Preface

About This Preface

This preface describes the objectives, audience, organization, and conventions of this document, and explains how to find additional information on related products and services. It contains the following sections:

- Document Objective, page v
- Audience, page v
- Document Organization, page vi
- Document Conventions, page vi
- Syntax Conventions, page vii
- Documentation Suite, page ix
- Obtaining Documentation, page ix
- Documentation Feedback, page x
- Cisco Product Security Overview, page x
- Obtaining Technical Assistance, page xi
- Obtaining Additional Publications and Information, page xiii
- Summary History of Document Changes, page xiii

Document Objective

This document describes the information regarding the Cisco Unity Express Simple Network Management Protocol (SNMP) Management Information Base (MIB). The document contains tables for you to use when using the SNMP MIB to monitor your system.

Audience

The primary audience for this document is network operators and administrators who have experience in the following areas:

- Telecommunications network operations
- Data network operations

- SNMP operation
- MIB syntax
- Telecommunications hardware
- Data network hardware

In addition, the following audiences may find this document useful:

- Software and hardware installers
- Network designers

Document Organization

This document contains the chapters listed in Table 1.

Table 1 Document Organization

Chapter	Title	Description
Chapter 1	Cisco Unity Express SNMP MIB Support	This chapter includes a description of the Cisco Unity Express MIB. It also includes the following information: • Prerequisites for the CISCO-UNITY-EXPRESS-MIB • Restrictions for the CISCO-UNITY-EXPRESS-MIB • CISCO-UNITY-EXPRESS-MIB Objects

Document Conventions

⚠

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

✎

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

🔍

Tip Means *the following information might help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

⏱

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Syntax Conventions

Syntax conventions used throughout this guide are shown in Table 2.

Table 2 Conventions

Convention	Meaning	Description/Comments
Boldface	Commands and keywords you enter as shown.	**offset-list**
Italics	Variables for which you supply values.	**command** *type interface* You replace the variable with the type of interface. In contexts that do not allow italics, such as online help, arguments are enclosed in angle brackets (< >).
Square brackets ([ ])	Optional elements.	**command** [abc] abc is optional (not required), but you can choose it.
Vertical bars (	)	Separated alternative elements.	**command** [abc	def] You can choose either abc or def, or neither, but not both.
Braces ({ })	Required choices.	**command** {abc	def} You must choose either abc or def, but not both.
Braces and vertical bars within square brackets ([{	}])	A required choice within an optional element.	**command** [abc {def	ghi}] You have three options: nothing abc def abc ghi
Caret character (^)	Control key.	The key combinations ^D and Ctrl-D are equivalent: Both mean "hold down the Control key while you press the D key." Keys are indicated in capital letters, but are not case sensitive.
A nonquoted set of characters	A string.	For example, when setting an SNMP community string to *public*, do not use quotation marks around the string; otherwise, the string will include the quotation marks.
`System prompts`	Denotes interactive sessions; indicates that the user enters commands at the prompt.	The system prompt indicates the current command mode. For example, the prompt `Router (config) #` indicates global configuration mode.

Table 2   Conventions (continued)

Convention	Meaning	Description/Comments
`Screen` font	Terminal sessions and information the system displays.	—
Angle brackets (< >)	Nonprinting characters such as passwords.	—
Exclamation point (!) at the beginning of a line	A comment line.	Comments are sometimes displayed by the Cisco IOS software.

Conventions used in the Cisco Unity Express system (such as in CLI commands) are shown in Table 3.

Table 3   Data Types

Data Type	Definition	Example

Integer	A series of decimal digits from the set of 0 through 9 that represents a positive integer. An integer may have one or more leading zero digits (0) to align the columns. Leading zeros are always valid as long as the number of digits is less than or equal to ten digits. Values of this type have a range of zero through 4294967295.	`123`
		`000123`
		`4200000000`

Signed integer	This data type has the same basic format as the integer but can be either positive or negative. When negative, it is preceded by the sign character (-). As with the integer data type, this data type can be as many as ten digits in length, not including the sign character. The value of this type has a range of minus 2147483647 through 2147483647.	`123`
		`-000123`
		`-21000000001`

Hexadecimal	A series of base-16 digits from the set of 0 through 9, a through f, or A through F. The hexadecimal number may have one or more leading zeros (0). For all hexadecimal values, the maximum size is 0xffffffff (eight hexadecimal digits).	`1f3` `01f3000`
Text	A series of alphanumeric characters from the ASCII character set, where defined. Tab, space, and double quote (" ") characters cannot be used. Text can be as many as 255 characters; however, it is recommended that you limit the text to no more than 32 characters for readability.	`EntityID` `LineSES_Threshold999`
String	A series of alphanumeric characters and white-space characters. A string is surrounded by double quotes (" "). Strings can be as many as 255 characters; however, it is recommended that you limit the strings to no more than 80 characters for readability.	`"This is a descriptive string."`

> **Note** Hexadecimal and integer fields in files may have different widths (number of characters) for column alignment.

Documentation Suite

Consult the following related documentation for information about Cisco Unity Express and the solutions it supports.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies — security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies — psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

> **Note** Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Summary History of Document Changes

Table 4 describes the document changes made after the initial release of the *Cisco Unity Express SNMP MIB Guide Release 2.2*.

Table 4 — Summary History of Document Changes

Subject	Document Number and Change Date	Change Summary
—	OL-7961-01, January 12, 2006	Initial release