通过 TAC 创建支持案例

本部分包含您与 TAC 联系时需要的信息类型，以及与 TAC 人员分享信息的方式的相关详情。

对于持有有效的 Cisco 服务合同的所有客户、合作伙伴、经销商和分销商，Cisco 技术支持中心将提供每天 24 小时的优质技术支持服务。Cisco 技术支持网站提供了联机文档和工具，用于排除和解决与 Cisco 产品和技术相关的技术问题。每年 365 天、每天 24 小时都可以访问以下 URL 的网站：*http://www.cisco.com/techsupport*

使用联机 TAC 服务请求工具是发出 S3 和 S4 服务请求的最为快捷的方法。（S3 和 S4 服务请求是指网络影响较轻，或为了获取产品信息的情形。）说明您的情况之后，TAC 服务请求工具会自动提供建议的解决方案。如果使用推荐的资源后仍未解决问题，您的服务请求将交由 Cisco TAC 工程师处理。请通过以下 URL 查找 TAC 服务请求工具：*http://www.cisco.com/techsupport/servicerequest*

对于 S1 或 S2 服务请求，或者如果您没不具备 Internet 接入，请通过电话联系 Cisco TAC。（S1 或 S2 服务请求是指营运网络无法运行或严重受损情形下的请求。）我们会立即派 Cisco TAC 工程师处理 S1 和 S2 服务请求，以确保您的业务能正常运作。

要通过电话发出服务请求，请使用下面的电话号码：

亚太：+61 2 8446 7411（澳大利亚：1 800 805 227）

欧洲、中东及非洲 (EMEA)：+32 2 704 55 55

美国：1 800 553 2447

要获得 Cisco TAC 联系方式的完整列表，请访问以下 URL：*http://www.cisco.com/techsupport/contacts*

您将需要的信息

当您使用 Cisco TAC 开启案例时，必须提供一些初步信息来更好地确定和限定问题。根据问题性质的不同，您可能需要提供其他信息。如果等到开启案例之后应工程师要求才开始收集以下信息，将不可避免地会耽搁解决问题的时间。

相关主题

Cisco Live!，第 5 页
Cisco Secure Telnet，第 6 页
常规信息，第 3 页
网络布局，第 2 页
联机案例，第 4 页
问题说明，第 3 页
Remote Access，第 5 页
必需的初步信息，第 2 页

必需的初步信息

对于所有问题，都必须将以下信息提供给 TAC。收集并保存这些信息以便在开启 TAC 案例时使用，并定期更新所作的任何更改。

相关主题

常规信息，第 3 页
网络布局，第 2 页
问题说明，第 3 页

网络布局

提供物理和逻辑设置的详细说明，以及语音网络（如果适用）中涉及到的以下网络元素：

- Unified Communications Manager
  - 版本（在 Unified Communications Manager 管理中，选择**详细信息**）
  - Unified Communications Manager 的数目
  - 设置（独立、群集）
    - Unity
  - 版本（在 Unified Communications Manager 管理中）
  - 集成类型
    - 应用程序

- 安装的应用程序列表
- 每个应用程序的版本号
    - IP/语音网关
- 操作系统版本
- 显示技术（IOS 网关）
- Unified Communications Manager 负载（Skinny 网关）
    - 切换
- 操作系统版本
- VLAN 配置
    - 拨号方案—编号方案、呼叫路由

最好能够提交 Visio 或其他详图，例如 JPG。如果使用白板，您还可以通过 Cisco Live! 会话提供图表。

问题说明

提供出现问题时用户执行的逐步操作详细说明。确保提供的详细信息包括：

- 预期行为
- 观察到的详细行为

常规信息

确保随时能够获得以下信息：

- 是新安装吗？
- 如果安装的是 Unified Communications Manager 的早期版本，是否从一开始就发生了这个问题？（如果不是，近期对系统做过什么更改？）
- 该问题可重现吗？
    - 如果可重现，是在正常情况还是特殊情况下？
    - 如果不可重现，该问题出现时是否有什么特殊情况？
    - 该问题出现的频率有多高？
- 受影响的设备有哪些？
    - 如果特定设备受到影响（非随机），它们有何共同之处？

- 包含此问题涉及的所有设备的 DN 或 IP 地址（如果为网关）。

- 哪些设备位于 Call-Path 上（如果适用）？

联机案例

通过 Cisco.com 在线创建支持案例是初始方法，优先于所有其他支持案例创建方法。但高优先级案例（P1 和 P2）例外。

开启案例时，请提供准确的问题说明。提供问题说明之后，系统会返回可以为您提供即时解决方案的 URL 链接。

如果未找到可解决问题的方案，请继续将您的案例发送给 TAC 工程师。

可维护性连接器

功能配置连接器概述

您可以使用 Webex 功能配置服务轻松收集日志。该服务会自动执行查找、检索和存储诊断日志及信息的任务。

此功能会使用部署在本地的功能配置连接器。功能配置连接器在网络中的专用主机（“连接器主机”）上运行。您可以将连接器安装到以下任一组件：

- 企业计算平台 (ECP)—推荐

  ECP 使用 Docker 容器隔离、保护和管理其服务。主机和 Serviceability Connector 应用程序从云端安装。无需手动升级即可确保其为最新且安全。

  重要事项 我们建议使用 ECP。我们未来的发展将集中在这个平台上。如果您在 Expressway 上安装了功能配置连接器，则部分些新功能将不可用。

- Cisco Expressway

您可以使用功能配置服务达成以下目的：

- 服务请求的自动日志和系统信息检索
- Cloud-Connected UC 部署中 Unified CM 群集的日志收集

使用功能配置服务的好处

该服务可带来以下好处：

- 加速日志收集。TAC 工程师在诊断问题时可以检索相关日志。他们可以避免请求额外日志以及等待手动收集和交付的延迟。这种自动化可能会将您解决问题所需的时间缩短数天。
- 与 TAC 的协作解决方案分析器及其诊断签名数据库一起使用。系统会自动分析日志，发现已知问题，并建议已知的修补程序或解决办法。

TAC 对于功能配置连接器的支持

有关功能配置连接器的更多详细信息，请参阅 https://www.cisco.com/go/serviceability 或联系您的 TAC 代表。

Cisco Live!

Cisco Live! 是一种经过加密的安全 Java 小程序，可让您和您的 Cisco TAC 工程师通过使用协作 Web 浏览/ URL 共享、白板、Telnet 和剪贴板工具更有效地协作。

通过以下 URL 访问 Cisco Live!：

`http://c3.cisco.com/`

Remote Access

借助远程访问功能，您可以与所有必要设备建立终端服务（远程端口 3389）、HTTP（远程端口 80）和 Telnet（远程端口 23）会话。

注意 在设置拨入时，不要使用 **login:cisco** 或 **password:cisco**，因为它们构成了系统的漏洞。

允许 TAC 工程师通过以下方法之一远程访问设备之后，您可以很快解决许多问题：

- 具有公共 IP 地址的设备。
- 拨号访问—按首选项的递减顺序排列：模拟调制解调器、集成服务数字网络 (ISDN) 调制解调器、虚拟专用网 (VPN)。
- 网络地址转换 (NAT)IOS 和专用 Internet 交换 (PIX) 允许访问具有专用 IP 地址的设备。

确保工程师干预期间防火墙不会阻碍 IOS 流量和 PIX 流量，并确保所有必要服务（例如终端服务）在服务器上启动。

注释 TAC 会非常审慎地处理所有访问信息，未经客户同意，不会对系统作任何更改。

Cisco Secure Telnet

Cisco Secure Telnet 为 Cisco 服务工程师 (CSE) 提供对您站点上的 Unified Communications Manager 服务器的透明防火墙访问权限。

Cisco Secure Telnet 可让 Cisco Systems 防火墙内的 Telnet 客户端连接到防火墙后面的 Telnet 守护程序。此安全连接可让您远程监控和维护 Unified Communications Manager 服务器，无需修改防火墙。

注释 Cisco 只会在您允许的情况下访问您的网络。您必须提供站点的网络管理员，以帮助启动此过程。

防火墙保护

几乎所有内部网络都使用防火墙应用程序来限制外部对内部主机系统的访问。这些应用程序通过限制网络与公共 Internet 之间的 IP 连接来保护您的网络。

防火墙会自动阻止从外部发起的 TCP/IP 连接，除非软件重新配置为允许此类访问。

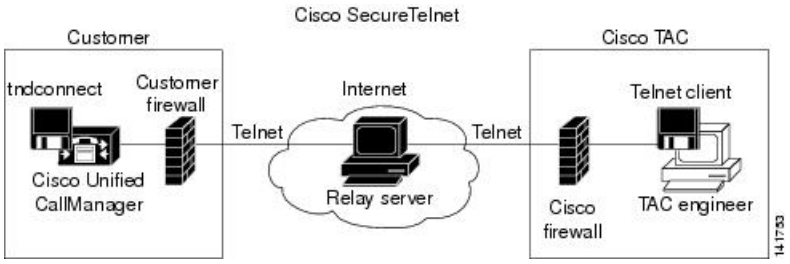
公司网络通常允许与公共 Internet 进行通信，但前提是指向外部主机的连接来自防火墙内部。

Cisco Secure Telnet 设计

Cisco Secure Telnet 利用了一个事实：可以很容易地从防火墙背后启动 Telnet 连接。使用外部代理计算机时，系统会将 TCP/IP 通信从防火墙背后中继到位于 *Cisco* 技术支持中心 (TAC) 的另一台防火墙背后的主机。

使用此中继服务器可以维护两个防火墙的完整性，同时支持受屏蔽的远程系统之间的安全通信。

图 *1: Cisco Secure Telnet* 系统



Cisco Secure Telnet 结构

外部中继服务器通过建立 Telnet 隧道在网络和 Cisco Systems 之间建立连接。这可让您将 Unified Communications Manager 服务器的 IP 地址和密码标识符传输到 CSE。

注释 密码包含您的管理员和 CSE 共同商定的文本字符串。

您的管理员通过启动 Telnet 隧道启动此过程，该隧道建立从防火墙内部到公共 Internet 上的中继服务器的 TCP 连接。然后，Telnet 隧道将与本地 Telnet 服务器建立另一个连接，在两个实体之间创建双向链路。

注释 Cisco TAC 的 Telnet 客户端与 Windows NT 和 Windows 2000 上运行的系统或 UNIX 操作系统兼容。

当您站点上的 Cisco Communications Manager 接受密码后，在 Cisco TAC 运行的 Telnet 客户端会连接到在您的防火墙背后运行的 Telnet 后台守护程序。产生的透明连接允许与本地使用机器相同的访问权限。

Telnet 连接稳定后，CSE 可以实施所有远程功能配置功能，在您的 Unified Communications Manager 服务器上执行维护、排查和故障诊断任务。

您可以查看 CSE 发送的命令和您 Unified Communications Manager 的服务器发布的响应，但命令和响应可能并非始终完全格式化。

设置远程帐户

在 Unified Communications Manager 中配置一个远程帐户，以便 Cisco 支持人员能够暂时访问您的系统进行故障诊断。

过程

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

步骤 2 在**帐户名**字段中，输入远程帐户的名称。

步骤 3 在**帐户期限**字段中，输入帐户期限，以天为单位。

步骤 4 单击**保存**。
系统将生成加密的密码短语。

步骤 5 与 Cisco 支持人员联系，向其提供远程支持帐户名和密码短语。