# Security and Cisco Smart Net Total Care Service

## Cisco Smart Net Total Care™ Service offers expert technical support and flexible hardware coverage provided by the Cisco® Technical Assistance Center (TAC). It also offers integrated smart capabilities that deliver extensive information about your installed base, contracts, and security alerts to enhance the efficiency of your support operations.

This document provides information on the security processes implemented by the Smart Net Total Care smart capabilities, including inventory collection, communication with the Cisco data center, processing the uploaded data, and reporting in the Smart Net Total Care portal.

# Contents

# Cisco Smart Net Total Care Service Overview

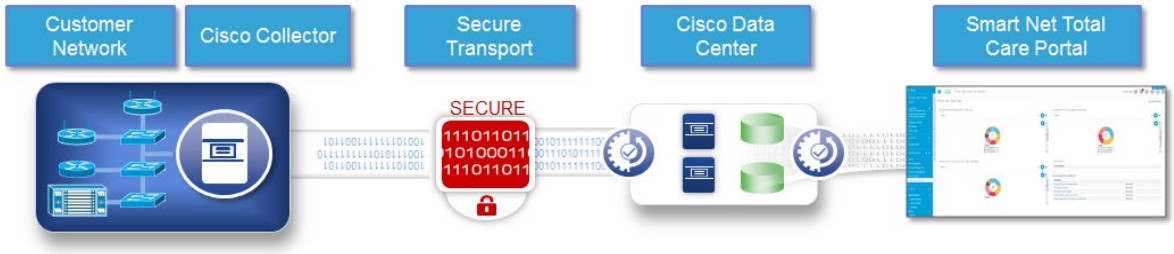
Cisco Smart Net Total Care is a smart support service that provides you with extensive installed base and contract management capabilities. Using information from a secure view of the Cisco products connected to your network, and correlating it with Cisco expertise, you receive actionable information that improves risk management, reduces costs, and speeds problem resolution.

The service uses a collector as the mechanism for gathering your network device information. The collector is installed on your network and uploads your installed base data to the Cisco data center located within the Cisco firewall where the information is validated and analyzed with our deep knowledge base of manufacturing, contract, security, and alerts data.

The resulting Information is delivered to users through the Smart Net Total Care portal. The portal reports provide detailed information about the identified equipment in your network, including device details, technical service coverage, lifecycle information, and security and product alerts.

# Smart Net Total Care Security Architecture

Smart Net Total Care provides an end-to-end secure architecture for your installed base data. The security functionality addresses all aspects including collection, transmission, processing, storage, and viewing.




Important security functionality that is outlined in this document includes:

- Securing the collector and data collection
- Secure connectivity and data transmission to the Cisco data center
- Data storage at the Cisco data center
- Controlling access to the portal data and reports

# Securing the Collector and Data Collection

### Collector Security

Smart Net Total Care uses a collector placed in your network to uniquely identify Cisco devices, and collect device details such as product identifier (PID), serial number, and IOS release. You deploy the software collector on a virtualized platform that you provide.

The CSPC collector software utilizes the CentOS 64 bit distribution of the Linux operating system.

Hardening measures applied to the CSPC software image include, but are not limited to, the following:

- All application code is deployed to an operating system image that is hardened per industry standard recommendations.
- No unsecured or non-essential accounts, ports, applications, or services are enabled.
- A firewall is installed and configured with a default set of rules tailored for the collector.
- Collector configuration auditing and logging for collector troubleshooting and monitoring is enabled.

- Privileged (**root**) access to the collector is restricted to administrator usage, with a limited and hardened command shell environment.
- Users authenticate through role-based access. For example, some users can be granted access to configure and manage the system while other users can perform view-only operations.

Collector administration functions are securely accessed through a web UI that utilizes industry-standard HTTPS for secure communications.

### Collector Access

The collector has an administrative shell that is accessible via a local console or, if enabled, via secure shell (SSH). The interface has both a web UI interface and a command-line shell interface that allows the administrator to perform basic tasks, such as creation and management of discovery and collection jobs, and operating system related tasks. The CSPC Quick Start Guide provides information on how to access the URL for the web UI. The web UI is accessible via the HTTPS protocol to enforce security.

Collector password policy requires passwords to be a minimum of nine characters in length and must contain upper case and lower case letters, numbers and special characters. In addition, we recommend changing passwords for both the nonprivileged account used to log in to the collector as well as the privileged password, every 90 days.

### Software Updates

The software update manager is located in the Cisco data center, and provides a repository for the collector software that can be updated.

A collector web UI is used to update software related to the collection process. The UI includes the ability for the customer administrator to check for updates and download them as available. If a security flaw or vulnerability is discovered by Cisco, an update will be made available as soon as a fix has been released. You have the option to choose between on-demand or automatic updates. We recommend selecting the automatic option.

All communications between the collector and the software update manager are conducted over a 128-bit HTTPS secured channel. For more details on the software update functionality, please refer to the CSPC Upgrade Guide.

### Collector Logging and Monitoring

All security sensitive events occurring on the collector are logged locally. Self-monitoring is used to examine the state of the collector at certain points in time and provide alerts on security sensitive events. This includes, but is not limited to:

- Unsuccessful login attempts
- Secure connectivity or cryptographic processing errors
- Policy configuration changes
- Collector subsystems status, such as the local database and file system
- Data access from collector user accounts
- Successful transmission of information to the Cisco data center

### Discovery and Collection

The collector gathers different pieces of information based on the device type. A serial number and PID are required to enable the software to uniquely identify a device. Device discovery can be controlled by several methods. The customer can choose different protocols for discovery, such as Address Resolution Protocol (ARP), Link Layer Discovery Protocol (LLDP), Border Gateway Protocol (BGP) and others. Additional device information, including Cisco OS version number, host name, IP address, memory installed, and firmware version number is collected to provide richer, more detailed information in Smart Net Total Care portal reports.

The collector queries the devices using Simple Network Management Protocol (SNMP), command-line interface (CLI) commands, and Simple Object Access Protocol (SOAP) to get the additional information. For Cisco IP phones, MAC addresses are obtained from the Unified Communications Manager with which the device is registered. The MAC addresses are used to identify the phones within the Cisco database.

Devices can be excluded from collection, and you can control what type of network data will be transferred to Cisco. Appendix A lists the default commands for Smart Net Total Care.

Device SNMP read-only (RO) credentials and basic TACACS access are required to perform a valid inventory collection. This information is entered on or imported to the collector, and used in the collection process.

Collection functionality can be configured. Policies can be set such that only a certain protocol such as SSH or Telnet is used during installed base collection. Smart Net Total Care data collection places a very light load on the network, and it is also possible to reduce the number of threads and throttle the collection traffic if network performance is a concern.

## Data Storage on the Collector

All collected inventory and device collection information is stored in a local structured query language (SQL) database on the collector, not as part of the general file system. The collected device data is not encrypted, but there is default masking of the passwords and SNMP strings before they are stored. There is a robust set of capabilities such that any portion of a device collection can be masked before insertion into the database or upload to Cisco.

All passwords and SNMP community strings are encrypted in the database with 256-bit AES encryption. There are different AES keys for database records, application code, and backups respectively. Device credentials are never transmitted to Cisco.

The collector can be configured to store data for the most recent 20 collection jobs. The default value configuration is for five data collections to be archived.

The collector can store passwords for local application and API access accounts. The passwords are stored as PBKDF2WithHmacSHA1 hashes.

## Data Privacy Feature

Data security can be enhanced further in Smart Net Total Care with the data privacy feature, which enables you to keep your IP addresses and hostnames private. You have the option to map the IP address and hostname fields in the data gathered by the collector before the data is sent to the Cisco data center. As a result, only the mapped values are sent to the Cisco data center; the actual hostname and/or IP address never leaves your network. You will need to translate the mapped values with actual values when reviewing any reports in the portal. Spreadsheet translation macros are provided for you to use with downloaded reports.

## Communication Between the Collector and Cisco Products on Your Network

A Cisco collector gathers data from supported Cisco devices using a variety of protocols.

### SNMP

The Cisco collector uses SNMP RO access to poll the devices in the network and collect inventory details from the devices.

### Commands Executed by the Collector

A list of commands that the collector is capable of executing is listed in Appendix A .

### SSH

The Cisco collector supports SSH-based CLI access to network devices. SSH provides a secure form of remote access to network devices by encrypting all traffic, including passwords, between the collector and devices on the network. The collector supports both SSH version 1.5 and 2.0. We recommend using this method for CLI access instead of less secure Telnet-based sessions.

**Telnet**

The Cisco collector uses Telnet to collect data for device configuration, additional inventory information, and exception-based data following critical events. The collector requires only basic TACACS user privileges to collect additional inventory information. Privileged mode access is required if configuration data needs to be collected. We recommend the use of a TACACS+ server that stores usernames and passwords to authenticate access to network devices. This type of access allows you to limit the types of commands that the collector can execute on the devices by appropriate configuration of the TACACS+ server. The recommended authentication method for the CLI is to use a TACACS+ server allowing all *show* commands needed.

**Internet Control Message Protocol (ICMP)**

The collector uses ICMP ping messages as a method of discovering Cisco devices and monitoring device and network availability.

Table 1. Port Usage in the Collector

| Purpose | Protocol | Type | Inbound Port | Outbound Port |
|---|---|---|---|---|
| Data Upload | **HTTP** | **TCP** | **NA** | **80** |
| | HTTPS/TLS | TCP | NA | 443 |
| | XMPP | TCP | NA | 5222 |
| | IPsec | UDP | NA | 4500 |
| Data Collection Discovery | ICMP-Echo | IP | | |
| | SNMP | UDP | NA | 161 |
| | TFTP | UDP | 69 | NA |
| | SSH | TCP | NA | 22 |
| | Telnet | TCP | NA | 23 |
| | HTTP | TCP | NA | 80 |
| | HTTPS | TCP | NA | 443 |
| | Syslog | UDP | 514 | NA |
| | FTP | TCP | 20, 21 | NA |
| | TL1 | TCP | NA | 3083 |
| | WMI | TCP | NA | 135 |
| | SNMP TRAP | UDP | 162 | NA |
| Lifecycle Management | HTTPS | TCP | NA | 443 |
| CSPC Administration | HTTPS | TCP | 8001 | NA |
| | FTP | TCP | NA | 20, 21 |
| | LDAP | TCP | NA | 389/636 |
| | TACACS | TCP | NA | 49 |
| | RADIUS | UDP | NA | 1812/1813 |
| | SNMTP | TCP | NA | 25 |
| | SSH | TCP | 22 | NA |

# Secure Connectivity and Data Transmission to the Cisco Data Center

### Data Transport Security

The connection for transferring data is always initiated from the collector to the Cisco upload server in the Cisco data center. At no point will the Cisco upload servers attempt to establish incoming connections to the collector in your network. The collector does not accept incoming connections from external sources. We recommend that all collectors be placed behind existing firewalls within your network to further reinforce this policy.

All sensitive device passwords/credentials – such as SNMP strings and encoded enable passwords – are masked in the associated device configurations so they are not visible during transport. Administrators are also able to specify specific devices or data strings to be excluded from the uploaded data file prior to transport.

Smart Net Total Care upload files are encrypted and transferred over the public Internet to the Cisco data center. The transferred data is encrypted at the application layer using a public key infrastructure (PKI) based 128-bit AES key that is generated per data upload. When an end-point wants to transfer a file, an HTTPS over SSL connection is established. During this SSL handshake, client certificates are used for authentication. The HTTPS over SSL transfer encrypts data at the transport layer using a 2048-bit PKI based system. This is in addition to the AES-128 encryption performed at the application layer by the collector software.

The data encryption has the following characteristics:

- A 128-bit AES key is generated dynamically for every data upload to encrypt the data transferred.
- The AES key itself is also encrypted with the public key generated by Cisco.
- In addition, every collector installation includes a pre-generated public and private key pair.
- The encrypted data plus the encrypted 128-bit AES key is signed using the private key pregenerated during installation to form the digital signature.

The file import capability allows you to augment collected data by securely uploading a .csv file which contains additional device information to the Cisco data center. The customer administrator is the only user who can upload file import information. The file is transferred using an HTTPS over SSL connection as described above, and data is transported and stored with the same secure methods as collected data.

### Data Authentication

In addition to the password-based authentication with the Cisco upload servers each collector is assigned a unique, randomly generated digital certificate. This digital certificate is registered and securely stored at the Cisco data center and is used to validate the authenticity of the data after arrival. Data transfers from clients with unregistered or nonexistent certificates are permanently deleted upon detection and never decrypted or transferred further.

### Key Composition

The public/private keys used to encrypt the HTTPS session keys are 2048 bits in length. AES-128 bit encryption is used at the application layer. The transport layer security (TLS) session key is 56-bits in length and is used in stream mode. As described in the previous section, the data is encrypted three times using three different keys.

### Key Management

PKI key exchange for application layer encryption is done dynamically during the upload. Trusted third-party external servers keep an up-to-date copy of both the public key used for application layer encryption and the public key used for SSL session setup. The collector supports all TLS protocols and a symmetric key is exchanged via encryption with PKI for a timed duration of the session.

### Upload Integrity

A message digest 5 (MD5) checksum is calculated from the upload data and is encrypted in the final package using the private key of the client. The MD5 value for a file is a 128-bit value very similar to a standard checksum. The additional length dramatically reduces the possibility of a different or corrupted file having the same MD5 value. The calculated MD5 value of the encrypted data pre-transfer is compared to the MD5 value of the data once it has arrived at the Cisco data center to verify authenticity.

### Data Upload Servers

We maintain hosts in its secure DMZ to receive uploaded encrypted files. These hosts do not store the keys necessary to decrypt information and only transport data to its final destination behind the Cisco firewall after the integrity of the data file is verified.

## Data Storage at the Cisco Data Center

### Data Storage

We are committed to protecting the privacy and confidentiality of the data we store. To help ensure this, the following steps are taken:

- The Smart Net Total Care environment that processes your data is located behind the Cisco firewall and on a secure switched segment of the network.
- The installation process for all Cisco IT machines follows a rigorous standard of security; this includes the application of hardening scripts to protect these machines.
- The machines are kept in a lock-and-key facility where access is restricted to Cisco IT administrators only.
- Our intrusion detection systems are deployed throughout the corporate network and the restricted network on which the data is stored.
- The uploaded network information is uncompressed and decrypted only on production machines inside the Cisco firewalls.

The data is protected with strict authentication and access control measures within the Cisco firewall. The database is secured using a role-based security model implemented natively through Oracle application schema grants and privileges, and a robust audit logging configuration. Application-level access to the data is protected through a single sign-on mechanism that is well accepted in the industry.

All access to data center data is through CA SiteMinder®-based authentication. Confidential information, such as community strings and passwords, is removed before storage. Data is stored according to our corporate IT best practices and data protection and retention policies.

### Storage Policies

Raw upload data is archived per our enterprise retention policies. The raw data is converted, processed, and stored in the data center database from which the portal reports are generated. Once the data is processed and analyzed, it is made available for display in the portal. Processed data is archived for two years.

Processed data is shown in the portal until the next set of data is uploaded and processed, at which point the existing set is overwritten with the new data. If the customer wants to remove uploaded data so that it is no longer available in the portal or offline reports, they can do so by uploading a new set of data that does not contain the information they wish to remove. Previous processed data is archived and is made available for Delta reports for a maximum of two years.

### Backup and Recovery

Installed base data resides at a Cisco data center. We back up information daily, and the information is stored locally.

### Cisco's Processes to Verify and Audit the Security of its Systems

Software developed for the collector and the datacenter is subject to the Cisco Secure Development Lifecycle (CSDL) process. CSDL uses a combination of static analysis at major releases and regular vulnerability testing to ensure products and services undergo security risk analysis,

security standards compliance testing, and vulnerability scans. Any issues discovered by these processes are reported and corrective action is handled through the standard Cisco Defect and Enhancements Tracking System (CDETS) process.

The collector software also periodically undergoes a rigorous security evaluation and is certified from an external security auditing agency.

# Controlling Access to the Portal Data and Reports

### Smart Net Total Care Portal Security

The Smart Net Total Care portal allows you to review processed information about your own network inventories and contract information. Your company's data is logically segregated from data from all other companies when viewing reports in the portal. The portal has the following security mechanisms in place:

- Unique, authorized Cisco.com ID and password, linked to the entitled company of the user
- Customer administration of user access to your Smart Net Total Care portal
- Server authenticated SSL v3
- Secured session management with expiration
- Hierarchical role-based access control
- Event logging and monitoring, such as failed logins and invalid resource access attempts

Your designated customer administrator controls access to the Smart Net Total Care portal. The administrator can register new users and de-register existing users; for example, if the user leaves the company or changes job responsibility. The process to register or remove users is documented in the Smart Net Total Care How-To videos.

### Contract Data Report Privacy

Smart Net Total Care business logic protects customer sensitive data if an address associated with a contract cannot be validated against the addresses in the customer's master data record. There are a variety of transactions that may impact the validated match of site information. The most likely reason is that the address on a contract may not have been added to your official customer record. In this case, the site information will be hidden, and will be labeled as "site verification required," until the site is added to your company's official master data customer record.

# Conclusion

The Smart Net Total Care smart capabilities provide a secure end-to-end architecture for the collection, processing, and transmission of your installed base information to the Cisco data center and the portal where you can access comprehensive reports that provide actionable intelligence about your Cisco devices and service contracts.

We take the security of your data very seriously. If you need further details about Smart Net Total Care and how we implement our security architecture, contact your Cisco sales representative or your Cisco authorized partner. They will be happy to set up a technical meeting to discuss your questions and provide details about your specific situation.

# Additional Resources

For more information about how we guard the privacy of customer data, refer to the following. Additional security details are available under non-disclosure agreement.

Cisco Security Vulnerability Policy:
http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

Cisco Privacy Portal:
http://www.cisco.com/web/about/doing_business/legal/privacy_compliance/index.html#~1

Smart Net Total Care How-To Videos:
https://www.cisco.com/c/en/us/support/services/sntc-portal/video-resources.html

Smart Net Total Care Collector Quick Start Guide:
http://www.cisco.com/c/dam/en/us/support/docs/cloud-systems-management/common-services-platform-collector-cspc/CSPC-Quick-Start-Guide.pdf

# Appendix A: Collector Command Execution Reference

Table 2 lists the default CLI commands that can be collected via Telnet or SSH.

Table 3 lists the default SNMP MIBs that can be collected via SNMP.

Table 2: Default CLI Commands for SNTC

| |
|---|
| 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 |

The default commands below are executed on a cluster member switch via rcommand from the cluster command switch:

| |
|---|
| 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 |

Table 3: Default SNMP MIBs for SNTC

| MIB | MIB Table Name |
|---|---|
| **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 |

| MIB | MIB Table Name |
|---|---|
| **CISCO-RHINO-MIB** | ciscoLS1010ModuleTable |
| **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 |

| MIB | MIB Table Name |
|---|---|
| **HOST-RESOURCES-MIB** | hrDiskStorageTable |
| **HOST-RESOURCES-MIB** | hrStorage |
| **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** | system |
| **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 |

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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



Printed in USA

Cxx-xxxxxx-xx 06/21