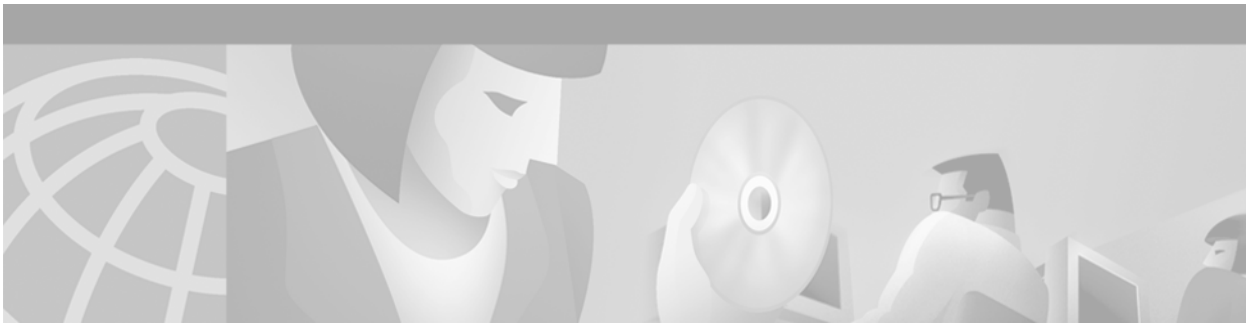

Release Notes for Cisco Subscriber Edge Services Manager, Release 3.1(1)

September 2001

These release notes contain important information regarding the Cisco Subscriber Edge Services Manager (Cisco SESM) Release 3.1(1).

Cisco SESM provides extremely robust, highly scalable connection management to Internet services. It provides the end user (the subscriber) with a single web page for accessing multiple Internet services. The ISPs and NAPs deploying Cisco SESM can customize the content of the web pages and thereby control the subscriber experience for different categories of subscribers.

Note For information about obtaining a license number, see the "Obtaining a License Number" section on page 8.

Contents

These release notes discuss the following topics:

Corporate Headquarters: Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

78-12897-01 B0

Introduction

Cisco SESM includes a set of Java-based components that are used by ISPs and NAPs to create customized web server applications. An SESM web application presents subscribers with a menu of services, enabling them to access and disconnect from different services using a web browser.

For subscribers of Internet services, SESM offers flexibility and convenience, including the ability to access multiple services simultaneously. Subscribers interact with SESM from a web page using a standard Internet browser. They do not need to download any software or plug-ins to use SESM.

For Internet service providers, SESM provides a way to control the user experience and promote customer loyalty. Service providers can change the look and feel of an SESM application, brand the application, and control the content of the pages displayed to their subscribers.

Cisco SESM Deployment Options

Cisco SESM Release 3.1(1) has three deployment options:

- RADIUS—In this deployment, the SESM web application and SSG query a RADIUS database for authentication and authorization information.
- DESS—In this deployment, the Cisco Directory Enabled Service Selection (DESS) component provides the libraries and directory schema extensions that enable queries to an LDAP directory for authentication and authorization information. The Cisco RADIUS/DESS Proxy server (the RDP Server) uses DESS to query the directory on behalf of SSG. The SESM web application also uses DESS to query the directory. In addition, DESS provides the model and libraries for implementing a role-based access control (RBAC) administration model in the directory.

  In DESS mode, changes to authentication and authorization information are immediately visible to the SESM web server application and the subscribers who are using it.
- Demo—In Demo mode, the SESM web application simulates the actions of an SESM application without using an SSG, RADIUS server, or LDAP directory.

All three deployment options are available from the same installation package. You choose the deployment option you want during the installation.

Software Components in Cisco SESM

The software components bundled in the Cisco SESM installation package are:

Component Name	Explanation
NWSP	New World Service Provider (NWSP) This component includes the NWSP sample application (including JSPs and images), SESM libraries, configuration files, and startup scripts.
Jetty	Jetty Web Server components
DESS	Directory-enabled service selection (DESS) components that provide the interface between SESM and the LDAP directory and the functionality for the role-based access control (RBAC) style authorization. The DESS components are: • DESS/AUTH class library • LDAP directory schema extensions • Top-level RBAC objects • Sample RBAC data

Component Name	Explanation
RDP	RADIUS/DESS Proxy (RDP) Server. This server responds to RADIUS requests from SSG by using the DESS application programming interface to query the LDAP directory.
CDAT	Cisco Distributed Administration Tool (CDAT). CDAT is a specialized SESM web application that administrators can use to populate and manage the DESS/AUTH extensions to the LDAP directory schema.

New World Service Provider Sample Application

The Cisco SESM installation package includes a sample SESM web server application, called the New World Service Provider (NWSP), that you can configure and subsequently execute as an example of SESM capabilities. You can create the desired look-and-feel and branded aspects of a customized SESM web server application by altering the sample application or writing your own application using the NWSP as an example.

Captive Portal Sample Application

The Cisco SESM installation package includes a captive portal sample application. This application demonstrates how several powerful features in SESM Release 3.1(1) work together to redirect unauthorized users to an SESM sign-on page immediately after opening a web browser. See the “New Features” section on page 5 for more information about this and other Cisco SESM features.

Demo Mode

The Cisco SESM installation package provides an option to install and configure a demonstration version of the NWSP and captive portal sample applications. The demo version simulates the actions of an SESM application without using an SSG, a RADIUS server, or an LDAP directory. The demo is intended for demonstration purposes only and does not predict SESM performance in a production environment.

Host Key Port Bundle Feature on SSG

The host key port bundle option is an important new feature on the SSG. The host key is a software token (or key) that uniquely identifies each subscriber currently logged on to SESM, even when multiple subscribers are using the same IP address. The host key is a unique combination of an SSG IP address from a range of IP addresses and a port number from a range of port numbers.

The host key port bundle feature provides the following advantages to SESM applications:

- The unique port identification allows SESM applications to robustly handle overlapping IP addresses, nonroutable IP addresses, and dynamically assigned IP addresses.
- The SSG IP address eliminates the need to explicitly map subscriber subnets to SSGs.

Jetty Server

SESM applications are Java 2 Platform, Enterprise Edition (J2EE) compliant web server applications. In the sample SESM application, J2EE services are provided by embedded Jetty server components from Mort Bay Consulting. The SESM installation procedure installs these Jetty server components along with the SESM application. If desired, web developers at your site can deploy a J2EE-compliant server other than the Jetty server.

Note Initially, the host key feature works only with SESM applications running on the Jetty server.

Additional Required Network Software

The following software components are used in a Cisco SESM deployment.

- Service Selection Gateway (SSG) in Cisco IOS Release 12.1(5)DC1—SSG is a feature in the Cisco IOS running on the node route processor (NRP) on the Cisco 6400 universal access concentrator (UAC).
- LDAP-compliant directory—*LDAP-compliant directory* refers to a file management server (a directory server) that conforms to the Lightweight Directory Access Protocol (LDAP). SESM is verified and officially supported to work with the Network Directory Service (NDS) eDirectory Version 8.5 from Novell, Inc. Although initial testing with the iPlanet Directory Server Version 5.0 indicates excellent results, Cisco has not fully verified it in an SESM deployment.
- RADIUS AAA Server—SSG and SESM work with any RADIUS product that can accept vendor-specific attributes (VSAs). The software is verified to work with Cisco Access Registrar (Cisco AR).

Upgrading from Cisco Service Selection Dashboard Release 3.0(1)

The Cisco Service Selection Dashboard (SSD) Release 3.0(1) software, released in June 2001, is essentially the same as SESM in RADIUS mode. An SSD Release 3.0(1) web application works in an SESM RADIUS mode deployment. See the "Upgrading from SSD Release 3.0(1)" section on page 11 for reinstallation procedures.

Upgrading from SSD Release 2.5(1) and Earlier Releases

The configuration and deployment of SESM Release 3.1(1) is different from the predecessor product, Service Selection Dashboard (SSD) Release 2.5(1) and earlier releases. The main differences are:

- The look and feel of an SESM web server application is controlled by Java Server Pages (JSPs) rather than HTML templates.
- The configuration is enhanced with the use of Java Management Extensions (JMX) and XML.

If you are currently using SSD Release 2.5(1) or earlier, see the "Upgrading from SSD Release 2.5(1)" section on page 11 for migration information.

Documentation Set

See the following documentation regarding SESM.

- *Cisco Subscriber Edge Services Manager and Subscriber Policy Engine Installation and Configuration Guide*
- *Cisco Subscriber Edge Services Manager Web Developer Guide*
- *Cisco Distributed Administration Tool Guide*
- *Cisco 6400 Feature Guide*, Chapter 4, "Service Selection Gateway"
- *Cisco 6400 Command Reference*
- *Cisco 6400 NRP–Release Notes for Cisco IOS Release 12.1(5)DC*

New Features

The key new features in SESM Release 3.1(1) are:

- Subscriber self care capabilities
- Subscriber service subscription
- Subscriber subaccount creation

The following key features were introduced in SSD Release 3.0(1):

- Captive portal
- JSP support
- Host key features, including support for overlapping IP addresses and nonroutable IP addresses
- Subscriber device and locale awareness
- Localization support

Features in Cisco SESM Release 3.1(1)

Table 1 describes the key features in Cisco SESM Release 3.1(1).

Table 1 Features in SESM Release 3.1(1)

Feature	Description
Multiple Internet service selection	An SESM web application provides a web portal from which subscribers can: • Authenticate or verify their identity • Select one or more services for connection • See which services are active in their current session and other session status information An SESM web application works in conjunction with SSG to authenticate the subscriber, to obtain the list of services that the subscriber is authorized to use, and to obtain the session status information. The SESM application sends service connection requests to SSG, which makes the connection.
Java Server Pages (JSPs)	JSPs provide a standard way to integrate Java code with HTML to present interactive, dynamically updated, personalized, and branded web pages to your subscribers.
Walled gardens, open gardens, retail pages, and service advertisements	The following features are implemented through the use of customized JSPs: • Walled Gardens—Service providers can customize the look and feel of the walled garden presentation to subscribers by altering the JSPs. Walled gardens are the services available to a subscriber that require authentication. The specific services available to each subscriber are configured in subscriber profiles and are not affected by the JSPs. • Open Gardens—Service providers can use SESM to offer open gardens, branded offerings of value-added services that do not require authentication and might be specific to the service provider. Links to these services can appear on a pre-authentication page, or you can customize the post authentication pages to include the open gardens. • Retail Pages—Wholesale providers can offer retail pages with a customized look and feel for each Internet service provider. • Service Advertisement—Service providers can use SESM to reach subscribers with targeted messages and thereby increase the acceptance of new services.

Table 1 Features in SESM Release 3.1(1) (continued)

Feature	Description
Captive portal	This feature works with the TCP redirect feature on the SSG to redirect HTTP requests for unauthenticated subscribers. • The TCP redirect feature on the SSG redirects incoming TCP packets to a specified SESM web application. With TCP redirect, service providers do not need to provide their subscribers with a URL to the SESM logon page. The subscribers are sent automatically to the logon page when they start a browser session. The TCP redirect feature in Cisco IOS Release 12.1(5)DC1 can redirect packets originating from unauthorized users, which, in effect, redirects packets from subscribers when they first open their Internet browsers and are not yet authenticated by SESM. Future releases will allow redirection based on the packet's source network or destination port. • If the SESM web application is running in captive portal mode, it has an associated captive portal application. The captive portal application: – Captures the original URL in the subscriber's request. For example, subscribers might have a home page setting, or they might open a browser and immediately enter a URL to a specific service or Internet reference page. (Original URLs are lost if you implement TCP redirect without captive portal.) – Redirects the browser to the authentication page of the main SESM application. – Includes the original URL in the redirect request, making this information available to the SESM web application. The NWSP sample application redirects the browser to the originally requested URL after successful authentication, thus honoring home page settings. You could customize your SESM web application to use this information in other ways.
Device and locale awareness	An SESM web application can detect a subscriber's preferred locale, device and browser type, and connection location and respond with web pages appropriate to the subscriber's preferred language, device capabilities, and connection type.
Single sign-on in a point-to-point (PPP) network	This feature offers a streamlined login procedure in a PPP network. A subscriber who logs on using a PPP client can access the SESM application without having to re-enter the username and password.
Host key port bundle	This feature on the SSG ensures that each currently logged-on subscriber is uniquely identified, regardless of the IP address being used. This SSG feature allows SESM applications to support the following types of subscribers: • Overlapping IP addresses in PPP and bridged environments—SESM can differentiate between various subscribers using the same IP address. • Nonroutable subscriber IP addresses—SESM supports subscribers at sites using private IP addressing schemes, including subscribers of ISPs using private addressing schemes. • Dynamic IP address assignment—The subscriber session state status within SSG and SESM remains synchronized when a subscriber's IP address changes. This feature also enhances scaling and configuration of large SESM deployments.

Table 1 Features in SESM Release 3.1(1) (continued)

Feature	Description
Highly scalable	An SESM web server application is highly scalable in the following ways: • SESM leverages the load-balancing features of J2EE technology. • When the SSG host key feature is enabled, SESM applications are completely stateless regarding subscriber sessions. SSG signals the SESM application whenever state changes occur. Therefore, the SESM applications can be started and stopped without affecting a subscriber. • The SSG host key port bundle feature simplifies large deployments because it eliminates manual mapping of subscriber subnets to SSGs.
The following features are available only when SESM is deployed in DESS mode.	
Subscriber account self care	This feature allows subscribers to change their own account details, such as address information and passwords. This subscriber updating capability relieves the service provider from time-consuming maintenance tasks. The NWSP sample application illustrates this feature.
Subscriber service subscription	This feature allows subscribers to subscribe to new services and have immediate access to those services. This feature relieves the service provider from time-consuming service enrollment tasks. It also benefits the subscriber because there is no delay in receiving access to a new service. Subscribers can also unsubscribe from a service. The NWSP sample application illustrates this feature.
Subscriber sub-account creation and management	This feature allows a subscriber with a main account to create subaccounts, with different services and access information in each subaccount. For example, a family might have subaccounts for each family member, with a different set of authorized services within each subaccount. The main account can create and delete subaccounts and subscribe to services for the subaccounts. The NWSP sample application illustrates this feature.
Cisco Distributed Administration Tool (CDAT)	CDAT is a web-based application for administrators to use in creating and maintaining the information on users, services, and access policy that is stored in an LDAP directory. The CDAT application is described in the *Cisco Distributed Administration Tool Guide.*
Role based access control (RBAC)	RBAC is an access model that allows administrators to manage groups of subscribers, rather than individuals. Using the RBAC model, administrators define roles, which have specific privileges, and groups, which have assigned roles. Individual subscribers are then assigned to a group and inherit the roles of that group. The Cisco DESS and AUTH APIs implement the RBAC model. See the *Cisco Distributed Administration Tool Guide* for more information about RBAC.

Installation Instructions

The following sections highlight some important installation information.

See the *Cisco Subscriber Edge Services Manager and Subscriber Policy Engine Installation and Configuration Guide* for complete installation instructions.

Obtaining a License Number

The SESM installation program provides for two types of installation:

- Evaluation—You can install a RADIUS mode evaluation or a DESS mode evaluation. The evaluation options do not require a license number and do not have an expiration period. An evaluation installation provides full software functionality.
- Licensed— You need a license number before deploying SESM in a production environment.

The license number is available on the License Certificate that is shipped with a purchased product. If you have purchased the product but have not yet received the CD-ROM and License Certificate, you can choose the evaluation option during installation. However, be sure to reinstall the SESM software using your license number when you receive the certificate.

The license number is important when you are requesting technical support for SESM from Cisco. After installation, you can see your license number and the software version in the licensenum.txt file under the installation directory.

Obtaining Cisco SESM Software Files

You can download the SESM software from the Cisco web site or copy it from the SESM product CD-ROM. The Cisco SESM software is contained in the following packages.

- For Sun platforms: sesm_sol.tar
- For Windows platforms: sesm_win.zip

If you purchased a contract that allows you to obtain the SESM software from the Cisco web site, follow these procedures:

Step 1 Open a web browser and go to:

http://www.cisco.com

Step 2 Click the **Login** button. Enter your Cisco user ID and password.

To access the Cisco images from the CCO Software Center, you must have a valid Cisco user ID and password. See your Cisco account representative if you need help.

Step 3 Under Service and Support, click **Software Center**.

Step 4 Click **Web Software**.

Step 5 Click **Cisco Subscriber Edge Services Manager**.

Step 6 Download the appropriate image based on the platform you intend to use for hosting the SESM web application.

SSG, RADIUS Server, and LDAP Server Status During Installation

The SSG, LDAP directory, and RADIUS components do not need to be installed and configured before you execute the Cisco SESM installation program. However, the installation program prompts you for configuration information about these components, such as IP addresses, ports, shared secrets, and other information required for the SESM components to communicate with them. You should know these values before you perform the installation. Otherwise, you will need to reconfigure the solution later.

In the case of the LDAP directory, it is advantageous to install the Cisco SESM solution when the directory is running and to have update rights to the directory. The installation program can install required extensions to the LDAP directory.

If you are installing the demo, the installation program does not prompt you for configuration information about SSGs, LDAP directories, or RADIUS servers.

Important Notes

The following sections describe some important considerations related to the Cisco SESM.

Installing on a Windows NT Platform from a CD-ROM

To install SESM on a Windows NT platform from the SESM product CD-ROM, copy the installation file from the CD-ROM onto a local drive and perform the installation using the local copy. For more information, see the explanation for caveat CSCuk27495, page 21.

Version Compatibility

The following features require support on the SSG:

- Captive portal
- Host key

To use the captive portal feature in SESM, the Cisco 6400 NRP must be running Cisco IOS Release 12.1(5)DC1 or later and the SSG TCP redirect must be configured appropriately.

To use the host key feature, the Cisco 6400 NRP must be running Cisco IOS Release 12.2(2)B or later and the SSG host key feature must be configured appropriately. The host key feature can be enabled and disabled on both the SESM and SSG products to ensure backwards compatibility.

JIT Error with Java Runtime Environment, Version 1.2.2

On Windows platforms, JRE Version 1.2.2 displays the following messages at SESM application startup:

```
A nonfatal internal JIT (3.10.107(x)) error 'Relocation error:
NULL relocation target' has occurred in
'org/apache/crimson/parser/Parser2.maybeComment (Z)Z': Interpreting method.
```

Ignore this message.

Poor Performance with Java Runtime Environment, Version 1.3.0 on Solaris

It has been observed that the performance of the Java Runtime Environment (JRE) Version 1.3.0 on Solaris is less than optimal. Later versions of the JRE may have improved performance. The reference JRE for SESM Release 3.1(1) is JRE Version 1.2.2_08.

JMX Management Console

The Sun example JMX server includes an HTML adaptor server that produces a web-based management console. This console displays the currently set values for all attributes in the XML configuration files and is useful for development environments.

However, the JMX HTML adaptor server is not production quality. For example, configuration changes that you make using this console are not persistent. You should remove this server from your configuration files before you transition the SESM application to public use.

To remove the JMX HTML adaptor server, comment out the following element in the nwsp/config/nwsp.xml file:

```
<Configure init="99"
class="com.sun.jdmk.comm.HtmlAdaptorServer"
name="com.cisco.aggbu:name=HtmlAdaptorServer">
<Set name="Port" type="int"><SystemProperty
name="management.portno"/></Set>
<Call name="start"/>
</Configure>
```

Cisco SESM Security

Cisco SESM Release 3.1(1) uses numerous security mechanisms:

- SESM uses Java technology based on the J2EE specification. SESM applications inherit the security features both of the Java language platform and the security framework in J2EE.
- SESM web server applications are deployed on a web server that enforces HTTP security.
- Because a Cisco SESM web server application plays a role in user authentication, it enforces constraints on user access.

Server Hardware

If you are using a Sun Ultra or Enterprise, you must use Solaris Version 2.6 or later. For live deployments, we recommend using an Enterprise class server with hot-swappable components and load-balancing across multiple servers. The Cisco Content Services Switch 11000 (CSS 11000) is preferred for load balancing.

For Windows NT installations, we highly recommend that you use hardware that meets the Windows NT Hardware Compatibility List (HCL) guidelines set by Microsoft with at least 64 MB of RAM (128 MB of RAM is recommended). Memory requirements are influenced by login rates, the number of subscribers concurrently logged on, and the number of services the subscribers are subscribed to use. See Chapter 5, “Running SESM Components,” in the *Cisco Subscriber Edge Services Manager and Subscriber Policy Engine Installation and Configuration Guide* for more details about memory requirements.

Upgrade Information

This section contains information about upgrading from previous releases of the software.

Upgrading from SSD Release 3.0(1)

SESM Release 3.1(1) in RADIUS mode is essentially the same as the Cisco Service Selection Dashboard (SSD) Release 3.0(1). An SSD Release 3.0(1) web application works in an SESM RADIUS mode deployment. Some changes were made in the XML Document Type Definition (DTD) for the MBean configuration files. Therefore, there are slight differences in the configuration files from those that were installed for SSD Release 3.0(1). There are a few new optional configuration parameters. Some Java APIs were deprecated, and the NWSP sample application was improved.

We recommend that you install SESM in a different directory from where you installed SSD Release 3.0(1), to preserve the configuration files (for your reference) and any JSP customizations that you made to the NWSP application. Be sure to copy the customizations into the new installation directory.

Upgrading from SSD Release 2.5(1)

This section describes how to upgrade your software from SSD Release 2.5(1) to SESM Release 3.1(1). The section discusses the following topics:

- Application Development Differences, page 11
- Configuration File Differences, page 11
- Configuration Parameter Differences, page 12

Application Development Differences

In SSD Release 2.5(1), the look and feel of the web server application was controlled by HTML templates defined for the Cisco solution.

In SESM Release 3.1(1), predefined templates are not used. Rather, you use standard JSP technology to customize the look and feel of your SESM web application.

To migrate from an SSD Release 2.5(1) web application to an SESM Release 3.1(1) web application, you must recode your application's web pages to integrate them into the JSP technology. In most cases, the design of your application presentation and the individual web page designs can be reused. SESM Release 3.1(1) allows but does not require frames. Graphic images and branding efforts can all be reused.

See the *Cisco Subscriber Edge Services Manager Web Developer Guid*e for information on creating an SESM Release 3.1(1) web server application.

Configuration File Differences

Table 2 shows configuration file differences between SSD Release 2.5(1) and SESM Release 3.1(1).

Table 2 Comparing Configuration Files in SSD Release 2.5(1) and SESM Release 3.1(1)

Configuration Files in SSD Release 2.5(1)	Configuration Files in SESM Release 3.1(1)
• dashboard.conf • servers.conf • dashboardRealm.properties • dashboard.xml	MBean configuration files, as explained in the *Cisco Subscriber Edge Services Manager and Subscriber Policy Engine Installation and Configuration Guide*

Configuration Parameter Differences

Table 3 is a reference for administrators who are familiar with SSD Release 2.5(1). The table explains how SESM Release 3.1(1) handles parameters and features that you might have implemented in SSD Release 2.5(1).

Table 3 Comparing Configuration Parameters and Features

Feature	Product Release	Sample Contents (from dashboard.conf and nwsp.xml, unless otherwise noted)
Single Sign-on	SSD 2.5(1)	`# To use SSO, set REAUTHENTICATE=off, otherwise on.` `REAUTHENTICATE=on`
	SESM 3.1(1)	`<Set name="singleSignOn" type="boolean">true</Set>`

Stress test	SSD 2.5(1)	`# STRESS_TEST=true allows the client IP address to be added to the URL. This allows a stress test client to be used,`
		`# to simulate connections from multiple IP addresses.`
		`STRESS_TEST=false`

	SESM 3.1(1)	The stress test feature is not implemented in SESM Release 3.1(1).

Demo mode	SSD 2.5(1)	`# DEMO_SSD=true will simulate an SSG and AAA server using data from the AAAFILE, otherwise false.`
		`DEMO_SSD=true`
		`# The resource or file containing user and service data for when FAKESSG=true.`
		`AAAFILE=com/cisco/aggregation/radius/util/session/aaa.txt`

	SESM 3.1(1)	The following element in the SSD MBean sets SESM to run in Demo mode.
		`<Set name="mode">Demo</Set>`
		The following element specifies the filename containing demonstration data.
		`<Configure name="com.cisco.aggbu:name=SSDDemoMode">`
		`<Set name="demoDataFile" type="java.lang.String"><SystemProperty name="application.home"/>/config/demo.txt</Set>`
		`</Configure>`

Service list format	SSD 2.5(1)	`# SERVICE_LIST=text displays service names as text; =icon displays them as images.` `SERVICE_LIST=text`
	SESM 3.1(1)	`<Put name="useIcons" type="boolean">TRUE</Put>`

Table 3 Comparing Configuration Parameters and Features (continued)

Feature	Product Release	Sample Contents (from dashboard.conf and nwsp.xml, unless otherwise noted)

Default template	SSD 2.5(1)	`# DEFAULT_TEMPLATE sets directory to find HTML images if no template directory matches a service name.`
		`# This is relative to the docRoot of the web server as defined in web.xml`
		`DEFAULT_TEMPLATE=/templates/default`

	SESM 3.1(1)	Not applicable. Templates are not used in this release.
Templates location	SSD 2.5(1)	`# TEMPLATE_ROOT_DIR is the root directory from which all template directories are enumerated.` `TEMPLATE_ROOT_DIR=/templates`
	SESM 3.1(1)	Not applicable. Templates are not used in this release.

Cache managing	SSD 2.5(1)	`# IDLE_TIMEOUT_SECONDS is the period for which a user object remains in the SSD cache.`
		`IDLE_TIMEOUT_SECONDS=86400`
		`# IDLE_TIMEOUT_SCAVENGE_INTERVAL_SECONDS is the time between checks for timed out user objects.`
		`IDLE_TIMEOUT_SCAVENGE_INTERVAL_SECONDS=3600`

	SESM 3.1(1)	Not applicable.

	SSD 2.5(1)	`# SERVICE_IDLE_TIMEOUT_SECONDS is the time before a service cache object is removed from memory.`
		`SERVICE_IDLE_TIMEOUT_SECONDS=86400`
		`# GROUP_IDLE_TIMEOUT_SECONDS is the time before a group cache object is removed from memory.`
		`GROUP_IDLE_TIMEOUT_SECONDS=86400`

	SESM 3.1(1)	`<Set name="profileCachePeriod" type="int">600</Set>`
Auto logon	SSD 2.5(1)	`# Specifies if SSD should perform service auto logons. Normally performed by SSG. Default is off.` `SSD_AUTO_LOGON=off`
	SESM 3.1(1)	`<Set name="autoConnect" type="boolean">false</Set>`
Sessions	SSD 2.5(1)	`# Initial number of session objects created in the SSD and added to a pool` `INITSESSIONPOOL=20`
	SESM 3.1(1)	Not applicable in the new SSG interface implementation.

Server URL	SSD 2.5(1)	`# Server URL. This specifies where clients go to in search of server pages.`
		`# If not specified or blank, the server name is used.`
		`SERVER_URL=`

	SESM 3.1(1)	Not applicable in this release.
Templates	SSD 2.5(1)	`# Period in seconds between checking for modified HTML files in cache for replacement.` `TEMPLATE_CLEANUP_PERIOD=3600`
	SESM 3.1(1)	Not applicable. Templates are not used in this release.

Table 3 Comparing Configuration Parameters and Features (continued)

Feature	Product Release	Sample Contents (from dashboard.conf and nwsp.xml, unless otherwise noted)

SSL redirects	SSD 2.5(1)	`# Redirect to SSL port. If set, all HTTP requests are redirected to`
		`# HTTPS at this port`
		`REDIRECT_TO_SSL_PORT=`
		`# Redirect to SSL uri. If redirecting to SSL, use this URL. If not`
		`# set use original request URI.`
		`REDIRECT_TO_SSL_URI=`
		`# Redirect to initial page. This URL is used by the Index servlet at /index.html to`
		`# redirect to the initial page`
		`REDIRECT_TO_INITIAL_URI=/templates/default/user.html`

	SESM 3.1(1)	Not applicable. Frames are not required in this release.

Authenticate level	SSD 2.5(1)	`# Authenticaton level 0=trust IP, 1=Trust SSL, 2=Trust Session 3=Trust SSL/Session`
		`4=No trust`
		`AUTHENTICATION_LEVEL=0`

	SESM 3.1(1)	This feature is implemented using a combination of HTTP sessions, cookies, and the host key feature.

Message server	SSD 2.5(1)	`# This section defines the messaging server to which the SSG can send system`
		`messages.`
		`[MESSAGING_SERVICE]`
		`# IP address of the message server, typically the same as the SSD address.`
		`IPADDRESS=127.0.0.1`
		`# Note that this port cannot be the same as a HTTPListener port as defined in`
		`dashboard.xml.`
		`PORT=9002`
		`# Maximum time in minutes for which a message is kept in the message server.`
		`MAX_MESSAGE_TIME_TO_LIVE=120`
		`# Maximum number of unread messages per user logged into the SSD.`
		`MAX_OUTSTANDING_MESSAGES_PER_USER=10`
		`# Maximum number of messages that the message server will keep absolutely.`
		`MAX_OUTSTANDING_MESSAGES=10000`

	SESM 3.1(1)	Not applicable. The SSG asynchronous messaging service is superseded by the host key feature and its ability to signal state changes.

Table 3 Comparing Configuration Parameters and Features (continued)

Feature	Product Release	Sample Contents (from dashboard.conf and nwsp.xml, unless otherwise noted)

AAA configuration, primary and secondary servers	SSD 2.5(1)	`This section defines the primary RADIUS server that the SSD queries for service profiles.`
		`[AAA_PRIMARY]`
		`PORT=1234`
		`SHAREDSECRET=cisco`
		`# Note that this must match the password defined for the service profile in the RADIUS dictionary.`
		`SERVICE_GROUP_PASSWORD=cisco`
		`TIMEOUTINSECONDS=10`
		`IPADDRESS=1.2.3.4`
		`PACKETRETRY=5`
		
		`# This section defines the RADIUS server to try if the primary times out on PACKETRETRY number of`
		`# requests and is a copy of the primary.`
		`[AAA_SECONDARY]`
		`PORT=1234`
		`SHAREDSECRET=cisco`
		`# Note that this must match the password defined for the service profile in the RADIUS dictionary.`
		`SERVICE_GROUP_PASSWORD=cisco`
		`TIMEOUTINSECONDS=10`
		`IPADDRESS=1.2.3.4`
		`PACKETRETRY=5`

	SESM 3.1(1)	`<Configure name="com.cisco.aggbu:name=AAA,connection=ServiceProfile">`
		`<Set name="timeOut" type="int">4</Set>`
		`<Set name="retryCount" type="int">3</Set>`
		`<Set name="primaryIP">127.0.0.1</Set>`
		`<Set name="primaryPort" type="int">1645</Set>`
		`<Set name="secret">cisco</Set>`
		`<Set name="secondaryIP">127.0.0.2</Set>`
		`<Set name="secondaryPort" type="int">1645</Set>`
		`<Set name="servicePassword">servicecisco</Set>`
		`<Call name="open"/>`
		`</Configure>`

SSG mappings	SSD 2.5(1)	servers.conf file

	SESM 3.1(1)	`<Configure name="com.cisco.aggbu:name=SSG">`
		`<Call name="setGlobalAttribute"><Arg>PORT</Arg><Arg>1645</Arg></Call>`
		`<Call name="setGlobalAttribute"><Arg>SECRET</Arg><Arg>cisco</Arg></Call>`
		`<Call name="setGlobalAttribute"><Arg>MASK</Arg><Arg>255.255.255.0</Arg></Call>`
		`<Call name="setGlobalAttribute"><Arg>BUNDLE_LENGTH</Arg><Arg>0</Arg></Call>`
		`<Call name="setSubnetAttribute"><Arg>10.1.1.0</Arg><Arg>255.255.255.0</Arg><Arg>IP</Arg><Arg>5.1.1.2</Arg></Call>`
		`</Configure>`

Localization	SSD 2.5(1)	localizationDB.conf file
	SESM 3.1(1)	.properties files For example, a file named message_en.properties holds English language message text. See the *Cisco Subscriber Edge Services Manager Web Developer Guide* for more information.

Caveats

Table 4 describes known problems in SESM Release 3.1(1).

Table 4 Caveats in SESM Release 3.1(1)

Caveats	Description
CSCdv02447	When CDAT displays subaccounts, it displays group membership and not blocked roles. **Workaround**: You can manipulate these values using an LDAP server administration tool, such as ConsoleOne, or by using the appropriate NWSP application self-care feature to modify the roles of a subaccount.
CSCdu12277	The status entry for a service in the NWSP application does not show bytes in/out. The byte and packet counts are currently not available from the SSG, but will be supported in a future release of SSG. **Workaround**: None.
CSCdu12329	The installation application does not check for incorrect entries, based on either content or format. **Workaround**: Make sure to enter the correct details during the installation.
CSCdv19095	When you install the DESS component, and you check the Extend Schema option, the installation program does not provide a warning message if it fails to extend the directory schema due to a permissions problem. **Workaround**: Make sure to enter a directory administrator with permissions to extend the directory schema if you want the installation program to perform that task. Also, use a directory administration tool, such as ConsoleOne, to check the schema after installation to ensure that the DESS and AUTH extensions were applied. If not, use ConsoleOne to grant schema extension permissions to a user. Then rerun the installation, using the correct user when you are prompted for a directory administrator.
CSCuk24636	In a Point-to-Point Protocol (PPP) deployment using the single sign-on (SSO) feature, if the subscriber logs off from the SESM web application, the SSO feature does not subsequently work for that subscriber for the same IP address. **Workaround**: Remove the logout button from SESM applications that will be used in PPP with SSO deployments. Subscribers can end their sessions by terminating the PPP session.

Table 4 Caveats in SESM Release 3.1(1) (continued)

Caveats	Description

CSCuk26887	If the default language of the Java virtual machine (JVM) is not English, the NWSP web application does not correctly display resources from resource bundles. In some circumstances, messages not intended for the end user appear.
	
	The default JVM language is normally the default language of the operating system on the Windows NT or Solaris server.
	
	Workarounds: There are three workarounds to this problem:
	
	1. Rename the installed resource bundle files
	2. Specify a default locale in the NWSP application code
	3. Change the default language of the JVM to English
	
	Rename the Installed Resource Bundle Files
	
	The installed resource files are named specifically for the English locale. You can change the names to the conventional default names, which work for all locales, or change the names to match the default language of your JVM. For example, rename resource_en.properties to resource.properties (the default name, which matches all locales) or resource_it.properties (to match the Italian locale), and so on. The messages still appear in English, unless you translate the contents of the files.
	
	To rename the resource bundle files, follow these procedures.
	
	1. Rename nwsp/docroot/WEB-INF/classes/messages_en.properties
	2. In nwsp/docroot/WEB-INF/lib:
	– Unbundle com.cisco.aggbu.contextlib.jar
	– Rename com/cisco/aggbu/radius/ssgError_en.properties
	– Bundle com.cisco.aggbu.contextlib.jar
	– Unbundle ssd.jar
	– Rename com/cisco/aggbu/ssd/core/exceptions/resource_en.properties
	– Rename com/cisco/aggbu/spis/dess/resource_en.properties
	– Bundle ssd.jar
	
	Note Use an extraction tool, such as WinZip, to unbundle and rebundle jar files.
	
	3. Restart the NWSP web application. You do not need to recompile the application.
	
	Specify a Default Locale in the NWSP Application Code
	
	This workaround overrides the default locale of the JVM by specifying a default for the application.
	
	1. In nwsp/docroot/decorator/createLocaleDimension.jspi, add a line that specifies the default locale to use. For example, to make the NWSP use the Italian locale (IT):
	
	`l10n:context`
	`locale='<%= new Locale("it","IT") %>' **Add this line**`
	`resourceBundleName="messages"`
	`scope="<%= pageContext.SESSION_SCOPE %>"`
	
	The locale of the browser overrides the default locale, which works if the resource bundle file names either match the browser's locale (for example, resource_fr.properties) or use the default names that work for all locales (for example, resource.properties).

Table 4 Caveats in SESM Release 3.1(1) (continued)

Caveats	Description
CSCuk26887 *(continued)*	2. Recompile and restart the NWSP application. Alternatively, if precompilation is not required, replace nwsp/docroot/WEB-INF/web.xml by web.recompile.xml and restart the NWSP application on a machine with a JDK. See the *Cisco Subscriber Edge Services Manager Web Developer Guide* for more information about recompiling NWSP. **Change the Default Language of the JVM to English** To change the default JVM language on Windows NT: 1. From the Start Menu, choose **Settings > Control Panel > Regional Options**. 2. In the Locale drop down box, choose any of the English language locales. To change the default JVM language on Solaris, follow instructions in the operating system documentation.
CSCuk26904	In CDAT, if you attempt to change the description of a service from the existing text to an empty string, an AccessException error occurs. **Workaround**: Do not change the service description field to an empty field. If there is no other description, enter the service name in the description field.
CSCuk26909	CDAT does not include fields for setting the state and postal code for a subscriber. **Workaround**: Use an LDAP server administration tool, such as ConsoleOne, or the self-care feature in the SESM web application (NWSP) to set these values.
CSCuk26929	The NWSP application does not allow a subscriber to log off from a service within a service group. **Workaround**: Correct the JSP that controls service logoffs as follows: 1. Edit the nwsp/docroot/serviceLogoff.jsp file. 2. Replace lines 54 to 66 in the file serviceLogoff.jsp with lines 62-66 and 72-112 from nwsp/docroot/serviceLogon.jsp. 3. In the copied code, replace the three references to serviceLogon.jsp with serviceLogoff.jsp in the Log.debug statements. 4. Recompile the NWSP application and restart it. Alternatively, if precompilation is not required, replace nwsp/docroot/WEB-INF/web.xml by web.recompile.xml and restart the NWSP application on a machine with a JDK. See the *Cisco Subscriber Edge Services Manager Web Developer Guide* for more information about recompiling NWSP.

Table 4 Caveats in SESM Release 3.1(1) (continued)

Caveats	Description

CSCuk26956	In the NWSP application deployed in DESS mode, if you create a subaccount and then subsequently change attributes for that subaccount, the modifications do not appear until the cache period for the authentication token expires. The changes are written to the directory but not to the cached object.
	
	Workaround: Tune the cache aging parameters to low values to minimize the time it takes the token to expire in the cache. You might notice a slight performance impact from this workaround. Follow these procedures:
	
	1. Edit the NWSP configuration file (nwsp/config/nwsp.xml).
	2. Find the DESSMode Configure element, which starts as follows:
	`<Configure jmxname="com.cisco.aggbu:name=DESSMode">`
	3. Set tokenCheckInterval to 1 and tokenMaxAge to 0, as follows:
	`<Set name="tokenCheckInterval" type="int">1</Set>`
	`<Set name="tokenMaxAge" type="int">0</Set>`
	These values cause changes to subaccount permissions to appear after a minute.
	4. Restart the NWSP application.

CSCuk26964	During RDP installation, if you choose the Add Services button, the installation program does not correctly change the rdp.xml file to add the handler that implements the RDP add services feature.
	
	Workaround: To implement the RDP add services feature, manually edit the rdp.xml configuration file, as follows:
	
	1. Edit the rdp.xml file.
	2. Find the RDPPacketFactory configure element, which starts as follows:
	`<Configure jmxname="com.cisco.aggbu:name=RDPPacketFactory">`
	3. Go to the second addType call. Find the following line:
	`<Arg>com.cisco.aggbu.rdp.UserLogonFramedPacket</Arg>`
	Replace the above line with the following line:
	`<Arg>com.cisco.aggbu.rdp.UserLogonFramedAddServicesPacket</Arg>`

Table 4 Caveats in SESM Release 3.1(1) (continued)

Caveats	Description
CSCuk26973	If you access the NWSP application from a Solaris machine using the Netscape 4.03 browser, a Javascript error occurs on the subaccount management page. **Workaround**: The best workaround is to update the browser. Otherwise, you can ignore this error message or edit the JSP to eliminate the problem. To edit the JSP, follow these procedures: 1. Edit nwsp/docroot/pages-ssm/subaccountManage.jsp. 2. Remove the preload from the body tag in line 345. To do this, find the following code: `<body topmargin="0" leftmargin="0" marginwidth="0" marginheight="0" text="#fffff f" link="#FFCC00" vlink="#FFCC00" alink="#FFCC00" onLoad="MM_callJS('pageOnLoad( )'); MM_preloadImages ('%3Cshape:path%20idFile=%27/images/subaccount_button_r2_c2_ f2.gif%27/%3E')" onUnload="MM_callJS('pageOnUnload()')">`  Replace the above lines with the following code:  `<body topmargin="0" leftmargin="0" marginwidth="0" marginheight="0" text="#fffff f" link="#FFCC00" vlink="#FFCC00" alink="#FFCC00" onLoad="MM_callJS('pageOnLoad( )')" onUnload="MM_callJS('pageOnUnload()')">` 3. Recompile and restart the NWSP application. Alternatively, if precompilation is not required, replace nwsp/docroot/WEB-INF/web.xml by web.recompile.xml and restart the NWSP application on a machine with a JDK. See the *Cisco Subscriber Edge Services Manager Web Developer Guide* for more information about recompiling NWSP.

CSCuk26991	If a subaccount is set so that it does not have the service subscription permission, it cannot see its own subscribed services. The parent account also cannot see the subscribed services. All services appear as unavailable and cannot be made available.
	
	Workaround: Modify the subaccount management JSP (nwsp/docroot/subaccountManage.jsp) so that it does not display the subscription check box; rather, subscription permissions will always be available by default. Make these changes by deleting or commenting out the following three lines of code:
	
	• line 125 (creating subaccount):
	
	`if (!checkedServiceSubscription.equals(""))`
	
	• line 148 (modifying subaccount):
	
	`if (!checkedServiceSubscription.equals(""))`
	
	• line 980 (display check box):
	
	`<td class="MediumText"><l10n:resource key="serviceSubscription">Service Subscription </l10n:resource> <input type="checkbox" name="serviceSubscription" value="true" <%= checkedServiceSubscription %> ></td>`
	
	Note This change does not affect the ability of the main account to block a subaccount from subscribing to specific services.
	
	After you modify the JSP, recompile the JSPs, or if precompilation is not required, copy nwsp/docroot/WEB-INF/web.recompile.xml to web.xml. Then restart the web server.

Table 4 Caveats in SESM Release 3.1(1) (continued)

Caveats	Description
CSCuk26995	On Windows NT platforms, the silent and console installation modes do not work. **Workaround**: Install SESM using the graphical user interface (GUI) installation mode.
CSCuk27063	If RDP is configured to proxy requests to another RADIUS server, authentication fails. **Workaround**: None. The RDP does not currently work in proxy mode due to incorrect password encryption.
CSCuk27495	If you are installing SESM from the SESM product CD-ROM onto a Windows NT platform, the installation application fails because it tries to write to the CD's partition, which is read only. **Workaround:** Copy the installation file to your Windows NT platform and execute the local copy to install SESM.
CSCuk27639	The fields associated with creating a tunnel service type in CDAT do not work. **Workaround:** Define the appropriate values using the local Cisco AV pairs as illustrated below: `vpdn:tunnel-id=`*`tunnelName`* `vpdn:l2tp-tunnel-password=`*`tunnelPassword`* `vpdn:tunnel-type=l2tp` `vpdn:ip-addresses=`*`tunnelIpAddress`*
CSCdu33191	The captive portal cannot determine the port number of the original HTTP request that was redirected by the SSG TCP redirect feature. When the captive portal recreates the original request, it uses the port number that the application server is listening on. **Workaround**: To ensure that the browser is redirected to the correct server and port after authentication, ensure the SESM web server is running on port 80 (which is the default HTTP port).
CSCdu47568	In some circumstances, the SESM web application can fail if the Java virtual machine (JVM) runs out of internal heap space. **Workaround**: If failure occurs repeatedly, consider one or both of the following: • Increase the amount of available heap space by increasing the -Xmx argument to the java command in the start script (jetty/bin/start.sh or jetty\bin\start.cmd). • Obtain an upgrade of the JVM from the Sun website at http://www.javasoft.com. Sun routinely improves JVM stability.

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. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

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

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

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

Contacting TAC by Telephone

If you have a priority level 1(P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

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

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.