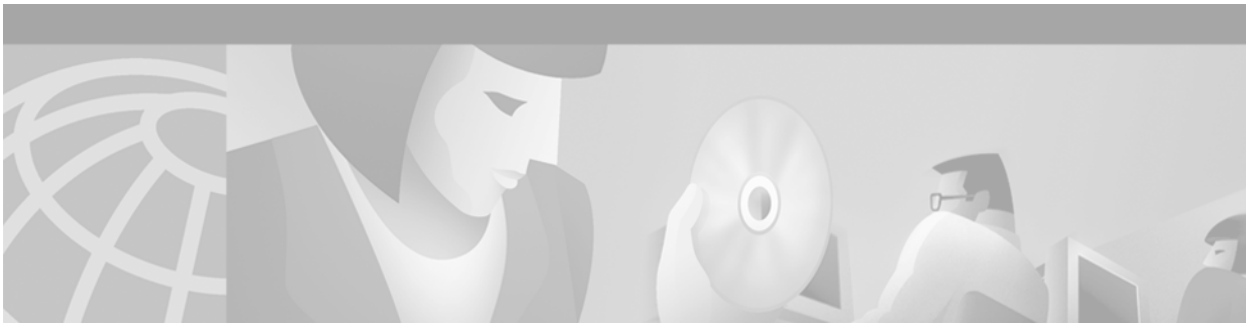

Release Notes for the Cisco Subscriber Edge Services Manager, Release 3.1(5)

August 2002

These release notes contain important information regarding the Cisco Subscriber Edge Services Manager (Cisco SESM) Release 3.1(5).

Note For information about obtaining a license number, see the "Obtaining a License Number" section on page 7.

Contents

These release notes discuss the following topics:

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

Introduction

Cisco SESM provides service selection and connection management in broadband and mobile wireless environments. Cisco SESM provides the end user (the subscriber) with a web portal for accessing multiple services. The ISPs and NAPs deploying Cisco SESM can customize the content of the web pages and thereby control the subscriber experience.

SESM Deployment Options

SESM Release 3.1(5) supports the following deployment options:

- RADIUS—In this deployment, the SESM web application and SSG query a RADIUS database for authentication and authorization information.
- LDAP—In this deployment, the Cisco Subscriber Policy Engine (SPE) provides the libraries and directory schema extensions that enable queries to an LDAP directory for authentication and authorization information.
- Demo—In Demo mode, the SESM web application simulates the actions of an SESM application without using an SSG, RADIUS server, or LDAP directory.

SESM Application Suite

SESM Release 3.1(5) includes the following sample web portal applications that can be installed and configured for demonstration purposes or used as a starting point for customizations:

- New World Service Provider (NWSP) portal—A comprehensive example of most features offered by the SESM web development kit.
- Wireless Access Protocol (WAP) portal—An application designed specifically for deployment in the mobile wireless industry.
- Personal Digital Assistant (PDA) portal—An application with web pages formatted for a PDA device.

You can optionally install the following applications to configure an SESM captive portal solution:

- Captive Portal application—A gateway application between the SSG and other applications in a captive portal solution. The default configuration for this application redirects subscriber browsers to either the Message Portal application or the NWSP application.
- Message Portal application—An SESM portal application that produces sample greetings and advertising pages to demonstrate SESM captive portal features.

The SESM software includes two additional supporting applications:

- Cisco Distributed Administration Tool (CDAT)—A web-based interface that is used for two purposes:
  - For configuring, managing, and monitoring SESM applications
  - For creating and maintaining the subscriber, service, and policy information used by SESM and the Service Selection Gateway (SSG) in an LDAP-mode deployment
- RADIUS Data Proxy (RDP) server—A RADIUS server that can proxy profile requests or use the SPE components to query the LDAP directory for profile information.

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

- J2EE management components
- SPE component—For SESM running in LDAP mode, the SPE component provide the interface between SESM applications and the LDAP directory.

System Requirements

This section describes hardware and software requirements for SESM deployments.

Hardware Supported

You can deploy SESM using the following platforms and SSG devices.

SESM Platforms

SESM applications can run on any platform that supports the Java Runtime Environment (JRE). Verified platforms are shown in Table 1.

Table 1 Verified Platforms

Platform	Specifications
Solaris	• Sun Ultra10 or Sun E250 (or later version) • Solaris Version 2.6 (or later version) operating system
Windows NT	• Pentium III (or equivalent) processor • Windows NT Version 4.0, Service Pack 5 (or later version)
Windows 2000	• Pentium III (or equivalent) processor
Linux	• Red Hat Linux Version 7.1 • SuSE Linux Version 7.3

Cisco Platforms with the SSG

Cisco SESM works with any router running Cisco IOS software with the Cisco Service Selection Gateway. The following devices, when they are running the Cisco IOS Release 12.2.(4)B or later with SSG enabled, work with SESM Release 3.1(5):

- Cisco 6400 Universal Access Concentrator (UAC)
- Cisco 7200 series high-performance multifunction routers
- Cisco 7400 series Internet routers

Software Compatibility

The following SESM features require support on the SSG:

- Captive portal
- Port-bundle host key

Captive Portal Compatibility

To use the captive portal feature in SESM to support unauthenticated user redirections:

- The SSG device must be running Cisco IOS Release 12.2(2)B or later, or Release 12.1(5)DC1 or later.
- The SSG TCP redirect feature must be configured appropriately.

To use the captive portal feature in SESM to support service redirections, initial logon redirections, and advertising redirections:

- The SSG device must be running Cisco IOS Release 12.2(4)B or later, or Release 12.1(5)DC1 or later.
- The SSG TCP redirect feature must be configured appropriately.

Port-bundle Host Key Compatibility

To use the port-bundle host key feature:

- The SSG device must be running Cisco IOS Release 12.2(2)B or later.
- 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.

New and Changed Features

This section describes new and changed features in SESM Release 3.1(5).

Note Starting with SESM Release 3.1(5), the *Cisco Subscriber Edge Services Manager and Subscriber Policy Engine Installation and Configuration Guide* has been renamed. The title is now the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*.

New and Changed Features for RADIUS and LDAP Mode

The following new features apply to SESM running in RADIUS or LDAP mode:

- CDAT has been improved and now supports:
  - Remote configuration—CDAT allows the deployment administrator to remotely view and change configuration attributes for SESM applications. In addition, the administrator can manage Java Virtual Memory (JVM) for running SESM portals.

  - Remote monitoring—CDAT allows the deployment administrator to remotely monitor SESM application activity and performance.

  For information on CDAT's remote configuration and monitoring capabilities, see the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*.

- Location-based branding—The SESM web-application software now provides enhanced mechanisms for identifying the subscriber's location and serving customized, location-specific JSP pages. The sample NWSP portal application can demonstrate these capabilities. For information on location-based branding, see the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*.
- Double-byte localization—The SESM web-application software now supports localization using double-byte (UTF-8) character sets. To demonstrate this capability, the resource bundles for the sample SESM web portals include properties files with all messages and text translated into Chinese and Japanese.
- In both RADIUS and LDAP mode installations, the SESM software now includes a RADIUS server. The bundled RADIUS server is suitable for development and testing purposes. When used for these purposes, the RADIUS server supports RADIUS attributes in Merit file format as well as a set of SESM-extended subattributes ($ subcodes) that allow testing of both RADIUS-mode and LDAP-mode functionality. For information on the bundled RADIUS server and the attributes that are supported, see the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*.

Note With SESM Release 3.1(5), the Merit file format that SESM uses for Demo mode has changed. Subattributes that used to be understood in Demo mode only are now defined with the $ subcode prefix in the account-info subattribute.

- The SESM software now includes a UNIX script (precompile.sh) to precompile modified JSP pages. The script is located in the *\install_dir*\tools\bin directory. For information on using the script, see "Precompiling JavaServer Pages" section on page 20.

Additional New and Changed Features for LDAP Mode

The following new and changed features apply to SESM running in LDAP mode.

New Features for LDAP Mode

New features in SESM Release 3.1(5) include:

- Subscriber personal firewall provisioning—The sample NWSP web portal application now includes functionality for implementing subscriber firewalls. NWSP includes an additional tab MY FIREWALL, which links to the firewall-management page. From this page, the subscriber can select from a number of deployer-configurable firewall settings. The NWSP subscriber firewall provisioning mechanisms are easy to use and require no knowledge of access control lists. For information on subscriber firewall provisioning, see the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*.
- Enhanced RADIUS attribute support—The CDAT mechanism for specifying RADIUS attributes in subscriber and services profiles has been simplified and enhanced. The new mechanism provides a way to dynamically define attributes for testing and development. For more information on these features, see the "Cisco Distributed Administration Tool Guide" section on page 16.

Changed Features for LDAP Mode

The following changed features apply to SESM running in LDAP mode.

RDP in Proxy Mode: Primary Services

In Proxy mode, the RDP forwards authentication requests to a configured RADIUS server. The basic meaning of authentication is to validate the user. However, the RDP authentication handler also adds attributes from the subscriber profile to the access-accept message. For information on the attributes that RDP adds, see the "Summary of RDP Protocol Handlers" section in Chapter 7 of the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*.

In the case of Proxy mode, if you want to add additional authentication attributes for a subscriber, you must add them in the profiles used by the proxied RADIUS server. If you add the attributes to the profiles on the LDAP directory, they are ignored.

Note In releases earlier than SESM Release 3.1(5), these additional authentication attributes were processed from the profiles on the LDAP directory.

Additional New Features for RADIUS Mode

The following new features apply to SESM running in RADIUS mode:

- CDAT is now available for remote configuration, management, and monitoring of SESM web applications. In RADIUS mode, you do not need to install SPE to install CDAT.

Enhanced Web-Application Software and Documentation

The SESM web-application software is enhanced in this release in the following ways:

- New software components for subscriber firewall provisioning—New control and JavaBean components for subscriber firewalls have been added to the com.cisco.sesm.webapp.control package. A new package is com.cisco.sesm.core.acl provides classes to handle access control list entries. The new JSP pages, firewall.jsp and firewallBody.jsp, provide the view components for firewall management.
- New properties files and buttons—The set of language-specific properties files for the sample SESM web application now include Chinese and Japanese. The text on NWSP buttons and icons is now translated into additional languages to better demonstrate a SESM web application's ability to provide language-specific resources customized for each subscriber's locale.

In addition, the Javadoc documentation that is installed with the SESM software has been improved. For example, descriptions for the com.cisco.sesm.navigator and com.cisco.webapp.control packages have been completed and expanded with more detailed explanations.

Installation Notes

The following sections highlight some important installation information.

See the *Cisco Subscriber Edge Services Manager 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 SESM using a RADIUS mode evaluation option or an LDAP mode evaluation option. 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.

A 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, the license number and the software version in the licensenum.txt file appear under the installation directory.

Obtaining Cisco SESM Software Files

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

- For Sun platforms: sesm-3.1.5-pkg-sol.tar
- For Linux platforms: sesm-3.1.5-pkg-linux.tar
- For Windows platforms: sesm-3.1.5-pkg-win32.zip

If you purchased a contract that allows you to obtain the SESM software from Cisco.com, 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.

Upgrade Information

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

Upgrading from SESM Release 3.1(3)

This section provides information on upgrading from SESM Release 3.1(3) to SESM Release 3.1(5).

Migrating a SESM Release 3.1(3) Web Portal Application

To migrate an SESM Release 3.1(3) web portal application to an SESM Release 3.1(5) deployment, perform the following steps:

Note Before you begin this procedure, ensure that a backup copy of your entire SESM web application is stored in a safe location.

Step 1 Install the SESM Release 3.1(5) software. For information on installing the software, see the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*.

Step 2 Copy your entire SESM web application into the install location of the SESM Release 3.1(5) software. For example, to copy a SESM web application located in the \mywebapp directory, you would copy all files and directories starting with the \mywebapp directory into the install location of the SESM Release 3.1(5) software. After the copy operation is complete, the following directories would exist below *SESM315_install_dir*\mywebapp:

- config
- docroot
- docs

Step 3 Install a *second copy* of the SESM Release 3.1(5) software into a location different from where you installed the first copy.

Step 4 From the second SESM install location, copy the following files into the corresponding SESM Release 3.1(5) location of your web application:

- docroot/WEB-INF/lib/com.cisco.contextlib.jar
- docroot/WEB-INF/lib/sesm.jar
- docroot/WEB-INF/lib/*.tld

Step 5 Depending on whether your web application contains customized versions of the JSP pages in the docroot/decorators directory, do one of the following:

- If your web application *does not* contain customized JSP pages in docroot/decorators, copy all files in docroot/decorators from the second SESM Release 3.1(5) install location into the corresponding SESM Release 3.1(5) location of your web application.
- If your web application *does* contain customized JSP pages in docroot/decorators, do the following:

a. Use a **diff** utility to compare your web application's files in docroot/decorators with the same files in the second SESM Release 3.1(5) install location.

b. Copy all files in docroot/decorators from the second SESM Release 3.1(5) install location into the corresponding SESM Release 3.1(5) location of your web application.

c. Using the **diff** output from step a, replicate any customizations in all files in docroot/decorators of your SESM Release 3.1(5) web application.

Step 6 In the SESM Release 3.1(5) location that contains your web application, change the name of the docroot/WEB-INF/*mywebapp*.xml file to *mywebapp*.xml.OLD. (The file *mywebapp*.xml is the name of your web application's deployment descriptor file.)

Step 7 From the second SESM install location, copy the docroot/WEB-INF/web.recompile.xml file into the corresponding SESM Release 3.1(5) location that contains your web application and rename the file *mywebapp*.xml.

Tip The web.recompile.xml file that is installed with the SESM software causes the web application's JSP pages to be used rather than any precompiled JSP pages. The web server compiles each JSP page the first time the JSP page is requested after the web application is started. For information on how to use precompiled JSP pages, see the "Precompiling JavaServer Pages" section on page 20.

Step 8 If your SESM web application's deployment descriptor file (*mywebapp*.xml) is customized in any way, modify the deployment descriptor file that you copied in step 7 so that it includes those customizations. For example, the number or order of user-shape dimensions that your web application uses may be different from the number or order found in the standard web.recompile.xml file.

Step 9 Update the Javadoc files in the *mywebapp*/docs directory by replacing them with the files in the nwsp/docs directory from the second SESM Release 3.1(5) install location.

Step 10 After successfully completing this procedure, you can delete the files that are associated with the second SESM Release 3.1(5) installation.

Installing SPE Schema Extensions in LDAP Mode

With LDAP mode, SESM Release 3.1(5) requires SPE software Release 1.11, which has changes to the directory schema extensions. You can use options in the SESM installation program to load the new schema extensions.

Note You must first delete the old extensions *before* you install the new SPE schema extensions.

If you are using the NDS eDirectory, you must export your data, reinstall the directory, and then install the new SPE schema extensions.

Uninstalling a Previous Installation

Use the uninstall utility provided with the SESM product to remove a previous installation. The uninstall utility is located in the following directory:

```
installDir
    _uninst
       uninstall.bin or uninstall.exe
```

The uninstall utility does the following:

- Lets you choose the components to uninstall.
- Verifies the installation directory that is being uninstalled.
- Uninstalls the SESM components. It does not remove the installation directory, only the contents under the installation directory.

After you run the uninstall utility, you can safely reinstall one or more SESM components into the same directory.

Note Do not uninstall SESM by manually deleting the contents of the installation directory. If you manually remove the contents of the directory and then attempt a reinstall into the same directory, the reinstall might not be complete.

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 in Table 2 for caveat CSCuk27495.

Modifying Java Server Pages

The SESM portal applications use precompiled JavaServer Pages. If you modify the JavaServer Pages in one of the SESM portal applications, you must recompile the JavaServer Pages before the changes are visible in the application. For information on recompiling, see the *Cisco Subscriber Edge Services Manager Web Developer Guide.*

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 recommended JRE for SESM Release 3.1(5) is JRE Version 1.3.1_02.

JMX Management Console

The Sun example JMX server includes an HTML adaptor server that produces a web-based management console. The JMX HTML adaptor server has been enhanced since the previous release and forms the basis of the new remote management and configuration support provided by the CDAT application. For example, an administrator can make configuration changes and can now have these changes persisted with this new support.

Note In the previous release, we recommended that the JMX HTML adaptor server functionality be removed when deployed in a production environment.

The JMX HTML adaptor server is now required if a deployer requires this feature as part of the CDAT application.

To prevent a subscriber from accessing a SESM application's management console, the JMX interface prompts for a username and password. For additional security, the deployer could deploy the SESM application behind a firewall.

For information on the login values used for a SESM application's management console, see the "Login Values for SESM Agent Views" section in Chapter 6 of the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide.*

Cisco SESM Security

Cisco SESM Release 3.1(5) uses the following 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 system, 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 9, "Running SESM Components," in the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide* for more details about memory requirements.

CDAT Remote Management

The remote-management persistence feature (the store operation) saves the current attribute values for the persisted MBean in the appropriate application XML file. The store operation writes over the existing MBean in the XML file, which has the following effects:

- Any comments in the MBean are lost.
- Any Java system property definitions in the MBean are lost. Attribute values are set to the current values of the running application.
- Any <Call> tag inside a <Configure> tag disappears if you persist the MBean with the remote management tool. If the <Call> element is setting an attribute value, the rewritten MBean contains the attribute assignment performed in a different way. However, if the <Call> element was used to perform an action other than setting an attribute value, the action is lost. The correct way to call methods is to use the <Action> tag.

Caveats

Table 2 describes known problems in SESM Release 3.1(5).

Table 2 Caveats in SESM Release 3.1(5)

Category	Caveat	Description
General Issues	CSCdw50552	Service and mutually exclusive groups are not displayed when you are using a Netscape Version 4.7 browser. Workaround: None
	CSCuk28056	When a subscriber with inherited Cisco AV Pairs from a user group creates a subaccount from the NWSP application, the subaccount does not inherit the parent's AV Pairs. If the parent account has a Local Cisco AV Pair, the subaccount inherits that AV Pair. Workaround: After a subscriber creates a subaccount, an administrator must use CDAT to set the Cisco AV Pairs either in the subaccount or in the parent account.
	CSCuk31287	A user group member is erroneously autoconnected to a service when the following conditions are true: • The user group has a subscribed service which is defined as auto-logon. • The service is a member of a service group, but the user is not subscribed to the service group. When the user logs on, the service is autoconnected even though the user is not subscribed to the service group. Workaround: Do not define services in a service group as auto-logon in a user group.
	CSCuk32602	In a captive portal deployment, when an unauthenticated WAP subscriber tries to connect to a service, the authentication page appears. After authentication, the service list page appears and the subscriber is not connected to the original service as a non-WAP based subscriber would be. **Note** If the WAP subscriber is already authenticated, this issue does not arise. Workaround: The subscriber manually selects the service from the service list.
General Issues (continued)	CSCuk34276	When deployed with a JRE, the NWSP application does not provide support for WAP devices. This support is only provided when the NWSP application is deployed with a full JDK. Workaround: Deploy with the full JDK.
	CSCuk35022	Nested Service Groups are not supported in the current NWSP application. Workaround: None with the current NWSP application but a deployer could modify the NWSP application JSP pages accordingly.

Table 2 Caveats in SESM Release 3.1(5) (continued)

Category	Caveat	Description
Install Issues	CSCuk27495	If you install 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.
	CSCuk31427	During the installation procedure, if you select the Proxy mode option for the RDP configuration, the installation program presents a panel prompting you for the Proxy RADIUS server details. If you decide to return to the previous panel and uncheck the Proxy mode option, the installation program still presents the Proxy RADIUS server panel, even though it is not required. Workaround: Cancel out of the installation application and restart the process.
	CSCuk31428	During a custom installation, if you select only the RDP component, the installation program also selects the Jetty component. The Jetty component cannot be unselected, even though the RDP does not require it. Workaround: Proceed as normal with the installation. The Jetty component has a very small footprint. Although it is installed, it does not have an impact on the operation of the RDP component.
	CSCuk31431	During a custom installation in LDAP mode, if you deselect all of the choices and then reselect the Web Applications, the installation application correctly autoselects the Jetty component but does not autoselect the SPE component. Workaround: If this sequence of events occurs, be sure to manually select the SPE component, as it is required for LDAP mode.
	CSCuk29291	The SESM installation application requires the JDK or JRE that you wish to use in your deployment to be located in a well-known directory; otherwise, the installation program does not find your installed version and uses the bundled JRE. Workarounds: • Ensure that the JRE or JDK you wish to use is located in one of the well-known directories. • Specify the location of the JRE or JDK by using a command line argument during the installation. • Specify the location in the startup scripts. See the Installation Components section in the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide* for further details, including a list of the well-known directories.

Table 2 Caveats in SESM Release 3.1(5) (continued)

Category	Caveat	Description
Install Issues (continued)	CSCuk31543	The silent install option does not perform correctly for the SESM applications, unless you intend to install in Demo mode. Configuration information for the web portal applications (NWSP, PDA, WAP) is not set, although the remaining applications and components (CDAT, RDP, Captive Portal, Message Portal) are configured as expected. Workaround: The preferred workaround is to use the normal or console-based installation mode. An alternative workaround is to manually edit the incorrect configuration files: • *applicationName*/config/*appName*.xml • jetty/config/*applicationName*.jetty.xml • jetty/bin/start*applicationName*.sh or jetty\bin\start*applicationName*.cmd
	CSCuk35416	For Solaris and Linux installations, the bundled RADIUS server does not start because the location of the JVM is not known. Workaround: Edit the start script for the bundled RADIUS server (.../tools/bin/start.sh) and set the JDK_HOME variable to the location of the JVM, as it is in the start.sh file under the /jetty/bin directory.
RDP Issues	CSCuk35196	If a subscriber has a Primary Service as a result of inheriting it from a User Group, the RDP does not pass the IP Pool associated with the Primary Service to the SSG. Workaround: For IP Pool to be passed to the SSG, the IP Pool attribute must be defined in the Local RADIUS Attributes field of the CDAT application at the User Group level.
	CSCuk35302	If a subscriber's profile contains an incorrect RADIUS attribute, which the RDP cannot parse, the RDP does not send any attributes back to the SSG and so the subscriber is not able log on. Workaround: Ensure that there are no incorrect RADIUS attributes in the user profile.
CDAT Issues	CSCuk29592	If an administrator deletes a service from CDAT that is defined as an autoconnected service in a subscriber's profile, some service-related attributes might not be deleted from the directory. The problem occurs regardless of whether the subscriber is logged in or logged out. These redundant attributes do not have an impact on the subscriber. Workaround: There is no impact in leaving these attributes in the directory, but administrators can manually remove the attributes if they wish.
	CSCuk31892	CDAT cannot distinguish between local and inherited generic RADIUS attributes in a user profile when the user is a member of a group for which the generic attributes are defined. Workaround: None
	CSCuk30471	CDAT cannot distinguish between user and group pool names. Workaround: None
	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.

Table 2 Caveats in SESM Release 3.1(5) (continued)

Category	Caveat	Description
CDAT Issues (continued)	CSCuk32178	In CDAT, the Block Inheritance and Service Filters attributes are not inherited by the user from a user group. Workaround: If these attributes are required, they must be directly assigned to each user.
	CSCuk32167	In CDAT, if you change a user from one user group to another, certain attributes become local to the user's profile, and are not inherited from the new user group. These attributes are: Home URL, Maximum number of subaccounts, Enable SSO, Pool name, Primary Service, and TCP redirection attributes. Workaround: None

Documentation Updates

This section includes new and updated information about SESM Release 3.1(5) that does not appear in the current SESM documentation set. The information contained in the following sections will appear in a future revision of the respective guides.

- *Cisco Distributed Administration Tool Guide, page 16*
- *Cisco Subscriber Edge Services Manager Web Developer Guide, page 20*

Cisco Distributed Administration Tool Guide

This information provides some updated information about the *Cisco Distributed Administration Tool Guide*.

New Management Capabilities

The capabilities of CDAT are expanded and now allow the deployment administrator to:

- Remotely view and change configuration attributes for SESM portal applications
- Remotely monitor SESM application activity and performance
- Remotely manage Java Virtual Memory (JVM) for running SESM portals

The initial CDAT window contains configurable hyperlinks (for example, Manage NWSP or Manage LDAP) that let the administrator choose the SESM applications to monitor and control and the data repositories to manage.

For information on installing, configuring, and using the remote configuration and monitoring capabilities of CDAT, see the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*.

DESS/AUTH Sample Data for iPlanet

A set of sample DESS/AUTH data is in the DESSusecasedata.ldf file, which is located in *install_dir*\dess-auth\schema\samples directory. This file is formatted for NDS eDirectory. To modify the data for use with iPlanet Directory Server, do the following:

- Replace all instances of "cn=admin" with "uid=admin"
- Replace all instances of "cn=bronzeuser" with "uid=bronzeuser"
- Replace all instances of "cn=silveruser" with "uid=silveruser"
- Replace all instances of "cn=golduser" with "uid=golduser"
- Replace all instances of "cn=subgolduser" with "uid=subgolduser"
- Remove all lines containing the string "ndsLoginProperties"
- Replace all instances of "uniqueMember” with "member"

DESS/AUTH Sample Data Installation

Note The instructions in the file *install_dir*\dess-auth\schema\README.LDIFload.html are no longer accurate. In their place, use the instructions in this section.

Starting with SESM Release 3.1(5), the DESS/AUTH sample data is contained in one LDIF file, DESSusecasedata.ldf file, which is located in the *install_dir*\dess-auth\schema\samples directory. The DESSadmin.ldf file in the same directory is no longer used.

You use the **ldapmodify** command to install the sample data. The examples that follow show the **ldapmodify** command line that is used for NDS eDirectory and for iPlanet Directory Server.

NDS eDirectory Example

For the following eDirectory example, assume that:

- 192.10.68.12 is the address of the server where the directory is located.
- 389 is the port number where the directory server listens.
- The directory administrator (with the password "cisco") is defined as follows in the NDS directory server configuration file:
  - Admin Name and Context: cn=admin.ou=sesm.o=cisco
- The following container exists in the directory:
  - Tree Name: sesm
  - Context: ou=sesm.o=cisco

The following **ldapmodify** command installs the sample data:

```
ldapmodify -h 192.10.68.12 -p 389 -c -v -D "cn=admin,ou=sesm,o=cisco" -w cisco
     -f DESSusecasedata.ldf
```

iPlanet Directory Server Example

For the following iPlanet example, assume that:

- 192.10.68.12 is the address of the server where the directory is located.
- The administrator (with the password "cisco") with the required permissions to create and modify objects in the SESM container is defined as follows in the iPlanet configuration:
  - name: uid=admin,ou=sesm,o=cisco
- The following container exists in the directory:
  - Tree Name: sesm
  - Context: ou=sesm.o=cisco

The following **ldapmodify** command installs the sample data:

```
ldapmodify -h 192.10.68.12 –c -v -D “uid=admin,ou=sesm,o-cisco” -w cisco
     -f DESSusecasedata.ldf
```

First CDAT Login

Note The instructions in the *Cisco Distributed Administration Tool Guide* for logging into CDAT for the first time are no longer accurate. Replace the old instructions with the instructions in this section.

To log in to CDAT for the first time, you must obtain a user name and password. The administrator who logs in first needs administrative privileges to set up the objects and attributes for services, subscribers, policy roles and rules, and so on.

When you log in to CDAT for the first time, you use the admin user name and the password that were set up when the directory was installed. To use the admin user name as the first-time CDAT administrator, you must do the following when installing the directory server and the SPE software:

1. When you install the directory server, set up an admin user with the needed permissions to access and create objects in the directory container (Organization Unit and Organization) where the SPE schema extensions and initial RBAC objects will be installed.
2. When you install the SPE software, select Install RBAC to install the initial RBAC objects. When you select **Install RBAC**, the SESM/SPE installation software *expects to find* an admin user ID so that it can grant that user the needed administrator privileges.

After the initial RBAC objects are installed, you can use the admin user name to log in to CDAT for the first time. The admin account is an administrative account with Cisco_Dess_Supervisor, Cisco_Azn_Super, and Cisco_Dess_Manage privileges, which are appropriate for a superuser-type administrator. The admin user can access all objects in the Organization Unit and can perform all CDAT tasks: access, create, delete, and modify all objects and attributes. The admin user can create user accounts, roles, and rules for all users, including administrators, account managers, and publishers.

RADIUS Attributes in Profiles

The CDAT fields that allow the administrator to specify RADIUS attributes, including Cisco attribute-value pairs (Cisco AV pairs), is now simplified and enhanced. Both standard RADIUS attribute names and Cisco SSG vendor-specific attributes (VSAs) can be specified in CDAT’s Local RADIUS Attributes box.

The ability to specify RADIUS attributes allows the administrator to define an attribute and value that *does not* appear in the boxes (fields) of a CDAT window. For example, the Users window does not have a box for a RADIUS attribute Calling-Station Id. You can enter this attribute in the Local RADIUS Attributes box.

The enhanced Local RADIUS Attributes box appears in the following CDAT windows:

- Users
- User Groups
- Services
- Service Groups
- NRPs

Note The Local Cisco AV Pairs field has been removed from the preceding CDAT windows. The administrator now uses the enhanced Local RADIUS Attributes box to enter Cisco AV pairs.

Using Predefined RADIUS Attributes

Both standard RADIUS attribute names and Cisco SSG vendor-specific attributes (VSAs) can be specified in CDAT's Local RADIUS Attributes box.

SESM applications, including CDAT, internally predefine the standard RADIUS attributes and the Cisco SSG VSAs. Some examples of the SESM-predefined RADIUS attributes that you can specify with CDAT include:

- CALLING_STATION_ID
- CISCO-AV

You can use these predefined RADIUS attributes in subscriber and service profiles whether or not they are defined in RADIUSDictionary MBean used by the RDP application. For the full list of predefined RADIUS attributes and Cisco SSG VSAs, see the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*.

To specify one of the predefined RADIUS attributes in CDAT's Local RADIUS Attributes box, use the following form:

ATTRIBUTE_NAME:*attribute_value*

ATTRIBUTE_NAME is one of the predefined RADIUS attributes, and *attribute_value* is the value given for the attribute. A colon (:) separates the two elements. Two examples follow:

```
CALLING_STATION_ID:978123456

CISCO-AV:ip:inacl#101=deny tcp 192.168.1.0 0.0.0.255 any eq 21
```

If SESM is running in LDAP mode, you can define new RADIUS attributes in the RADIUSDictionary MBean used by the RDP application. For information on this capability, see the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*.

Using Dynamically Defined Attributes

With the enhanced Local RADIUS Attributes box, you can also dynamically define a new attribute when you first use the attribute in a profile. This feature is intended only for testing, demonstration, and development purposes. With CDAT, use the dynamic attribute feature only in the following circumstances:

- The SESM portal is running in Demo mode.
- The SESM portal is running in LDAP mode in a testing or development environment.

For information on dynamically defining a new attribute, see the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide.*

Cisco Subscriber Edge Services Manager Web Developer Guide

This section provides information about SESM web application development that is not in the *Cisco Subscriber Edge Services Manager Web Developer Guide*.

Precompiling JavaServer Pages

The sample SESM web applications use JavaServer Pages (JSP pages), which allow for the combination of markup language (such as HTML or WML), use of custom beans and tag libraries, and Java if required.

The SESM software includes a set of precompiled JSP pages for the sample SESM web applications such as NWSP. In any production deployment, the default JSP pages require customization by the deployer. Two options are available for compiling a modified set of JSP pages.

- The first option is to use the JSP pages directly, in which case a page is compiled by the web server the first time it is requested after the web application is started. This option is convenient—especially for development—but it has two disadvantages:
  - The first time a page is requested, the access time is slow. Subsequent requests are processed faster because the compiled JSP page is stored.
  - The web server requires the presence of an installed JDK. This is not convenient for deployment.
- The second option is to precompile the modified JSP pages using the following instructions and UNIX script precompile.sh. The script is shipped with the SESM software in the *install_dir*\tools\bin directory. With precompilation, the JSP pages are translated into compiled Java servlet classes, and there is no significant performance impact when a page is requested the first time.

Note The precompile.sh script contains an error that you must correct before using the script. To correct the error, change line 193 of the script from:

```
$JDKDIR/bin/jar cvf0m $JARFILE $MANIFESTV\
    to
$JDKDIR/bin/jar cvf $JARFILE \
```

The precompile.sh script precompiles a full set of JSP pages for the SESM web application (for example, NWSP) that you specify when you invoke the script and creates a JAR file containing the resulting compiled servlet classes. The script also makes adjustments to the SESM web application's web.xml file so that the web application uses the precompiled JSP pages.

Using the Precompiling Script

To execute the precompile.sh script (located in *install_dir*\tools\bin) for precompiling a set of JSP pages, perform the following steps on a UNIX workstation where the SESM software is installed:

Step 1 To make the script executable, issue the following command:

```
chmod a+x precompile.sh
```

Step 2 Run the script precompile.sh and wait for completion, which may take some time.

Note The comments at the beginning of the precompile.sh script provide information on how to use the script.

You can run the script from any directory as the paths used in the script are all full path names. If you run the script from the recommended directory, set the environment variable `SESM_HOME` to be the full path name of the SESM installation directory.

Developing and Testing SESM Web Applications

This section contains information about developing and testing SESM web portal applications.

WAP Simulator

You cannot access the sample WAP application using the UP.Simulator Version 4.1 (part of the UP.SDK for WML from Openwave Systems Inc.). For example, if you issue the following request, a content type error results:

```
http://some_server:8080
```

To access the sample WAP application, use the Nokia Mobile Internet Toolkit's simulator.

Dreamweaver UltraDev Live Window Feature

If you use the Dreamweaver UltraDev Live Window feature, the NWSP web application's home page (home.jsp) does not work correctly. To use the Live Data window with home.jsp, comment out the following statement in home.jsp:

```
<%@ include file="/decorators/openWindow.jspf"%>
```

The commented-out statement is as follows:

```
<%-- @ include file="/decorators/openWindow.jspf" --%>
```

Before you test and deploy the web application, remove the comment delimiters.

If you use the Dreamweaver UltraDev Live Window feature, the NWSP web application's subscription and subaccount subscription pages do not work correctly. To access these pages, use Dreamweaver UltraDev normal mode (as opposed to Live Data mode). Alternatively, you can access the body JSP pages (for example, subscriptionManageBody.jsp) directly in Live Data mode.

File Tag in the Shape Tag Library

If the file tag from the Shape tag library (<shape:file name='...'/>) does not find the resource specified by the name attribute, the JSP page stops displaying. In some cases, the window goes or appears blank. This is normally only an issue during development and testing, as all resources should be available in a production application.

Related Documentation

See the following documentation regarding SESM.

- *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*
- *Cisco Subscriber Edge Services Manager Web Developer Guide*
- *Cisco Distributed Administration Tool Guide*

The online location for SESM documentation is:

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

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

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

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, please 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, please have available your service agreement number and your product serial number.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.