白皮书

安全与思科智能网络支持服务

思科® 智能网络支持服务可实现大范围的已安装的思科设备与合同管理，并为您的思科产品提供基础技术服务、设备故障诊断和风险通告功能。智能网络支持服务的智能支持服务功能可识别您的已安装的思科设备，并安全地将这些信息传送到思科数据中心；数据中心将根据思科内容丰富的知识库（包括制造、合同、技术支持和安全信息）对已安装的思科设备信息进行分析。

此主动维护打包解决方案能够改善风险管理、帮助快速解决问题，并降低运营支出。智能网络支持服务提供有价值的情报、贴切的建议、宝贵的信息和主动支持功能，帮助您降低运营成本，并最大限度地减少停机时间。

本文档主要介绍实施智能网络支持服务的安全流程，包括资产收集、与思科数据中心通讯、处理已上传的数据，以及在智能网络支持服务门户上生成报告。

目录

思科智能网络支持服务概述

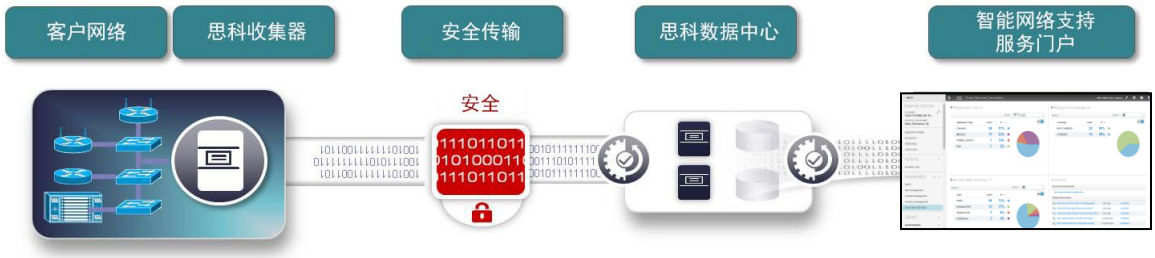
思科智能网络支持服务是新一代智能支持服务，可为您提供丰富的已安装的思科设备与合同管理功能。您的网络中连接的思科产品将显示在一个安全视图中。通过利用该视图中的信息，结合思科的专业知识，您将可以获得有价值的情报，以及有助于改善风险管理、降低成本、快速解决问题的主动支持功能。

智能网络支持服务收集器针对您的网络设备信息提供了一种数据收集机制。收集器安装在您的网络中，用于收集思科已安装的思科设备数据，并将其上传到位于思科防火墙内的思科数据中心；数据中心将使用思科内容丰富的知识库（包括制造、合同、安全和风险通告数据）对这些信息进行验证和分析。

相关信息可通过智能网络支持服务门户提供给网络管理员和用户。门户报告会显示有关您的网络中已确认的设备的详情，包括设备详细信息、技术服务覆盖、生命周期信息，以及安全与产品风险通告。

智能网络支持服务安全架构

智能网络支持服务可为您的已安装的思科设备数据提供端到端安全架构，该架构所提供的安全功能可满足所有层面的要求（包括数据收集、传输、处理、存储和查看）。



本文档将概括介绍下列重要安全功能：

- 收集器和数据收集安全
- 思科数据中心连接和数据传输安全
- 思科数据中心的数据存储
- 门户数据和离线报告的访问控制

收集器和数据收集安全

收集器安全

智能网络支持服务使用位于客户网络中的收集器，对思科设备进行唯一识别，并收集设备详细信息（如产品 ID [PID]、序列号和 IOS 版本）。客户可以选择购买针对智能网络支持服务的数据收集功能预打包的思科硬件收集器设备，也可以在客户自己提供的虚拟化环境中部署智能网络支持服务软件收集器。思科对硬件收集器和软件收集器采用相同的保护程序和保护方法。对于软件收集器，客户应根据需要验证物理主机的安全性。

智能网络支持服务采用 CentOS 发行版 Linux 操作系统。我们会在配置收集器的过程中实施安全强化措施。安全强化流程包括（但不限于）以下内容：

- 所有应用代码都将部署到按照行业标准建议强化的操作系统映像中。
- 不安全或非必要的帐户、端口、应用或服务不会被启用。
- 防火墙会按照一组专为收集器定制的默认规则进行安装和配置。
- 启用收集器配置审核与记录功能，以便为收集器的故障排除和监控提供支持。
- 收集器的特权 (**root**) 权限将仅限于管理员使用，而且该权限只能运行有限的经过强化的命令外壳。
- 用户身份验证通过基于角色的访问来实现。例如，可以为一些用户授予系统配置和管理权限，为另一些用户提供只能执行查看操作的权限。
- 收集器管理功能通过采用行业标准 HTTPS 的 Web UI 实现安全访问，以确保通讯安全。

收集器访问

收集器可以通过本地控制台或安全的 SSH（若开启）进行访问管理。该界面为命令行界面，可供管理员执行基本任务（例如 IP 地址分配，以及任何操作系统相关任务）。用于创建及管理发现与数据收集任务的用户界面则是 Web UI。有关如何访问该 Web UI 的 URL，请参考智能网络支持服务收集器快速入门指南。该 Web UI 可通过 HTTPS 协议进行访问，从而实现安全保护。

收集器密码策略要求密码至少包含九个字符（包含大写和小写字母、数字或特殊字符），且不可构成任何已知的英语单词或其他单词。此外，思科建议每 180 天更改一次用于登录收集器的非特权帐户密码以及特权帐户密码。

软件更新

软件更新管理器位于思科数据中心内，它为可上传的不同类型的收集器软件提供了一个存储库，其中包括完整版本、服务包更新、规则包和数据配置文件。

与数据收集过程相关的软件可通过收集器控制面板进行更新。控制面板包括一组命令，供客户管理员查看并下载可用更新。如果思科发现安全缺陷或漏洞，智能网络支持服务支持团队将在修复程序发布后立即将其更新到存储库中。客户可以选择按需更新或自动更新。思科建议选择自动更新选项。控制面板还可用于安装完整系统映像，使收集器通过备份恢复到其原始状态。

收集器和软件更新管理器之间的所有通讯均通过 128 位 HTTPS 安全信道进行。有关软件更新功能的详细信息，请参阅智能网络支持服务收集器快速入门指南。

收集器记录和监控

所有发生在收集器中的安全相关事件均记录在本地。系统会采用自我监控机制，以检查收集器在某些时间点的状态，并针对安全敏感型事件发出风险通告。此类事件包括（但不限于）：

- 登录尝试失败
- 安全连接或加密处理错误
- 策略配置更改
- 收集器子系统状态（例如本地数据库和文件系统）
- 从收集器用户帐户进行的数据访问
- 信息成功传输到思科数据中心

发现和收集

收集器基于设备类型收集不同的信息。为确保思科能够对设备进行唯一识别，需提供序列号和 PID。设备发现功能可通过多种方式进行控制。客户可以为发现功能选择不同的协议（如地址解析协议 [ARP]、链路层发现协议 [LLDP]、边界网关协议 [BGP] 等）。通过收集其他设备信息（包括思科操作系统版本号、主机名、IP 地址、已安装的内存和固件版本号），即可在智能网络支持服务门户报告中提供更丰富、更详细的信息。

收集器使用简单网络管理协议 (SNMP)、命令行界面 (CLI) 命令和简单对象访问协议 (SOAP) 查询设备，从而能够获得额外信息。思科 IP 电话的 MAC 地址可通过设备所注册的 Unified Communications Manager 获取。MAC 地址用于确定思科数据库中的电话。

您可以将设备排除在数据收集范围之外，也可以控制将哪些类型的网络数据传输给思科。附录 A 列出了智能网络支持服务的默认命令。

设备 SNMP 只读 (RO) 凭证和基本 TACACS 访问需要执行有效的资产数据收集。此类信息可输入或导入到收集器中，并用于数据收集过程。

您可以对数据收集功能进行配置。策略可以设置为在执行已安装的思科设备数据收集时仅使用特定协议（如 SSH 或 Telnet）。如果您对网络性能有所顾虑，智能网络支持服务数据收集正是不二之选，它不仅具有相当低的网络负载，而且还可以减少线程数量，并限制数据收集流量。有关收集器发现过程的详细信息，请参阅 CSPC 概述。

收集器的数据存储

所有收集到的资产和设备数据收集信息并非通用文件系统的一部分，并且都存储在收集器中的本地结构化查询语言 (SQL) 数据库中。所收集的设备数据不会进行加密，但是凭借一组强大的功能，设备数据收集的任何部分都可以经过屏蔽处理再嵌入或上传至思科。

数据库中的所有密码和 SNMP 社区字符串都使用 256 位 AES 加密算法进行加密。数据库记录、应用代码和备份各自使用不同的 AES 密钥。设备凭证绝不会传输给思科。

收集器可配置为存储最近 20 次数据收集作业的数据。默认值配置是可对五次数据收集作业进行存档。

数据隐私功能

智能网络支持服务的数据安全可通过数据隐私功能得到进一步的增强，从而使您能够保护 IP 地址和主机名的隐私性。在将数据发送到思科数据中心之前，您可以选择映射收集器所收集数据中的 IP 地址和主机名字段。因此，仅映射值会发送到思科数据中心；实际的物理主机名和/或 IP 地址绝不会离开您的网络。当您在门户中查看任何报告时，您需要通过实际值转换映射值。此外，思科还提供了电子表格转换宏，便于您使用所下载的报告。有关数据隐私功能的详细信息，请参阅智能网络支持服务增强型数据隐私功能应用说明。

网络中的收集器和思科产品之间的通讯

思科收集器使用多种协议从受支持的思科设备收集数据。

SNMP

思科收集器使用 SNMP RO 访问来轮询网络中的设备并从设备收集资产详细信息。

收集器执行的命令

附录 A 列出了收集器能够执行的命令列表。

SSH

思科收集器支持对网络设备的基于 SSH 的 CLI 访问。SSH 可通过加密收集器与网络设备之间的所有流量，提供一种安全的远程访问网络设备的形式。收集器支持 SSH 1.5 版和 2.0 版。思科建议使用此方法进行 CLI 访问，而非安全性较低的基于 Telnet 的会话。

表 1. 收集器的端口存储

端口	说明	入站接待	出站
22 TCP	SSH 访问	用于对收集器进行外壳访问，以执行管理任务	通过 SSH 访问在设备上执行 CLI 命令
23 TCP	Telnet		通过 Telnet 访问在设备上执行 CLI 命令
53 TCP/UDP	域名服务 (DNS)		用于与 DNS 服务器的出站连接
69 UDP	简单文件传输协议 (TFTP)	收集器 TFTP 服务侦听程序	用于连接到设备的 TFTP 服务
80 TCP	HTTP 服务		用于访问设备（如 Cisco Unified Communications Manager/IP 电话）或用于数据上传的思科 DMZ 连接服务的 HTTP 端口
161 UDP	SNMP 端口		用于对设备进行 SNMP 查询
443 TCP	SSL 连接		用于上传数据的 HTTPS 连接
514 UDP	系统日志端口	用于从设备接收系统日志消息的收集器系统日志服务	用于将消息发动到任何外部系统日志服务器
1098 TCP/UDP	Java 远程方法调用 (RMI) 激活		用于建立与 Java RMI 服务的初始连接
1099 TCP/UDP	Java RMI 端口		用于连接至执行外部 API 服务的外部 Java RMI 服务
3306 TCP/UDP	MySQL 数据库端口		用于连接至收集器设备外部的数据库服务（如果已配置）
42605 TCP	收集器 GUI/XML 端口	收集器 GUI/XML API 端口 用于从网络内部的远程设备使用收集器 GUI 客户端	用于要连接的收集器 GUI/XML API 端口
8001/8443 TCP	收集器 Web UI 端口	用于收集器 Web UI 访问	用于要连接的收集器 Web UI 端口
ICMP/IP	ICMP Ping		通过 ICMP 执行设备发现和故障排除

Telnet

思科收集器使用 Telnet 收集数据，包括设备配置、额外资产信息和关键事件后的异常数据。收集器仅需要基本的 TACACS 用户权限来收集额外资产信息。如需收集配置数据，则需要使用特权模式访问。思科建议使用可存储用户名和密码的 TACACS+ 服务器，以验证对网络设备的访问。通过适当配置 TACACS+ 服务器，此类访问允许您限制收集器可对设备执行的命令类型。对于 CLI，推荐的身份验证方法是使用允许执行所有需要的 *show* 命令的 TACACS+ 服务器。

互联网控制消息协议 (ICMP)

收集器使用 ICMP ping 消息作为发现思科设备和监控设备及网络可用性的方法。

思科数据中心连接和数据传输安全

数据传输安全性

传输数据的连接始终都是从收集器发起的，然后到达思科数据中心的思科上传服务器。在任何时候，思科上传服务器都会尝试建立到您网络中的收集器的传入连接。收集器不接受来自外部来源的传入连接。思科建议所有收集器都布置在您网络中的现有防火墙之后，以进一步强化此策略。

所有敏感设备的密码/凭证（如 SNMP 字符串和基于编码的密码）都会在关联设备配置中经过屏蔽处理，因此在传输过程中是不可见的。管理员还可以在传输之前指定要从已上传数据文件中排除的特定设备或数据串。

智能网络支持服务上传文件可经过加密并通过公共互联网传输到思科数据中心。所传输的数据将在应用层使用根据数据上传生成的基于公共密钥基础设施 (PKI) 的 128 位 AES 密钥进行加密。当终端要传输文件时，则会建立基于 SSL 连接的 HTTPS。在此 SSL 握手过程中，客户端凭证会用于身份验证。基于 SSL 的 HTTPS 将在传输层使用基于 2048 位 PKI 的系统传输加密数据。但这不包括收集器软件在应用层执行的 AES-128 加密。

数据加密具有以下特征：

- 每次上传数据都会动态生成 128 位 AES 密钥，从而加密所传输的数据。
- 不仅如此，AES 密钥本身也可使用由思科生成的公钥进行加密。
- 此外，每次安装收集器还会加入预先生成的所有收集器通用的公钥和私钥对。
- 加密数据及加密的 128 位 AES 密钥将使用安装过程中预先生成的私钥进行签名，从而形成数字签名。

利用文件导入功能，客户即可将包含额外设备信息的 .csv 文件安全上传至思科数据中心，从而扩充所收集的数据。客户管理员是唯一可以上传文件导入信息的用户。此文件将通过上文所述的基于 SSL 的 HTTPS 连接进行传输，并且数据传输与存储将使用与数据收集相同的安全策略。

数据验证

除了通过思科上传服务器进行基于密码的验证外，每个收集器都会分配到一个随机生成的唯一数字证书。此数字证书将在思科数据中心进行注册和安全存储，并将用于在数据到达后验证其真伪。在服务器检测到数据传输来自证书未注册或不存在的客户端后，将永久删除传输的数据，并且不再对其进行加密或传输。

密钥组成

公钥/私钥用于加密长度为 2048 位的 HTTPS 会话密钥。AES-128 位加密在应用层使用。传输层安全 (TLS) 会话密钥的长度为 56 位且用于流模式。如上文所述，数据将使用三种不同的密钥进行三次加密。

密钥管理

应用层加密的 PKI 密钥交换将在上传过程中动态完成。受信任的第三方外部服务器将保存用于应用层加密的公钥和用于 SSL 会话设置的公钥的最新副本。收集器支持所有 TLS 协议，并且对称密钥将在限定的会话持续时间内使用 PKI 通过加密进行交换。

上传完整性

信息摘要 5 (MD5) 校验和根据上传数据计算得出，并使用客户端的私钥在最终数据包中进行加密。文件的 MD5 值是一个与标准校验和非常类似的 128 位的值。附加长度可显著降低具有相同 MD5 值的文件发生变动和损坏的可能性。通过预先传输加密数据的 MD5 计算值，在数据到达思科数据中心后将其与数据的 MD5 值进行比较，即可验证数据的真伪。

数据上传服务器

思科在其安全 DMZ 内放置一些主机，以便接收上传的加密文件。这些主机不存储加密信息所需的密钥，只是在数据文件的完整性经过验证后将数据传输到思科防火墙后面的最终目标主机。

思科数据中心的数据存储

数据存储

思科致力于保护其存储数据的隐私性和机密性。为了保证这一点，思科将采取以下措施：

- 将处理数据的智能网络支持服务环境布置在思科防火墙的后面，并且使其处于可安全切换的网段之中。
- 所有思科 IT 计算机的安装过程均遵循一套严格的安全标准；这包括强化脚本的应用，从而保护这些计算机。
- 采用密码锁设备对这些计算机进行保护，但对密码锁设备的访问仅限于思科 IT 管理员。
- 将思科入侵检测系统部署在整个企业网络和存储数据的受限网络中。
- 仅在思科防火墙内的思科生产计算机上不对上传的网络信息进行压缩和加密。

在思科防火墙内通过严格的身份验证和访问控制措施对数据进行保护。使用在本地实施的基于角色的安全模式，通过 Oracle 应用架构授权和权限以及可靠的审核日志记录配置为数据库提供安全保护。对数据的应用级访问通过业界广泛接受的单点登录机制进行保护。

对数据中心数据的所有访问通过基于 CA SiteMinder® 的身份验证进行。机密信息（如社区字符串和密码）可在存储前进行删除。数据基于思科企业 IT 最佳实践和数据保护与保留策略进行存储。

存储策略

原始上传数据根据思科企业保留策略进行存档。原始数据在生成门户报告所在的数据中心数据库进行转换、处理和存储。数据经过处理和分析之后，即可在门户中显示。经过处理的数据可至少存档五年。

经过处理的数据将一直在门户中显示，直到下一个数据集完成上传和处理为止，届时新数据将覆盖现有数据集。如果客户想要删除上传的数据，只需上传不包含他们想要删除的信息的新数据集，即可不再在门户或离线报告中提供这些数据。之前处理的数据可进行存档，并且可在最长两年内用于 Delta 报告。

备份和恢复

已安装的思科设备数据可驻留在思科数据中心。思科每天都将进行信息备份，并且这些信息可在本地进行加密和存储。

思科系统安全验证和审核流程

通过结合使用主要版本中的静态分析和定期漏洞测试，思科能够确保产品和服务通过安全风险分析、安全标准合规性测试和漏洞扫描。借助这些流程发现的任何问题都将报告给系统，并且纠正措施也可通过思科标准缺陷和改进跟踪系统 (CDETS) 流程进行处理。

门户数据和离线报告的访问控制

智能网络支持服务门户安全

智能网络支持服务门户允许您查看有关您的网络资产和合同信息的处理信息。当您在门户中查看报告时，您公司的数据与所有其他公司的数据在逻辑上是相互隔离的。该门户具有以下安全机制：

- 唯一的授权 Cisco.com ID 和密码与用户所属授权公司进行关联
- 对您的智能网络支持服务门户的用户访问进行客户管理
- 服务器身份验证的 SSL v3
- 限时安全会话管理
- 基于角色的分级访问控制
- 事件记录和监控（如登录失败和无效的资源访问尝试）

您指定的客户管理员可对智能网络支持服务门户的访问进行控制。管理员可注册新用户和注销现有用户（例如用户离开公司或变更工作职责时）。如需了解注册或删除用户的流程，请参阅智能网络支持服务指导视频。

合同数据报告隐私

如果与合同关联的地址无法根据客户主数据记录中的地址进行验证，智能网络支持服务业务可为客户敏感数据提供逻辑保护。当前存在的多种事务都有可能影响经过验证的匹配站点信息。最可能的原因是合同中的地址尚未添加到您的思科官方客户记录中。在这种情况下，站点信息将被隐藏，并标记为“站点需要验证”(site verification required)，直到该站点添加到您公司的官方主数据客户记录中。

结论

智能网络支持服务可为您的已安装的思科设备信息收集、处理和传输到思科数据中心和智能网络支持服务门户提供安全的端到端架构，从而使您能够通过门户访问全面的报告，同时这些报告还可提供有关您的思科设备和服务合同的有价值的情报。

思科可为您的数据提供非常严格的安全保护。如需了解有关智能网络支持服务的详细信息，以及思科如何实施思科安全架构，请与您的思科销售代表或思科授权合作伙伴联系。他们将乐于为您安排技术会议，与您讨论相关问题并提供有关您的具体情况的详细信息。

其他资源

有关思科如何为客户数据隐私提供安全保护的详细信息，请参阅下列资源。其他安全详细信息将根据保密协议提供。

思科安全漏洞策略：

http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

思科隐私门户：
http://www.cisco.com/web/about/doing_business/legal/privacy_compliance/index.html#~1

智能网络支持服务指导视频：
http://www.cisco.com/E-Learning/bulk/subscribed/SNTC_3-x/index.htm

智能网络支持服务收集器快速入门指南：
http://www.cisco.com/en/US/docs/net_mgmt/inventory_and_reporting/CSPC_Quick_Start_Guide_for_SNTC.pdf

智能网络支持服务增强型数据隐私功能应用说明：
https://supportforums.cisco.com/docs/DOC-39968

公共服务平台收集器 (CSPC) 概述：
https://supportforums.cisco.com/docs/DOC-40159

附录 A：收集器命令执行参照表

表 2 列出的是可通过 Telnet 或 SSH 收集的默认 CLI 命令。

表 3 列出的是可通过 SNMP 收集的默认 SNMP MIB。

表 2：SNTC 的默认 CLI 命令

show ap summary
show c7200
show diag
show gsr chassis-info
show hardware
show idprom all
show inventory
show module
show rsp chassis-info
show running-config
show startup-config
show version

以下默认命令通过集群命令交换机的 rcommand 在集群成员交换机上执行：

cluster rcommand > show cluster
cluster rcommand > show env power
cluster rcommand > show flash
cluster rcommand > show interface
cluster rcommand > show inventory
cluster rcommand > show running-config
cluster rcommand > show startup-config
cluster rcommand > show switch
cluster rcommand > show version

表 3：SNTC 的默认 SNMP MIB

MIB	MIB 表名称
AIRESPACE-SWITCHING-MIB	agentInventoryGroup
AIRESPACE-WIRELESS-MIB	bsnAPTable
AIRESPACE-WIRELESS-MIB	bsnMobileStationTable
ALTIGA-HARDWARE-STATS	alStatsHardwareGlobal
ALTIGA-VERSION-STATS	alStatsVersionGlobal
ARROWPOINT-CHASSISMGREXT-MIB	apChassisMgrExtModuleTable
ARROWPOINT-CHASSISMGREXT-MIB	chassisMgrExt
BASIS-GENERIC-MIB	cardInformation
BASIS-SHELF-MIB	shelfTable
CALISTA-DPA-MIB	dpa
CISCO-CCM-MIB	ccmGatewayTable
CISCO-CCM-MIB	ccmGlobalInfo
CISCO-CCM-MIB	ccmGroupTable
CISCO-CCM-MIB	ccmPhoneExtnTable
CISCO-CCM-MIB	ccmPhoneTable
CISCO-CCM-MIB	ccmProductTypeTable
CISCO-CCM-MIB	ccmRegionTable
CISCO-CCM-MIB	ccmTable
CISCO-CCME-MIB	ccmeConfig
CISCO-CCME-MIB	ccmeEphoneActTable
CISCO-CCME-MIB	ccmeEphoneConfTable
CISCO-CDP-MIB	cdpCacheTable
CISCO-CLUSTER-MIB	ccCandidateTable
CISCO-CLUSTER-MIB	ccMemberTable
CISCO-ENHANCED-MEMPOOL-MIB	cempMemPoolTable
CISCO-ENTITY-ASSET-MIB	ceAssetTable
CISCO-ENTITY-FRU-CONTROL-MIB	cefcModuleTable
CISCO-FLASH-MIB	ciscoFlashDeviceTable
CISCO-FLASH-MIB	ciscoFlashFileTable
CISCO-FLASH-MIB	ciscoFlashPartitionTable
CISCO-IMAGE-MIB	ciscoImageTable
CISCO-MEMORY-POOL-MIB	ciscoMemoryPoolTable
CISCO-PROCESS-MIB	cpmCPUTotalTable
CISCO-PROCESS-MIB	cpmProcessExtTable
CISCO-PROCESS-MIB	cpmProcessTable
CISCO-RHINO-MIB	ciscoLS1010ChassisGroup
CISCO-RHINO-MIB	ciscoLS1010ModuleTable

MIB	MIB 表名称
CISCO-RHINO-MIB	ciscoLS1010SubModuleTable
CISCO-STACK-MIB	chassisGrp
CISCO-STACK-MIB	moduleTable
CISCO-STACK-MIB	systemGrp
CISCO-STACKWISE-MIB	cswGlobals
CISCO-STACKWISE-MIB	cswSwitchInfoTable
CISCO-TELEPRESENCE-CALL-MIB	ctpcInfoObjects
CISCO-TELEPRESENCE-CALL-MIB	ctpcStatObjects
CISCO-TELEPRESENCE-CALL-MIB	ctpcTable
CISCO-TELEPRESENCE-MIB	ctpPeripheralStatusTable
CISCO-UNIFIED-COMPUTING-ADAPTOR-MIB	cucsAdaptorUnitTable
CISCO-UNIFIED-COMPUTING-COMPUTE-MIB	cucsComputeBladeTable
CISCO-UNIFIED-COMPUTING-COMPUTE-MIB	cucsComputeBoardTable
CISCO-UNIFIED-COMPUTING-EQUIPMENT-MIB	cucsEquipmentFanTable
CISCO-UNIFIED-COMPUTING-EQUIPMENT-MIB	cucsEquipmentIOCardTable
CISCO-UNIFIED-COMPUTING-EQUIPMENT-MIB	cucsEquipmentPsuTable
CISCO-UNIFIED-COMPUTING-EQUIPMENT-MIB	cucsEquipmentSwitchCardTable
CISCO-UNIFIED-COMPUTING-EQUIPMENT-MIB	cucsEquipmentXcvrTable
CISCO-UNIFIED-COMPUTING-FABRIC-MIB	cucsFabricSwChPhEpTable
CISCO-UNIFIED-COMPUTING-FIRMWARE-MIB	cucsFirmwareBootUnitTable
CISCO-UNIFIED-COMPUTING-MEMORY-MIB	cucsMemoryUnitTable
CISCO-UNIFIED-COMPUTING-NETWORK-MIB	cucsNetworkElementTable
CISCO-UNIFIED-COMPUTING-PROCESSOR-MIB	cucsProcessorUnitTable
CISCO-UNIFIED-COMPUTING-STORAGE-MIB	cucsStorageLocalDiskTable
CISCO-UNIFIED-COMPUTING-VM-MIB	cucsVmInstanceTable
CISCO-VDC-MIB	ciscoVdcTable
CISCO-VIRTUAL-SWITCH-MIB	cvsChassisTable
CISCO-VIRTUAL-SWITCH-MIB	cvsCoreSwitchConfigTable
CISCO-VIRTUAL-SWITCH-MIB	cvsGlobalObjects
CPQHOST-MIB	cpqHoCpuUtilTable
CPQHOST-MIB	cpqHoInfo
CPQSINFO-MIB	cpqSiAsset
CPQSTDEQ-MIB	cpqSeCpuTable
ENTITY-MIB	entPhysicalTable
FCMGMT-MIB	connUnitTable
HOST-RESOURCES-MIB	hrDeviceTable
HOST-RESOURCES-MIB	hrDiskStorageTable
HOST-RESOURCES-MIB	hrStorage

MIB	MIB 表名称
HOST-RESOURCES-MIB	hrStorageTable
HOST-RESOURCES-MIB	hrSWInstalledTable
IF-MIB	ifTable
IF-MIB	ifXTable
IP-MIB	ipAddrTable
MSSQLSERVER-MIB	mssqlSrvTable
OLD-CISCO-CHASSIS-MIB	cardTable
OLD-CISCO-CHASSIS-MIB	chassis
OLD-CISCO-SYS-MIB	lsystem
PCUBE-SE-MIB	pmoduleTable
PCUBE-SE-MIB	pportTable
RADVISION-MIB	rvUnitGeneral
SNMPv2-MIB	系统
STARENT-MIB	starentChassis
STARENT-MIB	starFanTable
STARENT-MIB	starPowerTable
STARENT-MIB	starSlotTable
STRATACOM-MIB	shelfSlotInfoTable
SYSAPPL-MIB	sysApplInstallElmtTable
SYSAPPL-MIB	sysApplInstallPkgTable
SYSAPPL-MIB	sysApplRunTable
TOPSPIN-MIB	tsDevBackplane
TOPSPIN-MIB	tsDevCardTable
TOPSPIN-MIB	tsDevFanTable
TOPSPIN-MIB	tsDevPowerSupplyTable
UMSASSETID-MIB	iBMPSGSerialNumberInformationTable

美洲总部
Cisco Systems, Inc.
加州圣何西

亚太地区总部
Cisco Systems (USA) Pte.Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。 地址、电话号码和传真号码均列在思科网站 www.cisco.com/go/offices 中。

美国印刷 CXX-XXXXXX-XX 01/15