About This Guide

This preface introduces the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide.* The preface contains the following sections:

- Document Objectives
- Audience
- Document Organization
- Document Conventions
- Related Documentation
- Obtaining Documentation
- Obtaining Technical Assistance

Document Objectives

This guide explains how to install and configure Cisco Subscriber Edge Services Manager (Cisco SESM) applications and related components. Internet service providers (ISPs) and network access providers (NAPs) deploy SESM to provide their end users (subscribers) with a single web interface for accessing multiple Internet services.

Audience

This guide is intended for administrators and others responsible for:

- Installing and running the SESM sample applications in Demo mode, which simulates communication with other network components
- Installing, configuring, and running the SESM sample applications in RADIUS or DESS mode, both of which require communication with other network components
- Deploying a customized SESM application

Document Organization

This guide includes the chapters shown in the following table:

Chapter	Title	Description
Chapter 1	Preparing to Install SESM	Describes prerequisites to installing SESM applications.
Chapter 2	Installing SESM	Describes how to install the Cisco Subscriber Edge Services Manager (SESM) software and bundled components, including the Security Policy Engine.
Chapter 3	SESM Configuration Management	Describes the methods for viewing and changing configuration values, including how to use the SESM remote management tool.
Chapter 4	Configuring a Jetty Container for SESM Applications	Describes how to change or fine-tune the J2EE container configuration after installation.
Chapter 5	Configuring SESM Portal Applications	Describes how to change or fine-tune the SESM portal application configuration after installation.
Chapter 6	Configuring CDAT	Describes how to change or fine-tune the CDAT configuration after installation.
Chapter 7	Configuring RDP	Describes how to change or fine-tune the RDP configuration after installation.
Chapter 8	Configuring Security Policy Engine for SESM	Describes how to change or fine-tune the SPE configuration after installation.
Chapter 9	Running SESM Components	Describes how to start and stop SESM applications, including information about memory management.
Chapter 10	Troubleshooting SESM Installation and Configuration	Describes diagnostic procedures and methods and includes some troubleshooting tips.
Chapter 11	Deploying a Captive Portal Solution	Describes how to configure the sample captive portal solution.
Chapter 12	Deploying an SESM/SSG Solution	Summarizes all of the attributes that control communication between components in the SESM deployment.
Appendix A	SESM Security	Describes the security mechanisms used in SESM.
Appendix B	Configuring an LDAP Directory for SESM Deployment	Describes how to configure LDAP directories to work with SESM.
Appendix C	Configuring RADIUS for SESM Deployments	Describes the configuration steps required to include a RADIUS server in the SESM deployment.
Appendix D	Configuring the Bundled SESM RADIUS Server	Describes the configuration options for the bundled SESM RADIUS server.
Appendix E	SESM Load Balancing	Describes load balancing options for SESM deployments.
Appendix F	Configuring the SSG for SESM Deployments	Describes basic steps for configuring the SSG to work with SESM deployments.
Index		

Document Conventions

The following conventions are used in this guide:

- *Italic* font is used for parameters for which you supply a value, emphasis, and to introduce new terms.

- **Bold** font is used for user entry and command names.

- `Computer` font is used for examples.

✏️

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

⚠️

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

Related Documentation

Documentation for the Cisco SESM includes:

- *Release Notes for the Cisco Subscriber Edge Services Manager, Release 3.1(5)*

- *Cisco Subscriber Edge Services Manager Web Developer Guide*

- *Cisco Distributed Administration Tool Guide*

- *Cisco Subscriber Edge Services Manager Solutions Guide*

- *Cisco Subscriber Edge Services Manager Installation and Configuration Guide* (this guide)

The Cisco SESM documentation is online at:

http://www.cisco.com/univercd/cc/td/doc/solution/sesm/index.htm

Documentation for the Cisco SSG is online at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_4/122b4_sg/

Information related to configuring the SSG authentication, authorization, and accounting features is included in the following locations:

- *Cisco IOS Security Configuration Guide, Release 12.2*

- *Cisco IOS Security Command Reference, Release 12.2*

If you are including the Cisco Access Registrar (a RADIUS server) in your SESM deployment, see the following documents:

- *Cisco Access Registrar 1.6 Release Notes*

- *Cisco Access Registrar User Guide*

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

http://www.cisco.com

Translated documentation is available at the following URL:

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

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages

- Order Cisco learning materials and merchandise

- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.

- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.

- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.

- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

http://www.cisco.com/register/

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, have available your service agreement number and your product serial number.