集中所有节点的 Tomcat 服务器具有相同的证书，即多服务器 SAN 证书。

- **每个节点**—每个节点都有单独的 SAML 协议。

步骤 3 从 **SAML 单点登录** 窗口中，为证书字段选择一个选项。

- 使用系统生成的自签证书
- 使用 Tomcat 证书

步骤 4 单击**导出所有元数据**以导出元数据文件。

注释 如果您在步骤 3 中选择**群集范围**选项，将会为群集显示一个元数据 XML 文件以供下载。但是，如果您选择**每个节点**选项，则将为群集的每个节点显示一个元数据 XML 文件以供下载。

下一步做什么

完成 IdP 上的以下任务：

- 上传从 Unified Communications Manager 导出的 UC 元数据文件
- 在 IdP 上配置 SAML SSO
- 导出 IdP 元数据文件。此文件将导入到 Unified Communications Manager，以便完成信任圈关系。

在 Cisco Unified Communications Manager 中启用 SAML SSO

使用此程序在服务提供程序 (Unified Communications Manager) 上启用 SAML SSO。此程序包括将 IdP 元数据导入到 Unified Communications Manager 服务器中。



重要事项 Cisco 建议您在启用或禁用 SAML SSO 后重新启动 Cisco Tomcat 服务。



注释 在启用或禁用 SAML SSO 之后，Cisco CallManager 管理、Unified CM IM and Presence 管理、Cisco CallManager 功能配置和 Unified IM and Presence 功能配置等服务重新启动。

开始之前

在完成此程序之前，请确保以下各项：

- 您需要从 IdP 导出的元数据文件。
- 确保最终用户数据与 Unified Communications Manager 数据库同步
- 验证 Unified Communications Manager IM and Presence Cisco 同步座席服务已成功完成数据同步。通过选择**诊断 > 系统故障诊断程序**，在 **Cisco Unified CM IM and Presence 管理** 中检查此测试的状态。如果数据同步已成功完成，“验证同步座席是否已同步相关数据（例如设备、用户、许可信息）”测试显示“测试通过”结果
- 至少一个 LDAP 同步用户添加到“标准 CCM 超级用户”组以允许访问“Cisco Unified 管理”。有关同步最终用户数据以及将 LDAP 同步用户添加到组中的详细信息，请参阅《Unified Communications Manager 管理指南》中的“系统设置”和“最终用户设置”部分。

过程

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

步骤 2 单击启用 **SAML SSO**，然后单击**继续**。

警告消息会通知您所有服务器连接都将重新启动。

步骤 3 如果您配置了**群集范围**的 SSO 模式，则单击**测试多服务器 tomcat 证书**按钮。否则，您可以跳过此步骤。

步骤 4 单击**下一步**。

此时将显示一个可让您导入 IdP 元数据的对话框。要配置 IdP 与服务器之间的信任关系，必须从 IdP 获取信任元数据文件，并将该文件导入到所有服务器中。

步骤 5 导入您从 IdP 导出的元数据文件：

- 浏览以查找并选择导出的 IdP 元数据文件。
- 单击**导入 IdP 元数据**。
- 单击**下一步**。
- 在下载服务器元数据并在 **IdP** 上安装屏幕上，单击**下一步**

注释 仅当 IdP 元数据文件至少在群集中的一个节点上成功导入时，下一步按键才处于启用状态。

步骤 6 测试连接并完成配置：

- a) 在**最终用户配置**窗口中，从**权限信息**列表框中选择已 LDAP 同步并拥有“标准 CCM 超级用户”权限的用户。
- b) 单击**运行测试**。

IdP 登录窗口将会显示。

注释 直到测试成功后，才能启用 SAML SSO。

- c) 输入有效的用户名和密码。

在成功验证之后，将会显示以下消息：

SSO 测试成功

看到此消息之后关闭浏览器窗口。

如果身份验证失败或用时超过 60 秒，IdP 登录窗口上会显示“登录失败”消息。“SAML 单点登录”窗口上显示以下消息：

SSO 元数据测试超时

要再次尝试登录 IdP，请选择另一个用户，然后运行另一个测试。

- d) 单击**完成**以完成 SAML SSO 设置。

此时即启用 SAML SSO，并且所有参与 SAML SSO 的 Web 应用程序都重新启动。Web 应用程序重新启动可能需要一到两分钟的时间。

重新启动 Cisco Tomcat 服务

启用或禁用 SAML 单点登录之前和之后，请在运行单点登录的所有 Unified CM 以及 IM and Presence Service 群集节点上重新启动 Cisco Tomcat 服务。

过程

步骤 1 登录到命令行界面。

步骤 2 运行 `utils service restart Cisco Tomcat CLI` 命令。

步骤 3 在启用了单点登录的所有群集节点上重复此程序。

验证 SAML SSO 配置

在服务提供程序 (Unified Communications Manager) 和 IdP 上配置 SAML SSO 后，在 Unified Communications Manager 中使用此程序确认配置正常。

开始之前

确认以下各项：

- Unified CM 管理中的 **SAML 单点登录配置** 窗口表明您已成功导入 **IdP 元数据信任文件**。
- 服务提供程序元数据文件安装在 IdP 上。

过程

步骤 1 从 Cisco Unified CM 管理中，选择 **系统 > SAML 单点登录**，**SAML 单点登录配置** 窗口即会打开，然后单击 **下一步**。

步骤 2 从有效的管理员用户名区域选择管理用户，然后单击 **运行 SSO 测试 ...** 按钮。

注释 测试用户必须具有管理员权限，并且已作为用户添加到 IdP 服务器上。“有效的管理员用户名”区域显示可被选择来运行测试的用户列表。

如果测试成功，SAML SSO 即会被配置成功。



第 9 章

配置设备池的核心设置

- [设备池概述，第 67 页](#)
- [设备池前提条件，第 74 页](#)
- [设备池的核心设置配置任务流程，第 74 页](#)
- [呼叫保留，第 83 页](#)

设备池概述

设备池为一组设备提供通用配置集。您可以将设备池分配给设备，例如电话、网关、干线和 CTI 路由点。创建设备池后，您可以关联设备以使其继承设备池设置，而不是单独配置每个设备。

设备池可让您根据其位置配置设备，方法是分配与位置相关的信息（例如日期/时间组、区域和电话 NTP 引用）。您可以根据需要创建任意数量的设备池，通常是每个位置一个。不过，您也可以根据作业功能为设备池应用配置（例如，如果您的公司有呼叫中心，您可能想要将呼叫中心电话分配到一个设备池，并将管理办公室电话分配到另一个设备池）。

本节介绍为设备池设置核心设置所需的步骤，例如：

- 网络时间协议—配置电话 NTP 引用，以便为设备池中的 SIP 设备提供 NTP 支持。
- 区域—为进出特定区域的呼叫管理带宽和支持的音频编解码器。
- Cisco Unified Communications Manager 组—为您的设备配置呼叫处理冗余和分布式呼叫处理。

网络时间协议概述

网络时间协议 (NTP) 可让 SIP 电话等网络设备将其时钟与网络时间服务器或网络支持的时钟保持同步。NTP 对于确保所有网络设备都有相同的时间，并且审核日志中的时间戳与网络时间匹配至关重要。计费和呼叫详细信息记录等功能依赖于整个网络的准确时间戳。此外，系统管理员需要审核日志中准确的时间戳以进行故障排除。这可让他们比较来自不同系统的审核日志，并为其面临的任何问题创建可靠的时间线和事件顺序。

在安装过程中，您必须为 Unified Communications Manager 发布方节点设置 NTP 服务器。然后，订阅方节点将从发布方节点同步其时间。

您最多可以分配五台 NTP 服务器。

电话 NTP 引用

- 对于 **SIP** 电话：必须配置电话 NTP 引用，然后通过设备池分配它们。这些引用将 SIP 电话定向到可提供网络时间的适当 NTP 服务器。如果 SIP 电话无法从预配置的“电话 NTP 引用”获取其日期/时间，则电话会在其向 Unified Communications Manager 注册时收到此信息。
- 对于 **SCCP** 电话：不需要电话 NTP 引用，因为 SCCP 电话通过 SCCP 信令直接从 Unified Communications Manager 获取网络时间。

通过身份验证的 NTP

要为网络的 NTP 部分提供更多网络安全，您可以配置已通过身份验证的 NTP。已通过身份验证的 NTP 已在 Cisco Unified Communications Manager 发布方节点上配置。发布方节点和 IM and Presence 节点从 Unified CM 发布方节点同步时间。

您可以从以下验证方法中进行选择：

- **通过对称密钥验证**：如果选择此选项，网络中的设备将使用对称密钥加密和验证 NTP 消息。某些供应商（例如 RedHat）建议使用此选项。
- **通过自动密钥验证（基于 PKI 的基础设施）**：如果选择此选项，网络中的设备将使用自动密钥协议加密和验证 NTP 消息。此方法对于通用标准合规性是必需的。
- **无验证**：如果您选择不配置“通过对称密钥”或“通过自动密钥”方法，则 NTP 消息将不会进行验证。

区域概述

区域为您可能需要限制其中某些呼叫的带宽的 Unified Communications Manager 多站点部署提供容量控制。例如，您可以使用区域限制跨 WAN 链接发送的呼叫的带宽，同时保持较高的内部呼叫带宽。您可以通过将区域内或区域间呼叫的最大比特率设置为区域可以提供的任何值，从而使用区域来限制音频和视频呼叫的带宽。

此外，当您有仅支持特定编解码器的应用程序时，系统还使用区域设置音频编解码器优先级。您可以配置支持的音频编解码器的优先顺序列表，并将其应用到往来特定区域的呼叫。

当您在**区域配置**窗口中（或使用**服务参数配置**窗口中的服务参数）配置最大音频比特率设置时，此设置将用作过滤器。选择呼叫的音频编解码器后，Unified Communications Manager 会从呼叫分支的两侧获取匹配的编解码器，过滤掉超出配置的最大音频比特率的编解码器，然后在列表中剩余的编解码器中选取首选的编解码器。

Unified Communications Manager 最多支持 2000 个区域。

支持的音频编解码器

Unified Communications Manager 支持视频流加密和以下音频编解码器：

音频编解码器	说明
G.711	公共交换电话网上使用的最常受支持的编解码器。
G.722	视频会议中常使用的宽带编解码器。Unified Communications Manager 始终首选 G.722（除非其禁用），而不是 G.711。
G.722.1	以 24 和 32 kb/s 速率运行的低复杂度宽带编解码器。其音频质量接近 G.722，但最多使用一半的比特率。
G.728	视频终端支持的低比特率编解码器。
G.729	Cisco 7900 IP 电话支持的具有 8 kb/s 压缩的低比特率编解码器，通常用于 WAN 链接上的呼叫。
GSM	全球移动通信系统 (GSM) 编解码器。GSM 启用 MNET 系统以使 GSM 无线听筒与 Unified Communications Manager 一起运行。
L16	高级音频编码低延迟 (AAC-LD) 是一种超宽带音频编解码器，它为语音和音乐提供了卓越的音质。该编解码器即使比特率较低，但提供了与旧版编解码器同等或比其更好的音质。
AAC-LD (mpeg4-generic)	支持 SIP 设备，特别是 Cisco TelePresence 系统。
AAC-LD (MP4A-LATM)	低开销 MPEG-4 音频传输复用 (LATM) 是一种超宽带音频编解码器，可提供卓越音质。支持 SIP 设备，包括 Tandberg 和一些第三方终端。 注释 AAC-LD (mpeg4-generic) 和 AAC-LD (MP4A-LATM) 不兼容。
Internet 语音音频编解码器 (iSAC)	自适应宽带音频编解码器，特别设计用于在中低比特率应用程序中提供低延迟的宽带音质。
Internet 低比特率编解码器 (iLBC)	提供的音质介于 G.711 与 G.729 之间，比特率介于 15.2 到 13.3 kb/s 之间，同时允许独立编码的语音帧导致的有损网络中语音质量的平稳退化。iLBC 支持 SIP、SCCP、H323 和 MGCP 设备。 注释 H.323 出站 FastStart 不支持 iLBC 编解码器。
自适应多速率 (AMR)	基于 GSM (WDM、EDGE、GPRS) 的 2.5G/3G 无线网络所需的的标准编解码器。此编解码器以 4.75 到 12.2 kb/s 范围的可变比特率编码窄带 (200-3400 Hz) 信号，并从 7.4 kb/s 开始提供长途电话质量的语音。AMR 仅支持 SIP 设备。
自适应多速率宽带 (AMR-WB)	编码为 G.722.2，是一种 ITU-T 标准语音编解码器，正式名称为宽带编解码器，以大约 16 kb/s 编码语音。此编解码器为首选，因为它以相比其他窄带语音编解码器（如 AMR 和 G.711）较宽的语音带宽（50 Hz 到 7000 Hz）提供优质的语音质量。AMR-WB 仅支持 SIP 设备。

音频编解码器	说明
Opus	<p>Opus 编解码器是一种交互式语音和音频编解码器，特别设计用于处理各类交互式音频应用程序，比如：IP 语音、视频会议、游戏中聊天、分布式实时音乐性能。</p> <p>此编解码器可从窄带低比特率覆盖到高质量比特率，范围从 6 到 510 kb/s。</p> <p>默认情况下，所有 SIP 设备都启用 Opus 编解码器支持。您可以通过启用 Opus 编解码器 服务参数重新配置 Opus 支持（默认设置是所有设备启用）。您可以将此参数重新配置为禁用 Opus 编解码器支持，或仅启用非录音设备中的支持。</p> <p>注释 Opus 依赖于 G.722 编解码器。通告 G.722 编解码器 企业参数也应设置为启用，以便 SIP 设备使用 Opus。</p>

Cisco Unified CM 组概述

Unified Communications Manager 组是可供设备注册的最多三个冗余服务器组成的优先顺序列表。每个组包含一个主节点和最多两个备份节点。列出节点的顺序决定了他们的优先级，第一个节点为主节点，第二个是备份节点，第三个是第三节点。您可以通过**设备池配置**将设备分配给 Cisco Unified Communications Manager 组。

Unified Communications Manager 组为您的系统提供两个重要功能：

- 呼叫处理冗余—设备在注册时会尝试连接到分配至其设备池的组中的主（第一个）Unified Communications Manager。如果主 Unified Communications Manager 不可用，设备将尝试连接第一个备份节点，如果该节点不可用，它将尝试连接到第三节点。每个设备池都分配有一个 Unified Communications Manager 组。
- 分布式呼叫处理—您可以创建多个设备池和 Unified Communications Manager 组，以便跨多个 Unified Communications Manager 均匀分配设备注册。

对于大多数系统，将一个 Unified Communications Manager 分配到多个组以实现更好的负载分配和冗余。

呼叫处理冗余

Unified Communications Manager 组提供呼叫处理冗余和恢复：

- 故障转移—组中的主要 Unified Communications Manager 发生故障，且设备向该组中的备用 Unified Communications Manager 注册时进行。
- 回退—发生故障的主要 Unified Communications Manager 恢复服务，且该组中的设备向主要 Unified Communications Manager 注册时进行。

正常操作情况下，组中的主要 Unified Communications Manager 控制与该组关联的所有注册设备（例如电话和网关）的呼叫处理。

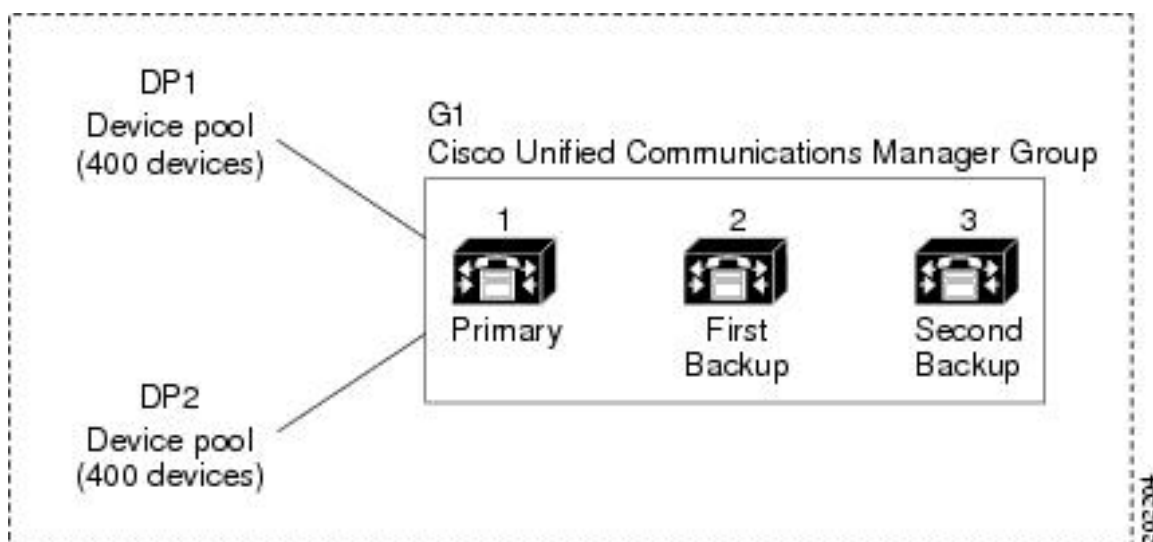
如果主要 Unified Communications Manager 出于任何原因发生故障，该组中的第一个备用 Unified Communications Manager 将控制向主要 Unified Communications Manager 注册的设备。如果指定该组的第二个备用 Unified Communications Manager，它将在主要和第一个备用 Cisco Unified Communications Manager 均发生故障时控制设备。

发生故障的 Unified Communications Manager 恢复服务后，它将再次控制该组，并且该组中的设备将自动向主要 Unified Communications Manager 注册。

示例

例如，下图所示为一个简单系统，在一个组中具有三个 Unified Communications Manager，控制 800 个设备。

图 4: Unified Communications Manager 组



该图描绘了分配有两个设备池、DP1 和 DP2 的 Unified Communications Manager 组 G1。Unified Communications Manager 1（作为组 G1 中的主要 Unified Communications Manager）在正常操作下控制 DP1 和 DP2 中的所有 800 个设备。如果 Unified Communications Manager 1 失败，所有 800 个设备的控制将转移到 Unified Communications Manager 2。如果 Unified Communications Manager 2 也失败，则所有 800 个设备的控制将转移到 Unified Communications Manager 3。

该配置提供呼叫处理冗余，但不会在示例中的三个 Unified Communications Manager 之间很好地分配呼叫处理负载。有关如何使用 Unified Communications Manager 组和设备池以在群集中提供分布式呼叫处理的信息，请参阅以下主题。



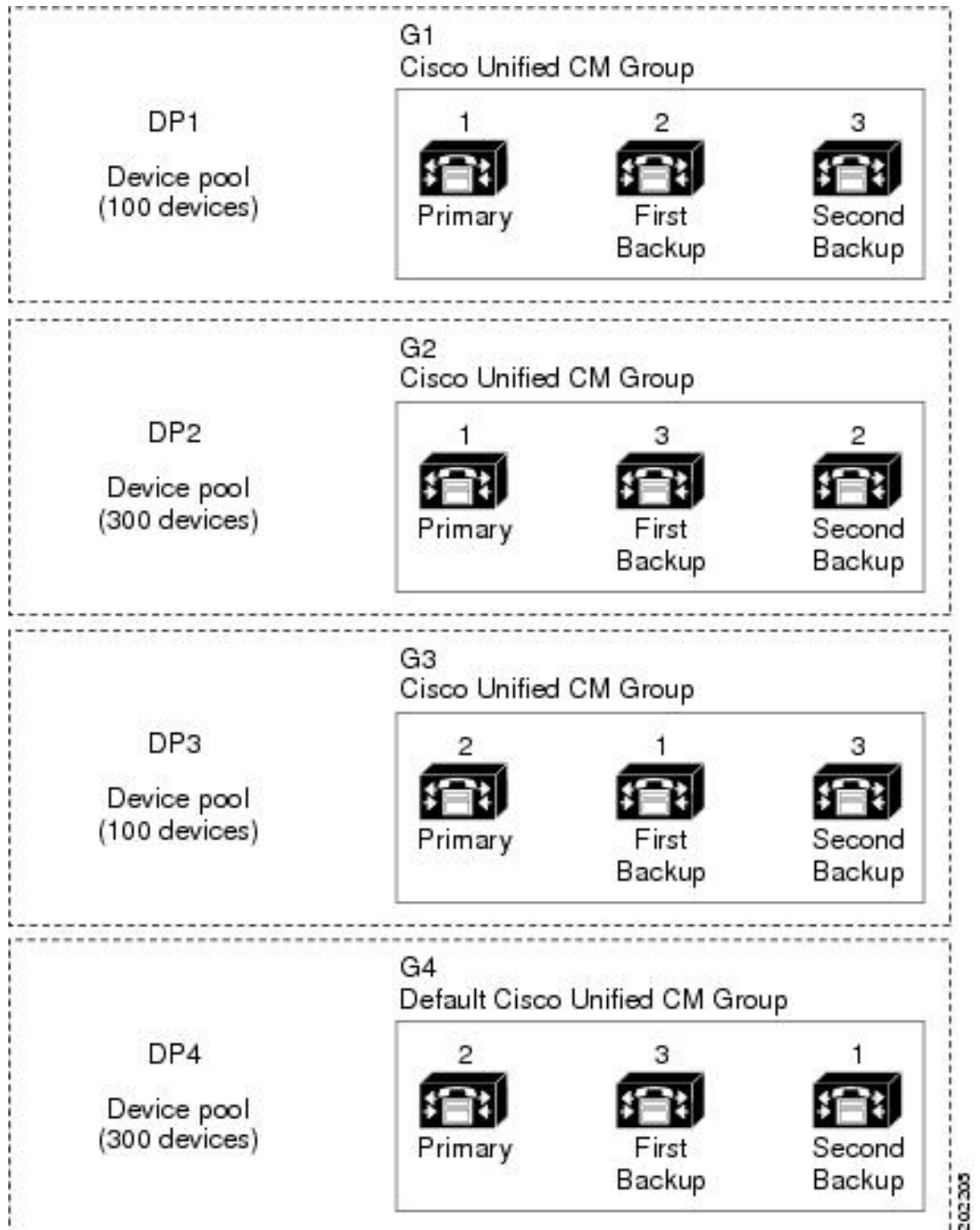
注释 空 Unified Communications Manager 组将不起作用。

分布式呼叫处理

Unified Communications Manager 组提供呼叫处理冗余和分布式呼叫处理。如何在各组之间分布设备、设备池和 Unified Communications Manager 决定了系统中的冗余级别和负载均衡。

在大多数情况下，您希望以组中的一个 Unified Communications Manager 发生故障时避免其他 Unified Communications Manager 过载的方式分布设备。下图所示为一种可能的方式，可配置 Unified Communications Manager 组和设备池以使三个 Unified Communications Manager 和 800 个设备的系统同时实现分布式呼叫处理和冗余。

图 5: 与分布式呼叫处理相结合的冗余



上图描述了配置和分配给设备池时的 Unified Communications Manager 组，所以 Unified Communications Manager 1 充当两个组 G1 和 G2 中的主控制器。如果 Unified Communications Manager 1 发生故障，

设备池 DP1 中的 100 个设备将重新注册为 Unified Communications Manager 2，而 DP2 中的 300 个设备将使用 Unified Communications Manager 3 重新注册。类似地，Unified Communications Manager 2 用作组 G3 和 G4 的主控制器。如果 Unified Communications Manager 2 发生故障，DP3 中的 100 个设备将使用 Unified Communications Manager 1 重新注册，并且 DP4 中的 300 个设备将使用 Unified Communications Manager 3 重新注册。如果 Unified Communications Manager 1 和 Unified Communications Manager 2 均失败，则所有设备都使用 Unified Communications Manager 3 重新注册。

设备池前提条件

请确保在配置设备池之前正确规划它们。配置设备池和冗余 Unified Communications Manager 组时，您要为电话提供服务器冗余，同时跨群集分布注册。有关可用于计划系统的其他信息，请参阅 <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html> 上的《Cisco 协作系统解决方案参考网络设计》。

要确保 Unified Communications Manager 包括最新的时区信息，可以安装 Cisco Options Package (COP) 文件，从而在安装 Unified Communications Manager 后更新时区信息。在主要时区更改事件后，我们将与您联系，让您知道您可以在 <https://software.cisco.com/download/navigator.html> 下载最新的 COP 文件。

将 CMLocal 的设置更改为本地日期和时间。

其他设备池配置

本章重点介绍核心设置，例如电话 NTP 引用、区域和通过 Unified Communications Manager 组的呼叫处理冗余。不过，您也可以通过设备池配置将这些可选功能和组件应用到设备：

- 媒体资源—分配会议桥等媒体资源和音乐保持到设备池中的设备。有关详细信息，请参阅本书的媒体资源配置任务流程一节。
- Survivable Remote Site Telephony (SRST)—如果您的部署使用 WAN 连接，请配置 SRST，以便在发生 WAN 中断时，IP 网关可以提供有限的呼叫支持。有关详细信息，请参阅本书中的 *Survivable Remote Site Telephony* 配置任务流程一节。
- 呼叫路由信息—有关如何在群集之间路由呼叫的信息，请参阅本书中的呼叫 *RoutingConfiguration* 任务流程一节。
- 设备移动—配置设备移动组以允许设备根据其物理位置假设设置。有关更多信息，请参阅《Cisco Unified Communications Manager 功能配置指南》的“配置设备移动”一章。

设备池的核心设置配置任务流程

完成这些任务以为使用设备池的设备设置那些设备池并应用设置（例如区域、电话 NTP 引用和冗余）。

过程

	命令或操作	目的
步骤 1	配置网络时间协议，第 75 页	完成此任务流程中的任务以在您的系统上设置 NTP。配置电话 NTP 引用并将其应用到您可以分配给设备池的日期/时间组。
步骤 2	配置区域关系，第 80 页	完成这些任务以为您的系统设置区域。您最多可以创建 2000 个区域并配置自定义的设置，例如基于区域可提供的自定义音频编解码器首选项和比特率限制。
步骤 3	配置 Cisco Unified CM 组，第 81 页	配置 Unified Communications Manager 组进行呼叫处理冗余和负载均衡。
步骤 4	配置设备池，第 82 页	设置系统设备的设备池。将您配置的其他核心设置应用到设备池，以便将这些设置应用到使用此设备池的设备。

配置网络时间协议

完成这些任务以为您的系统配置网络时间协议 (NTP)。配置电话 NTP 引用并将其应用到日期/时间组，然后您可以将其应用到设备池。

过程

	命令或操作	目的
步骤 1	添加 NTP 服务器，第 76 页	<p>可选。如果您需要添加 NTP 服务器，请使用此程序。最多可以添加五个 NTP 服务器。</p> <p>注释 在系统安装期间，您需要将 Unified Communications Manager 指向 NTP 服务器。如果要添加其他 NTP 服务器，您可以使用此程序。否则，您可以跳过此任务。</p>
步骤 2	选择以下一种方法来验证 NTP 消息： <ul style="list-style-type: none"> • 通过对称密钥配置 NTP 验证，第 76 页 • 通过自动密钥配置 NTP 验证，第 77 页 	<p>可选。如需更高的安全性，请配置通过身份验证的 NTP。您可以通过对称密钥或通过自动密钥配置身份验证。通用标准合规需要自动密钥方法。</p>
步骤 3	配置电话 NTP 首选项，第 77 页	对于 SIP 电话，必须配置电话 NTP 引用，然后通过日期/时间组和设备池应用它们。

	命令或操作	目的
步骤 4	添加日期/时间组，第 78 页	定义连接到系统的各个设备的时区，并将您设置的电话 NTP 引用分配到相应的日期/时间组。



注释 有关可用于故障排除和配置 NTP（例如 `utils ntp*` 命令集）的 CLI 命令的详细信息，请参阅《命令行界面参考指南》，位于 <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>。

添加 NTP 服务器

将 NTP 服务器添加到 Unified Communications Manager。



注释 也可以在 Cisco Unified 操作系统管理窗口的 NTP 服务器配置窗口（设置 > **NTP 服务器**）中添加 NTP 服务器。

过程

步骤 1 登录到命令行界面。

步骤 2 要确认发布方节点能够访问 NTP 服务器，请运行 `utils network ping <ip_address>`，其中 `ip_address` 代表 NTP 服务器的地址。

步骤 3 如果服务器可访问，请运行 `utils ntp server add <ip_address>` 以添加服务器。

步骤 4 使用 `utils ntp restart` 命令重新启动 NTP 服务。

通过对称密钥配置 NTP 验证

使用此程序可通过对称密钥验证网络中的 NTP 消息。



注释 确保按字符输入 SHA1 密钥字符。目前，CLI 框架不会读取粘贴的值。

过程

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

步骤 2 运行 `utils ntp auth-symmetric key status` 命令以验证当前 NTP 验证设置的状态。

步骤 3 执行以下任一操作：

- 要使用对称密钥启用 NTP 身份验证，请运行 `utils ntp auth symmetric-key enable` CLI 命令。
- 要使用对称密钥禁用 NTP 身份验证，请运行 `utils ntp auth symmetric-key disable` CLI 命令。

步骤 4 按照提示输入 NTP 服务器的密钥 ID 和对称密钥。

通过自动密钥配置 NTP 验证

如果您想要通过基于 PKI 的自动密钥配置 NTP 身份验证，请使用此程序。



注释 如果启用了使用对称密钥的 NTP 身份验证，则必须在启用使用自动密钥进行身份验证之前禁用此功能。要使用对称密钥禁用 NTP 身份验证，请参阅[通过对称密钥配置 NTP 验证，第 76 页](#)。

开始之前

要通过自动密钥启用 NTP 验证，必须启用通用标准模式。有关启用 Common Criteria 模式的详细信息，请参阅《*Cisco Unified Communications Manager 安全指南*》的“FIPS 设置”一章。

过程

步骤 1 登录到命令行界面。

步骤 2 运行 `utils ntp auth auto-key status` 命令以验证当前的 NTP 身份验证设置。

步骤 3 执行下列操作之一：

- 要启用 NTP 身份验证，请运行 `utils ntp auth auto-key enable` CLI 命令。
- 要启用 NTP 身份验证，请运行 `utils ntp auth auto-key disable` CLI 命令。

步骤 4 输入您要为其启用或禁用 NTP 身份验证的 NTP 服务器的号码。

步骤 5 如果要启用身份验证，请输入 IFF 客户端密钥。粘贴 NTP 服务器的客户端密钥。

配置电话 NTP 首选项

使用此程序可配置电话 NTP 引用，这对 SIP 电话是强制要求。您可以通过日期/时间组将您创建的 NTP 引用分配给设备池。该引用将 SIP 电话指向可提供网络时间的适当 NTP 服务器。对于 SCCP 电话，此配置并非必需。



注释 Cisco Communications Manager 不支持组播和任意播模式。如果您选择这些模式中的任一模式，您的系统将默认为定向广播模式。

过程

步骤 1 从 Cisco Unified CM 管理中，选择系统 > 电话 NTP 引用。

步骤 2 单击新增。

步骤 3 输入 NTP 服务器的 **IPv4 地址**或 **IPv6 地址**，具体取决于您的电话使用哪种寻址系统。

注释 必须输入 IPv4 地址或 IPv6 地址以保存电话 NTP 引用。如果同时部署 IPv4 电话和 IPv6 电话，则提供 NTP 服务器的 IPv4 地址和 IPv6 地址。

步骤 4 在说明字段中，输入电话 NTP 引用的说明。

步骤 5 在模式下拉列表中，从下列选项选择电话 NTP 引用的模式。

- **单播**—如果您选择该模式，则电话发送 NTP 查询包至特定 NTP 服务器。
- **定向广播**—如果选择此默认 NTP 模式，电话将从任何 NTP 服务器访问日期/时间信息，但给出所列 NTP 服务器的优先顺序（第 1 = 主，第 2 = 辅助）。

注释 Cisco TelePresence 和 Cisco Spark 设备类型仅支持单播模式。

步骤 6 单击保存。

下一步做什么

将电话 NTP 引用分配到日期/时间组。有关详细信息，请参阅 [添加日期/时间组](#)，第 78 页

添加日期/时间组

配置日期/时间组以定义系统中的时区。将您配置的电话 NTP 引用分配到适当的组。将新的日期/时间组添加到数据库后，可以将其分配给设备池，以配置该设备池中所有设备的日期和时间信息。

必须重置设备以应用所做的任何更改。



提示 由于 Cisco IP 电话分布于世界各地，因此需要为每个时区创建一个日期/时间组。

过程

步骤 1 从 Cisco Unified CM 管理中，选择系统 > 日期/时间组。

步骤 2 单击新增。

步骤 3 将 NTP 引用分配给此组：

- a) 单击添加电话 NTP 引用。
- b) 在查找并列出电话 NTP 引用弹出窗口中，单击查找并选择您在上一任务中配置的电话 NTP 引用。

- c) 单击添加选定项。

d) 如果添加了多个引用，请使用向上和向下箭头更改优先顺序。顶部的引用具有较高的优先级。
- 步骤 4 完成日期/时间组配置窗口中其余字段的设置。请参阅联机帮助，了解有关字段及其配置选项的更多信息。
- 步骤 5 单击保存。

配置区域

完成以下任务以配置您的设备池区域。配置区域之间的关系以更好地管理带宽。您可以使用区域控制某些类型的呼叫（例如，视频呼叫）的最大比特率，以及确定特定音频编解码器的优先顺序。

过程

	命令或操作	目的
步骤 1	自定义音频编解码器首选项，第 79 页	可选。如果您要自定义音频编解码器的优先级，请使用此程序。您可能想要这样做，以便优先于其他编解码器处理特定的音频编解码器。否则，您可以将其中一个默认音频编解码器列表分配给您的设备池。
步骤 2	配置群集范围内的区域默认设置，第 80 页	配置区域的群集范围默认设置。除非您在“区域配置”中进行配置，否则所有区域都将使用这些默认设置。
步骤 3	配置区域关系，第 80 页	设置新区域或编辑现有区域的设置。配置区域间和区域内呼叫的关系。

自定义音频编解码器首选项

使用此程序可自定义音频编解码器的优先级。通过复制现有列表中的设置，然后编辑新列表内的优先级顺序，创建新的音频编解码器首选项列表。



注释

如果不需要自定义音频编解码器优先级，则可以跳过此任务。配置设备池时，您可以分配一个默认的音频编解码器首选项列表。

过程

- 步骤 1 从 Cisco Unified CM 管理选择系统 > 区域信息 > 音频编解码器首选项列表。
- 步骤 2 单击新增。
- 步骤 3 从音频编解码器首选项列表下拉列表框中，选择一个现有的音频编解码器首选项列表。

即会为您选择的列表显示音频编解码器优先级列表。

步骤 4 单击**复制**。所复制列表的编解码器优先级列表将应用到新创建的列表。

步骤 5 编辑新音频编解码器列表的**名称**。例如，customizedCodecList。

步骤 6 编辑说明。

步骤 7 使用向上和向下箭头以按列表中的编解码器列表框中显示的优先级顺序移动编解码器。

步骤 8 单击**保存**。

您必须将新列表应用到区域，然后将该区域应用到设备池。设备池中的所有设备都将使用此音频编解码器首选项列表。

配置群集范围内的区域默认设置

使用此程序可配置区域的群集范围默认设置。默认情况下，这些设置应用于进出所有区域的呼叫，除非您在**区域配置**窗口中为个别区域配置了区域关系。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**系统 > 服务参数**。

步骤 2 从**服务器**下拉列表中，选择 Unified Communications Manager 节点。

步骤 3 从**服务**下拉列表中选择 **Cisco CallManager** 服务。

此时将显示**服务参数配置**窗口。

步骤 4 在**群集范围参数（系统 - 位置和区域）**下，配置所需的任何新服务参数设置。有关服务参数说明的详细信息，请单击任何参数名称查看帮助说明。

步骤 5 单击**保存**。

配置区域关系

使用此程序创建区域并为特定区域之间的呼叫分配自定义设置。您可以编辑设置，例如首选音频编解码器和最大比特率。例如，如果您有区域的带宽容量低于网络的其余部分，则可能要编辑往来于该区域的视频呼叫的最大会话比特率。您可以将此值重置为该区域可以提供的值。



注释 为了增强可扩展性，并确保系统使用更少的资源，我们建议您尽可能使用**服务参数配置**窗口中的默认值。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**系统 > 区域信息 > 区域**。

步骤 2 执行以下任一操作：

- 单击**查找**并选择一个区域。
- 单击**新增**以创建新的区域。
- 输入区域的**名称**。例如，NewYork。
- 单击**保存**。

只读的**区域关系**区域显示您在所选区域和另一区域之间设置的任何自定义设置。

步骤 3 要修改此区域与另一区域（或用于区域内呼叫的相同区域）之间的设置，请在**修改与其它区域的关系**区域中编辑设置：

- a) 在**区域**区域中，突出显示其他区域（对于区域内呼叫，突出显示您正在配置的相同区域）。
- b) 编辑相邻字段中的设置。有关这些字段及其设置的帮助，请参阅联机帮助。
- c) 单击**保存**。

现在，新设置显示为**区域关系**区域中的一个自定义规则。

注释 如果您在一个区域内编辑区域关系，则无需在另一区域中重复该配置，因为设置将在另一区域中自动更新。例如，假设您在**区域配置**窗口中打开区域 1，并且配置了区域 2 的自定义关系。如果随后打开区域 2，您将看到**区域关系**区域中显示的自定义关系。

配置 Cisco Unified CM 组

使用此程序可为设备池中的设备设置 Unified Communications Manager 组以实现呼叫处理冗余、负载均衡和故障转移。



提示 设置多个组和设备池，其中主服务器在每个组中不同，以便提供设备注册均布于群集节点的分布式呼叫处理。



注释 请勿使用默认服务器组，因为它不是描述性的，可能会引起混淆。

过程

步骤 1 从 Cisco Unified CM 管理中，选择系统 > **Cisco Unified CM 组**。

步骤 2 输入组的**名称**。

注释 考虑确定节点在名称中的顺序，以便能够轻松地将该组与其他组区分开来。例如，CUCM_PUB-SUB。

步骤 3 如果希望此 Unified Communications Manager 组在自动注册启用时成为默认的 Unified Communications Manager 组，请选中**自动注册 Cisco Unified Communications Manager 组**复选框。

- 步骤 4** 从可用 **Cisco Unified Communications Managers** 列表中，选择要添加到此组的节点，然后单击向下箭头以选择它们。您最多可以向组中添加三台服务器。
此组中的服务器显示在所选的 **Cisco Unified Communications Managers** 列表框中。列表顶部的服务器是主服务器
- 步骤 5** 使用所选的 **Cisco Unified Communications Manager** 列表框旁边的箭头更改哪些服务器为主服务器和备份服务器。
- 步骤 6** 单击保存。

配置设备池

设置系统设备的设备池。将您配置的其他核心设置应用到设备池，以便将这些设置应用到使用此设备池的设备。您可以配置多个设备池以满足您的部署需求。

开始之前

如果要分配 SRST 配置，请参阅 [Survivable Remote Site Telephony 配置任务流程](#)，第 110 页。

过程

- 步骤 1** 在 Cisco Unified CM 管理上，选择系统 > 设备池。
- 步骤 2** 执行以下任一操作：
- 单击**新增**以创建新的设备池。
 - 单击**查找**并选择现有设备池。
- 步骤 3** 在设备池名称字段中，输入设备池的名称。
- 步骤 4** 从 **Cisco Unified Communications Manager** 组下拉列表中，选择您设置用于处理呼叫处理冗余和负载均衡的组。
- 步骤 5** 从日期/时间组下拉列表中，选择您设置用于处理使用此设备池的设备的日期、时间和电话 NTP 引用的组。
- 步骤 6** 从区域下拉列表框中，选择要应用到此设备池的区域。
- 步骤 7** 从媒体资源组列表 下拉列表中，选择包含要应用到此设备池的媒体资源的列表。
- 步骤 8** 为此设备池应用 SRST 设置：
- a) 从 **SRST 参考**下拉列表中，分配 SRST 参考。
 - b) 在**连接监控持续时间**字段中分配值。此设置定义电话在从 SRST 注销并重新注册到 Unified Communications Manager 之前监视其连接到 Unified Communications Manager 的时间。
- 步骤 9** 完成设备池配置窗口中其余字段的设置。有关这些字段及其设置的帮助，请参阅联机帮助。
- 步骤 10** 单击保存。

下一步做什么

根据您的部署要求配置多个设备池。

基本设备池配置字段

表 5: 基本设备池配置字段

字段	说明
设备池名称	输入新设备池的名称。最多可以输入 50 个字符，可包含字母数字、点 (.)、连字符 (-)、下划线 (_) 和空格。
Cisco Unified Communications Manager 组	选择要分配到此设备池中设备的 Cisco Unified Communications Manager 组。Cisco Unified Communications Manager 组可指定最多三个 Unified Communications Manager 的优先顺序列表。列表中的第一个节点充当该组的主节点，而组的其他成员用作冗余备份节点。
日期/时间组	选择要分配到此设备池中设备的日期/时间组。日期/时间组指定日期和时间的时区及显示格式。
区域	选择要分配到此设备池中设备的区域。区域设置指定可用于区域内及其他区域之间通信的语音和视频编解码器。

呼叫保留

Unified Communications Manager 的呼叫保留功能可确保在 Unified Communications Manager 发生故障或设备与建立呼叫的 Unified Communications Manager 之间的通信发生故障时活动呼叫不会中断。

Unified Communications Manager 支持一组扩展 Cisco Unified Communications 设备的完全呼叫保留。这一支持包括 Cisco Unified IP 电话、支持外部交换局 (FXO)（非 loop-start 干线）和外部交换站 (FXS) 接口的媒体网关控制协议 (MGCP) 网关以及（在较小程度上）会议桥、MTP 和转码资源设备之间的呼叫保留。

通过将高级服务参数“允许对等机保留 H.323 呼叫”设置为“真”启用 H.323 呼叫保留。

以下设备和应用程序支持呼叫保留。如果双方均通过以下设备之一连接，Unified Communications Manager 将保持呼叫保留：

- Cisco Unified IP 电话
- SIP 干线
- 软件会议桥
- 软件 MTP
- 硬件会议桥（Cisco Catalyst 6000 8 端口语音 E1/T1 和服务模块、Cisco Catalyst 4000 访问网关模块）

- 转码器（Cisco Catalyst 6000 8 端口语音 E1/T1 和服务模块、Cisco Catalyst 4000 访问网关模块）
- 非 IOS MGCP 网关（Catalyst 6000 24 端口 FXS 模拟接口模块、Cisco DT24+、Cisco DE30+、Cisco VG200）
- Cisco IOS H.323 网关（例如 Cisco 2800 系列、Cisco 3800 系列）
- Cisco IOS MGCP 网关（Cisco VG200、Cisco Catalyst 4000 访问网关模块、Cisco 2620、Cisco 3620、Cisco 3640、Cisco 3660、Cisco 3810）
- Cisco VG248 模拟电话网关

以下设备和应用程序不支持呼叫保留：

- 报警器
- H.323 终端（例如 NetMeeting）或第三方 H.323 终端
- CTI 应用程序
- TAPI 应用程序
- JTAPI 应用程序

呼叫保留情景

下表说明如何在各种场景下处理呼叫保留。

表 6: 呼叫保留情景

场景	呼叫保留处理
Unified Communications Manager 发生故障。	Unified Communications Manager 故障导致通过故障 Unified Communications Manager 建立的所有呼叫的呼叫处理功能都将丢失。 Unified Communications Manager 将保持受影响的活动呼叫，直到最终用户挂机或直到设备能够确定媒体连接已释放。用户无法调用由于此故障而保持的呼叫的任何呼叫处理功能。

场景	呼叫保留处理
Unified Communications Manager 与设备之间发生通信故障。	<p>设备与控制该设备的 Unified Communications Manager 之间发生通信故障时，该设备将识别并保持活动的连接。Unified Communications Manager 将识别通信故障并清除与失去通信的设备中呼叫关联的呼叫处理实体。</p> <p>Unified Communications Manager 仍保持控制与受影响呼叫关联的幸存设备。Unified Communications Manager 将保持受影响的活动呼叫，直到最终用户挂机或直到设备能够确定媒体连接已释放。用户无法调用由于此故障而保持的呼叫的任何呼叫处理功能。</p> <p>注释 在故障转移情况下，当您打开保持连接计时器中的 Unified CM 节点时，即使呼叫处于保留模式，电话仍会保持注册到当前节点。保持连接计时器处于活动状态时可能发生这种情况。</p>
设备故障 (电话、网关、会议桥、转码器、MTP)	<p>设备发生故障时，通过设备存在的连接将停止流媒体。活动 Unified Communications Manager 将识别设备故障并清除与故障设备中呼叫关联的呼叫处理实体。</p> <p>Unified Communications Manager 保持控制与受影响呼叫关联的幸存设备。Unified Communications Manager 将保持与幸存设备关联的活动连接（呼叫），直到幸存的最终用户挂机或直到幸存设备能够确定媒体连接已释放。</p>



第 10 章

配置干线

- [SIP 干线概述](#)，第 87 页
- [SIP 干线前提条件](#)，第 87 页
- [SIP 干线配置任务流程](#)，第 88 页
- [SIP 干线相互作用和限制](#)，第 90 页
- [H.323 干线概述](#)，第 91 页
- [H.323 干线前提条件](#)，第 92 页
- [配置 H.323 干线](#)，第 92 页

SIP 干线概述

如果要部署 SIP 进行呼叫控制信令，请配置 SIP 干线将 Cisco Unified Communications Manager 连接到外部设备，例如 SIP 网关、SIP 代理服务器、Unified Communications applications、会议桥、远程群集或会话管理版本。

在 Cisco Unified CM 管理中，**SIP 干线配置**窗口中包含 Cisco Unified Communications Manager 用于管理 SIP 呼叫的 SIP 信令配置。

您可以使用 IPv4 或 IPv6 寻址、完全限定域名或单个 DNS SRV 记录为 SIP 干线分配多达 16 个不同的目标地址。

SIP 干线前提条件

在配置 SIP 干线之前，请执行以下操作：

- 规划您的网络拓扑，使您能够了解干线连接。
- 确保您了解干线所要连接的设备以及这些设备如何实施 SIP。
- 确保为干线配置了设备池。
- 如果您在干线上部署 IPv6，则必须通过群集范围企业参数或通过可应用到干线的通用设备配置来配置干线的寻址首选项。

- 如果存在与使用干线的应用程序的 SIP 互操作性问题，您可能需要使用默认的 SIP 标准化或透明脚本之一。如果没有任何默认脚本满足您的需要，您可以创建自己的脚本。有关创建自定义的 SIP 标准化和透明度脚本的详细信息，请参阅《Cisco Unified Communications Manager 功能配置指南》。

SIP 干线配置任务流程

完成这些任务以设置您的 SIP 干线。

过程

	命令或操作	目的
步骤 1	配置 SIP 配置文件，第 88 页	配置将应用到 SIP 干线的通用 SIP 设置。
步骤 2	配置 SIP 干线安全性配置文件，第 89 页	使用 TLS 信令或 Digest 验证等安全设置配置安全性配置文件。
步骤 3	配置 SIP 干线，第 89 页	设置 SIP 干线并将 SIP 配置文件和安全性配置文件应用到干线。

配置 SIP 配置文件

使用此程序配置具有通用 SIP 设置的 SIP 配置文件，您可分配给使用此配置文件的 SIP 设备和干线。

过程

- 步骤 1 从“Cisco Unified CM 管理”中，选择设备 > 设备设置 > SIP 配置文件。
- 步骤 2 请执行以下步骤之一：
 - 单击**查找**并选择 SIP 配置文件以编辑现有配置文件。
 - 单击**新增**以创建新的配置文件。
- 步骤 3 如果想要您的 SIP 电话和干线支持 IPv4 和 IPv6 堆栈，请选中**启用 ANAT** 复选框。
- 步骤 4 如果要分配 SDP 透明配置文件以解析 SDP 互操作性，请从 **SDP 透明配置文件** 下拉列表进行。
- 步骤 5 如果要分配标准化或透明度脚本来解决 SIP 互操作性问题，请从**标准化脚本**下拉列表中选择脚本。
- 步骤 6 （可选）对于您可能需要在 Cisco Unified Border Element 中路由呼叫的全局拨号方案复制部署，选中**发送 ILS 学习目标路由字符串**复选框。
- 步骤 7 完成 **SIP 配置文件配置**窗口中其余字段的设置。有关字段及其配置选项的更多信息，请参阅联机帮助。
- 步骤 8 单击**保存**。

配置 SIP 干线安全性配置文件

使用 Digest 验证或 TLS 信令加密等安全设置配置 SIP Trunk 安全性配置文件。将配置文件分配到 SIP 干线时，干线将采用安全性配置文件的设置。



注释 如果没有将 SIP Trunk 安全性配置文件分配给 SIP 干线，Cisco Unified Communications Manager 默认会分配不安全的配置文件。

过程

步骤 1 从 Cisco Unified CM 管理中，选择系统 > 安全性 > **SIP Trunk 安全性配置文件**。

步骤 2 单击**新增**。

步骤 3 要启用使用 TLS 的 SIP 信令加密，请执行以下操作：

- 从设备安全模式下拉列表中，选择**已加密**。
- 从传入传输类型和传出传输类型下拉列表中，选择**TLS**。
- 对于设备验证，在 **X.509 使用者名称** 字段中，输入 X.509 证书的使用者名称。
- 在**传入端口**字段中，输入您要在其上接收 TLS 请求的端口。TLS 的默认值为 5061。

步骤 4 要启用 digest 验证，请执行以下操作

- 选中**启用 Digest 验证**复选框。
- 输入**随机数有效性计时器**值以指示系统生成新的随机数之前必须经过的秒数。默认值为 600（10 分钟）。
- 要对应用程序启用 digest 验证，请选中**启用应用程序级授权**复选框。

步骤 5 完成 **SIP Trunk 安全性配置文件**配置窗口中的其他字段。有关字段及其配置选项的更多信息，请参阅联机帮助。

步骤 6 单击**保存**。

注释 必须在**干线配置**窗口中将配置文件分配给干线，以便干线能够使用这些设置。

配置 SIP 干线

使用此程序配置 SIP 干线。您可以为 SIP 干线分配多达 16 个目标地址。

过程

步骤 1 从 Cisco Unified CM 管理中，选择设备 > 干线。

步骤 2 单击**新增**。

步骤 3 从干线类型下拉列表中，选择 **SIP 干线**。

步骤 4 从协议类型下拉列表中，选择与您的部署匹配的 SIP 干线类型，然后单击下一步：

- 无（默认）
- 呼叫控制发现
- 跨群集分机移动
- Cisco 公司间媒体引擎
- IP 多媒体系统服务控制

步骤 5 （可选）如果想要将通用设备配置应用到此干线，从下拉列表中选择配置。

步骤 6 如果要在干线上允许加密的媒体，请选中允许 SRTP 复选框。

步骤 7 如果要启用所有群集节点的干线，请选中在所有活动的 Unified CM 节点上运行复选框。

步骤 8 配置 SIP 干线的目标地址：

- a) 在目标地址文本框中，输入您要连接到干线的服务器或端点的 IPv4 地址、完全限定的域名或 DNS SRV 记录。
- b) 如果干线为双堆栈干线，在目标地址 IPv6 文本框中，输入您要连接到干线的服务器或端点的 IPv6 地址、完全限定的域名或 DNS SRV 记录。
- c) 如果目标为 DNS SRV 记录，选中目标地址是 SRV 复选框。
- d) 要添加其他目标，请单击 (+)。

步骤 9 从 SIP Trunk 安全性配置文件下拉列表框中，分配安全性配置文件。如果不选择此选项，则会分配不安全的配置文件。

步骤 10 从 SIP 配置文件下拉列表中，分配 SIP 配置文件。

步骤 11 （可选）如果想要将标准化脚本分配给此 SIP 干线，从标准化脚本下拉列表中，选择您要分配的脚本。

步骤 12 在干线配置窗口中配置任何其他字段。有关字段及其配置选项的更多信息，请参阅联机帮助。

步骤 13 单击保存。

SIP 干线相互作用和限制

功能	说明
多个安全 SIP 干线到同一目标	<p>从版本 12.5(1) 开始，Cisco Unified Communications Manager 支持将多个安全 SIP 干线配置到相同的目标 IP 地址和目标端口号。此功能可提供以下优势：</p> <ul style="list-style-type: none"> • 带宽优化—为紧急呼叫提供路由，不限制带宽 • 基于特定区域或呼叫搜索空间配置的选择性路由
Unified Communications Manager 在收到 SIP 180 振铃时发送 SIP-UPDATE 消息	<p>sip 干线会在“183 会话进度”后收到“180 振铃”时发送“更新”SIP 消息，前提是呼叫流程中支持“更新”值。</p>

功能	说明
通过 BFCP 共享显示	<p>如果要为 Cisco 终端部署演示共享，请确保在所有中间 SIP 干线的 SIP 配置文件中选中允许通过 BFCP 显示共享复选框。</p> <p>注释 对于第三方 SIP 终端，您还必须确保在电话配置窗口中选中相同的复选框。</p>
iX 通道	<p>如果要部署 iX 媒体通道，请确保在所有中间 SIP 干线使用的 SIP 配置文件中选中允许 iX 应用程序媒体复选框。</p> <p>注释 有关加密 iX 通道的详细信息，请参阅《<i>Cisco Unified Communications Manager 安全指南</i>》。</p>
90 天评估许可证	<p>在 90 天评估期内运行时，您无法部署安全 SIP 干线。要部署安全的 SIP 干线，您的系统必须已注册到 Smart Software Manager 帐户，并且选择了允许导出受控的功能产品注册令牌。</p>

H.323 干线概述

如果采用 H.323 部署，H.323 干线提供远程群集和其他 H.323 设备（例如网关）的连接。H.323 干线支持 Unified Communications Manager 支持的用于群集内通信的大多数音频和视频编解码器，宽带音频和宽带视频除外。H.323 干线将 H.225 协议用于呼叫控制信令，并将 H.245 协议用于媒体信令。

在 Cisco Unified CM 管理内，H.323 干线可通过群集间干线（非网守控制）干线类型和协议选项进行配置。

如果采用非网守 H.323 部署，必须为本地 Cisco Unified Communications Manager 可以通过 IP WAN 呼叫的远程群集中的每个设备池配置单独的群集间干线。群集间干线静态指定远程设备的 IPv4 地址或主机名。

您可以为一个干线配置多达 16 个目标地址。

群集间干线

在两个远程群集之间配置群集间干线连接时，必须在每个群集上配置群集间干线，并匹配干线配置，以使一个干线使用的目标地址与远程群集中干线使用的呼叫处理节点相匹配。例如：

- 远程群集干线使用“在所有活动节点上运行”——远程群集干线使用所有节点进行呼叫处理和负载均衡。在源自本地群集的本地群集间干线中，为远程群集中的每个服务器添加 IP 地址或主机名。
- 远程群集未使用“在所有活动节点上运行”——远程群集干线使用 Unified Communications Manager 组中分配给该干线设备池的服务器进行呼叫处理和负载均衡。在本地群集间干线配置中，您必须添加远程群集干线设备池使用的 Unified Communications Manager 组中的每个节点的 IP 地址或主机名。

保证干线安全

要为 H.323 干线配置安全信令，必须在干线上配置 IPSec。有关详细信息，请参阅《Cisco Unified Communications Manager 安全指南》。要配置干线以允许媒体加密，请选中干线配置窗口中的“允许 SRTP”复选框。



注释 网守不再被广泛使用，但您也可以将 H.323 部署配置为使用网守控制干线。有关如何设置网守控制干线的详细信息，请参阅《Cisco Unified Communications Manager 管理指南 10.0(1) 版》。

H.323 干线前提条件

计划您的 H.323 部署拓扑。对于群集间干线，请确保您知道相应的远程群集干线使用哪些服务器进行呼叫处理和负载均衡。您必须配置本地群集间干线以连接到远程群集中的干线使用的每个呼叫处理服务器。

如果使用分配给干线设备池的 Cisco Unified Communications Manager 组进行干线上的负载均衡，请完成[设备池的核心设置配置任务流程](#)，第 74 页一节中的配置。

配置 H.323 干线

使用此程序可为 H.323 部署配置干线。

过程

- 步骤 1** 从 Cisco Unified CM 管理中，选择**设备 > 干线**。
- 步骤 2** 单击**新增**。
- 步骤 3** 从干线类型下拉列表框中，选择**群集间干线（非网守控制）**。
- 步骤 4** 从协议下拉列表框中，选择**群集间 SCCP**。
- 步骤 5** 在设备名称文本框中，输入干线的唯一标识符。
- 步骤 6** 从设备池下拉列表框中，选择您为此干线配置的设备池。
- 步骤 7** 如果要使用本地群集中的每个节点来处理此干线，请选中在**所有活动的 Unified CM 节点上运行**复选框。
- 步骤 8** 如果要在干线上允许加密的媒体，请选中**允许 SRTP**复选框。
- 步骤 9** 如果要配置 H.235 传递，请选中**允许通过允许传递**复选框。
- 步骤 10** 在**远程 Cisco Unified Communications Manager 信息**部分，输入此干线连接到的每个远程服务器的 IP 地址或主机名。



第 11 章

配置网关

- [网关概述，第 93 页](#)
- [网关设置前提条件，第 94 页](#)
- [网关配置任务流程，第 94 页](#)

网关概述

Cisco 提供各种各样的语音和视频网关。网关提供允许 Unified Communications 网络与外部网络通信的接口。传统上，网关用于将基于 IP 的 Unified Communications 网络连接到传统电话接口（例如 PSTN）、专用主机交换 (PBX) 或传统设备（例如模拟电话或传真机）。在最简单的形式中，语音网关有 IP 接口和传统电话界面，网关在两个网络之间转换消息，从而使两个网络能够通信。

网关协议

大多数 Cisco 网关提供多个部署选项，可以使用多个协议中的任意一种协议部署。根据您要部署的网关，您的网关可以使用以下任何通信协议进行配置：

- 媒体网关控制协议 (MGCP)
- 内部呼叫控制策略 (SCCP)
- 会话发起协议 (SIP)
- H.323

供应商接口卡

供应商接口卡 (VIC) 必须安装在网关上，以便为外部网络提供连接接口。大多数网关提供多个 VIC 选项，并且每个 VIC 可能为模拟和数字连接提供许多不同的端口和连接类型。

请参阅您的网关文档，了解与您的网关一起提供的协议、卡和连接。

网关设置前提条件

安装硬件

在 Cisco Unified Communications Manager 中配置网关之前，必须在网关硬件上执行以下任务：

- 安装和配置网关
- 在网关上安装任何供应商接口卡 (VIC)。
- 使用 CLI 在网关上配置 IOS。

有关详细信息，请参阅随您的网关提供的硬件和软件文档。



注释 要进入许多网关设备的默认网页，可以使用该网关的 IP 地址。确保超链接 url = http://x.x.x.x/，其中 x.x.x.x 是设备的点格式 IP 地址。每个网关的网页都包含网关的设备信息和实时状态。

规划网关部署

在 Cisco Unified Communications Manager 中配置网关之前，请确保您已准备好要在网关上配置的连接类型。可以使用 MGCP、SIP、H.323 或 SCCP 中的任何一种作为网关协议来配置许多网关。每类部署的连接类型根据您的协议和网关上安装的 VIC 而有所不同。请务必了解以下各项：

- 您的网关支持哪些网关协议。
- 网关上的 VIC 支持哪些类型的端口连接。
- 您计划配置哪些类型的连接？
- 对于模拟连接，您是连接到 PSTN、传统 PBX 还是传统设备。
- 对于数字接入连接，是连接到 T1 CAS 接口还是 PRI 接口？
- 对于 FXO 连接，您要如何定向来电？您是将来电定向到自动 IVR 还是助理？

网关配置任务流程

执行以下任务以将网络网关添加 Unified Communications Manager 中。

过程

	命令或操作	目的
步骤 1	根据您要部署的协议执行以下任一程序： <ul style="list-style-type: none">• 配置 MGCP 网关，第 95 页	在 Unified Communications Manager 中配置您的网关。可使用 MGCP、SCCP、SIP 或 H.323 中的任何一种作为网关协议来部署很多 Cisco

	命令或操作	目的
	<ul style="list-style-type: none"> 配置 SCCP 网关，第 102 页 配置 SIP 网关，第 105 页 配置 H.323 网关，第 106 页 	网关。查看网关文档确定您的网关支持哪些协议，以及哪种协议最适合您的部署。
步骤 2	为网关配置群集范围的呼叫分类，第 107 页	可选。配置群集范围内的服务参数以将来自网络中网关端口的所有呼叫归类为内部（网内）或外部（网外）。
步骤 3	阻止网外网关转移，第 108 页	可选。阻止 Unified Communications Manager 将来自外部（网外）网关的呼叫转接到另一外部网关，配置阻止网外到网外转接服务参数。

配置 MGCP 网关

执行以下任务配置 Cisco 网关配置以使用 MGCP 配置。

开始之前

确认 MGCP 网关的 Unified CM 端口连接。从 Cisco Unified CM 管理，转到 **系统 > Cisco Unified CM**，选择服务器并确认配置的 MGCP 侦听端口和 MGP 保持连接端口。在大多数情况下，无需更改默认端口设置。

过程

	命令或操作	目的
步骤 1	配置 MGCP (IOS) 网关，第 96 页	在 Cisco Unified CM 管理中添加网关，然后选择 MGCP 作为网关协议。使用适当的插槽和供应商接口卡 (VIC) 配置网关。
步骤 2	配置网关端口接口，第 96 页	<p>为连接至网关上安装的 VIC 的设备配置网关端口接口。大多数 VIC 包括多个端口连接和选项，因此您可能需要配置几种不同的端口接口类型。</p> <p>提示 配置端口接口后，从相关链接下拉列表中选择 返回到 MGCP 配置 选项，以返回网关配置窗口，您可在其中选择和配置另一端口接口。</p>
步骤 3	为 MGCP 网关添加数字接入 T1 端口，第 100 页	可选。如果您已配置数字接入 T1 CAS 端口接口，请将 T1 CAS 端口添加到网关。您可以逐个添加端口，也可以同时添加端口范围。

	命令或操作	目的
步骤 4	重置网关，第 101 页	配置更改将在重置网关后生效。

配置 MGCP (IOS) 网关

执行以下程序，向 Cisco Unified Communications Manager 添加并配置 MGCP (IOS) 网关。

过程

步骤 1 从 Cisco Unified CM 管理，选择 **设备 > 网关**。

步骤 2 单击新增。

步骤 3 从网关类型下拉列表中，选择网关，然后单击下一步。

步骤 4 从协议下拉列表中，选择 **MGCP**，然后单击下一步。

步骤 5 在配置的插槽、VIC 和终端区域中，执行以下步骤：

- a) 从每个模块下拉列表中，选择与网关上安装的网络接口模块硬件对应的插槽。
- b) 从每个子单元下拉列表中，选择安装在网关上的 VIC。
- c) 单击保存。

端口图标即会出现。每个端口图标对应于网关上的可用端口接口。您可以通过单击相应的端口图标来配置任何端口接口。

步骤 6 完成网关配置窗口中其余字段的设置。有关字段的更多信息，请参阅系统联机帮助。

步骤 7 单击保存。

配置网关端口接口

您可以为连接至网关上安装的 VIC 的设备配置端口连接。大多数 VIC 包括多个端口连接和选项，因此您可能需要配置几种不同的端口接口类型。

选择以下任何一项任务，具体取决于您要配置的接口类型：

- [配置数字接入 PRI 端口，第 96 页](#)
- [配置 MGCP 网关的数字接入 T1 端口，第 97 页](#)
- [配置 FXS 端口，第 98 页](#)
- [配置 FXO 端口，第 99 页](#)
- [配置 BRI 端口，第 99 页](#)

配置数字接入 PRI 端口

为 MGCP (IOS) 网关配置 PRI 端口接口。

开始之前

[配置 MGCP \(IOS\) 网关，第 96 页](#)

过程

步骤 1 从 Cisco Unified CM 管理中，选择 **设备 > 网关**。

步骤 2 单击**查找**并选择您要在其中配置 PRI 端口的网关。

步骤 3 在已配置的插槽、VIC 和终端区域中，找到包含您要配置的 BRI 端口的模块和子单元，然后单击与您要配置的 BRI 端口对应的端口图标。

网关配置窗口会显示 BRI 端口接口。

步骤 4 从设备池下拉列表中选择设备池。

步骤 5 完成网关配置窗口中其余字段的设置。请参阅联机帮助中的字段说明。

步骤 6 单击**保存**。

步骤 7 （可选）如果要为网关配置更多端口接口，请从**相关链接**下拉列表中选择**返回到 MGCP 配置**，然后单击**前往**。

网关配置窗口将显示网关可用的端口接口。

配置完更多端口接口后，请参阅[重置网关，第 101 页](#)。

配置 MGCP 网关的数字接入 T1 端口

为 MGCP (IOS) 网关上的数字接入 T1 CAS 端口配置端口接口。

开始之前

[配置 MGCP \(IOS\) 网关，第 96 页](#)

过程

步骤 1 从 Cisco Unified CM 管理，选择**设备 > 网关**。

步骤 2 单击**查找**并选择您要在其中配置 TI 端口的网关。

步骤 3 在配置的插槽、VIC 和终端区域中，找到您要设置数字接入 T1 (T1-CAS) 端口的模块和子单元，然后单击相应的端口图标。

步骤 4 从设备协议下拉列表中，选择**数字接入 T1**，并单击**下一步**。

步骤 5 输入合适的网关配置设置。

有关字段及其配置选项的更多信息，请参阅系统联机帮助。

步骤 6 单击**保存**。

有关向数字接入 T1 CAS 端口接口添加端口的详细信息，请参阅[为 MGCP 网关添加数字接入 T1 端口，第 100 页](#)。

配置 FXS 端口

在 MGCP 网关上配置外部交换站 (FXS) 端口。您可以使用 FXS 端口将网关连接到普通老式电话服务 (POTS) 传统电话或其他传统设备，例如传真机、免持话筒、传统语音留言系统或交互式语音应答 (IVR)。

开始之前

必须先添加网关，再配置端口。

过程

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

步骤 2 单击**查找**并选择您要在其中配置 FXS 端口的网关。

步骤 3 在配置的**插槽、VIC 和终端**区域，单击要配置的端口的 **FXS 端口** 图标。
此时会显示端口选择区域。

步骤 4 从**端口类型**下拉列表中，选择要配置的连接类型：

- **POTS**—如果要从此端口连接到 POTS 设备（例如传统电话），请选择此选项。
- **接地启动**—如果要使用接地启动信令将此端口连接到无人值守的传统设备（例如传真机、传统语音留言系统或 IVR），请选择此选项。
- **循环启动**—如果要使用循环启动信令将此端口连接到无人值守的传统设备（例如传真机、传统语音留言系统或 IVR），请选择此选项。

步骤 5 单击**下一步**。

端口配置窗口显示以模拟访问作为设备协议的端口接口的配置。

步骤 6 从**设备池**下拉列表中选择设备池。

步骤 7 完成**端口配置**窗口中其余字段的设置。

有关字段及其配置选项的更多信息，请参阅系统联机帮助。

步骤 8 单击**保存**。

步骤 9 （可选）要在 MGCP IOS 网关上配置更多端口接口，请从**相关链接**下拉列表中选择**返回到网关**，然后单击**前往**。

网关配置窗口将显示网关可用的端口。

配置完更多端口接口后，请参阅[重置网关，第 101 页](#)。

配置 FXO 端口

在 MGCP (IOS) 网关上配置外部交换局 (FXO) 端口。您可以使用 FXO 端口将网关连接到 PSTN 或传统 PBX。



注释 Unified Communications Manager 假定所有环路启动干线缺少积极断开连接监督。将具有积极断开连接监督的干线配置为接地启动，这样在服务器故障转移期间仍然可以维持正在进行的通话。

开始之前

[配置 MGCP \(IOS\) 网关，第 96 页](#)

过程

步骤 1 从 Cisco Unified CM 管理中，选择 **设备 > 网关**。

步骤 2 单击**查找**并选择您要为其配置 FXO 端口的网关。

步骤 3 在配置的插槽、VIC 和终端区域，找到包含您想要在其中设置 FXO 端口接口的 FXO 端口的模块和子单元并单击要配置的端口的端口图标。

步骤 4 从端口类型下拉列表中，选择**接地启动**或**环路启动**。

注释 如果配置 VIC-2 FXO 端口，则必须为子单元模块的两个端口选择相同的端口类型。

步骤 5 从设备池下拉列表中选择设备池。

步骤 6 在话务员目录号码文本框中，输入要从此端口连接路由所有传入呼叫的目录号码。例如，零或话务员目录号码。

步骤 7 完成端口配置窗口中任何其余字段的设置。请参阅联机帮助中的字段说明。

步骤 8 单击**保存**。

步骤 9 （可选）要在 MGCP IOS 网关上配置更多端口接口，请从**相关链接**下拉列表中选择**返回到网关**，然后单击**前往**。

网关配置窗口将显示网关可用的端口。

配置完更多端口接口后，请参阅[重置网关，第 101 页](#)。

配置 BRI 端口

为 MGCP (IOS) 网关配置 BRI 端口接口。

开始之前

[配置 MGCP \(IOS\) 网关，第 96 页](#)

过程

- 步骤 1 从 Cisco Unified CM 管理中，选择 **设备 > 网关**。
- 步骤 2 单击**查找**并选择您要在其中配置 BRI 端口的网关。
- 步骤 3 在配置的**插槽、VIC 和终端**部分，找到使用 BRI 端口的子单元并单击要配置的端口的**端口**图标。
网关配置窗口会显示 BRI 端口接口的信息。
- 步骤 4 从**设备池**下拉列表中选择设备池。
- 步骤 5 输入相应的“网关信息”和“端口信息”设置。有关字段及其配置选项的更多信息，请参阅系统联机帮助。
- 步骤 6 单击**保存**。
- 步骤 7 （可选）如果要为网关配置更多端口接口，请从**相关链接**下拉列表中选择**返回到 MGCP 配置**，然后单击**前往**。

网关配置窗口显示 MGCP 网关的可用端口接口。

配置完更多端口接口后，请参阅[重置网关，第 101 页](#)。

为 MGCP 网关添加数字接入 T1 端口

将 T1 CAS 端口添加并配置到 MGCP 网关的 T1 数字接入端口接口。您可以添加和配置最多 24 个 T1 CAS 端口。您也可以逐个添加端口，也可以同时添加和配置端口范围。如果您输入端口范围，Unified Communications Manager 会将配置应用到整个端口范围。

开始之前

[配置 MGCP 网关的数字接入 T1 端口，第 97 页](#)

过程

- 步骤 1 在 Cisco Unified CM 管理中，选择**设备 > 网关**。
- 步骤 2 单击**查找**并选择包含 T1 CAS 端口接口的网关。
- 步骤 3 单击**添加新端口**。
- 步骤 4 从**端口类型**下拉列表中，选择要添加的端口类型并单击**下一步**。
- 步骤 5 在**起始端口号**和**结束端口号**字段中输入端口号，以指定要添加和配置的端口范围。
例如，输入 **1** 和 **10** 可同时将端口 1 到 10 添加到端口接口。
- 步骤 6 从**端口方向**下拉列表中，配置通过此端口的呼叫的方向：
 - **双向**—如果端口允许入站和出站呼叫，则选择此选项。
 - **入站**—如果端口只允许入站呼叫，则选择此选项。
 - **出站**—如果端口只允许出站呼叫，则选择此选项。

步骤 7 对于 EANDM 端口，从主叫方选择下拉列表中，选择您希望主叫号码如何显示连接到此端口的设备上的出站呼叫的方式：

- 始叫方 - 发送呼叫设备的目录号码。
- 第一个重定向号码 - 发送重定向设备的目录号码。
- 最后一个重定向号码 - 发送最后一个重定向呼叫的设备的目录号码。
- 第一个重定向号码（外部） - 发送应用外部电话掩码的第一个重定向设备的目录号码。
- 最后一个重定向号码（外部） - 发送应用外部电话掩码的最后一个重定向设备的目录号码。

步骤 8 单击保存。

步骤 9 如果要为 MGCP 网关配置更多端口，请从相关链接中选择返回到网关，然后单击前往。当数字接入 T1 端口接口出现时，执行以下步骤之一：

- 如果要向此端口接口添加其他数字接入 T1 CAS 端口，请返回此程序的步骤 3（添加新端口）。
- 如果要在网关上配置多个端口接口，请从相关链接中选择返回到 MGCP 配置，然后单击前往。网关配置窗口将显示网关子单元模块的可用端口。
- 配置完更多端口接口后，请参阅[重置网关，第 101 页](#)。

重置网关

大多数网关需要重置，以使配置更改生效。我们建议您先完成所有必要的网关配置，然后再执行重置。



注释 重置 H.323 网关只重新初始化 Unified Communications Manager 加载的配置并且不会实际重新启动或重置网关。

过程

步骤 1 从 Cisco Unified CM 管理，选择设备 > 网关。

步骤 2 单击查找并选择网关。

步骤 3 单击要重置的网关旁边的复选框，然后单击重置选定项。设备重置对话框将会显示。执行下列操作之一：

步骤 4 单击重置。

MGCP 主叫方 ID 限制

如果 FROM 标头在传入 SIP 请求中包含特殊字符，它会影响 SIP-MGCP/323 呼叫流程，并且系统会断开呼叫或显示问题。因此，修复请求到达 Unified Communications Manager 的网络节点。

例如：

- 特殊字符与字母搭配使用（如 "Per%cent"）会影响显示名称。
- 由于 CRCX 可能有问题，远程名称被发送到 MGCP 端，许多特殊字符（如 "0%09%0A%01%05%0A%01%03%0A%01%04"）可能会断开呼叫。

配置 SCCP 网关

执行以下任务以配置 Cisco 网关来使用 SCCP 配置。

过程

	命令或操作	目的
步骤 1	将 SCCP 配置为网关协议，第 102 页	配置网关以将 SCCP 用作网关协议。
步骤 2	为未配置的模拟 FXS 端口启用自动注册	为未配置的模拟 FXS 端口启用自动注册。
步骤 3	为模拟电话启用自动注册，第 103 页	为指定端口启用自动注册以从自动注册 DN 池中获取 DN。

将 SCCP 配置为网关协议

您可以配置 Cisco 网关以将 SCCP 用作网关协议。您可以使用此部署选项以使用 FXS 或 BRI 端口将 Unified Communications Manager 连接至模拟访问设备或 ISDN BRI 设备。您无法连接 SCCP 网关至数字接入 T1 或 E1 干线。

过程

-
- 步骤 1

从 Cisco Unified CM 管理，选择设备 > 网关。
- 步骤 2

单击新增。
- 步骤 3

从网关类型下拉列表中，选择使用 SCCP 的网关，然后单击下一步。
- 步骤 4

从协议下拉列表，选择 SCCP。
- 步骤 5

在配置的插槽、VIC 和子单元部分，执行以下步骤：

a)

对于每个模块下拉列表，选择与网关上安装的网络接口模块硬件对应的插槽。

b)

从每个子单元下拉列表中，选择安装在网关上的 VIC。
- 步骤 6

完成网关配置窗口中其余字段的设置。

有关字段及其配置选项的更多信息，请参阅系统联机帮助。
- 步骤 7

单击保存。

端口图标显示在子单元模块旁边。每个端口图标对应网关上的一个可配置端口接口。您可以单击对应的端口图标配置端口上的模拟访问或 ISDN BRI 电话。
- 步骤 8

完成更新后将更改应用至网关：

a)

单击重置网关。重置网关弹出窗口即会出现。

- b) 单击**重置**。

为模拟电话启用自动注册

为指定端口启用自动注册以从自动注册 DN 池中获取目录号码。默认情况下，Unified Communications Manager 不允许自动注册模拟电话。管理员必须配置网关模块以支持模拟电话通过使用 SCCP 协议的对应网关向 Unified CM 自动注册。



注释 支持的网关类型有 VG310、VG350、VG400、VG450 和 ISR4K 系列。

开始之前

- 启用自动注册并在连接至网络时指定分配至新终端的 DN 的范围。有关详细信息，请参阅[启用自动注册，第 363 页](#)一节。
- 在网关中使用 SCCP 协议启用自动配置。有关详细信息，请参阅[《适用于 SCCP 网关的 CUCM 自动配置指南》](#)。

过程

步骤 1 从 Cisco Unified CM 管理中，选择 **设备 > 网关**。

步骤 2 单击**新增**。

步骤 3 从**网关类型**下拉列表中，选择使用 SCCP 的网关，然后单击**下一步**。

步骤 4 从**协议**下拉列表，选择 **SCCP**。

步骤 5 在**网关详细信息**部分，执行以下步骤：

- a) 在文本框中输入 10 位数的 **MAC 地址**。在您输入 MAC 地址时，会自动填充**说明**字段值。

注释 网关的 MAC 地址可以是与 Unified Communications Manager 通信的 SCCP 网关接口中分配的以太网 MAC 地址或虚拟 MAC 地址。

当您提供 MAC 地址时，每个 FXS 端口从所配置的 MAC 地址获取端口名称及其端口号。对应的模拟电话即会自动注册到此网关。

例如，如果在模块的插槽 0 下拉列表中选择了 NM-4VWIC-MBRD，并且在**子单元 0** 下拉列表中选择了 VIC3-4FXS/DID-SCCP，则会显示 4 个 FXS 端口值，即 **0/0/0**、**0/0/1**、**0/0/2**、**0/0/3**。单击每个端口以在**电话配置**窗口的**说明**字段中查看对应的端口名称。所显示的端口名称是 MAC 地址和端口值的组合。

网关根据配置使用虚拟 MAC 地址或以太网 MAC 地址与 Unified Communications Manager 进行通信。即使在更换损坏的网关时也可使用虚拟 MAC 地址，因此您无需在 Unified Communication Manager 应用程序中执行任何配置更改。

- b) 从下拉列表中选择所需的 **Cisco Unified Communications Manager 组**可启用自动注册。

步骤 6 在配置的插槽、VIC 和终端部分，执行以下步骤：

- a) 为每个模块下拉列表选择与网关上安装的网络接口模块硬件对应的插槽，然后单击**保存**以启用相应的子单元。
- b) 为一个或多个子单元选择安装在网关上的对应 VIC，然后单击**保存**。

注释 插槽和模块指示哪个插槽和模块具有 FXS 端口。同时还指示 FXS 端口数量。

自动注册并获取自动 DN 时，最多只能配置子单元级别的网关，而不能配置端口级别的网关。例如，为 FXS 选择了子单元时，对应的 FXS 端口会选择自动注册 DN 池中可用的一个 DN，并将该 DN 分配给选定的端口。

步骤 7 单击应用配置。

网关将为所有 FXS 配置的端口发送注册请求，而不管该端口是否连接到电话。

为未配置的模拟 FXS 端口启用自动注册

使用此程序可启用未配置的模拟 FXS 端口的自动注册。

过程

步骤 1 从 Cisco Unified CM 管理中，选择系统 > 服务参数。

步骤 2 从服务器下拉列表中，选择正在运行的所需服务器。

步骤 3 从服务下拉列表中选择 **Cisco Call Manager（活动）**。

步骤 4 在群集范围参数（设备-PRI 和 MGCP 网关）部分中，确保为 **FXS 端口启用自动注册** 下拉列表的值设置为真。

注释 将为 **FXS 端口启用自动注册** 的值设置为假以禁用未配置模拟 FXS 端口的自动注册。

步骤 5 单击保存。

故障诊断提示

在 Unified Communications Manager 中执行以下工作，确保端口已注册并获取自动 DN。

1. 将 SCCP 配置为网关类型。
2. 启用自动注册
3. 选择模拟电话作为设备类型
4. 确保池中有空有足够的 DN 以容纳语音端口数量。

配置 SIP 网关

执行以下任务以在 Unified Communications Manager 中配置 SIP 网关。许多 Cisco 网关和第三方网关均可进行配置以使用 SIP。Unified Communications Manager 不包含 SIP 网关的网关设备类型。

开始之前

您必须在网络中安装网关硬件并在网关上配置 IOS 软件，然后再在 Unified Communications Manager 中添加网关。

过程

	命令或操作	目的
步骤 1	配置 SIP 配置文件，第 105 页	配置 SIP 设置并应用到 SIP 配置文件。干线使用此设置连接到 SIP 网关。
步骤 2	配置 SIP 干线安全性配置文件。 ，第 106 页	配置 SIP Trunk 安全性配置文件，以便干线使用此配置文件连接到 SIP 网关。您可以配置安全性设置，例如设备安全性模式、Digest 验证以及传入/传出传输类型设置。
步骤 3	配置 SIP 网关的 SIP 干线，第 106 页	配置指向 SIP 网关的 SIP 干线。将 SIP 配置文件和 SIP 干线安全性配置文件应用到 SIP 干线。

配置 SIP 配置文件

为您的 SIP 网关连接配置一个 SIP 配置文件。

过程

步骤 1 从“Cisco Unified CM 管理”中，选择设备 > 设备设置 > **SIP 配置文件**。

步骤 2 请执行以下步骤之一：

- 单击**新增**以创建新的配置文件。
- 单击**查找**以选择现有的 SIP 配置文件。

步骤 3 在 **SIP 配置文件配置**窗口完成字段设置。

有关字段及其配置选项的更多信息，请参阅系统联机帮助。

步骤 4 单击**保存**。

配置 SIP 干线安全性配置文件。

为连接到 SIP 网关的干线配置带有安全性设置的 SIP Trunk 安全性配置文件。

过程

步骤 1 在 Cisco Unified CM 管理中，选择系统 > 安全性 > **SIP Trunk** 安全性配置文件。

步骤 2 请执行以下步骤之一：

- a) 单击**查找**以选择现有的配置文件。
- b) 单击**新增**以创建新的配置文件。

步骤 3 在 **SIP Trunk** 安全性配置文件配置窗口完成字段设置。

有关字段及其配置选项的更多信息，请参阅系统联机帮助。

步骤 4 单击保存。

配置 SIP 网关的 SIP 干线

配置 SIP 干线以将 Unified Communications Manager 连接到使用 SIP 的 Cisco 或第三方网关。在此配置下，不要在**网关配置**窗口中输入网关作为设备。

过程

步骤 1 从 Cisco Unified CM 管理中，选择设备 > 干线。

步骤 2 单击**新增**以设置新的 SIP 干线。

步骤 3 从干线类型下拉列表中，选择 **SIP 干线**。

步骤 4 从协议下拉列表，选择无。

步骤 5 在“SIP 信息”窗格的目标地址字段中，输入 SIP 网关的 IP 地址、完全限定域名或 DNS SRV 记录。

步骤 6 从 **SIP Trunk** 安全性配置文件下拉列表中，选择您为此网关配置的 SIP Trunk 安全性配置文件。

步骤 7 从 **SIP** 配置文件下拉列表框中，选择您为此网关配置的 SIP 配置文件。

步骤 8 完成 **SIP** 干线配置窗口中字段的设置。请参阅联机帮助中的字段说明。

步骤 9 单击保存。

配置 H.323 网关

在 Unified Communications Manager 中为非网守 H.323 部署配置 H.323 网关。



注释 如果您的部署包括 H.323 网守，您还可以通过设置网守控制的 H.225 干线来添加 H.323 网关。本指南中并未介绍这种场景，因为网守使用在最近几年持续下降。如果要配置网守和 H.225 网守控制的干线，请参阅《Cisco Unified Communications Manager 管理指南 10.0 (1) 版》。



注释 将网关注册到 Unified Communications Manager 时，注册状态可能在 Unified Communications Manager 管理中显示为未知。

过程

步骤 1 从 Cisco Unified CM 管理，选择设备 > 网关。

步骤 2 单击新增。

步骤 3 在网关类型下拉列表中，选择 **H.323 网关**。

步骤 4 在设备名称字段中，输入网关的 IP 地址或主机名。

步骤 5 如果要使用 H.235 配置安全通道，请选中 **H.235 数据直通** 复选框。

步骤 6 配置网关配置窗口中的字段。

有关字段及其配置选项的更多信息，请参阅系统联机帮助。

步骤 7 单击保存。

步骤 8 单击重置以重置网关并应用更改。

大多数网关需要重置，以使配置更改生效。我们建议您先完成所有必要的网关配置，然后再执行重置。

为网关配置群集范围的呼叫分类

为您的网络网关配置呼叫分类设置。此设置确定系统是将网络中的网关视为内部（网内）还是外部（网外）。

呼叫分类字段也会在单独的网关端口界面的配置窗口中显示。默认情况下，每个网关端口界面配置为使用群集范围服务参数中的设置。但是，如果端口上的呼叫分类配置不同于群集范围服务参数，则该端口上的设置将覆盖服务参数设置。

过程

步骤 1 从 Cisco Unified CM 管理中，选择系统 > 服务参数。

步骤 2 从服务器下拉列表框中选择运行 Cisco CallManager 服务的服务器。

步骤 3 从服务下拉列表中，选择 **Cisco CallManager**。

步骤 4 在群集范围参数（设备 - 常规）下，配置呼叫分类服务参数的以下值之一。

- 网内 - 来自此网关的呼叫被归类为来自公司网络内部的呼叫。
- 网外 - 来自此网关的呼叫被归类为来自公司网络外部的呼叫。

步骤 5 单击保存。

阻止网外网关转移

如果要将系统配置为阻止从一个外部（网外）网关转接到另一个外部（网外）网关的呼叫，请执行此程序。默认情况下，系统允许从一个外部网关转接到另一个外部网关。

确定网关是否为外部（网外）或内部（网内）的设置由呼叫分类设置确定。它使用群集范围服务参数或通过配置以下任何端口接口进行配置：

- MGCP T1/E1 端口接口
- MGCP FXO 端口接口
- H.323 网关
- SIP 干线

过程

步骤 1 从 Cisco Unified CM 管理中，选择系统 > 服务参数。

步骤 2 从服务器下拉列表框中选择运行 Cisco CallManager 服务的服务器。

步骤 3 从服务下拉列表中，选择 **Cisco CallManager**。

步骤 4 配置阻止网外到网外转接服务参数的设置：

- 真—选择此选项以取消两个外部（网外）网关之间的转接。
- 假—选择此选项以允许两个外部（网外）网关之间的转接。这是默认选项。

步骤 5 单击保存。

注释 您还可以通过将网关与路由模式关联，将通过网关的呼叫分类为网内或往外，并在路由模式配置窗口中配置呼叫类别。



第 12 章

配置 SRST

- [Survivable Remote Site Telephony 概述，第 109 页](#)
- [Survivable Remote Site Telephony 配置任务流程，第 110 页](#)
- [SRST 限制，第 113 页](#)

Survivable Remote Site Telephony 概述

Survivable Remote Site Telephony (SRST) 是一项可选功能，适用节点取决于到 Unified Communications Manager 节点的广域网 (WAN) 连接。SRST 参考是在 Unified Communications Manager 管理界面中配置的，允许 IP 网关在发生 WAN 中断时为远程站点上的 IP 电话提供有限的电话服务：

- 远程站点上的 IP 电话可以彼此呼叫
- 来自 PSTN 的呼叫可以接通 IP 电话
- 来自 IP 电话的呼叫可以通过 PSTN 接通外部世界

当远程站点的电话失去与所有关联 Unified Communications Manager 节点的连接后，电话将连接到 SRST 参考 IP 网关。IP 电话上的状态线路指示显示电话已故障转移至备份 SRST 网关。当恢复与 Unified Communications Manager 的连接后，IP 电话将向 Unified Communications Manager 注册并回复全部电话服务。

SRST 支持远程站点，其中除了 PSTN 网关访问外可能还有 SCCP 和 SIP 终端的混合。

连接监视器持续时间

一旦能够通过 WAN 链接建立与 Unified Communications Manager 的连接，通过广域网 (WAN) 连接到 SRST 网关的 IP 电话会立即将自身重新连接到 Unified Communications Manager。但如果 WAN 链接不稳定，IP 电话将在 SRST 网关与 Unified Communications Manager 之间来回切换。此情况可导致临时失去电话服务（无拨号音）。这些重新连接尝试（称为 WAN 链接间断问题）将继续，直到 IP 电话将自身成功重新连接到 Unified Communications Manager。

要解决 Unified Communications Manager 与 SRST 网关之间的 WAN 链接抖动问题，您可以定义 IP 电话在从 SRST 网关注销并重新注册到 Unified Communications Manager 之前监控其与 Unified Communications Manager 连接的秒数（连接监控持续时间）。IP 电话接收 XML 配置文件中的连接监控持续时间值。

Survivable Remote Site Telephony 配置任务流程

开始之前

检查拨号方案。如果拨号方案中有 7 或 8 位数字，可能需要配置转换规则。有关转换规则的详细信息，请参阅[配置转换模式](#)，第 181 页。

过程

	命令或操作	目的
步骤 1	配置 SRST 参考 ，第 110 页	配置可在所有其他 Unified Communications Manager 节点无法接通时提供有限呼叫控制功能的网关。
步骤 2	分配 SRST 参考给设备池 ，第 111 页	对于每个设备池，分配呼叫设备在 Unified Communications Manager 不可用时尝试完成呼叫时搜索的网关。
步骤 3	请执行以下任务之一： <ul style="list-style-type: none"> 配置群集的连接监控持续时间，第 111 页 配置设备池的连接监控持续时间，第 112 页 	可选： 配置连接监控持续时间。您可以应用群集范围内的默认值，或将配置应用到设备池中的设备。
步骤 4	在 SRST 网关上启用 SRST ，第 112 页	在网关上配置 SRST 参数。

配置 SRST 参考

SRST 参考包括当设备的所有其他 Cisco Unified Communications Manager 节点无法接通时可以提供有限 Cisco Unified Communications Manager 功能的网关。

过程

步骤 1 登录 Cisco Unified CM 管理，然后选择系统 > SRST。

步骤 2 单击新增。

步骤 3 配置 **SRST 参考** 配置窗口中的这些字段。有关字段及其配置选项的更多信息，请参阅系统联机帮助。

步骤 4 单击保存。

分配 SRST 参考给设备池

您可以为电话的每个设备池配置 SRST。分配 SRST 参考给设备池时，如果设备池中的所有电话无法接通任何 Cisco Unified Communications Manager 节点，它们将尝试连接到分配的 SRST 网关。

过程

步骤 1 在 Cisco Unified CM 管理上，选择系统 > 设备池。

步骤 2 单击**查找**并选择远程 IP 电话所注册的设备池。

步骤 3 在“漫游灵敏度设置”部分，从 **SRST 参考** 下拉列表中选择 SRST 参考。

SRST 参考 下拉列表包含以下选项：

- **禁用**—如果电话无法接通任何 Cisco Unified Communications Manager 节点，它不会尝试连接到 SRST 网关。
- **使用默认网关**—如果电话无法接通任何 Cisco Unified Communications Manager 节点，它将尝试作为 SRST 网关连接到其 IP 网关。
- **用户定义**—如果电话无法接通任何 Cisco Unified Communications Manager 节点，它不会尝试连接到此 SRST 网关。

步骤 4 单击**保存**。

配置群集的连接监控持续时间

此步骤是可选的。只有当您更改连接监控持续时间的系统值（企业参数）时，才需要完成此程序。

过程

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

步骤 2 在**连接监控持续时间**字段中输入值。默认值为 120 秒。您可以在此字段中输入的最大秒数为 2592000。

步骤 3 单击**保存**。

注释 您必须重新启动所有服务，此更改才能生效。

企业参数构成连接监控持续时间的群集默认值。但是，如果设备池中存在覆盖配置，则该设置将覆盖使用设备池的设备的企业参数设置。

配置设备池的连接监控持续时间

此步骤是可选的。仅在以下条件为真时才完成此程序：

- 您不想对连接监控持续时间使用群集范围内的值。
- 您要为此设备池定义单独的连接监控持续时间值。



提示 更改设备池的连接监控持续时间值时，只应用到所更新的设备池。所有其他设备池使用它们自己的连接监控持续时间字段中的值，或者使用在连接监控持续时间企业参数中配置的群集范围内的值。

过程

步骤 1 在 Cisco Unified CM 管理上，选择 **系统 > 设备池**。

步骤 2 单击 **查找** 并选择远程 IP 电话所注册的设备池。

步骤 3 在“漫游敏感设置”区域中，在 **连接监控持续时间** 字段中输入一个值。您可以在此字段中输入的最大秒数为 2592000。

注释 此设置将优先于连接监控持续时间的企业参数设置。

步骤 4 单击 **保存**。

在 SRST 网关上启用 SRST

开始之前

- [分配 SRST 参考给设备池，第 111 页](#)
- （可选）请执行以下任务之一：
 - [配置群集的连接监控持续时间，第 111 页](#)
 - [配置设备池的连接监控持续时间，第 112 页](#)

过程

步骤 1 登录到 SRST 网关（路由器）。

步骤 2 输入命令 **call-manager-fallback**
此命令在路由器上启用 SRST。

步骤 3 输入命令 **max-ephonesmax-phones**，其中 max-phones 是受支持的 Cisco IP 电话的最大数量。

- 步骤 4** 输入命令 **max-dn**max-directory-numbers，其中 max-directory-numbers 是路由器可支持的目录号码 (DN) 或虚拟语音端口的最大数量。
- 步骤 5** 输入命令 **ip source-address**ip-address，其中 ip-address 是预先存在的路由器 IP 地址，通常是路由器以太网端口的地址之一。
- 此命令可让 SRST 路由器通过指定的 IP 地址从 Cisco IP 电话接收消息。

SRST 限制

限制	说明
删除 SRST 参考	<p>您无法删除设备池或其他项目正在使用的 SRST 参考。要了解哪些设备池正在使用 SRST 参考，请单击 SRST 参考配置窗口中的从属关系记录链接。如果没有为系统启用从属关系记录，从属关系记录摘要窗口将显示一条消息。如果您试图删除正在使用的 SRST 参考，Unified Communications Manager 会显示一条错误消息。在删除当前正在使用的 SRST 参考前，执行以下一项或两项任务：</p> <ul style="list-style-type: none">• 将另一个 SRST 参考分配到正在使用您要删除的 SRST 参考的设备池。• 删除正在使用您要删除的 SRST 参考的设备池。 <p>注释 在删除 SRST 参考之前，请仔细检查以确保删除正确的 SRST 参考。删除后的 SRST 参考无法取回。如果意外删除了 SRST 参考，必须重新创建。</p>



第 13 章

配置媒体资源

- [关于媒体资源，第 115 页](#)
- [媒体资源配置任务流程，第 130 页](#)

关于媒体资源

Cisco Unified Communications Manager 功能需要使用媒体资源。Cisco Unified Communications Manager 包含媒体资源，例如：

- 报警器
- 交互式语音应答 (IVR)
- 媒体终结点 (MTP)
- 转码器
- 信任的中继点
- 会议桥
- 音乐保持/视频保持

您可以通过将媒体资源分配给媒体资源组列表，然后将该列表分配给设备池或单个设备，从而使呼叫可以使用媒体资源。单个设备的默认设置是使用分配给该设备所使用设备池的媒体资源。



注释 有关配置音乐保持的详细信息，请参阅《*Cisco Unified Communications Manager* 的功能配置指南》。

媒体终结点

媒体终结点 (MTP) 是一个实体，它接受两个全双工媒体流，将这些流桥接在一起，并允许独立设置和拆解它们。Cisco Unified Communications Manager 可以在媒体路径中插入 MTP 来解决许多问题：

- 充当信任的中继点 (TRP)

- 在 RTP 流的 IPv4 与 IPv6 之间进行转换
- 提供 SIP 干线上的 SIP Early Offer
- 解决 DTMF 传输不匹配
- 充当 RSVP 座席

H.323 呼叫的 MTP

可以将媒体终结点插入 H.323 呼叫的媒体路径中，以扩展补充服务，例如呼叫保持、呼叫转接、呼叫暂留和会议，这些功能通常在将呼叫路由到 H.323 终端时不可用。对于 H.323 补充服务，只有不支持空功能集 (ECS) 或 FastStart 的终端需要 MTP。支持 ECS 和 FastStart 的所有 Cisco 和其他第三方终端都不需要 MTP。

MTP 类型

Cisco Unified Communications Manager 支持以下 MTP 类型：

- IOS 网关中的软件 MTP
- IOS 网关中的硬件 MTP
- Cisco IP 语音媒体流服务提供的软件 MTP

Cisco 媒体终结点软件 MTP 类型默认提供 48 个 MTP（用户可配置）资源，具体取决于网络和网络接口卡 (NIC) 的速度。例如，100-MB 的网络/NIC 卡能够支持 48 个 MTP 资源，而 10-MB NIC 卡则不能。

对于 10 MB 网络/NIC 卡，可以提供大约 24 个 MTP 资源。但是，确切的可用 MTP 资源数量视该 PC 上其他应用程序消耗的资源、处理器的速度、网络负载及其他各种因素而定。

MTP 注册

如果该 Unified Communications Manager 可用，则 MTP 设备始终向其主 Unified Communications Manager 注册，并通知该 Unified Communications Manager 其支持多少 MTP 资源。您可以将多个 MTP 向同一 Unified Communications Manager 注册。多个 MTP 向同一 Unified Communications Manager 注册时，该 Cisco Unified Communications Manager 将控制每个 MTP 的资源组。

例如，考虑将 MTP 服务器 1 配置为用于 48 个 MTP 资源，而 MTP 服务器 2 配置为用于 24 个资源。如果两个 MTP 都向同一 Unified Communications Manager 注册，则该 Unified Communications Manager 维护两组共 72 个注册的 MTP 资源。

当 Unified Communications Manager 确定呼叫终端需要 MTP 时，它将从具有最少活动流的 MTP 分配一个 MTP 资源。该 MTP 资源代表终端被插入到呼叫中。MTP 资源使用对系统的用户和其代表插入的终端仍然不可见。如果 MTP 资源在需要时不可用，则呼叫将不使用 MTP 资源连接，并且该呼叫没有补充服务。

SRTP DTMF 交互工作



重要事项 此部分适用于 14SU3 及更高版本。

目前，Unified CM 会在安全呼叫和非安全呼叫中为 DTMF 不匹配插入 MTP。但是对于安全呼叫，虽然为 DTMF 不匹配插入了 MTP，但它只会通过媒体在双方之间传送。因此，DTMF 事件不会在各方之间发送。在 Unified CM Release 14SU3 之前，只有为 DTMF 不匹配分配了 MTP 时，DTMF 转换才会对非安全呼叫有效。

从网关 IOS 版本 17.10.1a 开始，支持安全 MTP 通过网关端进行 DTMF 转换。注册到 Unified Communications Manager 的基于安全 IOS 的 MTP 现在具有 SRTP DTMF 互通支持。通过这种从网关添加的支持，从版本 14SU3 开始，Unified CM 可以为安全终端之间的 DTMF 不匹配调用硬件 MTP（使用 SRTP DTMF 互通支持）。

Unified Communications Manager 现在将 SRTP 密钥发送到 SCCP 消息中的 MTP。MTP 使用密钥将带内 DTMF 事件解密为带外事件，并将其发送到其他呼叫分支。同样，对于带外 DTMF 事件，Unified Communications Manager 会将加密的带内 DTMF 事件加入其他呼叫分支。

重要注意事项

- Unified Communications Manager 从 14SU3 版开始支持此功能，其中 Cisco IOS XE 17.10.1a 向前执行以下操作：
 - Cisco 4461 集成多业务路由器 (ISR)
 - Cisco Catalyst 8200 系列边缘平台
 - Cisco Catalyst 8300 系列边缘平台
 - Cisco Catalyst 8000V 边缘软件



注释 有关此功能所需网关配置的详细信息，请参阅支持的 Cisco IOS XE 17.10.1a 和更高版本平台的相应配置指南。

- Unified Communications Manager 与网关之间成功的 TLS 1.2 连接是必需的。有关配置 TLS 1.2 的详细信息，请参阅 [Cisco Unified Communications Manager 安全指南](#)。
- 只有直通模式下的硬件 MTP 支持此功能，即使用 IOS 网关注册的 MTP，IOS 网关在直通模式下支持 DTMF-SRTP 互通。
- 基于 IPVMS 的 MTP 和 H.323 呼叫流程不支持此功能。

媒体终结点相互作用和限制

表 7: 媒体终结点相互作用和限制

限制	说明
Cisco IP 语音流应用	<p>每台服务器只能激活一个 Cisco IP 语音流应用。要提供更多 MTP 资源，您可以在其他联网的服务器上激活 Cisco IP 语音流应用。</p> <p>思科强烈建议您不要在呼叫处理负载较高的 Cisco Unified Communications Manager 上激活 Cisco IP 语音流媒体应用，否则可能会对 Cisco Unified Communications Manager 的性能产生不良影响。</p>
正在向 Cisco Unified Communications Manager 注册	<p>每个 MTP 一次只能向一个 Cisco Unified Communications Manager 注册。系统可能有多个 MTP，每个可注册到一个 Cisco Unified Communications Manager，具体视系统如何配置而定。</p>
故障转移和回退	<p>本节介绍 Cisco Unified Communications Manager 变为不可用时在其上注册的 MTP 设备如何故障转移和回退：</p> <ul style="list-style-type: none"> • 如果主要 Cisco Unified Communications Manager 发生出现故障，MTP 将尝试向指定用于 MTP 所属设备池的 Cisco Unified Communications Manager 组中下一个可用的 Cisco Unified Communications Manager 注册。 • 一旦主要 Cisco Unified Communications Manager 在故障后变为可用且当前未使用，MTP 设备将立即向其注册。 • 系统保持活动的呼叫或会议处于呼叫保留模式，直到所有各方断开连接。系统无法提供补充服务。 • 如果 MTP 尝试向新 Cisco Unified Communications Manager 注册并且从未收到注册确认，MTP 将向下一个 Cisco Unified Communications Manager 注册。 <p>MTP 设备在硬重置或软重置后将注销，然后断开连接。重置完成后，设备将向 Cisco Unified Communications Manager 重新注册。</p>

转码器

转码器是执行编解码器转换，将来自某个编解码器的输入流转换成使用不同编解码器的输出流的设备。例如，编解码器可以采用 G.711 流，并将其实时转换为 G.729 流。如果通话期间，两个终端使用不同的语音编解码器时，Cisco Unified Communications Manager 会在媒体路径中调用转码器。转码器在两个不兼容的编解码器之间转换数据流，以便设备之间能够通信。转码器对呼叫涉及的用户或终端不可见。

转码器资源由媒体资源管理器 (MRM) 管理。

Opus 编解码器转码器支持



重要事项 此部分适用于 14SU1 及更高版本。

Cisco Unified Communications Manager 现在包括信令客户端控制协议 (SCCP) 控制的基于 iOS 的注册媒体资源，支持成功媒体协商所需的转码 Opus 音频编解码器。

大多数 Cisco 终端都支持 Opus 编解码器。Opus 编解码器在低带宽环境中提供比 G711/G729 更好的质量。借助 Opus 编解码器转码器支持，Unified CM 调用转码器以解决 Opus 编解码器不匹配的问题，使得 Opus 编解码器端的比特率较低，远程端的比特率更高。但是，Opus 编解码器支持的转码器必须成功注册到 Unified CM。

支持的版本

Opus 转码功能适用于以下 Unified Communications Manager 和网关版本。

- Unified CM Version 14 SU1 和更高版本
- Gateway IOS 版本 IOS XE 17.6.1
- DSP 固件版本 58.2.0 和更高版本

配置

1. 使用支持 Opus 编解码器转码的集成服务路由器 (ISR) 网关配置转码器。Opus 编解码器必须添加到转码器配置文件中。
2. 在 Cisco Unified Communications Manager DSPFARM 配置文件中注册支持 Opus 编解码器的转码器。
3. 将转码器与请求转码的终端或干线的媒体资源组列表 (MRGL) 相关联，并将呼叫双方之间的区域设置配置为 7 kbps。



注释 当您将包含转码器的 MRGL 与呼叫双方的设备池相关联时，Unified CM 会调用适当的转码器进行媒体协商。有关详细信息，请参阅[配置转码器](#)。

具备 MTP 功能的转码器

除了编解码器转换之外，转码器还可以提供与媒体终结点 (MTP) 相同的功能。在需要转码器功能和 MTP 功能的情况下，系统将分配转码器，因为转码器可以同时提供这两组功能。如果只需要 MTP 功能，系统将从资源池分配转码器或 MTP。资源的选择将由媒体资源组决定。

如果软件 MTP 资源在需要时不可用，并且 Cisco Unified CM 管理 > 系统 > 服务参数 > 服务参数配置窗口中的如果信任的中继点分配失败则呼叫失效和如果 MTP 分配失败则呼叫失效字段设置为 'False'，

呼叫会尝试在不使用 MTP 资源的情况下连接。 如果需要硬件编解码器功能（以将一个编解码器转换为另一个）而转码器不可用，呼叫将失败。

转码器类型

Cisco Unified Communications Manager 管理中的转码器类型在下表中列出。



注释 用作转码器并提供 MTP/TRP 功能时，转码器支持 G.711 与所有编解码器（包括 G.711）之间的转码。

表 8: 转码器类型

转码器类型	说明
Cisco 媒体终结点硬件	此类型支持 Cisco Catalyst 4000 WS-X4604-GWY 和 Cisco Catalyst 6000 WS-6608-T1 或 WS-6608-E1，提供以下数量的转码会话： 对于 Cisco Catalyst 4000 WS-X4604-GWY <ul style="list-style-type: none">用于转码至 G.711-16 的 MTP 转码会话 对于 Cisco Catalyst 6000 WS-6608-T1 或 WS-6608-E1 <ul style="list-style-type: none">用于从 G.723 到 G.711 的转码/用于从 G.729 到 G.711-24 的 MTP 转码的每个物理端口转码会话数；每个模块 192 个会话
Cisco IOS 媒体终结点（硬件）	此类型支持 Cisco 2600XM、Cisco 2691、Cisco 3725、Cisco 3745、Cisco 3660、Cisco 3640、Cisco 3620、Cisco 2600 和 Cisco VG200 网关，提供以下数量的转码会话： 每个 NM-HDV <ul style="list-style-type: none">从 G.711 到 G.729-60 的转码从 G.711 到 GSM FR/GSM EFR- 45 的转码

转码器类型	说明
Cisco IOS 增强型媒体终结点（硬件）	<p>每个 NM-HD</p> <p>此类型支持 Cisco 2600XM、Cisco 2691、Cisco 3660、Cisco 3725、Cisco 3745 和 Cisco 3660 接入路由器，提供以下数量的转码会话：</p> <ul style="list-style-type: none"> • G.711 到 G.729a/G.729ab/GSMFR-24 的转码 • G.711 到 G.729/G.729b/GSM EFR-18 的转码 <p>每个 NM-HDV2</p> <p>此类型支持 Cisco 2600XM、Cisco 2691、Cisco 3725、Cisco 3745 和 Cisco 3660 接入路由器，提供以下数量的转码会话：</p> <ul style="list-style-type: none"> • G.711 到 G.729a/G.729ab/GSMFR-128 的转码 • G.711 到 G.729/G.729b/GSM EFR-96 的转码 <p>PVDM4</p> <ul style="list-style-type: none"> • 激活 PVDM4 模块（PVDM4-32、PVDM4-64、PVDM4-128、PVDM4-256） • T1/E1 模块上的 DSP 模块（PVDM4-32、PVDM4-64、PVDM4-128、PVDM4-256） • DSP NIM（NIM-PVDM4-32、NIM-PVDM4-64、NIM-PVDM4-128、NIM-PVDM4-256） <p>这些类型支持 ISR4K（ISR44xx、ISR43xx），C83xx 和 C82xx 平台提供以下数量的转码会话：</p> <ul style="list-style-type: none"> • G.711 到 G.729a/G.729ab/GSMFR-24 的转码 • G.711 到 G.729/G.729b/GSM EFR-18 的转码 • G.711 到 G.729a/G.729ab/GSMFR-128 的转码 • G.711 到 G.729/G.729b/GSM EFR-96 的转码 • G.711/G.729/G.729ab/G.729a/G.729b 到 Opus 的转码

转码器类型	说明
Cisco 媒体终结点 (WS-SVC-CMM)	<p>此类型为填充的每个子卡提供 64 个转码会话：一个子卡有 64 个转码会话，两个子卡有 128 个转码会话，三个子卡有 192 个转码会话，四个子卡有 256 个转码会话（最大值）。</p> <p>此类型提供以下编解码器任意组合之间的转码：</p> <ul style="list-style-type: none"> • G.711 a-law 和 G.711 mu-law • G.729 annex A 和 annex B • G.723.1 • GSM (FR) • GSM (EFR)

转码器相互作用和限制

转码器相互作用和限制

相互作用或限制	说明
删除转码器	<p>您无法删除已分配给媒体资源组的转码器。要找出哪些媒体资源组正在使用转码器，请在转码器配置窗口的相关链接下拉列表框中选择从属关系记录，然后单击前往。“从属关系记录摘要”窗口即会显示使用转码器的媒体资源组的相关信息。要查找有关媒体资源组的详细信息，请单击该媒体资源组，随后即会显示“从属关系记录详细信息”窗口。如果没有为系统启用从属关系记录，从属关系记录摘要窗口将显示一条消息。如果您试图删除正在使用的转码器，Cisco Unified Communications Manager 会显示一条消息。在删除某个正被使用的转码器前，必须从该转码器所分配到的媒体资源组中将其删除。</p>

相互作用或限制	说明
故障转移和回退	<p>转码器故障转移和回退运作方式如下：</p> <ul style="list-style-type: none"> 如果主 Unified Communications Manager 节点发生故障，转码器将尝试向指定用于转码器所属设备池的 Unified Communications Manager 组中的下一个可用节点注册。 一旦主 Cisco Unified Communications Manager 节点变为可用，转码器设备将立即向其注册。 转码器设备向变为不可访问的 Unified Communications Manager 节点注销。使用此转码配置文件进行转码的调用会移至保留状态，转码器会尝试向下一个可用节点注册。网关使用 RTP/RTCP 超时将资源释放通知给注册的 Unified Communications Manager。 如果转码器尝试向新的 Unified Communications Manager 节点注册并且从未收到注册确认，转码器将向列表中的下一个节点注册。 <p>硬重置或软重置之后，转码器设备将注销并断开连接。重置完成后，设备将向主 Cisco Unified Communications Manager 节点重新注册。</p>
Opus 编解码器转码器支持	<p>如果转码器配置文件已注册到 Unified Communications Manager，您将遇到以下场景：</p> <ul style="list-style-type: none"> 如果 ISR 网关支持 Opus 转码但 Unified CM 不支持，则系统会为编解码器不匹配分配转码器。但是，ISR 网关会拒绝 OpenReceiveChannel (ORC) 和 StartMediaTransmission (SMT) SCCP 消息，因为这些 SCCP 消息中不存在所需的参数。 如果 ISR 网关不支持 Opus 转码，而 Unified CM 支持 Opus 编解码器转码，则 Opus 的转码器分配请求失败。 如果终端支持 Opus 编解码器，其中文件组播传输协议 (FMTP) "sprop-stereo" 参数值之一在其 SDP 中设置为 1，则系统会将 "sprop-stereo" 值为 1 的 ORC/SMT 消息发送到网关，网关将拒绝 OLC/SMT。这最终会断开呼叫。

信任的中继点概述

信任的中继点 (TRP) 是 Cisco Unified Communications Manager 可以插入到媒体流以充当呼叫媒体控制点的 MTP 或转码器。TRP 可以在流上提供进一步的处理，并可确保流遵循特定的路径。

当呼叫需要信任的中继点时，Cisco Unified Communications Manager 分配已启用 TRP 功能的 MTP 或转码器。

配置

通过选中**媒体终结点配置**或**转码器配置**窗口中的**信任的中继点**复选框，MTP 和转码器都可被配置为提供 TRP 功能。

对于以下配置窗口，通过将**使用信任的中继点**字段设置为**打开**，您可以配置个别呼叫的 TRP 要求：

- 电话配置
- 网关配置
- 语音邮件端口配置
- 干线配置
- CTI 路由点配置
- 通用设备配置
- 通用设备模板配置
- 各种媒体资源配置（报警器、IVR、MTP、转码器、会议桥、音乐保持）

信任的中继点相互作用和限制

功能	交互和限制
资源预留协议 (RSVP)	如果为呼叫启用 RSVP，Cisco Unified Communications Manager 应首先尝试分配也标记为 TRP 的 RSVPAgent。否则，RSVPAgent 与终端之间将插入另一个 TRP 设备。
呼叫的转码器	如果呼叫需要转码器并且要在需要 TRP 的终端同一侧分配，Cisco Unified Communications Manager 应首先尝试分配也标记为 TRP 的转码器。否则，转码器与终端之间将插入另一个 TRP 设备。
终端的 MTP 分配	如果终端的需要媒体终结点和使用信任的中继点复选框已选中，Cisco Unified Communications Manager 应分配同时也是 TRP 的 MTP。如果管理员无法分配这类 MTP 或 TRP，则会显示呼叫状态。
TRP 分配	在大多数情况下，TRP 在用户应答呼叫后分配，因此如果呼叫由于无法分配 TRP 而失败，用户可能会在应答呼叫后收到忙音。（需要 MTP 的 SIP 出站分支或 H.323 出站 Faststart 代表例外。）
终端的 TRP 插入	如果为终端或者与设备关联的设备池选中 使用信任的中继点 复选框，Cisco Unified Communications Manager 必须为终端插入 TRP。如果 Cisco Unified Communications Manager 在如果信任的中继点分配失败则呼叫失败服务参数设置为真时无法分配 TRP，呼叫可能会失败。
TRP 和远程用户	不建议使用 TRP 为家庭远程用户提供安全的工作解决方案。Expressway 的 Mobile and Remote Access 才是建议的解决方案。

TRP 资源不足的呼叫行为

以下各节提供 MTP 资源分配不足时 Cisco Unified Communications Manager 如何处理呼叫的示例。最终的呼叫行为取决于那些终端是否需要 MTP 和 TRP，以及系统是否已配置为在 MTP 或 TRP 分配失败时自动使呼叫失败。

MTP 和 TRP 都需要

下表显示当为终端选中了需要媒体终结点 和使用信任的中继点选项，但没有充足的 MTP 和 TRP 资源时，呼叫是否失败。

最终呼叫状态取决于如果信任的中继点分配失败则呼叫失败 和如果 MTP 分配失败则呼叫失败服务参数是否设置为呼叫自动失败。

如果 TRP 分配失败则呼叫失败服务参数	如果 MTP 分配失败则呼叫失败服务参数	Unified CM 呼叫行为
真	真	是
真	假	是
假	真	是，如果 H.323 终端需要 MTP。
假	假	否

MTP/TRP 资源不足则呼叫自动失败未启用

下表显示当 MTP/TRP 资源存在不足以及如果信任的中继点分配失败则呼叫失败和如果 MTP 分配失败则呼叫失败 服务参数均设置为假时的呼叫行为。

需要 MTP = 是	使用 TRP = 是	资源分配状态	呼叫行为
Y	Y	已分配 TRP	由于不存在直通支持，因此仅限音频呼叫。
Y	是或否	仅 MTP	仅限音频呼叫。不支持 TRP。
Y	是或否	已分配“无”	如果为 H.323 终端选中“需要 MTP”，补充服务将被禁用。
N	Y	已分配 TRP	音频或视频呼叫取决于终端功能以及呼叫接收控制 (CAC)。补充服务仍然有效。
N	Y	已分配“无”	音频或视频呼叫。补充服务仍然有效，但不支持 TRP。

报警器概述

报警器是在 Cisco Unified Communications Manager 上运行的 SCCP 软件设备，可让您向 Cisco IP 电话和网关发送预先录制的消息和提示音。通过打开该节点上的 Cisco IP 语音媒体流服务，可以在群集节点上激活报警器。MLPP、SIP 干线、IOS 网关和软件会议桥等功能依赖于报警器将预定义的消息通过单向媒体流发送到电话或网关。此外：

- IPv4 和 IPV6 均受支持。当系统平台配置用于 IPv6 并且启用了 IPv6 企业参数时，报警器在双模式中自动配置。
- SRTP 受支持

报警器可扩展性

默认情况下，报警器支持 48 个并发的媒体流。您可以通过在其他节点上激活报警器或通过呼叫计数服务参数更改报警器媒体流的默认数量来添加容量。不过，除非在一个节点上禁用 **Cisco CallManager** 服务，否则建议不要在该节点上增大此值。

如果报警器在未运行 **Cisco CallManager** 服务的专用订阅方节点上运行，则报警器最多可支持 255 个并发通告流。如果专用订阅方节点满足 10000 个用户的 OVA 虚拟机配置，则报警器最多可以支持 400 个并发通告流。



注意 建议不要在具有高呼叫处理负载的 Unified Communications Manager 节点上激活报警器。

报警器与会议桥

在以下情况下，报警器将可用于会议桥：

- 如果包含信号器的媒体资源组列表被分配到会议桥所在的设备池。
- 如果信号器配置为默认媒体资源。

如果媒体资源组列表直接分配给控制会议的设备，则报警器对于会议桥不可用。

每个会议只支持一条通告。如果系统在播放当前通告时请求另一条通告，则新通告将预占正在播放的通告。

默认报警器通知和提示音

当您激活 Cisco IP 媒体流应用服务后，Cisco Unified Communications Manager 自动提供一组预先录制的报警器通知。通知或提示音将在以下情况下播放：

- 通知一为配置用于 Cisco 多级优先和预占的设备播放
- 插入音—参与者加入 ad hoc 会议之前。
- 回铃音—当您通过 IOS 网关在 PSTN 上转接呼叫时，报警器会播放提示音，因为网关在呼叫处于活动状态时无法播放提示音。

- 回铃音—当您在 H.323 群集间干线上转接呼叫时，播放提示音。
- 回铃音—当您将呼叫从运行 SCCP 的电话转接到 SIP 客户端时，播放提示音。

您无法更改默认的预先录制的报警器通知或添加其他通知。如果安装了 Cisco Unified Communications Manager 区域设置安装程序并且为 Cisco Unified IP 电话或设备池配置了区域设置，则支持通知的本地化。有关区域设置安装程序以及要为用户和（组合）网络区域设置安装的文件的信息，请参阅安装 *Cisco Unified Communications Manager*。要下载区域设置安装程序，请参阅 www.cisco.com 上的支持页面。

表 9: 预先录制的报警器通知

条件	通知
正在进行同等或较高优先级的呼叫。	因此无法完成您的呼叫。请挂断，然后重试。这是录音。
存在优先访问限制。	因此无法完成您的呼叫。请挂断，然后重试。这是录音。
有人尝试了未授权的优先级。	使用的优先级未授权用于您的线路。请使用授权的优先级或请求接线员协助。这是录音。
呼叫忙，或者管理员没有配置呼叫等待或预占的目录号码。	您拨打的号码正忙，而且没有配备呼叫等待或预占。请挂断，然后重试。这是录音。
系统无法完成呼叫。	您的呼叫在拨打后无法完成。请查阅您的目录并再次呼叫，或请求接线员协助。这是录音。
发生了服务中断。	因此无法完成您的呼叫。如果是紧急呼叫，请致电接线员。这是录音。

下表列出了报警器支持的提示音。

表 10: 提示音说明

类型	说明
忙音	当被叫号码忙时，会听到忙音。
插入音	在参与者加入 ad hoc 会议之前，听到的会议插入音。
回铃音	在以下场景下，会听到警报音： <ul style="list-style-type: none"> • 通过 IOS 网关在 PSTN 上转接呼叫时。 • 在 H.323 群集间干线上转接呼叫时。 • 当您将呼叫从 SCCP 电话转接到 SIP 客户端时。

交互式语音应答概述

交互式语音应答 (IVR) 设备可让 Cisco Unified Communications Manager 播放预录的功能通知（.wav 文件）到 Cisco Unified IP 电话和网关等设备。这些通知的播放设备所使用的功能需要“立即会议”等 IVR 通知。

添加节点时，IVR 设备会自动添加至该节点。IVR 设备将保持非活动状态，直到该节点上激活 Cisco IP 语音媒体流应用服务。

默认情况下，IVR 支持同时存在 48 个主叫方。您可以使用“Cisco IP 语音媒体流应用”服务参数更改 IVR 主叫方的数量。但我们建议您在节点上不要超过 48 个 IVR 主叫方。您可以根据要加入“立即会议”的到 IVR 的预计并行呼叫配置 IVR 的主叫方数量。



注意 不要在具有高呼叫处理负载的 Cisco Unified Communications Manager 节点上激活 IVR 设备。

默认 IVR 通知和提示音

当您激活 Cisco IP 媒体流应用服务后，Cisco Unified Communications Manager 自动提供一组预先录制的交互式应答响应 (IVR) 通知。您可以替换默认的预先录制的 IVR 通知。通知在以下情况下播放：

表 11: 预先录制的 IVR 通知

通知	条件
ConferenceNowAccessCodeFailed 通知	当与会者在超过最大尝试次数后输入错误的访问代码来加入 Conference Now 时播放。
ConferenceNowAccessCodeInvalid 通知	当与会者输入错误的访问代码时播放。
ConferenceNowCFBFailed 通知	在发起 Conference Now 时超出会议桥容量限制时播放。
ConferenceNowEnterAccessCode 通知	当与会者现在加入 Conference Now 并且主持人设置与会者访问代码时播放。
ConferenceNowEnterPIN 通知	当主持人或与会者尝试加入会议时播放。
ConferenceNowFailedPIN 通知	在主持人超出输入正确 PIN 的最大尝试次数后播放。
ConferenceNowGreeting 通知	播放 Conference Now 的问候语提示。
ConferenceNowInvalidPIN 通知	当主持人输入错误的 PIN 时播放。
ConferenceNowNumberFailed 通知	当主持人或与会者在超出最大尝试次数后输入错误会议号码时播放。
ConferenceNowNumberInvalid 通知	当主持人或与会者输入错误的会议号码时播放。

交互式语音应答限制

功能	限制
负载均衡	交互式语音应答 (IVR) 通过通用媒体设备驱动程序使用实时协议 (RTP) 流。此设备驱动程序也由 Cisco IP 语音媒体流应用服务提供的音乐保持 (MOH)、软件媒体终结点 (MTP)、软件会议桥 (CFB) 和报警器等其他软件媒体设备使用。 配置较大的呼叫量会影响系统性能。如果 Call Manager 服务在同一服务器节点上处于活动状态，这也会影响呼叫处理。
DTMF 数字	IVR 仅支持带外 (OOB) DTMF 数字收集方法。如果主叫设备与 IVR 之间的 DTMF 功能不匹配，则会分配 MTP。
编解码器	IVR 仅支持编解码器 G.711 (a-law 和 mu-law)、G.729 和宽频带 256K。如果主叫设备与 IVR 之间的编解码器不匹配，将分配转码器。

通知概述

在 Cisco Unified Communications Manager 管理中，使用 **菜单资源 > 通知** 菜单路径配置通知。通知有两种类别：

- 系统通知—用于正常的呼叫处理或作为示例功能通知的预定义通知。
- 功能通知—音乐保持 (MoH)、使用呼叫队列或外部呼叫控制的寻线引导等功能使用。您可以通过上传 Cisco 提供的音频文件或上传自定义 .wav 文件自定义您自己的功能通知。上传所有自定义通知 .wav 文件到群集中的所有服务器。



注释 如果您通过干线或网关连接，您可以听到自定义通知（例如警告或重拨提示音）。但是，您无法听到两个 IP 电话或 IP 电话与 Jabber 客户端之间的呼叫的自定义通知。

格式

建议的通知格式包括以下规格：

- 16 位 PCM wav 文件
- 立体声或单声道
- 48 kHz、44.1 kHz、32 kHz、16 kHz 或 8 kHz 的采样率

默认通知

您可以为系统通知上传自定义通知 .wav 文件或更改 Cisco 提供的文件。但是，您无法更改通知标识符。例如，当主叫方拨打无效的号码时播放系统通知 (VCA_00121)。这通常称为空呼叫通知。

表 12: “查找并列出通知” 窗口中的通知

通知标识符	说明
Gone_00126	系统: 死机
MLPP-BNEA_00123	系统: MLPP 忙灯未配备
MLPP-BPA_00122	系统: MLPP 较高优先级
MLPP-ICA_00120	系统: MLPP 服务中断
MLPP-PALA_00119	系统: MLPP 优先级访问限制
MLPP-UPA_00124	系统: MLPP 未授权优先级
Mobility_VMA	请按 1 连接
MonitoringWarning_00055	系统: 监控或录音
RecordingWarning_00038	系统: 录音
TemporaryUnavailable_00125	系统: 暂时不可用
VCA_00121	系统: 拨打是空号/无效号码
Wait_In_Queue_Sample	内置: 示例队列主叫方定期通知
Welcome_Greeting_Sample	内置: 示例主叫方问候语

媒体资源配置任务流程

完成这些任务以为您的系统配置媒体资源。

过程

	命令或操作	目的
步骤 1	激活软件媒体资源，第 131 页	打开 IPVMS 服务会激活服务器上的软件媒体资源。
步骤 2	配置媒体终结点，第 131 页	为您的系统配置媒体终结点 (MTP)。
步骤 3	配置转码器，第 132 页	将转码器资源添加到系统。
步骤 4	配置交互式语音应答 (IVR)，第 133 页	配置系统 IVR 的默认设置。
步骤 5	配置报警器，第 133 页	配置报警器的系统设置。

	命令或操作	目的
步骤 6	配置媒体资源组，第 133 页	将您的媒体资源添加到媒体资源组中。设置具有不同资源组合的多个组。
步骤 7	配置媒体资源组列表，第 134 页	创建可分配至终端或终端类的媒体资源组列表。
步骤 8	将媒体资源分配给设备或设备池，第 134 页	通过将媒体资源分配至设备或设备池，将媒体资源提供给终端。
步骤 9	配置通知，第 135 页	可选。 配置特定公告的设置。公告用于正常处理，或用于“保持音乐”或 IVR 之类的功能。
步骤 10	上传自定义通知，第 135 页	可选。 上传预录的公告。将文件分配给新的或现有的公告。

激活软件媒体资源

激活 **Cisco IP** 语音媒体流传输服务以打开以下软件媒体资源：

- 报警器
- 交互式语音应答 (IVR)
- 媒体终结点 (MTP)
- 软件会议桥
- 音乐保持

过程

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

步骤 2 从服务器中，选择 Unified Communications Manager 节点。

步骤 3 选中 **Cisco IP 语音媒体流传输服务** 并单击 **保存**。

配置媒体终结点

此程序用于配置软件媒体终结点 (MTP)。

开始之前

必须运行 **Cisco IP 语音媒体流服务**，软件媒体终结点 (MTP) 才能激活。

确定所需的 MTP 资源数量和提供这些资源所需的 MTP 设备数量。

过程

步骤 1 从 Cisco Unified CM 管理中，选择媒体资源 > 媒体终结点。

步骤 2 执行以下任一操作：

- 单击**查找**并选择现有 MTP。
- 单击**新增**以创建新的 MTP。

步骤 3 分配媒体终结点名称。

步骤 4 分配设备池。

步骤 5 如果要将此 MTP 指定为信任的中继点 (TRP)，请选中**信任的中继点**复选框。

步骤 6 单击**保存**。

配置转码器

转码器是用于将来自某个编解码器的输入流转换成使用不同编解码器的输出流的设备。

开始之前

要使 IVR 处于活动状态，必须运行 Cisco IP 语音媒体流服务。

确定所需的转码器资源数量和提供这些资源所需的转码器设备数量。

过程

步骤 1 登录 Cisco Unified CM 管理，然后选择媒体资源 > 转码器。

步骤 2 执行以下任一操作：

- 单击**查找**并选择现有转码器。
- 单击**新增**。

步骤 3 选择转码器类型。

步骤 4 输入转码器的 MAC 地址。

步骤 5 从下拉菜单中分配设备池。

步骤 6 如果您想将此转码器用作受信任的中继点，请选中**信任的中继点**复选框。

步骤 7 单击**保存**。

配置交互式语音应答 (IVR)

使用此程序可配置 IVR 的设置。

开始之前

要使交互式语音应答 (IVR) 处于活动状态，必须运行 Cisco IP 语音媒体流服务。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**媒体资源 > 交互式语音应答**。

步骤 2 单击**查找**并选择 IVR。

步骤 3 输入名称和说明。

步骤 4 如果想要 IVR 呼叫使用信任的中继点，请将**使用信任的中继点**下拉列表设置为**开**。

步骤 5 完成**交互式语音应答配置**窗口中其余字段的设置。有关这些字段及其设置的帮助，请参阅联机帮助。

步骤 6 单击**保存**。

配置报警器

配置报警器的系统设置。

开始之前

要使报警器处于活动状态，必须运行 Cisco IP 语音媒体流服务。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**媒体资源 > 报警器**。

步骤 2 单击**查找**并选择报警器。

步骤 3 输入名称和说明。

步骤 4 选择设备池。

步骤 5 如果想要报警器使用信任的中继点，请将**使用信任的中继点**下拉列表设置为**开**。

步骤 6 单击**保存**。

配置媒体资源组

媒体资源组包含要分配给终端或终端组的媒体资源列表。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**媒体资源 > 媒体资源组**。

步骤 2 执行以下任一操作：

- 单击**查找**并选择现有的媒体资源组。
- 单击**新增**以创建新的媒体资源组。

步骤 3 配置**媒体资源组配置**窗口中的字段。请参阅联机帮助，了解有关字段及其配置选项的信息。

步骤 4 输入组的名称和说明。

步骤 5 从**可用媒体资源**中，选择要添加到此组的资源，然后使用箭头将资源移至**所选的媒体资源**。

步骤 6 （可选）要将组播用于音乐保持音频，请选中**对 MOH 音频使用组播**复选框。

步骤 7 单击**保存**。

配置媒体资源组列表

创建媒体资源组的优先顺序列表。您可以将此列表分配到单个设备或设备池。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**媒体资源 > 媒体资源组列表**。

步骤 2 执行以下任一操作：

- 单击**查找**并选择现有列表。
- 单击**新增**并创建一个新列表。

步骤 3 输入媒体资源组列表的名称。

步骤 4 从**可用的媒体资源组**中，选择要添加的组，然后使用箭头将其移动到**所选媒体资源组**。

步骤 5 单击**保存**。

注释 要让终端使用这些媒体资源，必须将列表分配到设备池、网关端口或设备。

将媒体资源分配给设备或设备池

通过将优先媒体资源组列表关联到设备池或个别设备，将媒体资源分配给终端。

过程

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

- 要将媒体资源添加到设备池，请选择**系统 > 设备池**。
- 要将媒体资源直接添加到终端，请选择**设备 > 电话**。

步骤 2 单击**查找**，然后选择要将这些媒体资源分配到其中的设备池或设备。

步骤 3 从媒体资源组列表下拉列表中，选择一个列表。

步骤 4 单击**保存**。

步骤 5 单击**应用配置到选定项**。

应用配置窗口将会显示，其中显示了设备名称和适用的配置更改。

配置通知

您可以配置可用作系统通知或功能通知的通知。系统通知用于呼叫处理或使用示例功能通知，而功能通知用于特定功能，例如音乐保持 (MOH) 与寻线引导呼叫队列或外部呼叫控制关联。

您可以在 Cisco Unified Communications Manager 中修改现有通知或配置新通知。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**媒体资源 > 通知**。

步骤 2 执行下列操作之一：

- 单击**查找**并选择要编辑的现有通知。
- 单击**新增**以添加新通知。

步骤 3 配置**通知配置**窗口中的字段。有关字段及其配置选项的更多信息，请参阅系统联机帮助。

步骤 4 单击**保存**。

上传自定义通知

您可以使用上传的具有不同通知的自定义 .wav 文件修改默认通知。当您导入音频来源文件时，Unified Communications Manager 会处理该文件，并将其转换为供音乐保持 (MOH) 服务器使用的适当格式。



注释 通知是区域设置（语言）特定的。如果您的安装使用多种语言区域设置，则每个自定义通知必须以每种语言录制一个单独的 .wav 文件，然后使用正确的区域设置上传。此任务还要求在上传非美式英语的自定义通知 .wav 文件之前，必须在每个服务器上安装正确的区域设置包。

像 MOH 音频来源文件一样，建议的通知格式包括以下规格：

- 16 位 PCM .wav 文件
- 立体声或单声道
- 48 kHz、44.1 kHz、32 kHz、16 kHz 或 8 kHz 的采样率

您无法更新在 Unified Communications Manager 的**查找并列出通知**窗口中没有超链接的通知。您可以为 Cisco 提供的通知添加自定义的通知，这些通知在此窗口中有超链接。例如，MLPP-ICA_00120 和 MonitoringWarning_00055。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**媒体资源 > 通知**。

步骤 2 从**查找并列出通知**窗口中，输入搜索条件，单击**查找**，然后从结果列表中单击该通知的超链接。

步骤 3 在**通知配置**窗口中，单击**上传文件**。

步骤 4 在**上传文件**弹出窗口中，选择区域设置，输入文件名或浏览以选择 .wav 文件，然后单击**上传文件**。

上传过程开始，并且状态在处理完成后进行了更新。选择**关闭**以关闭**上传文件**窗口。

步骤 5 （可选）如果希望 Unified Communications Manager 播放自定义的通知，而不播放 Cisco 提供的通知，请选中**通知配置**窗口的按**区域设置**划分的**通知**窗格中的**启用**复选框。

如果**启用**复选框未选中，Unified Communications Manager 将播放 Cisco 提供的通知。

步骤 6 单击**保存**。

下一步做什么

为群集中的每个节点上传通知，因为通知文件不会在群集中的服务器之间传播。浏览群集中每个服务器上的 Cisco Unified Communications Manager 管理，并重复上传过程。



第 14 章

配置会议桥

- [会议桥概述，第 137 页](#)
- [会议桥类型，第 137 页](#)
- [会议桥配置任务流程，第 142 页](#)

会议桥概述

用于 Cisco Unified Communications Manager 的会议桥是专用于允许 ad hoc 和 ad hoc 语音会议的软件或硬件应用程序。其他会议桥类型支持其他类型的会议，包括视频会议。每个会议桥都可以托管多个同时进行的多方会议。硬件和软件会议桥可以同时激活。软件与硬件会议桥支持的流数和编解码器类型不同。当您添加新的服务器时，系统会自动添加软件会议桥。



注释

创建 Cisco Unified Communications Manager 服务器时，也会自动创建会议桥软件，并且不能删除。您无法将会议桥软件添加到 Cisco Unified Communications Manager 管理。

会议桥类型

以下会议桥类型可用于 Cisco Unified Communications Manager 管理。

表 13: 会议桥类型

会议桥类型	说明
Cisco 会议桥硬件	<p>此类型支持 Cisco Catalyst 4000 和 6000 语音网关模块及以下会议会话数量：</p> <p>Cisco Catalyst 6000</p> <ul style="list-style-type: none"> • G.711 或 G.729a 会议 - 每个端口 32 个参与者；每个会议最多 6 个参与者；每个模块总共 256 个参与者；10 个桥及三个参与者。 • GSM - 每个端口 24 个参与者；每个会议最多 6 个参与者；每个模块总共 192 个参与者。 <p>Cisco Catalyst 4000</p> <p>仅 G.711 会议 - 24 个与会者；最多 4 个会议，每个会议 6 个参与者</p>
Cisco 会议桥软件	<p>软件会议设备默认支持 G.711 编解码器。</p> <p>此类型的主叫方最大数量等于 256。设置为 256 时，软件会议桥可以支持 4 方，每方 64 个会议会话。会议会话中的主叫方的最大数量通过最大 Ad Hoc 会议和最大 MeetMe 会议单播服务参数指定。</p> <p>注意 此类会议桥（SW 会议桥）是一种简化实施。它不会识别静音方，并且使用简单的求和算法，当有大量参与者时，可能会导致会议的音频质量和音量较低。</p>
Cisco IOS 会议桥	<ul style="list-style-type: none"> • 使用 NM-HDV 或 NM-HDV-FARM 网络模块。 • G.711 a/mu-law、G.729、G.729a、G.729b 和 G.729ab 参与者可以加入一个会议呼叫 • 最多可以六方加入一个会议呼叫 <p>Cisco Unified Communications Manager 在动态基础上为呼叫分配会议资源。</p> <p>有关 Cisco IOS 会议和转码语音网关路由器的详细信息，请参阅随此产品收到的 Cisco IOS 文档。</p>

会议桥类型	说明
Cisco IOS 增强型网桥	<ul style="list-style-type: none"> 在 Cisco 2800 和 3800 系列语音网关路由器上使用板载思科数据包语音/传真数字信号处理器模块 (PVDM2) 或者使用 NM-HD 或 NM-HDV2 网络模块。 G.711 a-law/mu-law、G.729、G.729a、G.729b、G.729ab、GSM FR 和 GSM EFR 参与者可加入一个会议 最多可以八方加入一个呼叫。 <p>注释 由于 Unified Communications Manager 4096 最大流限制，所以使用 ISR4000 路由器和以及任何 SM-X-PVDM-3000/ SM-X-PVDM-2000/ SM-X-PVDM-1000/ SM-X-PVDM-500 时，每个会议桥配置文件最多可以注册 512 个会话。</p> <p>Cisco Unified Communications Manager 在动态基础上为呼叫分配会议资源。</p> <p>有关 Cisco IOS 增强型会议和转码语音网关路由器的详细信息，请参阅随此产品收到的 Cisco IOS 文档。</p> <p>对于部署了 ISR 4000 系列网关的受支持的 SIP 电话，此会议桥类型支持使用 AES_CM_128_HMAC_SHA1_80 的 SRTP 媒体加密。SCCP 电话和不支持的 SIP 电话回退到 AES_CM_128_HMAC_SHA1_32 加密。</p> <p>注释 请确保网关负载支持密码。有关支持的详细信息，请参阅网关文档。</p>
Cisco 会议桥 (WS-SVC-CMM)	<p>此会议桥类型支持 Cisco Catalyst 6500 系列和 Cisco 7600 系列通信媒体模块 (CMM)。</p> <p>它支持每个会议最多八方以及每个端口适配器最多 64 个会议。此会议桥类型支持以下编解码器：此会议桥类型支持 ad hoc 会议。</p> <ul style="list-style-type: none"> G.711 a-law/mu-law G.729 annex A 和 annex B G.723.1
Cisco 视频会议桥 (IPVC-35xx)	<p>Cisco 视频会议桥为 Cisco IP 视频电话、H.323 终端和纯音频 Cisco Unified IP 电话提供音频和视频会议功能。Cisco 视频会议桥支持 H.261、H.263 和 H.264 编解码器用于视频。</p>

会议桥类型	说明
Cisco IOS 异构视频会议桥	<p>思科集成业务路由器第 2 代 (ISR G2) 可用作基于 IOS 的会议桥，支持临时和 Meet-Me 视频会议。路由器上必须安装 DSP 模块才可用作会议桥。</p> <p>在异构视频会议中，所有会议参与者通过使用不同视频格式属性的电话连接到会议桥。异构视频会议需要 DSP 中的转码和传输功能来转换不同格式之间的信号。</p> <p>对于异构视频会议，主叫方在下列任一情况下作为音频参与者连接到会议：</p> <ul style="list-style-type: none"> • DSP 资源不足。 • 会议桥未配置为支持电话的视频功能。 <p>有关采用 ISR G2 路由器的视频会议的更详细信息，请参阅文档《配置视频会议和视频转码》。</p>
Cisco 担保音频视频会议桥	<p>思科集成业务路由器第 2 代 (ISR G2) 可用作基于 IOS 的会议桥，支持临时和 Meet-Me 语音和视频会议。路由器上必须安装 DSP 模块才可用作会议桥。</p> <p>DSP 资源保留用于会议的音频部分，视频服务不受保证。如果 DSP 资源在会议开始时可用，视频电话的主叫方便可使用视频服务。否则，主叫方将像音频参与者一样连接到会议。</p> <p>有关采用 ISR G2 路由器的视频会议的更详细信息，请参阅文档《配置视频会议和视频转码》。</p>
Cisco IOS 同构视频会议桥	<p>思科集成业务路由器第 2 代 (ISR G2) 可用作基于 IOS 的会议桥，支持临时和 Meet-Me 视频会议。路由器上必须安装 DSP 模块才可用作会议桥。</p> <p>Cisco IOS 同构视频会议桥是基于 IOS 的会议桥类型，支持同构视频会议。在同构视频会议中，所有会议参与者使用相同的视频格式属性连接。所有视频电话支持相同的视频格式，会议桥也向所有视频参与者发送相同的数据流格式。</p> <p>如果会议桥未配置为支持电话的视频格式，则该电话上的主叫方将作为纯音频参与者连接到会议。</p> <p>有关采用 ISR G2 路由器的视频会议的更详细信息，请参阅文档《配置视频会议和视频转码》。</p>

会议桥类型	说明
Cisco TelePresence MCU	<p>Cisco TelePresence MCU 是一组用于 Cisco Unified Communications Manager 的硬件会议桥。</p> <p>Cisco TelePresence MCU 是一种高清 (HD) 多点视频会议桥，其分辨率可达 1080p (30 帧/秒)，为所有会议提供完全的连续在网状态，可全面转码，非常适合于混合式 HD 终端环境。</p> <p>Cisco TelePresence MCU 支持以 SIP 作为信令呼叫控制协议。它内置有 Web 服务器，可用于全面配置、控制和监控系统及会议。Cisco TelePresence MCU 提供 HTTP 上的 XML 管理 API。</p> <p>Cisco TelePresence MCU 支持临时和 Meet-me 音频及视频会议。每个会议桥都可以托管多个同时进行的多方会议。</p> <p>Cisco Unified Communications Manager 支持 Unified Communications Manager 与 Cisco TelePresence MCU 之间二进制层控制协议 (BFCP) 的演示共享。</p> <p>Cisco TelePresence MCU 必须在端口预留模式下进行配置。有关详细信息，请查阅《<i>Cisco TelePresence MCU 配置指南</i>》。</p> <p>注释 Cisco TelePresence MCU 不支持通用的带外 DTMF 方法。在默认设置下，Cisco Unified Communications Manager 将无需媒体终结点 (MTP)。但是，如果“需要媒体终结点”复选框已选中，Cisco Unified Communications Manager 将分配 MTP，并且 SIP 干线将根据 RFC 2833 协商 DTMF。</p>
Cisco TelePresence Conductor	<p>Cisco TelePresence Conductor 提供智能的会议管理控制，可以扩展，支持用于在 MCU 之间均衡负载的设备群集以及多设备可用性。管理员可在支持 Cisco Unified Computing System (Cisco UCS) 平台或第三方平台的 VMware 上将 Cisco TelePresence Conductor 实施为设备或虚拟化应用程序。</p> <p>Cisco TelePresence Conductor 为每个新的会议动态选择最合适的 Cisco TelePresence 资源。临时、“Meet-me”以及计划的语音和视频会议可能动态扩展，超出个别 MCU 的容量。最多可以将三个 Cisco TelePresence Conductor 设备或虚拟化应用程序组成群集，提供更大的适应性。一个 Cisco TelePresence Conductor 设备或 Cisco TelePresence Conductor 群集的系统容量为 30 个 MCU 或 2400 个 MCU 端口。</p>

会议桥类型	说明
Cisco Meeting Server	<p>Cisco Meeting Server 会议桥解决方案支持临时会议、碰头会会议、Conference Now 会议和定点会议。此会议桥基于现场的音频、视频和 Web 会议，并可与第三方内地基础设施配合使用。它可扩展为小型或大型部署。您可以根据需要逐步增加容量，以确保您能够支持组织的当前和未来需求。此会议桥提供高级互操作性。任何数量的参加者都可以从以下位置创建和加入会议：</p> <ul style="list-style-type: none"> • Cisco 或第三方会议室或桌面视频系统 • Cisco Jabber Client • Cisco 会议应用（可以是本地或 WebRTC 兼容浏览器） • Skype 企业版 <p>使用 Cisco 会议服务器会议桥要求 Cisco 会议服务器的最低版本为 2.0。</p> <p>Cisco Meeting Server 支持以 SIP 作为信令呼叫控制协议。它内置有 Web 服务器，可用于全面配置、控制和监控系统及会议。Cisco Meeting Server 提供 HTTP 上的 XML 管理 API。</p> <p>注释 Cisco Meeting Server 不支持 H.265 视频编解码器和远端摄像机控制。</p>

会议桥配置任务流程

过程

	命令或操作	目的
步骤 1	配置会议桥，第 142 页	配置硬件或软件会议桥以允许临时和碰头会语音会议。
步骤 2	为会议桥配置服务参数，第 143 页	当您的网络中包含 Cisco IOS 会议桥和 Cisco IOS 增强型会议桥时，请执行此程序。
步骤 3	配置到会议桥的 SIP 干线连接，第 143 页	执行此程序以配置会议桥的 SIP 干线连接。

配置会议桥

您必须配置硬件或软件会议桥以允许临时和碰头会语音会议。

过程

步骤 1 从 Cisco Unified CM 管理中，选择媒体资源 > 会议桥。

步骤 2 单击新增。

步骤 3 配置会议桥配置窗口中的字段。要查看详细的字段说明，请参阅联机帮助。

步骤 4 单击保存。

下一步做什么

当您的网络中包含 Cisco IOS 会议桥和 Cisco IOS 增强型会议桥时，[为会议桥配置服务参数](#)，第 143 页。

为会议桥配置服务参数

当您的网络中包含 Cisco IOS 会议桥和 Cisco IOS 增强型会议桥时，请执行此程序。

过程

步骤 1 从 Cisco Unified CM 管理中，选择系统 > 服务参数。

步骤 2 在服务参数配置窗口中，选择服务器并选择 Cisco CallManager 服务。

步骤 3 在“群集范围参数（功能 - 会议）”部分中，将以下参数设置为 6：

- 最多临时会议
- 最多 MeetMe 会议单播

步骤 4 单击保存。

配置到会议桥的 SIP 干线连接

过程

步骤 1 从 Cisco Unified CM 管理中，选择设备 > 干线

步骤 2 完成以下步骤之一：

- 要创建新的 SIP 干线，请单击新增。
- 要将连接添加到现有干线，请单击“查找”并选择适当的干线。

步骤 3 选择设备协议作为 SIP。

步骤 4 选择干线服务类型作为无。

步骤 5 通过添加会议桥的 IP 地址或主机名，在目标区域中为会议桥创建条目。如果您需要一条新线路，可以单击 (+) 进行添加。

步骤 6 从**标准化脚本**下拉列表框中选择标准化脚本。例如，以下脚本为必需

- **cisco-telepresence-conductor-interop** - 如果您将此干线连接到 Cisco TelePresence Conductor，则选择此脚本。
- **cisco-telepresence-mcu-ts-direct-interop** - 如果您将此干线连接到 Cisco TelePresence MCU，则选择此脚本。
- **cisco-meeting-server-interop** - 如果您将此干线连接到 Cisco Meeting Server，则选择此脚本。

步骤 7 完成“干线配置”窗口中其余字段的设置。有关这些字段及其设置的帮助，请参阅联机帮助。

步骤 8 单击“保存”。



第 15 章

配置增强位置通话准入控制

- 增强位置通话准入控制概述，第 145 页
- 增强位置 CAC 前提条件，第 147 页
- 增强位置 CAC 任务流程，第 147 页
- 增强位置 CAC 相互作用限制，第 151 页

增强位置通话准入控制概述

增强型位置通话准入控制 (CAC) 可让您在复杂的 WAN 拓扑和群集间网络上调节音频质量和视频可用性。这包括多层和多跃点网络。

您可以创建完整网络拓扑的模型，表示连接这些位置的不同位置 (LAN) 和 WAN 链接。对于每个位置和 WAN 链接，分配带宽限制，表示一次可用于该链路上所有呼叫的总带宽。如果没有带宽可用于特定呼叫，系统会用占线信号拒绝呼叫。这样可以防止由于 WAN 链接被超额订用而导致音频和视频质量下降。

借助位置带宽管理器 (LBM) 复制组的群集间复制功能，您可以跨群集间网络复制位置配置，从而简化大型群集间网络中的管理工作。

增强型位置 CAC 组件

此功能使用以下组件：

- 位置 — 位置表示 LAN。位置可以包含终端，也可以仅作为链路之间的过渡位置用于 WAN 网络建模。Cisco Unified Communications Manager 最多支持 2000 个位置。
- 链路 — 两个位置之间的连接。配置此功能时，您可以为每个链路分配带宽分配和权重。
- 权重 — 在任何位置对之间形成有效路径时链路的相对优先级。权重仅在两个位置之间存在多个路径时使用。权重用于计算有效路径（累积权重最小的路径）。
- 带宽分配 — 在特定链路上分配给特定类型流量（音频、桌面视频、沉浸式视频）的总带宽。也可以为内部呼叫分配带宽（默认设置为无限制）。

- 位置带宽管理器 (LBM) — 必须在 Cisco Unified 功能配置中激活功能服务，增强型位置 CAC 才能发挥作用。此服务通过添加源和目标之间的所有链路和位置的权重，并选择累积权重最小的路径，来组装网络模型并计算位置之间的有效路径。

与区域的位置关系

增强型位置通话准入控制的位置配置与区域一起用于管理呼叫的带宽：

- 区域配置中的带宽分配旨在分配两个区域之间，呼叫中的终端可以使用的总带宽量。
- 位置配置中的带宽分配旨在分配这些位置之间，所有呼叫可以使用的总带宽量。对于单个呼叫，将从位置配置可用的带宽量中减去区域配置内的带宽。例如，如果位置配置指定特定链路上有 160 kb/s 的带宽可用，则该链路可以同时支持两个 80 kb/s 的 G.711 呼叫。



注释 在生产时间内，不要更改位置带宽管理器带宽或链路配置，因为这可能会不必要地导致服务器上的 CPU 使用率达到峰值。

Cisco Unified Communications Manager 支持每个群集 2,000 个位置和 2,000 个区域。

群集间 LBM 复制

位置带宽管理器中枢的群集间复制功能可让您跨较大的群集间网络复制位置和链路分配。您可以将 LBM 分配到 LBM 中枢角色，从而让它们主动在网状群集间网络中复制位置和链路信息。LBM 中枢通过共同的连接发现彼此，并形成完全网状结构的复制网络。分配了星形角色的 LBM 通过群集中的 LBM 中枢间接参与到群集间复制中。

群集间拓扑管理

配置和管理群集间网络的方式有多种。下表总结了两种配置和管理群集间拓扑的方法：

设计方法	说明
位置和链路管理群集	<p>使用单个群集配置和管理跨群集间网络的所有链路的带宽分配。此方法简化了配置开销，尤其是在有许多公共位置的部署中。群集间配置方法如下：</p> <p>在管理群集中，为整个拓扑配置所有位置和链路（包括带宽分配和权重）。此信息将复制到群集间网络。</p> <p>对于拓扑中的其他群集：</p> <ul style="list-style-type: none">• 仅配置本地群集的位置。这只是将设备关联到位置。• 不要配置链路信息。• 将本地群集中的所有带宽分配保留为无限制。如果管理群集复制的带宽分配小于本地群集，则将应用更严格的配置。

设计方法	说明
群集间增强型位置 CAC	<p>使用这种方法：</p> <ul style="list-style-type: none"> 在每个群集内，将本地位置和链路信息配置到仅相邻群集。 将链路信息（包括权重和带宽分配）分配到仅相邻群集。拓扑其余部分复制于 Hub_None 位置必须在每个群集中重命名，否则它将成为群集间的共同位置。 每个群集都需要一个唯一的群集 ID。 <p>注释 所有群集之间一致地命名群集对复制至关重要。</p>

增强位置 CAC 前提条件

确保您了解您的 LAN 和 WAN 网络拓扑之后，再尝试配置此功能。这是为位置和链路分配带宽的必须要求。

增强位置 CAC 任务流程

完成这些任务可在您的系统上配置增强位置通话准入控制。

过程

	命令或操作	目的
步骤 1	激活位置带宽管理器，第 148 页	Cisco 位置带宽管理器功能服务必须至少在一个群集节点上运行。
步骤 2	配置 LBM 组，第 148 页	默认情况下，Cisco CallManager 服务与本地 LBM 服务通信。不过，LBM 组可用于管理此通信，提供主动和备用 LBM 来实现冗余。
步骤 3	配置位置和链路，第 149 页	为您的网络创建位置 (LAN)，并为连接这些位置的 WAN 链接指定带宽分配。
步骤 4	配置 LBM 群集间复制组，第 149 页	创建将配置的 CAC 信息复制到其他群集的群集间复制组。
步骤 5	配置 SIP 群集间干线，第 150 页	将影子位置分配给网络中的 SIP 群集间干线。
步骤 6	配置通话准入控制服务参数，第 150 页	可选。为通话准入控制配置服务参数设置。对于许多部署而言，默认设置可能就足够了。

激活位置带宽管理器

对于增强位置通话准入控制，您必须在群集中的至少一个节点上激活 Cisco 位置带宽管理器功能服务。此服务默认关闭。

过程

步骤 1 从 Cisco Unified 功能配置中，选择工具 > 服务激活。

步骤 2 从服务器下拉列表中，选择要在其上运行该服务的群集节点，然后单击“转至”。

步骤 3 在 CM 服务下，选中 **Cisco 位置带宽管理器服务**

步骤 4 单击保存。

步骤 5 如果要在其他节点上启动该服务，请重复此任务。

注释 Cisco 建议在也同时运行 Cisco CallManager 服务的群集中的每个订阅方节点上运行 Cisco 位置带宽管理器服务。

配置 LBM 组

使用此程序可配置 LBM 组。默认情况下，Cisco CallManager 服务与本地 LBM 服务通信。不过，LBM 组可用于管理此通信，提供主动和备用 LBM 来实现冗余。



注释 Cisco CallManager 服务使用 LBM 的顺序如下：

- 指定 LBM 组
- 本地 LBM（共存）

过程

步骤 1 从 Cisco Unified CM 管理中，选择系统 > 位置 > 位置带宽管理器组。

步骤 2 单击新增。

步骤 3 为组指定名称。

步骤 4 从活动成员下拉列表中，选择此组的活动成员。

步骤 5 在备用成员下拉列表中，选择活动成员不可用时想要使用的备用成员。

步骤 6 单击保存。

配置位置和链路

使用此程序可在您的网络中创建位置 (LAN)。为使用这些位置间 WAN 链接的呼叫分配总带宽和权重。有关这些字段及其设置的帮助，请参阅联机帮助。

过程

-
- 步骤 1 从 Cisco Unified CM 管理中，选择系统 > 位置信息 > 位置。
 - 步骤 2 单击**新增**以创建新的位置。
 - 步骤 3 分配名称给位置。
 - 步骤 4 在**链路 - 介于此位置和相邻位置间的带宽**区域中，配置指向另一个位置的 WAN 链接设置：
 - a) 从**位置**列表框中选择另一个位置。
 - b) 配置**权重**以反映形成有效路径时此链路的相对优先级。
 - c) 配置音频、视频和沉浸式视频 (TelePresence) 呼叫的总带宽。
 - d) 重复这些子步骤以配置指向任何其他位置的链路。
 - 步骤 5 可选。展开**位置内 - 在此位置内的设备的带宽**区域，并为新创建的位置配置内部呼叫的总带宽分配。这些呼叫的所有媒体类型的默认设置为**无限制**。
 - 步骤 6 在**修改设置到其他位置**区域中，将 RSVP 设置配置到其他位置：
 - a) 在**位置**列中，选择其他位置。
 - b) 为这些位置之间的呼叫选择 **RSVP** 设置。
 - c) 重复这些子步骤以为具有其他位置的呼叫添加 RSVP 设置。
 - 步骤 7 单击**保存**。
 - 步骤 8 重复此过程可创建其他位置以及配置往来于这些新位置的链路。
-

配置 LBM 群集间复制组

使用此程序配置 LBM 群集间复制组。这是必需程序以复制群集间网络中增强型位置呼叫准入控制带宽信息。

过程

-
- 步骤 1 从 Cisco Unified CM 管理中，选择系统 > 位置信息 > 位置带宽管理器 (LBM) 群集间复制组。
 - 步骤 2 单击**新增**。
 - 步骤 3 输入组的名称。
 - 步骤 4 在**引导程序服务器**区域中，分配一个或多个 LBM 服务器，以负责将连接信息复制到其他中枢。
 - 步骤 5 在**角色分配**区域中，使用向上和向下箭头选择将充当中枢的本地 LBM 服务器，以及将保持为星形的 LBM 服务器。

步骤 6 单击保存。

配置 SIP 群集间干线

使用增强型位置通话准入控制，必须将影子位置分配给群集间网络中的 SIP 群集间干线。

过程

步骤 1 从 Cisco Unified CM 管理，选择设备 > 干线。

步骤 2 单击查找，然后选择适当的群集间干线。

步骤 3 从位置下拉列表，选择影子。

步骤 4 完成要在干线配置窗口中设置的任何其余字段。有关这些字段及其设置的帮助，请参阅联机帮助。

步骤 5 单击保存。

步骤 6 对于任何将复制增强型位置通话准入控制信息的任何其他集群间干线，请重复此任务。

配置通话准入控制服务参数

使用此程序配置增强型位置通话准入控制的可选服务参数。

过程

步骤 1 从 Cisco Unified CM 管理中，选择系统 > 服务参数。

步骤 2 从服务器下拉列表中，选择群集节点。

步骤 3 配置 Cisco CallManager 服务的服务参数：

- 从服务下拉列表中，选择 Cisco CallManager。
- 在群集范围参数（通话准入控制）区域中，配置任何服务参数。有关参数帮助说明，请单击 GUI 中的参数名称。
- 单击保存。

步骤 4 配置 Cisco 位置带宽管理器服务的设置：

- 从服务下拉列表中，选择 Cisco 位置带宽管理器。
 - 配置所需的任何服务参数。有关参数帮助说明，请单击 GUI 中的参数名称。
 - 单击保存。
-

增强位置 CAC 相互作用限制

下表显示增强型位置通话准入控制的功能相互作用和限制。

功能	交互和限制
LBM 安全模式	<p>默认情况下，LBM 安全模式为“不安全”。您可以使用 LBM 安全模式 企业参数重新配置此设置。此参数可设置为安全、不安全或混合。</p> <p>混合设置可临时使用以在确保所有群集安全时保持通信，之后可以将此设置更改为安全。</p> <p>更改此参数后，您必须重置群集中的所有 Cisco LBM 服务中枢以使其生效。</p>
视频呼叫中的音频带宽扣除	默认情况下，用于视频呼叫音频部分的带宽会从视频池扣除。您可以重新配置系统，通过将从视频呼叫的音频池扣除音频部分服务参数设置为真（默认设置为假），从音频池扣除视频呼叫的音频部分。
视频呼叫类别	<p>Cisco TelePresence 终端有不可配置的沉浸式视频呼叫分类。</p> <p>其他终端有不可配置的桌面视频呼叫分类。</p> <p>对于 SIP 干线，您可以通过配置关联 SIP 配置文件中的视频呼叫流量类别，以设置视频分类（桌面、沉浸式或混合）。</p>
媒体资源	媒体资源的带宽不会通过通话准入控制分配。
位置适用性	Cisco Unified 功能配置界面包含用于管理和监控位置拓扑的其他工具。有关详细信息，请参阅《Cisco Unified 功能配置管理指南》中的“位置”主题。
会话带宽限定符	您可以分配 SIP 终端在“SIP 配置文件配置”窗口中使用的会话带宽限定符。
带宽分配冲突	如果共同链路或位置上的带宽容量或权重分配有冲突，则本地群集使用最小的赋值。
设备支持	您的系统和 LBM 管理各类设备的带宽，包括 IP 电话、网关以及 H.323 和 SIP 干线目标。但是，群集间增强型位置 CAC 要求 SIP ICT 分配到系统影子位置。所有其他类型的设备仅在分配到普通（固定）位置时才受支持。
网络故障	在网络故障情况下，Unified Communications Manager 计算的带宽预留路径可能不会准确反映网络状况。没有合适的方法允许模型中的这种情景。
同步问题	系统创建的模型并非总是完美地同步。使用预留带宽分配可满足此限制。

功能	交互和限制
WAN 群集	对于通过 WAN 和本地故障转移部署的群集，群集内 LBM 流量已经被计算到 WAN 带宽中。
灵活 DSCP 标记	<p>对于其他 QoS，您可以使用 DSCP 标记来分配优先使用特定类型呼叫流的标记。例如，您可以确定音频优先级高于视频，以便在即使网络拥堵阻止视频媒体时，也可通过音频继续进行基本通信。</p> <p>您可以通过以下两种方式配置 DSCP 标记：</p> <ul style="list-style-type: none"> • 服务参数—在服务参数配置窗口的群集范围参数（系统 - QoS）部分中配置群集范围 DSCP 默认值。 • SIP 配置文件—在 SIP 配置文件中配置自定义 DSCP 设置，并将其应用到特定的 SIP 设备组。此设置将覆盖群集范围默认值。
APIC-EM 控制器	您可以使用 APIC_EM 控制器来管理外部 QoS 管理的 SIP 媒体流。有关详细信息，请参阅《Cisco Unified Communications Manager 功能配置指南》。



第 16 章

配置资源预留协议

- [RSVP 通话准入控制概述，第 153 页](#)
- [RSVP 通话准入控制前提条件，第 153 页](#)
- [RSVP 配置任务流程，第 153 页](#)

RSVP 通话准入控制概述

资源预留协议 (RSVP) 指定资源预留传输层协议，以预留 IP 网络中的资源。您可以使用 RSVP 替代增强型位置通话准入控制 (CAC)。RSVP 会为特定会话保留资源。会话包含具有特定目标地址、目标端口和协议标识符 (TCP 或 UDP) 的流。

RSVP 通话准入控制前提条件

您必须使用 IPv4 寻址。RSVP 不支持 IPv6 寻址。

RSVP 配置任务流程

过程		
	命令或操作	目的
步骤 1	配置群集范围的默认 RSVP 策略，第 154 页	配置群集中所有节点的 RSVP 策略。
步骤 2	配置位置对 RSVP 策略，第 155 页	可选。如果您希望位置对使用与群集其余部分不同的策略，可以为特定位置对配置 RSVP 策略。
步骤 3	配置 RSVP 重试，第 155 页	配置 RSVP 重试的频率和数量。
步骤 4	配置呼叫中 RSVP 错误处理，第 156 页	配置呼叫期间 RSVP 出现故障时系统的响应方式。

	命令或操作	目的
步骤 5	配置 MLPP 到 RSVP 优先级映射，第 157 页	可选。如果您使用多级优先和预占 (MLPP)，请将主叫方 MLPP 优先级映射为 RSVP 优先级。
步骤 6	配置 RSVP 座席。	在您的网关设备上执行此 IOS 程序。有关如何配置 RSVP 座席的信息，请参阅设备的文档。
步骤 7	配置应用程序 ID，第 158 页	配置 RSVP 应用程序 ID 时，系统会将标识符添加到语音和视频流量，以便 Cisco RSVP 座席能够根据其收到的标识符为任一类型的流量设置单独的带宽限制。
步骤 8	配置 DSCP 标记，第 158 页	配置 DSCP 标记，以便在 RSVP 保留失败时，系统可以指示 RSVP 座席或终端设备将媒体差分服务控制点 (DSCP) 标记更改为尽力而为。否则，过量 EF 标记的媒体数据包可能降低服务质量 (QoS)，甚至是有保留的流。

配置群集范围的默认 RSVP 策略

配置群集中所有节点的 RSVP 策略。

过程

步骤 1 在 Cisco Unified Communications Manager 管理中，选择系统 > 服务参数。

步骤 2 在服务参数配置窗口中，选择服务器并选择 Cisco CallManager 服务。

步骤 3 在群集范围参数（系统 - RSVP）部分中，配置“默认位置间 RSVP 策略”服务参数。

您可以将此服务参数设置为以下值：

- 无保留 - 无法在任意两个位置之间获得 RSVP 保留。
- 可选（需要视频） - 如果无法为音频和视频流获得保留，呼叫可以作为尽力而为的纯音频呼叫而继续。RSVP 座席会继续尝试音频的 RSVP 保留，并在保留成功时通知 Cisco Unified Communications Manager。
- 必需 - Cisco Unified Communications Manager 在 RSVP 保留对音频流（如果呼叫是视频呼叫，则还包括视频流）成功之前不会在终止设备上振铃。
- 必需（需要视频） - 如果对音频流的保留成功但视频流的保留不成功，视频呼叫可以作为纯音频呼叫继续。

下一步做什么

选择下列选项之一：

- 如果您希望位置对使用不同于群集其余部分的策略，则[配置位置对 RSVP 策略，第 155 页](#)。
- 如果对群集中的所有节点使用相同的 RSVP 策略，则[配置 RSVP 重试，第 155 页](#)。

配置位置对 RSVP 策略

如果您希望位置对使用与群集其余部分不同的策略，可以为特定位置对配置 RSVP 策略。使用此程序时，为位置对配置的 RSVP 策略会覆盖您为群集配置的策略。

过程

步骤 1 在 Cisco Unified Communications Manager 管理中，选择**系统 > 位置**。

步骤 2 查找位置对的一个位置，然后选择此位置。

步骤 3 要修改所选位置与另一个位置之间的 RSVP 策略，请选择位置对中的另一个位置。

步骤 4 在 **RSVP 设置** 下拉列表中，选择此位置对的 RSVP 策略。

您可以将此字段设置为以下值：

- **使用系统默认值** - 位置对的 RSVP 策略与群集范围的 RSVP 策略匹配。
- **无保留** - 无法在任意两个位置之间获得 RSVP 保留。
- **需要视频（可选）** - 如果无法为音频和视频流获得保留，呼叫可以作为尽力而为的纯音频呼叫而继续。RSVP 座席会继续尝试音频的 RSVP 保留，并在保留成功时通知 Cisco Unified Communications Manager。在针对音频流（如果是视频呼叫，则为视频流）的 RSVP 保留成功之前，系统不会振铃终端设备。
- **需要视频** - 如果对音频流的保留成功但对视频流的保留不成功，视频呼叫可以作为纯音频呼叫继续。

下一步做什么

[配置 RSVP 重试，第 155 页](#)

配置 RSVP 重试

使用此程序配置 RSVP 重试的频率和数量。

开始之前

- [配置群集范围的默认 RSVP 策略，第 154 页](#)

- 可选。 [配置位置对 RSVP 策略，第 155 页](#)

过程

步骤 1 在 Cisco Unified Communications Manager 管理中，选择系统 > 服务参数。

步骤 2 在“服务参数配置”窗口中，选择服务器并选择 Cisco CallManager 服务。

步骤 3 在“群集范围参数（系统 - RSVP）”部分中，配置指定的服务参数。

您可以将这些服务参数设置为以下值：

- **RSVP 重试计时器** - 指定 RSVP 重试计时器值（秒）。如果将此参数设置为 0，可在系统中禁用 RSVP 重试。
 - **必需 RSVP 呼叫中重试计数器** - 指定当 RSVP 策略为“必需”且呼叫中错误处理选项设置为“超出以下重试计数器时呼叫失败”时的呼叫中 RSVP 重试计数器。默认值为 1 次。如果将该服务参数设置为 -1，重试将无限期继续，直到预留成功或呼叫被中断。
-

下一步做什么

[配置呼叫中 RSVP 错误处理，第 156 页](#)

配置呼叫中 RSVP 错误处理

使用此程序配置呼叫中 RSVP 错误处理。

开始之前

[配置 RSVP 重试，第 155 页](#)

过程

步骤 1 在 Cisco Unified Communications Manager 管理中，选择系统 > 服务参数。

步骤 2 在“服务参数配置”窗口中，选择服务器并选择 Cisco CallManager 服务。

步骤 3 在“群集范围参数（系统 - RSVP）”部分中，配置指定的服务参数。

可将“必需 RSVP 呼叫中错误处理选项”服务参数设置为以下值：

- **呼叫变为尽力而为** - 如果 RSVP 在呼叫期间失败，呼叫将变为尽力而为的呼叫。如果重试已启用，将同时开始 RSVP 重试尝试。

- 超出以下重试计数器时呼叫失败 - 如果 RSVP 在呼叫期间失败，呼叫将在 N 次重试 RSVP 后失败，其中“必需 RSVP 呼叫中重试计数器”服务参数指定为 N。

下一步做什么

在网关设备上配置 RSVP 座席。有关如何配置 RSVP 座席的信息，请参阅设备的文档。在网关上配置 RSVP 座席后，返回 Cisco Unified Communications Manager 管理，然后选择以下选项之一：

- 可选。[配置 MLPP 到 RSVP 优先级映射](#)，第 157 页如果您在网络中使用多级优先和抢占。
- [配置应用程序 ID](#)，第 158 页

配置 MLPP 到 RSVP 优先级映射

可选。使用以下群集范围（系统 - RSVP）服务参数配置从呼叫者 MLPP 优先级到 RSVP 优先级的映射：

- MLPP 执行优先到 RSVP 优先级映射
- MLPP 闪烁优先到 RSVP 优先级映射
- MLPP 闪烁到 RSVP 优先级映射
- MLPP 即时到 RSVP 优先级映射
- MLPP PL 优先级到 RSVP 优先级映射
- MLPP PL 常规到 RSVP 优先级映射

要查找和配置这些服务参数，请执行以下步骤：

过程

步骤 1 在 Cisco Unified Communications Manager 管理中，选择系统 > 服务参数。

步骤 2 在“服务参数配置”窗口中，选择服务器并选择 Cisco CallManager 服务。

步骤 3 在“群集范围参数（系统 - RSVP）”部分中，配置指定的服务参数。

这些服务参数功能如下：

- Cisco Unified Communications Manager 在发起基于以下配置的 RSVP 保留时将主叫方优先级映射到 RSVP 优先级：服务参数值越高，优先级越高。
- IOS 路由器会根据 RSVP 优先级抢占呼叫。
- RSVP 座席必须通知 Cisco Unified Communications Manager 关于 RSVP 保留故障的原因，包括抢占的原因。

- Cisco Unified Communications Manager 使用现有的 MLPP 机制通知预占的主叫方和被叫方关于预占。

下一步做什么

在网关设备上配置 RSVP 座席。有关如何配置 RSVP 座席的信息，请参阅设备的文档。在网关上配置 RSVP 座席后，返回 Cisco Unified Communications Manager 管理和 [配置应用程序 ID，第 158 页](#)。

配置应用程序 ID

配置 RSVP 应用程序 ID 时，系统会将标识符添加到语音和视频流量，以便 Cisco RSVP 座席能够根据其收到的标识符为任一类型的流量设置单独的带宽限制。

在开始此程序之前，请在网关设备上配置 RSVP 座席。有关如何配置 RSVP 座席的信息，请参阅设备的文档。

开始之前

要在网络中部署 RSVP 应用程序 ID，您必须在 Cisco RSVP 座席路由器上使用最低版本的 Cisco IOS 版本 12.4(6)T 或更高版本。

过程

步骤 1 在 Cisco Unified Communications Manager 管理中，选择系统 > 服务参数。

步骤 2 在服务参数配置窗口中，选择服务器并选择 Cisco CallManager 服务。

步骤 3 在群集范围参数（系统 - RSVP）部分，配置 RSVP 音频应用程序 ID 服务参数。

（默认值 = AudioStream）

步骤 4 在群集范围参数（系统 - RSVP）部分，配置 RSVP 视频应用程序 ID

（默认值 = VideoStream）

下一步做什么

[配置 DSCP 标记，第 158 页](#)

配置 DSCP 标记

如果 RSVP 预留失败，系统会指示 RSVP 座席或终端设备（以防分配 RSVP 座席失败）将媒体差分服务控制点 (DSCP) 标记更改为尽力而为。否则，过量 EF 标记的媒体数据包可能降低服务质量 (QoS)，甚至是有保留的流。

开始之前

[配置应用程序 ID，第 158 页](#)

过程

步骤 1 在 Cisco Unified Communications Manager 管理中，选择系统 > 服务参数。

步骤 2 在服务参数配置窗口中，选择服务器并选择 Cisco CallManager 服务。

步骤 3 在群集范围参数（系统 - QoS）部分，配置 **RSVP** 失败时音频呼叫的 **DSCP** 服务参数。

步骤 4 在群集范围参数（系统 - QoS）部分，配置 **RSVP** 失败时音频呼叫的 **DSCP** 服务参数。



第 17 章

配置推送通知

- [推送通知概述，第 161 页](#)
- [推送通知配置，第 165 页](#)

推送通知概述

当您的群集启用推送通知时，Unified Communications Manager 和 IM and Presence Service 使用 Google 和 Apple 的基于云的推送通知服务来推送语音和视频呼叫通知、即时消息通知到以挂起模式（也称为后台模式）运行的 Android 和 iOS 客户端上的 Cisco Jabber 或 Cisco Webex。推送通知可让您的系统与 Cisco Jabber 或 Cisco Webex 保持永久通信。对于从企业网络内部连接的 Android 和 iOS 客户端上的 Cisco Jabber 和 Cisco Webex，以及通过 Expressway 的移动和远程访问功能注册到内部部署的客户端而言，推送通知都是必需的。

推送通知的工作原理

在启动时，安装在 Android 和 iOS 平台设备上的客户端会注册到 Unified Communications Manager、IM and Presence Service 以及 Google 和 Apple 云。通过移动和远程访问部署，客户端通过 Expressway 注册到内部服务器。只要 Cisco Jabber 和 Cisco Webex 客户端在前台模式下运行，Unified Communications Manager 和 IM and Presence Service 就可以直接向客户端发送呼叫和即时消息。

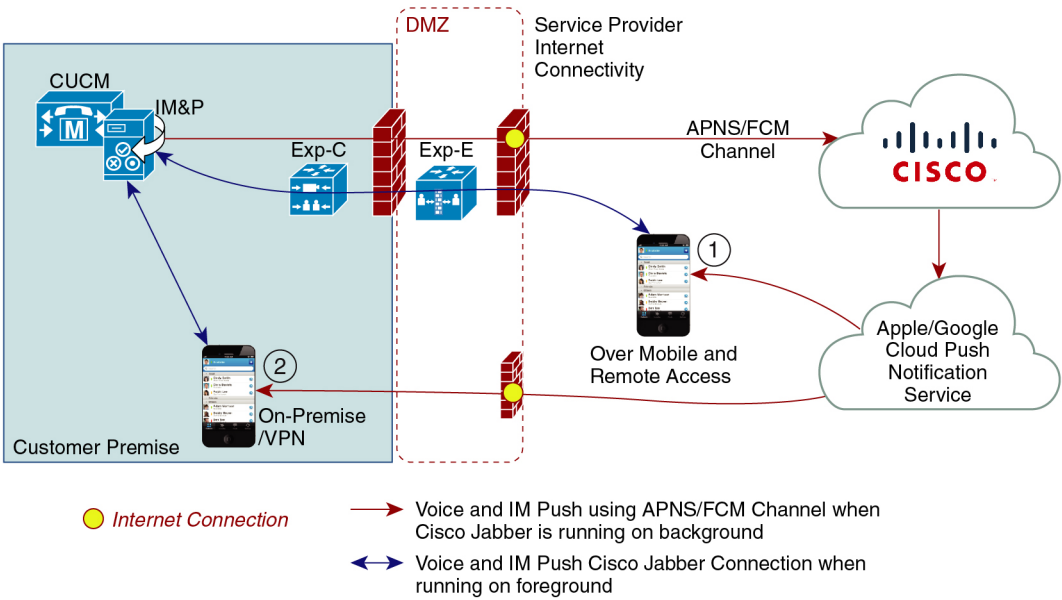
但是，一旦 Cisco Jabber 或 Cisco Webex 客户端进入挂起模式（例如为了延长电池使用时间），标准通信通道就不可用，从而导致 Unified Communications Manager 和 IM and Presence Service 无法直接与客户端通信。推送通知提供了另一个通过合作伙伴云联系客户端的渠道。



注释 如果以下任一情况属实，Cisco Jabber 和 Cisco Webex 将被视为在挂起模式下运行：

- Cisco Jabber 或 Cisco Webex 应用程序离屏运行（例如在后台运行）
- Android 或 iOS 设备已锁定
- Android 或 iOS 设备屏幕关闭

图 6: 推送通知架构



449023

上图显示了当 Cisco Jabber 或 Cisco Webex Android 和 iOS 版本客户端在后台运行或停止运行时会发生什么。图中展示了：(1) 移动和远程访问部署，其中客户端通过 Expressway 与现场 Cisco Unified Communications Manager 和 IM and Presence Service 部署连接，以及 (2) 直接与企业网络内的现场部署连接的 Cisco Jabber 或 Cisco Webex Android 和 iOS 客户端。



注释 从 iOS13（适用于 Apple 客户端和支持的 Android 客户端）开始，语音呼叫和消息使用单独的推送通知通道（“VoIP”和“消息”）访问在后台模式下运行的客户端。不过，这两个通道的常规流是相同的。对于 iOS 12，语音呼叫和消息使用相同的通道发送。

Cisco Jabber 和 Cisco Webex 的推送通知行为

下表介绍了 iOS 12 和 iOS 13 下注册到 Unified Communications Manager 和 IM and Presence Service 的 Cisco Jabber 或 Cisco Webex iOS 客户端的行为。

Cisco Jabber 或 Cisco Webex 客户端正在运行...	Cisco Jabber 正在 iOS12 设备上运行	Cisco Jabber 正在 iOS13 设备或 Android 设备上运行
前台模式	<p><u>语音和视频呼叫</u></p> <p>Unified Communications Manager 使用标准 SIP 通信通道直接向 Cisco Jabber 或 Cisco Webex 客户端发送语音和视频呼叫。</p> <p>对于呼叫，Unified Communications Manager 还会将推送通知发送到处于前台模式的 Cisco Jabber 或 Cisco Webex 客户端。不过，标准 SIP 通道（而不是推送通知通道）用于建立呼叫。</p> <p><u>留言</u></p> <p>IM and Presence Service 服务使用标准 SIP 通信通道直接将消息发送到客户端。对于消息，推送通知不会发送到处于前台模式的客户端。</p>	行为与 iOS12 相同。

Cisco Jabber 或 Cisco Webex 客户端正在运行...	Cisco Jabber 正在 iOS12 设备上运行	Cisco Jabber 正在 iOS13 设备或 Android 设备上运行
挂起模式（背景模式）	<p>语音或视频呼叫</p> <p>标准通信通道不可用。Unified CM 使用推送通知通道。</p> <p>收到通知后，Cisco Jabber 或 Cisco Webex 客户端将自动重新进入前台模式，客户端会振铃。</p> <p>消息传送</p> <p>标准通信通道不可用。IM and Presence Service 使用通知推送通道发送 IM 通知，如下所示：</p> <ol style="list-style-type: none"> 1. IM and Presence Service 将 IM 通知发送到思科云中的 Push REST 服务，该服务会将通知转发到 Apple 云。 2. Apple 云将 IM 通知推送到 Cisco Jabber 或 Cisco Webex 客户端，通知显示在 Cisco Jabber 或 Cisco Webex 客户端上。 3. 当用户单击通知时，Cisco Jabber 或 Cisco Webex 客户端将移回前台。Cisco Jabber 或 Cisco Webex 客户端会恢复与 IM and Presence Service 的会话并下载即时消息。 <p>注释 当 Cisco Jabber 或 Cisco Webex 客户端处于挂起模式时，用户的在线状态显示为离开。</p>	<p>使用 iOS13 时，呼叫流量和消息流量拆分为单独的推送通知通道：用于呼叫的 "VoIP" 通道，以及用于消息传送的 "消息" 通道。</p> <p>语音或视频呼叫</p> <p>标准通信通道不可用。Unified CM 使用推送通知 "VoIP" 通道。</p> <p>在收到 VoIP 通知后，Jabber 将使用主叫号码启动 CallKit。</p> <p>此行为适用于 Cisco Jabber 或 Cisco Webex iOS 客户端。</p> <p>消息传送</p> <p>标准通信通道不可用。IM and Presence Service 服务使用推送通知 "消息" 通道。</p> <ol style="list-style-type: none"> 1. IM and Presence Service 将 IM 通知发送到思科云中的 Push REST 服务，该服务会将通知转发到 Apple 云。 2. Apple 云会将 IM 通知推送到 Cisco Jabber 或 Cisco Webex 客户端。 3. 当用户单击通知时，Cisco Jabber 或 Cisco Webex 客户端将移回前台模式。Cisco Jabber 或 Cisco Webex 客户端会恢复与 IM and Presence Service 的会话并下载消息。 <p>注释 当 Cisco Jabber 或 Cisco Webex 客户端处于挂起模式时，用户的在线状态显示为离开。</p>

推送通知支持的客户端

客户端	操作系统	平台云	云服务
Cisco Jabber iPhone 和 iPad 版本	iOS	Apple	Apple 推送通知服务 (APNS)
Cisco Jabber Android 版本	Android	Google	Android PNS 服务
Webex iOS 版本	iOS	Apple	Apple 推送通知服务 (APNS)

客户端	操作系统	平台云	云服务
Webex Android 版本	Android	Google	Android PNS 服务

推送通知配置

有关如何配置和部署推送通知的详细信息，请参阅部署 *iPhone* 和 *iPad* 版 *Cisco Jabber* 的推送通知，网址：<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>。



第 II 部分

拨号方案

- [配置分区，第 169 页](#)
- [安装国家编号方案，第 175 页](#)
- [配置呼叫路由，第 179 页](#)
- [配置寻线引导，第 203 页](#)
- [配置群集间查询服务，第 211 页](#)
- [配置全球拨号方案复制，第 219 页](#)
- [主叫方标准化，第 235 页](#)
- [配置拨号规则，第 243 页](#)



第 18 章

配置分区

- [分区概述，第 169 页](#)
- [呼叫搜索空间概述，第 169 页](#)
- [服务级别，第 170 页](#)
- [分区配置任务流程，第 171 页](#)
- [分区相互作用和限制，第 173 页](#)

分区概述

分区是以下任何项的逻辑组：

- 路由模式
- 目录号码 (DN)
- 转换模式
- 转换模式
- 通用资源指示灯 (URI)
- 寻线引导

分区根据类似的易访问性要求、组织、位置和呼叫类型，将路由计划划分成逻辑子集，从而简化呼叫路由。

呼叫搜索空间概述

呼叫搜索空间 (CSS) 是按优先顺序排列的分区列表。呼叫搜索空间确定可供主叫方呼叫的呼叫目标。呼叫目标必须位于主叫方呼叫搜索空间可用分区中，否则，主叫方无法呼叫该目标。您可以为目录号码和设备（例如电话和网关）分配呼叫搜索空间。

如果呼叫搜索空间同时分配给主叫方的电话和主叫方的目录号码，系统会将两者串联来为主叫方提供 CSS。

您可以使用分区和呼叫搜索空间来根据呼叫权限组织系统。例如，您可以：

- 限制一些员工拨打长途呼叫
- 限制大厅电话直接呼叫 CEO

服务级别

您可以使用分区和呼叫搜索空间 (CSS) 配置服务类别。下表提供您可以为提供 PSTN 访问的服务类别创建的分区和呼叫搜索空间的示例：

- 紧急呼叫
- 本地呼叫
- 国内呼叫
- 国际拨号

表 14: 分区和呼叫搜索空间的示例

呼叫搜索空间	路由分区 1	路由分区 2	路由分区 3	功能
Base_CSS	Base_PT	—	—	<ul style="list-style-type: none"> • 危急 • 网内
LocalPSTN_CSS	PSTN_Local_PT	—	—	<ul style="list-style-type: none"> • 危急 • 网内 • 本地
NationalPSTN_CSS	PSTN_Local_PT	PSTN_National_PT	—	<ul style="list-style-type: none"> • 危急 • 网内 • 本地 • 国内
InternationalPSTN_CSS	PSTN_Local_PT	PSTN_National_PT	PSTN_Intl_PT	<ul style="list-style-type: none"> • 危急 • 网内 • 本地 • 国内 • 国际

设备会自动向呼叫搜索空间（例如 Base_CSS）注册。这样，所有设备都可以拨打网内和应急网外号码。您必须将其余呼叫搜索空间分配给用户设备配置文件上的目录号码，以提供本地 7 位或本地 10 位、国内和国际拨号功能。

分区配置任务流程

过程

	命令或操作	目的
步骤 1	配置分区，第 171 页	配置分区以创建具有类似可接通性特征的系统资源的逻辑分组。
步骤 2	配置呼叫搜索空间，第 172 页	配置主叫设备在尝试完成呼叫时搜索的分区。

配置分区

配置分区以创建具有类似可接通性特征的系统资源的逻辑分组。您可以创建以下任何一项的分区：

- 路由模式
- 目录号码 (DN)
- 转换模式
- 转换模式
- 通用资源指示灯 (URI)
- 寻线引导

分区根据组织、位置和呼叫类型将路由计划分成逻辑子集，简化了呼叫路由。您可以配置多个分区。

过程

- 步骤 1 从 Cisco Unified CM 管理中，选择呼叫路由 > 控制级 > 分区。
- 步骤 2 单击新增以创建新的分区。
- 步骤 3 在分区名称、说明字段中，为分区输入一个在路由计划中唯一的名称。
分区名称可以包含字母数字字符，以及空格、连字符 (-) 和下划线 (_)。请参阅联机帮助，了解有关分区名称的指导原则。
- 步骤 4 在分区名称后面输入逗号 (,)，并在同一行上输入分区的说明。
说明最多可以包含 50 个任何语言的字符，但不能包含双引号 (")、百分号 (%)、与符号 (&)、反斜线 (\)、尖括号 (<>) 或中括号 ([])。

如果不输入说明，Cisco Unified Communications Manager 将自动在此字段中输入分区名称。

步骤 5 要创建多个分区，请每个分区条目使用一行。

步骤 6 从下拉列表中，选择与此分区关联的时间表。

时间表指定分区何时可用于接收来电。如果您选择无，该分区将始终保持活动状态。

步骤 7 选择下列单选按钮之一以配置时区：

- **始叫设备** — 当选择此单选按钮时，系统会将主叫设备的时区与时间表作比较，以确定分区是否可用来接收来电。
- **特定时区** — 选择此单选按钮后，从下拉列表中选择时区。系统会将所选的时区与时间表作比较，以确定分区是否可用来接收来电。

步骤 8 单击保存。

分区名称指导原则

呼叫搜索空间中的分区列表限制为最多 1024 个字符。这意味着，根据分区名称的长度不同，CSS 中的最大分区数会有所变化。使用下表确定在分区名称长度固定的情况下可添加到呼叫搜索空间的最大分区数量。

表 15: 分区名称指导原则

分区名称长度	最大分区数量
2 个字符	340
3 个字符	256
4 个字符	204
5 个字符	172
...	...
10 个字符	92
15 个字符	64

配置呼叫搜索空间

呼叫搜索空间是一份通常分配给设备的路由分区顺序列表。呼叫搜索空间决定主叫设备在尝试完成呼叫时可以搜索的分区。

过程

步骤 1 从 Cisco Unified CM 管理中，选择呼叫路由 > 控制级 > 呼叫搜索空间。

步骤 2 单击**新增**。

步骤 3 在**名称**字段中输入名称。

确保每个呼叫搜索空间名称在系统中都是唯一的。名称最多可以包含 50 个字母数字字符，可以包含空格、点(.)、连字符(-)和下划线(_)。

步骤 4 在**说明**字段中，输入说明。

说明最多可以包含 50 个任何语言的字符，但不能包含双引号(")、百分号(%)、与符号(&)、反斜线(\) 或尖括号(<>)。

步骤 5 从可用分区下拉列表中，执行以下步骤之一：

- 对于单个分区，选择该分区。
- 对于多个分区，按住**控制 (CTRL)** 键，然后选择适当的分区。

步骤 6 在方框之间选择向下箭头，以将分区移至**所选分区**字段。

步骤 7 （可选） 使用**所选分区**框右侧的箭头键更改所选分区的优先级。

步骤 8 单击**保存**。

分区相互作用和限制

表 16: 分区限制

功能或操作	限制
删除分区	<p>在删除分区之前，请确保完成以下任务之一：</p> <ul style="list-style-type: none"> • 为正在使用要删除的分区的呼叫搜索空间、设备或其他项目分配另一个分区。 • 删除正在使用要删除的分区的呼叫搜索空间、设备或其他项目。 <p>请仔细检查以确保您正在删除正确的分区，因为您无法检索删除的分区。如果意外误删了某个分区，必须重新创建。</p>
转换模式	转换模式包含数字处理并分配给分区。当呼叫与转换模式匹配时，Unified CM 执行转换，然后使用转换模式指定的呼叫搜索空间重新路由呼叫。有关转换模式的详细信息，请参阅“配置呼叫路由”一章。
每日路由时间	配置分区可用于接受来电的计划。有关配置每天路由时间的详细信息，请参阅“配置呼叫路由”一章。

功能或操作	限制
逻辑分区	可选： 可让您通过网关和干线从外部网络拆分内部 VoIP 网络。逻辑分区对于大多数部署是可选的，但在印度的国家/地区是必需的，其中，规章要求离开内部网络的所有呼叫都将进入本地 PSTN 网关。有关配置逻辑分区的详细信息，请参阅《 <i>Cisco Unified Communications Manager</i> 功能配置指南》中的“配置逻辑分区”一节。



第 19 章

安装国家编号方案

- 国家编号方案概述，第 175 页
- 国家编号方案前提条件，第 175 页
- 国家编号方案安装任务流程，第 176 页

国家编号方案概述

Unified Communications Manager 默认提供北美编号方案 (NANP)。对于具有不同拨号方案要求的国家/地区，您可以安装 Cisco 国际拨号方案，并使用它创建特定于您的要求的唯一编号方案。

编号方案包含特定于该编号方案的丢弃数字指令 (DDI) 和标签。配置呼叫路由时，您可以使用这些项目创建适用于编号方案的路由规则。

本章介绍如何安装国家编号方案。有关使用国家编号方案的详细信息，请参阅《*Unified Communications Manager 拨号方案部署指南*》，位于 <http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>。

国家编号方案前提条件

如果要为北美以外的国家/地区安装国家编号方案，请下载包含当前版本的国际拨号方案的 Cisco 选项包 (COP) 文件。COP 文件使用命名规则 IDP v.x，可从 Cisco 网站获取：

- <https://software.cisco.com/download/navigator.html>

将文件放在 Unified Communications Manager 可以访问的外部 FTP 或 SFTP 服务器上。

国家编号方案安装任务流程

过程

	命令或操作	目的
步骤 1	安装 COP 文件，第 176 页	可选。要为北美以外的国家/地区安装编号方案，请下载包含当前版本的国际拨号方案的 Cisco 选项包 (COP) 文件。
步骤 2	安装国家编号方案，第 177 页	在群集中的每个 Unified Communications Manager 节点上安装国家编号方案。只有在为北美之外的国家/地区安装国家编号方案时，才执行此程序。
步骤 3	重新启动 CallManager 服务，第 177 页	更改在您重新启动服务后生效。

安装 COP 文件

此程序用于安装包含国际拨号方案的 Cisco 选项包 (COP) 文件。

过程

- 步骤 1 请在 Unified Communications Manager 发布方节点上开始执行此程序。从 Cisco Unified Communications 操作系统管理中，选择软件升级 > 安装。
此时将显示软件安装/升级窗口。
- 步骤 2 在源字段中，选择远程文件系统。
- 步骤 3 配置软件安装/升级窗口中的字段。请参阅“相关主题”，了解有关字段及其配置选项的更多信息。
- 步骤 4 单击下一步。
窗口将刷新，其中会列出可用的软件选项和升级。
- 步骤 5 从选项/升级下拉列表中，选择 **DP COP** 文件，然后单击下一步。
此时安装文件窗口将打开，并从 FTP 服务器下载文件。窗口中会显示下载的进度。
- 步骤 6 当校验和窗口显示时，对照下载文件的校验和验证校验和值。
- 步骤 7 单击下一步继续软件升级。
此时会显示一则警告消息，其中包含您选择要安装的 DP COP 文件。
- 步骤 8 单击安装。
此时将显示安装状态窗口。
- 步骤 9 单击完成。
- 步骤 10 在 Unified Communications Manager 订阅方节点上重复此程序。必须在群集中的所有节点上安装 COP 文件。

相关主题

[COP 文件安装字段](#)，第 177 页

COP 文件安装字段

字段	说明
目录	输入 COP 文件所在的目录。
远程服务器	输入 COP 文件所在服务器的主机名或 IP 地址。
远程用户	输入远程服务器的用户名。
远程密码	输入远程服务器的密码。
传输协议	选择连接远程服务器时要使用的协议。

安装国家编号方案

只有在为北美之外的国家/地区安装国家编号方案时，才执行此程序。

在群集中的每个 Unified Communications Manager 节点上安装国家编号方案。从 Unified Communications Manager 发布方节点开始。

过程

- 步骤 1** 从 Cisco Unified Communications Manager 管理中，选择呼叫路由 > 拨号方案安装程序。
 - 步骤 2** 输入搜索条件，然后单击**查找**。
 - 步骤 3** 从可用版本下拉列表框中选择要安装的拨号方案版本。
 - 步骤 4** 单击**安装**。
“状态”将显示拨号方案已安装。
 - 步骤 5** 对群集中的每个订阅方节点重复此程序。
-

重新启动 CallManager 服务

过程

- 步骤 1** 在 Cisco Unified 功能配置界面中，选择工具 > 控制中心 - 功能服务。
- 步骤 2** 从服务器下拉列表中选择 Unified Communications Manager 服务器。
在“CM 服务”区域，Cisco CallManager 显示在服务名称列中。

步骤 3 选择与 Cisco CallManager 服务对应的单选按钮。

步骤 4 单击**重新启动**。

服务会重新启动并显示消息：服务已成功重新启动。



第 20 章

配置呼叫路由

- 呼叫路由概述，第 179 页
- 呼叫路由前提条件，第 180 页
- 呼叫路由配置任务流程，第 181 页
- 呼叫路由限制，第 195 页
- 使用被叫号码分析器进行故障诊断，第 196 页
- 线路组设置，第 197 页

呼叫路由概述

系统使用路由计划确定如何在群集间路由呼叫以及如何将外部呼叫路由到专用网络或公共交换电话网 (PSTN)。您配置的路由计划指定系统用于路由每种呼叫类型的路径。例如，您可以创建一个路由计划，使用 IP 网络进行网内呼叫，或者对本地 PSTN 呼叫使用一个运营商，对国际呼叫使用另一运营商。

转换模式

您可以配置转换模式以处理任何类型的呼叫的数字。转换模式遵循相同的一般规则，并使用相同的通配符作为路由模式。与路由模式一样，您可将转换模式分配给分区。然而，当被叫数字与转换模式匹配时，Unified CM 不将呼叫路由到网关等外部实体；而是先进行转换，然后再次路由该呼叫，这次使用在转换模式中配置的呼叫搜索空间进行路由。



注释 对于您创建的每个转换模式，确保分区、路由过滤器和编号方案的组合是唯一的。如果收到指示条目重复的错误，检查路由模式或寻线引导、转换模式、目录号码、呼叫暂留号码、呼叫代答号码或 meet-me 号码配置窗口。

转换模式

转换模式可用于丢弃数字、添加前缀数字、添加主叫方转换掩码以及在系统将呼叫发送到电话或 PSTN 之前控制主叫方号码的显示。

配置转换模式并将其关联到路由分区，从而将该模式分配到包含该分区的呼叫搜索空间。您可以通过配置窗口中的“主叫方转换CSS”或“被叫方转换CSS”字段，将模式分配给特定设备、设备池、网关或干线的呼叫设置。

您可以配置以下转换模式：

- **主叫方转换模式**— 允许系统将主叫方号码的国际格式转换为与路由组设备（如网关或干线）相连的群集外网络所要求的本地格式。
- **被叫方转换模式**— 允许系统将被叫方号码的国际格式转换为与路由组设备（如网关或干线）相连的群集外网络所要求的本地格式。

路由模式

系统有一个使用以下组件的三层路由规划方法：

- **路由模式** — 系统搜索与外部拨号字符串匹配的已配置路由模式，并用其将呼叫定向至网关或路由列表。您可以将路由模式分配到网关、干线或者包含一个或多个路由组的路由列表。
- **路由列表** — 呼叫可用路径的优先顺序列表。
- **路由组**— 可用路径；路由组将呼叫分配到网关和干线。

其他呼叫路由

路由计划还可以包含以下可选组件：

- **本地路由组**— 如果您有多个站点，则可以使用本地路由组，以便将网外呼叫路由到设备池指定的网关，而不是路由模式配置指定的网关。这可让您对多个位置使用一套路由模式。
- **路由过滤器** — 创建路由过滤器并将其添加到您的路由模式或寻线引导，以限制用户使用该模式。路由过滤器为必需，您使用的是拨号方案安装程序文件，但对于手动拨号方案配置为可选。对于手动配置，路由过滤器仅适用于您的模式使用 @ 通配符的情况。
- **自动备用路由** — 当系统因带宽不足而阻止呼叫时，自动通过 PSTN 或其他网络重新路由呼叫。
- **每日定时路由** — 创建时间表来指定给定分区可用于传入呼叫的时间。

呼叫路由前提条件

- 完成[分区配置任务流程](#)，第 171 页中的任务。
- 确保掌握以下信息：
 - 内线号码分机
 - 列出路由到每个网关的呼叫的计划

有关规划呼叫路由的详细信息，请参阅《Cisco Collaboration System Solution Reference Network Design》中的呼叫控制和路由主题。

呼叫路由配置任务流程

过程

	命令或操作	目的
步骤 1	配置转换模式，第 181 页	配置转换模式以指定如何完成特定分区中呼叫的数字转换。
步骤 2	配置主叫方转换模式，第 182 页	此程序用于转换主叫号码。例如，您可以配置转换模式，以在呼叫 PSTN 时将主叫方的分机替换为办公室的主号码。
步骤 3	配置被叫方转换模式，第 183 页	此程序用于转换被叫号码。例如，您可以配置仅保留十位主叫号码的最后五位的转换模式。
步骤 4	配置本地路由组，第 183 页	可选。本地路由组可让您对多个位置使用一套路由模式。Unified CM 根据主叫设备的位置而不是路由模式分配网关。
步骤 5	配置路由组，第 185 页	可选。配置路由组来设置网关设备的选择顺序。路由组包含一个或多个设备。
步骤 6	配置路由列表，第 185 页	可选。路由列表包含一个或多个路由组。配置路由列表来控制路由组的选择顺序。
步骤 7	配置路由过滤器，第 186 页	可选。使用路由过滤器可以限制路由模式允许的某些数字。
步骤 8	配置路由模式，第 189 页	配置路由模式来将呼叫定向到特定的设备并包括或排除特定的数字模式。
步骤 9	启用群集范围内的自动路由迂回，第 193 页	可选。启用自动路由迂回(AAR)，以让系统在因带宽不足而阻止呼叫时将呼叫重新路由到 PSTN 或其他网络。
步骤 10	配置 AAR 组，第 193 页	可选。配置包含数字转换的 AAR 组以应用自动路由迂回。
步骤 11	配置每天定时路由时间，第 194 页	可选。创建时间表来指定给定分区何时可用于接收来电。

配置转换模式

配置转换模式以在拨号字符串与模式匹配时将数字处理应用到主叫和被叫号码。系统完成数字转换，然后重新路由呼叫。

过程

步骤 1 从 Cisco Unified CM 管理中，选择呼叫路由 > 转换模式。

步骤 2 选择下列选项之一：

- 单击**新增**以添加新的转换模式。
- 单击**查找**，然后选择现有的转换模式。

步骤 3 在转换模式字段中，输入您想要系统与使用此模式的拨号字符串相匹配的模式。

步骤 4 从分区下拉列表中，选择您要在其中分配此模式的分区。

步骤 5 完成转换模式配置窗口中的其余字段的设置。有关字段及其配置选项的更多信息，请参阅系统联机帮助。

步骤 6 单击保存。

配置主叫方转换模式

此程序用于转换主叫号码。例如，您可以配置转换模式，以在呼叫 PSTN 时将主叫方的分机替换为办公室的主号码。

过程

步骤 1 从 Cisco Unified CM 管理中，选择呼叫路由 > 转换 > 转换模式 > 主叫方转换模式。

步骤 2 选择下列选项之一：

- 单击**新增**以添加新的主叫方转换模式。
- 单击**查找**并选择现有模式。

步骤 3 从模式字段中，输入要与主叫方号码匹配的模式。

注释 对于出站呼叫：

系统将根据转换前的主叫方号码选择主叫方转换掩码。（分机分配给 IP 电话）。

在 SIP 干线上选择主叫方转换掩码时，如果主叫方号码转换为路由模式/组上的另一个号码，则始终使用转换前主叫号码来选择主叫方转换掩码。

尽管根据被叫号码分析器 (DNA)，转换后的号码才用于选择主叫方转换掩码。但是，这是 DNA 的错误行为。

步骤 4 在主叫方转换模式配置窗口中完成其余字段的设置。有关字段及其配置选项的更多信息，请参阅联机帮助。

步骤 5 单击保存。

配置被叫方转换模式

此程序用于转换被叫号码。例如，您可以配置转换模式，仅保留十位被叫号码中的最后五位数。

过程

- 步骤 1** 从 Cisco Unified CM 管理中，选择呼叫路由 > 转换 > 转换模式 > 被叫方转换模式。
- 步骤 2** 选择下列选项之一：
 - 单击**新增**以添加新的被叫方转换模式。
 - 单击**查找**并选择现有模式。
- 步骤 3** 从模式字段中，输入要与被叫号码匹配的模式。
- 步骤 4** 在被叫方转换模式配置窗口中完成其余字段的设置。有关字段及其配置选项的更多信息，请参阅系统联机帮助。
- 步骤 5** 单击**保存**。

配置本地路由组

可选。您可以配置本地路由组以减少所需的路由列表数量。路由列表指向系统用于路由呼叫的 PSTN 网关，具体取决于 PSTN 网关的位置。或者，您也可以使用本地路由组将 PSTN 网关的位置与用于访问网关的路由模式解耦。此配置可让不同位置的电话和其他设备使用一组路由模式，同时 Cisco Unified Communication Manager 选择正确的网关以路由呼叫。

例如，本地路由组可让您为整个国家/地区设置一个拨号方案，而不是为该国家/地区的每个城市使用单独的拨号方案。此方法只适用于集中式呼叫部署方案。

过程

	命令或操作	目的
步骤 1	配置本地路由组名称，第 184 页	可选。 系统提供称为标准本地路由组的默认本地路由组，但您可以配置其他本地路由组。使用此程序命名其他本地路由组。
步骤 2	将本地路由组关联到设备池，第 184 页	要确保预配置了系统中的每个设备以了解其本地路由组，请将本地路由组与设备池关联。
步骤 3	将本地路由组添加到路由列表，第 184 页	可选。 配置可添加到路由列表中的本地路由组。当您创建本地路由组时，系统会将去电路由到在设备池级别为用户定义的网关。

配置本地路由组名称

可选。系统提供称为标准本地路由组的默认本地路由组，但您可以配置其他本地路由组。使用此程序命名其他本地路由组。

过程

步骤 1 从 Cisco Unified CM 管理中，选择呼叫路由 > 路由/寻线 > 本地路由组名称。

步骤 2 单击添加行。

步骤 3 输入新路由组的名称和说明。

步骤 4 单击保存。

将本地路由组关联到设备池

您可以根据源设备的设备池设置，分配本地路由组以使用现有路由组。此配置可让不同位置的电话和其他设备使用一组路由模式，同时 Unified Communications Manager 选择正确的网关以路由呼叫。

要确保预配置了系统中的每个设备以了解其本地路由组，请将本地路由组与设备池关联。

过程

步骤 1 在 Cisco Unified CM 管理上，选择系统 > 设备池。

步骤 2 输入搜索条件，单击查找，然后从结果列表中选择设备池。

步骤 3 在本地路由组设置区域中，从标准本地路由组下拉列表选择一个路由组。

步骤 4 单击保存。

将本地路由组添加到路由列表

配置可添加到路由列表中的本地路由组。当您创建本地路由组时，系统会将去电路由到在设备池级别为用户定义的网关。

过程

步骤 1 从 Cisco Unified CM 管理中，选择呼叫路由 > 路由/寻线 > 路由列表。

步骤 2 选择下列选项之一：

- 单击 "新增" 按钮以添加新的路由列表。
- 单击查找并从结果列表中选择路由列表，以修改现有路由列表的设置。

路由列表配置窗口将会显示。

步骤 3 要将本地路由组添加到路由列表，请单击添加路由组按钮。

步骤 4 从路由组下拉列表中，选择要添加到路由列表的本地路由组。您可以添加标准本地路由组，也可以添加自己创建的自定义本地路由组。

步骤 5 单击保存。

步骤 6 单击应用配置。

配置路由组

配置路由组以确定系统为去电选择网关的优先顺序。使用此程序将具有类似特征的网关编组在一起，以便组中的任何网关可以拨打呼叫。系统会根据您在配置路由组时指定的顺序选择要使用的网关。

您可以将设备分配到多个路由组。

过程

步骤 1 从 Cisco Unified CM 管理中，选择呼叫路由 > 路由/寻线 > 路由组。

路由组配置窗口将会显示。

步骤 2 选择下列选项之一：

- 单击**新增**，添加新的路由组。
- 单击**查找**并从结果列表中选择路由组，以修改现有路由组的设置。

路由组配置窗口将会显示。

步骤 3 配置路由组配置窗口中的字段。有关字段及其配置选项的更多信息，请参阅系统联机帮助。

步骤 4 单击保存。

配置路由列表

配置路由列表以标识一组路由组，并按优先顺序放置它们。Unified Communications Manager 使用路由列表中的顺序搜索传出呼叫的可用设备。

如果您配置路由列表，则必须配置至少一个路由组。路由列表只能包含路由组和本地路由组。



注释 通过出站呼叫通过路由列表发送时，路由列表进程会锁定出站设备，以避免在呼叫完成之前发送警报消息。在出站设备被锁定后，寻线列表将停止寻找传入呼叫。

过程

步骤 1 从 Cisco Unified CM 管理中，选择呼叫路由 > 路由/导线 > 路由列表。

步骤 2 选择下列选项之一：

- 单击**新增**添加新的路由列表。
- 单击**查找**并从结果列表中选择路由列表，以修改现有路由列表的设置。

步骤 3 配置路由列表配置窗口中的字段。有关字段及其配置选项的更多信息，请参阅系统联机帮助。

步骤 4 要将路由组添加到路由列表，请单击**添加路由组**按钮。

步骤 5 从路由组下拉列表中，选择要添加到路由列表的路由组。

步骤 6 单击**保存**。

步骤 7 单击**应用配置**。

配置路由过滤器

路由过滤器使用拨出数字字符串确定如何处理呼叫。路由过滤器仅在配置包含 @ 通配符的模式时适用。当路由模式包含 @ 通配符时，Unified Communications Manager 将根据此程序中指定的编号方案路由呼叫。

如果使用拨号方案安装程序，必须使用路由过滤器；也就是说，如果您安装了拨号方案文件，则根据该编号方案配置路由模式。手动配置拨号方案时，路由计划是可选的。

如果您要手动配置拨号方案，则需要在有包含 @ 通配符的路由模式时配置路由过滤器。当路由模式包含 @ 通配符时，系统将根据您使用路由过滤器指定的编号方案路由呼叫。



注释 当您配置呼叫路由时，确保不要将一个路由过滤器分配给过多的路由模式。如要编辑具有数百个关联路由模式的路由过滤器，可能会导致系统核心。这是因为必须进行额外的系统处理，以便为使用该路由过滤器的所有路由模式更新呼叫路由。创建重复的路由过滤器，并将任何单个路由过滤器与不超过 250 个路由模式相关联。

过程

步骤 1 从 Cisco Unified CM 管理中，选择呼叫路由 > 路由过滤器。

步骤 2 从编号方案下拉列表中，选择编号方案并单击**下一步**。

步骤 3 在路由过滤器名称字段中输入名称。

确保每个路由过滤器名称对路由计划是唯一的。

步骤 4 选择路由过滤器标签和运算符，并为此路由过滤器创建语句。

关于可用路由过滤器标签的详细信息，请参阅[路由过滤器标签](#)，第 187 页。

注释 不要为使用运算符 EXISTS、DOES-NOT-EXIST 或 NOT-SELECTED 的标签输入路由过滤器标签值。

步骤 5 选择路由过滤器运算符，并输入适当的数据，为此路由过滤器创建语句。
关于可用路由过滤器运算符的详细信息，请参阅[路由过滤器运算符](#)，第 188 页。

步骤 6 单击**保存**。
步骤 7 单击**应用配置**。

路由过滤器设置

路由过滤是不考虑将某些路由包含在本地路由数据库中的过程。其仅适用于配置了路由模式的情况。

以下主题列出了关于路由过滤器首选项的信息。

- [路由过滤器标签](#)，第 187 页
- [路由过滤器运算符](#)，第 188 页
- [路由过滤器示例](#)，第 189 页

路由过滤器标签

标签是路由过滤器的核心部分，它将名称应用到拨出数字字符串的子集。例如，NANP 号码 972-555-1234 包含 LOCAL-AREA-CODE (972)、OFFICE-CODE (555) 和 SUBSCRIBER (1234) 路由过滤器标签。

路由过滤器标签需要运算符，可能需要其他值来决定过滤哪些呼叫。

路由过滤器标签字段的值可以包含通配符字符 X、*、#、[、]、-、^ 和数字 0 至 9。下表中的说明使用 [2-9] 和 XXXX 的表示法代表实际数字。在此表示法中，[2-9] 代表 2 至 9 范围中的任意单一数字，X 代表范围 0 至 9 中的任意单一数字。因此，[2-9]XX 形式的三位数区号表示您可以输入实际数字 200 至 999、所有通配符，或者符合该范围内模式的实际数字与通配符的任意混合。

路由过滤器标签根据您从“路由过滤器配置”窗口的“编号方案”下拉列表框中选择的编号方案而有所不同。下表说明北美编号方案的路由过滤器标签。

表 17: 路由过滤器标签

标签	说明
AREA-CODE	这个 [2-9]XX 形式的三位数区号用于识别长途电话的区号。
COUNTRY CODE	这些一位数、两位数或三位数代码用于指定国际电话的目标国家/地区。
END-OF-DIALING	这个单一字符用于识别拨出数字字符串的末尾。对于 NANP 中拨出的国际号码，# 字符用作拨号结束的信号。
INTERNATIONAL ACCESS	这个两位数接入码用于指定国际拨号。从美国发起的呼叫使用 01 表示此代码。

标签	说明
INTERNATIONAL-DIRECT-DIAL	这个一位数代码用于识别直接拨出的国际呼叫。从美国发起的呼叫使用 1 表示此代码。
INTERNATIONAL-OPERATOR	这个一位数代码用于识别接线员协助的国际呼叫。从美国发起的呼叫使用 0 表示此代码。
LOCAL-AREA-CODE	这个 [2-9]XX 形式的三位数区号用于识别 10 位数本地电话的本地区号。
LOCAL-DIRECT-DIAL	这个一位数代码用于识别直接拨出的本地呼叫。NANP 呼叫使用 1 表示此代码。
LOCAL-OPERATOR	这个一位数代码用于识别接线员协助的本地呼叫。NANP 呼叫使用 0 表示此代码。
LONG-DISTANCE-DIRECT-DIAL	这个一位数代码用于识别直接拨出的长途电话。NANP 呼叫使用 1 表示此代码。
LONG-DISTANCE-OPERATOR	这些一位数或两位数代码用于识别 NANP 内接线员协助的长途电话。接线员协助的呼叫使用 0 表示此代码，接线员接入则使用 00。
NATIONAL-NUMBER	此标签指定用于国际呼叫的数字字符串中特定国家特定的部分。
OFFICE-CODE	此标签以 [2-9]XX 形式指定七位数目录号码的前三位。
SATELLITE-SERVICE	这个一位数代码用于接入卫星连接以进行国际呼叫。
SERVICE	这个三位数代码指定服务，例如 911 是应急呼叫，611 是报修电话，411 是查询电话。
SUBSCRIBER	此标签以 XXXX 形式指定七位数目录号码的最后四位。
TRANSIT-NETWORK	这个四位数值用于识别长途运营商。 不要在 TRANSIT-NETWORK 值中包含前导 101 运营商接入码前缀。有关详细信息，请参阅 TRANSIT-NETWORK-ESCAPE。
TRANSIT-NETWORK-ESCAPE	这个三位数值显示在长途运营商识别号前面。此字段的值为 101。不要在 TRANSIT-NETWORK-ESCAPE 值中包含四位数运营商识别码。有关详细信息，请参阅 TRANSIT-NETWORK。

路由过滤器运算符

路由过滤器标签运算符确定是否根据与该标签关联的拨出数字字符串过滤呼叫。运算符 EXISTS 和 DOES-NOT-EXIST 只检查拨出数字字符串是否存在该部分。运算符 == 与采用指定值或模式的实际拨出数字匹配。下表说明可用于路由过滤器标签的运算符。

表 18: 路由过滤器运算符

运算符	说明
NOT-SELECTED	指定不要根据与此标签关联的拨出数字字符串过滤呼叫。 注释 存在或缺乏与运算符关联的标签不会阻止 Cisco Unified Communications Manager 路由呼叫。
EXISTS	指定在找到与此标签关联的拨出数字字符串时过滤呼叫。 注释 Cisco Unified Communications Manager 仅在拨出数字字符串包含与标签关联的数字序列时才路由或阻止呼叫。
DOES-NOT-EXIST	指定在未找到与此标签关联的拨出数字字符串时过滤呼叫。 注释 Cisco Unified Communications Manager 仅在拨出数字字符串不含与标签关联的数字序列时才路由或阻止呼叫。
==	指定在此标签关联的拨出数字字符串与指定值匹配时过滤呼叫。 注释 Cisco Unified Communications Manager 仅在拨出数字字符串包含与标签关联的数字序列并且在附加字段中指定的编号范围内时才路由或阻止呼叫。

路由过滤器示例

- 示例 1: 使用 AREA-CODE 和运算符 DOES-NOT-EXIST 的路由过滤器选择不含区号的所有拨出数字字符串。
- 示例 2: 使用 AREA-CODE、运算符 == 和条目 515 的路由过滤器选择包含 515 区号的所有拨出数字字符串。
- 示例 3: 使用 AREA-CODE、运算符 == 和条目 5[2-9]X 的路由过滤器选择包含 520 至 599 范围内区号的所有拨出数字字符串。
- 示例 4: 使用 TRANSIT-NETWORK、运算符 == 和条目 0288 的路由过滤器选择包含运营商接入码 1010288 的所有拨出数字字符串。

配置路由模式

Unified Communications Manager 使用路由模式来路由或阻止内部和外部呼叫。您可以将路由模式分配到网关、干线或者包含一个或多个路由组的路由列表。



虽然路由模式可直接指向网关，但我们建议您配置路由列表和路由组。这种方法可在呼叫路由和可扩展性方面提供最大的灵活性。

过程

步骤 1 从 Cisco Unified CM 管理中，选择呼叫路由 > 路由/寻线 > 路由模式。

步骤 2 执行下列操作之一：

- 单击**新增**以创建新的路由模式。
- 单击**查找**并选择现有路由模式。

路由模式配置窗口将会显示。

步骤 3 在路由模式字段中，输入拨号字符串必须匹配的号码模式。

步骤 4 从网关/路由下拉列表中，选择要与此路由模式匹配的呼叫发送到的目标。

步骤 5 完成路由模式配置窗口中其余字段的设置。有关字段及其配置选项的更多信息，请参阅系统联机帮助。

步骤 6 单击保存。

路由模式设置

您可以创建包括一串数字（地址）和一组关联的数字的不同路由模式，以启用 Unified CM 将呼叫路由到路由列表或网关。

以下是您要配置的路由模式类型的示例：

- [路由模式中的通配符和特殊字符，第 190 页](#)
- [丢弃前置点数字示例，第 192 页](#)
- [数字前缀示例，第 192 页](#)
- [网内和网外模式示例，第 193 页](#)
- [阻止和路由模式示例，第 193 页](#)

路由模式中的通配符和特殊字符

路由模式中的通配符和特殊字符允许单一路由模式匹配数字（地址）范围。使用这些通配符和特殊字符还可以构建指令，可使 Unified Communications Manager 处理号码，然后将其发送到相邻系统。

下表说明 Unified Communications Manager 支持的通配符和特殊字符。

字符	说明	示例
@	@ 符号通配符匹配所有国内编号方案号码。 每个路由模式只能有一个 @ 通配符。	路由模式 9.@ 路由或阻止国内编号方案识别的所有号码。 以下路由模式示例展示 @ 通配符包含的国内编号方案号码： <ul style="list-style-type: none"> • 0 • 1411 • 19725551234 • 101028819725551234 • 01133123456789
X	X 通配符匹配范围 0 至 9 的任何单一数字。	路由模式 9XXX 路由或阻止范围 9000 至 9999 的所有号码。
!	惊叹号 (!) 通配符匹配范围 0 至 9 的一个或多个数字。	路由模式 9! 路由或阻止范围 910 至 91999999999999999999999999999999 的所有号码。
?	问号 (?) 通配符匹配零次或多次出现的前置数字或通配符值。 注释 如果使用问号 (??) 通配符，第二个问号与空输入不匹配。路由器模式示例： *33X?*X?*X?#	路由模式 91X? 路由或阻止范围 91 至 91999999999999999999999999999999 的所有号码。
+	加号 (+) 通配符匹配一次或多次出现的前置数字或通配符值。	路由模式 91X+ 路由或阻止范围 910 至 91999999999999999999999999999999 的所有号码。
[]	方括号 ([]) 字符括起值范围。	路由模式 813510[012345] 路由或阻止范围 8135100 至 8135105 的所有号码。
-	连字符 (-) 与方括号一起使用，用于指示值范围。	路由模式 813510[0-5] 路由或阻止范围 8135100 至 8135105 的所有号码。
^	抑扬符号 (^) 与方括号一起使用，用于排除值范围。确保第一个字符后跟左括号 ([)。 每个路由模式只能有一个 ^ 字符。	路由模式 813510[^0-5] 路由或阻止范围 8135106 至 8135109 的所有号码。

字符	说明	示例
.	点 (.) 字符用作分隔符，分隔 Cisco Unified Communications Manager 访问代码与目录号码。 使用此特殊字符及丢弃数字指令，剥离 Cisco Unified Communications Manager 访问代码，然后再发送该号码到相邻系统。 每个路由模式只能有一个点 (.) 字符。	路由模式 9.@ 确定开头的 9 作为国内编号方案呼叫中的 Cisco Unified Communications Manager 访问代码。
*	星号 (*) 字符可为特殊被叫号码提供一位额外的数字。	可以配置路由模式 *411 以提供内部接线员目录协助的访问。
#	井号 (#) 字符通常标识拨号序列的结尾。 确保 # 字符为模式中的最后一个字符。	路由模式 901181910555# 路由或阻止从国内编号方案拨打的国际号码。最后的 5 之后的 # 字符将此数字标识为序列中的最后一位数字。
\+	加号前置反斜线（即 \+）表示想要配置国际转义符 +。	使用 \+ 意味着国际转义符 + 用作可拨打的数字，而不是通配符。

丢弃前置点数字示例

在路由模式中使用前置点数字丢弃的一个示例是，您希望电话用户拨打接入码来接通外线。在北美洲，用户通常会拨打 9 以访问外线。您可以使用以下路由模式指定：

- 本地呼叫：9.@ 或 9.[2-9]XXXXXX
- 国内呼叫：9.1[2-9]XX
- 国际呼叫：9.011!#

在这些模式中，9 是外线的接入码，点 (.) 是分隔符，通过指示哪些数字在网络内部，哪些数字在网络外部来帮助格式化路由模式。当系统将被叫数字发送到 PSTN 时，您可以使用“丢弃数字”选项从被叫字符串中剥离前置点数字，以便 PSTN 可以路由呼叫。

数字前缀示例

在路由模式中使用数字前缀的一个示例是在站点之间配置网内拨号的场景。您可以创建一个路由模式，以便您的组织内的用户拨打 8 + XXX-XXXX 以在站点之间进行呼叫。对于网外呼叫，您可以删除前缀数字 (8) 并添加新的前缀 1<area code>，以便您可以将呼叫路由到 E.164 格式的 PSTN。

网内和网外模式示例

您可以使用**呼叫分类**字段将路由模式配置为“网内”或“网外”。如果您希望用户获得辅助拨号音以让他们知道其电话在组织外部，则可以将呼叫分类为“网外”。例如，如果您创建的路由模式要求用户拨打 9 来访问外线，并且将其归类为“网外”模式，系统会提供以下拨号音：

- 当您摘机并拨出 9 之前，电话发出拨号音。
- 在您拨打 9 后的第二个拨号音，表明系统已准备好呼叫公共交换电话网 (PSTN) 号码。

使用此选项时，请确保取消选中**允许设备覆盖**复选框。

阻止和路由模式示例

使用阻止和路由模式来阻止您不想要路由的传出或传入呼叫。使用阻止模式以：

- 阻止特定模式。例如，阻止模式 91900XXXXXXX 可以防止用户向 900 个服务发出呼叫。
- 通过阻止拨打特定区号和位置的电话来防止收费欺诈。

启用群集范围内的自动路由迂回

为群集启用自动路由迂回 (AAR)。

过程

-
- 步骤 1** 从 Cisco Unified CM 管理中，选择系统 > 服务参数。
 - 步骤 2** 在服务器下拉框中选择一个节点。
 - 步骤 3** 从服务下拉列表中，选择 Cisco Call Manager。
 - 步骤 4** 在“群集范围参数（系统 - CCM 自动路由迂回）”区域中，将**启用自动路由迂回**参数设置为真。
-

配置 AAR 组

配置自动路由迂回 (AAR)，以让系统因位置带宽不足而阻止呼叫时自动通过 PSTN 或其他网络重新路由呼叫。通过 AAR，主叫方无需挂机和重拨被叫方。

过程

-
- 步骤 1** 从 Cisco Unified CM 管理中，选择呼叫路由 > AAR 组。
 - 步骤 2** 选择下列选项之一：
 - 单击**新增**以添加新的 AAR 组。
 - 单击**查找**并从结果列表中选择 AAR 组，以修改现有 AAR 组的设置。

AAR 组配置窗口即会显示。

步骤 3 在名称字段中，输入您要分配给新的 AAR 组的名称。

名称最多可以包含 20 个字母数字字符，可以包含空格、点(.)、连字符(-)和下划线(_)的任意组合。
窗口刷新并显示其他字段。

步骤 4 在 AAR 组配置窗口上配置字段。有关字段及其配置选项的更多信息，请参阅系统联机帮助。

步骤 5 单击保存。

注释 可选。要启用 AAR 与寻线引导一起使用，请参阅[寻线引导配置任务流程](#)，第 203 页。

配置每天定时路由时间

可选。创建时间表来指定分区何时可用于接收来电。



注释 没有为留言通知指示灯 (MWI) 截取实施每天定时路由时间。

过程

	命令或操作	目的
步骤 1	配置时段 ，第 194 页	此程序用于定义时段。您可以定义开始时间和结束时间，还可以将重复间隔指定为星期几或年历中的指定日期。
步骤 2	配置时间表 ，第 195 页	使用此程序创建时间表。您在之前的程序中配置的时段是此时间表的构建块。您可以将时段分配到多个时间表。
步骤 3	将时间表与分区关联 ，第 195 页	关联时间表与分区以确定主叫设备在每日特定时间尝试完成呼叫时搜索的分区。

配置时段

此程序用于定义时段。您可以定义开始时间和结束时间，还可以将重复间隔指定为星期几或年历中的指定日期。

过程

步骤 1 从 Cisco Unified CM 管理中，选择呼叫路由 > 控制级 > 时段。

步骤 2 配置时段配置窗口中的字段。有关字段及其配置选项的更多信息，请参阅系统联机帮助。

步骤 3 单击保存。

配置时间表

使用此程序创建时间表。您在之前的程序中配置的时段是此时间表的构建块。您可以将时段分配到多个时间表。

过程

- 步骤 1 从 Cisco Unified CM 管理中，选择呼叫路由 > 控制级 > 时间表。
- 步骤 2 配置时间表配置窗口中的字段。有关字段及其配置选项的更多信息，请参阅系统联机帮助。
- 步骤 3 单击保存。

将时间表与分区关联

关联时间表与分区以确定主叫设备在每日特定时间尝试完成呼叫时搜索的分区。

过程

- 步骤 1 从 Cisco Unified CM 管理中，选择呼叫路由 > 控制级 > 分区。
- 步骤 2 从下拉列表中，选择与此分区关联的时间表。
时间表指定分区何时可用于接收来电。如果您选择无，该分区将始终保持活动状态。
- 步骤 3 单击保存。

呼叫路由限制

功能	限制
路由过滤器关联	配置呼叫路由时，小心不要将一个路由过滤器分配给过多的路由模式。如要编辑具有数百个关联路由模式的路由过滤器，可能会导致系统核心崩溃。这是因为必须进行额外的系统处理，以便为使用该路由过滤器的所有路由模式更新呼叫路由。创建重复的路由过滤器，以确保表示不会出现这种情况。

功能	限制
外部呼叫控制	<p>外部呼叫控制可让附属路由服务器通过 Cisco Unified 路由规则界面对 Unified Communications Manager 进行呼叫路由决策。配置外部呼叫控制时，Unified Communications Manager 发出包含主叫方和被叫方信息的路由请求到附属路由服务器。该服务器接收请求，应用适当业务逻辑，并返回一个路由回复，指示您的系统如何路由呼叫以及要应用的任何其他呼叫处理。</p> <p>有关详细信息，请参阅《Cisco Unified Communications Manager 功能配置指南》的配置外部呼叫控制一章。</p>
呼叫控制发现	<p>使用呼叫控制发现，Unified Communications Manager 群集可以通过订阅名为服务广告框架 (SAF) 的 Cisco IOS 服务路由协议，自动交换其托管的 DN 范围。此功能可让群集将自己的托管的 DN 范围公告到网络中，以及订阅由网络中的其他呼叫座席生成的通告。</p> <p>使用 SAF CCD 的主要优点是：</p> <ul style="list-style-type: none"> 在参与同一 SAF CCD 网络的呼叫座席之间自动分配呼叫路由信息，从而避免添加新呼叫座席或将新的 DN 范围添加到呼叫座席时增加配置工作。 不依赖于集中式拨号方案解析控制点。 发生路由更改时（包括多个 Unified CM 群集合并时）自动恢复呼叫座席间呼叫路由信息。 <p>要配置呼叫控制发现，请参阅《Cisco Unified Communications Manager 功能配置指南》的配置呼叫控制发现一章。</p>
路由计划报告	<p>您可以在 Cisco Unified CM 管理的“路由计划报告”窗口（呼叫路由 > 路由计划报告）中查看详细的路由计划。通过路由计划报告可以查看路由计划的部分或完整列表，也可以单击报告的“模式/目录号码”、“分区”或“路由详细信息”列中的条目直接进入关联的配置窗口。</p> <p>此外，路由计划报告还可让您将报告数据保存到可以导入其他应用程序的 .csv 文件。.csv 文件包含的信息比网页更详细，其中包括电话的目录号码、路由模式、模式的使用、设备名称以及设备说明。</p>

使用被叫号码分析器进行故障诊断

被叫号码分析器作为功能服务随 Cisco Unified Communications Manager 安装。该工具可让您在部署 Cisco Unified Communications Manager 拨号方案配置之前测试它。您还可以使用该工具在部署拨号方案后分析拨号方案。

因为拨号方案可能很复杂，涉及多个设备、转换模式、路由模式、路由列表、路由组、主叫和被叫方转换以及设备级转换，所以拨号方案可能有错误。您可以使用被叫号码分析器，提供拨号数字作为输入，测试拨号方案。该工具分析拨号数字并显示呼叫的详细信息。您可以使用这些结果诊断拨号方案、识别问题（如果有），并在部署前修复拨号方案。

有关如何设置和使用被叫号码分析器的详细信息，请参阅《Cisco Unified Communications Manager 被叫号码分析器》，位于 <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>。

线路组设置

本章提供添加或删除线路组、添加目录号码或者从线路组删除目录号码的信息。

有关其他信息，请参阅《Cisco Unified Communications Manager 系统指南》中与了解路由方案相关的主题。

关于线路组设置

在 Cisco Unified Communications Manager 管理中，使用呼叫路由 > 路由/寻线 > 线路组菜单路径配置线路组。

使用线路组，可以指定选择目录号码的顺序。Cisco Unified Communications Manager 根据呼叫分配算法和“无应答振铃复原 (RNAR) 超时”设置将呼叫分配给线路组的空闲或可用成员。



注释 用户无法使用定向呼叫代答功能代答到属于某个线路组的 DN 的呼叫。



提示 尽管您可以配置一个没有任何成员（目录号码）的空线路组，但是 Cisco Unified Communications Manager 不支持将此配置用于路由呼叫。如果线路组不包含任何成员，则在将呼叫路由至空线路组时，寻线列表将停止寻线。为了避免出现这种情况，请务必至少在线路组中配置一个成员。

线路组配置提示

在配置线路组之前，您必须定义一个或多个目录号码。

在配置或更新线路组后，可以在该线路组中添加或删除成员。

删除线路组

您可以删除一个或多个路由/寻线列表引用的线路组。如果您试图删除正在使用的线路组，Cisco Unified Communications Manager 会显示一条错误消息。



提示 线路组不支持从属关系记录。最好的做法是，始终在删除线路组之前检查配置。

线路组设置

字段	说明
线路组信息	
线路组名称	<p>输入此线路组的名称。名称最多可以包含 50 个字母数字字符，可以包含由空格、点号 (.)、连字符 (-) 和下划线 (_) 组成的任意组合。确保每个线路组名称是路由方案唯一的。</p> <p>便捷程序 对线路组使用简明的描述性名称。CompanynameLocationGroup 格式通常能够提供足够详细的信息，且够简短，可供您快速轻松地标识线路组。例如，CiscoDallasAA1 标识了用于思科达拉斯办公室的 Cisco Access Analog 线路组。</p>
RNA 复原超时	<p>输入时间（单位为秒），当呼叫无应答并且选择了第一个寻线选项“试拨下一个成员；然后，试拨寻线列表中的下一组”时，则经过该指定秒数后 Unified Communications Manager 会将呼叫分配到线路组中下一个可用或空闲的成员，或者分配到下一个线路组。“RNA 复原超时”在线路组层级应用到所有成员。</p>
分配算法	<p>从下拉列表框中的选项选择在线路组层级应用的分配算法：</p> <ul style="list-style-type: none"> • 自上而下 — 如果选择此分配算法，Unified Communications Manager 将从线路组中第一个空闲或可用的成员开始分配呼叫，一直到最后一个空闲或可用的成员。 • 循环 — 如果选择此分配算法，Unified Communications Manager 将从路由组中第 (n+1) 个空闲或可用成员开始分配呼叫，第 n 个成员是指列表中空闲或者忙碌但未“关闭”的下一个顺序成员。如果第 n 个成员是路由组的最后一个成员，Unified Communications Manager 将从路由组顶部开始分配呼叫。 • 最长空闲时间 — 如果选择此分发算法，Unified Communications Manager 只将呼叫分发给空闲的成员，顺序是从线路组中空闲时间最长的成员到空闲时间最短的成员。 • 广播 — 如果选择此分发算法，Unified Communications Manager 会同时将某个呼叫分发给线路组中的所有空闲或可用的成员。有关使用广播分配算法的其他限制，请参阅“所选 DN/路由分区”字段说明中的“注意”。 <p>默认值为“最长空闲时间”。</p>
寻线选项	

字段	说明
无应答	<p>指定分配算法后，为 Unified Communications Manager 选择在呼叫分配到无法应答的线路组成员时要使用的寻线选项。此选项在成员层级应用。从下拉列表框中选择选项：</p> <ul style="list-style-type: none"> • 试拨下一个成员；然后，试拨寻线列表中的下一组 - 如果选择此寻线选项，Unified Communications Manager 将从线路组中第一个空闲或可用的成员开始分配呼叫，一直到最后一个空闲或可用的成员。如果不成功，Unified Communications Manager 然后会尝试寻线列表中的下一个线路组。 • 试拨下一个成员，但不要转至下一组 - 如果选择此寻线选项，Unified Communications Manager 将从线路组中第一个空闲或可用的成员开始分配呼叫，一直到最后一个空闲或可用的成员。Unified Communications Manager 在到达当前线路组的最后一个成员后将停止试拨。 • 跳过其余成员，直接转至下一组 — 如果选择此寻线选项，当试拨第一个成员经过了 RNA 复原超时值后，Unified Communications Manager 将跳过此线路组的其余成员。然后，Unified Communications Manager 直接转到寻线列表中的下一个线路组。 • 停止寻线 — 如果选择此寻线选项，Unified Communications Manager 将在尝试分配呼叫到此线路组的第一个成员但该成员不应答呼叫后停止寻线。
无应答时自动注销寻线成员	<p>如果选中此复选框，线路成员将自动从寻线列表注销。线路成员可以使用 "HLOG" 软键或 PLK 重新登录。</p>

字段	说明
忙	<p>指定分配算法后，为 Unified Communications Manager 选择在呼叫分配到忙碌的线路组成员时要使用的寻线选项。 从下拉列表框中选择选项：</p> <ul style="list-style-type: none"> • 试拨下一个成员；然后，试拨寻线列表中的下一组 - 如果选择此寻线选项，Unified Communications Manager 将从线路组中第一个空闲或可用的成员开始分配呼叫，一直到最后一个空闲或可用的成员。如果不成功，Unified Communications Manager 然后会尝试寻线列表中的下一个线路组。 • 试拨下一个成员，但不要转至下一组 - 如果选择此寻线选项，Unified Communications Manager 将从线路组中第一个空闲或可用的成员开始分配呼叫，一直到最后一个空闲或可用的成员。Unified Communications Manager 在到达当前线路组的最后一个成员后将停止试拨。 • 跳过其余成员，直接转至下一组 - 如果选择此寻线选项，Unified Communications Manager 在遇到忙线成员时将跳过此线路组的其余成员。Unified Communications Manager 将直接转到寻线列表中的下一个线路组。 • 停止寻线 - 如果选择此寻线选项，Unified Communications Manager 将在尝试分配呼叫到此线路组的第一个忙线成员后停止寻线。
不可用	<p>指定分配算法后，为 Unified Communications Manager 选择在呼叫分配到无法接通的线路组成员时要使用的寻线选项。 当与相关目录号码关联的电话未注册时，将会发生“无法接通”的情况。当分机移动在使用中并且目录号码/用户未登录时，也会发生“无法接通”。请从下拉列表中选择选项：</p> <ul style="list-style-type: none"> • 试拨下一个成员；然后，试拨寻线列表中的下一组 - 如果选择此寻线选项，Unified Communications Manager 将从线路组中第一个空闲或可用的成员开始分配呼叫，一直到最后一个空闲或可用的成员。如果不成功，Unified Communications Manager 然后会尝试寻线列表中的下一个线路组。 • 试拨下一个成员，但不要转至下一组 - 如果选择此寻线选项，Unified Communications Manager 将从线路组中第一个空闲或可用的成员开始分配呼叫，一直到最后一个空闲或可用的成员。Unified Communications Manager 在到达当前线路组的最后一个成员后将停止试拨。 • 跳过其余成员，直接转至下一组 - 如果选择此寻线选项，Unified Communications Manager 在遇到第一个无法接通的成员时将跳过此线路组的其余成员。Unified Communications Manager 将直接转到寻线列表中的下一个线路组。 • 停止寻线 - 如果选择此寻线选项，Unified Communications Manager 将在尝试分配呼叫到此线路组的第一个无法接通的成员后停止寻线。

字段	说明
线路组成员信息	
查找要添加到线路组的目录号码	
分区	从下拉列表框中为此线路组选择路由分区。默认值为 <None>。 如果单击“查找”，“可用 DN/路由分区”列表框将会显示属于所选分区的所有目录号码。
目录号码包含	输入您要查找的目录号码中包含的字符，然后单击“查找”按钮。与输入的字符匹配的目录号码显示在“可用 DN/路由分区”框中。
可用 DN/路由分区	在“可用 DN/路由分区”列表框中选择一个目录号码，并单击“添加到线路组”将其添加到“所选 DN/路由分区”列表框中。
当前线路组成员	
采用共享线路目录号码的广播算法	要更改目录号码的优先级，请在“所选路由分区”列表框中选择一个目录号码。单击列表框右侧的箭头，可在列表中上移或下移目录号码。 要反向排列“所选 DN/路由分区”中目录号码的优先顺序，请单击“反转所选 DN/路由分区的顺序”。 注释 将目录号码和路由分区添加到线路组时，请勿在使用“广播”分配算法的线路组中添加是共享线路的目录号码。如果目录号码是使用“广播”分配算法的线路组成员，Unified Communications Manager 无法显示是设备（其中的目录号码配置为共享线路）上共享线路的所有目录号码。
删除的 DN/路由分区	在“所选 DN/路由分区”列表框中选择一个目录号码，并单击两个列表框之间的向下箭头将其添加到“删除的 DN/路由分区”列表框中。
目录号码	
（当前属于此线路组的目录号码列表）	单击此列表中的目录号码可进入指定目录号码的“目录号码配置”窗口。 注释 添加新的线路组时，此列表在该线路组保存之前不会显示。

向线路组添加成员

您可以添加成员到新线路组或现有线路组。以下程序介绍添加成员到现有线路组。

开始之前

执行此程序之前，您必须定义一个或多个目录号码。

过程

步骤 1 选择呼叫路由 > 路由/寻线 > 线路组。

步骤 2 找到您要添加成员的线路组。

步骤 3 如果需要查找目录号码，从“分区”下拉列表框中选择一个路由分区，在“目录号码包含”字段中输入一个搜索字符串，然后单击“查找”。要查找属于分区的所有目录号码，请将“目录号码包含”字段留空，然后单击“查找”。

“可用 DN/路由分区”列表框中将显示匹配目录号码的列表。

步骤 4 在“可用 DN/路由分区”列表框中，选择要添加的目录号码，然后单击“添加到线路组”将其移动到“所选 DN/路由分区”列表框。对您要添加到此线路组的每个成员重复此步骤。

步骤 5 在“所选 DN/路由分区”列表框中，选择此线路组中要访问的新目录号码的顺序。要更改该顺序，单击一个目录号码，并使用列表框右侧的“向上”和“向下”箭头更改目录号码的顺序。

步骤 6 单击“保存”以添加新目录号码并更新此线路组的目录号码顺序。

从线路组中删除成员

您可以从新线路组或现有线路组删除成员。以下程序介绍如何从现有线路组删除目录号码。

过程

步骤 1 选择呼叫路由 > 路由/寻线 > 线路组。

步骤 2 找到要从中删除目录号码的线路组。

步骤 3 在“所选 DN/路由分区”列表框中，选择要删除的目录号码，然后单击列表框下面的向下箭头将其移到“删除的 DN/路由分区”列表框中。对您要从此线路组删除的每个成员重复此步骤。

步骤 4 要删除成员，请单击“保存”。



第 21 章

配置寻线引导

- [寻线引导概述，第 203 页](#)
- [寻线引导配置任务流程，第 203 页](#)
- [寻线引导相互作用和限制，第 208 页](#)

寻线引导概述

寻线引导包含一个号码或模式以及一组关联的数字处理，可将呼叫路由到线路组中的一组电话或目录号码。

寻线引导与寻线列表配合使用，即用于确定传入呼叫的合格路径（线路组）优先级列表。当呼叫拨打到寻线引导 DN 时，系统会将呼叫提供给寻线列表中指定的第一个线路组。如果第一个线路组中无人应答呼叫，则系统会将呼叫提供给寻线列表中指定的下一个线路组。线路组控制呼叫分配到组内电话的顺序。它们指向特定的分机，通常是 IP 电话分机或语音邮件端口。线路组不能指向计算机电话集成 (CTI) 端口和 CTI 路由点，因此您无法使用寻线引导将呼叫分配到通过 Cisco 客户响应解决方案 (CRS) 或 IP 交互式语音应答 (IP IVR) 等 CTI 应用程序控制的终端。

寻线引导可以将呼叫分配到任何其所分配线路组，即使线路组和寻线引导位于不同的分区。寻线引导所分配的呼叫将超越所有分区和呼叫搜索空间限制。

寻线引导配置任务流程

完成这些任务以为您的系统配置寻线引导。寻线引导可用于将呼叫路由到线路组中的一组电话或目录号码。

过程

	命令或操作	目的
步骤 1	配置线路组，第 204 页	创建一个线路组，使多部电话能够应答定向到单个目录号码 (DN) 的呼叫。
步骤 2	配置寻线列表，第 204 页	使用线路组的优先顺序配置寻线列表。

	命令或操作	目的
步骤 3	配置寻线引导，第 205 页	配置系统用于将呼叫定向到寻线列表的寻线引导号码或模式。

配置线路组

线路组允许多部电话应答定向到单个目录号码的呼叫。分配算法控制来电分配到组中电话的顺序。

过程

步骤 1 从 Cisco Unified CM 管理中，选择呼叫路由 > 路由/寻线 > 线路组。

步骤 2 选择下列选项之一：

- 单击**新增**以创建新的线路组。
- 单击**查找**并选择现有线路组。

步骤 3 输入线路组名称。

步骤 4 从分配算法字段中，选择要用于分配呼叫的算法类型。

步骤 5 配置要添加到线路组的线路组成员部分的字段，以将目录号码添加到线路组：

- 选择要添加的目录号码所在的分区。
- 可选。填写目录号码包含字段以过滤搜索。
- 单击**查找**。分区中的目录号码列表将显示在框中。
- 在可用目录号码/路由分区列表框中，选择要添加到组的每个目录号码，然后单击**添加到线路组**。

步骤 6 完成线路组配置窗口中其余字段的设置。请参阅联机帮助，了解有关字段及其配置选项的更多信息。

步骤 7 单击**保存**。

配置寻线列表

寻线列表是按优先顺序排列的线路组列表。当系统通过寻线列表路由呼叫时，它将按您在寻线列表中定义的顺序使用线路组。

过程

步骤 1 从 Cisco Unified CM 管理中，选择呼叫路由 > 路由/寻线 > 寻线列表。

步骤 2 选择下列选项之一：

- 单击**新增**以创建一个新的列表。
- 单击**查找**并选择现有列表。

步骤 3 输入寻线列表的名称。

步骤 4 选择要向其注册寻线列表的 **Cisco Unified Communications Manager** 组。

步骤 5 选中**启用此寻线列表**复选框可让您在单击“保存”时立即启用寻线列表。

步骤 6 如果寻线列表用于语音信箱，选中**用于语音信箱**复选框。

步骤 7 单击**保存**。

步骤 8 将线路组添加到寻线列表：

- a) 单击**添加线路组**。
- b) 从**线路组**下拉列表中，选择要添加到寻线列表的线路组。
- c) 单击**保存**。
- d) 重复上述步骤添加其他线路组。

配置寻线引导

配置系统用于将呼叫路由到线路组的寻线引导号码或模式。



注释 有关可用于寻线引导的通配符和特殊字符的信息，请参阅[寻线引导中的通配符和特殊字符](#)，第 205 页。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**呼叫路由 > 路由/寻线 > 寻线引导**。

步骤 2 选择下列选项之一：

- 单击**新增**以创建一个新的寻线引导。
- 单击**查找**并选择现有寻线引导。

步骤 3 在**寻线引导**字段中，输入要用于路由呼叫的号码或模式。

步骤 4 从**寻线列表**下拉列表中，选择您要将与寻线引导号码匹配的呼叫定向到其中的寻线列表。

步骤 5 完成**寻线引导配置**窗口中其余字段的设置。有关这些字段及其设置的帮助，请参阅联机帮助。

步骤 6 如果要启用呼叫队列，请选中**队列呼叫**复选框并配置**队列**部分中的字段。

步骤 7 分配您要应用到呼叫、已接通或被叫方的任何数字转换模式。

步骤 8 单击**保存**。

寻线引导中的通配符和特殊字符

寻线引导中的通配符和特殊字符允许寻线引导匹配数字（地址）范围。使用这些通配符和特殊字符还可以构建指令，允许 Cisco Unified Communications Manager 操纵号码，然后将其发送到相邻系统。

下表说明 Cisco Unified Communications Manager 支持的通配符和特殊字符。

表 20: 通配符和特殊字符

字符	说明	示例
@	@ 符号通配符匹配所有国内编号方案号码。 每个路由模式只能有一个 @ 通配符。	路由模式 9.@ 路由或阻止国内编号方案识别的所有号码。 以下路由模式示例展示 @ 通配符包含的国内编号方案号码： <ul style="list-style-type: none"> • 0 • 1411 • 19725551234 • 101028819725551234 • 01133123456789
X	X 通配符匹配范围 0 至 9 的任何单一数字。	路由模式 9XXX 路由或阻止范围 9000 至 9999 的所有号码。
!	惊叹号 (!) 通配符匹配范围 0 至 9 的一个或多个数字。	路由模式 91! 路由或阻止范围 910 至 91999999999999999999999999999999 的所有号码。
?	问号 (?) 通配符匹配零次或多次出现的前置数字或通配符值。 注释 如果使用问号 (??) 通配符，第二个问号与空输入不匹配。路由器模式示例：*33X?*X?*X?#	路由模式 91X? 路由或阻止范围 91 至 91999999999999999999999999999999 的所有号码。
+	加号 (+) 通配符匹配一次或多次出现的前置数字或通配符值。	路由模式 91X+ 路由或阻止范围 910 至 91999999999999999999999999999999 的所有号码。
[]	方括号 ([]) 字符括起值范围。	路由模式 813510[012345] 路由或阻止范围 8135100 至 8135105 的所有号码。
-	连字符 (-) 与方括号一起使用，用于指示值范围。	路由模式 813510[0-5] 路由或阻止范围 8135100 至 8135105 的所有号码。

字符	说明	示例
^	抑扬符号 (^) 与方括号一起使用，用于排除值范围。确保第一个字符后跟左括号 ([]。 每个路由模式只能有一个 ^ 字符。	路由模式 813510[^0-5] 路由或阻止范围 8135106 至 8135109 的所有号码。
.	点 (.) 字符用作分隔符，分隔 Cisco Unified Communications Manager 访问代码与目录号码。 使用此特殊字符及丢弃数字指令，剥离 Cisco Unified Communications Manager 访问代码，然后再发送该号码到相邻系统。 每个路由模式只能有一个点 (.) 字符。	路由模式 9.@ 确定开头的 9 作为国内编号方案呼叫中的 Cisco Unified Communications Manager 访问代码。
*	星号 (*) 字符可为特殊被叫号码提供一位额外的数字。	可以配置路由模式 *411 以提供内部接线员目录协助的访问。
#	井号 (#) 字符通常标识拨号序列的结尾。 确保 # 字符为模式中的最后一个字符。	路由模式 901181910555# 路由或阻止从国内编号方案拨打的国际号码。最后的 5 之后的 # 字符将此数字标识为序列中的最后一位数字。
\+	加号前置反斜线 (即 \+) 表示想要配置国际转义符 +。	使用 \+ 意味着国际转义符 + 用作可拨打的数字，而不是通配符。

寻线引导的性能和可扩展性

以下性能和可扩展性限制适用：

- 一个 Unified CM 群集最多支持 15,000 个寻线列表设备。
- 一个 Unified CM 订阅方最多支持每个节点 100 个启用了呼叫排队的寻线引导。
- 寻线列表设备可以是如下组合：1500 个寻线列表，每个寻线列表中 10 部 IP 电话；750 个寻线列表，每个寻线列表中 20 个 IP 电话；或类似的组合。



注释

在使用广播算法进行呼叫覆盖时，寻线列表设备的数量受忙时呼叫尝试次数 (BHCA) 的限制。请注意，指向包含 10 部电话的寻线列表或寻线组的寻线引导上 BHCA 为 10，与具有 BHCA 为 10 的 10 部电话等效。

- 寻线引导的最大数量为每个 Unified CM 订阅方节点 100，并且在配置了队列中允许的 32 个主叫方时启用了呼叫队列。每个节点队列槽的最大数量（合并节点上所有启用呼叫排队的寻线引导的“队列中允许的最高主叫方数目”的值）限于 3200。每个寻线引导的队列中并发主叫方最大数量为 100，表示每个寻线列表 100 个主叫方在队列中是允许的，寻线引导最大数量减为 32。启用呼叫排队时，所有寻线列表中的最大成员数不变。
- 队列中您可以为每个寻线引导配置的最长等待时间范围是 0 到 3600 秒（默认值为 900）。如果寻线列表数增加，则可能需要增加 Unified Communications Manager 服务参数中指定的拨号方案初始化计时器的值。如果您配置了 1500 个寻线列表，我们建议您将拨号方案初始化计时器设置为 600 秒。
- 对呼叫排队使用广播算法时，我们建议单个线路组不超过 35 个目录号码。此外，广播线路组的数量取决于忙时呼叫完成率 (BHCC)。如果在一个 Unified CM 系统中有多组广播线路组，线路组中的最大目录号码数必须小于 35。所有广播线路组的忙时呼叫尝试次数 (BHCA) 不应超过每秒 35 个呼叫的设置。

寻线引导相互作用和限制

功能	交互和限制
一号通与寻线组	<p>如果配置了寻线组，并且寻线组指向的一个或多个目录号码也启用了一号通 (SNR)，则呼叫不会扩展到 SNR 远程目标，除非寻线组中的所有设备都已登录。</p> <p>对于寻线组中的每个设备，必须在该设备的电话配置窗口中选中登录寻线组复选框。</p>
呼叫排队	<p>呼叫排队是寻线引导的子功能。当启用了呼叫排队并且对特定寻线引导的来电要求超出可用来应答呼叫的寻线成员数量时，系统会将来电排队，直到寻线成员可以应答它们为止。您可以配置通知和音乐保持，以便在主叫方等待时为其播放。</p> <p>有关其他配置详细信息，请参阅Cisco Unified Communications Manager 功能配置指南的“配置呼叫排队”一章。</p>
Unified Mobility	我们不建议在寻线引导中配置 Unified Mobility 设备。

未分配的呼叫

表 21: 呼叫不使用循环算法分配

限制	说明
对于使用 BOT 和 TCT 设备的线路组，不会在循环算法中正确分配呼叫。	当呼叫转至处于“已注销”状态的某个座席并且该呼叫通过 "Huntlogout" 类型以外的拒绝类型被拒绝。然后，索引将不会递增，并且呼叫将转至已应答上一个呼叫的同一座席。
呼叫不能按线路组的循环算法正确分配。	<p>在按循环算法分配呼叫时，当座席忙时，该呼叫将转至下一个有空座席（即，下一个座席将代表忙碌座席应答呼叫）。</p> <p>注释 在同时进行多个呼叫的情况下，下一个有空座席将应答该呼叫。</p>



第 22 章

配置群集间查询服务

- [ILS 概述，第 211 页](#)
- [ILS 配置任务流程，第 212 页](#)
- [ILS 相互作用和限制，第 215 页](#)

ILS 概述

Cisco 群集间查询服务 (ILS) 使创建共享数据的远程 Cisco Unified Communications Manager 群集的多群集网络变得很容易。

ILS 无需管理员手动配置群集之间的连接。在中枢群集上配置 ILS 后，您可以通过在新群集上启用 ILS 并将新群集指向现有中枢来连接新的群集。ILS 会自动连接群集，让我们的两个群集了解较大 ILS 网络的拓扑。

ILS 网络组件

ILS 网络由以下组件组成：

- **中枢群集**—中枢群集使用自动网格功能构成 ILS 网络中枢，通过其他中枢群集创建完整的网状拓扑。中枢群集在 ILS 网络中中继和共享信息，以实现各种功能。
- **星形群集**—星形群集仅连接本地中枢群集，从不直接与其他中枢群集或其他星形群集直接联系。星形群集依靠其本地中枢在整个网络中共享和中继信息。
- **全局拨号方案导入的类目**—如果您已配置全局拨号方案复制，并且您与 Cisco TelePresence Video communication Server 或第三方呼叫控制系统互操作，则应用此可选组件。手动将从其他系统导出的 CSV 文件导入目录 URI 或 +E.164 号码类目，从而允许 ILS 网络中的用户从其他系统中呼叫用户。

群集视图

ILS 的远程群集查看功能可用于映射网络。每个群集将交换更新消息，这些消息称为对等成员信息载体，它们向远程群集通知网络中每个群集的状态。这些更新消息包含有关网络中已知群集的信息，包括：

- 群集 ID

- 发布方的对等成员 Id
- 群集说明和版本
- 主机的完全限定域名 (FQDN)
- 已激活 ILS 的群集节点的 IP 地址和主机名

功能支持

全局拨号方案复制和分机移动漫游等功能依赖于 ILS 创建群集间网络，其中群集共享拨号方案信息。这可让您使用视频呼叫、URI 拨号和群集间移动功能设置群集间呼叫网络。

如果您将 IM and Presence 中心群集连接到多个电话群集，则 IM and Presence Service 的集中式部署也会使用 ILS。ILS 用于创建 IM and Presence 中心群集与电话群集之间的连接。

ILS 网络容量

在规划 ILS 网络时，建议您记住以下容量：

- ILS 网络最多支持 10 个中枢群集，每个中枢群集 20 个星形群集，总计最多 200 个群集。中枢和星形组合拓扑用于避免在每个群集中创建多个 TCP 连接。
- 中枢和星形群集数目达到或超过最大值可能会对性能产生影响。将过多的星形群集添加到单个中枢会导致额外的连接，从而增加内存或 CPU 处理量。建议连接到中枢群集的星形群集数目不超过 20 个。
- ILS 网络会将额外的 CPU 处理添加到您的系统。CPU 利用率和同步时间取决于在整个群集内同步的记录数。规划中枢和星形拓扑时，请确保您的中枢群集有 CPU 来处理负载。



注释 这些建议基于系统测试，并且会考虑资源使用情况。尽管系统不会阻止您超出这些建议，但这样做会导致过度使用资源的风险。为获得最佳性能，Cisco 建议采用上述容量。

ILS 配置任务流程

完成这些任务以设置 ILS 网络。

开始之前

确保对您的 ILS 拓扑进行规划，以便了解哪些群集将成为中枢群集，哪些将是星形群集。

过程

	命令或操作	目的
步骤 1	配置群集 ID，第 213 页	ILS 网络中的每个群集都必须具有唯一的群集 ID
步骤 2	配置 ILS，第 213 页	在网络的各种群集中配置和激活 ILS。
步骤 3	验证 ILS 正在运行，第 214 页	确认 ILS 网络已启动并正在运行。
步骤 4	配置远程群集视图，第 215 页	为 ILS 网络配置远程群集视图。

配置群集 ID

ILS 网络中的每个群集都必须具有唯一的群集 ID。如果您的远程群集保留群集 ID 的默认 **StandAloneCluster** 值，则 ILS 不工作。

过程

- 步骤 1 登录到发布方节点上的 Cisco Unified CM 管理。
- 步骤 2 选择系统 > 企业参数。
- 步骤 3 将群集 ID 的值设置为唯一标识该群集的值。
- 步骤 4 单击保存。
- 步骤 5 在每个群集的发布方节点上重复此程序。

配置 ILS

使用此程序在您的网络中激活并配置群集间查询服务 (ILS)。



注释 您配置的第一个群集必须是中枢群集。

过程

- 步骤 1 登录到发布方节点上的 Cisco Unified CM 管理。
- 步骤 2 选择高级功能 > ILS 配置。
- 步骤 3 从角色下拉列表框中，根据您要设置的群集类型，选择中枢群集或星形群集。
- 步骤 4 如果要启用全局拨号方案复制，请选中与远程群集交换全局拨号方案复制数据复选框。

注释 通告 URI 模式 (user@domain) 时，在 **SIP 配置文件配置窗口** 中，确保拨号字符串解析字段设置为**始终将所有拨号字符串视为 URI 地址**，以防止设备拨打 URI 学习的模式，其中仅将用户部分中的数字作为目录号码模式。或者，可以通过 ILS 在用户部分中仅通告带有文本字符串的 URI 模式。

步骤 5 在网络中的各个群集之间配置 **ILS 身份验证** 详细信息：

- 对于 TLS 验证，选中**使用 TLS 证书**复选框。请注意，如果选择此选项，则必须在群集中的节点之间交换 CA 签名的证书。
- 对于密码身份验证（无论是否使用 TLS），请选中**使用密码**复选框并输入密码详细信息。

步骤 6 单击**保存**。

步骤 7 在 **ILS 群集注册**弹出窗口中，配置您的注册详细信息：

- 在**注册服务器**文本框中，输入要将此群集连接到的中枢群集的发布方节点 IP 地址或 FQDN。如果这是您网络中的第一个中枢群集，可以将此字段留空
- 确保选中在此群集中的发布方上**激活群集间查询服务**复选框。
- 单击**确定**。

步骤 8 在要加入到 ILS 网络的每个群集的发布方节点上重复此程序。将新群集添加为中枢或星形群集。

注释 根据您配置的同步值，群集信息在整个网络中传播时可能会有延迟。

如果您选择在群集之间使用传输层安全 (TLS) 验证，则必须在 ILS 网络中每个群集的发布方节点之间交换 Tomcat 证书。在 Cisco Unified 操作系统管理中，使用“批量证书管理”功能：

- 将证书从每个群集的发布方节点导出到中心位置
- 在 ILS 网络中合并导出的证书
- 将证书导入网络中每个群集的发布方节点

有关详细信息，请参阅《Cisco Unified Communications Manager 管理指南》的“管理证书”一章。

验证 ILS 正在运行

确认 ILS 网络已启动并运行。

过程

步骤 1 登录到任一电话群集的发布方节点。

步骤 2 从 Cisco Unified CM 管理中，选择高级功能 > **ILS 配置**。

步骤 3 选中 **ILS 群集**和**全局拨号方案**导入的类目部分。此时您的 ILS 网络拓扑会显示。

配置远程群集视图

使用此程序配置 ILS 网络的远程群集视图。

过程

- 步骤 1 在 Cisco Unified CM 管理中，选择高级功能 > 群集视图。
- 步骤 2 在查找并列出远程群集窗口中，选择任何之前创建的远程群集。
- 步骤 3 从“远程群集服务配置”窗口中，选中相应的复选框可为远程群集配置跨群集分机移动、TFTP 和 RSVP 座席等服务。
- 步骤 4 单击保存。

ILS 相互作用和限制

ILS 相互作用

表 22: ILS 相互作用

功能	互动
群集发现	<p>ILS 群集发现允许 Cisco Unified Communications Manager 群集动态了解远程群集，无需管理员手动配置这些群集之间的连接。</p> <p>ILS 网络中的每个群集将交换更新消息，这些消息称为对等成员信息载体，它们用于向远程群集通知网络中每个群集的状态。这些更新消息包含有关网络中已知群集的信息，包括：</p> <ul style="list-style-type: none">• 群集 ID• 群集说明和版本• 主机的完全限定域名• 已激活 ILS 的群集节点的 IP 地址和主机名 <p>ILS 群集发现功能将自动填充远程群集列表，在 Cisco Unified CM 管理中选择高级功能 > 群集视图即可查看该列表。在此窗口中，您可以为远程群集配置诸如跨群集分机移动、TFTP 和 RSVP 座席等服务。</p> <p>注释 远程群集的完全限定域名（如群集视图中所示）必须是可解析的 DNS，才能使 ILS 发现正常工作。</p>

功能	互动
全球拨号方案复制	<p>在跨 ILS 网络启用全球拨号方案复制后，ILS 网络中的远程群集将共享全球拨号方案数据，包括以下项目：</p> <ul style="list-style-type: none"> • 目录 URI • 备用号码 • 备用号码模式 • 路由字符串 • PSTN 故障转移号码
屏蔽来电	<p>要根据基于 ILS 的网络中的主叫方号码屏蔽来电，必须在主叫方 CSS 中包含 SIP 路由模式的分区。例如，如果从 SIP 干线发起呼叫，则 SIP 干线入站 CSS 必须有 SIP 路由模式的分区。</p>

ILS 限制

表 23: ILS 限制

限制	说明
ILS 服务	ILS 服务仅在 Unified Communications Manager 发布方节点上运行。
群集	一个中枢群集可以连接到多个星形群集，但一个星形群集只能连接到一个中枢群集。
ILS 网络	您不能将第三方呼叫控制系统连接到 ILS 网络。
群集导入	您只能将第三方类目导入到中枢群集中。
重复的 URI	如果学习的 ILS 群集包含来自另一个远程群集的重复 URI，并且向该 URI 发起呼叫，则该群集将路由到其 URI 已获知的群集并首先插入到数据库中。
数据库复制状态	虽然在 ILS 网络上成功交换全局拨号方案数据，但 ILS 接收群集在完成其数据库复制状态之前不会将学习的信息写入数据库中。
导入	对于导入的第三方目录 URI 和模式，CSV 文件格式必须与管理窗口示例文件中所示的正确语法匹配，否则导入将失败。

限制	说明
ILS 中枢	<p>将其他中枢群集添加到 ILS 网络中时，请确保对主 ILS 中枢节点验证符合以下条件：</p> <ul style="list-style-type: none"> • 群集 ID 在 ILS 群集中的所有中枢节点上都是唯一的。 • 完全限定域名 (FQDN) 已配置。 • ILS 群集中的所有中枢节点上都在运行 UDS 和 EM 服务 • DNS 主和反向解析工作正常。 • 从所有中枢节点导入合并的 Tomcat 证书。 <p>否则，即使在重新启动群集或更正错误后，“版本”信息也不会显示在查找并列出远程群集窗口中。解决办法是从 ILS 网络中删除中枢群集，遵守上述要求，然后将中枢群集添加回 ILS 网络。</p>



第 23 章

配置全球拨号方案复制

- [全局拨号方案复制概述，第 219 页](#)
- [全局拨号方案复制前提条件，第 223 页](#)
- [全局拨号方案复制配置任务流程，第 223 页](#)
- [全局拨号方案复制相互作用和限制，第 232 页](#)

全局拨号方案复制概述

全局拨号方案复制让使用 URI 拨号、企业号码或、E.164 号码进行拨号的视频呼叫设置群集间 VoIP 网络变得很容易。

全局拨号方案复制通过将全局拨号方案数据元素复制到 ILS 网络中的远程群集来利用 Cisco 群集间查询服务。ILS 网络中的每个群集都会学习其他群集的全局拨号方案元素，以及主群集的路由字符串。

通过 ILS 全局通告

全局拨号方案复制将以下拨号方案元素通告到 ILS 网络，从而在远程群集中复制此数据：

- **目录 URI**—在本地群集中，预配置电子邮件风格的目录 URI（例如 `alice@cisco.com`）。URI 拨号提供以用户为中心的拨出呼叫方法。全局拨号方案复制允许您将目录 URI 的本地类目通告到 ILS 网络中的其他群集，以启用群集间 URI 拨号。
- **企业和 E.164 备用号码**—备用号码是通过将带有前置数字指令的掩码应用到原始目录号码而创建的原始分机的别名。备用号码可以从 ILS 网络中的任何位置拨打。有两种类型的备用号码。您可以在本地群集中预配置备用号码，然后将每个号码通告到 ILS 网络，或配置用于汇总备用号码范围的通告号码模式，并将该模式通告到 ILS 网络。
- **通告的模式**—通告的模式汇总了企业备用号码或 +E.164 备用号码的范围。您可以在整个 ILS 网络中复制模式，而不是单独的备用号码，以便在远程群集中保存数据库空间。通告的模式仅从 ILS 网络中的远程群集使用—您无法将这些模式用于路由本地呼叫。
- **PSTN 故障转移号码**—此选项可让您将企业备用号码或 E.164 备用号码分配为 PSTN 故障转移号码。如果通过 VoIP 通道路由到全局拨号方案元素的呼叫失败，故障转移号码将提供备用路由方法。在远程群集中，您必须配置将 PSTN 故障转移路由到相应网关的路由模式。

- **路由字符串**—每个群集都有随全局拨号方案类目一起复制的路由字符串。路由字符串标识目录 URI 或备用号码的主群集。对于群集间呼叫，必须在每个远程群集中配置将路由字符串路由回其主群集的 SIP 路由模式。
- **学习的全局拨号方案数据**—要确保复制的数据达到 ILS 网络中的所有群集，每个群集都会复制其本地预配置的全局拨号方案数据以及从其他群集学习的类目。
- **导入的全局拨号方案数据**—如果您在互操作 Cisco Unified Communications Manager 与 Cisco TelePresence Video Communications 服务器或第三方呼叫控制系统，可将全局拨号方案从其他系统导出到一个 csv 文件，然后将该 csv 文件导入到 ILS 网络的中枢群集中。全局拨号方案复制会将导入的类目复制到 ILS 网络中的其他群集，从而让您向注册到其他系统的目录 URI 和备用号码拨打呼叫。

全局拨号方案映射示例

以下示例显示映射到电话分机 4001 的全局拨号方案数据元素示例。如果呼叫路由配置正确，则拨打任何这些号码都会振铃分机 4001。

- **企业备用号码**—应用至分机 4001 的 5XXXX 的数字掩码会创建企业备用号码 54001。
- **E164 备用号码**—应用至分机 4001 的 1972555XXXX 的号码掩码将创建 +E.164 备用号码 19725554001。
- **PSTN 故障转移**—将企业备用号码或 +E.164 备用号码作为 PSTN 故障转移分配，并将呼叫路由到相应的网关。
- **通告的模式**—模式 54XXX 可用于汇总 54000-54999 范围内的所有企业备用号码。您可以为企业和 +E.164 备用号码创建模式。
- **目录 URI**—alice@cisco.com



注释 目录 URI 可以分配至一个目录号码或一个最终用户。与最终用户关联的目录 URI 也将关联至用户的主分机（目录号码），并且会主分机上振铃（如果已分配）。

URI 拨号

URI 拨号是全局拨号方案复制的子功能，它允许主叫方使用目录 URI 作为拨号字符串来发出呼叫。目录 URI 是一个字母数字文本字符串，看起来像电子邮件地址（例如 alice@cisco.com）。

虽然 URI 类似于电子邮件地址，但目录 URI 本身并不是可路由的实体。对于本地呼叫，只要目录 URI 位于主叫方呼叫搜索空间内的分区中，就可以路由到目录 URI 的呼叫。对于群集间呼叫，系统将提取使用“全局拨号方案复制”复制的群集路由字符串，并尝试将 SIP 路由模式与路由字符串匹配。

目录 URI 类型

目录 URI 有两种类型，其类型取决于您预配置目录 URI 的方式：

- 基于用户的 URI—目录 URI 在**最终用户配置**中分配给用户。所有这些 URI 自动分配到本地目录 URI 分区，即本地不可删除的分区。如果用户也有主分机，则 URI 也会作为该分机的主 URI 出现在**目录号码配置**中。
- 基于线路的 URI—在**目录号码配置**窗口中最多可以直接为目录号码分配五个额外的目录 URI。对于这些 URI，您可以分配任何本地分区。

目录 URI 格式

目录 URI 是由用户名和主机地址组成的字母数字字符串，中间用 @ 符号分隔。

Cisco Unified Communications Manager 支持以下格式的目录 URI：

- user@domain（例如 joe@cisco.com）
- user@ip_address（例如 joe@10.10.10.1）

系统支持目录 URI 的用户部分（@ 符号之前的部分）采用以下格式：

- 接受的字符包括 a-z、A-Z、0-9、!、\$、%、&、*、_、+、~、-、=、?、‘、.、/、(和)。
- 用户部分最多可包含 47 个字符。
- 当目录 URI 保存于数据库中时，Cisco Unified Communications Manager 自动对以下字符应用百分号编码：
% ^ ` { } | \ : " < > [] \ ' 和空格。



注释

默认情况下，目录 URI 的用户部分区分大小写。您可以通过编辑 **URI 查找策略** 企业参数，将用户部分编辑为不区分大小写。

应用百分号编码时，目录 URI 的数字长度会增加。例如，如果输入 joe smith#@cisco.com（20 个字符）作为目录 URI，Unified Communications Manager 会将该目录 URI 以 joe%20smith%23@cisco.com（24 个字符）的形式存储在数据库中。由于数据库限制，**目录 URI** 字段最多只能包含 254 个字符。

Cisco Unified Communications Manager 支持目录 URI 的主机部分（@ 符号之后的部分）采用以下格式：

- 支持 IPv4 地址或全限定域名。
- 接受的字符有字母数字字符、连字符 (-) 和点号 (.)。
- 主机部分不能以连字符 (-) 开头或结尾。
- 主机部分一行中不能有两个点。
- 主机部分的最小长度为两个字符。

- 主机部分不区分大小写。



注释 在 **Cisco Unified Communications Manager** 管理中，使用批量管理导入包含内嵌有双引号和逗号的目录 URI 的 CSV 文件时，必须用双引号 (") 括住整个目录 URI。

呼叫前转到 URI

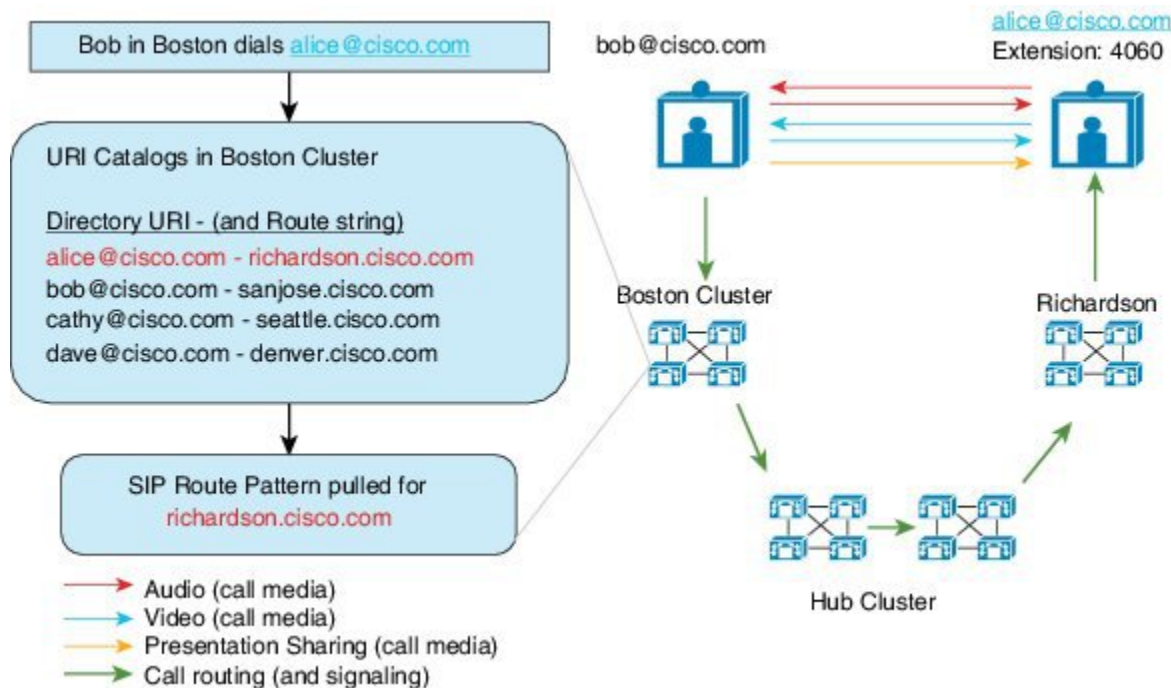
- 无法从实际电话呼叫前转到 URI。
- 呼叫前转到 URI 只能通过应用程序进行配置，前提是该 URI 已经在 Unified Communications Manager 数据库中。如果 URI 不在数据库中，则在尝试配置呼叫前转时，应用程序会将“呼叫前转设置失败 /n 无法前转呼叫到：新号码”计为错误。
- 可以通过“Unified Communications Manager 管理”页面为任何 URI 配置呼叫前转，无论 URI 是否存在于数据库中。
- 您可以在 **Cisco Unified Communications 自助门户 > 最终用户** 页上配置呼叫前转到任何 URI，无论其是否存在于数据库中。在输入 # % ^ ` { } | \ : ? < > [] \ ' 字符时，必须使用“百分号编码”。例如，**%3A** 用于表示 **:**，而 **%20** 用于表示空格。
- 如果您需要前转呼叫到 URI **"mobile: 12345@cisco.com"**，则必须在 **Cisco Unified Communications 自助门户 > 最终用户** 页的“呼叫前转”部分下提供 **"mobile%3A%2012345@cisco.com"**。

全局拨号方案复制呼叫路由

对于群集内呼叫，全局拨号方案数据通过分区和呼叫搜索空间进行路由。对于到本地目录 URI 的呼叫，使用企业备用号码或 E.164 备用号码，URI 或号码必须存在于主叫方使用的呼叫搜索空间的分区中。

群集间呼叫使用全局拨号方案复制通告的群集路由字符串将呼叫发送到被叫方的主群集。当主叫方将呼叫放入另一个群集中的目录 URI 或备用号码时，系统会提取关联的路由字符串，匹配路由字符串的 SIP 路由模式，然后将呼叫发送到 SIP 路由模式指定的目标。为使此功能正常工作，您必须在远程群集中配置 SIP 路由模式，以将路由字符串路由回其主群集。

如果呼叫路由失败，系统也可以使用关联的 PSTN 故障转移号码。不过，您需要在远程群集中配置路由模式，以便 PSTN 故障转移呼叫可以发送到适当的网关。



38/40/49

全局拨号方案复制前提条件

您必须：

- 配置 Cisco 群集间查询服务 (ILS)
- 计划您打算如何部署全局拨号方案：
 - 是否要通过为您的用户预配置目录 URI 来部署 URI 拨号？您可以使用全局拨号方案复制在 ILS 网络中复制目录 URI。
 - 是否要部署备用号码拨号？是否要使用企业备用号码或 E.164 备用号码？您将使用哪个作为 PSTN 故障转移？
 - 如果要部署备用号码，请计划编号方案。对于大型网络，您可以通过将号码模式通告到 ILS 网络而不是单独的备用号码来节省数据库空间和带宽。

全局拨号方案复制配置任务流程

完成这些任务以配置全局拨号方案复制和 URI 拨号。您必须在 ILS 网络的每个群集中完成这些任务。

过程

	命令或操作	目的
步骤 1	启用 ILS 对全局拨号方案复制的支持，第 224 页	在本地群集中启用对全局拨号方案复制的支持。
步骤 2	配置 SIP 配置文件，第 225 页	配置支持全局拨号方案复制和 URI 拨号的 SIP 设置。
步骤 3	为 URI 拨号配置 SIP 干线，第 225 页	对于 URI 拨号，配置系统是在联系人标头中插入了目录 URI、目录号码还是混合地址。
步骤 4	配置 SIP 路由模式，第 226 页	对于群集间路由，在将学习路由由字符串路由回其主群集的每个群集中配置 SIP 路由模式。
步骤 5	设置对学习的数据的数据库限制，第 227 页	设置 ILS 可写入本地数据库的数据量上限。
步骤 6	分配学习号码和模式的分区，第 227 页	为企业备用号码、+E.164 备用号码和学习号码模式分配路由分区。
步骤 7	为备用号码设置通告的模式，第 228 页	可选。通告一个概括企业或 +E.164 备用号码范围的号码模式。
步骤 8	阻止学习模式，第 229 页	可选。配置阻止呼叫到特定号码或号码模式的模式。此配置将在本地应用，不会复制到 ILS 网络。
步骤 9	导入全局拨号方案数据，第 230 页	可选。如果要与 Cisco TelePresence Video Communications Server 或第三方呼叫控制系统进行互操作，则将目录 URI 的类目、+E.164 号码和 PSTN 故障转移号码从其他系统导入到 ILS 网络的中枢群集中。
步骤 10	预配置全局拨号方案数据，第 229 页	<p>将目录 URI、企业备用号码和 +E.164 备用号码分配到目录号码。</p> <p>注释 对于多个用户，使用 LDAP 目录同步或批量管理为一项操作中的大量用户分配全局拨号方案数据。请参阅本指南的“预配置用户”部分。</p>

启用 ILS 对全局拨号方案复制的支持

在本地群集中启用 ILS 对全局拨号方案复制的支持，请执行此程序：

过程

- 步骤 1 登录 Cisco Unified Communications Manager 发布方节点。
- 步骤 2 从 Cisco Unified CM 管理中，选择高级功能 > **ILS 配置**。
- 步骤 3 选中与远程群集交换全局拨号方案复制数据复选框。
- 步骤 4 在通告的路由字符串文本框中，为本地群集分配一个路由字符串。
- 步骤 5 单击保存。

配置 SIP 配置文件

此程序用于编辑网络中的 SIP 配置文件，以支持全局拨号方案复制和 URI 拨号。

过程

- 步骤 1 在 Cisco Unified CM 管理中，选择设备 > 设备设置 > **SIP 配置文件**。
- 步骤 2 单击查找并选择现有的 SIP 配置文件。
- 步骤 3 从拨号字符串解析下拉列表中，配置系统用于确定将呼叫路由为目录 URI 还是目录号码的策略：
 - 始终将所有拨号字符串处理为 URI 地址
 - 电话号码包含字符 0-9、A-D、* 和 + (其他字符被处理为 URI 地址)。
 - 电话号码包含字符 0-9、* 和 + (其他字符被处理为 URI 地址)—这是默认选项。
- 步骤 4 选中在 SIP 请求中使用完全限定的域名复选框。
- 步骤 5 可选。在干线特定配置下，如果想要能够跨 Cisco Unified Border Element 路由群集间呼叫，请选中发送 ILS 学习目标路由字符串复选框。
- 步骤 6 单击保存。

为 URI 拨号配置 SIP 干线

如果要部署 URI 拨号，请为网络中的 SIP 干线配置联系人标头寻址策略。Cisco Unified Communications Manager 可以在传出 SIP 消息的 SIP 标头中插入目录号码、目录 URI 或包含目录号码和目录 URI 的混合地址。

过程

- 步骤 1 从 Cisco Unified CM 管理中，选择设备 > 干线。
- 步骤 2 单击查找并选择现有的 SIP 干线。
- 步骤 3 在出站呼叫区域中，从呼叫和连接方信息格式下拉列表中选择以下选项之一：

- 在连接方仅提供 **DN**—在传出 SIP 消息中，Unified Communications Manager 在 SIP 联系标头信息中插入主叫方的目录号码。这是默认设置。
- 在连接方仅提供 **URI**（如果可用）—在传出 SIP 消息中，Unified Communications Manager 在 SIP 联系标头中插入发送方的目录 URI。如果目录 URI 不可用，Unified Communications Manager 则会插入目录号码。
- 在连接方提供 **URI** 和 **DN**（如果可用）—在传出 SIP 消息中，Unified Communications Manager 在 SIP 联系标头中插入包含主叫方目录 URI 和目录号码的混合地址。如果目录 URI 不可用，Unified Communications Manager 只插入目录号码。

步骤 4 单击保存。

配置 SIP 路由模式

对于全局拨号方案复制和 URI 拨号的群集间呼叫路由，您必须配置将学习的路由字符串路由回它们的主群集的 SIP 路由模式。

过程

步骤 1 从 Cisco Unified CM 管理中，选择呼叫路由 > **SIP 路由模式**。

步骤 2 单击新增。

步骤 3 从模式使用下拉列表中，选择域路由。

步骤 4 根据您是部署 IPv4 还是 IPv6，在 **IPv4 地址**或 **IPv6 地址**文本框中输入路由字符串。

步骤 5 在 **SIP 干线/路由列表**下，选择指向下一跳群集的 SIP 干线或路由列表，以路由回路字符串的主群集。

步骤 6 完成 **SIP 路由模式配置**窗口中其余字段的设置。有关字段及其配置选项的更多信息，请参阅系统联机帮助。

步骤 7 单击保存。

步骤 8 为每个学习的路由字符串创建 SIP 路由模式。

步骤 9 对 ILS 网络中的每个群集重复上述步骤。



注释 如果 SIP 路由模式名称包含破折号，则必须确保在破折号之间没有数字。不过，如果有多条破折号，则使用字母和数字的组合或仅字母。下面列出了正确和错误 SIP 路由模式的示例：

正确的模式：

- abc-1d-efg.xyz.com
- 123-abc-456.xyz.com

不正确的模式：

- abc-123-def.xyz.com
- 1bc-2-3ef.xyz.com

设置对学习的数据的数据库限制

设置数据库限制，以确定 Unified Communications Manager 可以写入本地数据库的学习对象的数量。

过程

步骤 1 从 Cisco Unified CM 管理中，选择系统 > 服务参数。

步骤 2 选择要在其中配置参数的服务器。

步骤 3 从服务下拉列表中，选择 **Cisco 群集间查询服务（活动）**。如果服务没有显示为活动，请确保在 Cisco Unified 功能配置中激活该服务。

步骤 4 在群集范围参数 (ILS) 部分下，设置数据库中的 **ILS 最大学习对象数** 服务参数的上限。

步骤 5 单击保存。



注释 此服务参数确定 Unified Communications Manager 可以为通过 ILS 学习的数据写入到数据库的最大条目数。该服务参数的默认值为 100,000，最大值为 1,000,000

如果您将该服务参数减小到一个值，而该值小于数据库中保存的 ILS 学习条目的当前数量，Unified Communications Manager 就无法将更多 ILS 学习对象写入到数据库。不过，当前数据库条目仍保留。

分配学习号码和模式的分区

您必须分配学习号码和学习模式给分区。您可以定义自己的分区，也可以使用预定义的默认分区。Unified Communications Manager 已安装了以下预定义的学习备用号码和号码模式分区：

- 全局学习企业号码。

- 全局学习 E.164 号码。
- 全局学习企业模式。
- 全局学习 E.164 模式。



注释 您不能分配学习号码或学习模式给空分区。

过程

步骤 1 从 Cisco Unified CM 管理中，选择呼叫路由 > 全局拨号方案复制 > 学习号码和模式的分区。

步骤 2 配置学习号码和模式的分区窗口中的字段。有关字段及其配置选项的更多信息，请参阅系统联机帮助。

步骤 3 单击保存。

注释 路由分区还必须存在于主叫方使用的呼叫搜索空间中，以便要拨打的呼叫号码在分区中。

为备用号码设置通告的模式

使用通告的模式汇总企业备用号码或 E.164 备用号码的范围。您可以向 ILS 网络通告该模式，以使群集间呼叫与该模式匹配的号码。

过程

步骤 1 从 Cisco Unified CM 管理中，选择呼叫路由 > 全局拨号方案复制 > 通告的模式。

步骤 2 从查找并列出通告的模式窗口中，执行以下任一操作：

- 单击**查找**并选择现有模式。
- 单击**新增**以创建新的模式。

步骤 3 在模式字段中，输入号码模式。例如，54XXX 会汇总 54000 - 54999 之间的数字范围。

步骤 4 在模式类型字段中，选择模式类型：**企业号码模式**或**E.164 号码模式**。

步骤 5 从单选按钮中，选择是否要应用 PSTN 故障转移。

- 不使用 **PSTN 故障转移**
- 使用模式作为 **PSTN 故障转移**
- 应用剥离数字和预挂起数字到模式并用于 **PSTN 故障转移**—如果选择此选项，请在 "**PSTN 故障转移剥离数字和PSTN 故障转移前置数字**" 字段中输入数字。

步骤 6 单击保存。

阻止学习模式

如果您要设置阻止规则以阻止本地群集将呼叫路由到特定的企业备用号码、+E.164 备用号码或通过 ILS 学习的号码模式，请完成此可选任务。

在将呼叫路由至学习号码或学习模式之前，ILS 会检查本地阻止规则是否与拨号字符串匹配。如果阻止规则匹配，Unified Communications Manager 不路由呼叫。

过程

步骤 1 从 Cisco Unified CM 管理中，选择呼叫路由 > 全局包好方案复制 > 阻止学习号码和模式。

步骤 2 请执行以下任务之一：

- 单击**查找**并选择要编辑的现有阻止规则。
- 单击**新增**以创建新的阻止规则。

步骤 3 在**模式**字段中，输入要阻止的模式或号码。例如，206XXXXXXX 可用于阻止呼叫 2065551212。

步骤 4 如果想要基于拨号字符串前缀阻止呼叫，请输入**前缀**。

步骤 5 如果您想阻止呼叫被发送至特定群集，请输入群集的**群集 ID**。

步骤 6 从**模式类型**下拉列表中，选择要应用阻止规则的方式：

- **任何**—如果对企业号码模式和 +E.164 模式都应用阻止规则，请选择此选项。
- **企业模式**—如果只对企业号码模式应用阻止规则，请选择此选项。
- **+E.164 模式**—如果只对 +E.164 号码模式应用阻止规则，请选择此选项。

步骤 7 单击保存。

预配置全局拨号方案数据

使用此程序将目录 URI、企业备用号码、+E.164 备用号码和 PSTN 故障转移规则添加到目录号码。



注释

如果您有大量的用户，请配置通用线路模板，并将其应用于预配置工具（例如 LDAP 同步或批量管理），以便在一次操作中为大量用户预配置全局拨号方案数据。请参阅本书的“预配置用户”部分。

过程

步骤 1 从 Cisco Unified CM 管理中，选择呼叫路由 > 目录号码。

步骤 2 执行以下任一操作：

- 单击**查找**并选择要为其添加全局拨号方案数据的现有目录号码。
- 单击**新增**以创建新的目录号码。

步骤 3 如果要创建新号码，请输入目录号码，然后单击**保存**。

步骤 4 要添加企业备用号码，请单击**添加企业备用号码**按钮并执行以下操作：

- a) 输入**号码掩码**。例如，5XXXX 作为 4001 的备用号码。生成的企业备用号码(54001)会显示在**备用号码**字段中。
- b) 选中**添加到本地路由分区**复选框以添加至本地路由分区。
- c) 从路由分区下拉列表中，选择分区。
- d) 如果要将此备用号码通告到 ILS 网络，请选中**通过 ILS 全局通告**。

注释 如果配置了通告模式，当企业备用号码或 +E.164 备用号码就在模式范围内时，则无需单独通告备用号码。

步骤 5 要添加 +E.164 备用号码，请单击**添加 +E.164 备用号码**，然后执行以下操作：

- a) 输入**号码掩码**。例如，1972555XXXX 作为分机 4001 的备用号码。生成的 +E.164 备用号码(19725554001)会显示在**备用号码**字段中。
- b) 选中**添加到本地路由分区**复选框以添加至本地路由分区。
- c) 从路由分区下拉列表中，选择分区。
- d) 如果要将此备用号码通告到 ILS 网络，请选中**通过 ILS 全局通告**。

步骤 6 在目录 **URI** 部分中，添加目录 URI 到此目录号码：

- a) 在 **URI** 字段中，输入目录 URI。例如，alice@cisco.com。
- b) 从分区下拉列表中，将目录 URI 分配到本地分区。
- c) 选中**通过 ILS 全局通告**复选框以在通告的类目中包含此目录 URI。
- d) 单击**添加行**以添加其他目录 URI。您最多可以添加五个目录 URI。

步骤 7 在通告的**故障转移号码**字段中，选择企业备用号码或 +E.164 备用号码作为 PSTN 故障转移。

步骤 8 完成**目录号码配置**窗口中其余字段的设置。有关字段及其配置选项的更多信息，请参阅系统联机帮助。

步骤 9 单击**保存**。

导入全局拨号方案数据

如果要与 Cisco TelePresence Video Communications Server、第三方呼叫控制系统或未运行 ILS 的另一系统进行互操作，请使用此程序。您可以将目录 URI 的类目、+E.164 模式和 PSTN 故障转移规则从其他系统导入到 ILS 网络中的中枢群集中。ILS 在整个 ILS 网络中复制类目，以便群集可以呼叫其他系统。

开始之前

将您的拨号方案类目从其他系统导出到一个 CSV 文件。

过程

步骤 1 从 Cisco Unified CM 管理中，选择呼叫路由 > 全局拨号方案复制 > 导入的全局拨号方案类目。

步骤 2 在查找并列出的导入的全局拨号方案类目窗口中，执行以下任务之一：

- 单击**查找**并从结果列表选择现有类目。
- 单击**新增**以添加新类目。

步骤 3 从导入的全局拨号方案类目设置窗口中，在名称字段中输入唯一的名称以标识您要导入的类目。

步骤 4 （可选）在说明字段中，输入类目的说明。

步骤 5 在路由字符串字段中，为您要从其中导入类目的系统创建一个路由字符串。

注释 路由字符串最多可以包含 250 个字母数字字符，可以包含点号和连字符。

步骤 6 单击**保存**。

步骤 7 在 Cisco Unified CM 管理中，选择批量管理 > 上传/下载文件。

- 单击**新增**。
- 单击**浏览**并选择您要导入的类目的 CSV 文件。

注释 确保您用于导入的 CSV 文件兼容 Cisco Unified Communications Manager 的版本。例如，某个 CSV 文件与版本 9.0(1) 兼容，可以导入，但与版本 10.0(1) 不兼容。

步骤 8 在选择目标下拉列表中，选择导入的目录 **URI** 和模式。

步骤 9 在选择事务类型下拉列表中，选择插入导入的目录 **URI** 和模式。

步骤 10 单击**保存**。

步骤 11 从 Cisco Unified CM 管理中，选择批量管理 > 目录 **URI** 和模式 > 插入导入的目录 **URI** 和模式。

步骤 12 在文件名下拉列表中，选择包含您要导入的类目的 CSV 文件。

步骤 13 在已导入目录 **URI** 类目下拉列表中，选择您在导入的全局拨号方案类目窗口中指定的类目。

步骤 14 在作业说明文本框中，输入您要运行的作业的名称。

步骤 15 请执行以下步骤之一：

- 如果要立即运行该作业，请选择**立即运行**选项，然后单击**提交**。
- 如果要计划作业在指定时间运行，请选择**稍后运行**单选按键，然后单击**提交**。

注释 如果选择**稍后运行**选项，您必须使用批量管理作业计划程序计划何时运行作业。

Cisco Unified Communications Manager 将所有导入的 +E.164 模式保存到学习的全局 +E.164 模式分区。



注释 您还可以将所有本地配置的目录 URI、+E.164 号码模式及其关联的 PSTN 故障转移规则导出到可导入至其他呼叫控制系统的 CSV 文件。请参阅**批量管理 > 目录 URI 和模式 > 导出本地目录 URI 和模式**下的菜单了解详细信息。

全局拨号方案复制相互作用和限制

下表汇总了全局拨号方案复制和 URI 拨号的一些功能相互作用。

功能	交互和限制
导出目录 URI 和 +E.164 模式	<p>您还可以导出本地群集中配置的所有目录 URI 和 +E.164 号码模式，然后将其导出为可以导入到其他系统的 csv 文件。</p> <ol style="list-style-type: none">在 Cisco Unified CM 管理中，选择批量管理 > 目录 URI 和模式 > 导出本地目录 URI 和模式。单击以下其中一个单选按钮以定义要附加到导出文件的域名：<ul style="list-style-type: none">组织顶级域—单击此单选按钮以将组织顶级域企业参数的值用于导出文件域名。路由字符串域—单击此单选按钮以将“路由字符串”字段的值（在“ILS 配置”中配置）用于导出文件域名。用户定义的域—单击此单选按钮以创建要附加到导出文件的自定义域名。如果您选择了此选项，请在域名文本框中输入域名。单击导出本地目录 URI 和模式按钮。将 CSV 文件保存到本地驱动器

功能	交互和限制
使用 URI 拨号分区	<p>使用目录 URI 分区取决于您如何预配置目录 URI。</p> <ul style="list-style-type: none"> 对于在最终用户配置中分配给最终用户的、基于用户的目录 URI，会自动将本地不可删除的目录 URI 分区分配给 URI。您不能分配其他分区，但可以通过配置目录 URI 别名分区企业参数，将管理员管理的分区用作本地目录 URI 分区的别名。 对于将 URI 直接分配到目录号码配置中目录号码的基于线路的目录 URI，您可以单独分配每个 URI 到本地分区。 <p>如果您使用 LDAP 同步和批量管理等工具配置目录 URI：</p> <ul style="list-style-type: none"> 通过 LDAP 同步预配置的目录 URI 基于用户，并在最终用户配置中分配给用户。这些 URI 将分配给本地目录 URI 分区。如果用户也有主分机，则 URI 也会作为主 URI 出现在目录号码配置中。不过，分配的分区是目录 URI 分区。 对于通过批量管理预配置的目录 URI，它取决于您如何应用更新。例如，如果使用 bat.xlt 电子表格创建 csv 导入文件，则用户将是基于用户的 URI（如果您使用电子表格上的用户或更新用户选项卡添加目录 URI）。但是，如果您通过单击创建文件格式时显示的线路字段选项添加目录 URI，则可以将 URI 分配到目录号码，然后将本地分区直接分配给 URI。
目录 URI 区分大小写	默认情况下，目录 URI 的用户部分（@ 前面的部分）区分大小写。您可以通过编辑 URI 查找策略企业参数，使用户部分不区分大小写。
呼叫搜索空间	要可拨叫，目录 URI、企业备用号码和 +E.164 备用号码必须位于主叫方呼叫搜索空间中可用的分区中。
使用 URI 拨号的数字转换	<p>如果您使用数字转换，并且要部署群集间 URI 拨号，则针对电话配置或电话使用的设备池应用数字转换。</p> <ul style="list-style-type: none"> 对于个别电话，将转换应用到远程号码部分中的主叫方转换 CSS字段。 对于设备池，您可以根据设备移动相关信息下的主叫方转换 CSS字段应用转换。 <p>注释 对于漫游设备，设备池设置优先于电话配置，即使电话配置窗口中取消选中使用设备池主叫方转换 CSS复选框亦是如此。</p>



第 24 章

主叫方标准化

- [主叫方标准化概述，第 235 页](#)
- [主叫方标准化前提条件，第 236 页](#)
- [主叫方标准化配置任务流程，第 236 页](#)
- [主叫方标准化相互作用和限制，第 240 页](#)

主叫方标准化概述

主叫方标准化允许您全球化和本地化电话号码，以便在电话上显示相应的主叫代码。主叫方标准化可增强一些电话的拨号功能，并在呼叫路由到多个地理位置时改进回呼功能。此功能使您可以将全球主叫方号码映射到其本地化的变体，以便电话可以在不修改电话呼叫日志目录中的目录号码的情况下返回呼叫。

主叫方号码的全球化

通过在 Cisco Unified CM 管理中配置主叫方号码类型和前缀，您可以将 Cisco Unified Communications Manager 设置为将在被叫电话上显示的主叫方号码重新格式化为全球化的版本（包括国际国家/地区代码等前缀），从而允许从世界任何地方拨打号码。

Cisco Unified Communications Manager 使用不同的号码模式（例如路由模式或转换模式）以及主叫方号码类型的值来进行电话号码全球化。例如，您可以配置 Cisco Unified Communications Manager 来获取具有订户主叫方号码类型的本地化德国电话号码 069XXXXXXX，并将其全球化为 +49 40 69XXXXXXX，其中包括德国国家代码和城市代码。

对于路由到多个地理位置的呼叫，为每个路由路径应用的不同转换设置可以为每个呼叫路径进行唯一的主叫方号码全球化。还可以配置 Cisco Unified Communications Manager，以使电话在电话屏幕上显示本地化的主叫方号码，并在电话的呼叫日志目录中显示全球化的号码。要确保电话用户在发出呼叫之前无需编辑电话上的呼叫日志目录条目，请将全局主叫方号码映射到其本地变体。

主叫方号码的本地化

对于主叫方号码的最终显示，您可以为每个主叫方号码类型（国内、国际、订户和未知）配置主叫方转换模式，并对该呼叫的主叫方号码类型应用剥离数字和前缀说明。这将允许 Cisco Unified

Communications Manager 重新格式化主叫方号码，以便在被叫电话上显示的主叫方号码是不包含不必要国家代码和国际接入码的本地化号码。

例如，假设来自 PSTN 的来电的全球号码为 +49 40 69XXXXXXX，其中 +49 代表国家/地区代码，40 代表城市代码，则主叫方号码类型为“订户”。可以使用主叫方转换模式以及剥离国家/地区代码、城市代码和添加前缀 0 的说明配置 Cisco Unified Communications Manager。应用说明后，主叫方号码在被叫电话中显示为 069XXXXXXX。

将全球化的主叫方号码映射到本地化版本

为确保电话用户无需编辑电话上的呼叫日志目录条目即可拨出呼叫，请使用路由模式和被叫方转换模式将全局主叫方号码映射到本地化版本。这可确保被叫方返回呼叫时，Cisco Unified Communications Manager 可以将呼叫路由到正确的网关。

映射全局主叫方号码可改进回呼功能，以便被叫方可以返回呼叫，而无需修改电话上呼叫日志目录中的目录号码。

主叫方标准化前提条件

确保先激活 Cisco Unified 功能配置中的 **Cisco CallManager** 服务，然后再配置主叫方标准化。有关详细信息，请参阅《Cisco Unified 功能配置管理指南》。

如果想要 Cisco Unified Communications Manager 确定主叫方号码类型，请配置模式来分配与您预期的呼叫匹配的主叫方号码类型值。您可以在以下配置窗口中创建和应用模式：

- 路由模式
- 寻线引导
- 转换模式
- 主叫方号码转换模式



注释 主叫方转换仅适用于原始主叫方。对重定向号码进行的任何修改都只影响转移标头。从 "SIP 干线" 一章查看您的配置，并在 SIP 干线上添加转移标头。

主叫方标准化配置任务流程

主叫方标准化前缀和剥离数字规则可在 Unified Communications Manager 中以各种方式应用。例如，您可以对设备池、路由模式、转换模式、寻线引导、网关和干线应用数字转换。应用数字转换的模式取决于您部署拨号方案、设备和干线的方式。有关详细信息，请查看与拨号方案、路由模式、转换模式和转型模式相关的主题。

过程

	命令或操作	目的
步骤 1	如果想要 Unified Communications Manager 确定主叫方号码类型，请创建一个模式并配置与您预期的呼叫匹配的主叫方号码类型。您可以在以下配置窗口中创建和应用模式： <ul style="list-style-type: none"> • 路由模式 • 寻线引导 • 转换模式 • 主叫方号码转换模式 	
步骤 2	全球化主叫方号码，第 237 页	对于通过 PSTN 到达的传入呼叫，配置将全球化主叫方号码的设置。
步骤 3	设置呼叫搜索空间，第 238 页	设置分区和呼叫搜索空间。
步骤 4	创建主叫方转换模式，第 238 页	创建将主叫方号码转换为全球化或本地化版本的主叫方转换模式，并将每个模式分配给分区。
步骤 5	将主叫方转换模式应用到呼叫搜索空间，第 239 页	将来电主叫方转换 CSS 应用到设备，例如设备池、网关和干线

全球化主叫方号码

对于通过 PSTN 收到的来电，配置将全球化主叫方号码的设置。您可以应用将全球化主叫方号码的设置，并将其应用到设备池或个别设备。或者，您也可以配置将在群集范围基础上应用主叫方标准化设置的服务参数。

要全球化主叫方号码，请执行以下步骤：

过程

步骤 1 如果要将主叫方标准化设置应用到特定设备，请执行以下步骤：

- 打开要在其中应用设置的设备的配置窗口。例如，设备池、网关、电话和干线。
- 在配置窗口的“来电主叫方设置”部分中，对每个主叫方号码类型应用前缀和剥离数字指令。

注释 Cisco Unified Communications Manager 将包含主叫方号码字段中的前缀用于所有其他操作，例如包括呼叫前转、呼叫暂留、语音留言、CDR 数据等等与呼叫有关的补充服务。

步骤 2 如果要使用服务参数来全球化所有设备群集范围上的主叫方号码，请执行以下步骤：

- 从 Cisco Unified CM 管理中，选择 **系统 > 服务参数**。
- 从 **服务器** 下拉列表中，选择要在其上运行该服务的服务器。

- c) 从**服务**下拉列表中，选择 Cisco CallManager。
- d) 单击**高级**。
- e) 配置以下参数的值，它们可在群集范围基础上应用到电话、MGCP 网关或 H.323 网关：

- 来电主叫方国内号码前缀
- 来电主叫方国际号码前缀
- 来电主叫方未知号码前缀
- 来电主叫方用户号码前缀

注释 为使 Cisco Unified Communications Manager 在特定电话上应用群集范围服务参数设置，该电话的前缀设置必须在设备和设备池级别上设置为默认选项。

设置呼叫搜索空间

如果您要设置呼叫搜索空间来处理主叫方标准化功能，请使用此过程。

过程

- 步骤 1** 在 Cisco Unified CM 管理中，选择**呼叫路由 > 控制级 > 分区**。
- 步骤 2** 为您的网络创建分区。
- 步骤 3** 在 Cisco Unified CM 管理中，选择**呼叫路由 > 控制级 > 呼叫搜索空间**。
- 步骤 4** 为您的主叫方转换模式创建呼叫搜索空间。
- 步骤 5** 对每个呼叫搜索空间，分配分区到呼叫搜索空间

创建主叫方转换模式

如果您要设置主叫方转换模式来处理主叫方标准化功能，请使用此程序。

过程

- 步骤 1** 在 Cisco Unified CM 管理中，选择**呼叫路由 > 转换模式 > 主叫方转换模式**。
- 步骤 2** 创建转换模式。
- 步骤 3** 对于您创建的每个主叫方转换模式，分配要全球化或本地化主叫方号码的前缀或剥离数字命令。
- 步骤 4** 对于每个主叫方转换模式，分配与您的一个呼叫搜索空间关联的分区。

将主叫方转换模式应用到呼叫搜索空间

对于您的设备，将来电主叫方转换 CSS 分配到设备，例如设备池、网关和干线。

过程

- 步骤 1**
在 Cisco Unified CM 管理中，选择适用于您要应用主叫方转换的设备的配置窗口。
 - 网关
 - 干线
 - 设备池
- 步骤 2**
要本地化主叫方号码，在“呼叫搜索空间”下拉列表框中，选择包含要应用到的主叫方转换模式的 CSS。

注释
 如果根据设备池配置 CSS，您还必须将该设备池应用到您的电话。
- 步骤 3**
要全球化主叫方号码，请在“来电主叫方设置”部分中，选择包含要应用的主叫方转换模式的呼叫搜索空间。

主叫方标准化服务参数示例

以下服务参数可在群集范围基础上应用到电话、MGCP 网关或 H.323 网关。为使特定设备使用群集范围参数，设备配置中的前缀必须设置为 Default.:

- 来电主叫方国内号码前缀
- 来电主叫方国际号码前缀
- 来电主叫方未知号码前缀
- 来电主叫方用户号码前缀

下表提供前缀和剥离数字配置的示例，以及如何使用这些值来转换主叫方号码的显示。对于服务参数配置，冒号后面的数字表示从主叫方号码开头要剥离的位数，而冒号后面的数字表示添加到主叫方号码开头的前缀。

表 24: 主叫方号码标准化服务参数示例

原主叫号码	服务参数值	说明	最终主叫号码
04423452345	+:1	剥离第一个数字，然后添加前缀 +	+4423452345
04423452345	:2	剥离前两位数字	423452345
552345	+1:6	剥离前 6 位数字，然后添加前缀 +1	+1

原主叫号码	服务参数值	说明	最终主叫号码
552345	+1:8	最终号码为空，因为要剥离的位数比可用位数多	
552345	123	添加前缀 123	123552345
空白	+1:2	如果主叫号码为空，则不应用前缀	空白
0442345	:26	主叫方标准化只允许剥离 24 位数字	Cisco Unified Communications Manager 不允许此配置

主叫方标准化相互作用和限制

主叫方标准化相互作用

下表描述了与主叫方标准化功能的功能交互。

功能	互动
已转接的呼叫	<p>在某些转接的呼叫方案中，可能不支持主叫方标准化，因为转接功能依赖于通话中更新，并且主叫方标准化发生在每个呼叫跃点的初始呼叫建立期间。下面是如何使用主叫方标准化来进行转接的一个示例。</p> <p>号码为 972 500 2345、分机为 12345 的电话 A 呼叫号码为 972 500 4321、分机为 54321 的电话 B。电话 B 上会显示主叫方号码 12345，但是电话 B 通过 San Jose 网关将呼叫转接到电话 C。在初始转接期间，电话 C 显示主叫方号码 972 500 4321，但是在转接完成之后，电话 C 会将电话 A 的主叫方号码显示为 12345。</p>
前转的呼叫	<p>前转的呼叫支持主叫方号码全球化和本地化。例如，使用电话 F 的主叫方通过 PSTN 呼叫位于达拉斯的电话 G，但电话 G 将呼叫前转到圣何塞的电话 H。在传入的达拉斯网关上，主叫方号码显示为 555-5555/订约方，但呼叫会前转到圣何塞网关。来自达拉斯的去电显示为 972 555 5555。在传入的圣何塞网关上，+1 将加上前缀，电话 F 显示主叫号码 +1 972 555 5555。</p>
呼叫详细记录	<p>有关主叫方标准化如何处理呼叫详细记录(CDR)的信息，请参阅《Cisco Unified Communications Manager 呼叫详细记录管理指南》。</p>

功能	互动
Cisco Unified Communications Manager Assistant	<p>如果您配置了主叫方标准化功能，则 Cisco Unified Communications Manager Assistant 自动支持本地化和全球化的呼叫。Cisco Unified Communications Manager Assistant 可在用户界面上显示本地化的主叫方号码。此外，对于拨至经理的来电，Cisco Unified Communications Manager Assistant 可以在进行过滤模式匹配时显示本地化和全球化的主叫方号码。有关 Cisco Unified Communications Manager Assistant 的配置信息，请参阅《Cisco Unified Communications Manager 功能配置指南》，位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html。</p>
Cisco Unity Connection	<p>Cisco Unity Connection 不支持国际转义符 (+)。因此，您必须确保对 Cisco Unity Connection 的呼叫不包含 +，从而确保语音留言功能按照预期方式运作。</p> <p>为使 Cisco Unity Connection 按预期方式运作，请将此应用程序视为设备，并且配置主叫方转换，确保+不会发送到此语音留言应用程序。如果 Cisco Unity Connection 服务器使用北美的拨号方案，则在 Cisco Unity Connection 接收主叫方号码之前，将主叫方号码本地化为 NANP 格式。由于 Cisco Unified Communications Manager 管理中不存在用于语音留言端口的主叫方转换选项，因此请确保在与语音留言端口关联的设备池中配置主叫方号码转换。要本地化主叫方号码，还要考虑加上接入码前缀，以便语音留言应用程序可以轻松重拨特定功能（例如即时回复）的号码。例如，您可以将 +12225551234 转换为 912225551234，并且可以将国际号码 +4423453456 转换为包含国际转义码 90114423453456。</p>
设备移动	<p>漫游设备池的主叫方转换 CSS 将覆盖同一设备移动组中漫游电话的设备级配置，即使在电话配置窗口中未勾选“使用设备池主叫方转换 CSS”复选框。</p> <p>以下示例说明了主叫方标准化如何与设备移动功能配合用于主地点在达拉斯、当前在圣何塞漫游的电话。</p> <p>当电话在圣何塞漫游时，呼叫通过 PSTN 从达拉斯的 972 500 1212 <National> 发出。在圣何塞接收网关中，主叫方号码转换为全局格式 +1 408 500 1212。在目前位于圣何塞的电话上，主叫方号码显示为 1 972 500 1212。</p> <p>当电话在圣何塞漫游时，呼叫将通过 PSTN 从圣何塞的七位数拨号区域中的 500 1212 <Subscriber> 发出。在圣何塞接收网关中，主叫方号码转换为全局格式 +1 408 500 1212。在目前位于圣何塞的电话上，主叫方号码显示为 9 500 1212。</p>

主叫方标准化限制

下表显示了主叫方标准化功能对 Cisco Unified Communications Manager 的某些功能和系统组件的限制。

表 25: 对主叫方标准化的限制

功能	限制
共享线路	对共享线路显示的主叫方号码取决于 Cisco Unified Communications Manager 中呼叫控制事件的顺序。要避免在共享线路上显示不正确的本地化主叫方号码（特别是当共享线路在不同地理位置出现时），请确保为共享相同线路的不同设备配置相同的主叫方转换 CSS。
SIP 干线和 MGCP 网关	SIP 干线和 MGCP 网关可以支持发送呼叫的国际转义符 (+)。H.323 网关不支持 +。QSIG 干线不会尝试发送 +。对于通过支持 + 的网关的去电，Cisco Unified Communications Manager 可以发送 + 及拨号数字到网关。对于通过不支持 + 的网关的去电，国际转义符 + 在 Cisco Unified Communications Manager 发送呼叫信息到网关时剥离。
SIP	SIP 不支持号码类型，因此通过 SIP 干线的呼叫仅支持主叫方号码类型未知的传入号码设置。
QSIG	QSIG 配置通常支持统一拨号方案。如果您使用 QSIG，数字和前缀转换可能会导致功能相互作用问题。
主叫方转换 CSS	要本地化主叫方号码，设备必须使用数字分析应用转换。如果将“主叫方转换 CSS”配置为无，则转换不匹配，因此不会应用。确保在不用于路由的非空分区中配置主叫方转换模式。
T1 CAS 和 FXO 端口	“主叫方转换 CSS”设置不适用于网关上的 T1-CAS 和 FXO 端口。
Cisco Unity Connection	CiscoUnity Connection 不支持国际转义符 (+)。因此，您必须确保对 CiscoUnity Connection 的呼叫不包含 +，从而确保语音留言功能按照预期方式运作。 有关 Cisco Unity Connection 的详细信息，请转至 http://www.cisco.com/c/en/us/products/unified-communications/unity-connection/index.html 。



第 25 章

配置拨号规则

- [拨号规则概述，第 243 页](#)
- [拨号规则前提条件，第 243 页](#)
- [拨号规则配置任务流程，第 244 页](#)
- [拨号规则相互作用和限制，第 249 页](#)

拨号规则概述

Unified CM 支持以下类型的拨号规则：

- **应用程序拨号规则：** 管理员使用应用程序拨号规则以添加和排序应用程序（例如 Cisco Web Dialer 和 Cisco Unified Communications Manager Assistant）的拨号规则的优先级。
- **目录查找拨号规则：** 管理员使用目录查找拨号规则转换主叫方识别号码，并从 Cisco Unified Communications Manager Assistant 等应用程序中的 Assistant Console 执行目录搜索。
- **SIP 拨号规则：** 管理员使用 SIP 拨号规则执行系统数字分析和路由。管理员配置 SIP 拨号规则，并在进行呼叫处理之前将 SIP 拨号规则添加到 Cisco Unified IP 电话。

拨号规则前提条件

- 对于 SIP 拨号规则配置，设备必须在运行 SIP
- 管理员将 SIP 拨号规则与以下设备关联：Cisco 7911、7940、7941、7960、7961、7970 和 7971 IP 电话

拨号规则配置任务流程

过程		
	命令或操作	目的
步骤 1	配置应用程序拨号规则，第 244 页	配置应用程序拨号规则以添加和排序应用程序（例如 Cisco Web Dialer 和 Cisco Unified Communications Manager Assistant）的拨号规则的优先级。
步骤 2	配置目录查找拨号规则，第 245 页	配置目录查找拨号规则将主叫方识别号码转化为能在目录中查找的号码。
步骤 3	配置 SIP 拨号规则，第 245 页	使用 SIP 拨号规则配置为运行 SIP 的电话配置拨号方案。
步骤 4	重排拨号规则优先顺序，第 248 页	可选。如果存在多个拨号规则，请在 Cisco Unified Communications Manager 管理窗口中更改拨号规则的优先级。

配置应用程序拨号规则

Cisco Unified Communications Manager 支持应用程序拨号规则，从而允许您添加和排序应用程序（例如 Cisco Web Dialer 和 Cisco Unified Communications Manager Assistant）的拨号规则的优先级。应用程序拨号规则将自动从用户拨打的电话号码中剥离某些数字或者向其中添加某些数字。例如，拨号规则可自动在 7 位数电话号码前添加数字 9，以访问外线。



注释 Cisco Unified Communications Manager 会自动将应用程序拨号规则应用到 CTI 远程设备的所有远程目标号码。

执行以下程序以添加新的应用程序拨号规则或更新现有的应用程序拨号规则。

过程

- 步骤 1 从 Cisco Unified Communications Manager 管理选择呼叫路由 > 拨号规则 > 应用程序拨号规则。
- 步骤 2 在查找并列出应用程序拨号规则窗口中，执行以下步骤之一：
 - 单击**新增**。
 - 单击**查找**并选择现有的应用程序拨号规则。
- 步骤 3 配置应用程序拨号规则配置窗口中的字段。要查看详细的字段说明，请参阅联机帮助。

步骤 4 单击保存。

下一步做什么

执行以下任务：

- [配置目录查找拨号规则，第 245 页](#)
- [配置 SIP 拨号规则，第 245 页](#)

配置目录查找拨号规则

目录查找拨号规则将呼叫方识别号码转化为能在目录中查找的号码。每个规则指定哪些号码将根据号码的起始位和长度进行转换。例如，您可以创建从 10 位电话号码自动删除区号和 2 位前缀的目录查找规则，这样 4085551212 就会转换为 51212。

执行以下程序以添加新的目录查找拨号规则或更新现有的目录查找拨号规则。

过程

- 步骤 1 从 Cisco Unified Communications Manager 管理中，选择呼叫路由 > 拨号规则 > 目录查找拨号规则。
- 步骤 2 在目录查找拨号规则查找并列出窗口目录查找拨号规则查找并列出 窗口中，执行以下步骤之一：
- 单击新增。
 - 单击查找并选择现有的目录查找拨号规则。
- 步骤 3 配置目录查找拨号规则配置窗口中字段的设置。要查看详细的字段说明，请参阅联机帮助。
- 步骤 4 单击保存。

下一步做什么

[配置 SIP 拨号规则，第 245 页](#)

配置 SIP 拨号规则

SIP 拨号规则为运行 SIP 的 Cisco IP 电话提供本地拨号方案，因此用户无需按下按键或等待计时器到期即可处理呼叫。管理员配置 SIP 拨号方案并将其应用到运行 SIP 的电话。

过程

	命令或操作	目的
步骤 1	设置 SIP 拨号规则，第 246 页	配置和更新 SIP 拨号规则，并将其与运行 SIP 的电话关联。

	命令或操作	目的
步骤 2	重置 SIP 拨号规则，第 247 页	在 SIP 拨号规则更新时重置或重启运行 SIP 的电话，让电话使用新的 SIP 拨号规则更新。
步骤 3	与 SIP 电话同步 SIP 拨号规则设置，第 248 页	（可选）将 SIP 电话与更改了配置的 SIP 拨号规则同步，这将以干扰最小的方式应用尚未应用的配置设置。例如，对某些受到影响的 SIP 电话，可能不要求重置或重启。

相关主题

模式格式，第 246 页

模式格式

表 26: SIP 拨号规则的模式格式

拨号规则模式	值
7940_7960_OTHER	<ul style="list-style-type: none">点号 (.) 可以匹配任何字符井号 (#) 作为终止键，仅当匹配情况符合 ># 时才应用终止。星号 (*) 也可用作终止键。 注释 您必须在模式字段中配置井号，以使其对 7940_7960_OTHER 有效。星号 (*) 匹配一个或多个字符，并被处理为通配符字符。通过在 * 前放置反斜线 (\) 转义序列（形成顺序 *），可以覆盖星号。电话会自动剥离\，因此反斜线不会在出站拨号字串中显示。当 * 作为拨号数字收到时，它通过通配符 * 和点号 (.) 进行匹配。逗号 (,) 会导致电话生成辅助拨号音。 例如，7.... 将与任何以 7 开头的 4 位数目录号码匹配。8,..... 将与 8 匹配，播放辅助拨号音（默认值），然后与任意 5 位数目录号码匹配。

设置 SIP 拨号规则

配置运行 SIP 的电话的拨号方案。

过程

步骤 1 从 Cisco Unified Communications Manager 管理，选择呼叫路由 > 拨号规则 > SIP 拨号规则。

步骤 2 在查找并列出 SIP 拨号规则窗口。请执行以下步骤之一：

- 单击**新增**
- 单击**查找** 并选择现有的 SIP 拨号规则

步骤 3 配置 SIP 拨号规则配置窗口中的字段。要查看详细的字段说明，请参阅联机帮助。

步骤 4 单击**保存**。

注释 在 Cisco Unified Communications Manager 管理中添加或更新 SIP 拨号规则时，请注意，Cisco TFTP 服务会重建所有电话配置文件，从而可能导致其中运行 Cisco TFTP 服务的服务器上 CPU 使用达到高峰，特别是包含许多电话的大型系统。为确保 CPU 使用不达到高峰，请在维护期间添加或更新 SIP 拨号规则，或者先在 Cisco Unified 功能配置中临时停止 Cisco TFTP 服务，然后再更改配置。如果停止 Cisco TFTP 服务，请记住，在添加或更新 SIP 拨号规则后要在 Cisco Unified 功能配置中重新启动服务。

下一步做什么

[重置 SIP 拨号规则，第 247 页](#)

相关主题

[模式格式，第 246 页](#)

重置 SIP 拨号规则

执行以下程序以在 SIP 拨号规则更新时重置或重启运行 SIP 的电话，让电话使用新的 SIP 拨号规则更新。

开始之前

[设置 SIP 拨号规则，第 246 页](#)

过程

步骤 1 从 Cisco Unified Communications Manager 管理选择呼叫路由 > 拨号规则 > 应用程序拨号规则。

步骤 2 在查找并列出 SIP 拨号规则窗口中，单击**查找**，然后选择要重置的现有 SIP 拨号规则。

步骤 3 在 SIP 拨号规则配置窗口中，单击**重置**。

步骤 4 在设备重置对话框中执行以下任务之一：

- 要重新启动所选设备而不将其关闭，并向 Cisco Unified Communications Manager 重新注册它们，然后单击**重新启动**。
- 要关闭然后重新启动设备，请单击**重置**。
- 要关闭“设备重置”对话框而不执行任何操作，请单击**关闭**。

管理员配置 SIP 拨号规则并将其应用到运行 SIP 的电话后，数据库将向 TFTP 服务器发送通知，以便其能够构建一组新的配置文件用于运行 SIP 的电话。TFTP 服务器通知 Cisco Unified Communications Manager 关于新配置文件，并且更新的配置文件将发送到电话。请参阅适用于运行 SIP 的 Cisco Unified IP 电话的[配置 TFTP 服务器](#)了解更多信息。

下一步做什么

[与 SIP 电话同步 SIP 拨号规则设置，第 248 页](#)

与 SIP 电话同步 SIP 拨号规则设置

要将 SIP 电话与更改了配置的 SIP 拨号规则同步，请执行以下程序。

开始之前

[重置 SIP 拨号规则，第 247 页](#)

过程

-
- 步骤 1 从 Cisco Unified Communications Manager 管理，选择呼叫路由 > 拨号规则 > **SIP 拨号规则**。
 - 步骤 2 在查找并列出 **SIP 拨号规则**窗口中，单击**查找**，然后选择要与适用的 SIP 电话同步的现有 SIP 拨号规则。
 - 步骤 3 进行任何其他配置更改，然后在 **SIP 拨号规则配置**中单击**保存**。
 - 步骤 4 单击**应用配置**。
 - 步骤 5 单击**确定**。
-

重排拨号规则优先顺序

在拨号规则配置窗口中添加和排序拨号规则的优先级。

过程

-
- 步骤 1 从 Cisco Unified Communications Manager 管理中，选择呼叫路由 > 拨号规则。
 - 步骤 2 选择下列项之一：
 - 应用程序拨号规则
 - 目录查找拨号规则
 - **SIP 拨号规则**
 - 步骤 3 在“查找并列出”窗口中，选择拨号规则并单击拨号规则名称。

拨号规则配置窗口将会显示。

步骤 4 使用向上和向下箭头可在列表中上下移动拨号规则。

步骤 5 排定优先顺序后，单击**保存**。

拨号规则相互作用和限制

SIP 拨号规则相互作用

SIP 拨号规则相互作用

Cisco Unified IP 电话	互动
运行 SIP 的 7911、7941、7961、7970 和 7971	这些电话使用 7940_7960_OTHER 拨号规则模式。按键标记语言 (KPML) 允许数字逐个发送到 Cisco Unified Communications Manager；SIP 拨号规则允许先在电话上本地收集数字模式，然后再发送到 Cisco Unified Communications Manager。如果未配置 SIP 拨号规则，将使用 KPML。为提升 Cisco Unified Communications Manager 的性能（增加处理的呼叫数），思科建议管理员配置 SIP 拨号规则。
运行 SIP 的 7940 和 7960	这些电话使用 7940_7960_OTHER 拨号规则模式，不支持 KPML。如果管理员不为这些电话配置 SIP 拨号方案，则用户必须等待指定的时间，然后数字才会发送到 Cisco Unified Communications Manager 进行处理。这将延迟实际呼叫的处理。

目录查找拨号规则限制

目录查找拨号规则限制

字段	限制
号码始于	此字段仅支持数字和字符 +、* 和 #。长度不能超过 100 个字符。
数字数目	此字段仅支持数字，该字段中的值不能小于“模式”字段中指定的模式长度。

字段	限制
要删除的数字总数	此字段仅支持数字，该字段中的值不能大于 数字数目 字段中的值。
前缀和模式	<p>“加以前缀”字段仅支持数字和字符+、*和#。 长度不能超过 100 个字符。</p> <p>注释 不允许拨号规则的要删除的数字总数字段和前缀和模式字段同时为空。</p>



第 III 部分

集成应用程序

- [集成 Cisco 应用程序，第 253 页](#)
- [配置 CTI 应用程序，第 259 页](#)



第 26 章

集成 Cisco 应用程序

- [Cisco Unity Connection](#)，第 253 页
- [Cisco Expressway](#)，第 255 页
- [Cisco Emergency Responder](#)，第 256 页
- [Cisco Paging Server](#)，第 256 页
- [Cisco Unified Contact Center Enterprise](#)，第 257 页
- [Cisco Unified Contact Center Express](#)，第 257 页
- [高级 QoS APIC-EM 控制器](#)，第 257 页
- [配置 Cisco WebDialer 服务器](#)，第 258 页

Cisco Unity Connection

在开始配置语音邮件和留言传送系统时，请注意添加用户、启用功能以及将 Cisco Unified Communications Manager 与 Cisco Unity Connection 集成的选项。

与 Cisco Unified Communications Manager 集成时，Cisco Unity Connection（语音邮件和留言系统）为您提供通过 AXL 服务或通过 LDAP 集成手动配置的用户提供语音留言功能。用户的语音信箱收到语音留言后，用户会在电话上收到留言等待灯信号。用户可以使用内部或外部呼叫访问语音留言系统，以检索、收听、回复、前转和删除留言。

您的系统支持直接连接和基于网关的留言系统。直接连接的语音留言系统使用数据包协议与 Cisco Unified Communications Manager 通信。基于网关的语音留言系统通过连接到 Cisco 网关的模拟或数字干线连接到 Cisco Unified Communications Manager。

当您集成 Unified Communications Manager 和 Cisco Unity Connection 时，您可以为您的用户配置以下功能：

- 呼叫前转到个人问候语
- 呼叫前转到忙线问候语
- 主叫方 ID
- 轻松访问消息（用户无需输入 ID 即可检索消息；Cisco Unity Connection 根据发起呼叫的分机识别用户；可能需要密码）

- 识别用户留言（Cisco Unity Connection 根据发起呼叫的分机，自动识别前转内部呼叫期间留言的用户）
- 留言通知指示灯 (MWI)
- 在 Cisco Unified Communications Manager 与 Cisco Unity Connection 服务器之间配置安全 SIP 干线集成需要在混合模式下配置 Cisco Unified Communications Manager 群集。

Cisco Unified Communications Manager 通过下列一个接口与 Cisco Unity Connection 互动：

- SIP 干线—您可以使用 SIP 集成 Cisco Unity Connection 和 Unified Communications Manager。不是多个 SCCP 参与的传统继承，SIP 对每个 Unity Connection 服务器使用一个干线。SIP 集成无需为语音邮件端口和留言通知指示灯 (MWI) 配置目录号码。
- SCCP 协议—您通过创建语音邮件端口，可将接口配置为直接连接语音留言系统。这在 Unified Communications Manager 和 Cisco Unity Connection 之间建立了链路。

要处理到语音留言系统的多个并发呼叫，您可创建多个语音邮件端口，然后将端口置于线路组中并将线路组置于路由/寻线列表中。

Cisco Unified Communications Manager 将生成 SCCP 消息，这些消息通过 Cisco Unity Connection 进行转换。语音邮件系统通过呼叫留言通知打开和关闭号码发送留言通知指示 (MWI)。

配置语音邮件端口和 Cisco Unity SCCP 设备的安全性时，每个设备接受另一个设备的证书后，将为验证的设备打开一个 TLS 连接（握手）；类似地，系统将在设备之间发送 SRTP 流；也就是说，配置设备进行加密。

设备安全模式设置为已验证或已加密时，Cisco Unity TSP 将通过 Unified Communications Manager TLS 端口连接到 Cisco Unified Communications Manager。安全模式为不安全时，Cisco Unity TSP 将通过 Unified Communications Manager SCCP 端口连接到 Cisco Communications Manager。

有关配置 Cisco Unity Connection 以与您的系统集成的详细信息，请参阅《用于 Cisco Unity Connection 的 Cisco Unified Communications Manager SCCP 集成指南》或《用于 Cisco Unity Connection 的 Cisco Unified Communications Manager SIP 干线集成指南》，位于 <http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-and-configuration-guides-list.html>。

启用 PIN 同步

使用此程序启用 PIN 同步，以便最终用户可以使用相同的 PIN 登录到 Extension Mobility、Conference Now、Mobile Connect 和 Cisco Unity Connection 语音邮件。



注释 仅当 Cisco Unified Communications Manager 发布方数据库服务器在运行并完成其数据库复制时，Cisco Unity Connection 和 Cisco Unified Communications Manager 之间的 PIN 同步才能成功。当 Cisco Unity Connection 上的 PIN 同步失败时，将显示以下错误消息：无法在 CUCM 上更新 PIN。原因：获取 PIN 时出错。

如果 PIN 同步已启用，并且最终用户更改了该 PIN，则会在 Cisco Unified Communications Manager 中更新该 PIN。只有在至少一台已配置的 Unity Connection 应用服务器中成功更新 PIN 后，才会发生这种情况。



注释 为了使 PIN 同步生效，管理员必须在成功启用该功能后强制用户更改他们的 PIN。

开始之前

此程序假定您已经与 Cisco Unity Connection 设置建立了应用服务器连接。如果没有，请参见“相关主题”部分了解有关如何添加新的应用服务器的更多信息。

要启用 PIN 同步功能，您需要首先将用于 Cisco Unity 服务器连接的有效证书从 Cisco Unified 操作系统管理页面上上传到 Cisco Unified Communications Manager tomcat-trust。有关如何上传证书的详细信息，请参阅《Cisco Unified Communications Manager 管理指南》中的“管理安全证书”一章，位于 <http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>。

Cisco Unity Connection 服务器中的用户 ID 必须与 Cisco Unified Communications Manager 中的用户 ID 相匹配。

过程

步骤 1 从 Cisco Unified CM 管理，选择系统 > 应用服务器。

步骤 2 选择您为 Cisco Unity Connection 设置的应用服务器。

步骤 3 选中启用最终用户 PIN 同步复选框。

步骤 4 单击保存。

相关主题

[配置应用服务器](#)

Cisco Expressway

Cisco Unified Communications Manager 与 Cisco Expressway 集成以提供 Cisco Unified Communications 移动和远程访问。Cisco Unified Communications 移动和远程访问是思科协作边缘架构的核心部分。它允许终端（例如 Cisco Jabber）未在企业网络中时执行 Cisco Unified Communications Manager (Unified CM) 提供的注册、呼叫控制、部署、消息传送和 Presence 服务。Expressway 为 Unified CM 注册提供安全的防火墙穿越和线路端支持。

总体解决方案提供以下功能：

- 场外访问—为 Cisco Jabber 和 EX/MX/SX 系列客户端提供一致的网络外侧体验。
- 安全—安全的企业对企业通信。

- 云服务—企业级灵活性和可扩展解决方案，提供丰富的 Webex 集成和服务提供程序服务。
- 网关和互操作性服务—媒体和信令标准化并支持非标准终端。

对于部署详细信息，请参阅通过 *Cisco Expressway* 移动和远程访问部署指南，位于 <https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html>。

Cisco Emergency Responder

Cisco Emergency Responder (Emergency Responder) 帮助您管理电话网络中的紧急呼叫，以便您可以对这些呼叫作出有效回应，并有助于符合当地与紧急呼叫处理有关的法令。在北美地区，这些当地法令称为“增强型 911”或 E911。其他国家和地区有类似的法令。

即便在一个国家、地区、省市，甚至城市圈内，紧急呼叫条例都可能因地而异，因此 Emergency Responder 为您提供灵活性，以使紧急呼叫配置与特定的地区要求相符合。但是，由于条例因地而异，安全要求因公司而不同，所以您必须在部署 Emergency Responder 之前研究您的安全和法律需求。

有关如何安装 Cisco Emergency Responder 并将其与 Cisco Unified Communications Manager 集成的详细信息，请参阅《*Cisco Emergency Responder* 管理指南》，位于 <https://www.cisco.com/c/en/us/support/unified-communications/emergency-responder/products-maintenance-guides-list.html>

Cisco Unified Communications Manager 的功能支持

以下 Cisco Unified Communications Manager 功能支持与 Cisco Emergency Responder 的集成。有关如何在 Cisco Unified Communications Manager 上配置这些功能的信息，请参阅《*Cisco Unified Communications Manager* 功能配置指南》，位于 <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>。

- 位置感知
- 紧急处理程序

Cisco Paging Server

Cisco Unified Communications Manager 可被配置为与 Cisco 寻呼服务器集成，为 Cisco IP 电话和各种终端提供基本的寻呼服务。Cisco 寻呼服务器产品通过 InformaCast 虚拟设备提供，并具有以下部署选项：

- 基本寻呼—为 Cisco IP 电话提供电话到电话和组实时音频寻呼。系统的所有用户都可以参与发起和接收基本寻呼。
- 高级通知—提供功能完备的紧急通知解决方案，能让您使用文本和实时音频或预录音频消息来接通不限数量的电话

有关 Cisco 寻呼服务器的详细信息和文档，请参阅<https://www.cisco.com/c/en/us/products/unified-communications/paging-server/index.html>。

配置

有关如何配置 Cisco Unified Communications Manager 进行基本寻呼或高级通知的详细信息，请参阅《Cisco Unified Communications Manager 功能配置指南》中的“寻呼”一章。

Cisco Unified Contact Center Enterprise

您可以使用系统中的 Cisco Unified Contact Center Enterprise (Unified CCE) 来通过 IP 网络将智能呼叫路由、网络到桌面计算机电话集成 (CTI) 和多通道联系管理集成到联系中心座席。Unified CCE 将软件 IP 自动呼叫分配 (ACD) 与 Cisco Unified Communications 相结合，以便您快速部署先进的分布式联系中心。

有关如何配置 Unified CCE 以与您的系统集成的任务详细信息，请参阅《Cisco Unified Contact Center Enterprise 安装和升级指南》，位于 <http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html>。

Cisco Unified Contact Center Express

Cisco Unified Contact Center Express (Unified CCX) 为您的系统提供封装在单或双服务器部署中的大型联系中心的功能。Unified CCX 最多可扩展到 400 个并发座席、42 主管、150 座席组和 150 技能组。它包括电子邮件、聊天、出站呼叫、入站呼叫、员工优化和报告。

Unified CCX 与 Unified Communication Manager 配合使用，从而代表 Unified CCX 管理所有联系中心呼叫。当有拨向帮助台的呼叫时，您的呼叫系统会识别该号码将发送到 Unified CCX 应用程序服务器。使用此配置时，Unified CCX 将接收传入呼叫，并根据拨打的分机号码处理请求。脚本会播放提示、收集数字，如有必要，还会使用来自主叫方的信息来选择适当的座席。如果分配的座席没空，则呼叫将被置于相应的队列中，并且会将录制的消息或音乐流传输给主叫方。座席有空后，Unified CCX 将指示 Unified Communications Manager 振铃座席的电话。

当座席代答时，会向座席的桌面应用程序提供相应的呼叫上下文。此步骤可确保座席提前掌握正确的信息以支持客户。

有关如何配置 Unified CCX 与您的系统集成的详细任务，请参阅《Cisco Unified CCX 管理指南》，位于 <http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-installation-and-configuration-guides-list.html>。

高级 QoS APIC-EM 控制器

APIC-EM 控制器提供管理网络流量的集中式系统，以便您始终有带宽来维护通信，即使是在拥挤的网络中。您可以将 Cisco Unified Communications Manager 配置为使用 APIC-EM 控制器来管理 SIP 媒体流，从而获得以下优势：

- 集中管理 QoS，从而剔除终端分配 DSCP 值的必要性。
- 对不同的媒体流应用差异化 QoS 处理方式。例如，您可以将音频优先于视频，以确保即使网络带宽很低，也能始终保持基本的音频通信。
- SIP 配置文件中的外部 QoS 设置允许您将使用 APIC-EM 的用户作为目标。例如，您可将 Cisco Jabber 用户使用 APIC-EM 管理媒体流，而 Cisco Unified IP 电话用户在 Cisco Unified Communications Manager 中使用 DSCP 设置。

配置详细信息

有关其他详细信息，包括如何配置 Cisco Unified Communications Manager 以与 APIC-EM 控制器集成的信息，请参阅《Cisco Unified Communications Manager 功能配置指南》的“使用 APIC-EM 控制器配置服务质量”一章。

配置 Cisco WebDialer 服务器

将 Cisco WebDialer 应用程序服务器配置为 **WebDialers** 列表服务参数的备用项，这将限制您可以输入的字符数。如果在应用服务器配置窗口中添加 Cisco WebDialer 应用服务器，该服务器将显示在 Cisco WebDialer Web 服务的 **服务参数配置** 窗口中的“WebDialer 列表”字段中。有关配置 Cisco WebDialer 的完整详细信息，请参阅《Cisco Unified Communications Manager 功能配置指南》，位于 <http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>。

过程

-
- 步骤 1 从 Cisco Unified CM 管理中，选择 **系统 > 应用服务器**。
 - 步骤 2 单击 **新增**。
 - 步骤 3 从应用服务器类型下拉列表中，选择 **Cisco Web Dialer**，然后单击下一步。
 - 步骤 4 在主机名或 IP 地址字段中，输入 WebDialer 服务器的主机名或 IP 地址。
 - 步骤 5 从重定向器节点下拉列表中，选择 **< None >** 或特定的 Unified Communications Manager 节点。
< None > 表示 WebDialer 服务器将应用到所有节点。
 - 步骤 6 单击 **保存**。
 - 步骤 7 在 Cisco Unified 功能配置中，选择 **工具 > 控制中心 - 功能服务**。
 - 步骤 8 单击 **Cisco WebDialer Web 服务** 单选按钮。
 - 步骤 9 单击 **重新启动**。
-



第 27 章

配置 CTI 应用程序

- [CTI 应用程序概述，第 259 页](#)
- [CTI 应用程序前提条件，第 261 页](#)
- [配置 CTI 应用程序任务流程，第 261 页](#)

CTI 应用程序概述

在拨打、接收和管理电话呼叫时，您可以使用计算机电话集成 (CTI) 来利用计算机处理功能。CTI 应用程序允许您执行诸如使用主叫方 ID 从数据库检索客户信息之类的任务，或使用交互式语音应答 (IVR) 系统收集的信息将客户的呼叫连同其信息一起路由到相应的客户服务代表。

想要终止路由点呼叫媒体的应用程序必须逐个呼叫指定呼叫的媒体和端口。CTI 应用程序可以使用静态或动态 IP 地址和端口号终止 CTI 端口和 CTI 路由点上的媒体。

本章介绍如何配置 Cisco Unified Communications Manager 使用 CTI 应用程序。有关如何配置特定应用程序的详细信息，请参阅《*Cisco Unified Communications Manager 功能配置指南*》。

可用的一些 Cisco CTI 应用程序包括：

- **Cisco IP Communicator:** 一款桌面应用程序，凭借呼叫跟踪、桌面协作以及从在线目录一键拨号的额外优势，将您的计算机变成一部功能齐备的电话。
- **Cisco Unified Communications Manager Auto-Attendant:** 配合 Cisco Unified Communications Manager 使用，接收特定电话分机上的呼叫并允许主叫方选择适当的分机。
- **Cisco Web Dialer:** 允许 Cisco IP 电话用户从 web 和桌面应用程序进行呼叫。
- **Cisco Unified Communications Manager Assistant:** 可让经理及其助理更高效地共同工作。该功能包含呼叫路由服务、经理和助理电话功能增强以及主要供助理使用的 Assistant Console 界面。



注释

要确定哪些 Unified Communications Manager CTI 应用程序支持 SIP IP 电话，请参阅应用程序特定的文档。

CTI 路由点概述

CTI 路由点虚拟设备可接收多个并行呼叫以实现应用程序控制的重定向。可在用户可以呼叫以访问应用程序的 CTI 路由点上配置一条或多条线路。应用程序可以应答路由点的呼叫，也可以将呼叫重定向到 CTI 端口或 IP 电话。CTI 应用程序使用重定向 API 请求重定向呼叫时，Cisco Unified Communications Manager 将线路/设备呼叫搜索空间的配置用于重定向方。

通过 CTI 路由点，您可以：

- 应答呼叫
- 发起和接收多个活动呼叫
- 重定向呼叫
- 保留呼叫
- 取消保留呼叫
- 丢弃呼叫

Cisco Unified Communications Manager 上的 CTI 冗余

群集中的 Unified Communications Manager 节点发生故障时，CTIManager 通过在另一个 Unified Communications Manager 节点上重新打开这些设备来恢复受影响的 CTI 端口和路由点。如果应用程序有打开的电话设备，CTIManager 在电话故障转移到不同 Unified Communications Manager 时也将重新打开电话。如果 Cisco IP 电话没有故障转移到不同的 Unified Communications Manager，CTIManager 无法打开电话或电话上的线路。CTIManager 使用分配给设备池的 Unified Communications Manager 组决定哪个 Unified Communications Manager 用于恢复应用程序打开的 CTI 设备和电话。

CTIManager 上的 CTI 冗余

CTIManager 发生故障时，连接到 CTIManager 的应用程序可以通过在另一个 CTIManager 上重新打开这些设备恢复受影响的资源。基于设置应用程序时定义为主要和备用的 CTIManager 确定使用哪个 CTIManager（如果该应用程序支持）。应用程序连接到 CTIManager 时，其可以重新打开以前打开的设备和线路。应用程序可以在电话重新连接到新 Unified Communications Manager 之前重新打开 Cisco IP 电话；但无法控制电话，直到重新连接完成。



注释 应用程序恢复服务时不会重新连接到主要 CTIManager。如果重新启动该应用程序或备用 CTIManager 发生故障，应用程序会故障回复到主要 CTIManager。

应用程序故障的 CTI 冗余

当应用程序（TAPI/JTAPI 或直接连接至 CTIManager 的应用程序）失败时，CTIManager 会关闭应用程序并将 CTI 端口和路由点上未终结的呼叫重定向到所配置的故障时呼叫前转 (CFOF) 号码。

CTIManager 还会将进入 CTI 端口和路由点的后续呼叫路由至所配置的无应答时呼叫前转 (CFNA) 号码，直至应用程序恢复并注册那些设备。

CTI 应用程序前提条件

必须配置设备池，然后才能为 CTI 应用程序配置 Cisco Unified Communications Manager。

为每个 CTI 应用程序添加和配置 IP 电话。有关添加和配置 IP 电话的详细信息，请参阅《Cisco Unified IP 电话》。

配置将使用 CTI 应用程序的最终用户和应用程序用户。

计算机电话集成 (CTI) 通过支持 IPv4 和 IPv6 地址的 JTAPI 和 TAPI 接口提供 IP 地址信息。如果要支持 IPv6 地址，请确保您的应用程序正在使用支持 IPv6 的 JTAPI/TAPI 客户端接口版本。

配置 CTI 应用程序任务流程

要为 CTI 应用程序配置 Cisco Unified Communications Manager，请执行以下任务。

过程

	命令或操作	目的
步骤 1	激活 CTIManager 服务，第 262 页	在适当的服务器上激活 CTIManager 服务，如果其尚未激活。
步骤 2	配置 CTIManager 和 Cisco Unified Communications Manager 服务参数，第 262 页	配置与 CTI Super Provider 功能配合使用的 CTIManager 高级群集范围服务参数：
步骤 3	要配置 CTI 路由点，请执行以下程序： <ul style="list-style-type: none"> 配置 CTI 路由点，第 263 页 配置新呼叫接受计时器，第 263 页 配置并发活动呼叫，第 264 页 同步 CTI 路由点，第 264 页 	配置一个或多个 CTI 路由点虚拟设备，这些设备可以接收多个同时呼叫，以进行应用程序控制的重定向。
步骤 4	配置 CTI 设备目录号码，第 264 页	配置 CTI 设备的目录号码。
步骤 5	将设备与组关联，第 265 页	将该应用程序将用于应用程序用户和最终用户的所有设备与适当的 Cisco Unified Communications Manager 组关联（通过设备池）。
步骤 6	添加最终用户和应用程序用户，第 265 页	通过将最终用户和应用程序用户添加到“标准 CTI 已启用”用户组，可让 CTI 应用程序控制 Cisco Unified Communications Manager 系统中配置的任何 CTI 控制设备。

	命令或操作	目的
步骤 7	(可选) 配置 CTI 冗余以解决应用程序故障，第 266 页	定义 CTIManager 期望在两个连续间隔内从应用程序接收消息的间隔。

激活 CTIManager 服务

过程

- 步骤 1 在 Cisco Unified 功能配置上，选择工具 > 服务激活。
- 步骤 2 从服务器下拉列表中选择节点。
- 步骤 3 选中 CM 服务部分的 **Cisco CTIManager** 复选框。
- 步骤 4 单击保存。

配置 CTIManager 和 Cisco Unified Communications Manager 服务参数

配置与 CTI Super Provider 功能配合使用的 CTIManager 高级群集范围服务参数：



注释 如果超出配置的限制，CTI 将生成警报，但应用程序会继续打开额外的设备。

过程

- 步骤 1 从 Cisco Unified CM 管理中，选择系统 > 服务参数。
- 步骤 2 从服务器下拉列表中选择节点。
- 步骤 3 从服务下拉列表中选择 Cisco CTIManager（活动）。
- 步骤 4 在服务参数配置窗口中，单击高级。
- 步骤 5 在每个提供商的最大设备数字段中，输入一个 CTI 应用程序可以打开的最大设备数。默认为 2000 个设备。
- 步骤 6 在“每个节点的最大设备数”字段中，输入所有 CTI 应用程序可以在 Unified Communications Manager 系统中的任何 CTIManager 节点上打开的最大设备数。默认为 800 个设备。
- 步骤 7 单击保存。

配置 CTI 路由点任务流程

过程

	命令或操作	目的
步骤 1	配置 CTI 路由点，第 263 页	添加新的或修改现有的 CTI 路由点。
步骤 2	配置新呼叫接受计时器，第 263 页	配置新呼叫接受计时器，从而在呼叫到达新的路由点时，应用程序将在指定的时间内进行处理（接受、应答、重定向）。
步骤 3	配置并发活动呼叫，第 264 页	配置路由点上的并发活动呼叫数。
步骤 4	可选： 同步 CTI 路由点，第 264 页	将 CTI 路由点与最新的配置更改同步，这将以干扰最小的方式应用尚未应用的配置设置。（例如，对某些受到影响的设备，可能不要要求重置/重启。）

配置 CTI 路由点

添加新的或修改现有的 CTI 路由点。

过程

步骤 1 从 Cisco Unified CM 管理中，单击设备 > CTI 路由点。

步骤 2 请执行以下任务之一：

- 单击**新增**，可添加新的网关。
- 单击**查找**，然后从结果列表中选择 CTI 路由点以修改现有 CTI 路由点的设置，输入搜索条件。

步骤 3 配置 CTI 路由点配置窗口中的字段。有关字段及其配置选项的更多信息，请参阅系统联机帮助。

步骤 4 单击**保存**。

配置新呼叫接受计时器

配置新呼叫接受计时器，从而在呼叫到达新的路由点时，应用程序将在指定的时间内进行处理（接受、应答、重定向）。

过程

步骤 1 从 Cisco Unified CM 管理中，选择系统 > 服务参数。

步骤 2 从服务器下拉列表中选择节点。

步骤 3 从“服务”下拉列表中选择 **Cisco CallManager（活动）**。

步骤 4 在 **CTI 新呼叫接受计时器** 字段中，指定您希望允许呼叫被应答的时间。默认值为 4。

步骤 5 单击保存。

配置并发活动呼叫

配置路由点上的并发活动呼叫数。



注释 如果打算通过 Cisco CallManager 电话服务提供程序 (TSP) 使用 TAPI 应用程序控制 CTI 端口设备，每个 CTI 端口设备只能配置一条线路。

过程

步骤 1 从 Cisco Unified CM 管理中，单击呼叫路由 > 目录号码。

步骤 2 在“目录号码配置”窗口上，单击**新增**。

步骤 3 填写必填字段：

步骤 4 单击保存。

同步 CTI 路由点

将 CTI 路由点与最新的配置更改同步，这将以干扰最小的方式应用尚未应用的配置设置。（例如，对某些受到影响的设备，可能不要求重置/重启。）

过程

步骤 1 从 Cisco Unified CM 管理中，单击设备 > **CTI 路由点**。

步骤 2 在**查找并列出 CTI 路由点**窗口中，单击**查找**以显示 CTI 路由点的列表。

步骤 3 选中要同步的 CTI 路由点旁边的复选框。要选择窗口中的所有 CTI 路由点，请选中匹配记录标题栏中的复选框。

步骤 4 单击**应用配置到选定项**。

步骤 5 单击**确定**。

配置 CTI 设备目录号码

配置 CTI 设备的目录号码。

过程

步骤 1 从 Cisco Unified CM 管理中，选择呼叫路由 > 目录号码。

步骤 2 在查找并列出目录号码窗口中，单击新增。

步骤 3 在目录号码配置窗口中，输入所需的字段。

步骤 4 单击保存。

将设备与组关联

将该应用程序将用于应用程序用户和最终用户的所有设备与适当的 Cisco Unified Communications Manager 组关联（通过设备池）。

过程

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

步骤 2 在查找并列出应用程序用户窗口上，单击新增。这会将您带到“应用程序用户配置”窗口。

步骤 3 在“设备信息”窗格中，通过将您的设备从“可用设备”列表移至“受控设备”列表来关联设备。

步骤 4 单击保存。

步骤 5 要关联最终用户的设备，请单击用户管理 > 最终用户。

步骤 6 重复步骤 2 - 4。

添加最终用户和应用程序用户

通过将最终用户和应用程序用户添加到“标准 CTI 已启用”用户组，可让 CTI 应用程序控制 Cisco Unified Communications Manager 系统中配置的任何 CTI 控制设备。

过程

步骤 1 从 Cisco Unified CM 管理中，单击用户管理 > 用户设置 > 访问控制组。

步骤 2 在查找并列出访问控制组窗口中，单击查找以显示当前的访问控制组列表。

步骤 3 单击**标准 CTI 已启用**将进入此组的“访问控制组配置”窗口。确保所有 CTI 用户均位于“标准 CTI 已启用”用户组中。有关有空组及其功能的完整列表，请参阅访问控制组配置选项。


步骤 4 如果要添加最终用户，请单击**将最终用户添加到组**，或者，如果要添加应用程序用户，请单击**将应用程序用户添加到组**。


步骤 5 单击**查找**以显示当前用户的列表。


步骤 6 选中您要分配到“标准 CTI 已启用”用户组的用户。

步骤 7 单击添加选定项。

访问控制组配置选项

- 

注释 CTI 应用程序必须支持其分配到的指定用户组。
- 

注释 Cisco 建议与“标准 CTI 允许控制所有设备”用户组关联的用户也与“标准 CTI 安全连接”用户组关联。
- 

注释 您必须为下表中列出的所有角色添加**受控设备**下的特定设备，才能正常工作。

字段	说明
标准 CTI 允许呼叫监控	此用户组允许应用程序监控呼叫。
标准 CTI 允许呼叫暂留监控	此用户组允许应用程序在呼叫暂留/取消暂留到所有呼叫暂留目录号码时接收通知。
标准 CTI 允许呼叫录音	此用户组允许应用程序对呼叫进行录音。
标准 CTI 允许主叫号码修改	此用户组允许应用程序修改支持的 CTI 应用程序中的主叫方号码。
标准 CTI 允许控制所有设备	此用户组允许应用程序控制或监控系统中任何 CTI 控制的设备。
标准 CTI 允许接收 SRTP 重要材料	此用户组允许应用程序接收解密已加密媒体流所必需的信息。该组通常出于录音和监控目的使用。
启用标准 CTI	此用户组为所有 CTI 应用程序必需，允许应用程序连接到 Cisco Unified Communications Manager 以访问 CTI 功能。
标准 CTI 安全连接	纳入本组将需要应用程序具有到 Cisco Unified Communications Manager 的安全 (TLS) CTI 连接并且 Cisco Unified Communications Manager 群集安全性已启用。

配置 CTI 冗余以解决应用程序故障

定义 CTIManager 期望在两个连续间隔内从应用程序接收消息的间隔。

过程

- 步骤 1 从 Cisco Unified CM 管理中，选择系统 > 服务参数。
 - 步骤 2 从服务器下拉列表中选择节点。
 - 步骤 3 从服务下拉列表中选择 **Cisco CTIManager**（活动）。
 - 步骤 4 在服务参数配置窗口中，单击高级。
 - 步骤 5 在应用程序心跳最小间隔字段中，输入最小间隔的时间。默认值为 5。
 - 步骤 6 在应用程序心跳最大间隔字段中，输入最大间隔的时间。默认为 3600。
 - 步骤 7 单击保存。
-



第 **IV** 部分

预配置最终用户

- [配置预配置配置文件，第 271 页](#)
- [配置 LDAP 同步，第 285 页](#)
- [使用批量管理工具预配置用户和设备，第 293 页](#)



第 28 章

配置预配置配置文件

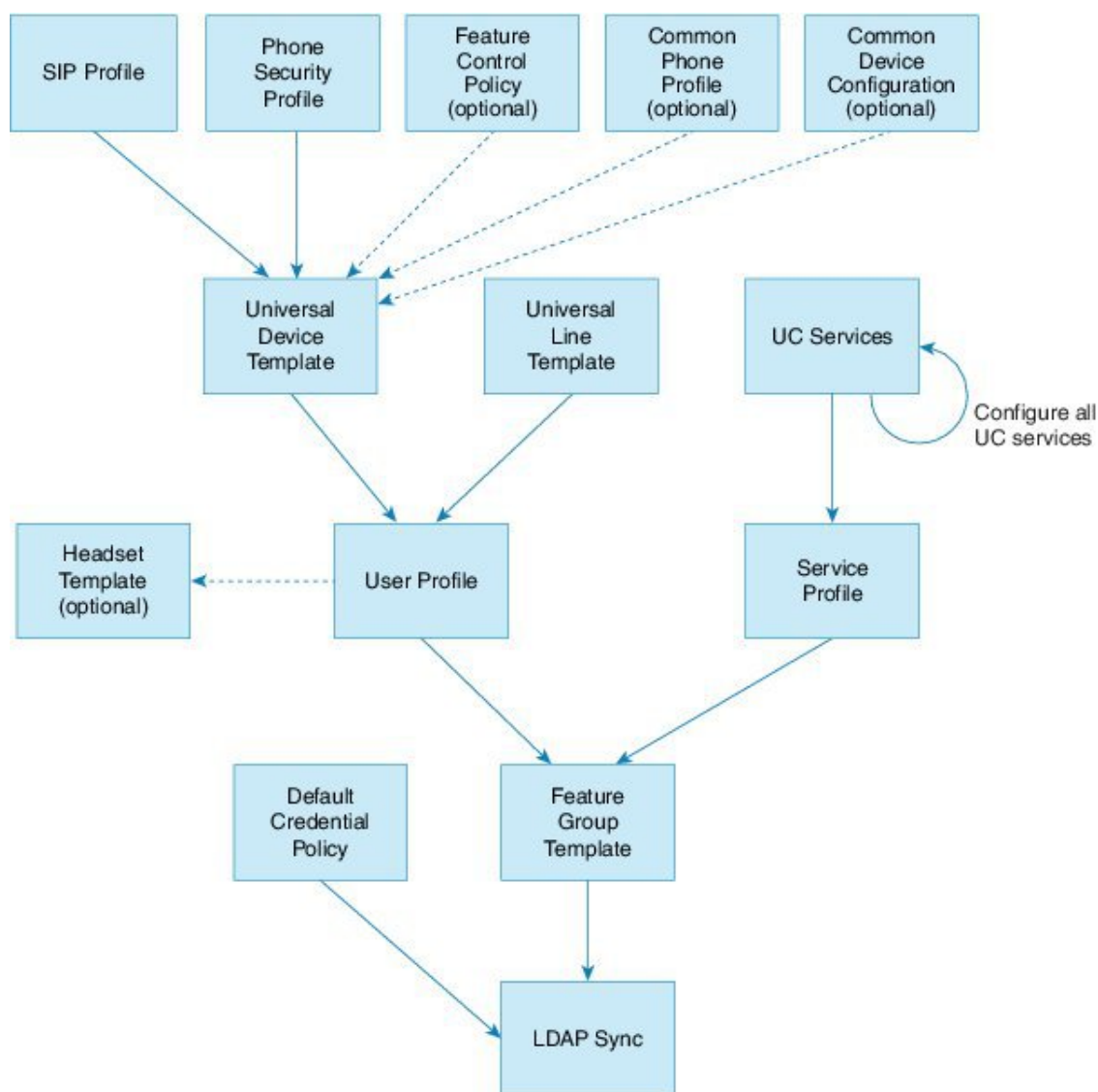
- 预配置配置文件概述，第 271 页
- 预配置配置文件任务流程，第 272 页
- 配置 SIP 配置文件，第 274 页
- 配置电话安全性配置文件，第 274 页
- 创建功能控制策略，第 275 页
- 创建通用电话配置文件，第 276 页
- 配置通用设备配置，第 277 页
- 配置通用设备模板，第 277 页
- 配置通用线路模板，第 278 页
- 配置用户配置文件，第 278 页
- 配置头戴式耳机模板，第 280 页
- 配置 UC 服务，第 280 页
- 配置服务配置文件，第 281 页
- 配置功能组模板，第 282 页
- 配置默认凭证策略，第 283 页

预配置配置文件概述

Unified Communications Manager 包含一组可分配给新用户的配置文件和模板。如果您预先设置了这些配置文件和通用设置，则在预配置新用户和分配设备时，系统会根据应用的设置自动配置用户和设备。

预配置用户时，将其关联到包含他们所需设置的用户配置文件和服务配置文件。此外，为用户添加设备时，系统会使用与用户的用户配置文件关联的通用线路和通用设备模板快速配置其设备和目录号码。

您可以使用以下配置文件和模板根据用户需求将通用设置应用于用户和终端。



394052

预配置配置文件任务流程

如果要配置大量用户和设备，可以使用适用于特定组（例如客户支持）中的用户的模板和通用设置来设置用户配置文件和服务配置文件，从而简化配置过程。

预配置用户时，将其关联到包含他们所需设置的用户配置文件和服务配置文件。此外，为用户添加设备时，系统会使用与用户的用户配置文件关联的通用线路和通用设备模板快速配置其设备和目录号码。

您可以使用以下配置文件和模板根据用户需求将通用设置应用于用户和终端。

过程

	命令或操作	目的
步骤 1	配置 SIP 配置文件，第 274 页	设置将与您部署的 SIP 终端关联的通用 SIP 设置。
步骤 2	配置电话安全性配置文件，第 274 页	配置您将分配给预配置终端的安全性配置文件。分配 TLS 和 TFTP 加密等设置。
步骤 3	创建功能控制策略，第 275 页	可选。使用此策略可启用特定功能并控制电话软键的显示。
步骤 4	创建通用电话配置文件，第 276 页	可选。使用此配置文件可将 TFTP 数据和产品特定的配置默认值分配到您可以分配给终端组的配置文件。
步骤 5	配置通用设备配置，第 277 页	可选。使用此配置可将用户特定的设置和 IPv6 首选项分配给终端。
步骤 6	配置通用设备模板，第 277 页	此模板包含用于配置新预配置的电话的通用设置。还可以将已配置的配置文件分配给此模板。
步骤 7	配置通用线路模板，第 278 页	此模板包含用于配置新预配置的分机的通用设置。您也可以为分机配置企业和 E.164 号码。
步骤 8	配置用户配置文件，第 278 页	使用新预配置的用户设备模板、线路模板和通用设置设置用户配置文件。
步骤 9	配置头戴式耳机模板，第 280 页	可选。如果您计划使用 Cisco Headsets 配置头戴式耳机模板，并将其分配给您设置的用户配置文件。
步骤 10	配置 UC 服务，第 280 页	配置 UC 服务，例如 IM and Presence Service 和目录服务。
步骤 11	配置服务配置文件，第 281 页	创建包含要分配给预配置用户的 UC 服务的服务配置文件。
步骤 12	配置功能组模板，第 282 页	对于 LDAP 同步，将您的用户配置文件和服务配置文件添加到您可以分配到 LDAP 同步用户的功能组模板。
步骤 13	配置默认凭证策略，第 283 页	配置将分配给新预配置的用户凭证策略。

下一步做什么

- 设置 LDAP 同步以预配置新用户

- 如果未部署 LDAP，可以使用批量管理来批量预配置用户。

配置 SIP 配置文件

使用此程序配置 SIP 配置文件，其中包含您可以分配给 SIP 设备的通用 SIP 设置。

过程

步骤 1 从 Cisco Unified CM 管理，选择设备 > 设备设置 > SIP 配置文件。

步骤 2 请执行以下步骤之一：

- 要编辑现有配置文件，请单击**查找**并选择 SIP 配置文件。
- 要创建新的配置文件，请单击**新增**。

步骤 3 输入配置文件的名称。

步骤 4 如果在部署 URI 拨号，则配置**拨号字符串解析**以指示系统是将呼叫作为目录 URI 还是电话号码处理。

步骤 5 在**电话中使用的参数**下，完成 DSCP 设置以为使用此配置文件的呼叫类型定义 QoS 处理。

步骤 6 （可选）如果需要分配标准化脚本，请从“标准化脚本”下拉列表中选择一个默认脚本。

注释 您也可以创建自己的脚本。有关详细信息，请参阅《*Cisco Unified Communications Manager 功能配置指南*》。

步骤 7 如果您希望此配置文件同时支持 IPv4 和 IPv6 堆栈，请选中**启用 ANAT** 复选框。

步骤 8 如果想要用户能够共享显示，请选中**允许通过 BFCP 共享显示**复选框。

步骤 9 完成“SIP 配置文件配置”窗口中其余字段的设置。有关这些字段及其设置的帮助，请参阅联机帮助。

步骤 10 单击**保存**。

配置电话安全性配置文件

如果想要为终端启用 TLS 信令、CAPF 和 Digest 验证要求等安全性功能，则必须配置可以将其应用到终端的新的安全性配置文件。



注释 默认情况下，如果您不将 SIP 电话安全配置文件应用于预配置的设备，则该设备将使用非安全配置文件。

过程

- 步骤 1** 从 Cisco Unified CM 管理中，选择系统 > 安全性 > 电话安全性配置文件。
- 步骤 2** 单击**新增**。
- 步骤 3** 从电话安全性配置文件类型下拉列表中，选择通用设备模板以创建通过设备模板预配置时可以使用配置文件。
注释 或者，您也可以为特定设备型号创建安全性配置文件。
- 步骤 4** 选择协议。
- 步骤 5** 在名称字段中输入配置文件的相应名称。
- 步骤 6** 如果要使用 TLS 信令连接到设备，请将设备安全模式 设置为已验证或已加密，并将“传输类型”设置为 **TLS**。
- 步骤 7** （可选）如果您希望电话使用 Digest 验证，请选中**启用 OAuth 验证**复选框。
- 步骤 8** （可选）如果要使用加密 TFTP，请选中 **TFTP 加密配置**复选框。
- 步骤 9** 完成“电话安全性配置文件配置”窗口中其余字段的设置。有关这些字段及其设置的帮助，请参阅联机帮助。
- 步骤 10** 单击**保存**。

创建功能控制策略

请按照以下步骤创建功能控制策略。使用此策略以启用或禁用特定功能，从而控制电话上显示的软键的外观。

过程

- 步骤 1** 从 Cisco Unified CM 管理中，选择设备 > 设备设置 > 功能控制策略。
- 步骤 2** 请执行以下任务之一：
 - 要修改现有策略的设置，请输入搜索条件，单击**查找**，然后从结果列表中选择策略。
 - 要添加新策略，请单击**新增**。功能控制策略配置窗口将会显示。
- 步骤 3** 在名称字段中，输入功能控制策略的名称。
- 步骤 4** 在说明字段中，输入功能控制策略的说明。
- 步骤 5** 在功能控制部分，对于列出的每个功能，选择是否覆盖系统默认值，以及启用还是禁用此设置：
 - 如果默认启用此功能，而您要禁用此设置，则选中**覆盖默认值**下的复选框，并取消选中**启用设置**下的复选框。

- 如果默认禁用此功能，而您要启用此设置，则选中**覆盖默认值**下的复选框，并选中**启用设置**下的复选框。

步骤 6 单击**保存**。

创建通用电话配置文件

通用电话配置文件是可选配置文件，可用于为使用该配置文件的电话配置 TFTP 数据和产品特定配置默认设置。

过程

步骤 1 从 Cisco Unified CM 管理，选择**设备 > 设备设置 > 通用电话配置文件**菜单路径以配置通用电话配置文件。

步骤 2 单击**新增**。

步骤 3 输入配置文件的名称。

步骤 4 输入配置文件说明。

步骤 5 如果您为使用此配置文件的电话设置了**功能控制策略**，请从下拉列表中选择该策略。

步骤 6 在**通用电话配置文件配置**窗口中完成其余字段的设置。有关这些字段及其设置的帮助，请参阅联机帮助。

步骤 7 配置“产品特定配置布局”下的字段 对于字段说明，单击 (?) 可查看字段特定帮助。

步骤 8 （可选）如果要为移动电话和远程访问电话启用交互式连接建立 (ICE):

a) 将 ICE 下拉列表设置为**已启用**。

b) 将**默认候选者类型**设置为以下之一:

- **主机一**—通过选择主机设备上的 IP 地址获得的候选者。这是默认值。
- **服务器自反一**—通过发送 STUN 请求获得的 IP 地址和端口候选者。通常，这可能代表 NAT 的公共 IP 地址。
- **已中继一**—从 TURN 服务器获得的 IP 地址和端口候选者。IP 地址和端口驻留在 TURN 服务器上，以便媒体通过 TURN 服务器中继。

c) 配置其余 ICE 字段。

步骤 9 单击**保存**。

配置通用设备配置

通用设备配置包含用户特定的服务和功能属性。如果要部署 IPv6，可以使用此配置为 SIP 干线或 SCCP 电话分配 IPv6 首选项。

过程

步骤 1 从 Cisco Unified CM 管理中，选择设备 > 设备设置 > 通用设备配置。

步骤 2 单击新增。

步骤 3 对于 SIP 干线、SIP 电话或 SCCP 电话，从 **IP 寻址模式** 下拉列表中选择一个值：

- **仅 IPv4**—对于媒体和信令，设备仅使用 IPv4 地址。
- **仅 IPv6**—对于媒体和信令，设备仅使用 IPv6 地址。
- **IPv4 和 IPv6（默认）**—设备为双堆栈设备，并使用任何可用的 IP 地址类型。如果设备上配置了两种 IP 地址类型，则对于信令，设备使用用于信令的 **IP 寻址模式** 首选项设置，对于媒体，设备使用用于媒体的 **IP 寻址模式** 首选项企业参数。

步骤 4 如果您在上一步中配置 IPv6，则为用于信令的 **IP 寻址模式** 下拉列表配置 IP 寻址首选项：

- **IPv4**—双堆栈设备首选 IPv4 地址进行信令。
- **IPv6**—双堆栈设备首选 IPv6 地址进行信令。
- **使用系统的默认值**—设备将该设置用于用于信令的 **IP 寻址模式** 首选项企业参数。

步骤 5 配置通用设备配置窗口中的其余字段。有关字段及其配置选项的更多信息，请参阅系统联机帮助。

步骤 6 单击保存。

配置通用设备模板

通用设备模板可让您轻松地将配置设置应用到新预配置的设备。预配置的设备使用通用设备模板的设置。可以配置不同的设备模板来满足不同用户群体的需求。还可以将已配置的配置文件分配给此模板。

过程

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

步骤 2 单击新增。

步骤 3 输入以下必填字段：

- a) 为模板输入设备说明。
- b) 从下拉列表中选择设备池类型。

- c) 从下拉列表中选择设备安全性配置文件。
- d) 从下拉列表中选择 **SIP** 配置文件。
- e) 从下拉列表中选择电话按键模板。

步骤 4 完成通用设备模板配置窗口中其余字段的设置。要查看字段说明，请参阅联机帮助。

步骤 5 在电话设置下，填写以下可选字段：

- a) 如果配置了通用电话配置文件，分配该配置文件。
- b) 如果配置了通用设备配置，分配该配置。
- c) 如果配置了功能控制策略，分配该策略。

步骤 6 单击保存。

配置通用线路模板

通过通用线路模板，您可以轻松地将通用设置应用到新分配的目录号码。配置不同的模板以满足不同用户组的需求。

过程

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

步骤 2 单击新增。

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

步骤 4 如果要部署具有备用号码的全局拨号方案复制，展开企业备用号码和 +E.164 备用号码部分，然后执行以下操作：

- a) 单击添加企业备用号码按钮和/或添加 +E.164 备用号码按钮。
- b) 添加要用于分配到备用号码的号码掩码。例如，一个 4 位分机可能会将 5XXXX 用作企业号码掩码，并将 1972555XXXX 用作 +E.164 备用号码掩码。
- c) 分配要为其分配备用号码的分区。
- d) 如果想要通过 ILS 通告此号码，请选中通过 **ILS 全局通告** 复选框。请注意，如果您使用通告模式来汇总备用号码的范围，可能不需要通告单独的备用号码。
- e) 展开 **PSTN 故障转移** 部分，然后选择企业号码或 +E.164 备用号码作为正常呼叫路由失败时要使用的 PSTN 故障转移。

步骤 5 单击保存。

配置用户配置文件

通过用户配置文件将通用线路和通用设备模板分配给用户。为不同的用户组配置多个用户配置文件。您还可以为使用此服务配置文件的用户启用自预配置。

过程

-
- 步骤 1** 从 Cisco Unified CM 管理中，选择用户管理 > 用户设置 > 用户配置文件。
- 步骤 2** 单击**新增**。
- 步骤 3** 输入用户配置文件的**名称**和**描述**。
- 步骤 4** 分配通用设备模板以应用到用户的桌面电话、移动和桌面设备，以及远程目标/设备配置文件。
- 步骤 5** 分配通用线路模板以应用到此用户配置文件中的用户的电话线路。
- 步骤 6** 如果您希望此用户配置文件中的用户能够使用自预配置功能部署他们自己的电话，请执行以下操作：
- 选中**允许最终用户部署自己的电话**复选框。
 - 在**一旦最终用户拥有这么多电话即限制部署**字段中，输入允许用户部署的最大电话数量。最大值为 20。
 - 选中**允许预配置已分配给其他最终用户的电话**复选框以确定与此配置文件关联的用户是否有迁移或重新分配已归其他用户所有的设备的权限。默认情况下，此复选框未选中。
- 步骤 7** 如果您希望与此用户配置文件关联的 Cisco Jabber 用户能够使用 Mobile and Remote Access 功能，请选中**启用 Mobile and Remote Access** 复选框。
- 注释**
- 默认情况下，此复选框为选中状态。当取消选中此复选框时，**客户端策略**部分会被禁用，并且默认情况下会选中“无服务”客户端策略选项。
 - 此设置仅对使用 OAuth 刷新登录名的 Cisco Jabber 用户是必需的。非 Jabber 用户无需此设置即可使用 Mobile and Remote Access。Mobile and Remote Access 功能仅适用于 Jabber Mobile and Remote Access 用户，不适用于任何其他终端或客户端。
- 步骤 8** 为此用户配置文件分配 Jabber 策略。从**桌面客户端策略**以及**移动客户端策略**下拉列表中，选择以下选项之一：
- 无服务 — 此策略禁止访问所有 Cisco Jabber 服务。
 - 仅 IM & Presence — 此策略仅启用即时消息和在线状态功能。
 - IM & Presence、语音和视频呼叫 — 此策略为所有拥有音频和视频设备的用户启用即时消息、在线状态、语音邮件和会议功能。这是默认选项。
- 注释** Jabber 桌面客户包括 Cisco Jabber Windows 版本用户和 Cisco Jabber Mac 版本用户。Jabber 移动客户包括 Cisco Jabber iPad 和 iPhone 版本用户以及 Cisco Jabber Android 版本用户。
- 步骤 9** 如果想要此用户配置文件中的用户通过 Cisco Unified Communications Self Care 门户为分机移动或跨群集分机移动设置最长登录时间，选中**允许最终用户设置其分机移动最长登录时间**复选框。
- 注释** 允许最终用户设置其分机移动最长登录时间复选框默认未选中。
- 步骤 10** 单击**保存**。
-

配置头戴式耳机模板

遵照此程序，使用可应用于思科头戴式耳机的自定义设置配置头戴式耳机模板。您可以创建自定义模板，也可以使用系统定义的标准默认头戴式耳机模板。



注释 标准默认头戴式耳机配置模板是系统定义的模板。您可以将新的用户配置文件分配给标准的默认头戴式耳机模板，但不能编辑模板。默认情况下，所有用户配置文件都会分配给此模板。要取消与此模板的用户配置文件关联，必须将配置文件分配给新的模板。

过程

步骤 1 从 Cisco Unified CM 管理中，选择设备 > 头戴式耳机 > 头戴式耳机模板。

步骤 2 执行以下任一操作：

- 要编辑现有模板，请选择模板。
- 要创建新模板，请选择任何现有模板，然后单击**复制**。现有设置将应用到您的新模板。

步骤 3 为模板添加名称和说明。

步骤 4 在**型号和固件设置**下，指定您要应用到此模板的任何自定义头戴式耳机设置。要添加新设置，单击**添加按钮**并配置设置。

步骤 5 使用向上和向下箭头将要分配给此模板的用户配置文件移至**分配的用户配置文件**列表框。分配给这些配置文件的所有用户也将分配给此头戴式耳机模板。

步骤 6 单击**保存**。

步骤 7 使用**设为默认设置**按键可恢复为默认的模板设置。

步骤 8 单击**应用配置**。

对于标准默认头戴式耳机配置模板，**应用配置**按键对以下设备有效：

- 您添加到“分配的用户配置文件”列表的用户拥有的设备
- 匿名设备

对于自定义头戴式耳机配置模板，**应用配置**按键仅对您添加到**分配的用户配置文件**列表的用户拥有的设备有效。

配置 UC 服务

此程序用于配置您的用户将使用的 UC 服务连接。您可以为以下 UC 服务配置连接：

- 语音邮件

- 邮件存储
- 会议
- 目录
- IM and Presence Service
- CTI
- 视频会议计划门户
- Jabber 客户端配置 (jabber-config.xml)



注释 这些字段可能根据您配置的 UC 服务而有所不同。

过程

- 步骤 1** 从 Cisco Unified CM 管理中，选择**用户管理 > 用户设置 > UC 服务**。
- 步骤 2** 单击**新增**。
- 步骤 3** 从“UC 服务类型”下拉列表中，选择要配置的 UC 服务，然后单击**下一步**。
- 步骤 4** 选择**产品类型**。
- 步骤 5** 输入服务的**名称**。
- 步骤 6** 输入服务所在服务器的主机名或 **IP 地址**。
- 步骤 7** 完成**端口和协议**信息。
- 步骤 8** 配置其余字段。有关这些字段及其设置的帮助，请参阅联机帮助。字段选项根据您部署的 UC 服务而有所不同。
- 步骤 9** 单击**保存**。
- 步骤 10** 重复此程序，直到您预配置所需的所有 UC 服务。

注释 如果要将服务放在多台服务器上，请配置指向不同服务器的不同 UC 服务连接。例如，通过 IM and Presence Service 集中式部署，建议配置多个 IM and Presence Service，使其指向不同的 IM and Presence 节点。在配置所有 UC 连接后，您可以将其添加到服务配置文件。

配置服务配置文件

配置服务配置文件，其中包含要分配给使用该配置文件的最终用户的 UC 服务。

开始之前

您必须先设置 Unified Communications (UC) 服务，然后才能将其添加到服务配置文件。

过程

- 步骤 1 从 Cisco Unified CM 管理中，选择用户管理 > 用户设置 > 服务配置文件。
 - 步骤 2 单击新增。
 - 步骤 3 输入所选服务配置文件配置的名称。
 - 步骤 4 输入所选服务配置文件配置的说明。
 - 步骤 5 对于您希望成为此配置文件一部分的每个 UC 服务，为该服务分配主、辅助和三级连接。
 - 步骤 6 完成服务配置文件配置窗口中其余字段的设置。有关字段详细说明，请参阅联机帮助。
 - 步骤 7 单击保存。
-

配置功能组模板

功能组模板可帮助您非常快速地为预配置的用户配置电话、线路和功能，从而为您的系统部署提供帮助。如果要从公司 LDAP 目录同步用户，请使用希望用户从目录同步使用的用户配置文件和服务配置文件配置功能组模板。您也可以通过此模板为同步的用户启用 IM and Presence Service。

过程

- 步骤 1 在 Cisco Unified CM 管理中，选择用户管理 > 用户/电话添加 > 功能组模板。
 - 步骤 2 单击新增。
 - 步骤 3 输入功能组模板的名称和说明。
 - 步骤 4 如果您想要使用本地群集作为所有使用此模板的用户的主群集，请选中主群集复选框。
 - 步骤 5 选中为 **Unified CM IM and Presence** 启用用户复选框，以允许使用此模板的用户交换即时消息和在线状态信息。
 - 步骤 6 从下拉列表中，选择一个服务配置文件和用户配置文件。
 - 步骤 7 填写功能组模板配置窗口中的其余字段。请参阅联机帮助中的字段说明。
 - 步骤 8 单击保存。
-

下一步做什么

关联功能组模板与 LDAP 目录同步，以便将模板中的设置应用到同步的最终用户。

配置默认凭证策略

此程序用于配置应用到新预配置用户的群集范围的默认凭证策略。您可以为以下每种凭证类型应用单独的凭证策略：

- 应用程序用户密码
- 最终用户密码
- 最终用户 PIN

过程

步骤 1 配置凭证策略的设置：

- 从 Cisco Unified CM 管理中，选择**用户管理 > 用户设置 > 凭证策略**。
- 执行以下任一操作：
 - 单击**查找**并选择一个现有的凭证策略。
 - 单击**新增**以创建新的凭证策略。
- 如果您希望系统检查是否有容易遭受攻击的密码（例如 ABCD 或 123456），请选中**检查常用密码**复选框。
- 填写**凭证策略配置**窗口中的字段。有关这些字段及其设置的帮助，请参阅联机帮助。
- 单击**保存**。
- 如果要为其他凭证类型之一创建不同的凭证策略，请重复这些步骤。

步骤 2 将凭证策略应用到凭证类型之一：

- 从 Cisco Unified CM 管理中，选择**用户管理 > 用户设置 > 凭证策略默认设置**。
- 选择要应用凭证策略的凭证类型。
- 从**凭证策略**下拉框中，选择要应用到此凭证类型的凭证策略。例如，您可以选择您创建的凭证策略。
- 在**更改凭证**和**确认凭证**字段中输入默认密码。用户必须在下次登录时输入这些密码。
- 配置**凭证策略默认配置**窗口中的其余字段。有关这些字段及其设置的帮助，请参阅联机帮助。
- 单击**保存**。
- 如果要为其他凭证类型之一分配凭证策略，请重复这些步骤。



注释

对于单个用户，您还可以从该用户的**最终用户配置**窗口或**应用程序用户配置**窗口分配策略到特定的用户凭证。单击凭证类型（密码或个人识别码）旁边的**编辑凭证**按钮以打开该用户凭证的**凭证配置**设置。



第 29 章

配置 LDAP 同步

- [LDAP 同步概述，第 285 页](#)
- [LDAP 同步前提条件，第 286 页](#)
- [LDAP 同步配置任务流程，第 286 页](#)

LDAP 同步概述

轻型目录访问协议 (LDAP) 同步可帮助为您的系统设置和配置最终用户。LDAP 同步期间，系统会将用户和关联的用户数据列表从外部 LDAP 目录导入 Unified Communications Manager 数据库。您还可以在导入时配置您的最终用户。



注释 Unified Communications Manager 支持 LDAPS（通过 SSL 的 LDAP），但不支持通过 StartTLS 的 LDAP。确保您将 LDAP 服务器证书作为 Tomcat-Trust 上传到 Unified Communications Manager。

有关受支持的 LDAP 目录的信息，请参阅《Cisco Unified Communications Manager 和 IM and Presence Service 的兼容性值表》。

LDAP 同步会通告以下功能：

- **导入最终用户**—您可以在初始系统设置期间使用 LDAP 同步将用户列表从公司 LDAP 目录导入 Unified Communications Manager 数据库。如果您已预先配置了功能组模板、用户配置文件、服务配置文件、通用设备和线路模板等项目，可以将配置应用到您的用户，并在同步过程中分配配置的目录号码和目录 URI。LDAP 同步过程将导入用户和用户特定数据列表，并应用您设置的配置模板。



注释 一旦发生初始同步，您将无法编辑 LDAP 同步。

- **计划的更新**—您可以将 Unified Communications Manager 配置为按计划的时间间隔与多个 LDAP 目录同步，以确保定期更新数据库且用户数据为最新。

- **验证最终用户**—您可以将系统配置为针对 LDAP 目录而不是 Cisco Unified Communications Manager 数据库验证最终用户密码。LDAP 验证使得公司能够为最终用户分配一个适用于所有公司应用程序的密码。此功能不适用于 PIN 或应用程序用户密码。
- **针对思科移动和远程访问客户端及终端的目录服务器用户搜索**—即使在企业防火墙外部运行，您也可以搜索公司目录服务器。启用此功能后，用户数据服务 (UDS) 将充当代理，并将用户搜索请求发送到公司目录，而不是发送到 Unified Communications Manager 数据库。

LDAP 同步前提条件

先决任务

从 LDAP 目录导入最终用户之前，请完成以下任务：

- 配置用户访问权限。决定要将哪个访问控制组分配给用户。对于许多部署而言，默认组即已足够。如果您需要自定义您的角色和组，请参阅《管理指南》的“管理用户访问”一章。
- 配置默认情况下应用于新的预配置用户的凭证策略的默认凭证。
- 如果要从 LDAP 目录同步用户，请确保设置了一个功能组模板，其中包含要分配给用户电话和电话分机的用户配置文件、服务配置文件以及通用线路和设备模板设置。



注释 对于您希望将其数据同步到您的系统的用户，请确保他们在 Active Directory 服务器上的电子邮件 ID 字段是唯一的条目或留空。

LDAP 同步配置任务流程

执行以下任务以从外部 LDAP 目录提取用户列表并将其导入 Cisco Unified Communications Manager 数据库。



注释 如果您已同步 LDAP 目录一次，仍可以从外部 LDAP 目录同步新项目，但无法在 Cisco Unified Communications Manager 中将新配置添加到 LDAP 目录同步。在这种情况下，您可以使用批量管理工具和菜单，例如“更新用户”或“插入用户”。请参阅《Cisco Unified Communications Manager 批量管理指南》。

过程

	命令或操作	目的
步骤 1	激活 Cisco DirSync 服务，第 287 页	登录到 Cisco Unified 功能配置并激活 Cisco DirSync 服务。

	命令或操作	目的
步骤2	启用 LDAP 目录同步，第 287 页	在 Unified Communications Manager 中启用 LDAP 目录同步。
步骤3	创建 LDAP 过滤器，第 288 页	可选。如果希望 Unified Communications Manager 只同步公司 LDAP 目录中的一部分用户，请创建 LDAP 过滤器。
步骤4	配置 LDAP 目录同步，第 288 页	配置 LDAP 目录同步的设置，例如字段设置、LDAP 服务器位置、同步计划以及访问控制组、功能组模板和主分机的分配。
步骤5	配置企业目录用户搜索，第 291 页	可选。配置系统以用于企业目录服务器用户搜索。请遵照此程序配置系统中的电话和客户端，以对企业目录服务器而不是数据库执行用户搜索。
步骤6	配置 LDAP 验证，第 291 页	可选。如果要使用 LDAP 目录进行最终用户密码验证，请配置 LDAP 验证设置。
步骤7	自定义 LDAP 协议服务参数，第 292 页	可选。配置可选的 LDAP 同步服务参数。对于大多数部署而言，默认值已足够。

激活 Cisco DirSync 服务

执行以下程序可在 Cisco Unified 功能配置中激活 Cisco DirSync 服务。如果要同步公司 LDAP 目录中的最终用户设置，必须激活此服务。

过程

- 步骤1 从 Cisco Unified 功能配置中，选择工具 > 服务激活。
- 步骤2 从服务器下拉列表中，选择发布方节点。
- 步骤3 在目录服务下，单击 **Cisco DirSync** 单选按钮。
- 步骤4 单击保存。

启用 LDAP 目录同步

如果要为 Unified Communications Manager 配置为从公司 LDAP 目录同步最终用户设置，请执行此程序。



注释 如果您已同步 LDAP 目录一次，仍可以从外部 LDAP 目录同步新用户，但无法在 Unified Communications Manager 中将新配置添加到 LDAP 目录同步。您还不能向基础配置项目（如功能组模板或用户配置文件）添加编辑。如果已经完成一个 LDAP 同步，并且想要添加具有不同设置的用户，则可以使用批量管理菜单，例如“更新用户”或“插入用户”。

过程

- 步骤 1** 在 Cisco Unified CM 管理中，选择系统 > **LDAP** > **LDAP 系统**。
- 步骤 2** 如果您希望 Unified Communications Manager 从 LDAP 目录导入用户，选中从 **LDAP 服务器** 启用同步复选框。
- 步骤 3** 从 **LDAP 服务器类型** 下拉列表中，选择您公司使用的 LDAP 目录服务器类型。
- 步骤 4** 在用户 **ID** 的 **LDAP 属性** 下拉列表中，选择您希望 Unified Communications Manager 为最终用户配置窗口中的用户 **ID** 字段同步的公司 LDAP 目录属性。
- 步骤 5** 单击保存。

创建 LDAP 过滤器

您可以创建 LDAP 过滤器以将 LDAP 同步范围限制为 LDAP 目录中的部分用户。将 LDAP 过滤器应用于 LDAP 目录时，Unified Communications Manager 只会导入 LDAP 目录中与过滤器匹配的用户。



注释 您配置的 LDAP 过滤器必须符合 RFC4515 中规定的 LDAP 搜索过滤器标准。

过程

- 步骤 1** 在 Cisco Unified CM 管理中，选择系统 > **LDAP** > **LDAP 过滤器**。
- 步骤 2** 单击新增以创建新的 LDAP 过滤器。
- 步骤 3** 在过滤器名称文本框中，输入您的 LDAP 过滤器的名称。
- 步骤 4** 在过滤器文本框中，输入过滤器。过滤器最多可包含 1024 个 UTF-8 字符，且必须括在括号中 ()。
- 步骤 5** 单击保存。

配置 LDAP 目录同步

此程序用于将 Unified Communications Manager 配置为与 LDAP 目录同步。通过 LDAP 目录同步，您可以将最终用户数据从外部 LDAP 目录导入 Unified Communications Manager 数据库，以便其显示

在“最终用户配置”窗口中。如果您具有带通用线路和设备模板的设置功能组模板，可以将设置自动分配给新预配置的用户及其分机。



提示 如果要分配访问控制组或功能组模板，则可以使用 LDAP 过滤器将导入限制为具有相同配置要求的用户组。

过程

步骤 1 从 Cisco Unified CM 管理中，选择系统 > **LDAP** > **LDAP 目录**。

步骤 2 请执行以下步骤之一：

- 单击**查找**并选择现有的 LDAP 目录。
- 单击**新增**以创建新的 LDAP 目录。

步骤 3 在 **LDAP 目录配置**窗口中，输入以下内容：

- a) 在 **LDAP 配置名称**字段中，为 LDAP 目录分配唯一的名称。
- b) 在 **LDAP 管理员判别名字段**中，输入具有 LDAP 目录服务器访问权限的用户 ID。
- c) 输入并确认密码详细信息。
- d) 在 **LDAP 用户搜索空间**字段中，输入搜索空间详细信息。
- e) 在**用户同步的 LDAP 自定义过滤器**字段中，选择**仅限用户**或者**用户和组**。
- f) （可选）。如果要导入限制为满足特定配置文件的部分用户，请从**适用于组的 LDAP 自定义过滤器**下拉列表中选择 LDAP 过滤器。

步骤 4 在 **LDAP 目录同步计划**字段中，创建 Unified Communications Manager 用于同外部 LDAP 目录同步数据的计划。

步骤 5 填写**要同步的标准用户**字段部分。对于每个最终用户字段，选择 LDAP 属性。同步过程会将 LDAP 属性的值分配给 Unified Communications Manager 中的最终用户字段。

步骤 6 如果您正在部署 URI 拨号，请确保分配用于用户主目录 URI 地址的 LDAP 属性。

步骤 7 在**要同步的自定义用户**字段部分，输入具有所需 LDAP 属性的自定义用户字段名称。

步骤 8 要将导入的最终用户分配给所有导入的最终用户通用的访问控制组，请执行以下操作：

- a) 单击**添加到访问控制组**。
- b) 在弹出窗口中，单击要分配给所导入最终用户的每个访问控制组对应的复选框。
- c) 单击**添加选定项**。

步骤 9 如果要分配功能组模板，从**功能组模板**下拉列表中选择模板。

注释 只有在最终用户第一次未显示时，才会将用户与所分配的功能组模板同步。如果现有功能组模板被修改且为关联的 LDAP 执行了完全同步，则修改内容不会更新。

步骤 10 如果要对导入的电话号码应用掩码以分配主分机，请执行以下操作：

- a) 选中**应用掩码到同步的电话号码**以为插入的用户创建新线路复选框。
- b) 输入**掩码**。例如，如果导入的电话号码是 8889945，则掩码 11XX 会创建一个主分机 1145。

步骤 11 如果要从目录号池分配主分机，请执行以下操作：

- a) 选中如果未根据同步的 **LDAP** 电话号码创建新线路，请从池列表分配一条新线路复选框。
- b) 在 **DN 池开始**和 **DN 池结束**文本框中，输入要从中选择主分机的目录号码范围。

步骤 12 （可选）如果要创建 Jabber 设备，请在“Jabber 终端预配置”部分中，从下列下拉列表中选择一个所需的 Jabber 设备进行自动预配置：

- 适用于 Android 的 Cisco 双模 (BOT)
- Cisco Dual Mode for iPhone (TCT)
- Cisco Jabber 平板电脑版 (TAB)
- Cisco Unified Client Services Framework (CSF)

注释 写回到 **LDAP** 选项可让您将选中的主目录号码从 Unified CM 写回到 LDAP 服务器。可用于写回的 LDAP 属性包括：**telephoneNumber**、**ipPhone** 和 **mobile**。

步骤 13 在 **LDAP 服务器信息**部分，输入 LDAP 服务器的主机名或 IP 地址。

步骤 14 如果想使用 TLS 创建到 LDAP 服务器的安全连接，则选中**使用 TLS**复选框。

步骤 15 单击**保存**。

步骤 16 要完成 LDAP 同步，请单击**立即执行完全同步**。否则，您可以等待预定的同步。



注释 在 LDAP 中删除用户时，他们会在 24 小时后自动从 Unified Communications Manager 中删除。此外，如果为以下任何设备将已删除用户配置为移动用户，则这些非活动的设备也将自动删除：

- 远程目标配置文件
- 远程目标配置文件模板
- 移动智能客户端
- CTI 远程设备
- Spark 远程设备
- Nokia S60
- Cisco Dual Mode for iPhone
- IMS 集成移动 (基本)
- 运营商集成的移动
- 适用于 Android 的 Cisco 双模

配置企业目录用户搜索

此程序用于配置系统中的电话和客户端，以对企业目录服务器而不是数据库执行用户搜索。

开始之前

- 确保您选择用于 LDAP 用户搜索的主、辅和第三服务器均可通过网络连接到 Unified Communications Manager 订阅方节点。
- 依次选择系统 > **LDAP** > **LDAP 系统**，从 **LDAP 系统配置**窗口的**LDAP 服务器类型**下拉列表配置 LDAP 服务器的类型。

过程

步骤 1 在 Cisco Unified CM 管理中，选择系统 > **LDAP** > **LDAP 搜索**。

步骤 2 要使用企业 LDAP 目录服务器执行用户搜索，选中**启用企业目录服务器用户搜索**复选框。

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

步骤 4 单击**保存**。

注释 要在 OpenLDAP 服务器中搜索表示为会议室对象的会议室，请将自定义过滤器配置为 `(objectClass=inetOrgPerson)(objectClass=rooms)`。这将允许 Cisco Jabber 客户端按名称搜索会议室并拨打与聊天室关联的号码。

如果 OpenLDAP 服务器中针对会议室对象配置了 **givenName**、**sn**、**mail**、**displayName** 或 **telephonenumber** 属性，会议室将可搜索。

配置 LDAP 验证

如果要启用 LDAP 验证，请执行此程序，以便根据公司 LDAP 目录中分配的密码对最终用户密码进行验证。此配置仅适用于最终用户密码，不适用于最终用户 PIN 或应用程序用户密码。

过程

步骤 1 在 Cisco Unified CM 管理中，选择系统 > **LDAP** > **LDAP 验证**。

步骤 2 选中**对最终用户使用 LDAP 验证**复选框以使用 LDAP 目录进行用户验证。

步骤 3 在 **LDAP 管理员判别名字段**中，输入具有 LDAP 目录访问权限的 LDAP 管理员的用户 ID。

步骤 4 在**确认密码**字段中，输入 LDAP 管理器的密码。

步骤 5 在 **LDAP 用户搜索库**字段中，输入搜索条件。

步骤 6 在 **LDAP 服务器信息**部分，输入 LDAP 服务器的主机名或 IP 地址。

步骤 7 如果想使用 TLS 创建到 LDAP 服务器的安全连接，则选中**使用 TLS**复选框。

步骤 8 单击保存。

下一步做什么

[自定义 LDAP 协议服务参数，第 292 页](#)

自定义 LDAP 协议服务参数

执行此程序可配置自定义 LDAP 协议的系统级设置的可选服务参数。如果不配置这些服务参数，Unified Communications Manager 将应用 LDAP 目录集成的默认设置。对于参数说明，在用户界面中单击参数名称。

您可以使用服务参数自定义以下设置：

- 协议的最大数—默认值为 20。
- 主机的最大数—默认值为 3。
- 主机出现故障时的重试延迟（秒）—主机故障的默认值为 5。
- **HotList** 出现故障时的重试延迟（分钟）—hostlist 故障的默认值为 10。
- **LDAP** 连接超时（秒）—默认值为 5。
- 延迟同步开始时间（分钟）—默认值为 5。
- 用户客户映射审核时间

过程

步骤 1 从 Cisco Unified CM 管理中，选择系统 > 服务参数。

步骤 2 从服务器下拉列表框中，选择发布方节点。

步骤 3 从服务下拉列表框选择 **Cisco DirSync**。

步骤 4 配置 Cisco DirSync 服务参数的值。

步骤 5 单击保存。



第 30 章

使用批量管理工具预配置用户和设备

- [批量管理工具概述，第 293 页](#)
- [批量管理工具前提条件，第 294 页](#)
- [批量管理工具任务流程，第 294 页](#)

批量管理工具概述

批量管理工具 (BAT) 是一个基于 web 的应用程序，可用来批量处理 Unified Communications Manager 数据库中的事务。BAT 可用于同时添加、更新或删除大量类似的电话、用户或端口。



注释 “批量管理”菜单仅在 Unified Communications Manager 服务器的第一个节点上可见。

Cisco 批量预配置服务 (BPS) 管理和维护通过 Cisco Unified CM 管理的“批量管理”菜单提交的所有作业。您可以从 Cisco Unified 功能配置启动这项服务。您只需在 Unified Communications Manager 的第一个节点上激活 Cisco 批量预配置服务。

您可以使用 BAT 执行以下操作：

- 成批添加、更新或删除大量电话
- 定义常见电话属性以添加一组新电话
- 创建新的 BAT 电话模板
- 添加一组新用户并将用户关联到电话和其他 IP 电话设备
- 从 BAT 电子表格创建用户 CSV 数据文件
- 创建 CSV 数据文件以批量添加电话和用户
- 将一组电话和用户添加到 Unified Communications Manager 数据库和目录

批量管理工具前提条件

- 配置用户和服务配置文件

批量管理工具任务流程

过程

	命令或操作	目的
步骤 1	添加电话到数据库，第 295 页	您使用 BAT 将电话和其他 IP 电话设备批量添加到 Unified Communications Manager 数据库。
步骤 2	创建新的 BAT 电话模板，第 295 页	您可以创建新的 BAT 电话模板。
步骤 3	使用 BAT 电子表格创建电话 CSV 数据文件，第 299 页	您可以使用设计为与 BAT 配合使用的 .xls 电子表格将新电话或 IP 电话设备添加到系统。
步骤 4	使用文本编辑器创建自定义电话文件格式，第 302 页	您可以使用文本编辑器为 CSV 数据文本文件创建自定义电话文件格式。
步骤 5	将电话插入到 Unified Communications Manager，第 303 页	您可以将电话、Cisco VGC 电话、CTI 端口或 H.323 客户端添加到 Unified Communications Manager 数据库中。
步骤 6	添加用户，第 304 页	您可以使用 BAT 添加一组新用户，以及将用户与电话和其他 IP 电话设备关联。
步骤 7	从 BAT 电子表格创建用户 CSV 数据文件，第 305 页	您可以提供在 BAT 电子表格中将新用户添加到 Unified Communications Manager 数据库，然后将其转换为 CSV 数据文件的详细信息。
步骤 8	将用户插入到 Unified Communications Manager 数据库，第 306 页	可以使用 CSV 数据文件将一组用户添加到 Unified Communications Manager 数据库。
步骤 9	添加电话和用户文件格式，第 307 页	您可以使用 CSV 数据文本文件添加电话和用户文件格式。在创建 CSV 数据文件后，需要关联文件格式与 CSV 数据文本文件。
步骤 10	将电话和用户插入到 Unified Communications Manager，第 308 页	您可以将一组电话和用户添加到 Unified Communications Manager 数据库和目录。

添加电话到数据库

使用 BAT 将电话和其他 IP 电话设备批量添加到 Unified Communications Manager 数据库时，您可以为每部电话添加多个线路、服务和快速拨号。您还可以添加 CTI 端口和 H.323 客户端。

您有两个选项用于创建电话的 CSV 数据文件：

- 使用 BAT 电子表格 (BAT.xlt) 并将数据导出为 CSV 格式
- 使用文本编辑器创建 CSV 格式的文本文件（适用于有经验的用户）

过程

步骤 1 选择批量管理 > 电话 > 电话模板。

此时将显示查找并列出电话模板窗口。

步骤 2 创建 CSV 数据文件以插入电话模板。

执行下列选项之一：

- a) 使用 BAT 电子表格创建 CSV 数据文件。
- b) 使用文本编辑器创建 CSV 数据文件如下：
 1. 选择批量管理 > 电话 > 电话文件格式 > 创建文件格式。
 2. 使用文本编辑器，然后遵循您想要使用的文件格式，创建电话的 CSV 数据文件。
 3. 选择批量管理 > 电话 > 电话文件格式 > 添加文件格式以将文本文件格式与 CSV 数据文件关联。

步骤 3 选择批量管理 > 电话 > 验证电话。

步骤 4 选择批量管理 > 电话 > 插入电话以将电话记录插入到 Unified Communications Manager 数据库中。

创建新的 BAT 电话模板

您可以创建新的 BAT 电话模板。在创建电话模板后，可以添加线路、服务和快速拨号。

过程

步骤 1 选择批量管理 > 电话 > 电话模板。

步骤 2 单击新增。此时将显示添加新的电话模板窗口。

步骤 3 从电话类型下拉列表中选择要为其创建模板的电话型号。单击下一步。

步骤 4 从选择设备协议下拉列表中选择设备协议。单击下一步。

此时将显示电话模板配置窗口，其中包含所选设备类型的字段和默认条目。

步骤 5 在模板名字段中输入模板名称。

名称最多可以包含 50 个字母数字字符。

步骤 6 在“设备信息”区域中，输入此批次的公共电话设置。

有些电话型号和设备类型没有表中列出的全部属性。有关所有属性的信息，请参阅电话型号文档。

步骤 7 为此 BAT 电话模板输入所有设置后，单击**保存**。

当状态指示事务已完成时，可以添加线路属性。

在 BAT 模板中添加或更新电话线路

您可以将一条或多条线路添加到 BAT 模板，或者更新现有线路。用于 BAT 模板的按键模板确定您可以添加或更新的线路数量。您可以创建有多条线路的主电话模板。然后，您可以使用标准模板添加具有一条线路或不超过标准模板中最多线路数的电话。这一批的所有电话或用户设备配置文件都将使用您选择的设置。

思科建议您对线路模板值使用字母数字字符，因此如果指定数字，则存在与实际目录号码冲突的几率。这还可避免与呼叫代答组号码和呼叫暂留号码等功能冲突。

BAT 模板显示的最大线路数取决于您创建 BAT 电话模板时选择的型号和按键模板。对于某些 Cisco Unified IP 电话型号，您还可以将 Cisco Unified IP 电话服务和快速拨号添加到模板。

过程

步骤 1 查找您要在其中添加线路的电话模板。

步骤 2 在电话模板配置窗口的关联信息区域中单击**线路 [1] 添加新目录号码**。

此时将显示**线路模板配置**窗口。

步骤 3 为线路设置输入或选择适当的值。

步骤 4 单击**保存**。

步骤 5 要添加任何其他线路的设置，请重复**步骤 2**，第 296 页至**步骤 4**，第 296 页。

如果从**线路模板配置**窗口右上角的**相关链接**下拉列表框中选择**返回查找/列出**，将显示**查找并列出行路模板**窗口。

a) 要查找现有线路模板，请输入适当的搜索条件，然后单击**查找**。

b) 要添加新的线路模板，请单击**新增**。

在 BAT 模板中添加或更新 IP 服务

您可为在 BAT 模板中直接包含此功能的 Cisco Unified IP 电话型号预订 Cisco Unified IP 电话服务。要为用户或电话批量预订 IP 服务，IP 服务必须具有通用服务参数，且通过电话模板预订。无法批量预订具有唯一服务参数的 IP 服务。对于具有唯一参数的服务，请使用 CSV 文件。

过程

- 步骤 1 找到要在其中添加 IP 服务的电话模板。
- 步骤 2 在电话模板配置窗口的**相关信息**区域中单击**添加新 SURL**。
此时将显示一个弹出窗口。在此窗口中，您可以订阅可用的 Cisco Unified IP 电话服务。
- 步骤 3 在**选择服务**下拉列表框中，选择要为所有电话预订的服务。**服务说明**框将显示所选服务的详细信息。
- 步骤 4 单击**下一步**。
- 步骤 5 在**服务名称**字段中，按需要修改服务的名称。
- 步骤 6 将选择的服务关联到模板，或将更多服务添加到模板。
 - a) 要将这些电话服务关联到电话模板，请单击**保存**。
 - b) 要添加更多服务，请重复**步骤 3**，[第 297 页](#)到**步骤 6**，[第 297 页](#)。
 - c) 要将所有服务添加到模板，请单击**更新**。在为选择的模板添加或更新服务后，继续下一步。
- 步骤 7 关闭弹出窗口。

在 BAT 模板中添加或更新快速拨号

如果电话按键模板提供了快速拨号按键，则您可使用 BAT 模板为电话和 Cisco VGC 电话添加和更新快速拨号。BAT 模板所使用的电话按键模板将决定可用快速拨号按键的数量。

过程

- 步骤 1 查找您要在其中添加快速拨号的电话模板。
- 步骤 2 从电话模板配置窗口，执行下列操作之一：
 - a) 在**相关信息**区域单击**添加新的快速拨号**。
 - b) 从窗口右上角的**相关链接**下拉列表框中选择**添加/更新快速拨号**。此时将显示一个弹出窗口。在此窗口中，可指定 CiscoUnifiedIPPhones 快速拨号按键和扩展模块。
- 步骤 3 在**快速拨号设置**区域的**号码**字段，输入电话号码，包括任何接入代码或长距离代码。

注释 输入电话号码时，其后可输入强制授权码 (FAC)/客户码 (CMC)，如适用。您可按顺序输入电话号码、FAC、CMC 或用逗号 (,) 隔开。快速拨号可能包括任何 PIN、密码或呼叫连接后作为 DTMF 位数发送的任何其他位数。如果您在通过快速拨号连接时需要暂停，您可输入一个或多个逗号 (,)，其中每个逗号代表一次 2 秒的暂停。DTMF 位数将在呼叫连接后发送，系统将输入与逗号个数对应的暂停时长。
- 步骤 4 在**标签**字段，输入一个快速拨号号码对应的标签。
- 步骤 5 在**缩拨设置**区域，您可为适用 IP 电话模式设置缩略快速拨号。重复**步骤 3**，[第 297 页](#)。
- 步骤 6 单击**保存**。

BAT 将在模板中插入快速拨号设置，弹出窗口将关闭。

在 BAT 模板中添加或更新忙灯字段

如果电话按键模板提供快速拨号按键，您可以在 BAT 模板中为电话和 Cisco VGC 电话添加和更新忙灯字段。BAT 模板使用的电话按键模板决定可用的 BLF 快速拨号按键数量。

过程

步骤 1 查找您要在其中添加快速拨号的电话模板。

步骤 2 在电话模板配置窗口中，执行下列操作之一：

- a) 在相关信息区域中单击添加新的 **BLF 快速拨号**。
- b) 从窗口右上角的**相关链接**下拉列表中选择添加/更新忙灯字段快速拨号。

此时将显示一个弹出窗口。在此窗口中，可指定 CiscoUnifiedIPPhones 和扩展模块的忙灯字段快速拨号 (BLF SD) 按钮。

步骤 3 在快速拨号设置区域中，在目标字段中输入目标，包括任何接入代码或长途代码。

步骤 4 从下拉列表中选择目录号码。可以单击**查找搜索**目录号码。

步骤 5 在标签字段中，输入与 BLF SD 号码对应的标签。

步骤 6 单击**保存**。

BAT 在模板中插入 BLF SD 设置，弹出窗口关闭。

在 BAT 模板中添加或更新忙灯字段定向呼叫暂留

如果电话按键模板提供快速拨号按键，您可以在 BAT 模板中为电话和 Cisco VGC 电话添加和更新忙灯字段 (BLF) 定向呼叫暂留。BAT 模板使用的电话按键模板决定可用的 BLF 定向呼叫暂留按键数量。

过程

步骤 1 找到要为其添加 BLF 快速定向呼叫暂留的电话模板。

步骤 2 在电话模板配置窗口中，执行下列操作之一：

- a) 在相关信息区域中单击添加新的 **BLF 定向呼叫暂留**。
- b) 从窗口右上角的**相关链接**下拉列表框中选择添加/更新 **BLF 定向呼叫暂留**。

此时将显示一个弹出窗口。在此窗口中，可以为 CiscoUnifiedIP 电话和扩展模块指定 BLF 定向呼叫暂留按键。

步骤 3 在未分配的忙灯字段/定向呼叫暂留设置区域中，从下拉列表中选择目录号码。可以单击**查找搜索**目录号码。

步骤 4 在标签字段中，输入与 BLF 定向呼叫暂留号码对应的标签。

步骤 5 单击**保存**。

BAT 在模板中插入 BLF 定向呼叫暂留设置，弹出窗口关闭。

在 BAT 模板中添加或更新内部通信模板

您可以将一个或多个内部通信模板添加到 BAT 模板，或更新 BAT 模板中现有的内部通信模板。BAT 模板使用的按键模板决定您可以添加或更新的线路数量。您可以创建有多条线路的标准电话模板。然后，您可以使用标准模板添加具有一条线路或不超过标准模板中最多线路数的电话。这一批的所有电话或用户设备配置文件都将使用您为内部通信模板选择的设置。

我们建议您对内部通信模板使用字母数字字符，因此如果指定数字，则存在与实际目录号码冲突的几率。这还可避免与呼叫代答组号码和呼叫暂留号码等功能冲突。

BAT 模板显示的最大线路数取决于您创建 BAT 电话模板时选择的型号和按键模板。对于某些 Cisco Unified IP 电话型号，您还可以将 Cisco Unified IP 电话服务和快速拨号添加到模板。

过程

步骤 1 找到要为其添加内部通信模板的电话模板。

步骤 2 在电话模板配置窗口的相关信息区域中单击**内部通信 [1] - 添加新内部通信**。

此时将显示**内部通信模板配置**窗口。

步骤 3 为内部通信模板设置输入或选择适当的值。

步骤 4 单击**保存**。

BAT 会将内部通信模板添加到电话模板配置。

步骤 5 要添加任何其他内部通信模板的设置，请重复**步骤 2**，[第 299 页](#)至**步骤 4**，[第 299 页](#)。

如果从**内部通信模板配置**窗口右上角的**相关链接**下拉列表框中选择**返回查找/列出**，将显示**查找并列出内部通信目录号码**窗口。

注释 如果从**内部通信模板配置**窗口右上角的**相关链接**下拉列表框中选择**返回查找/列出**，将显示**查找并列出内部通信目录号码**窗口。

a) 单击**查找**然后输入适当的搜索条件，以查找现有内部通信目录号码。

b) 在**查找并列出内部通信目录号码**窗口中单击**新增**，以添加新的内部通信目录号码。

使用 BAT 电子表格创建电话 CSV 数据文件

使用 BAT 电子表格创建 CSV 数据文件。您可以在电子表格中定义文件格式，然后 BAT 电子表格将使用该数据文件格式显示 CSV 数据文件的字段。



注释 如果在其中一个字段中输入逗号，则导出为 BAT 格式时，BAT.xlt 会将该字段条目用双引号括住。

如果在 BAT 电子表格中输入了空行，系统会将该空行视为文件结束，不会将空行后所输入的数据转换为 BAT 格式。

在添加 CTI 端口时可以使用虚拟 MAC 地址选项。此选项以虚拟 MAC 地址的形式为每个 CTI 端口提供唯一的设备名称，您以后可以使用 Cisco Unified Communications Manager 管理或 UnifiedCM 自动注册电话工具手动更新。不要对 H.323 客户端、VGC 电话或 VGC 虚拟电话使用虚拟 MAC 地址选项。

虚拟 MAC 地址选项会自动生成以下格式的虚拟 MAC 地址：

XXXXXXXXXXXX

其中 X 表示任意 12 个字符的十六进制（0-9 和 A-F）数字。



注意 您在 BAT 电子表格中为电话定义的线路和快速拨号数量，不得超过在 BAT 电话模板中定义的数量，否则在尝试插入 CSV 数据文件和 BAT 模板时会发生错误。

BAT 电子表格中所有字段的编辑完成后，您可将内容导出到 CSV 格式的数据文件。系统将为导出的 CSV 格式的数据文件分配默认文件名：

<tabname>-<timestamp>.txt

其中 <tabname> 表示您创建的输入文件类型，比如电话，<timestamp> 表示创建该文件的精确日期和时间。

您可在导出的文件保存到本地工作站后对 CSV 格式的数据文件重命名。



注释 您无法将包含逗号（例如 abcd,e.txt）的 CSV 文件名上传到 Unified Communications Manager 服务器。

过程

步骤 1 要打开 BAT 电子表格，找到并双击 BAT.xlt 文件。

步骤 2 提示时，单击启用宏以使用电子表格功能。

步骤 3 要显示电话选项，请单击电子表格底部的电话选项卡。

步骤 4 从下列一种设备类型对应的单选按键：

您选择的设备类型决定 BAT 电子表格中数据的验证条件。

- 电话
- CTI 端口
- H.323 客户端

- VGC 电话
- VGC 虚拟电话
- Cisco IP Communicator 电话

电子表格显示可用于所选设备的选项。例如，在选择电话时，电话线路数量和快速拨号数量的对应字段将会显示。

步骤 5 为每部电话选择要出现在 BAT 电子表格中的设备和线路字段。执行以下操作：

- a) 单击**创建文件格式**。
- b) 要选择设备字段，请单击**设备字段框**中的设备字段名称，然后单击箭头将该字段移至**所选设备字段框**中。

CSV 数据文件必须包含 **MAC 地址/设备名称和说明**；因此，这些字段始终保持选中状态。

提示 要选择列表中一个范围内的项目，请按住 **Shift** 键。要选择随机字段名称，请按住 **Ctrl** 键并单击字段名称。

- c) 单击**线路字段框**中的线路字段名称，然后单击箭头将该字段移至**所选线路字段框**中。

提示 要更改**所选线路和设备框**中项目的顺序，请选择一个项目，然后使用向上和向下箭头在列表中上下移动字段。

- d) 此时将显示一条消息，询问您是否要覆盖现有 CSV 格式。单击**创建**可修改 CSV 数据文件格式。
- e) 单击**确定**。
所选字段的新列将在 BAT 电子表格中按您指定的顺序显示。

步骤 6 向右滚动以找到**电话线路数量框**，然后输入电话的线路数量。

注释 您输入的线路数量不得超过 BAT 模板中配置的线路数量。

步骤 7 对于电话，必须在**快速拨号的最大数量框**中输入快速拨号按键的数量。

注释 您输入的快速拨号数量不得超过 BAT 模板中配置的快速拨号数量。

输入数量后，将显示每个快速拨号号码的列。

步骤 8 在**BLF 快速拨号的最大数量框**中输入忙灯字段 (BLF) 快速拨号按键的数量。
输入数量后，将显示每个 BLF 快速拨号号码的列。

步骤 9 在电子表格中的每一行输入个人电话数据。

完成所有必填字段以及任何相关的可选字段。每个列标题将指定字段的长度，并指明属于必填字段还是可选字段。请参阅联机帮助中的电话字段说明。

步骤 10 如果未输入每部电话的 MAC 地址，请选中**创建虚拟 MAC 地址**复选框。

注意 不要对 H.323 客户端、VGC 电话或 VGC 虚拟电话使用虚拟 MAC 地址选项。

步骤 11 要将数据从 BAT Excel 电子表格传输到 CSV 格式的数据文件，请单击**导出为 BAT 格式**。

提示 有关如何读取已导出的 CSV 数据文件的信息，请单击“在 BAT 的插入电话窗口中查看样例文件”链接。

系统以默认文件名：`<tabname>-<timestamp>.txt` 将该文件保存到您选择的本地工作站上的文件夹。

使用文本编辑器创建自定义电话文件格式

您可以使用文本编辑器为 CSV 数据文本文件创建自定义电话文件格式。

过程

步骤 1 选择批量管理 > 电话 > 电话文件格式 > 创建文件格式。

步骤 2 单击新增。

步骤 3 在格式名称字段中，输入此自定义格式的名称。

步骤 4 选择在自定义文件格式中显示的字段。执行以下操作：

- a) 要选择设备字段，请单击设备字段框中的设备字段名称，然后单击箭头将该字段移至所选设备字段框中。

CSV 数据文件必须包含 **MAC 地址/设备名称和说明**；因此，这些字段始终保持选中状态。

提示 要选择列表中一个范围内的项目，请按住 **Shift** 键。要选择随机字段名称，请按住 **Ctrl** 键并单击字段名称。

- b) 单击线路字段框中的线路字段名称，然后单击箭头将该字段移至所选线路字段框中。

- c) 单击内部通信 DN 字段框中的内部通信 DN 字段名，然后单击箭头键将字段移到所选内部 DN 字段顺序框。

提示 您可以更改所选线路字段、所选设备字段和所选内部 DN 字段顺序框中项目的顺序。选择一个项目，使用上下箭头可将该字段在列表中上移或下移。

步骤 5 在 IP 电话服务最大值区域中，输入以下字段的最大值：

- 快速拨号的最大数量
- BLF 快速拨号的最大数量
- BLF 定向呼叫暂留的最大数量
- IP 电话服务的最大数量
- IP 电话服务参数的最大数量

步骤 6 单击保存。

自定义文件格式的名称在查找并列出电话文件格式窗口的文件格式名称中显示。

将电话插入到 Unified Communications Manager

在 Unified Communications Manager 数据库中插入电话记录时，定义目标 CSV 数据文件和插入电话记录的方式。选择所列操作的任意组合以覆盖现有电话记录，或者选择在上传过程中插入记录：

- 在添加新的快速拨号前删除所有现有快速拨号
- 在添加新的 BLF 快速拨号前删除所有现有 BLF 快速拨号
- 在添加新的 BLF 定向呼叫暂留前删除所有现有 BLF 定向呼叫暂留
- 在添加新的已开通服务前删除所有现有已开通服务



注释 电话记录在插入前必须进行验证。



注释 BAT 预期目录号码的“目录号码 URI”字段采用以下格式：

目录号码 1 上的 URI 1、目录号码 1 上的 URI 1 路由分区、目录号码 1 上的 URI 1 是目录号码 1 的主 URI。

您可以使用虚拟 MAC 地址选项。添加 CTI 端口时，此选项以虚拟 MAC 地址的形式提供每个 CTI 端口唯一的设备名称，您可在稍后使用 Unified Communications Manager 管理或 UnifiedCM 自动注册电话工具手动更新这些地址。不要对 H.323 客户端、VGC 电话或 VGC 虚拟电话使用虚拟 MAC 地址选项。

虚拟 MAC 地址选项会自动生成以下格式的虚拟 MAC 地址：

XXXXXXXXXXXX

其中 X 表示任意 12 个字符的十六进制（0-9 和 A-F）数字。

开始之前

- 您必须拥有所添加的设备对应的 Unified Communications Manager 批量管理 (BAT) 电话模板。您可以选择数据文件上传的目标和方法。电话记录在插入前必须进行验证。
- 您必须拥有逗号分隔值 (CSV) 格式、其中包含电话或其他 IP 电话设备唯一详细信息的数据文件。

过程

步骤 1 选择批量管理 > 电话 > 插入电话。

步骤 2 指定您上传的电话记录的文件格式类型。

- a) 要插入使用自定义文件格式的电话记录，请单击插入电话特定详细信息单选按钮并继续步骤 3，第 304 页和步骤 5，第 304 页。
- b) 要插入使用所有详细信息选项生成的导出电话文件中的电话记录，请单击插入电话所有详细信息单选按钮。

步骤 3 在**文件名**下拉列表框中，选择为此特定批量事务创建的 CSV 数据文件。接下来，选中**允许使用自定义文件更新电话**复选框，以允许使用所选的自定义文件更新电话。

步骤 4 选中**覆盖现有配置**复选框，以使用要插入的文件中包含的信息覆盖现有电话设置。接下来，选中要在上传过程中执行的上传操作旁边的复选框。

在选中**覆盖现有配置**复选框后，以下上传操作将对所选项目启用。

- 在添加新的快速拨号前删除所有现有快速拨号。
- 在添加新的 BLF 快速拨号前删除所有现有 BLF 快速拨号。
- 在添加新的 BLF 定向呼叫暂留前删除所有现有 BLF 定向呼叫暂留。
- 在添加新的已开通服务前删除所有现有已开通服务。

注释 不要选中在上传时将这些记录附加到 CSV 数据文件中的现有记录的复选框。

步骤 5 对于特定详细信息选项，在**电话模板名**下拉列表中，选择您为此类批量事务创建的 BAT 电话模板。

注意 如果没有在 CSV 数据文件中输入单独的 MAC 地址，则必须选中**创建虚拟 MAC 地址**复选框。您可以稍后手动更新此信息。跳至**步骤 8，第 304 页**。如果您在数据输入文件中提供 MAC 地址或设备名称，请不要选择此选项。

如果您不知道分配给用户的电话的 MAC 地址，请选择此选项。插入电话后，将注册该设备的 MAC 地址。

步骤 6 在**作业信息**区域中输入作业说明。

步骤 7 选择插入方法。执行下列操作之一：

- a) 单击**立即运行**以立即插入电话记录。
- b) 单击**稍后运行**以在稍后插入电话记录。

步骤 8 单击**提交**以创建插入电话记录的作业。

使用**作业配置**窗口来计划或激活此作业。

下一步做什么

如果插入的电话属于 Cisco Unified Mobile Communicator 类型，则在插入作业完成后必须重置设备。可使用**批量管理 > 电话 > 重置/重新启动电话选项**重置电话。

添加用户

必须创建 CSV 数据文件才可使用 BAT 电子表格向 Unified Communications Manager 数据库批量添加用户。对于其应用程序需要 CTI 端口（例如 CiscoIPSoftPhone）的用户，BAT 可以将 CTI 端口关联到现有用户。

过程

步骤 1 创建一个逗号分隔值 (CSV) 数据文件，为您要添加的每个用户定义单独的值。

步骤 2 使用 BAT 在 Unified Communications Manager 数据库中插入用户。

从 BAT 电子表格创建用户 CSV 数据文件

您可以提供在 BAT 电子表格中将新用户添加到 Unified Communications Manager 数据库，然后将其转换为 CSV 数据文件的详细信息。



注释 如果在 BAT 电子表格中输入了空行，系统会将该空行视为文件结束，不会将空行后所输入的数据转换为 BAT 格式。

在 BAT 电子表格中完成字段编辑以添加用户后，可将内容导出为 CSV 格式的数据文件。系统将为导出的 CSV 格式的数据文件分配默认文件名：

`<tabname>-<timestamp>.txt`

其中 `<tabname>` 表示您创建的输入文件类型，比如电话，`<timestamp>` 表示创建该文件的精确日期和时间。

您可在导出的文件保存到本地工作站后对 CSV 格式的数据文件重命名。如果在其中一个字段中输入逗号，则导出为 BAT 格式时，BAT.xlt 会将该字段条目用双引号括住。



注释 包含逗号的 CSV 文件名（例如 `abcd,e.txt`）无法上传到 Unified Communications Manager 服务器。

过程

步骤 1 要打开 BAT 电子表格，找到并双击 BAT.xlt 文件。

步骤 2 提示时，单击**启用宏**以使用电子表格功能。

步骤 3 要添加用户，请单击电子表格底部的**用户**选项卡。

步骤 4 完成所有必填字段以及任何相关的可选字段。每个列标题将指定字段的长度，并指明属于必填字段还是可选字段。

在每一行中，如联机帮助文件中所述提供信息。

- 如果用户有多个设备，设备名称应重复，每个设备一次。
- 要输入将关联到新用户的其他设备名称，请在**受控设备数量**文本框中输入一个值。

注释 您可以将所有设备（包括 CTI 端口、ATA 端口和 H.323 客户端）与用户关联。

步骤 5 要输入将关联到新用户的其他设备名称，请在**受控设备数量**文本框中输入一个值。

步骤 6 单击**导出为 BAT 格式**以将数据从 BAT Excel 电子表格转换为 CSV 格式的数据文件。

系统会将该文件以默认文件名 <tablename>-<timestamp>.txt 保存到 C:\XLSDDataFiles，或使用浏览将该文件保存到其他现有文件夹。

提示 有关如何读取已导出的 CSV 数据文件的信息，请单击“在 BAT 的插入用户窗口中查看**样例文件**”链接。

下一步做什么

必须将 CSV 数据文件上传到 Unified Communications Manager 数据库服务器的第一个节点，以便 BAT 能够访问该数据文件。

将用户插入到 Unified Communications Manager 数据库

可以使用 CSV 数据文件将一组用户添加到 Unified Communications Manager 数据库。为插入用户而在 CSV 文件中输入的字段值会覆盖用户模板中提供的值。



注意 如果凭证策略启用了“检查简单密码”，并且用户模板中的密码为用户 ID，则用户 ID 不满足简单密码的必要条件时，通过 BAT 插入用户可能会失败。

用户可以使用 BAT 插入，主分机配置而不为受控设备选择任何设备。要实现这一点，必须在使用 BAT 插入用户之前预填充 Unified Communications Manager 中的目录号码。以下步骤概述预填充 DN 的过程：

1. 创建要与目录号码页面中用户的主分机关联的 DN 范围。
2. 创建主分机已配置（应与 DN 的填充内容相同）的 BAT 模板。
3. 使用 BAT 插入用户（如以下程序中所示）

开始之前

您必须拥有保存为 UTF-8 编码格式的 CSV 数据文件，该文件中包含用户名、受控设备名称和目录号码。可使用以下方法之一创建 CSV 数据文件：

- 已转换成 CSV 格式的 BAT 电子表格
- 生成用户数据导出文件的导出实用工具



注释 使用导出的 BAT 文件插入用户时，对于在多个文件中导出的某些用户，您可能会收到错误，表明“用户 ID 已存在”。例如，第一条线路经理列表和用户列表可能均包含相同的经理用户 ID。

过程

步骤 1 选择批量管理 > 用户 > 插入用户。

步骤 2 在文件名字段中，选择为此批量事务创建的 CSV 数据文件。

步骤 3 如果 CSV 数据文件使用导出实用程序创建，请选中使用导出用户创建的文件复选框。

步骤 4 从用户模板名下拉列表中选择要用于此插入的用户模板。

注释 Unified Communications Manager 数据库中应存在“用户配置文件”、“受控设备名称”和“目录号码”。受控设备名称应完整输入。如果其仅包含 MAC 地址，则 BAT 将显示不存在的设备错误。

步骤 5 在作业信息区域中输入作业说明。

步骤 6 选择插入方法。执行下列操作之一：

- a) 单击**立即运行**立即插入用户记录。
- b) 单击**稍后运行**以后插入用户记录。

步骤 7 要创建插入用户记录的作业，请单击**提交**。

要计划和/或激活此作业，请使用**批量管理**主菜单中的“作业计划程序”选项。

使用 BAT 电子表格添加电话及用户

创建 CSV 数据文件以批量添加电话和用户。

过程

步骤 1 要打开 BAT 电子表格，找到并双击 BAT.xlt 文件。

您可以下载 BAT.xlt 文件。

步骤 2 提示时，单击**启用宏**以使用电子表格功能。

步骤 3 在电子表格底部单击**电话-用户**选项卡。

步骤 4 执行[使用 BAT 电子表格创建电话 CSV 数据文件](#)，第 299 页中的步骤 4 至 10。

添加电话和用户文件格式

您可以使用 CSV 数据文本文件添加电话和用户文件格式。在创建 CSV 数据文件后，需要关联文件格式与 CSV 数据文本文件。在关联文件格式与 CSV 文件后，每个字段的名称在 CSV 数据文中显示为第一条记录。您可以使用此信息检查是否按正确顺序输入每个字段的值。

开始之前

必须创建 CSV 数据文件，定义要更新的每个用户的个别值。

使用文本编辑器创建 CSV 数据文件时，您创建用于在文本文件中输入值的文件格式。在文本文件中输入值时按照文件格式指定的顺序输入。

过程

步骤 1 选择 **批量管理 > 电话和用户 > 电话和用户文件格式 > 指定文件格式**。

此时将显示添加文件格式配置窗口。

步骤 2 在 **文件名** 字段中，选择您为此事务创建的 CSV 文本文件。

步骤 3 在 **格式文件名** 字段中，选择您为此类批量事务创建的文件格式。

步骤 4 要创建将匹配的文件格式与 CSV 数据文件关联的作业，请单击 **提交**。

步骤 5 要计划和/或激活此作业，请使用 **批量管理** 主菜单中的“作业计划程序”选项。

注释 添加文件格式时，会自动添加用户字段。

将电话和用户插入到 Unified Communications Manager

您可以将一组电话和用户添加到 Unified Communications Manager 数据库和目录。



注释 电话记录在插入前必须进行验证。

您可以使用虚拟 MAC 地址选项。添加 CTI 端口时，此选项以虚拟 MAC 地址的形式提供每个 CTI 端口唯一的设备名称，您可在稍后使用 Unified Communications Manager 管理或 UnifiedCM 自动注册电话工具手动更新这些地址。不要对 H.323 客户端、VGC 电话或 VGC 虚拟电话使用虚拟 MAC 地址选项。

虚拟 MAC 地址选项会自动生成以下格式的虚拟 MAC 地址：

XXXXXXXXXXXX

其中 X 表示任意 12 个字符的十六进制（0-9 和 A-F）数字。

开始之前

1. 创建一个逗号分隔值 (CSV) 数据文件，以定义单独的值用于要插入的每个电话及用户。您可以使用 BAT 电子表格 (BAT.xls) 创建 CSV 数据文件以添加电话及用户，或创建 CSV 格式的自定义文本文件以添加电话及用户组合。
2. 将文件格式与 CSV 数据文件关联。
3. 验证电话及用户记录。

过程

步骤 1 选择**批量管理 > 电话和用户 > 插入电话和用户**。

步骤 2 在**文件名字段**中，选择为此批量事务创建的 CSV 数据文件。

步骤 3 在**电话模板名字段**中，选择用于此事务的 BAT 电话模板。

注意 如果没有在 CSV 数据文件中输入单独的 MAC 地址，则必须选中**创建虚拟 MAC 地址复选框**。您可以稍后手动更新此信息。如果您在数据输入文件中提供 MAC 地址或设备名称，请不要选择此选项。

如果您不知道分配给用户的电话的 MAC 地址，请选择此选项。插入电话后，将注册该设备的 MAC 地址。

步骤 4 在**用户模板名字段**中，选择用于此事务的 BAT 用户模板。

步骤 5 在**作业信息区域**中输入作业说明。

步骤 6 选择插入方法。执行下列操作之一：

- a) 单击**立即运行**立即插入电话及用户。
- b) 单击**稍后运行**以后插入电话及用户。

步骤 7 要创建插入电话和用户记录的作业，请单击**提交**。

要计划和激活此作业，请使用**批量管理**主菜单中的“**作业计划程序**”选项。



第 **V** 部分

预配置终端

- [配置终端，第 313 页](#)
- [配置 CAPF，第 321 页](#)
- [配置 TFTP 服务器，第 337 页](#)
- [通过激活码激活设备，第 345 页](#)
- [配置自动注册，第 359 页](#)
- [配置自我预配置，第 367 页](#)



第 31 章

配置终端

- [终端预配置默认设置，第 313 页](#)
- [终端预配置默认设置前提条件，第 313 页](#)
- [终端预配置默认设置任务流程，第 314 页](#)
- [配置设备默认设置，第 314 页](#)
- [配置企业电话，第 317 页](#)
- [Self Care 自助门户，第 318 页](#)

终端预配置默认设置

使用这部分中的信息配置终端设备，以及如何将用户与终端关联。

Unified Communications Manager 包含您可以在添加终端之前配置的一组设备默认值。如果预先设置了这些设备的默认设置，则在预配置新用户和设备时，将根据应用的设置自动配置。

以下是终端预配置的两个默认配置：

- [配置设备默认设置](#)
- [配置企业电话设置](#)

终端预配置默认设置前提条件

确认为终端注册配置的端口。从 Cisco Unified CM 管理，转至 **系统 > Cisco Unified CM**，选择服务器并确认配置的端口设置。



注释 在大多数情况下，无需更改端口的默认设置。

终端预配置默认设置任务流程

完成以下任务流程以配置系统的设备。

过程

	命令或操作	目的
步骤 1	配置设备默认设置，第 314 页	您可以更改应用到自动注册到 Unified Communications Manager 节点的设备的默认设置。每种类型的设备都有一组特定的默认值。
步骤 2	配置设备配置文件，第 317 页	可选。您可以配置设备配置文件包含一组与用于的特定设备关联的属性。
步骤 3	配置默认设备配置文件，第 315 页	您可以配置默认设备配置文件，以便电话在用户登录到没有用户设备配置文件的电话上时使用。
步骤 4	在默认设备配置文件中配置软键模板，第 315 页	可选。您可以将默认设备配置文件添加到软键模板。
步骤 5	配置企业电话，第 317 页	您可以配置适用于同一群集中所有电话的基本企业电话设置。

配置设备默认设置

更新设备默认设置

使用此程序配置设备默认设置，以让您分配默认固件加载、默认设备池、软键模板和注册方法：自动注册或激活代码。

开始之前

在更新设备默认设置之前，请执行下列适用于您系统的任务：

- 将设备的新固件文件添加到 TFTP 服务器。
- 如果使用设备默认值分配目录中不存在的固件加载，这些设备将无法加载分配的固件。
- 配置新设备池。如果设备是电话，请配置新电话模板。

过程

步骤 1 在 Cisco Unified CM 管理中，选择设备 > 设备设置 > 设备默认设置。

步骤 2 在设备默认配置窗口中，修改您要更新的设备类型的适用设置，然后单击**保存**。要查看字段说明，请参阅联机帮助。

- 加载信息
- 设备池
- 电话模板

步骤 3 单击显示在设备名称左侧的**重置**图标，以重置群集中所有节点上该类型的所有设备，并加载新的默认设置到的所有设备上。

如果不重置所有设备，则只有节点上自动注册的新设备会被配置为更新后的默认值。

配置默认设备配置文件

当用户登录到其没有用户设备配置文件的电话时，电话将采用默认设备配置文件。

默认设备配置文件包括设备类型（电话）、用户区域设置、电话按键模板、软键模板以及多级优先和预占 (MLPP) 信息。

过程

步骤 1 从 **Cisco Unified CM** 管理窗口，选择设备 > 设备设置 > 默认设备配置文件。

步骤 2 在默认设备配置文件配置窗口中，从设备配置文件类型 下拉列表中选择适当的 Cisco Unified IP Phone。

步骤 3 单击下一步。

步骤 4 从设备协议下拉列表中，选择适当的协议。

步骤 5 单击下一步。

步骤 6 配置默认设备配置文件配置窗口中的字段。请参阅联机帮助，了解有关字段及其配置选项的更多信息。

步骤 7 单击**保存**。

在默认设备配置文件中配置软键模板

Cisco Unified Communications Manager 包含用于呼叫处理和应用程序的标准软键模板。创建自定义软键模板时，复制标准模板并根据需要进行修改。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**设备 > 设备设置 > 软键模板**。

步骤 2 执行以下步骤以创建新的软键模板；否则，继续下一步。

- a) 单击**新增**。
- b) 选择默认模板，然后单击**复制**。
- c) 在**软键模板名称**字段中输入模板的新名称。
- d) 单击**保存**。

步骤 3 执行以下步骤以将软键添加到现有模板。

- a) 单击**查找**并输入搜索条件。
- b) 选择所需的现有模板。

步骤 4 选中**默认软键模板**复选框以将此软键模板指定为默认软键模板。

注释 如果将软键模板指定为默认软键模板，则除非先删除默认指定，否则无法删除该模板。

步骤 5 从右上角的**相关链接**下拉列表中选择**配置软键布局**，然后单击**转至**。

步骤 6 从**选择要配置的呼叫状态**下拉列表中，选择想要软键显示的呼叫状态。

步骤 7 从**未选择的软键**列表中，选择要添加的软键，然后单击向右箭头将该软键移至**所选软键**列表。使用向上和向下箭头更改新软键的位置。

步骤 8 要在其他呼叫状态中显示软键，请重复上一步。

步骤 9 单击**保存**。

步骤 10 请执行以下任务之一：

- 如果您修改了已与设备关联的模板，请单击**应用配置**以重新启动设备。
- 如果您创建了新的软键模板，请将模板与设备关联，然后重新启动设备。有关详细信息，请参阅将软键模板添加到通用设备配置和将软键模板与电话关联部分。

下一步做什么

您可以从以下配置窗口之一的“软键模板”下拉框中选择相应的模板，将自定义的软键模板应用到设备：

- 电话配置
- 通用设备模板
- BAT 模板
- 通用设备配置
- 设备配置文件
- 缺省设备配置文件

- UDP 配置文件

配置设备配置文件

设备配置文件包含一组与特定设备关联的属性。您可以将您创建的设备配置文件与最终用户关联，以便使用 Cisco Extension Mobility 功能。

过程

- 步骤 1 从 **Cisco Unified CM 管理** 窗口，选择 **设备 > 设备设置 > 设备配置文件**。
- 步骤 2 在 **设备配置文件配置** 窗口中，从 **设备配置文件类型** 下拉列表中选择适当的 Cisco Unified IP 电话。
- 步骤 3 单击 **下一步**。
- 步骤 4 从 **设备协议** 下拉列表中，选择适当的协议。
- 步骤 5 单击 **下一步**。
- 步骤 6 从 **电话按键模板** 下拉列表，选择一个模板。
- 步骤 7 （可选）从 **软键模板** 下拉列表，选择一个软键模板。
- 步骤 8 配置 **设备配置文件配置** 窗口中的字段。请参阅联机帮助，了解有关字段及其配置选项的更多信息。
- 步骤 9 单击 **保存**。

注释 有关使用设备配置文件设置 Cisco Extension Mobility 的详细信息，请参阅《Cisco Unified Communications Manager 版本 12.5(1)SU1 功能配置指南》。

配置企业电话

配置企业电话设置

此程序用于配置网络中的电话可以使用的默认“产品特定配置”字段设置。

在此窗口中设置的参数也可能会出现在“通用电话配置文件配置”窗口以及各设备的“电话配置”窗口中。如果在另外这些窗口中也设置了相同的参数，则应用设置的优先顺序确定如下：1) “电话配置”窗口设置，2) “通用电话配置文件”窗口设置，3) “企业电话配置”窗口设置。

过程

- 步骤 1 从 **Cisco Unified CM 管理** 中，选择 **系统 > 企业电话配置**。
- 步骤 2 填写 **产品特定配置布局** 部分的必填字段。

要查看所有企业电话参数的说明，请单击“企业电话参数配置”窗口中的 ? 按键。

步骤 3 完成“企业电话配置”窗口中其余字段的设置。有关这些字段及其设置的帮助，请参阅联机帮助。

配置电话

执行以下步骤以手动将电话添加到 Unified Communications Manager 数据库。如果使用自动注册，则无需执行这些步骤。如果使用自动注册，Unified Communications Manager 将自动添加电话并分配目录号码。

过程

步骤 1 从 Cisco Unified CM 管理中，选择设备 > 电话。

步骤 2 单击新增。

步骤 3 从电话类型下拉列表中，选择适当的 Cisco IP 电话型号。

步骤 4 单击下一步。

步骤 5 从选择设备协议下拉列表中选择以下协议之一：

- SCCP
- SIP

步骤 6 单击下一步。

步骤 7 配置电话配置窗口中的字段。请参阅联机帮助，了解有关字段及其配置选项的更多信息。

注释 在安全性配置文件中配置的 CAPF 设置与“电话配置”窗口中显示的“证书权限代理功能”设置相关。必须为涉及厂商预装证书 (MIC) 或本地有效证书 (LSC) 的证书操作配置 CAPF 设置。有关在“电话配置”窗口中更新的 CAPF 设置如何影响安全性配置文件 CAPF 设置的详细信息，请参阅《Cisco Unified Communications Manager 安全指南》。

步骤 8 单击保存。

步骤 9 在关联区域中，单击线路 [1] - 添加新目录号码。

步骤 10 在目录号码字段中，输入您希望与电话关联的目录号码。

步骤 11 单击保存。

Self Care 自助门户

自助门户可用作部署过程的一部分，用于预配置和配置新电话：

- 最终用户可以使用门户自定义其电话的功能和设置。
- 通过设备激活代码自行激活，用户可以选择使用门户激活自己的电话。
- 用户还可以使用门户自助预配置自己的一号通远程目标。

最终用户需要通过访问权限进行设置，然后才能使用门户。有关如何设置门户的详细信息，请参阅《*Cisco Unified Communications Manager* 功能配置指南》的“自助门户”一章。



第 32 章

配置 CAPF

- [证书权限代理功能 \(CAPF\) 概述，第 321 页](#)
- [CAPF 前提条件，第 323 页](#)
- [证书权限代理功能配置任务流程，第 324 页](#)
- [CAPF 管理任务，第 332 页](#)
- [CAPF 系统相互作用和限制，第 333 页](#)

证书权限代理功能 (CAPF) 概述

Cisco 证书权限代理功能 (CAPF) 是颁发当地有效证书 (LSC) 和验证 Cisco 终端的 Cisco 专有服务。CAPF 服务在 Unified Communications Manager 上运行并执行以下任务：

- 颁发 LSC 给受支持的 Cisco Unified IP 电话。
- 在启用混合模式时验证电话。
- 升级电话的现有 LSC。
- 检索电话证书进行查看和故障排除。

CAPF 运行模式

您可以配置 CAPF 在以下模式下运行：

- Cisco 权限代理功能—Unified Communications Manager 上的 CAPF 服务颁发由 CAPF 服务本身签名的 LSC。该模式为默认模式。
- 在线 CA—使用此选项可让外部在线 CA 签名电话的 LSC。CAPF 服务会自动连接到外部 CA。提交 CSR 后，CA 将会签名并自动返回 CA 签名的 LSC。
- 离线 CA—如果要使用离线外部 CA 为电话签名 LSC，则使用此选项。此选项要求您手动下载 LSC，将其提交到 CA，然后在就绪后上传 CA 签名的证书。



注释 如果您想要使用第三方 CA 签名 LSC，Cisco 建议使用**在线 CA**选项而不是**离线 CA**，因为该流程已自动化，所以要快得多并且不容易遇到问题。

CAPF 服务证书

安装 Unified Communications Manager 后，CAPF 服务将自动安装，并且生成 CAPF 特定的系统证书。应用安全性后，Cisco CTL 客户端会将证书复制到所有群集节点。

电话证书类型

Cisco 为电话使用以下 X.509v3 证书类型：

- 本地有效证书 (LSC)—在您执行与 Cisco 证书权限代理功能 (CAPF) 关联的必要任务后安装在受支持的电话上的证书。将设备安全模式配置为验证或加密后，LSC 保护 Unified Communications Manager 和电话之间的连接安全。



注释 对于在线 CA，LSC 有效性基于 CA，并且只要 CA 允许，就可以使用。

- 厂商预装证书 (MIC) — Cisco 厂商自动安装 MIC 到支持的电话型号中。厂商预装证书向 Cisco 证书权限代理功能 (CAPF) 验证以进行 LSC 安装。您不能覆盖或删除厂商预装证书。



注释 Cisco 建议您仅针对 LSC 安装使用厂商预装证书 (MIC)。Cisco 支持 LSC 验证与 Unified Communications Manager 的 TLS 连接。由于 MIC 根证书可能受损，配置电话使用 MIC 进行 TLS 验证或进行其他操作的客户要自行承担风险。思科不承担 MIC 受损产生的任何责任。

通过 CAPF 生成 LSC

配置 CAPF 后，在电话上添加所配置的身份验证字符串。密钥和证书交换在电话和 CAPF 之间进行，并会发生以下情况：

- 电话使用所配置的身份验证方法向 CAPF 验证自身身份。
- 电话生成公钥-私钥对。
- 电话通过签名消息前转公钥给 CAPF。
- 私钥仍在电话中，并且绝不会外泄。
- CAPF 签名电话证书，然后通过签名消息将证书发送给电话。



注释 请注意，电话用户可以退出电话上的证书操作或查看操作状态。



注释 设置于低优先级的密钥生成可让电话在进行该操作的同时正常运行。虽然证书生成期间电话功能正常，但增加的 TLS 流量会导致电话出现微小的呼叫处理中断；例如，在安装结束将证书写入闪存时可能出现音频卡顿。

CAPF 前提条件

在配置用于生成 LSC 的证书权限代理功能之前，请执行以下操作：

- 如果想要使用第三方 CA 签署您的 LSC，请在外部配置您的 CA。
- 计划如何验证您的电话。
- 在生成 LSC 之前，请确保拥有以下各项：
 - Unified Communications Manager 版本 12.5 或更高版本。
 - 对证书使用 CAPF 的终端（包括 Cisco IP 电话和 Jabber）。
 - Microsoft Windows Server 2012 和 2016。
 - 已配置域名服务 (DNS)。
- 在生成 LSC 之前，必须上传 CA 根证书和 HTTPS 证书。在安全的 SIP 连接期间，HTTPS 证书通过 CAPF-trust，而 CA 根证书则通过 CAPF-trust 和 CallManager 信任。互联网信息服务 (IIS) 会托管 HTTPS 证书。CA 根证书用于签署证书签名请求 (CSR)。

出现以下情况时，必须上传证书：

表 27: 上传证书的情况

场景	结果
CA 根证书和 HTTPS 证书相同。	上传 CA 根证书。
CA 根证书和 HTTPS 证书不同，且 HTTPS 证书由同一 CA 根证书颁发。	上传 CA 根证书。
中间 CA 和 HTTPS 证书不同，且由 CA 根证书颁发。	上传 CA 根证书。
CA 根证书和 HTTPS 证书不同，且由同一 CA 根证书颁发。	上传 CA 根证书和 HTTPS 证书。



注释 Cisco 强烈建议您在计划的维护窗口期间使用 CAPF，因为同时生成很多证书可能导致呼叫处理中断。

证书权限代理功能配置任务流程

完成这些任务以配置证书权限代理功能 (CAPF) 服务来为终端颁发 LSC:



注释 在重新生成或上传新的 CAPF 证书后，您无需重新启动 CAPF 服务。

过程

	命令或操作	目的
步骤 1	上传第三方 CA 的根证书	如果想要 LSC 经过第三方 CA 签名，请将 CA 根证书链上传到 CAPF-trust 存储区。否则，您可以跳过此任务。
步骤 2	上传证书颁发机构 (CA) 根证书 ，第 325 页	上传 CA 根证书到 Unified Communications Manager 信任存储区。
步骤 3	配置在线证书颁发机构设置 ，第 326 页	使用此程序生成电话 LSC 证书。
步骤 4	配置离线证书颁发机构设置	使用此程序可通过离线 CA 生成电话 LSC 证书。
步骤 5	激活或重新启动 CAPF 服务	在配置 CAPF 系统设置后，激活基本 CAPF 服务。
步骤 6	使用以下程序之一在 Unified Communications Manager 中配置 CAPF 设置： <ul style="list-style-type: none">在通用设备模板中配置 CAPF 设置，第 328 页通过批量管理更新 CAPF 设置，第 329 页配置电话的 CAPF 设置，第 331 页	使用以下选项之一将 CAPF 设置添加到电话配置： <ul style="list-style-type: none">如果尚未同步 LDAP 目录，请将 CAPF 设置添加到通用设备模板，并通过初始 LDAP 同步应用设置。使用批量管理工具可在一次操作中将 CAPF 设置应用到多部电话。您可以逐个电话应用 CAPF 设置。
步骤 7	设置保持连接计时器 ，第 331 页	(可选) 设置 CAPF 终端连接的保持连接值，以使其不会被防火墙超时。默认值为 15 分钟。

上传第三方 CA 的根证书

将 CA 根证书上传到 CAPF-trust 存储区，Unified Communications Manager 信任存储区使用外部 CA 签名 LSC 证书。



注释 如果您不想使用第三方 CA 签名 LSC，请跳过此任务。

过程

- 步骤 1 从 Cisco Unified OS 管理中，选择安全 > 证书管理。
- 步骤 2 单击上传证书/证书链。
- 步骤 3 从证书用途下拉列表，选择 **CAPF-trust**。
- 步骤 4 输入证书说明。例如，适用于外部 LSC 签名 CA 的证书。
- 步骤 5 单击浏览，导航至文件，然后单击打开。
- 步骤 6 单击上传。
- 步骤 7 重复此任务，将证书上传到 **callmanager-trust** 证书用途。

上传证书颁发机构 (CA) 根证书

上传群集范围证书，以将其分发至群机内的所有服务器。

过程

- 步骤 1 从 Cisco Unified OS 管理中，选择安全 > 证书管理。
- 步骤 2 单击上传证书/证书链。
- 步骤 3 从证书用途下拉列表，选择 **callmanager-trust**。
- 步骤 4 输入证书说明。例如，适用于外部 LSC 签名 CA 的证书。
- 步骤 5 单击浏览，导航至文件，然后单击打开。
- 步骤 6 单击上传。

重要事项 此备注适用于 14 SU2 及更高版本。

注释 对于任何根或中间 CA 证书，它应包括以下默认 X509 扩展名：

X509v3 Basic Constraints:

CA:TRUE, pathlen:0

X509v3 Key Usage:

Digital Signature, Certificate Sign

如果证书中缺少这些扩展名，TLS 连接将失败。

重要事项 此备注适用于 14 SU3 及更高版本，并且仅适用于 IPsec 证书。

注释 对于任何 CA 签名的 IPsec 证书，不应包括以下扩展名：

X509v3 Basic Constraints:

CA:TRUE

配置在线证书颁发机构设置

在 Unified Communications Manager 中使用此程序以通过在线 CAPF 生成电话 LSC。

过程

步骤 1 从 Cisco Unified CM 管理中，选择系统 > 服务参数。

步骤 2 从服务器下拉列表中，选择您要其中激活 Cisco 证书权限代理功能（活动）服务的节点。

步骤 3 从服务下拉列表中，选择 **Cisco 证书权限代理功能（活动）**。确认服务名称旁边显示“活动”一词。

步骤 4 从证书颁发者到终端下拉列表中，选择**在线 CA**。对于 CA 签名的证书，我们建议使用在线 CA。

步骤 5 在证书有效的持续时间（日）字段中，输入介于 1 到 1825 之间的数字以表示 CAPF 颁发的证书的有效天数。

步骤 6 在**在线 CA 参数**部分，设置以下参数，以便创建到“在线 CA”部分的连接。

- 在线 CA 主机名—主题名称或通用名称 (CN) 应与 HTTPS 证书的完全限定域名 (FQDN) 相同。

注释 主机名配置为与 Microsoft CA 上运行的 Internet Information Services (IIS) 托管的 HTTPS 证书通用名称 (CN) 相同。

- 在线 CA 端口—输入在线 CA 的端口号。例如，443
- 在线 CA 模板—输入模板的名称。Microsoft CA 将创建模板。

注释 仅当在线 CA 类型为 Microsoft CA 时，才会启用此字段。

- 在线 CA 类型—为终端证书的自动注册选择 Microsoft CA 或 EST 支持的 CA。
 - Microsoft CA - 当 CA 是 Microsoft CA 时，使用此选项向设备分配数字证书。

注释 Microsoft CA 不支持 FIPSS 启用模式。

- **重要事项** 从 14SU2 版开始支持。

EST 支持的 CA - 当 CA 支持自动注册的内置 EST 服务器模式时，使用此选项。

- 在线 CA 用户名—输入 CA 服务器的用户名。
- 在线 CA 密码—输入 CA 服务器用户名的密码。
- 证书注册配置文件标签—使用有效字符输入 EST 支持的 CA 的数字标识。

注释 仅当在线 CA 类型为 EST 支持的 CA 时，才会启用此字段。

步骤 7 完成其余的 CAPF 服务参数。单击参数名称可查看服务参数帮助系统。

步骤 8 单击保存。

步骤 9 重新启动 **Cisco 证书权限代理功能**以使更改生效。即会自动重新启动 Cisco 证书登记服务。

当前在线 CA 限制

- 如果 CA 服务器使用除英语之外的任何其他语言，则在线 CA 功能不工作。CA 服务器只能以英语响应。
- 在线 CA 功能不支持使用 CA 的 mTLS 验证。
- 使用在线 CA 进行 LSC 操作时，如果没有为 LSC 证书提供“数字签名”和“密钥加密”密钥使用情况，设备安全注册将失败。
- 使用在线 CA 进行 LSC 操作时，如果没有为 LSC 证书提供“数字签名”和“密钥加密”，设备安全注册将失败。

配置离线证书颁发机构设置

如果您决定使用离线 CA 生成电话 LSC 证书，请遵循此高级流程。



注释 离线 CA 选项比在线 CA 更费时，涉及许多手动步骤。如果在证书生成和传输过程中出现任何问题（例如，网络中断或电话重置），请重新启动此过程。

过程

步骤 1 从第三方证书颁发机构下载根证书链。

步骤 2 将根证书链上传到 Unified Communications Manager 中要求的信任（CallManager 信任 CAPF 信任）。

步骤 3 通过将证书颁发给终端服务参数设置为“离线 CA”，配置 Unified Communications Manager 使用离线 CA。

步骤 4 为您的电话 LSC 生成 CSR。

步骤 5 发送 CSR 到证书颁发机构。

步骤 6 从 CSR 那里获取签名的证书。

有关如何使用离线 CA 生成电话 LSC 的详细示例，请参阅 [CUCM 第三方 CA 签名 LSC 生成和导入配置](#)。

激活或重新启动 CAPF 服务

在配置 CAPF 系统设置后激活必要的 CAPF 服务。如果 CAPF 服务已激活，则重新启动。

过程

步骤 1 从 Cisco Unified 功能配置，选择工具 > 服务激活。

步骤 2 从服务器下拉列表中，选择发布方节点并单击前往。

步骤 3 从安全服务窗格中，选中适用的服务：

- **Cisco 证书登记服务**—如果您使用的是在线 CA，则选中此服务，否则请不要选中。
- **Cisco 证书权限代理功能**—如果未选中（已取消激活），则选中此服务。如果服务已激活，则重新启动。

步骤 4 如果您修改了任何设置，请单击保存。

步骤 5 如果 **Cisco 证书权限代理功能** 服务已选中（已激活），则重新启动：

- a) 从相关链接下拉列表中，选择控制中心 - 功能服务并单击前往。
- b) 在安全设置窗格中，选中 **Cisco 证书权限代理功能** 服务，然后单击重新启动。

步骤 6 完成以下程序，配置针对个别电话的 CAPF 设置。

- a) [在通用设备模板中配置 CAPF 设置，第 328 页](#)
 - b) [通过批量管理更新 CAPF 设置，第 329 页](#)
 - c) [配置电话的 CAPF 设置，第 331 页](#)
-

在通用设备模板中配置 CAPF 设置

使用此程序将 CAPF 设置配置为通用设备模板 通过功能组模板配置将模板应用于 LDAP 目录同步。模板中的 CAPF 设置适用于使用此模板的所有同步设备。



注释 您只能将通用设备模板添加到尚未同步的 LDAP 目录中。如果初始 LDAP 同步已进行，请使用批量管理来更新电话。有关详细信息，请参阅[通过批量管理更新 CAPF 设置，第 329 页](#)。

过程

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

步骤 2 执行以下任一操作：

- 单击**查找**并选择现有模板。
- 单击**新增**。

步骤 3 展开证书权限代理功能 (CAPF) 设置区域

步骤 4 在证书操作下拉列表中，选择**安装/升级**。

步骤 5 从身份验证模式下拉列表菜单中，为设备选择一个选项以验证自身身份。

步骤 6 如果选择使用身份验证字符串，请在文本框中输入**身份验证字符串**，或单击**生成字符串**以让系统为您生成字符串。

注释 如果设备本身未配置此字符串，身份验证会失败。

步骤 7 从其余字段，配置密钥信息。有关这些字段的帮助，请参阅联机帮助。

步骤 8 单击**保存**。

注释 确保您已使用在此程序中分配的相同身份验证方法配置了使用此模板的设备。否则，设备身份验证会失败。有关如何为电话配置身份验证的详细信息，请参阅电话文档。

步骤 9 将模板设置应用到使用此配置文件的设备。

- a) 将通用设备模板添加到功能组模板配置。
- b) 将功能组模板添加到未同步的 LDAP 目录配置。
- c) 完成 LDAP 同步。CAPF 设置会应用到所有已同步的设备。

有关配置功能部件组模板和 LDAP 目录的详细信息，请参阅[Cisco Unified Communications Manager 系统配置指南](#)的“配置最终用户”一节。

通过批量管理更新 CAPF 设置

使用批量管理的**更新电话**查询在一次操作中为许多现有电话配置 CAPF 设置和 LSC 证书。



注释 如果您尚未预配置电话，请使用批量管理的**插入电话**菜单，使用 CSV 文件中的 CAPF 设置预配置新电话。有关如何从 CSV 文件插入电话的详细信息，请参阅[Cisco Unified Communications Manager 批量管理指南](#)的“电话插入”一节了解详细信息。

确保使用您计划在此程序中添加的相同字符串和身份验证方法配置了您的电话。否则，您的电话将不会向 CAPF 进行验证。有关如何在电话上配置身份验证的详细信息，请参阅您的电话文档。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**批量管理 > 电话 > 更新电话 > 查询**。

步骤 2 使用过滤器选项将搜索限制为您要更新的电话，然后单击**查找**。

例如，使用**查找电话位置**下拉列表选择所有电话，其中 LSC 在特定日期之前或特定设备池中过期。

步骤 3 单击**下一步**。

步骤 4 从**注销/重置/重新启动**部分，选择**应用配置**单选按钮。当作业运行时，CAPF 更新将应用到所有更新了的电话。

步骤 5 在**证书权限代理功能 (CAPF) 信息**下，选中**证书操作**复选框。

步骤 6 从**证书操作**下拉列表中，选择**安装/升级**以使 CAPF 在电话上安装新的 LSC 证书。

步骤 7 从**身份验证模式**下拉列表中，选择您希望电话在 LSC 安装期间验证自身身份的方式。

注释 在电话上应配置相同的身份验证方法。

步骤 8 如果您选择**按验证字符串**作为**验证模式**，请完成以下步骤之一：

- 如果要对每个设备使用唯一的验证字符串，请选中**为每个设备生成唯一的验证字符串**。
- 在**验证字符串**文本框中输入字符串，如果想要对所有设备使用相同的验证字符串，则单击**生成字符串**。

步骤 9 完成**更新电话**窗口的**证书权限代理功能 (CAPF) 信息**部分中其余字段的设置。有关这些字段及其设置的帮助，请参阅联机帮助。

步骤 10 从**作业信息**部分，选择**立即运行**。

注释 如果想要在计划的时间运行作业，则选择**稍后运行**。有关计划作业的详细信息，请参阅[Cisco Unified Communications Manager 批量管理指南](#)中的“管理计划作业”一节。

步骤 11 单击**提交**。

注释 如果在此程序中没有选择**应用配置**选项，则为所有更新了的电话应用**电话配置**窗口中的配置。

配置电话的 CAPF 设置

使用此程序可为个人电话上的 LSC 证书配置 CAPF 设置。



注释 使用批量管理或同步 LDAP 目录将 CAPF 设置应用到大量电话。

使用您计划在此程序中添加的相同字符串和身份验证方法配置您的电话。否则，电话不会向 CAPF 验证自身身份。有关如何在电话上配置身份验证的详细信息，请参阅您的电话文档。

过程

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

步骤 2 单击 **查找** 并选择现有电话。 **电话配置** 页面将会显示。

步骤 3 导航至 **证书权限代理功能 (CAPF) 信息** 窗格。

步骤 4 从 **证书操作** 下拉列表中，选择 **安装/升级 CAPF** 以在电话上安装新的 LSC 证书。

步骤 5 从 **身份验证模式** 下拉列表中，选择您希望电话在 LSC 安装期间验证自身身份的方式。

注释 电话应配置为使用相同的身份验证方法。

步骤 6 如果您选择了 **按验证字符串**，则输入文本字符串或单击 **生成字符串** 以为您生成字符串。

步骤 7 在 **电话配置** 页的 **证书权限代理功能 (CAPF) 信息** 窗格的其余字段中输入详细信息。有关这些字段及其设置的帮助，请参阅联机帮助。

步骤 8 单击 **保存**。

设置保持连接计时器

使用此程序设置 CAPF - 终端连接的群集范围保持连接计时器，以使该连接不会被防火墙超时。计时器默认值为 15 分钟。在每个间隔后，CAPF 服务会发送保持连接信号给电话以使该连接保持接通状态。

过程

步骤 1 使用命令行界面以登录发布方节点。

步骤 2 运行 `utils capt keep_alive` CLI 命令。

步骤 3 输入 5 到 60（分钟）之间的数字，然后单击 **Enter**。

CAPF 管理任务

在配置 CAPF 并颁发 LSC 证书后，可以使用以下任务来定期管理 LSC 证书。

证书状态监控

您可将系统配置为自动监控证书状态。当证书接近到期时，系统将向您发送电子邮件，然后在过期后吊销证书。

有关如何配置证书监控检查的详细信息，请参阅“管理证书”一章中的[证书监控和吊销任务流程](#)。

运行过时的 LSC 报告

使用此程序从 Cisco Unified 报告运行过时的 LSC 报告。过时的 LSC 是为响应终端 CSR 而生成但未安装的证书，因为在安装过时的 LSC 之前，终端生成了新的 CSR。



注释 您还可以通过 在发布方节点上运行 `utils capf stale-lsc list` CLI 命令获取过时 LSC 证书的列表。

过程

- 步骤 1** 从 Cisco Unified 报告，选择系统报告。
- 步骤 2** 在左侧导航栏中，选择过时的 LSC。
- 步骤 3** 单击生成新报告。

查看待处理的 CSR 列表

使用此程序可查看待处理的 CAPF CSR 文件列表。所有 CSR 文件都有时间戳。

过程

- 步骤 1** 使用命令行界面以登录发布方节点。
- 步骤 2** 运行 `utils capf csr list` CLI 命令。
有时间戳的待处理 CSR 文件列表将会显示。

删除过时的 LSC 证书

使用此程序从系统中删除过时的 LSC 证书。

过程

- 步骤 1** 使用命令行界面以登录发布方节点。
- 步骤 2** 运行 `utils capf stale-lsc delete all` CLI 命令
系统将删除所有过时的 LSC 证书。

CAPF 系统相互作用和限制

功能	互动
验证字串	电话的 CAPF 验证方式，操作后在电话上必须输入相同的验证字符串，否则操作将失败。如果启用了 TFTP 已加密配置企业参数，并且您没有输入验证字符串，电话将出现故障并且无法恢复，直至在电话上输入匹配的验证字符串。
群集服务器凭证	Unified Communications Manager 群集中的所有服务器必须使用相同的管理员用户名和密码，以便 CAPF 能够验证群集中的所有服务器。
迁移安全电话	如果安全的电话被移至另一个群集，Unified Communications Manager 将不信任电话发送的 LSC 证书，因为它是由另一 CAPF 颁发的，而其证书不在 CTL 文件中。 要启用安全的电话以注册，请删除现有 CTL 文件。然后，您可以使用安装/升级选项来安装使用新的 CAPF 的新证书，并重置电话以使用新的 CTL 文件（或使用 MIC）。在移动电话之前，使用电话配置窗口 CAPF 部分的删除选项删除现有 LSC。

功能	互动
Cisco Unified 6900 系列、7900 系列、8900 系列和 9900 系列 IP 电话	<p>Cisco 建议升级 Cisco Unified 6900 系列、7900 系列、8900 系列和 9900 系列 IP 电话以使用 LSC 进行至 Unified Communications Manager 的 TLS 连接，并从 CallManager 信任存储区中删除 MIC 根证书以避免今后出现兼容性问题。请注意有些使用 MIC 进行至 Unified Communications Manager 的 TLS 连接的电话型号可能无法注册。</p> <p>管理员应该从 CallManager 信任存储区中删除以下 MIC 根证书：</p> <ul style="list-style-type: none">• CAP-RTP-001• CAP-RTP-002• Cisco_Manufacturing_CA• Cisco_Root_CA_2048
电源故障	<p>发生通信或电源故障时，以下信息适用。</p> <ul style="list-style-type: none">• 如果在证书安装期间电话发生通信故障，电话将以 30 秒为间隔尝试获取证书三次。您无法更改这些值。• 如果在电话尝试与 CAPF 进行会话期间发生电源故障，电话将使用存储在闪存中的验证模式，亦即，电话重新启动后，不能从 TFTP 服务器加载新的配置文件。证书操作完成后，系统将清除闪存中的值。
证书加密	<p>从 Unified Communications Manager 版本 11.5 (1) SU1 开始，CAPF 服务颁发的所有 LSC 证书都使用 SHA-256 算法签名。因此，IP 电话 7900/8900/9900 系列型号支持 SHA-256 签名的 LSC 证书和外部 SHA2 身份证书（Tomcat、CallManager、CAPF、TVS 等等）。对于需要验证签名的任何其他加密操作，仅支持 SHA-1。</p> <p>注释 如果您使用的电话型号软件维护终止或寿命结束，我们强烈建议您使用 11.5 (1) SU1 版本之前的 Unified Communications Manager。</p>

7942 和 7962 电话的 CAPF 示例

用户或 Unified Communications Manager 重置电话时，请考虑以下 CAPF 如何与 Cisco Unified 7962 和 7942 IP 电话交互的相关信息。



注释 在以下示例中，如果电话中尚不存在 LSC 且为“CAPF 验证模式”选中**按现有证书**，CAPF 证书操作将失败。

示例 — 不安全设备安全模式

在本例中，在您将“设备安全模式”配置为不安全，将“CAPF 验证模式”配置为按空字符串或按现有证书 (优先于...)后，电话将重置。电话重置后，它将立即向主 Cisco Unified Communications Manager 注册并接收配置文件。然后，电话将自动发起与 CAPF 的会话以下载 LSC。电话安装 LSC 后，将设备安全模式配置为“已验证”或“已加密”。

示例 — 已验证/已加密设备安全模式

本例中，在您将设备安全模式配置为已验证或已加密，将“CAPF 验证模式”配置为按空字符串或按现有证书 (优先于...)后，电话将重置。电话不会向主 Unified Communications Manager 注册，直至 CAPF 会话结束并且电话安装了 LSC。会话结束后，电话注册并立即在已验证或已加密模式下运行。

本例中，您不能配置按验证字符串，因为电话不会自动联系 CAPF 服务器；如果电话没有有效的 LSC，注册将失败。

CAPF 与 IPv6 寻址的相互作用

CAPF 可以发行和升级证书给使用 IPv4、IPv6 或同时使用两类地址的电话。要颁发或升级运行 SCCP 的使用 IPv6 地址的电话的证书，您必须在 Unified Communications Manager 管理中将“启用 IPv6”服务参数设置为真。

电话连接至 CAPF 获取证书时，CAPF 使用“启用 IPv6” (Enable IPv6) 企业参数中的配置确定是发行还是升级证书到电话。如果该企业参数设为“假” (**False**)，CAPF 会忽略/拒绝来自使用 IPv6 地址的电话的连接，该电话不会收到证书。

下表介绍使用 IPv4、IPv6 或同时使用两类地址的电话如何连接到 CAPF。

表 28: IPv6 或 IPv4 电话如何连接到 CAPF

IP 电话模式	电话上的 IP 地址	CAPF IP 地址	电话如何连接到 CAPF
双堆栈	IPv4 和 IPv6 可用	IPv4, IPv6	电话使用 IPv6 地址连接 CAPF。如果电话无法通过 IPv6 地址连接，将尝试使用 IPv4 地址连接。
双堆栈	IPv4	IPv4, IPv6	电话使用 IPv4 地址连接 CAPF。
双堆栈	IPv6	IPv4, IPv6	电话使用 IPv6 地址连接 CAPF。如果尝试失败，电话将使用 IPv4 地址连接 CAPF。
双堆栈	IPv4	IPv4	电话使用 IPv4 地址连接 CAPF。
双堆栈	IPv4 和 IPv6 可用	IPv6	电话使用 IPv6 地址连接 CAPF。
双堆栈	IPv4 和 IPv6 可用	IPv4	电话使用 IPv4 地址连接 CAPF。
双堆栈	IPv4	IPv6	电话无法连接 CAPF。

IP 电话模式	电话上的 IP 地址	CAPF IP 地址	电话如何连接到 CAPF
双堆栈	IPv6	IPv4	电话无法连接 CAPF。
双堆栈	IPv6	IPv6	电话使用 IPv6 地址连接 CAPF。
IPv4 堆栈	IPv4	IPv4, IPv6	电话使用 IPv4 地址连接 CAPF。
IPv6 堆栈	IPv6	IPv4, IPv6	电话使用 IPv6 地址连接 CAPF。
IPv4 堆栈	IPv4	IPv4	电话使用 IPv4 地址连接 CAPF。
IPv4 堆栈	IPv4	IPv6	电话无法连接 CAPF。
IPv6 堆栈	IPv6	IPv6	电话使用 IPv6 地址连接 CAPF。
IPv6 堆栈	IPv6	IPv4	电话无法连接 CAPF。



第 33 章

配置 TFTP 服务器

- [代理 TFTP 部署概述，第 337 页](#)
- [TFTP 服务器配置任务流程，第 340 页](#)

代理 TFTP 部署概述

使用代理简单文件传输协议(TFTP)服务器提供您网络中的终端所需的配置文件，例如：拨号方案、铃声文件和设备配置文件。TFTP 服务器可以安装在部署中的任何群集中，并且可以服务来自多个群集上的终端的请求。DHCP 作用域指定代理 TFTP 服务器的 IP 地址以用于获取配置文件。

冗余和对等代理 TFTP 服务器

在单一群集部署中，群集必须有至少一个代理 TFTP 服务器。您可以将另一个代理 TFTP 服务器添加到群集以实现冗余。第二个代理 TFTP 服务器添加到 IPv4 的选项 150 中。对于 IPv6，您添加第二个代理服务器至 DHCP 作用域中的 TFTP 服务器地址子选项类型 1。

在多群集部署中，您可以指定最多三个远程代理 TFTP 服务器作为主代理 TFTP 服务器的对等群集。如果想要为多个 DHCP 作用域仅配置一个代理 TFTP 服务器，或只有一个 DHCP 作用域，则此功能很有用。主代理 TFTP 服务器提供网络中所有电话和设备的配置文件。

您必须创建每个远程代理 TFTP 服务器与主代理 TFTP 服务器之间的对等关系。



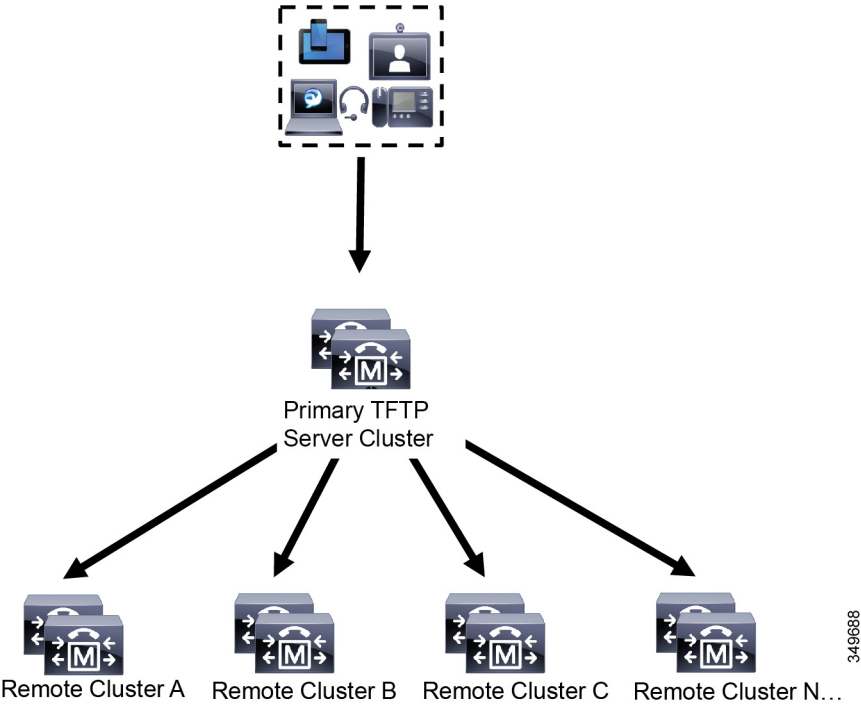
提示 在您的网络中配置远程代理 TFTP 服务器之间的对等关系时，请保持关系的层次。确保远程群集上的对等代理 TFTP 服务器没有指向彼此以避免可能的循环。例如，如果主节点 A 与节点 B 和 C 之间有对等关系。您不应在节点 B 和 C 之间创建对等关系。如果是这样，您就创建了一个循环。

代理 TFTP

在多群集系统中，代理 TFTP 服务可通过单个主要 TFTP 服务器从多个群集提供 TFTP 文件。代理 TFTP 在以下情况下可以充当单个 TFTP 引用：单个子网或 VLAN 包含来自多个群集的电话，或者多个群集共享相同的 DHCP TFTP 选项 (150)。

如图所示，代理 TFTP 服务用作单级层次结构。不支持更复杂多级层次结构。

图 7:代理 TFTP 的单级层次结构



在上图中，一组设备与主 TFTP 服务器联系以获取配置文件。当收到设备的 TFTP 请求时，主 TFTP 会在自己的本地缓存中以及任何其他远程配置的群集（例如远程群集 A、B、C 或 N）中查找配置文件。

可以在主 TFTP 服务器上配置任意数量的远程群集；但是，每个远程群集仅可包含最多 3 个 TFTP IP 地址。推荐的冗余设计是每个群集 2 个 TFTP 服务器，因此主 TFTP 服务器上的每个远程群集有 2 个 IP 地址以实现冗余。

使用案例和最佳实践

考虑详细介绍如何使用代理 TFTP 的以下场景以及实施的最佳实践。

- 1. 群集只能充当代理 TFTP 群集，而无其他用途。在这种情况下，群集与其他群集之间没有任何关系，也不会处理呼叫。对于此场景，建议手动定义远程群集 TFTP 并回滚至 8.0 以前。



注释 在此场景中，自动注册将不工作。

- 2. 群集是远程群集，同时也充当远程群集的代理 TFTP 服务器。远程群集是手动定义的，不应启用自动注册。

TFTP 对 IPv4 和 IPv6 设备的支持

我们建议您启用 IPv4 电话和网关，以使用 DHCP 自定义选项 150 查找 TFTP 服务器 IP 地址。使用选项 150 时，网关和电话会发现 TFTP 服务器 IP 地址。有关详细信息，请参阅随设备提供的文档。

在 IPv6 网络中，我们建议您使用 Cisco 供应商特定的 DHCPv6 信息将 TFTP 服务器 IPv6 地址传递给终端。通过此方法，可将 TFTP 服务器 IP 地址配置为选项值。

如果某些终端使用 IPv4，而某些终端使用 IPv6，则建议您将 DHCP 自定义选项 150 用于 IPv4，并将 TFTP 服务器地址子选项类型 1（一种 Cisco 供应商特定信息选项）用于 IPv6。在 TFTP 服务器使用 IPv4 处理请求时，如果终端获取 IPv6 地址并且发送请求到 TFTP 服务器，TFTP 服务器不会收到请求，因为 TFTP 服务器没有侦听 IPv6 堆栈上的请求。在此情况下，终端无法向 Cisco Unified Communications Manager 注册。

您可以使用其他方法为 IPv4 和 IPv6 设备查找 TFTP 服务器的 IP 地址。例如，您可以对 IPv4 设备使用 DHCP 选项 066 或 CiscoCM1。对于您的 IPv6 设备，其他方法包括使用 TFTP 服务子选项类型 2 或在终端上配置 TFTP 服务器的 IP 地址。建议不要使用这些替代方法。使用任何替代方法前，请咨询您的 Cisco 服务提供程序。

TFTP 部署的终端和配置文件

SCCP 电话、SIP 电话和网关在它们初始化时请求配置文件。每当您更改设备配置时，更新的配置文件都会发送到终端。

配置文件包含一些信息，例如 Unified Communications Manager 节点的优先顺序列表、用于连接到这些节点的 TCP 端口以及其他可执行文件。对于有些终端，配置文件还包含消息、目录、服务和信息等电话按钮的区域设置信息和 URL。网关的配置文件包含设备要求的所有配置信息。

代理 TFTP 的安全考虑事项

Cisco 代理 TFTP 服务器处理签名和未签名请求并在非安全模式或混合模式下运行。当电话请求文件时，代理 TFTP 服务器会搜索本地文件系统或数据库，如果找不到，则会将请求发送到远程群集。当电话要求服务器提供名称为 `ringlist.xml.sgn` 的通用文件、区域设置文件等，服务器将从电话的主群集发送文件的本地副本而不是文件本身。

接收来自代理 TFTP 的文件时，因为该文件代理服务器的签名与电话的初始信任列表 (ITL) 不匹配，因此签名验证失败，从而导致电话拒绝该文件。要解决此问题，您可以禁用电话的默认安全 (SBD) 或将代理 TFTP 的 `callmanager` 证书导入到新的（远程/主）群集 `phone-sast-trust`。然后，电话可以联系信任验证服务 (TVS) 并信任代理 TFTP 证书。如果在部署中启用了 EMCC，则需要批量证书交换要禁用“默认安全”，请参阅 [Cisco Unified Communications Manager 安全指南](#) 的“更新 Cisco Unified IP 电话的 ITL 文件”一节。

混合模式下的代理 TFTP


在混合模式下运行的远程群集上的 TFTP 服务器必须将主代理 TFTP 服务器证书添加到其 Cisco 证书信任列表 (CTL) 文件中。否则，注册到启用安全性的群集的终端将无法下载所需的文件。在执行证书批量导入-导出后实现此 CTL 文件更新。

在群集间迁移 IP 电话以执行批量证书到处时，请参阅[Cisco Unified Communications Manager 安全指南](#)中的“批量证书导出”一节了解更多信息。

在代理 TFTP 环境中的群集之间移动电话

在代理 TFTP 环境中将电话从一个远程群集移动到另一个时，请执行以下操作：

- 1. 将电话详细信息添加到远程群集 B（目标群集）。
- 2. 从远程群集 A（源群集）删除电话详细信息。



注释 代理 TFTP 中的电话配置需要 30 分钟才会过期。为避免找不到任何文件响应，您可以重新启动代理群集的 TFTP 服务。

- 3. 重置电话以从远程群集 B 下载配置文件并注册到远程群集 B。

TFTP 服务器配置任务流程

如果您为群集配置了跨群集分机移动 (EMCC)，则可以让系统动态配置代理 TFTP 服务器。如果不这样做，可以设置 TFTP 服务器并手动设置安全模式。

过程

	命令或操作	目的
步骤 1	使用以下方法之一设置 TFTP 服务器： <ul style="list-style-type: none">• 动态配置 TFTP 服务器，第 341 页• 手动配置 TFTP 服务器，第 341 页	如果您配置了群集间查询服务 (ILS)，您可以动态设置 TFTP 服务器。 如果未配置 EMCC，则手动设置 TFTP 服务器。您必须指明群集是安全还是不安全。默认情况下，群集被视为不安全。
步骤 2	(可选) 更新 TFTP 服务器的 CTL 文件，第 342 页	安装 CTL 客户端插件，并将主代理 TFTP 服务器添加到在混合模式下运行的所有远程群集中所有代理 TFTP 服务器的 Cisco 证书信任列表 (CTL) 文件。
步骤 3	(可选) 请参阅您的终端设备的支持文档。	如果代理 TFTP 部署具有远程群集，则将代理 TFTP 服务器添加到所有远程终端的信任验证列表 (TVL)。
步骤 4	(可选) 修改 TFTP 服务器的非配置文件，第 343 页	您可以从代理 TFTP 服务器修改终端请求的非配置文件。

	命令或操作	目的
步骤 5	(可选) 停止和启动 TFTP 服务，第 343 页	如果您已为终端上传了修改的非配置文件，请停止并重新启动代理 TFTP 节点上的 TFTP 服务。
步骤 6	(可选) 请参阅您的 DHCP 服务器的支持文档。	对于多个群集部署，修改各个远程节点的 DHCP 作用域以包括主代理 TFTP 服务器的 IP 地址。

动态配置 TFTP 服务器

如果您的网络配置了群集间查询服务 (ILS)，则可以动态配置 Cisco 代理 TFTP 服务器。

开始之前

为您的网络配置 EMCC。有关详细信息，请参阅《Cisco Unified Communications Manager 功能和服务指南》，位于 <http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>。

如果启用了 SIP OAuth，我们必须将群集外 Tomcat 证书的根 CA 证书复制到代理电话边缘信任库。

过程

在 Cisco Unified Communications Manager 管理中，选择高级功能 > 群集视图 > 立即更新远程群集。系统会自动为群集配置 TFTP 服务器。

下一步做什么

您必须将任何远程代理 TFTP 服务器添加到终端的信任验证列表 (TVL)；否则，它们将不接受来自远程群集上代理 TFTP 服务器的配置文件。有关说明，请参阅您的终端设备的支持文档。

手动配置 TFTP 服务器

如有要在未配置 EMCC 的情况下，在网络中配置 TFTP，必须执行手动程序。

您可以从群集视图中，设置主代理 TFTP 服务器与其他 TFTP 服务器之间的对等关系。最多可以添加三个对等 TFTP 服务器。

代理 TFTP 部署中的每个远程 TFTP 服务器必须包含到主代理 TFTP 服务器的对等关系。为避免产生循环，确保远程群集上的对等 TFTP 服务器不会指向彼此。

开始之前



重要事项 从 14SU1 版开始，启用 SIP OAuth 时，您必须将群集外的根 CA 证书（Tomcat 证书）复制到代理电话边缘信任库。

过程

步骤 1 创建远程群集。请执行以下操作：

- a) 从 Cisco Unified CM 管理中，选择高级功能 > 群集视图。
- b) 单击**新增**。此时将显示**远程群集配置**窗口。
- c) 为 TFTP 服务器输入最多 50 个字符的群集 ID 和完全限定域名 (FQDN)，然后单击**保存**。

群集 ID 的有效值包括字母数字字符、点号 (.) 和连字符 (-)。FQDN 的有效值包括字母数字字符、点号 (.)、破折号 (-)、星号 (*) 和空格。

- d) （可选）在**远程群集服务配置**窗口中，为远程群集输入最多 128 个字符的说明。

请勿使用引号 (“ ”)、左右尖括号 (> <)、反斜线 (\)、破折号 (-)、与符号 (&) 或百分号 (%)。

步骤 2 选中 **TFTP** 复选框为远程群集启用 TFTP。

步骤 3 单击 **TFTP**。

步骤 4 在**远程群集服务手动覆盖配置**窗口中，选择**手动配置远程服务地址**。

步骤 5 输入 TFTP 服务器的 IP 地址，以创建与这些 TFTP 服务器的对等关系。

最多可以输入三个 TFTP 服务器 IP 地址。

步骤 6 （可选）如果在安全群集中部署了代理 TFTP 服务器，请选中**群集是安全的**复选框。

步骤 7 单击**保存**。

下一步做什么

必须将任何远程 TFTP 服务器添加到终端的信任验证列表 (TVL)，否则，它们将不接受来自远程群集上的代理 TFTP 服务器的配置文件。有关说明，请参阅您的终端设备的支持文档。

更新 TFTP 服务器的 CTL 文件

通过在每个混合模式下的群集中运行 `utils ctl`，从发布方节点更新 CTL 文件。确保在代理 TFTP 服务器和所有群集之间实现完整的安全网络，即在代理与远程群集之间批量导入和导出证书交换。

使用 CTLClient 时，您必须将主 TFTP 服务器或主 TFTP 服务器的 IP 地址添加到混合模式下运行的远程群集中的所有 TFTP 服务器的 Cisco 证书信任列表 (CTL) 文件中。这是必要的，以便启用安全的群集中的终端可以成功下载其配置文件。

有关安全性和使用 Cisco CTL CLI 的详细信息，请参阅[Cisco Unified Communications Manager 安全指南](#)中的“关于 Cisco CTL 设置”一节。

过程

- 步骤 1 从 Cisco Unified CM 管理中，选择应用程序 > 插件。
- 步骤 2 单击查找以列出您可以安装的所有插件。
- 步骤 3 单击下载链接以获取 Cisco CTL 客户端。
系统安装客户端，它会对存储在 TFTP 服务器上的证书进行数字签名。
- 步骤 4 重新启动 TFTP 服务器。

修改 TFTP 服务器的非配置文件

您可以修改终端从代理 TFTP 服务器请求的非配置文件，例如加载文件或 ringlist.xml。完成此程序后，将修改的文件上传到代理 TFTP 服务器的 TFTP 目录。

过程

- 步骤 1 在 Cisco Unified Communications 操作系统管理中，选择软件升级 > TFTP 文件管理。
TFTP 文件管理窗口将会显示。
- 步骤 2 单击上传文件。
上传文件弹出窗口将会显示。
- 步骤 3 执行以下操作之一：
 - 单击浏览以浏览到要上传的文件的目录位置。
 - 将更新文件的完整目录路径粘贴到目录字段中。
- 步骤 4 单击上传文件或单击关闭退出而不上传文件。

下一步做什么

使用 Cisco Unified 功能配置管理停止并重新启动代理 TFTP 节点上的 Cisco TFTP 服务。

停止和启动 TFTP 服务

按照以下程序在代理 TFTP 节点上停止和重新启动 TFTP 服务。

有关服务激活、停用和重新启动的详细信息，请参阅《Cisco Unified 功能配置管理指南》，位于<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>。

过程

步骤 1 在 Cisco Unified 功能配置中，选择工具 > 控制中心 - 功能服务。

步骤 2 在控制中心 - 功能服务窗口中，选择服务器下拉列表中的代理 TFTP 节点。

步骤 3 在 CM 服务区域中选择 TFTP 服务，然后单击停止。

状态更改会体现更新后的状态。

提示 要查看服务的最新状态，单击刷新。

步骤 4 在 CM 服务区域中选择 TFTP 服务，然后单击开始。

状态更改会体现更新后的状态。



第 34 章

通过激活码激活设备

- [激活代码概述，第 345 页](#)
- [激活代码前提条件，第 347 页](#)
- [现场模式下使用激活代码自行激活设备任务流程，第 348 页](#)
- [设备自行激活任务流程（移动和远程访问模式），第 354 页](#)
- [激活代码的其他任务，第 356 页](#)
- [激活代码用例，第 357 页](#)

激活代码概述

激活代码使自行激活新预配置的电话变得轻松。激活代码由 16 位数字组成，只能单次使用，用户注册电话时必须在电话上输入该值。激活代码提供了一种设置和注册电话的简便方法，无需管理员手动收集和输入每部电话的 MAC 地址。此方法是自动注册的简单替代方法，您可以使用此方法来预配置大量的电话、一部电话甚至重新注册现有电话。

此外，您还可以使用激活代码轻松且安全地使用移动和远程访问兼容设备注册移动和远程访问。

激活代码设备自行激活在以下模式下工作：

- 现场
- 移动远程访问 (MRA)



注释 TFTP 代理设置不支持使用激活代码激活和 MRA 的终端注册。

激活代码具有以下优点：

- 使用激活代码自行激活可确保所有新预配置的电话或不受信任的电话都由 Unified Communications Manager 评估并验证过它们的厂商预装证书 (MIC)。



注释 Cisco 厂商根证书必须存在于 CallManager 信任存储区中，以执行自行激活活动。

- 无需手动输入实际 MAC 地址。管理员可以使用虚拟 MAC 地址，在注册期间，电话会使用真实 MAC 地址自动更新配置。
- 无需部署 IVR（例如 TAPS），即可将电话名称从 BAT 转换为 SEP。

电话用户可以通过自助门户获取其激活代码，前提是显示电话已做好准备激活参数设置为真。否则，管理员必须提供代码给电话用户。



注释 当您预配置 BAT MAC 地址时，激活代码将绑定到电话型号。BAT MAC 是对以 "BAT" 开头的设备名称的引用，后面跟有与 MAC 地址类似的随机 12 位十六进制数字。保存带有空白 MAC 地址字段的“设备配置”页时，将为您创建一个具有此格式的随机名称。您必须输入与电话型号匹配的激活代码，才能激活电话。

为增强安全性，您可以使用电话的实际 MAC 地址预配置电话。此选项涉及更多配置，因为管理员必须在预配置期间收集并输入每个电话的 MAC 地址，但提供更高的安全性，因为用户必须输入与电话上的实际 MAC 地址相匹配的激活代码。

由于技术限制，代理 TFTP 部署不支持通过激活代码进行设备激活

现场模式下的自行激活工作流程

，以下是通过激活代码自行激活新电话的工作流程：

1. 管理员可设置配置以要求用户输入激活代码进行自行激活。
2. 管理员预配置和配置电话。如果使用了 BAT MAC 地址，管理员将不会输入实际的 MAC 地址。
3. 电话通过 DHCP opt 150 获取 TFTP 的 IP 地址，或从“电话设置”中配置的备用 TFTP 获取。电话将下载 XMLDefault 文件，并检测到正在使用的激活代码。
4. 用户在电话上输入激活代码。
5. 电话通过激活代码和制造商安装的证书向 Cisco Unified Communications Manager 进行验证。
6. 在使用激活代码自行激活电话时，电话需要 TVS 服务。ITL 文件提供此 TVS 功能，其中包含在 Unified CM 服务器 TCP 端口 2445 上运行的 TVS 服务的证书。
7. Cisco Unified Communications Manager 使用实际 MAC 地址更新设备配置。TFTP 服务器检测到电话的设备配置，允许电话进行注册。请注意，设备注册最长可达五分钟。



注释 建议添加另一个订阅方到默认的 Communication Manager 组以进行现场激活代码自行激活。此外，当默认 Communication Manager 组中的节点关闭时，您可能会面临自行激活问题。

移动和远程访问模式下的自行激活工作流程

当您使用移动和远程访问模式时，以下是通过激活代码自行激活新电话的工作流程：

1. 管理员可配置云/混合通信以启用使用 Cisco 云的激活代码，并指定移动和远程访问激活域。
2. 如有必要，管理员可配置额外的移动和远程访问服务域。
3. 管理员在不指定 MAC 地址（BAT、AXL、GUI）的情况下创建完整设备配置。设备名称将是随机 BAT MAC 地址。
4. 管理员请求此设备的激活代码。设备激活服务从基于云的设备激活服务请求代码。
5. 用户可以从自助门户获取代码，或者管理员可以将其发送给用户。
6. 用户打开电话电源并输入激活代码。
7. 电话从云学习 Expressway 的位置，并验证移动和远程访问/Cisco Unified Communications Manager。
8. 设备激活服务使用电话的 MAC 地址更新数据库中的设备配置。

电话现在可以从 TFTP 注册和获取其电话特定的配置文件，如普通的移动和远程访问，以及向 Cisco Unified Communications Manager 注册。



注释 要为家庭远程用户提供安全的工作解决方案，推荐使用 Expressway 的移动和 Remote Access 解决方案，而不推荐 TRP。

激活代码前提条件

从版本 12.5(1) 开始，以下 Cisco IP 电话型号支持通过激活代码自行激活：7811、7821、7832、7841、7861、8811、8841、8845、8851、8851NR、8861、8865 和 8865NR。

对于现场和 MRA，版本 12.5SR3 均支持在 Cisco IP 电话型号上自行激活。

此外，版本 12.5(1)SU1 支持以下 Cisco IP 电话型号：8832 和 8832NR

对于云自行激活过程，以下域名应通过 Cisco Unified Communications Manager 解析：

- fos-a.wbx2.com
- idbroker.webex.com
- push.webexconnect.com

- btpush.webexconnect.com

Self Care 自助门户

如果您打算让您的用户使用自助门户来自行激活电话，您需要提前设置该门户网站，以便您的用户能够访问。有关详细信息，请转至 *Cisco Unified Communications Manager* 功能配置指南的“自助门户”一章。

现场模式下使用激活代码自行激活设备任务流程

完成这些任务以使用激活代码自行激活新电话。

过程

	命令或操作	目的
步骤 1	激活设备激活服务，第 348 页	Cisco 设备激活服务 必须正在 Cisco Unified 功能配置中运行。
步骤 2	设置注册方法以使用激活代码，第 349 页	在“设备默认值”下，设置默认注册方法以对支持的电话型号使用激活代码。
步骤 3	使用激活代码预配置电话的要求。以下是两个预配置示例选项： <ul style="list-style-type: none"> • 使用激活代码添加电话的要求，第 349 页 • 通过批量管理使用激活代码添加电话，第 350 页 	Cisco Unified Communications Manager 有各种预配置方法，包括左侧的选项。不论您选择哪种方法，请确保选中电话的 电话配置 内的 需要用于自行激活的激活代码 复选框。
步骤 4	激活电话，第 353 页	分发激活代码给用户。用户必须在电话上输入该代码以使用电话。

激活设备激活服务

要使用激活代码，**Cisco 设备激活服务**必须正在 Cisco Unified 功能配置中运行。使用此程序确认服务正在运行。

过程

- 步骤 1** 从 Cisco Unified 功能配置中，选择工具 > 服务激活。
- 步骤 2** 从服务器下拉列表中，选择 Unified Communications Manager 发布方节点并单击前往。
- 步骤 3** 在 CM 服务下，确认 **Cisco 设备激活服务**的状态为已激活。

步骤 4 如果服务未运行，请选中相邻的复选框，然后单击**保存**。

下一步做什么

[设置注册方法以使用激活代码，第 349 页](#)

设置注册方法以使用激活代码

使用此程序配置系统默认值，以使特定型号类型的电话使用激活代码注册 Unified Communications Manager。



注释 此程序仅适用于现场终端的自行激活。设备默认值下的“激活方法”设置不适用于使用激活代码的移动和远程访问终端的激活。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**设备 > 设备设置 > 设备默认设置**。

步骤 2 在设备默认配置窗口中，选择要在双区信息部分中使用激活代码进行注册的设备类型，然后将现场自行激活方法从自动注册更改为激活代码。

步骤 3 单击**保存**。

注释 设备默认设置为激活代码时，如果电话类型先前使用的是“自动注册”，则后续添加新电话应遵循激活代码自行激活或电话的手动配置（使用 MAC 地址）和注册。

有关详细信息，请参阅[使用激活代码添加电话的要求](#)和[通过批量管理使用激活代码添加电话](#)部分以预配置新电话。

使用激活代码添加电话的要求

如果要预配置具有激活代码要求的新电话，请使用此程序。

开始之前

使用您要应用的设置配置通用设备和线路模板，因为这会使预配置过程更快。



注释 如果您选择不使用模板，则可以添加新的电话和手动配置设置，或通过 BAT 模板添加设置。在每种情况下，都必须在**电话配置**窗口中选中需要用于自行激活的激活代码复选框。

过程

-
- 步骤 1** 从 Cisco Unified CM 管理中，选择**设备 > 电话**。
- 步骤 2** 单击**从模板新增**可从通用线路或设备模板添加设置。
- 步骤 3** 从**电话类型**下拉菜单中，选择电话型号。
- 步骤 4** 在 **MAC 地址** 字段中，输入 MAC 地址。使用激活代码，您可以使用虚拟 MAC 地址或电话的实际 MAC 地址。
- 在以下场景下，您可以修改电话的 MAC 地址：
- **BAT{mac}->SEP{mac}**：保存时，您应该知道确切的设备名称，以使前缀从 ?BAT? 改到 ?SEP?。
 - **SEP{mac}->BAT{mac}**：您可以清空 MAC 地址，以使前缀从 ?SEP? 改为 ?BAT?，并且新的设备名称前缀为 ?BAT?。
- 如果启用了激活代码，**MAC 地址** 字段可留空。它会自动填充虚拟 MAC 地址。
- 步骤 5** 从**设备模板**下拉列表中，选择一个模板，例如具有您想要应用的设置的现有通用设备模板。
- 步骤 6** 从**目录号码**字段中，选择现有的目录号码，或单击“新建”并执行以下操作：
- a) 在**添加新分机**弹出菜单中，输入新的目录号码和包含您要应用的设置的线路模板。
 - b) 单击**保存**，然后单击**关闭**。
- 新的分机将出现在**目录号码**字段中。
- 步骤 7** 可选。从**用户**字段中，选择您要应用到此电话的用户 ID。
- 步骤 8** 单击**添加**。
- 步骤 9** 选中需要用于自行激活的**激活代码**复选框。如果是移动和远程访问模式，请选中**允许通过移动和远程访问使用激活代码**复选框。
- 步骤 10** 配置您要应用的任何其他设置。有关这些字段及其设置的帮助，请参阅联机帮助。
- 步骤 11** 单击**保存**，然后单击**确定**。
- 电话配置会生成新的激活代码。如果要查看代码，请单击**查看激活代码**。
-

下一步做什么

[激活电话，第 353 页](#)

通过批量管理使用激活代码添加电话

此可选任务流程包含使用批量管理工具的插入电话功能通过一次操作预配置大量电话的预配置示例。这些电话将使用激活代码进行注册。

过程

	命令或操作	目的
步骤 1	配置 BAT 预配置模板，第 351 页	配置 BAT 模板，其中包含您要应用到已预配置电话的设置。
步骤 2	创建包含新电话的 CSV 文件，第 352 页	创建一个 CSV 文件，其中包含您要添加的新电话。
步骤 3	嵌入电话，第 352 页	使用批量管理的“插入电话”功能将新电话添加到数据库中。

配置 BAT 预配置模板

使用此程序可创建具有通用设置的电话模板，您可以通过批量管理将其应用到特定电话型号的新预配置的电话。

开始之前

此程序假设您的用户已部署在系统中，并且您已经设置了满足您需要的设备池、SIP 配置文件和电话安全性配置文件。

过程

- 步骤 1 从 Cisco Unified CM 管理中，选择批量管理 > 电话 > 电话模板。
- 步骤 2 单击新增。
- 步骤 3 从电话类型下拉列表中，选择要为其创建模板的电话型号。
- 步骤 4 输入模板名。
- 步骤 5 选中需要用于自行激活的激活代码复选框。如果是移动和远程访问模式，请选中允许通过移动和远程访问使用激活代码复选框。
- 步骤 6 为以下必填字段配置值：
 - 设备池
 - 电话按键模板
 - 所有者用户 ID
 - 设备安全性配置文件
 - SIP 配置文件
- 步骤 7 完成电话模板配置窗口中其余任何字段的设置。有关这些字段及其设置的帮助，请参阅联机帮助。
- 步骤 8 单击保存。

下一步做什么

[创建包含新电话的 CSV 文件，第 352 页](#)

创建包含新电话的 CSV 文件

使用此程序可使用新电话创建新的 csv 文件。



注释 您也可以手动创建 csv 文件。

过程

- 步骤 1 在 Cisco Unified CM 管理中，选择批量管理 > 上传/下载文件。
- 步骤 2 单击查找。
- 步骤 3 选择并下载 **bat.xlt** 电子表格。
- 步骤 4 打开电子表格并转至电话选项卡。
- 步骤 5 将新电话的详细信息添加到电子表格。如果您使用虚拟 MAC 地址，请将“MAC 地址”字段留空。选中需要用于自行激活的激活代码复选框。如果是移动和远程访问模式，请选中允许通过移动和远程访问使用激活代码复选框。
- 步骤 6 完成后，单击导出为 **BAT** 格式。
- 步骤 7 在 Cisco Unified CM 管理中，选择批量管理 > 上传/下载文件。
- 步骤 8 上传 csv 文件
 - a) 单击新增。
 - b) 单击选择文件，然后选择要上传的 csv 文件。
 - c) 选择电话作为目标。
 - d) 为事务类型选择插入电话 - 特定详细信息。
 - e) 单击保存。

下一步做什么

[嵌入电话，第 352 页](#)

嵌入电话

使用此程序可从 csv 文件插入新电话。

过程

- 步骤 1 选择批量管理 > 电话 > 插入电话。

步骤 2 从文件名下拉列表中，选择您的 csv 文件。

步骤 3 从电话模板名称下拉列表中，选择您创建的预配置模板。

步骤 4 选中创建虚拟 MAC 地址复选框。

注释 为了增加安全性，您可以将实际的 MAC 地址添加到 csv 文件，以便激活代码仅适用于具有匹配 MAC 地址的电话。在这种情况下，不选中此复选框。

步骤 5 选中立即运行复选框可立即运行作业。如果您选择以后运行作业，则必须在批量管理工具的作业计划程序中计划该作业。

步骤 6 单击提交。

下一步做什么

[激活电话，第 353 页](#)

激活电话

预配置后，将激活代码分配给您的电话用户，以便他们能够激活自己的电话。以下是用于收集和分发激活代码的两个选项：

- 自助门户—电话用户可以登录到自助门户，以获取适用于其电话的激活代码。他们可以手动在电话上输入代码，也可以使用他们电话的摄像头扫描自助门户中显示的条形码。两种方法都适用。要使用自助门户激活电话，必须在 Cisco Unified Communications Manager 中将显示电话已做好准备激活企业参数设置为 **真**（这是默认设置）。



注释 有关如何为自助门户配置用户访问的其他要求，请参阅 *Cisco Unified Communications Manager* 功能配置指南的“自助门户”一章。

- CSV 文件—您还可以将未处理的用户和激活代码列表导出到 csv 文件，然后将该文件分发给您的用户。有关过程，请参阅[导出激活代码，第 354 页](#)。

注册流程

电话用户必须在他们的电话上输入激活代码，才能使用自己的电话。电话用户在电话上输入正确的激活代码后，将发生以下情况：

- 他们的电话通过 Cisco Unified Communications Manager 进行验证。
- Cisco Unified Communications Manager 中的电话配置将使用电话的实际 MAC 地址进行更新。
- 电话将从 TFTP 服务器下载配置文件和任何其他相关文件，并向 Cisco Unified Communications Manager 注册。

后续操作

电话现已准备就绪，可供使用。

导出激活代码

使用此程序导出激活代码的 csv 文件及其对应的电话和用户。 您可以使用此文件分发激活代码给您的用户。

过程

- 步骤 1 从 Cisco Unified CM 管理中，选择设备 > 电话。
- 步骤 2 从相关链接中，选择导出激活代码，然后单击转至。

设备自行激活任务流程（移动和远程访问模式）

在移动和远程访问模式下，使用激活代码完成这些任务以自行激活新电话。

开始之前

Cisco 设备激活服务必须在 Cisco Unified 功能配置中运行（该服务默认在运行）。 要验证服务正在运行，请转至[激活设备激活服务](#)，第 348 页。

过程

	命令或操作	目的
步骤 1	通过移动和远程访问启用思科云自行激活 ，第 355 页	在云自行激活 下，生成凭证、启用激活代码自行激活和指定移动和远程访问激活域。
步骤 2	移动和远程访问服务域配置（可选） ，第 355 页	在云端自行激活群集，以允许远程移动和远程访问设备自行激活到特定的移动和远程访问激活域。
步骤 3	上传自定义证书（可选） ，第 355 页	可选。 如果要使用自己的自定义证书，则远程移动和远程访问终端将能够从云下载这些证书并使用它们连接到 Expressway。
步骤 4	使用激活代码预配置电话的要求。 以下是两个预配置示例选项： <ul style="list-style-type: none">使用激活代码添加电话的要求，第 349 页通过批量管理使用激活代码添加电话，第 350 页	您必须在 Unified CM 数据库中预配置电话。 Unified CM 有多种预配置方法可供您使用，包括这些示例选项。

	命令或操作	目的
步骤 5	激活电话，第 353 页	分发激活代码给用户。用户必须在电话上输入该代码以使用电话。

通过移动和远程访问启用思科云自行激活

过程

- 步骤 1** 要授权群集（CCMAct 服务）连接到基于云的设备激活服务，请单击生成凭证按钮生成凭证。
- 步骤 2** 指定移动和远程访问激活域。（这会自动复制到移动和远程访问服务域列表。）
- 步骤 3** 通过选中“启用激活代码自行激活”和“允许移动和远程访问自行激活”复选框，启用激活代码自行激活。如果您配置了设备默认设置使用“自动注册”自行激活，则“允许移动和远程访问自行激活”复选框将被禁用并自动选中，因为它只适用于移动和远程访问模式下中的电话。如果您配置了设备默认设置使用“激活代码”自行激活，则这两个复选框都可用。
- 步骤 4** 单击保存。

移动和远程访问服务域配置（可选）

要配置电话的移动和远程访问服务域，请使用以下程序：

过程

- 步骤 1** 选择高级功能 > 移动和远程访问服务域以访问移动和远程访问服务域窗口。
- 步骤 2** 输入移动和远程访问服务域名称。
- 步骤 3** 输入用于激活的 Expressway-E 的 SRV 记录。
- 步骤 4** 通过选中所选域旁边的默认复选框，选择默认的移动和远程访问服务域。这是您在设备池级别选择“< None >”时使用的域。
- 步骤 5** 使用该记录的行中的链接访问从属关系记录，还会列出从属关系数。

上传自定义证书（可选）

要上传证书，请使用以下程序。

过程

- 步骤 1** 上传证书到 Expressway。不要删除任何其他证书。

- 步骤 2** 使用路径 **CUCM OS 管理 > 证书管理** 将新证书上传到 Unified Communications Manager。使用 “Phone-Edge-trust” 类型。（Unified Communications Manager 将这些发送到云，然后发送到电话以访问 Expressway。）
- 步骤 3** 根据需要删除所有其他 “Phone-Edge-trust” 类型的证书，以便仅使用自定义证书。

激活代码的其他任务

下表列出了可能需要为激活代码执行的其他任务。

任务	程序
生成注册电话的激活代码	<p>如果要为已注册的电话生成激活代码：</p> <ol style="list-style-type: none"> 1. 从 Cisco Unified CM 管理中，选择设备 > 电话。 2. 搜索并打开您要为其生成激活代码的电话的电话配置。 3. 选中需要用于自行激活的激活代码复选框，然后单击保存。
重新生成未注册电话的激活代码	<p>要为未注册电话生成新的激活代码（例如，新电话的激活过程失败时会需要），请进行以下操作：</p> <ol style="list-style-type: none"> 1. 从 Cisco Unified CM 管理中，选择设备 > 电话。 2. 搜索并打开您要为其生成激活代码的电话的电话配置。 3. 单击发布激活代码 4. 单击生成新的激活代码，然后单击保存。
设置可选的激活代码参数	<p>如果要配置激活代码的可选服务参数。</p> <ol style="list-style-type: none"> 1. 从 Cisco Unified CM 管理中，选择系统 > 服务参数。 2. 从服务器下拉列表中，选择发布方节点。 3. 从服务下拉列表中选择 Cisco 设备激活服务。 4. 配置以下可选服务参数的值。有关这些设置的帮助，请参阅上下文相关帮助 <ul style="list-style-type: none"> • 激活生存时间（小时） 代码保持活动的小时数。默认为 168 • 启用移动和远程访问激活 —将此字段设置为“真”（默认设置）以启用移动和远程访问激活。 • 移动和远程访问激活域—发生移动和远程访问设备激活的域。 5. 单击保存。

激活代码用例

下表通过激活代码突出显示使用设备自行激活的示例使用案例。

使用案例	说明
更换现有电话	<p>激活代码使您可以轻松地替换现有电话。例如，假设远程员工需要新电话，因为他们电话已损坏。</p> <ul style="list-style-type: none">• 管理员将在 Unified Communications Manager 中打开已损坏电话的电话配置设置。• 管理员将会留空 MAC 地址，选中需要用于自行激活的激活代码复选框，然后单击保存。• 用户将获取同一电话型号的新电话，然后将电话插入网络。• 用户登录到自助服务以获取其激活代码，并在电话上输入代码。电话自行激活成功。 <p>注释 在此场景中，用户可以自行激活任何新电话，只要新电话与损坏的电话型号相同即可。在较安全的环境中，管理员可能需要预配置替代电话来替换旧电话（请参阅下文）。</p>
使用激活代码安全发货新电话	<p>在较安全的环境中，您可以通过将激活代码 ting 到特定的 MAC 地址来确保电话发货过程的安全，如下所示：</p> <ul style="list-style-type: none">• 管理员在 Unified Communications Manager 中预配置新电话。• 在新电话的电话配置设置中，管理员输入电话的实际 MAC 地址，然后选中需要用于自行激活的激活代码复选框。• 管理员将电话打包并将电话发给用户。• 用户将新电话插入到网络中。• 用户登录到自助服务以获取激活代码，在电话上输入代码。电话自行激活成功。 <p>注释 在这种情况下，用户只能在此特定电话上自行激活。</p>

使用案例	说明
新电话（自动注册）的安全发货	<p>除了激活代码方法之外，您还可以使用自动注册和 TAPS 将电话安全地发货给远程员工：</p> <ul style="list-style-type: none"> 在设备默认配置中，管理员可确保电话型号的自行激活方法为自动注册。 管理员在 Unified Communications Manager 中预配置新电话。在新电话的电话配置中，管理员将会留出电话的实际 MAC 地址。 管理员将电话打包并将电话发给用户。 用户将新电话插入到网络中，并让其自动注册。 用户使用 TAPS 将自动注册记录重新映射到旧记录。 <p>注释 这种情况要求您同时配置自动注册和 TAPS。</p>
通过自动注册重新自行激活电话	<p>通过设备默认配置窗口中的现场自行激活方法字段，您可以在激活代码与自动注册之间切换特定电话型号的自行激活方法。</p> <p>注释 如果要通过自动注册重新自行激活现有电话，则必须从数据库中删除现有的记录，自动注册才能工作。</p>
自行激活要在移动和远程访问模式中使用的现场电话	<p>您可以在现场自行激活电话，然后标记电话以在移动和远程访问模式中再次自行激活，从而利用到 Expressway 的 OAuth 连接以及从 Expressway 到 Cisco Unified Communications Manager 的信任连接的安全性。</p> <p>在此场景中，如果启用了“允许通过移动和远程访问使用激活代码”，则电话现场自行激活、验证其收到的 OAuth 访问令牌，然后切换到移动和远程访问模式并发起与 Expressway 的通信。如果您的内部网络不允许从现场与 Expressway 通信，则电话不会注册，但会准备好在场外接通电源时联系 Expressway。</p> <p>注释 未注册的场外电话无法更新其固件加载。此场景非常适用于需要在本地使用的开箱即用电话来下载最新固件并使用激活代码功能。</p> <p>选中允许激活代码用于 MRA 复选框后，电话将切换到 MRA 模式，并且具有 MRA 服务域和 OAuth 令牌。</p>
通过零接自行激活来自行激活现场电话	<p>注册现场电话并将安全性配置文件配置为 OAuth 后，电话将在重置或重新启动时隐式获取访问令牌。</p>



第 35 章

配置自动注册

- 自动注册概述，第 359 页
- 配置自动注册任务流程，第 359 页

自动注册概述

将新电话插入网络时，自动注册使得 Unified Communications Manager 能够自动为其分配目录号码。

现在安全模式下启用了自动注册。此增强功能为您的系统提供了更高的安全性，因为您可以在预配置新电话时保护群集的安全。它还简化了注册过程，因为您不必禁用群集安全来注册新电话。

如果创建的设备池仅允许 911（紧急）和 0（接线员）呼叫，则可以使用此功能来阻止未经授权的终端在自动注册启用时连接到您的网络。新终端可以注册到此池，但其访问受到限制。可以防止不断启动并尝试注册到您的网络的恶意设备未经授权的访问。您可以将已经自动注册的电话移至新位置以及分配到不同的设备池，而不会影响其目录号码。

系统不知道自动注册的新电话是否在运行 SIP 或 SCCP，因此您在启用自动注册时必须指定。同时支持 SIP 和 SCCP 的设备（例如 Cisco 7911、7940、7941、7960、7961、7970 和 7971 IP 电话）将向“自动注册电话协议”企业参数中指定的协议自动注册。

仅支持单个协议的设备将使用该协议自动注册。“自动注册电话协议”设置将被忽略。例如，即使“自动注册电话协议”参数设置为 SIP，任何仅支持 SCCP 的 Cisco IP 电话都将自动向 SCCP 注册。

当网络中要添加的电话少于 100 部时，我们建议使用自动注册。如果要添加的电话超过 100 部，则使用批量管理工具 (BAT)。有关详细信息，请参阅《Cisco Unified Communications Manager 批量管理指南》，位于 <http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>。

配置自动注册任务流程

启用自动注册会带来安全风险。在将新终端添加到网络中时，仅短暂启用自动注册。

过程

	命令或操作	目的
步骤 1	配置自动注册分区，第 360 页	配置路由分区以专用于自动注册，从而将自动注册的电话限制为仅内部呼叫。
步骤 2	配置用于自动注册的呼叫搜索空间，第 361 页	配置呼叫搜索空间以专用于自动注册，从而将自动注册的电话限制为仅内部呼叫。
步骤 3	配置自动注册设备池，第 362 页	创建使用为自动注册配置的呼叫搜索空间的设备池。
步骤 4	设置自动注册的设备协议类型，第 363 页	使用此程序将协议设置为 SCCP 或 SIP 以匹配您要自动注册的电话类型。
步骤 5	启用自动注册，第 363 页	在要用于自动注册的节点上启用自动注册，然后设置自动注册 Cisco Unified Communications Manager 组参数以为用于自动注册的 Cisco Unified Communications Manager 组启用自动注册。
步骤 6	禁用自动注册，第 365 页	一旦完成注册新设备后，就禁用节点的自动注册。
步骤 7	重复使用自动注册号码，第 365 页	可选。已被禁用的设备的自动注册号码可以重复使用。当您重置自动注册目录号码的范围时，就会强制系统从起始号码重新搜索。可用的目录号码将重复使用。

配置自动注册分区

配置路由分区以专用于自动注册，从而将自动注册的电话限制为仅内部呼叫。

过程

- 步骤 1 从 Cisco Unified CM 管理中，选择呼叫路由 > 控制级 > 分区。
- 步骤 2 单击新增以创建新的分区。
- 步骤 3 在分区名称、说明字段中，为分区输入一个在路由计划中唯一的名称。
分区名称可以包含字母数字字符，以及空格、连字符 (-) 和下划线 (_)。请参阅联机帮助，了解有关分区名称的指导原则。
- 步骤 4 在分区名称后面输入逗号 (,)，并在同一行上输入分区的说明。
说明最多可以包含 50 个任何语言的字符，但不能包含双引号 (")、百分号 (%)、与符号 (&)、反斜线 (\)、尖括号 (<>) 或中括号 ([])。
如果不输入说明，Cisco Unified Communications Manager 将自动在此字段中输入分区名称。

步骤 5 要创建多个分区，请每个分区条目使用一行。

步骤 6 从下拉列表中，选择与此分区关联的时间表。

时间表指定分区何时可用于接收来电。如果您选择无，该分区将始终保持活动状态。

步骤 7 选择下列单选按钮之一以配置时区：

- **始叫设备**—当选择此单选按钮时，系统会将主叫设备的时区与时间表作比较，以确定分区是否可用接收来电。
- **特定时区**—选择此单选按钮后，从下拉列表中选择时区。系统会将所选的时区与时间表作比较，以确定分区是否可用接收来电。

步骤 8 单击保存。

下一步做什么

[配置用于自动注册的呼叫搜索空间，第 361 页](#)

配置用于自动注册的呼叫搜索空间

配置呼叫搜索空间以专用于自动注册，从而将自动注册的电话限制为仅内部呼叫。

开始之前

[配置自动注册分区，第 360 页](#)

过程

步骤 1 从 Cisco Unified CM 管理中，选择呼叫路由 > 控制级 > 呼叫搜索空间。

步骤 2 单击新增。

步骤 3 在名称字段中输入名称。

确保每个呼叫搜索空间名称在系统中都是唯一的。名称最多可以包含 50 个字母数字字符，可以包含空格、点 (.)、连字符 (-) 和下划线 (_)。

步骤 4 在说明字段中，输入说明。

说明最多可以包含 50 个任何语言的字符，但不能包含双引号 (")、百分号 (%)、与符号 (&)、反斜线 (\) 或尖括号 (<>)。

步骤 5 从可用分区下拉列表中，执行以下步骤之一：

- 对于单个分区，选择该分区。
- 对于多个分区，按住控制 (CTRL) 键，然后选择适当的分区。

步骤 6 在方框之间选择向下箭头，以将分区移至所选分区字段。

步骤 7 （可选）使用所选分区框右侧的箭头键更改所选分区的优先级。

步骤 8 单击保存。

下一步做什么

[配置自动注册设备池，第 362 页](#)

相关主题

[服务级别，第 170 页](#)

配置自动注册设备池

您可以使用默认设备池进行自动注册，也可以为 SIP 和 SCCP 设备配置单独的设备池以进行自动注册。

要配置默认设备池进行注册，将默认 Cisco Unified Communications Manager 组和自动注册呼叫搜索空间 (CSS) 分配给默认设备池。如果您选择为 SIP 和 SCCP 设备配置单独的默认设备池，请使用默认的设备池值。

开始之前

[配置用于自动注册的呼叫搜索空间，第 361 页](#)

过程

步骤 1 从 Cisco Unified Communications Manager 管理中，选择系统 > 设备池。

步骤 2 要修改默认设备池进行自动注册，请执行以下操作：

- a) 单击**查找**，然后从设备池列表中选择**默认**。
- b) 在**设备池配置**窗口中的**用于自动注册的呼叫搜索空间**字段中，选择要用于自动注册的 CSS，然后单击**保存**。

步骤 3 要为自动注册创建新的设备池，请执行以下操作：

- a) 单击**新增**。
 - b) 在**设备池配置**窗口中，为设备池输入唯一的名称。
最多可以输入 50 个字符，可包含字母数字、点 (.)、连字符 (-)、下划线 (_) 和空格。
 - c) 设置以下字段以匹配默认设备池。请参阅联机帮助了解字段说明。
 - 在 **Cisco Unified Communications Manager** 组中，选择**默认**。
 - 在**日期/时间**组中，选择 **CMLocal**
 - 在**区域**中，选择 **默认**。
 - d) 在**用于自动注册的呼叫搜索空间**字段中选择要用于自动注册的 CSS，然后单击**保存**。
-

下一步做什么

[设置自动注册的设备协议类型，第 363 页](#)

设置自动注册的设备协议类型

如果您的 SIP 和 SCCP 设备是自动注册的，必须先将“自动注册电话协议”参数设置为 SCCP，然后安装运行 SCCP 的所有设备。然后将“自动注册电话协议”参数更改为 SIP 并自动注册所有正在运行 SIP 的设备。

开始之前

[配置自动注册设备池，第 362 页](#)

过程

步骤 1 在 Cisco Unified Communications Manager 管理中，选择系统 > 企业参数。

步骤 2 在企业参数配置窗口中，在自动注册电话协议下拉列表中选择 **SCCP** 或 **SIP**，然后单击保存。

下一步做什么

[启用自动注册，第 363 页](#)

启用自动注册

其中自动注册时，您必须指定在连接至网络时会分配至新终端的目录号码的范围。作为每个新终端连接时，会分配下一个可用目录号码。在所有可用的自动注册目录号码使用完后，任何终端都无法自动注册。

新终端会使用启用自动注册 **Cisco Unified Communications Manager** 组设置的组中首个 Unified Communications Manager 节点自动注册。然后，该节点根据设备类型自动将每个自动注册的终端分配给默认设备池。

开始之前

[设置自动注册的设备协议类型，第 363 页](#)

- 创建设备池、呼叫搜索空间和路由分区，从而限制自动注册的设备访问，仅允许内部呼叫。
- 确保目录号码在自动注册范围中可用。
- 确保有足够的许可点以注册新电话。
- 检查 SIP 和 SCCP 的正确电话图像名称显示在**设备默认值配置**窗口中。尽管 TFTP 服务器上应该有大多数通用设备配置文件，但请确保您设备的配置文件确在其中。
- 确保 Cisco TFTP 服务器在线并且 TFTP 的 DHCP 选项指定了正确的服务器。

过程

步骤 1 从 Cisco Unified Communications Manager 管理中，选择系统 > **Cisco Unified CM**，然后在查找并列出 **Cisco Unified Communications Managers** 窗口中单击查找。

步骤 2 在群集中选择要用于自动注册的 Cisco Unified Communications Manager 屏幕。

步骤 3 在 **Cisco Unified CM** 配置窗口中，为自动注册信息部分中的节点配置自动注册参数，然后单击保存。有关字段及其配置选项的更多信息，请参阅系统联机帮助。

a) 从下拉列表中选择要用于自动注册的通用设备模板。

如果没有为自动注册创建通用设备模板，则可以选择默认的通用设备模板。从用户管理 > 用户/电话添加 > 通用设备模板，确保所选模板指定了要用于自动注册的设备池。

b) 从下拉列表中选择要用于自动注册的通用线路模板。

如果没有为自动注册创建通用线路模板，则可以选择默认的通用线路模板。从用户管理 > 用户/电话添加 > 通用线路模板，确保所选模板指定了要用于自动注册的呼叫搜索空间和路由分区。

c) 在起始目录号码和结束目录号码字段中输入起始和结束目录号码。

将起始和结束目录号码设置为相同的值会禁用自动注册。

d) 取消选中在此 **Cisco Unified Communications Manager** 上禁用自动注册以启用自动注册。

仅在所选 Unified Communications Manager 节点上始终启用或禁用自动注册。如果您将自动注册功能切换到群集中的另一个节点，则必须重新配置 Cisco Unified Communications Manager 节点、默认 Unified Communications Manager 组以及您使用的默认设备池。

步骤 4 选择系统 > **Cisco Unified CM** 组，然后在查找并列出 **Cisco Unified Communications Manager** 组窗口中单击查找。

步骤 5 选择 Unified Communications Manager 组以启用自动注册。

在大多数情况下，此组的名称为默认。您可以选择其他 Cisco Unified Communications Manager 组。组必须至少选择一个节点。

步骤 6 在该组的 **Cisco Unified CM** 组配置窗口中，选择自动注册 **Cisco Unified Communications Manager** 组以为此组启用自动注册，然后单击保存。

提示 确保所选的 **Cisco Unified Communications Manager** 列表包含要为自动注册配置的节点。使用箭头可移动节点以在列表中显示。Unified Communications Manager 节点选择顺序与它们的列出顺序一致。保存您的更改。

步骤 7 安装您要自动注册的设备。



注释 您可以继续以重新配置自动注册的电话并将其分配给永久设备池。分配给电话的目录号码不会因您更改电话位置而发生变化。



注释 要注册不同类型的电话，请在禁用自动注册之前更改设备协议类型并安装这些设备。

禁用自动注册

一旦完成注册新设备后，就禁用节点的自动注册。

开始之前

[启用自动注册，第 363 页](#)

过程

步骤 1 在 Cisco Unified Communications Manager 管理中，选择系统 > **Cisco Unified CM**，然后在查找并列出 **Cisco Unified CM** 窗口单击查找。

步骤 2 从节点列表中选择 **Cisco Unified Communications Manager**。

步骤 3 在选定节点的 **Cisco Unified CM** 配置窗口中，选中在此 **Cisco Unified Communications Manager** 上禁用自动注册复选框以为此节点禁用自动注册，然后单击保存。

提示 在起始目录号码和结束目录号码字段中设置为相同的值也会禁用自动注册。

下一步做什么

可选。如果手动更改自动注册设备的目录号码，或者从数据库中删除该设备，您可以重复使用该目录号码。有关详细信息，请参阅[重复使用自动注册号码，第 365 页](#)。

重复使用自动注册号码

当您新设备连接到网络时，系统会为该设备分配下一个可用的自动注册目录号码。如果手动更改自动注册设备的目录号码，或者从数据库中删除该设备，则该设备的自动注册目录号码可以重用。

当设备尝试自动注册时，系统将搜索您指定的自动注册号码范围，并且尝试查找下一个可用的目录号码以分配给设备。它从上一个分配的目录号码之后按顺序开始搜索下一个号码。到达范围的结束目录号码后，系统将继续从范围的起始目录号码搜索。

您可以重置自动注册目录号码的范围，并且强制系统从范围的起始号码开始搜索。

过程

步骤 1 在 Cisco Unified Communications Manager 管理中，选择系统 > **Cisco Unified Communications Manager**

步骤 2 选择 Cisco Unified Communications Manager 以重置自动注册。

步骤 3 记下起始目录号码和结束目录号码字段中的当前设置。

步骤 4 单击在此 **Cisco Unified Communications Manager** 上禁用自动注册，然后单击保存。

在自动注册禁用时，新电话无法自动注册。

步骤 5 将起始目录号码和结束目录号码字段设置为之前的值，然后单击保存。

提示 您可以将这些字段设置为新值。



第 36 章

配置自我预配置

- [自我预配置概述，第 367 页](#)
- [自我预配置前提条件，第 368 页](#)
- [自我预配置配置任务流程，第 369 页](#)

自我预配置概述

通过让最终用户能够预配置自己的电话而无需联系管理员，自我预配置功能可帮助您为网络预配置电话。如果系统配置为自我预配置，并且单个最终用户启用了自我预配置，则最终用户可以通过将电话插入网络并按照指定的一些提示来预配置新电话。Cisco Unified Communications Manager 通过应用预先配置的模板来配置电话和电话线路。

自我预配置可供管理员使用以代表其最终用户预配置电话，也可供最终用户使用自我预配置来预配置自己的电话。

无论群集安全设置是不安全还是混合模式，都支持自我预配置。

安全模式

您可以通过以下两种模式之一配置自我预配置：

- **安全模式**—在安全模式下，用户或管理员必须经过验证，才能访问自我预配置。最终用户可以根据他们密码或 PIN 进行验证。管理员可以输入预先配置的验证代码。
- **不安全模式**—在不安全模式下，用户或管理员可以输入其用户 ID 或自我预配置 ID，以便将电话关联到用户帐户。不建议在日常使用中不使用安全模式。

通过通用线路和设备模板配置

自我预配置使用通用线路模板和通用设备模板配置为最终用户配置预配置的电话和电话线路。当用户预配置自己的电话时，系统将引用该用户的用户配置文件，并将关联的通用线路模板应用到预配置的电话线路以及将通用设备模板应用到预配置的电话。

自我预配置电话

配置该功能后，您可以通过执行以下操作来预配置电话：

- 将电话插入网络。
- 拨打自我预配置 IVR 分机。
- 按照提示配置电话，然后将该电话关联到最终用户。最终用户可以输入用户密码、PIN 或管理验证代码，具体取决于您配置自我预配置的方式。



提示 如果您要代表最终用户预配置大量电话，请在通用设备模板上配置前转到自我预配置 IVR 分机的快速拨号。

自我预配置模拟 FXS 端口

您可以在模拟 FXS 端口上启用自我预配置，以便用户可以呼叫自我预配置 IVR 并将其关联的目录号码分配给该模拟端口。此外，对于预配置的电话，用户可以取消分配与模拟语音网关端口关联的目录号码，然后将其分配给另一用户。

程序

1. 在网关的 FXS 语音端口中插入模拟电话。由于端口自动注册或预先配置（手动），电话将自动从自动注册的池或已分配的目录号码自动获取目录号码。
2. 从自动注册的模拟设备呼叫自我预配置 IVR。
3. 输入自助服务 ID 和 PIN。



注释 确认后，将使用最终用户主分机预配置模拟设备。自动注册的目录号码将释放到池。

自我预配置前提条件

在最终用户可以使用自我预配置之前，必须为最终用户配置了以下项目：

- 最终用户必须具有主分机。
- 最终用户必须与包含通用线路模板、通用设备模板的用户配置文件或功能组模板相关联。必须为自我预配置启用了用户配置文件。

自我预配置配置任务流程

过程

	命令或操作	目的
步骤 1	激活自我预配置服务，第 369 页	在 Cisco Unified 功能配置中，激活自我预配置 IVR 和 CTI Manager 服务。
步骤 2	启用自我预配置自动注册，第 370 页	为自我预配置启用自动注册参数
步骤 3	配置 CTI 路由点，第 370 页	配置 CTI 路由点来处理自我预配置 IVR 服务。
步骤 4	将目录号码分配给 CTI 路由点，第 371 页	配置用户将拨打的分机，以便访问自我预配置 IVR，并将该分机关联到 CTI 路由点。
步骤 5	配置应用程序用户进行自我预配置，第 371 页	为自我预配置 IVR 配置应用程序用户。将 CTI 路由点与应用程序用户相关联。
步骤 6	配置系统以进行自我预配置，第 372 页	为您的系统配置自我预配置设置，包括将应用程序用户和 CTI 路由点关联到自我预配置 IVR。
步骤 7	在用户配置文件中启用自我预配置，第 372 页	允许用户在其分配到的用户配置文件中自我预配置电话。

激活自我预配置服务

此程序用于激活支持自我预配置功能的服务。确保自我预配置 IVR 和 Cisco CTI Manager 服务都在运行。

过程

- 步骤 1 从 Cisco Unified 功能配置中，选择工具 > 服务激活。
- 步骤 2 从服务器下拉列表中，选择发布方节点并单击前往。
- 步骤 3 在 CM 服务下，选中 Cisco CTI Manager。
- 步骤 4 在 CTI 服务下，选中自我预配置 IVR。
- 步骤 5 单击保存。

启用自我预配置自动注册

要使用此程序进行自我预配置，必须在发布方上配置自动注册参数。

过程

-
- 步骤 1 在 Cisco Unified CM 管理中，选择系统 > **Cisco Unified CM**。
 - 步骤 2 单击发布方节点。
 - 步骤 3 选择要应用到预配置电话的**通用设备模板**。
 - 步骤 4 选择要应用到预配置电话的电话线路的**通用线路模板**。
 - 步骤 5 使用**起始目录号码**和**结束目录号码**字段输入要应用到预配置电话的目录号码范围。
 - 步骤 6 取消勾选此 **Cisco Unified Communications Manager 禁用自动注册**复选框。
 - 步骤 7 确认要用于 SIP 注册的端口。在大多数情况下，无需更改端口的默认设置。
 - 步骤 8 单击**保存**。
-

配置 CTI 路由点

此程序用于为自我预配置 IVR 配置 CTI 路由点。

过程

-
- 步骤 1 从 Cisco Unified CM 管理中，选择**设备** > **CTI 路由点**。
 - 步骤 2 完成下列步骤之一：
 - a) 单击**查找**并选择现有的 CTI 路由点。
 - b) 单击**新增**以创建新的 CTI 路由点。
 - 步骤 3 在**设备名称**字段中，输入用于标识路由点的唯一名称。
 - 步骤 4 从**设备池**下拉列表中，选择指定此设备属性的设备池。
 - 步骤 5 从**位置**下拉列表中，为此 CTI 路由点选择适当的位置。
 - 步骤 6 从**使用信任的中继点**下拉列表中，可以启用或禁用 Unified Communications Manager 对此媒体终端插入信任的中继点 (TRP) 设备。默认设置是使用与此设备关联的通用设备配置设置。
 - 步骤 7 完成 **CTI 路由点配置**窗口中其余字段的设置。有关字段及其设置的更多信息，请参阅联机帮助。
 - 步骤 8 单击**保存**。
-

将目录号码分配给 CTI 路由点

此程序用于设置用户拨入的分机以访问自我预配置 IVR。您必须将此分机与想要用于自我预配置的 CTI 路由点相关联。

过程

- 步骤 1 从 Cisco Unified CM 管理中，选择设备 > **CTI 路由点**。
- 步骤 2 单击**查找**并选择您为自我预配置设置的 CTI 路由点。
- 步骤 3 从关联下，单击**线路 [1] - 添加新目录号码**。
此时将显示**目录号码配置**窗口。
- 步骤 4 在**目录号码**字段中，输入您希望用户拨打的分机以访问自我预配置的 IVR 服务。
- 步骤 5 单击**保存**。
- 步骤 6 完成**目录号码配置**窗口中其余字段的设置。有关字段及其设置的更多信息，请参阅联机帮助。
- 步骤 7 单击**保存**。

配置应用程序用户进行自我预配置

必须为自我预配置 IVR 设置一个应用程序用户，并将您创建的 CTI 路由点与该应用程序用户关联。

过程

- 步骤 1 从 Cisco Unified CM 管理中，选择用户 > **应用程序用户**。
- 步骤 2 请执行以下步骤之一：
 - a) 要选择现有的应用程序用户，请单击**查找**并选择应用程序用户。
 - b) 要创建新的应用程序用户，请单击**新增**。
- 步骤 3 在**用户 ID** 文本框中，输入应用程序用户的唯一 ID。
- 步骤 4 为应用程序用户选择 **BLF 在线状态组**。
- 步骤 5 通过执行以下步骤，将您创建的 CTI 路由点与应用程序用户关联：
 - a) 如果您创建的 CTI 路由点没有出现在**可用设备**列表框中，请单击**查找更多路由点**。
您创建的 CTI 路由点将显示为可用设备。
 - b) 在**可用设备**列表中，选择您为自我预配置创建的 CTI 路由点，然后单击向下箭头。
CTI 路由点显示在**受控设备**列表中。
- 步骤 6 填写**应用程序用户配置**窗口中的其余字段。有关这些字段及其设置的帮助，请参阅联机帮助。
- 步骤 7 单击**保存**。

配置系统以进行自我预配置

此程序用于配置您的系统进行自我预配置。自我预配置可让您网络中的用户能够通过 IVR 系统添加自己的桌面电话，而无需与管理员联系。



注释 为了使用自我预配置功能，您的最终用户还必须在用户配置文件中启用该功能。

过程

步骤 1 从 Cisco Unified CM 管理中，选择用户管理 > 自我预配置。

步骤 2 通过单击下列单选按钮之一，配置您是否要自我预配置 IVR 验证最终用户：

- **需要验证**—为了使用自我预配置 IVR，最终用户必须输入其密码、PIN 或系统验证代码。
- **无需验证**—最终用户无需验证即可访问自我预配置 IVR。

步骤 3 如果自我预配置 IVR 配置为“需要验证”，则单击以下单选按钮之一来配置 IVR 验证最终用户的方法：

- **仅允许最终用户验证**—最终用户必须输入其密码或个人识别码。
- **允许用户（通过密码/PIN）和管理员（通过验证代码）验证**—最终用户必须输入验证代码。如果选择此选项，请在验证代码文本框中输入 0 到 20 位之间的整数，以配置验证代码。

步骤 4 在 IVR 设置列表框中，使用箭头选择您希望用于 IVR 提示的语言。可用语言的列表取决于您安装在系统中的语言包。如果要下载其他语言包，请参阅 cisco.com 的下载部分。

步骤 5 从 CTI 路由点下拉列表中，选择您为自我预配置 IVR 配置的 CTI 路由点。

步骤 6 从应用程序用户下拉列表中，选择您为自我预配置所配置的应用程序用户。

步骤 7 单击保存。

在用户配置文件中启用自我预配置

要使用户能够自我预配置电话，必须在其分配到的用户配置文件中启用此功能。



注释 如果您不知道用户使用的是哪个用户配置文件，可以在“最终用户配置”窗口中打开用户的设置，然后查看用户配置文件字段以获取正确的配置文件。

过程

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

步骤 2 单击**查找**并选择用户分配到的用户配置文件。

步骤 3 将**通用线路模板**和**通用设备模板**分配给用户配置文件。

步骤 4 配置自我预配置的用户设置：

- 选中**允许最终用户部署自己的电话**复选框。
- 输入用户可以预配置的电话数的限制。默认值为 10。
- 如果您希望用户能够使用自我预配置来重新分配之前分配的电话，请在与旧设备的最终用户关联的用户配置文件页面选中**允许预配置已分配给不同最终用户的电话**设置。只有在与旧设备关联的用户配置文件中启用了此复选框的情况下，用户才可以重新分配之前分配的电话。

步骤 5 单击**保存**。

在用户配置文件中启用自我预配置



第 **VI** 部分

参考信息

- [Cisco Unified Communications Manager TCP 和 UDP 端口使用情况](#)，第 377 页
- [IM and Presence Service 的端口使用信息](#)，第 393 页



第 37 章

Cisco Unified Communications Manager TCP 和 UDP 端口使用情况

- [Cisco Unified Communications Manager TCP 和 UDP 端口使用情况概述，第 377 页](#)
- [端口说明，第 379 页](#)
- [端口参考，第 391 页](#)

Cisco Unified Communications Manager TCP 和 UDP 端口使用情况概述

Cisco Unified Communications Manager TCP 和 UDP 端口分为以下几类：

- Cisco Unified Communications Manager 服务器之间的群集内端口
- 公共服务端口
- Cisco Unified Communications Manager 与 LDAP 目录之间的端口
- 从 CCMAAdmin 或 CCMUser 到 Cisco Unified Communications Manager 的 Web 请求
- 从 Cisco Unified Communications Manager 到电话的 Web 请求
- 电话和 Cisco Unified Communications Manager 之间的信令、媒体和其他通信
- 网关和 Cisco Unified Communications Manager 之间的信令、媒体和其他通信
- 应用程序和 Cisco Unified Communications Manager 之间的通信
- CTL 客户端和防火墙之间的通信
- HP 服务器上的特殊端口

有关上述每个类别中的端口详细信息，请参阅“端口说明”。



注释 对于这些端口，Cisco 并未验证所有可能的配置情形。如果您在使用此列表时遇到配置问题，请联系 Cisco 技术支持人员寻求帮助。

提及的端口只适用于 Cisco Unified Communications Manager。某些端口因版本而异，而且将来的版本可能会引入新的端口。因此，对于所安装的 Cisco Unified Communications Manager 版本，请确保使用本文档的正确版本。

虽然几乎所有协议都是双向的，但是假定从会话发起者的角度看待方向性。在某些情况下，管理员可以手动更改默认端口号，但思科不建议将此作为最佳做法。请注意，Cisco Unified Communications Manager 会严格打开多个端口以供内部使用。

安装 Cisco Unified Communications Manager 软件会自动安装以下网络服务以实现可维护性并默认激活它们。请参阅“《Cisco Unified Communications Manager 服务器之间的群集内端口》”获取详细信息：

- Cisco 日志分区监控（监控并清理通用分区。此过程不使用自定义通用端口。）
- Cisco 跟踪收集服务（TCTS 端口使用情况）
- Cisco RIS 数据收集器（RIS 服务器端口使用情况）
- Cisco AMC 服务（AMC 端口使用情况）

根据拓扑、电话设备的放置以及与网络安全设备的放置相关的服务以及所用的应用程序和电话扩展，防火墙、ACL 或 QoS 的配置将有所不同。另外，请记住，ACL 的格式因设备和版本不同而异。



注释 您也可以在 Cisco Unified Communications Manager 中配置多播音乐保持 (MOH) 端口。多播 MOH 的端口值未提供，因为管理员指定了实际的端口值。



注释 系统的临时端口范围为 32768 至 61000，端口需要打开以保持电话为注册状态。有关详细信息，请参阅 <http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html>。



注释 请确保配置防火墙，以便与端口 22 的连接处于打开状态，并且不受限制。在安装 IM and Presence 订阅方节点期间，到 Cisco Unified Communications Manager 发布方节点的多个连接将连续快速打开。限制这些连接可能会导致安装失败。

端口说明

Cisco Unified Communications Manager 服务器之间的群集内端口

表 29: Cisco Unified Communications Manager 服务器之间的群集内端口

从（发送方）	至（监听方）	目标端口	目的
终端	Unified Communications Manager	514 / UDP	系统日志记录服务
Unified Communications Manager	Unified Communications Manager	443 / TCP	在订阅方节点中，在事件期间，此端口用于发布方之间的通信。
Unified Communications Manager	RTMT	1090、1099 / TCP	Cisco AMC 服务，用于性能监控、数据收集、记录和警报
Unified Communications Manager (DB)	Unified Communications Manager (DB)	1500、1501 / TCP	数据库连接（1500 是主连接，1501 是备用连接）
Unified Communications Manager (DB)	Unified Communications Manager (DB)	1510 / TCP	CAR IDS DB。用于侦听并等待来自订阅方的请求。
Unified Communications Manager (DB)	Unified Communications Manager (DB)	1511 / TCP	CAR IDS DB。用于在订阅方节点间调出第二个 CAR IDS DB 的备用端口。
Unified Communications Manager (DB)	Unified Communications Manager (DB)	1515 / TCP	安装期间节点之间的通信控制
Cisco 扩展功能 (QRT)	Unified Communications Manager (DB)	2552 / TCP	允许订阅方接收来自 Cisco Unified Communications Manager 数据库更改通知
Unified Communications Manager	Unified Communications Manager	2551 / TCP	Cisco 扩展服务之间的通信，由备份确定的群集成员
Unified Communications Manager (RIS)	Unified Communications Manager (RIS)	2555 / TCP	实时信息服务器之间的通信
Unified Communications Manager (AMC/RTMT/SOAP)	Unified Communications Manager (RIS)	2556 / TCP	适用于 Cisco RIS 服务的 (RIS) 数据库

从（发送方）	至（监听方）	目标端口	目的
Unified Communications Manager (DRS)	Unified Communications Manager (DRS)	4040 / TCP	DRS 主要代理
Unified Communications Manager (Tomcat)	Unified Communications Manager (SOAP)	5001/TCP	SOAP 监控器将此端时监控服务。
Unified Communications Manager (Tomcat)	Unified Communications Manager (SOAP)	5002/TCP	SOAP 监控器将此端能监控服务。
Unified Communications Manager (Tomcat)	Unified Communications Manager (SOAP)	5003/TCP	SOAP 监控器将此端制中心服务。
Unified Communications Manager (Tomcat)	Unified Communications Manager (SOAP)	5004/TCP	SOAP 监控器将此端志收集服务。
标准 CCM 管理员用户 / 管理员	Unified Communications Manager	5005 / TCP	此端口由 SOAP CDROnDemand2 服
Unified Communications Manager (Tomcat)	Unified Communications Manager (SOAP)	5007 / TCP	SOAP 监控器
Unified Communications Manager (RTMT)	Unified Communications Manager (TCTS)	临时 / TCP	Cisco 跟踪收集工具 (TCTS) -- 用于 RTMT 日志中心 (TLC) 的
Unified Communications Manager (Tomcat)	Unified Communications Manager (TCTS)	7000、7001、7002 / TCP	此端口用于 Cisco 跟踪具服务和 Cisco 跟踪务程序之间的通信。
Unified Communications Manager (DB)	Unified Communications Manager (CDLM)	8001 / TCP	客户端数据库更改通
Unified Communications Manager (SDL)	Unified Communications Manager (SDL)	8002 / TCP	群集内通信服务
Unified Communications Manager (SDL)	Unified Communications Manager (SDL)	8003 / TCP	群集内通信服务（到
Unified Communications Manager	CMI 管理器	8004 / TCP	Cisco Unified Comm Manager 和 CMI 管理的群集内通信
Unified Communications Manager (Tomcat)	Unified Communications Manager (Tomcat)	8005 / TCP	Tomcat 关闭脚本使用侦听端口
Unified Communications Manager (Tomcat)	Unified Communications Manager (Tomcat)	8080 / TCP	用于诊断测试的服务通信

从（发送方）	至（监听方）	目标端口	目的
网关	Unified Communications Manager	8090	用于 CuCM 和 G（接口）之间通信的端口，针对网关录
Unified Communications Manager	网关		
Unified Communications Manager (IPSec)	Unified Communications Manager (IPSec)	8500 / TCP 和 UDP	IPSec 群集管理器之间的群集内复制
Unified Communications Manager (RIS)	Unified Communications Manager (RIS)	8888-8889 / TCP	RIS 服务管理器之间的复制
位置带宽管理器 (LBM)	位置带宽管理器 (LBM)	9004 / TCP	LBM 之间的群集
Unified Communications Manager 发布方	Unified Communications Manager 订阅方	22 / TCP	Cisco SFTP 服务订阅方时，您必须
Unified Communications Manager	Unified Communications Manager	8443 / TCP	允许访问控制中的功能和网络服

公共服务端口

表 30: 公共服务端口

从（发送方）	至（监听方）	目标端口	目的
终端	Unified Communications Manager	7	互联网控制消息协议 (ICMP) 此协议号携带与回声相关的流量。它不构成列标题中指示的端口。
Unified Communications Manager	终端		
Unified Communications Manager (DRS、呼叫详细信息记录)	SFTP 服务器	22 / TCP	发送备份数据到 SFTP 服务器。（DRS 本地代理） 将呼叫详细信息记录数据发送到 SFTP 服务器。
终端	Unified Communications Manager (DHCP 服务器)	67 / UDP	Cisco Unified Communications Manager 充当 DHCP 服务器 注释 思科不建议在 Cisco Unified Communications Manager 上运行 DHCP 服务器。

从（发送方）	至（监听方）	目标端口	目的
Unified Communications Manager	DHCP 服务器	68 / UDP	Cisco Unified Communications Manager 充当 DHCP 客户端 注释 思科不建议在 Cisco Unified Communications Manager 上运行 DHCP 客户端。使用静态 IP 地址配置 Cisco Unified Communications Manager。）
终端设备或网关	Unified Communications Manager	69, 6969, 然后临时 / UDP	TFTP 服务至电话和网关
终端设备或网关	Unified Communications Manager	6970 / TCP	主服务器与代理服务器之间的 TFTP。 从 TFTP 服务器到电话和网关的 HTTP 服务。
Unified Communications Manager	NTP 服务器	123 / UDP	网络时间协议 (NTP)
SNMP 服务器	Unified Communications Manager	161 / UDP	SNMP 服务响应（来自管理应用程序的请求）
CUCM 服务器 SNMP 主代理应用程序	SNMP 陷阱目标	162 / UDP	SNMP 陷阱
SNMP 服务器	Unified Communications Manager	199 / TCP	用于 SMUX 支持的内置 SNMP 代理侦听端口
Unified Communications Manager	DHCP 服务器	546 / UDP	DHCPv6. IPv6 的 DHCP 端口。
Unified Communications Manager 功能配置	位置带宽管理器 (LBM)	5546 / TCP	增强位置 CAC 功能配置
Unified Communications Manager	位置带宽管理器 (LBM)	5547 / TCP	呼叫准入请求和带宽扣除
Unified Communications Manager	Unified Communications Manager	6161 / UDP	用于主代理与本机代理之间的通信，以处理本机代理 MIB 请求

从（发送方）	至（监听方）	目标端口	目的
Unified Communications Manager	Unified Communications Manager	6162 / UDP	用于主代理与本机代理之间的通信，以前转本机代理生成的通知
集中 TFTP	备用 TFTP	6970 / TCP	集中式 TFTP 文件定位器服务
Unified Communications Manager	Unified Communications Manager	7161 / TCP	用于 SNMP 主代理和子代理之间的通信
SNMP 服务器	Unified Communications Manager	7999 / TCP	Cisco Discovery Protocol 代理与 CDP 可执行程序之间的通信
终端	Unified Communications Manager	443、8443 / TCP	使用 Cisco 用户数据服务 (UDS) 请求
Unified Communications Manager	Unified Communications Manager	9050 / TCP	通过 TAPS 驻留在 Cisco Unified Communications Manager 上的服务 CRS 请求
Unified Communications Manager	Unified Communications Manager	61441 / UDP	Cisco Unified Communications Manager 应用程序通过 UDP 向此端口发出警报。Cisco Unified Communications Manager MIB 代理侦听此端口，并按照 Cisco Unified Communications Manager MIB 定义生成 SNMP 陷阱。
Unified Communications Manager	Unified Communications Manager	5060、5061 / TCP	提供基于干线的 SIP 服务
Unified Communications Manager	Unified Communications Manager	7501	由群集间查询服务 (ILS) 用于基于证书的验证。
Unified Communications Manager	Unified Communications Manager	7502	由 ILS 用于基于密码的验证。
Unified Communications Manager	Unified Communications Manager	9966	启用防火墙时，Cisco 推送通知服务用于在群集中的节点之间通信。
Unified Communications Manager	Unified Communications Manager	9560	由本地推送通知服务 (LPNS) 使用。

从（发送方）	至（监听方）	目标端口	目的
--	--	8000-48200	ASR 和 ISR G3 平台默认端口范围。
		16384-32766	ISR G2 平台默认端口范围。

Cisco Unified Communications Manager 与 LDAP 目录之间的端口

表 31: Cisco Unified Communications Manager 与 LDAP 目录之间的端口

从（发送方）	至（监听方）	目标端口	目的
Unified Communications Manager	外线目录	389、636、3268、3269 / TCP	轻型目录访问协议(LDAP)对外部目录（Active Directory、Netscape Directory）的查询
外线目录	Unified Communications Manager	临时	

从 CCMAdmin 或 CCMUser 到 Cisco Unified Communications Manager 的 Web 请求

表 32: 从 CCMAdmin 或 CCMUser 到 Cisco Unified Communications Manager 的 Web 请求

从（发送方）	至（监听方）	目标端口	目的
浏览器	Unified Communications Manager	80、8080 / TCP	超文本传输协议 (HTTP)
浏览器	Unified Communications Manager	443、8443 / TCP	通过 SSL 的超文本传输协议 (HTTPS)
浏览器	Unified Communications Manager	9463 / TCP	SSL 上的超文本传输协议 (HTTPS) 仅支持 TLS

从 Cisco Unified Communications Manager 到电话的 Web 请求

表 33: 从 Cisco Unified Communications Manager 到电话的 Web 请求

从（发送方）	至（监听方）	目标端口	目的
Unified Communications Manager <ul style="list-style-type: none"> • QRT • RTMT • 查找并列出电话页面 • 电话配置页面 	Phone	80 / TCP	超文本传输协议

电话和 Cisco Unified Communications Manager 之间的信令、媒体和其他通信

表 34: 电话和 Cisco Unified Communications Manager 之间的信令、媒体和其他通信

从（发送方）	至（监听方）	目标端口	目的
Phone	DNS 服务器	53/ TCP	会话发起协议 (SIP) 电话会使用域名系统 (DNS) 解析完全限定域名 (FQDN) 注释 默认情况下，某些无线接入点会阻止 TCP 53 端口，这会在使用 FQDN 配置 CUCM 时阻止无线 SIP 电话注册。
Phone	Unified Communications Manager (TFTP)	69，然后临时 / UDP	用于下载固件和配置文件的普通文件传输协议 (TFTP)
Phone	Unified Communications Manager	2000 / TCP	信令客户端控制协议 (SCCP)
Phone	Unified Communications Manager	2443 / TCP	安全信令客户端控制协议 (SCCPS)
Phone	Unified Communications Manager	2445 / TCP	为终端提供信任验证服务。

从（发送方）	至（监听方）	目标端口	目的
Phone	Unified Communications Manager (CAPF)	3804 / TCP	证书颁发机构代理职能 (CAPF) 侦听端口以颁发本地有效证书 (LSC) 给 IP 电话
Phone	Unified Communications Manager	5060 / TCP 和 UDP	会话发起协议 (SIP) 电话
Unified Communications Manager	Phone		
Phone	Unified Communications Manager	5061 TCP	安全会话发起协议 (SIPS) 电话
Unified Communications Manager	Phone		
Phone	Unified Communications Manager (TFTP)	6970 TCP	基于 HTTP 下载固件和配置文件
Phone	Unified Communications Manager (TFTP)	6971、6972 / TCP	TFTP 的 HTTPS 接口。电话使用此端口将从 TFTP 下载安全配置文件。
Phone	Unified Communications Manager	8080 / TCP	用于 XML 应用程序、验证、目录、服务等电话 URL。您可以基于每个服务配置这些端口。
Phone	Unified Communications Manager	9443 / TCP	电话使用此端口进行经过验证的联系人搜索。
Phone	Unified Communications Manager	9444	电话利用此端口号码使用头戴式耳机管理功能。
iPhone/iPad（Webex 应用）	Unified Communications Manager	9560/安全 Web 套接字	Webex 应用使用此端口号来实现 LPNS 功能。
IP VMS	Phone	16384 - 32767 / UDP	实时协议 (RTP)、安全实时协议 (SRTP) 注释 Cisco Unified Communications Manager 只使用 24576-32767，尽管其他设备使用整个范围。
Phone	IP VMS		

网关和 Cisco Unified Communications Manager 之间的信令、媒体和其他通信

表 35: 网关和 Cisco Unified Communications Manager 之间的信令、媒体和其他通信

从（发送方）	至（监听方）	目标端口	目的
网关	Unified Communications Manager	47, 50, 51	通用路由封装 (GRE)、安全负载 (ESP)、认证头 (AH)。这些协议加密的 IPSec 流量。成列标题中指示
Unified Communications Manager	网关		
网关	Unified Communications Manager	500 / UDP	用于建立 IP 安全的 Internet 密钥交换
Unified Communications Manager	网关		
网关	Unified Communications Manager (TFTP)	69, 然后临时 / UDP	普通文件传输协议
Unified Communications Manager 与 Cisco Intercompany Media Engine (CIME) 干线	CIME ASA	1024-65535 / TCP	端口映射服务。路径外部署模型
网守	Unified Communications Manager	1719 / UDP	网守 (H.225) RA
网关	Unified Communications Manager	1720 / TCP	用于 H.323 网关和 (ICT) 的 H.225 信
Unified Communications Manager	网关		
网关	Unified Communications Manager	临时 / TCP	网守控制干线上服务
Unified Communications Manager	网关		

从（发送方）	至（监听方）	目标端口	目的
网关	Unified Communications Manager	临时 / TCP	建立语音、视频和媒体 H.245 信令服务
Unified Communications Manager	网关		注释 远程系统使用 H.245 端口于网关的。对于 IOS 的 H.245 端口是 11000 和 65535。
网关	Unified Communications Manager	2000 / TCP	信令客户端控制协议
网关	Unified Communications Manager	2001 / TCP	使用 Cisco Unified Communications Manager 升级 6608 网关的端
网关	Unified Communications Manager	2002 / TCP	使用 Cisco Unified Communications Manager 升级 6624 网关的端
网关	Unified Communications Manager	2427 / UDP	媒体网关控制协议 (MGCP) 网关控制
网关	Unified Communications Manager	2428 / TCP	媒体网关控制协议 (MGCP) 传
--	--	4000-4005 / TCP	当 Cisco Unified Communications Manager 用于这些媒体的端口用作音频、视频流的虚拟实时传输协议和实时传输控制协议端口。
网关	Unified Communications Manager	5060 / TCP 和 UDP	会话初始协议 (SIP) 集间干线 (ICT)
Unified Communications Manager	网关		
网关	Unified Communications Manager	5061 / TCP	安全会话发起协议 (SIP) 和群集间干线 (ICT)
Unified Communications Manager	网关		

从（发送方）	至（监听方）	目标端口	目的
网关	Unified Communications Manager	16384 - 32767 / UDP	实时协议 (RTP)、 议 (SRTP)
Unified Communications Manager	网关		注释 Cisco Comm Mana 2457 管其 整个

应用程序和 Cisco Unified Communications Manager 之间的通信

表 36: 应用程序和 Cisco Unified Communications Manager 之间的通信

从（发送方）	至（监听方）	目标端口	目的
CTL 客户端	Unified Communications Manager CTL 提供程序	2444 / TCP	Cisco Unified Com Manager 中的证 (CTL) 提供程序
Cisco Unified Communications 应用程序	Unified Communications Manager	2748 / TCP	CTI 应用程序服
Cisco Unified Communications 应用程序	Unified Communications Manager	2749 / TCP	CTI 应用程序 (J CTIManager 之间
Cisco Unified Communications 应用程序	Unified Communications Manager	2789 / TCP	JTAPI 应用程序
Unified Communications Manager Assistant Console	Unified Communications Manager	2912 / TCP	Cisco Unified Com Manager Assistan 称 IPMA)
Unified Communications Manager Attendant Console	Unified Communications Manager	1103-1129 / TCP	Cisco Unified Com Manager Attendan (AC) JAVA RMI
Unified Communications Manager Attendant Console	Unified Communications Manager	1101 / TCP	RMI 服务器将 R 发送到这些端口
Unified Communications Manager Attendant Console	Unified Communications Manager	1102 / TCP	Attendant Consol 服务器绑定端口 器在这些端口上 息。

从（发送方）	至（监听方）	目标端口	目的
Unified Communications Manager Attendant Console	Unified Communications Manager	3223 / UDP	Cisco Unified Communications Manager Attendant Console (AC) 服务器线路状态。话务台服务器接收并注册消息，并将线路状态话务台服务器。
Unified Communications Manager Attendant Console	Unified Communications Manager	3224 / UDP	Cisco Unified Communications Manager Attendant Console (AC) 客户端向 AC 注册以获取线路和设备信息。
Unified Communications Manager Attendant Console	Unified Communications Manager	4321 / UDP	Cisco Unified Communications Manager Attendant Console (AC) 客户端向 AC 注册以进行呼叫控制。
Unified Communications Manager 与 SAF/CCD	IOS 路由器运行 SAF 图像	5050 / TCP	多服务 IOS 路由器 EIGRP/SAF 协议。
Unified Communications Manager	Cisco Intercompany Media Engine (IME) 服务器	5620 / TCP 思科建议此端口的值为 5620，但您可以在 Cisco IME 服务器上执行 add ime vapserver 或 set ime vapserver port CLI 命令以更改值。	用于与 Cisco Intercompany Media Engine 服务器 VAP 协议。
Cisco Unified Communications 应用程序	Unified Communications Manager	8443 / TCP	AXL / SOAP API，应用程序方式读取或写入第计费或电话管理应用用的 Cisco Unified Communications Manager 库。

CTL 客户端和防火墙之间的通信

表 37: CTL 客户端和防火墙之间的通信

从（发送方）	至（监听方）	目标端口	目的
CTL 客户端	TLS 代理服务器	2444 / TCP	证书信任列表 (CTL) 程序在 ASA 防火墙中

思科智能许可服务和思科智能软件管理器之间的通信

Unified Communications Manager 中的思科智能许可服务通过 Call Home 与思科智能软件服务器建立直接通信。

表 38: 思科智能许可服务和思科智能软件管理器之间的通信

从（发送方）	至（监听方）	目标端口	目的
Unified Communications Manager（思科智能许可服务）	思科智能软件管理器 (CSSM)	443 / HTTPS	智能许可服务会将许可证使用情况发送给 CSSM 以检查 Unified CM 是否为投诉。

HP 服务器上的特殊端口

表 39: HP 服务器上的特殊端口

从（发送方）	至（监听方）	目标端口	目的
终端	HP SIM	2301 / TCP	HP 代理的 HTTP
终端	HP SIM	2381 / TCP	HP 代理的 HTTP
终端	Compaq 管理代理	25375、25376、25393 / UDP	COMPAQ 管理代理 (cmaX)
终端	HP SIM	50000-50004 / TCP	HP SIM 的 HTTP

端口参考

防火墙应用程序检测指南

ASA 系列参考信息

<http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html>

PIX 应用程序检测配置指南

<http://www.cisco.com/c/en/us/support/security/pix-firewall-software/products-installation-and-configuration-guides-list.html>

FWSM 3.1 应用程序检测配置指南

http://www-author.cisco.com/c/en/us/td/docs/security/fwsm/fwsm31/configuration/guide/fwsm_cfg/inspct_f.html

IETF TCP/UDP 端口分配列表

互联网地址分配机构 (IANA) IETF 分配的端口列表

<http://www.iana.org/assignments/port-numbers>

IP 电话配置和端口利用指南

Cisco CRS 4.0 (IP IVR 和 IPCC Express) 端口利用指南

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

Cisco ICM/IPCC 企业和托管版端口利用指南

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_installation_and_configuration_guides_list.html

Cisco Unified Communications Manager Express 最佳实践安全指南

http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e30.html

Cisco Unity Express 最佳实践安全指南

http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e31.html#wp41149

VMware 端口分配列表

vCenter 服务器、ESX 主机和其他网络组件管理访问的 TCP 和 UDP 端口



第 38 章

IM and Presence Service 的端口使用信息

- [IM and Presence Service 端口使用概述](#)，第 393 页
- [表中列出的信息](#)，第 393 页
- [IM and Presence Service 端口列表](#)，第 394 页

IM and Presence Service 端口使用概述

本章介绍了 IM and Presence Service 用于群集内连接以及与外部应用程序或设备通信的 TCP 和 UDP 端口列表。其中包含实施 IP 通信解决方案时，用于在网络上配置防火墙、访问控制列表 (ACL) 和服务质量 (QoS) 的重要信息。



注释 对于这些端口，Cisco 并未验证所有可能的配置情形。如果您在使用此列表时遇到配置问题，请联系 Cisco 技术支持人员寻求帮助。

虽然几乎所有协议都是双向的，但本文档从会话发起者的角度看待方向性。在某些情况下，管理员可以手动更改默认端口号，但思科不建议将此作为最佳做法。请注意，IM and Presence Service 会严格打开多个端口以供内部使用。

本文档中的端口只适用于 IM and Presence Service。某些端口因版本而异，而且将来的版本可能会引入新的端口。因此，对于所安装的 IM and Presence Service 版本，请确保使用本文档的正确版本。

根据拓扑、设备的放置以及与网络安全设备的放置相关的服务以及所用的应用程序和电话扩展，防火墙、ACL 或 QoS 的配置将有所不同。另外，请记住，ACL 的格式因设备和版本不同而异。

表中列出的信息

此表定义了本文档中每个表中的信息。

表 40: 表信息定义

表标题	说明
从	客户端将请求发送到此端口
至	客户端在此端口上接收请求
角色	客户端或服务器应用程序或过程
协议	用于建立和结束通信的会话层协议，或用于请求和响应事务的应用层协议
传输协议	传输层协议，面向连接 (TCP) 或无连接 (UDP)
目的地 / 侦听程序	用于接收请求的端口
源 / 发送方	用于发送请求的端口

IM and Presence Service 端口列表

下表显示 IM and Presence Service 用于群集内和群集间流量的端口。

表 41: IM and Presence Service 端口 - SIP 代理请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
SIP 网关 ----- IM and Presence	IM and Presence ----- SIP 网关	SIP	TCP/UDP	5060	临时	默认 SIP 代理 UDP 和 TCP 侦听程序
SIP 网关	IM and Presence	SIP	TLS	5061	临时	TLS 服务器验证侦听程序端口
IM and Presence	IM and Presence	SIP	TLS	5062	临时	TLS 相互验证侦听程序端口
IM and Presence	IM and Presence	SIP	UDP / TCP	5049	临时	内部端口。仅限本地主机流量。
IM and Presence	IM and Presence	HTTP	TCP	8081	临时	用于来自配置代理的 HTTP 请求，用以指示配置更改。
第三方客户端	IM and Presence	HTTP	TCP	8082	临时	默认 IM and Presence HTTP 侦听程序。用于要连接的第三方客户端

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
第三方客户端	IM and Presence	HTTPS	TLS / TCP	8083	临时	默认 IM and Presence HTTPS 侦听程序。用于要连接的第三方客户端

表 42: IM and Presence Service 端口 - Presence Engine 请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence	IM and Presence (Presence Engine)	SIP	UDP / TCP	5080	临时	默认 SIP UDP/TCP 侦听程序端口
IM and Presence (Presence Engine)	IM and Presence (Presence Engine)	Livebus	UDP	50000	临时	内部端口。仅限本地主机流量。LiveBus 消息传送端口。IM and Presence Service 使用此端口进行群集通信。

表 43: IM and Presence Service 端口 - Cisco Tomcat WebRequests

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
浏览器	IM and Presence	HTTPS	TCP	8080	临时	用于 web 访问
浏览器	IM and Presence	AXL / HTTPS	TLS / TCP	8443	临时	提供通过 SOAP 访问数据库和功能配置的权限
浏览器	IM and Presence	HTTPS	TLS / TCP	8443	临时	提供 Web 管理访问权限
浏览器	IM and Presence	HTTPS	TLS / TCP	8443	临时	提供用户选项页面的访问权限
浏览器	IM and Presence	SOAP	TLS / TCP	8443	临时	可以通过 SOAP 访问 Cisco Unified Personal Communicator、Cisco Unified Mobility Advantage 和第三方 API 客户端的权限

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
浏览器	即时消息和在线状态	HTTPS	TCP	9463	临时	SSL 上的超文本传输协议 (HTTPS) 仅支持 TLS1.3 (v6)。

表 44: IM and Presence Service 端口 - 外部公司目录请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence ----- 外部公司目录	外部公司目录 ----- IM and Presence	LDAP	TCP	389 / 3268	临时	允许目录协议与外部公司目录集成。LDAP 端口取决于公司目录（389 为默认值）。对于 Netscape Directory，客户可以配置不同的端口来接受 LDAP 流量。 允许 LDAP 在 IM&P 和 LDAP 服务器之间通信以进行验证。
IM and Presence	外部公司目录	LDAPS	TCP	636	临时	允许目录协议与外部公司目录集成。LDAP 端口取决于公司目录（636 为默认值）。

表 45: IM and Presence Service 端口 - 配置请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence（配置代理）	IM and Presence（配置代理）	TCP	TCP	8600	临时	配置代理心跳端口

表 46: IM and Presence 服务端口 - 证书管理器请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence	证书管理器	TCP	TCP	7070	临时	内部端口 - 仅限本地主机流量

表 47: IM and Presence Service 端口 - IDS 数据库请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence（数据库）	IM and Presence（数据库）	TCP	TCP	1500	临时	数据库客户端的内部 IDS 端口。仅限本地主机流量。
IM and Presence（数据库）	IM and Presence（数据库）	TCP	TCP	1501	临时	内部端口 - 用于在升级期间调出第二个 IDS 实例的备用端口。仅限本地主机流量。
IM and Presence（数据库）	IM and Presence（数据库）	XML	TCP	1515	临时	内部端口。仅限本地主机流量。数据库复制端口

表 48: IM and Presence Service 端口 - IPSec 管理器请求

从发送方	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence (IPSec)	IM and Presence (IPSec)	受限于专有环境	UDP/TCP	8500	8500	内部端口 - ipsec_mgr 守护程序用于平台数据（主机）证书群集复制的群集管理器端口

表 49: IM and Presence Service 端口 - DRF 主代理服务器请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence (DRF)	IM and Presence (DRF)	TCP	TCP	4040	临时	DRF 主代理服务端口，从本地代理、GUI 和 CLI 接受连接

表 50: IM and Presence Service 端口 - RISDC 请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence (RIS)	IM and Presence (RIS)	TCP	TCP	2555	临时	实时信息服务器 (RIS) 数据库服务器。连接到群集中的其他 RISDC 服务，以提供群集范围的实时信息

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence (AMC RTMT // SOAP)	IM and Presence (RIS)	TCP	TCP	2556	临时	适用于 Cisco RIS 的实时信息服务 (RIS) 数据库客户端。允许 RIS 客户端连接以检索实时信息
IM and Presence (RIS)	IM and Presence (RIS)	TCP	TCP	8889	8888	内部端口。仅限本地主机流量。RISDC (System Access) 用来通过 TCP 链接到 servM，以进行服务状态请求和获取回复

表 51: IM and Presence Service 端口 - SNMP 请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
SNMP 服务器	IM and Presence	SNMP	UDP	161, 8161	临时	为基于 SNMP 的管理应用程序提供服务
IM and Presence	IM and Presence	SNMP	UDP	6162	临时	本地 SNMP 代理侦听 SNMP 主代理转发的请求
IM and Presence	IM and Presence	SNMP	UDP	6161	临时	SNMP 主代理从本地 SNMP 代理侦听陷阱并转发到管理应用程序
SNMP 服务器	IM and Presence	TCP	TCP	7999	临时	用作 cdp 代理与 cdp 二进制通信的套接字
IM and Presence	IM and Presence	TCP	TCP	7161	临时	用于 SNMP 主代理和子代理之间的通信
IM and Presence	SNMP 陷阱监控	SNMP	UDP	162	临时	发送 SNMP 陷阱到管理应用程序
IM and Presence	IM and Presence	SNMP	UDP	最大值	61441	内部 SNMP 陷阱接收者

表 52: IM and Presence Service 端口 - *Racoon* 服务器请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
网关 ----- IM and Presence	IM and Presence ----- 网关	Ipsec	UDP	500	临时	启用互联网安全关联和密钥管理协议

表 53: IM and Presence Service 端口 - 系统服务请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence (RIS)	IM and Presence (RIS)	XML	TCP	8888 和 8889	临时	内部端口。仅限本地主机流量。用于侦听客户端域 RIS 服务管理器 (servM) 的通信。

表 54: IM and Presence Service 端口 - *DNS* 请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence	DNS 服务器	DNS	UDP	53	临时	DNS 服务器侦听 IM and Presence DNS 查询的端口。 到：DNS 服务器 从：IM and Presence

表 55: IM and Presence Service 端口 - *SSH/SFTP* 请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence	终端	SSH / SFTP	TCP	22	临时	许多应用程序使用它来获取对服务器的命令行访问权限。也在节点之间用于证书和其他文件交换 (sftp)

表 56: IM and Presence Service 端口 - ICMP 请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence ----- Cisco Unified Communications Manager	Cisco Unified Communications Manager ----- IM and Presence	ICMP	IP	不适用	临时	互联网控制信息协议 (ICMP)。用于同 Cisco Unified Communications Manager 服务器通信

表 57: IM and Presence Service 端口 - NTP 请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence	NTP 服务器	NTP	UDP	123	临时	Cisco Unified Communications Manager 充当 NTP 服务器。订阅方节点使用它来同发布方节点同步时间。

表 58: IM and Presence Service 端口 - Microsoft Exchange 通知请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
Microsoft Exchange	IM and Presence	HTTP (HTTPu)	1) WebDAV - HTTP /UDP/IP 通知 2) EWS - HTTP/TCP /IP SOAP 通知	IM and Presence 服务器端口（默认值为 50020）	临时	Microsoft Exchange 使用此端口来发送通知（使用 NOTIFY 消息），以指明对日历事件特定订阅标识符的更改。用于与网络配置中的任何 Exchange 服务器集成。两个端口都会创建。发送的消息类型取决于配置的日历在线状态后端网关的类型。

表 59: IM and Presence Service 端口 - SOAP 服务请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence (Tomcat)	IM and Presence (SOAP)	TCP	TCP	5007	临时	SOAP 监控器端口

表 60: IM and Presence Service 端口 - AMC RMI 请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence	RTMT	TCP	TCP	1090	临时	AMC RMI 对象端口。Cisco AMC 服务，用于 RTMT 性能监控、数据收集、日志记录和警报。
IM and Presence	RTMT	TCP	TCP	1099	临时	AMC RMI 注册端口。Cisco AMC 服务，用于 RTMT 性能监控、数据收集、日志记录和警报。

表 61: IM and Presence Service 端口 - XCP 请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
XMPP 客户端	IM and Presence	TCP	TCP	5222	临时	客户端访问端口
IM and Presence	IM and Presence	TCP	TCP	5269	临时	服务器到服务器连接 (S2S) 端口
第三方 BOSH 客户端	IM and Presence	TCP	TCP	7335	临时	HTTP 侦听端口由 XCP Web 连接管理器用于 BOSH 第三方 API 连接
IM and Presence (XCP 服务)	IM and Presence (XCP 路由器)	TCP	TCP	7400	临时	XCP 路由器主机接受端口。从开放端口配置（例如 XCP 验证组件服务）连接到路由器的 XCP 服务通常在此端口上连接。

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence （XCP 路由器）	IM and Presence （XCP 路由器）	UDP	UDP	5353	临时	MDNS 端口。群集中的 XCP 路由器使用此端口来发现彼此。
IM and Presence （XCP 路由器）	IM and Presence （XCP 路由器）	TCP	TCP	7336	HTTPS	MFT 文件传输（仅限内部）。

表 62: IM and Presence Service 端口 - 外部数据库请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence	PostgreSQL 数据库	TCP	TCP	5432 ¹	临时	PostgreSQL 数据库侦听端口
即时消息和在线状态	Oracle 数据库	TCP	TCP	1521	临时	Oracle 数据库侦听端口
IM and Presenc	MSSQL 数据库	TCP	TCP	1433	临时	MSSQL 数据库侦听端口

¹ 这是默认端口，但您可以将 PostgreSQL 数据库配置为侦听任意端口。

表 63: IM and Presence Service 端口 - 高可用性请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence (Server Recovery Manager)	IM and Presence (Server Recovery Manager)	TCP	TCP	20075	临时	Cisco Server Recovery Manager 用于提供管理 rpc 请求的端口。
IM and Presence (Server Recovery Manager)	IM and Presence (Server Recovery Manager)	UDP	UDP	21999	临时	Cisco Server Recovery Manager 用于同其对等节点通信的端口。

表 64: IM and Presence Service 端口 - 内存中的数据库复制消息

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence	IM and Presence	受限于专有环境	TCP	6603*	临时	Cisco Presence 数据存储器
IM and Presence	IM and Presence	受限于专有环境	TCP	6604*	临时	Cisco 登录数据存储器
IM and Presence	IM and Presence	受限于专有环境	TCP	6605*	临时	Cisco SIP 注册数据存储器
IM and Presence	IM and Presence	受限于专有环境	TCP	9003	临时	Cisco 在线状态数据存储器双节点 presence 冗余组复制。
IM and Presence	IM and Presence	受限于专有环境	TCP	9004	临时	Cisco 登录数据存储器双节点 presence 冗余组复制。
IM and Presence	IM and Presence	受限于专有环境	TCP	9005	临时	Cisco SIP 注册数据存储器双节点 presence 冗余组复制。

* 如果使用 `utils imdb_replication status` 命令运行管理 CLI 诊断实用程序，必须在群集中的 IM and Presence Service 节点之间配置的所有防火墙上打开这些端口。 正常操作不需要此设置。

表 65: IM and Presence Service 端口 - 内存中的数据库 SQL 消息

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence	IM and Presence	受限于专有环境	TCP	6603	临时	Cisco 在线状态数据存储器 SQL 查询。
IM and Presence	IM and Presence	受限于专有环境	TCP	6604	临时	Cisco 登录数据存储器 SQL 查询。
IM and Presence	IM and Presence	受限于专有环境	TCP	6605	临时	Cisco SIP 注册数据存储器 SQL 查询。
IM and Presence	IM and Presence	受限于专有环境	TCP	6606	临时	Cisco 路由数据存储器 SQL 查询。

表 66: IM and Presence Service 端口 - 内存中的数据库通知消息

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence	IM and Presence	受限于专有环境	TCP	6607	临时	Cisco 在线状态数据存储基于 XML 的更改通知。
IM and Presence	IM and Presence	受限于专有环境	TCP	6608	临时	Cisco 登录数据存储基于 XML 的更改通知。
IM and Presence	IM and Presence	受限于专有环境	TCP	6609	临时	Cisco SIP 注册数据存储基于 XML 的更改通知。
IM and Presence	IM and Presence	受限于专有环境	TCP	6610	临时	Cisco 路由数据存储基于 XML 的更改通知。

表 67: IM and Presence Service 端口 - 强制手动同步/X.509 证书更新请求

从（发送方）	至（监听方）	协议	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence（群集间同步代理）	IM and Presence（群集间同步代理）	TCP	TCP	37239	临时	思科群集间同步代理服务使用此端口建立用于处理命令的套接字连接。

表 68: IM and Presence Service 端口 - ICMP 请求

从（发送方）	至（监听方）	目标端口	目的
终端/IM and Presence	即时消息和在线状态	7	互联网控制消息协议。此协议号携带与回声明量。它不构成列标的端口。
即时消息和在线状态	终端/IM and Presence		

表 69: 用于 IM and Presence 的端口 - Cisco Unified CM 通信以及 IM and Presence 发布方 - 订阅方通信

从（发送方）	至（监听方）	传输协议	目的地 / 侦听程序	源 / 发送方	备注
Cisco Unified Communications Manager	IM and Presence 发布方	TCP	1500	双向	数据库客户端的内部 ID 端口。仅限本地主机流量。

从（发送方）	至（监听方）	传输协议	目的地 / 侦听程序	源 / 发送方	备注
Cisco Unified Communications Manager	IM and Presence 发布方	TCP	8443	双向	提供 Web 管理访问权限。
Cisco Unified Communications Manager	IM and Presence 发布方	TCP	1090	双向	AMC RMI 对象端口。Cisco AMC 服务，用于 RTMT 性能监控、数据收集、日志记录和警报。
Cisco Unified Communications Manager	IM and Presence 发布方	TCP	2555	双向	双向实时信息服务器 (RIS) 数据库服务器。连接到群集中的其他 RISDC 服务，以提供群集范围的实时信息。
Cisco Unified Communications Manager	IM and Presence 发布方	TCP	8500	双向	内部端口 - ipsec_mgr 守护程序用于平台数据（主机）证书群集复制的群集管理器端口。
Cisco Unified Communications Manager	IM and Presence 发布方	TCP	8600	双向	配置代理心跳端口
Cisco Unified Communications Manager	IM and Presence 发布方	UDP	123	双向	用于网络时间同步的网络时间协议 (NTP)。
IM and Presence 发布方	IM and Presence 订阅方	UDP	50000	双向	内部端口。仅限本地主机流量。LiveBus 消息传送端口。IM and Presence Service 使用此端口进行群集通信。
IM and Presence 发布方	IM and Presence 订阅方	UDP	21999	双向	Cisco Server Recovery Manager 用于同其对应节点通信的端口。
IM and Presence 发布方	Cisco Unified Communications Manager	TCP	4040	双向	从本地代理、GUI 和 CLI 接受连接的 DRF 主代理服务端口。
IM and Presence 发布方	Cisco Unified Communications Manager	TCP	8001	双向	在配置永久聊天时使用。

从（发送方）	至（监听方）	传输协议	目的地 / 侦听程序	源 / 发送方	备注
IM and Presence 发布方	Cisco Unified Communications Manager	TCP	6379	双向	在配置托管文件传输 (MFT) 时使用。
IM and Presence 发布方	IM and Presence 订阅方	TCP	7	双向	在配置外部数据库 (MSSQL) 时使用。
IM and Presence 发布方	IM and Presence 订阅方	TCP	20075	双向	Cisco Server Recovery Manager 用于提供管理 RPC 请求的端口。
IM and Presence 发布方	IM and Presence 订阅方	TCP	8600	双向	配置代理心跳端口
IM and Presence 订阅方	IM and Presence 发布方	TCP	9005	双向	Cisco SIP 注册数据存储器双节点 presence 冗余组复制。
IM and Presence 订阅方	IM and Presence 发布方	TCP	9003	双向	Cisco 在线状态数据存储器双节点 presence 冗余组复制。
IM and Presence 订阅方	IM and Presence 发布方	TCP	20075	双向	Cisco Server Recovery Manager 用于提供管理 RPC 请求的端口。
IM and Presence 订阅方	IM and Presence 发布方	TCP	9004	双向	Cisco 登录数据存储器双节点 presence 冗余组复制。
Cisco Unified Communications Manager	IM and Presence 发布方	TCP	5070	双向	在呼叫配置中使用
IM and Presence 发布方	IM and Presence 订阅方	TCP	44000	双向	在呼叫配置中使用

表 70: On-a-call_Presence

从（发送方）	至（监听方）	源端口	目标端口	协议	备注
Cisco Unified Communications Manager	IM and Presence 发布方	[37240 - 61000]	5070	TCP	
IM and Presence 发布方	XMPP 客户端 (Jabber)	5222	64846	TCP	客户端访问端口
IM and Presence 发布方	XMPP 客户端 (Jabber)	5222	56361	TCP	客户端访问端口

表 71: MS-SQL 数据库配置

从（发送方）	至（监听方）	源端口	目标端口	协议
IM and Presence 发布方	数据库	[37240 - 61000]	7	TCP

表 72: MS-SQL 永久聊天配置

从（发送方）	至（监听方）	源端口	目标端口	协议
IM and Presence 发布方	数据库	37240 - 61000	1433	TCP

表 73: 托管文件传输 (MFT) 配置

从（发送方）	至（监听方）	源端口	目标端口	协议
IM and Presence 发布方	外部文件服务器	37240 - 61000	7	TCP
IM and Presence 发布方	外部文件服务器	37240 - 61000	22	TCP
IM and Presence 发布方	外部文件服务器	37240 - 61000	5432	TCP
IM and Presence 发布方	数据库	54288 - 54292	5432	TCP

有关 SNMP 的信息，请参阅《Cisco Unified 功能配置管理指南》。

当地语言翻译版本说明

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