Release Notes for the Cisco Subscriber Edge Services Manager, Release 3.1(7)

December 2002

These release notes contain important information regarding the Cisco Subscriber Edge Services Manager (Cisco SESM) Release 3.1(7).

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(7) 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(7) 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.

- Web Services Gateway (WSG) application—Provides a Simple Objects Access Protocol (SOAP)-based interface that allows third-party web portals and subscriber management systems to integrate with the SESM and SSG solution.

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 provides 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(7):

- 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
- Complete ID

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.

Complete ID Compatibility

To use the complete ID feature for portal location awareness and branding, the SSG device must be running Cisco IOS Release 12.3(1)T or the X train for Cisco IOS Release 12.2(8)B.

New and Changed Features

This section describes new and changed features in SESM Release 3.1(7).

New and Changed Features for RADIUS and LDAP Mode

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

New Features for RADIUS and LDAP Mode

- Location awareness using complete ID attributes from SSG—The SESM location awareness feature is expanded to include additional attributes to determine subscriber location. These new location attributes are obtained from the complete subscriber identification (complete ID) received from SSG. The location attributes can consist of the client IP address, client subnet, VPI, SSG subinterface, and MSISDN, depending on the network deployment.

  Note To use the complete ID feature for portal location awareness and branding, the SSG device must be running Cisco IOS Release 12.3(1)T or the X train for Cisco IOS Release 12.2(8)B.

  The specific attributes used to determine the location, and hence the location branding, are configurable. See Chapter 10, “Configuring SESM Features,” in the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide* for more information.

- Developer access to complete ID attributes from SSG—SESM application developers can access any of the attributes in the SSG complete ID feature by using the session.getAVPairs() method in the SESM API. The attributes in the SSG complete ID include the subscriber IP address, MAC address, VPI/VCI, SSG subinterface, and MSISDN. The SSG device must be running Cisco IOS Release 12.3(1)T or the X train for Cisco IOS Release 12.2(8)B.
- Dynamic host key mapping—This feature provides flexibility with the policies used to map subscriber IP addresses to the host SSGs when the port-bundle host key feature is not being used. (When port-bundle host key is enabled, no mapping is required.) The dynamic host key mapping feature allows deployers to specify any mapping policy they choose, including customized policies and external applications that perform the mapping function.
- Web application archive (WAR) directory structure—The installed directory structure for each of the SESM Release 3.1(7) web portal applications is suitable for creating a WAR file for use in J2EE containers other than the installed Jetty container. For information on creating a WAR file, see the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide.*
- Web Services Gateway (WSG) application—The WSG application provides a Simple Objects Access Protocol (SOAP)-based interface enabling third-party web portals and subscriber management systems to integrate with the SESM and SSG solution. The WSG installation includes a web application configured to run in a Jetty container and a command-line client script for demonstration purposes. See the “Web Services Gateway” section on page 22 for information about installing and using the WSG application.

Changed Features for RADIUS and LDAP Mode

- For each of the SESM web portals, the web-application directory structure has changed to support the creation of WAR files.
  - The /docroot folder is now named /webapp.
  - All Java archive (JAR) files needed for an SESM web portal application now reside in the \web_app_name\\webapp\\WEB-INF\\lib\\ directory, where *web_app_name* is the directory in which a sample SESM web application, such as NWSP, is installed.
- The names of the files containing sample profiles for Demo mode have changed as follows:
  - nwsp/config/demo.txt is now nwsp/config/aaa.properties.
  - pda/config/pdademo.txt is now pda/config/aaa.properties.
  - wap/config/wapdemo.txt is now wap/config/aaa.properties.
- In the XML configuration files, some <SystemProperty> tags were replaced with a new tag named <Property>. The tags identify attributes with properties similar to Java system properties. The difference between the tags is:
  - SystemProperty defines attribute values for the container space; that is, all applications in the same container share the same value.
  - Property defines attribute values for an application space.
- The default location of log files has been standardized to a logs directory under the web application directory (for example, nwsp/logs). The directory is created the first time that the web application runs. In support of this change, the application.log system property has been eliminated from the start script and the configuration files.

Additional New and Changed Features for LDAP Mode

This section describes new and changed features that apply to running in LDAP mode. For other new and changed features for SESM Release 3.1(7), see the preceding section, "New and Changed Features for RADIUS and LDAP Mode" section on page 5.

New Features for LDAP Mode

- Advanced firewall features—The advanced firewall features complement the basic firewall features available in SESM Release 3.1(5). In SESM Release 3.1(7), the NWSP application includes two firewall pages:
  - The basic My Firewall page, which existed in SESM Release 3.1(5), lets subscribers choose from user-friendly options for creating a personal firewall.
  - The Advanced Firewall page, which is new in SESM Release 3.1(7), lets subscribers create and modify more detailed filters than the basic page. Subscribers can create permit or deny filters for specific source and destination IP addresses, ranges of IP addresses, or ports.

  Filters created using the advanced page have a higher priority than those created on the basic page. Administrative filters, entered by deployers using CDAT, have the highest priority. For more information about the SESM firewall features, see Chapter 10, "Configuring SESM Features," in the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*.

Changed Features for LDAP Mode

- The Cisco Security Policy Engine (Cisco SPE) configuration file name has changed. Also, each SESM application that includes the SPE libraries uses its own version of the SPE configuration file, whereas in previous releases, all applications installed in the same directory structure shared the same SPE configuration file.

  In previous SESM releases, the SPE configuration file name was:

  ```
  dessauth/config/config.xml
  ```

  In SESM Release 3.1(7), the SPE configuration file names are as follows:

  ```
  nwsp/config/dessauth.xml
  pda/config/dessauth.xml
  wap/config/dessauth.xml
  rdp/config/dessauth.xml
  cdat/config/dessauth.xml
  ```

- In the Cisco Distributed Administration Tool (CDAT), the Block Inheritance checkbox in the Users and Users Groups window has changed:
  - In the Users window, the Block Inheritance box is now named Block Service Inheritance.
  - In the User Groups window, the Block Inheritance box was removed.

Enhanced Web-Application Software

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

- So that the deployer can easily create a WAR file for an SESM web application, all JAR files needed for an SESM web portal application now reside in the /*web_app_name*/webapp/WEB-INF/lib directory, where *web_app_name* is the name of the web application.
- NWSP web components now include the control, view JavaBeans, and JSP pages needed for the Advanced Firewall page.

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-3.1.7-pkg-sol.tar
- For Linux platforms: sesm-3.1.7-pkg-linux.tar
- For Windows platforms: sesm-3.1.7-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 Click **Technical Support**.

Step 4 In the pop-up window, click **Software Center**.

Step 5 Click **Web Software**.

Step 6 Click **Cisco Subscriber Edge Services Manager**.

Step 7 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) or 3.1(5)

This section provides information on upgrading from SESM Release 3.1(3) or 3.1(5) to SESM Release 3.1(7).

Preserving Customizations

To preserve your previous SESM installation, including changes to configuration files and customized web applications, install SESM Release 3.1(7) in a different directory from previous installations.

To reuse the same installation directory, perform the following steps:

Step 1 Ensure that a backup copy of your previous SESM installation is stored in a safe location.

Step 2 Uninstall the previous release of SESM using instructions in the "Uninstalling a Previous Installation" section on page 15.

Step 3 Install the current release of SESM.

Step 4 Migrate the SESM Release 3.1(3) or 3.1(5) set of configuration files to SESM Release 3.1(7). Use either of the following methods:

- When the application is running, use the Agent View to update attributes to the values used in the previous installation. Be sure to use the apply and store operations to persist the new values across application restarts.
- When the application is not running, edit the XML files, updating attribute values to the values used in the previous installation.

Step 5 Migrate your web portal applications to the new installation, as described in the following section.

Migrating an SESM Release 3.1(3) or 3.1(5) Web Portal Application

To migrate an SESM Release 3.1(3) or 3.1(5) web portal application to SESM Release 3.1(7), 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(7) software. For information on installing the software, see the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*.

Step 2 Copy the NWSP web application in \install_dir\nwsp to \install_dir\mywebapp, where \install_dir is the location in which you installed SESM Release 3.1(7), and *mywebapp* is the name of your SESM web application. This creates an SESM web application named *mywebapp* under \install_dir.

Step 3 Copy these files from the install location of the SESM Release 3.1(7) software.

a. In \install_dir\jetty\bin, copy startNWSP.sh to start*MYWEBAPP*.sh. Edit the startMYWEBAPP.sh file and replace APP=nwsp with APP=*mywebapp*. (For an SESM installation on a Windows platform, the suffix of the start file is .cmd.)

b. In \install_dir\jetty\config, copy nwsp.jetty.xml to *mywebapp*.jetty.xml. Edit the *mywebapp*.jetty.xml file and replace nwspkeystore with *mywebapp*keystore. Also, replace any comments that refer to NWSP.

c. In \install_dir\jetty\config, copy *mywebapp*keystore from your previous installation into this directory.

d. In \install_dir\jetty\config, copy nwsp.web-jetty.xml to *mywebapp*.web-jetty.xml.

Step 4 Verify the previous steps by starting the web application *mywebapp* in Demo mode.

a. In the /jetty/bin directory, run the start script. For example, on UNIX:

start*MYWEBAPP*.sh -mode Demo

b. Log in to the web application using the user name **golduser** and the password **cisco**. You should be able to use the SESM web application in Demo mode.

c. Stop the server.

Note To update the directory structure for a SESM web application, you usually must update only the contents of the WEB-INF subdirectory with the customizations for your web application. Step 5 overwrites almost the entire web application directory structure with the old web application directory. You then update certain files.

If your web application consists of minimal changes to the NWSP web application components, it may be more appropriate for you to leave the new SESM web application directory as is, and then overwrite only certain subdirectories from the previous SESM directory structure, such as the pages and images directories. If web.xml has been customized, then follow the instructions in the Step 12 for updating this file.

Step 5 Copy the following directories (and all directories and files under them) from your previous SESM web application into the \install_dir\mywebapp location of the SESM Release 3.1(7) software.

- docroot
- docs

Step 6 In the install location of the SESM Release 3.1(7) software, rename the docroot directory to **webapp**.

Step 7 Install a *second copy* of the SESM Release 3.1(7) software into a location different from where you installed the first copy.

Step 8 From the second SESM install location, copy the following files into the corresponding SESM Release 3.1(7) location of your web application:

- webapp\WEB-INF\lib\com.cisco.sesm.lib.jar
- webapp\WEB-INF\lib\sesm.jar
- webapp\WEB-INF\lib\jsp.jar
- webapp\WEB-INF\lib\*.tld

For deployments in which a WAR file will be created, copy these additional files:

- webapp\WEB-INF\lib\com.cisco.contextlib.jar
- webapp\WEB-INF\lib\jmxri.jar
- webapp\WEB-INF\lib\jmxtools.jar

For LDAP-mode deployments only, copy these additional files:

- webapp\WEB-INF\lib\dess.jar
- webapp\WEB-INF\lib\auth.jar
- webapp\WEB-INF\lib\authentication.jar
- webapp\WEB-INF\lib\protect.jar

Step 9 Depending on whether your web application contains customized versions of the JSP pages in the webapp\decorators directory, do one of the following:

- If your web application *does not* contain customized JSP pages in webapp\decorators, copy all files in webapp\decorators from the second SESM Release 3.1(7) install location into the webapp\decorators directory at the SESM Release 3.1(7) location of your web application.
- If your web application *does* contain customized JSP pages in webapp\decorators, do the following:

a. Use a **diff** utility to compare your web application's files in webapp\decorators with the same files in the second SESM Release 3.1(7) install location.

b. Copy all files in webapp\decorators from the second SESM Release 3.1(7) install location into the corresponding SESM Release 3.1(7) location (webapp\decorators) of your web application.

c. Using the **diff** output from step a, replicate any customizations in all files in webapp\decorators of your SESM Release 3.1(7) web application.

Step 10 In the SESM Release 3.1(7) location that contains your web application, change the name of the webapp\WEB-INF\web.xml file to web.xml.OLD. The file web.xml is the web application's deployment descriptor file.

Step 11 Do one of the following depending on whether you have updated jsp.jar file (using the precompile.sh script).

- If you have updated the jsp.jar file, copy the WEB-INF\web.xml from the second SESM install location to web.xml.
- If you have not updated the jsp.jar file, copy the webapp\WEB-INF\web.recompile.xml file from the second SESM install location into the corresponding SESM Release 3.1(7) location that contains your web application, and rename the file web.xml.

Tip The web.recompile.xml file 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 *Cisco Subscriber Edge Services Manager Web Developer Guide* and the "Precompiling JavaServer Pages" section on page 27.

Step 12 If your SESM web application's deployment descriptor file (web.xml) is customized in any way, modify the deployment descriptor file that you created in Step 10 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.xml or web.recompile.xml file.

Step 13 In the *mywebapp*\config\ directory of the SESM Release 3.1(7) location, rename the file nwsp.xml to ***mywebapp*.xml**.

Step 14 In the *mywebapp*\config\ directory of the SESM Release 3.1(7) location, change the attribute values in *mywebapp*.xml file so that their values are identical to the values used in your previous SESM installation. Use either of the following methods:

a. When the application is running, use the Agent View to update attributes to the values used in the previous installation. Be sure to use the apply and store operations to persist the new values across application restarts.

b. When the application is not running, edit the *mywebapp*.xml file, updating attribute values to the values used in the previous SESM installation.

Step 15 After you successfully complete this procedure, you can optionally delete the files that are associated with the second SESM Release 3.1(7) installation.

Searches for Java Classes. The deployer should be aware that the SESM web portals are, by default, run in a mode that is compliant with the Java 2, Enterprise Edition (J2EE) specification. This mode is controlled by the following line in the Jetty container MBean configuration file (for example, \install_dir\jetty\config\nwsp.jetty.xml):

```
<Set name="classLoaderJava2Compliant">TRUE</Set>
```

The preceding line has the following effects on how the web server searches for classes from JAR files:

- If `classLoaderJava2Compliant` is set to TRUE, classes from any JAR files in the \web_app_name\webapp\WEB-INF\lib directory are used *after* classes from any JAR files in the system CLASSPATH. This mode is compliant with J2EE.
- If `classLoaderJava2Compliant` is set to FALSE, classes from any JAR files in the \web_app_name\webapp\WEB-INF\lib directory are used *before* classes from any JAR files in the system CLASSPATH. This mode is compliant with the Java 2 Servlet Specification.

Installing SPE Schema Extensions in LDAP Mode

With LDAP mode, SESM Release 3.1(7) requires SPE software Release 1.11.

- If you are upgrading from SESM Release 3.1(5), which also used SPE Release 1.11, you *do not* have to install any SPE directory schema extensions.
- If you are upgrading from a SESM release earlier than Release 3.1(5), you *must* install SPE directory schema extensions. These earlier releases did not use SPE Release 1.11. SPE Release 1.11 included some schema extension changes.

You can use options in the SESM software installation program to load the new schema extensions.

Note If you must install SPE directory schema extensions, 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.

iPlanet Directory Server Manual LDIF Installation

When using the iPlanet Directory Server with SESM Release 3.1(7), the recommended way to load the SPE schema extensions and RBAC objects is to use the SESM software installation program.

Note In situations where you must manually install the schema extensions, *use the following directions in place of the directions* in the README.SESM.LDIF.html, which is located in the \install_dir\dess-auth\schema directory.

For the iPlanet Directory Server, the files to use to manually install the SPE schema extensions and initial RBAC objects are located in the \install_dir\dess-auth\schema\Netscape and \install_dir\dess-auth\schema\NDS directories. The files are:

\install_dir\dess-auth\schema\Netscape\authattr.ldf

\install_dir\dess-auth\schema\Netscape\authclas.ldf

\install_dir\dess-auth\schema\Netscape\dessattr.ldf

\install_dir\dess-auth\schema\Netscape\dessclas.ldf

\install_dir\dess-auth\schema\NDS\Policy15.ldf.nds

Note For SESM Release 3.1(7), if you choose to manually install the schema extensions for iPlanet Directory Server, *do not use* the policy15.conf file from the \install_dir\dess-auth\schema\Netscape directory. In its place, use the Policy15.ldf.nds from the \install_dir\dess-auth\schema\NDS directory.

The LDIF files must be loaded in the sequence shown in the preceding list.

Modifying the Policy15.ldf.nds File. You must edit and modify the Policy15.ldf.nds file before using it with the iPlanet Directory Server as follows:

1. Replace two occurrences of:

   1.3.6.1.4.1.1466.115.121.1.44

   with

   1.3.6.1.4.1.1466.115.121.1.24

2. Replace two occurrences of:

   1.3.6.1.4.1.1466.115.121.1.38

   with:

   1.3.6.1.4.1.1466.115.121.1.15

Installing the Schema Extensions Example. The iPlanet example given in the README.SESM.LDIF.html file for installing the SPE schema extensions and initial RBAC objects is *not correct*. The iPlanet example should be as follows:

```
ldapmodify -h 192.10.68.12 -c -v -D "cn=Directory Manager" -w cisco -f authattr.ldf
```

In the preceding example:

- `192.10.68.12` is the address of the server where the directory is located.
- `cn=Directory Manager` specifies the Directory Manager, an administrative user who has all required permissions to update the directory schema.

Upgrading from SESM Release 3.1(1)

This section provides information on upgrading from SESM Release 3.1(1) to SESM Release 3.1(7). In general, the two tasks needed for this upgrade are described in these sections:

- Migrating an SESM Release 3.1(1) Web Portal Application, page 14
- Installing SPE Schema Extensions in LDAP Mode, page 12

Migrating an SESM Release 3.1(1) Web Portal Application

Significant improvements and changes were made to the JSP pages and other web components of the SESM web application (New World Service Provider) starting with Release 3.1(3) including:

- The SESM web components that accomplish decoration were re-engineered.
- The Java code for interactions with the SESM model was moved from the JSP pages to the SESM control servlets. This change should minimize the modifications to the JSP pages as the SESM model evolves in the future.
- Implementing these changes required that numerous Java classes and methods be deprecated for SESM Release 3.1(3). In subsequent SESM releases, these classes and methods were removed.

Because of this extensive redesign, it is not practical to use JSP pages that were developed for SESM Release 3.1(1). After SESM 3.1(3), these JSP pages would need to be modified so as to replace use of the deprecated classes and methods that have now been removed. This task would be achieved by referring to the Javadoc included in the SESM installation.

Instead of modifying the JSP pages, the *recommended strategy* for migrating an SESM Release 3.1(1) web application is to use the SESM Release 3.1(7) software and web components, including the JSP pages and deployment descriptor file in a sample web application like NWSP. Using this approach, you would typically do the following:

1. Recreate the customizations from your SESM Release 3.1(1) web application in the set of JSP pages in the SESM Release 3.1(7) NWSP. For this step, you might need to accomplish one or more of the following changes to the sample SESM Release 3.1(7) web application:
    - Modify the functionality of the web application
    - Customize the look and feel of web elements such as icons, images, background colors, and style sheets
    - Localize web elements
    - Code revised or new JSP-page dimension decorators for the user-shape mechanism

    If you use Dreamweaver UltraDev or Dreamweaver MX and the templates provided with the sample NWSP web application, the HTML customizations can be accomplished more efficiently. For detailed information on customizing and developing an SESM Release 3.1(7) web application, see the *Cisco Subscriber Edge Services Manager Web Developer Guide* at:

http://www.cisco.com/univercd/cc/td/doc/solution/sesm/sesm_317/webdevgd/index.htm

2. Configure the SESM Release 3.1(7) web application deployment descriptor file (web.xml) as described in the *Cisco Subscriber Edge Services Manager Web Developer Guide* at:

http://www.cisco.com/univercd/cc/td/doc/solution/sesm/sesm_317/webdevgd/ch3_adv.htm#xtocid35

3. Configure the customized SESM Release 3.1(7) web application as described in the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide* at:

http://www.cisco.com/univercd/cc/td/doc/solution/sesm/sesm_317/instconf/05portal.htm#xtocid17

4. Precompile the finalized production JSP pages using the directions and script provided in the "Precompiling JavaServer Pages" section on page 27.

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 (JSP). If you modify the JSP pages in one of the SESM portal applications, you must recompile the JSP 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.

Compatibility and Performance with Java Runtime Environment

The recommended JRE for SESM Release 3.1(7) is JRE Version 1.3.1_03, which is bundled with the SESM product.

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 have improved performance.

SESM Release 3.1(7) does not work with JRE Version 1.4.

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 forms the basis of the remote management and configuration support provided by the CDAT application. For example, an administrator can make configuration changes and can have these changes persisted with this new support.

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

Starting with SESM Release 3.1(5), the JMX HTML adaptor server is required if a deployer needs this feature as part of the CDAT application.

To protect access to SESM application management consoles, the JMX interface prompts for a username and password. For additional security, the deployer could deploy the SESM application behind a firewall.

For information about configuring the login values for SESM application management consoles, see the "Configuring the Management Console MBean" section in the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide,* Chapter 3, "SESM Configuration Management."

Cisco SESM Security

Cisco SESM Release 3.1(7) 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 using 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 is 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.

iPlanet Directory Server 5.0 Fails to Remove Attribute

A known problem in iPlanet Directory Server 5.0 affects the CDAT application. The problem is that removing an attribute does not fully remove it. See Bug 554309 at this location:

http://docs.sun.com/source/816-5604-10/index.html

This issue has an impact on the CDAT application in the following situation. If `InetOrgPerson=UID` and an administrator changes the value of the Poolname (`CiscoDESSpoolName`) or Primary Service (`CiscoDESSprimaryService`) attribute to null, an exception is thrown. After the exception, unexpected behavior occurs in the CDAT application. The problem does not occur if the administrator changes Poolname or Primary Service to a value other than null.

The workarounds are:

- Rather than attempting to change the attribute value for Poolname or Primary Service in CDAT to null, change the values to something other than null.
- Apply iPlanet Directory Server 5.0 Service Patch 1
- Upgrade to iPlanet Directory Server 5.1

Caveats

Table 2 describes known problems in SESM Release 3.1(7).

Table 2 Caveats in SESM Release 3.1(7)

Category	Caveat	Description
General Issues	CSCdw50552	With a Netscape Version 4.7 browser, the following problems exist concerning the service list display area in the SESM application pages: • Service groups or mutually exclusive services cannot be collapsed. • When the subscriber has no subscribed services, the service list contains a white space where the Current Services folder should be. 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.
	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.
	CSCuk35634	The SESM applications do not work and are not supported with the Sun Version 1.4.0 JVM. Workaround: Use the Sun Version 1.3.1 JVM instead.

Table 2 Caveats in SESM Release 3.1(7) (continued)

Category	Caveat	Description
General Issues *(continued)*	CSCuk38280	The Web Services Gateway (WSG) application currently does not support single sign-on or Port Bundle Host Key (PBHK) mode. Workaround: None.
	CSCuk38635	During SESM web application development with the Jetty web server, compilation of JSP pages only occurs once while the web application is running. If a JSP page is modified more than once while the web application is running, the changes cannot be observed until the web server is restarted. Workaround 1: Use Java 2 SDK version 1.4.1 (JDK 1.4.1) and Demo mode for SESM web application development. The JDK 1.4.1 is available at: http://java.sun.com/j2se/1.4.1/index.html For information on what you need to do if you install a JDK after installing the SESM software, see the “Installing a Java 2 SDK After Installing SESM” section in Chapter 2 in the *Cisco Subscriber Edge Services Manager Web Developer Guide*. The JDK 1.4.1 should not be used for SESM deployment. Under Windows, you may find that a JSP-page file is locked for writing after pointing the browser at the page. The lock is released if you point the browser to a different page. Workaround 2: Use Dreamweaver UltraDev’s Live Data window, which artificially requests different pages each time. Changes to a JSP page can be observed immediately without restarting the web server. For information on using the Live Data window, see Chapter 2 of the *Cisco Subscriber Edge Services Manager Web Developer Guide*. **Note** The use of the Live Data window feature with Dreamweaver MX for JSP-page SESM development has currently not been tested. The Live Data window feature of Dreamweaver UltraDev has been verified for use with SESM development.

	CSCuk39499	The SESM web application does not display the service list when a session update determines that the user has changed. The problem occurs because the account profile is not being cached.
		Workaround: Change the profile and session timeouts to small values (such as two and four seconds, respectively). The configuration attributes for these timeouts are in the *web_app*/config/*web_app*.xml file (for example, nwsp/config/nwsp.xml), where *web_app* is the name of the SESM web application.
		After changing the timeout values, save the file and restart the web application.
		The lines for the attributes that control these timeouts are as follows:
		`<!--`
		`- This is the number of seconds between clearing group`
		`- and service caches.`
		`-->`
		`<Set name="profileCachePeriod" type="int">2</Set>`
		`<!--`
		`- This is the minimum length of time in seconds that an`
		`SESMSession`
		`- is held in memory without being accessed. SESMSessions are`
		`checked`
		`- regularly according to the profileCachePeriod.`
		`- If this is set to 0 (or undefined) profileCachePeriod*2 is used.`
		`-->`
		`<Set name="sessionCachePeriod" type="int">4</Set>`

Table 2 Caveats in SESM Release 3.1(7) (continued)

Category	Caveat	Description
Installation 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 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(7) (continued)

Category	Caveat	Description
Installation 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
	CSCuk37938	For a Linux custom installation, the installation process may lock up on the feature selection page if you make changes too soon after the page is displayed. Workaround: If the installation has locked up, use **Ctrl-C** on the command line, then restart the install and proceed as before to the Custom Installation page. Wait until the window is fully updated, typically indicated by a brief flicker in the window. After this occurs, it is safe to proceed with any feature selection as planned. If no flicker is noticed, it should be safe to proceed after approximately 10 seconds. This duration is dependent on the speed of the target server system.
	CSCuk37523	The console version of the uninstall process does not work. Workaround: Use the standard GUI-based uninstall process instead.
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.

Table 2 Caveats in SESM Release 3.1(7) (continued)

Category	Caveat	Description
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.
	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.
	CSCuk39878	On Windows-based installations of CDAT, the script cdatsvc.cmd, which installs the Windows service for CDAT, does not work correctly. This script is located in the *install_dir*\jetty\bin directory. Workaround: Use the startCDAT.cmd script to start CDAT. This script is also located in *install_dir*\jetty\bin.

Documentation Updates

This section includes new and updated information about SESM Release 3.1(7) 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 Subscriber Edge Services Manager Solutions Guide

The following information will appear in a future revision of the *Cisco Subscriber Edge Services Manager Solutions Guide*.

Web Services Gateway

The Web Services Gateway (WSG) application provides a Simple Objects Access Protocol (SOAP)-based interface enabling third-party web portals and subscriber management systems to integrate with the SESM and SSG solution. Any client application can interface with SSG through the WSG using SOAP over HTTP communication.

The WSG installation includes a web application configured to run in a Jetty container and a command-line client script for demonstration purposes. The WSG web application runs in RADIUS and LDAP modes. It does not work in Demo mode.

In this first release, the WSG client interface enables access to the SSG for the following activities:

- Authenticating, starting, and ending sessions on the SSG
- Obtaining session status
- Connecting and disconnecting services

Note This first release of WSG offers a preview of future development efforts. We invite interested parties to contact us through a Cisco account representative to discuss potential uses for WSG and participate in feature planning efforts for future releases.

Installing WSG

To install WSG:

1. In the SESM installation program, choose the custom installation option.
2. Check the WSG box in the list of custom installation options.

WSG is installed in the *install_dir*\wsg directory.

Configuring WSG

WSG is configured by default to run in a Jetty container on port 8100.

To change the Jetty container configuration for the WSG application, edit the following file:

```
jetty
    config
        wsg.jetty.xml
```

To change the WSG application configuration, you can either:

- Access the MBeans through the WSG AgentView (port 8200)
- Manually edit the following MBean configuration files:

```
wsg
    config
       lib.xml
       sesm.xml
       dessauth.xml
```

For explanations of the MBeans, see Chapter 5, “Configuring SESM Portals” in the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*.

Starting and Stopping the WSG Application

The SESM installation process installs and configures the WSG application to run in a Jetty container. To start and stop WSG, run its startup or stop script:

```
jetty
    bin
        WSGstart
        WSGstop
```

This script accepts all of the options and parameters that other SESM web applications use, including the mode option, which allows you to switch between LDAP, RADIUS, and Demo modes at run time. See Chapter 9, “Running SESM Applications,” in the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide* for more information.

The installed default port for the WSG is 8100. The management console (Agent View) runs on port 8200.

Running the Demonstration Client Interface

Note The client interface is intended for demonstration purposes only. It can provide an understanding of the WSG interface and possibilities for development. Contact us through your Cisco account representative to discuss your development goals and deployment requirements regarding a WSG interface.

The demonstration client interface script provides command line access to the WSG using SOAP remote procedure calls (RPC). The script is located in:

```
wsg
    bin
        wsgClient
```

To start the client, enter the following command:

wsgClient [*endpoint*]

Where *endpoint* is always:

http://*WSGhost*:8100/services/SESM

If you do not supply the endpoint, the script provides command usage help. The wsgClient command-line prompt is:

wsg>

At the prompt, enter **help** to display available commands. At subsequent prompts, enter any of the commands.

Examples

The following examples show the WSG client command-line interface and output from various commands.

```
user1> wsgClient.sh http://localhost:8100/services/SESM
wsg/webapp/WEB-INF/lib/auth.jar:wsg/webapp/WEB-INF/lib/authentication.jar:wsg/webapp/WEB-I
NF/lib/axis.jar:wsg/webapp/WEB-INF/lib/com.cisco.sesm.contextlib.jar:wsg/webapp/WEB-INF/li
b/com.cisco.sesm.lib.jar:wsg/webapp/WEB-INF/lib/com.cisco.sesm.wsg.jar:wsg/webapp/WEB-INF/
lib/commons-logging.jar:wsg/webapp/WEB-INF/lib/dess.jar:wsg/webapp/WEB-INF/lib/jaxrpc.jar:
wsg/webapp/WEB-INF/lib/jmxri.jar:wsg/webapp/WEB-INF/lib/jmxtools.jar:wsg/webapp/WEB-INF/li
b/log4j-1.2.4.jar:wsg/webapp/WEB-INF/lib/mail.jar:wsg/webapp/WEB-INF/lib/protect.jar:wsg/w
ebapp/WEB-INF/lib/saaj.jar:wsg/webapp/WEB-INF/lib/sesm.jar:wsg/webapp/WEB-INF/lib/tt-bytec
ode.jar:wsg/webapp/WEB-INF/lib/wsdl4j.jar:lib/lib/com.cisco.sesm.lib.jar:redist/axis/lib/a
xis.jar:redist/axis/lib/commons-logging.jar:redist/axis/lib/jaxrpc.jar:redist/axis/lib/log
4j-1.2.4.jar:redist/axis/lib/mail.jar:redist/axis/lib/saaj.jar:redist/axis/lib/tt-bytecode
.jar:redist/axis/lib/wsdl4j.jar:redist/jaxp/lib/crimson.jar:redist/jaxp/lib/jaxp.jar:redis
t/jaxp/lib/xalan.jar

wsg> help
act[ivateService] svc [user passwd] - Activate service
auth[enticate] user passwd - Authenticate username/password
dea[ctivate] svc - Deactivate service
```

```
end[session] - End the session
get[status] - Get status
h[elp] - This summary
host[key] ip[/port][;name=value ..] - Set hostkey
q[uit] - Quit client

wsg> hostkey 121.121.122.3
hostkey=121.121.122.3
```

In the preceding command, 121.121.122.3 is the IP address of the subscriber. The SSG must be able to route this address. It uses the address to bind a downlink interface when it creates the edge session for the subscriber.

```
wsg> authenticate ug1-u1 cisco      // username/password respectively
authenticate=true

wsg> get
Identity user: ug1-u1
Service proxy3: off
Service Chris-PT1: off
Service proxy2: ON
Service proxy1: off
Service tunnel7200uk7: off
Service ptSg2: off
Service ptSg1: off
Service pt2: off
Service pt1: off
Service SgMutexSelct1: off
Service sg1: off
Service tunnelNrp4: off
Service Chris-PT-Seq2: off
Service Chris-PT-Seq1: off
Service ?????: off
Service ptMutexSelect3: off
Service ptMutexSelect2: off
Service ptMutexSelect1: off

wsg> act pt1
activate pt1 = true

wsg> get
Identity user: ug1-u1
Service proxy3: off
Service Chris-PT1: off
Service proxy2: ON
Service proxy1: off
Service tunnel7200uk7: off
Service ptSg2: off
Service ptSg1: off
Service pt2: off
Service pt1: ON
Service SgMutexSelct1: off
Service sg1: off
Service tunnelNrp4: off
Service Chris-PT-Seq2: off
Service Chris-PT-Seq1: off
Service ?????: off
Service ptMutexSelect3: off
Service ptMutexSelect2: off
Service ptMutexSelect1: off

wsg> dea pt1
deactivate pt1
```

```
wsg> act tunnelNrp4 cisco cisco   // An example of activating authenticated tunnel service
activate tunnelNrp4 = true

wsg> get
Identity user: ug1-u1
Service proxy3: off
Service Chris-PT1: off
Service proxy2: ON
Service proxy1: off
Service tunnel7200uk7: off
Service ptSg2: off
Service ptSg1: off
Service pt2: off
Service pt1: off
Service SgMutexSelct1: off
Service sg1: off
Service tunnelNrp4: ON
Service Chris-PT-Seq2: off
Service Chris-PT-Seq1: off
Service ?????: off
Service ptMutexSelect3: off
Service ptMutexSelect2: off
Service ptMutexSelect1: off

wsg> deactivate tunnelNrp4
deactivate tunnelNrp4

wsg> get
Identity user: ug1-u1
Service proxy3: off
Service Chris-PT1: off
Service proxy2: ON
Service proxy1: off
Service tunnel7200uk7: off
Service ptSg2: off
Service ptSg1: off
Service pt2: off
Service pt1: off
Service SgMutexSelct1: off
Service sg1: off
Service tunnelNrp4: off
Service Chris-PT-Seq2: off
Service Chris-PT-Seq1: off
Service ?????: off
Service ptMutexSelect3: off
Service ptMutexSelect2: off
Service ptMutexSelect1: off

wsg> end
endSession

wsg> quit
test-user-u10:165>
```

Cisco Distributed Administration Tool Guide

The following information will appear in a future revision of the *Cisco Distributed Administration Tool Guide*.

The Block Inheritance checkbox in the Users and Users Groups window has changed:

- In the Users window, the Block Inheritance box is now named Block Service Inheritance. If this box is checked, subaccounts created by this user inherit service subscriptions from this user account (the parent account). If this box is not checked, subaccounts created by this user inherit service subscriptions from the user groups to which the parent account belongs.
- In the User Groups window, the Block Inheritance box has been removed.

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*.

Note The precompile.sh script that is included with the SESM Release 3.1(7) software is compatible with an earlier release (SESM Release 3.1(5)) but *not compatible* with SESM Release 3.1(7). The precompile.sh script for SESM Release 3.1(7) and instructions for its use are contained in the *"Precompiling JavaServer Pages"* section that follows.

Precompiling JavaServer Pages

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 for the first time.

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.

A precompiling script is currently not available for Windows-based workstations.

Using the Precompiling Script

Note Before using the precompiling script, ensure that you have a backup copy of two files that your SESM web application is currently using: the web.xml file in /*install_dir*/*web_app_name*/webapp/WEB-INF and the jsp.jar file in /*install_dir*/*web_app_name*/webapp/WEB-INF/lib. Because the precompiling script overwrites these two files, you should copy them to some other safe location where you can retrieve them if you need a copy.

To create and execute the script needed to precompile a set of JSP pages, perform the following steps on a UNIX workstation where the SESM software is installed:

Step 1 Change directories so that /*install_dir*/tools/bin is your current directory, where /*install_dir* is the location where the SESM software is installed.

Step 2 Using a text editor, create a shell script by copying and pasting the script in Figure 1 (below) into a file. Name the file precompile.sh and save it in the tools/bin directory.

Step 3 To make the script executable, issue the following command:

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

Step 4 Run the script precompile.sh and wait for completion, which may take a few minutes.

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

The script can be run from any directory because the paths used in the script are all full path names. If you do *not* run the script from the recommended directory, then set the environment variable `SESM_HOME` to be the full path name of the SESM installation directory.

Figure 1 Script for Precompiling JSP Pages

```
#!/bin/sh
#
# Copyright (c) 2002 by Cisco Systems, Inc.
#
# For versions of SESM from 3.1(7) onwards.
#
# This script pre-compiles JSPs and creates a jar file
# in the specified SESM application directory.
#
# It is intended for a pre-built instance of SESM which already
# includes the application for which the JSPs are to be updated.
#
# Note: this script cannot be converted to run on Windows,
# as JspC does currently not work on Wintel.
#
# Note: the search for the SESM install directory is:
# 1) look two directories up from this script
# 2) use the environment variable SESM_HOME if set
# 3) use the default value for INSTALLDIR given below.
#
# Note: the search for the JDK directory is:
# 1) use the environment variable JDK_HOME if set
# 2) use the default value for JDKDIR given below.
#
# Minor note: to eg set the environment variable JDK_HOME
# in Bourne shell: JDK_HOME=/usr/myJDK; export JDK_HOME
# in C shell: setenv JDK_HOME /usr/myJDK
# in K-shell: export JDK_HOME=/usr/myJDK
#
# Minor note: As opposed to the original jar file, no
# property files are included in the updated jar file,
# as they serve no further purpose there.

# The default SESM application
# This value is overridden by an optional argument
APPLICATION=nwsp

# The directory that SESM is installed in.
# If the application dir is not found in ../..
# (the script is assumed to be in <install dir>/test/bin)
# and if the env var SESM_HOME is not set, then
# this default is used.
INSTALLDIR=/opt/cisco/sesm_3.1.7

# The default directory that the JDK is installed in
# This value is overridden by the env var JDK_HOME
JDKDIR=/usr/java

usage()
{
    echo "Usage: `basename $0` [application]"
    echo "where the optional SESM application name (default: nwsp)"
    echo "is eg nwsp, pda, wap or messageportal"
    exit 1
}

# Handle command line options
if  [ $# -eq 1 ]
then
        case $1 in
             -? | -help | -* )
        usage
        ;;
        * )
             APPLICATION=$1
        esac
elif  [ $# -gt 1 ]
then
        echo Too many arguments
        usage
fi
echo "SESM application: $APPLICATION"

# Find the installation directory
DEFAULTDIR=$INSTALLDIR
cd `dirname $0`/../..
INSTALLDIR=`pwd`
if [ ! -d $INSTALLDIR/$APPLICATION ]
then
        INSTALLDIR=${SESM_HOME:=$DEFAULTDIR}
        if [ ! -d $INSTALLDIR/$APPLICATION ]
        then
                echo Directory $INSTALLDIR/$APPLICATION does not exist.
                echo This script searches first two directories up from
                echo where it resides. If it does not find the
                echo application directory there, it checks the environment
                echo variable SESM_HOME. If this is not set, it looks
                echo in the default directory $DEFAULTDIR.
                exit 1
        fi
fi
echo "SESM directory:   $INSTALLDIR"

# Find the JDK directory: use the env var JDK_HOME if defined
JDKDIR=${JDK_HOME:=$JDKDIR}
echo "JDK directory:    $JDKDIR"

JAVACEXE=javac
JAVAEXE=java

JAVAC=$JDKDIR/bin/$JAVACEXE
JAVA=$JDKDIR/bin/$JAVAEXE

if [ ! -x $JAVAC ]
then
        echo The environment variable JDK_HOME must point to a valid JDK.
        echo The JSPs have not been compiled.
        exit 1
fi

# Check we can find a suitable version of the JDK
JAVA_VER=`$JAVA -version 2>&1 | grep 'java version' 2>&1\
 | sed -e 's/\.//g' -e 's/java version "\([0-9]*\).*"/\1/g'`

if [ ! $JAVA_VER -ge 122 ]
then
        echo Java version must be >= 1.2.2 - it is $JAVA_VER.
        echo Have you set the environment variable JDK_HOME?
        echo The JSPs have not been compiled.
        exit 1
fi

echo ""

# Application directory
APPDIR=$INSTALLDIR/$APPLICATION

# Location for generated xml for JSPs
XMLINC=$APPDIR/config/jsp.xml

# Temporary directory for source code
SRCDIR=$APPDIR/gensrc
if [ ! -d $SRCDIR ] ; then
    mkdir $SRCDIR
fi

# Temporary directory for classes
CLASSESDIR=$APPDIR/genclasses
if [ ! -d $CLASSESDIR ] ; then
    mkdir $CLASSESDIR
fi

# Create java files from the JSPs
echo "Creating Java files from the JSPs ..."
$JDKDIR/bin/java -classpath $INSTALLDIR/jetty/lib/javax.servlet.jar:\
$INSTALLDIR/jetty/lib/org.apache.jasper.jar:\
$INSTALLDIR/dess-auth/lib/auth.jar:\
$INSTALLDIR/dess-auth/lib/dess.jar:\
$INSTALLDIR/dess-auth/lib/protect.jar:\
$INSTALLDIR/dess-auth/lib/authentication.jar:\
$INSTALLDIR/redist/jmx/lib/jmxri.jar:\
$INSTALLDIR/jetty/lib/org.mortbay.jetty.jar:\
$INSTALLDIR/redist/jaxp/lib/jaxp.jar:\
$INSTALLDIR/redist/jaxp/lib/crimson.jar:\
$APPDIR/webapp/WEB-INF/lib/sesm.jar:\
$APPDIR/webapp/WEB-INF/lib/com.cisco.sesm.contextlib.jar:\
$INSTALLDIR/lib/lib/com.cisco.sesm.lib.jar org.apache.jasper.JspC \
 -die -d $SRCDIR -webinc $XMLINC -uriroot $APPDIR/webapp \
 -webapp $APPDIR/webapp

# Compile the java files
echo "Compiling Java files ..."
$JDKDIR/bin/javac -deprecation  -classpath \
$INSTALLDIR/jetty/lib/javax.servlet.jar:\
$INSTALLDIR/jetty/lib/org.apache.jasper.jar:\
$INSTALLDIR/dess-auth/lib/auth.jar:\
$INSTALLDIR/dess-auth/lib/dess.jar:\
$INSTALLDIR/dess-auth/lib/protect.jar:\
$INSTALLDIR/dess-auth/lib/authentication.jar:\
$INSTALLDIR/redist/jmx/lib/jmxri.jar:\
$INSTALLDIR/jetty/lib/org.mortbay.jetty.jar:\
$INSTALLDIR/redist/jaxp/lib/jaxp.jar:\
$INSTALLDIR/redist/jaxp/lib/crimson.jar:\
$APPDIR/webapp/WEB-INF/lib/com.cisco.sesm.contextlib.jar:\
$INSTALLDIR/lib/lib/com.cisco.sesm.lib.jar:\
$APPDIR/webapp/WEB-INF/lib/sesm.jar -d $CLASSESDIR \
 `find $SRCDIR -name '*.java' -print`

# Create the jar file
JARFILE=$APPDIR/webapp/WEB-INF/lib/jsp.jar
echo "Creating jsp.jar ..."
cd $CLASSESDIR
rm -f $JARFILE
$JDKDIR/bin/jar cvf $JARFILE \
 `find . -type f -print | sed -e 's=^\./=='`

# Modify web.xml
XMLSRC=$APPDIR/webapp/WEB-INF/web.recompile.xml
XMLTMP=$APPDIR/webapp/WEB-INF/web.tmp.xml
XMLDEST=$APPDIR/webapp/WEB-INF/web.xml
if fgrep -s PRE_COMPILE $XMLSRC
then
    echo "Updating web.xml ..."
    rm -f $XMLTMP $XMLDEST
    sed -e 's=<jsp-file>/\(.*\)\.jsp=<jsp-file>\1=' \
            -e '/<jsp-file>/s=/=.=g' \
            -e 's=<jsp-file>\(.*\)<\.jsp-file>=<servlet-class>\1</servlet-class>=g' \
            $XMLSRC >$XMLTMP
    sed -e  "/PRE_COMPILE/r $XMLINC" \
            -e 's=JASPER:==' $XMLTMP >$XMLDEST
    chmod a-w $XMLDEST
fi

# Clean up
echo "Cleaning up ..."
cd $APPDIR
rm -rf $SRCDIR $CLASSESDIR $XMLINC $XMLTMP

echo "Done."
```

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*
- *Cisco Subscriber Edge Services Manager Solutions 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 you call, check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, have your service agreement number and your product serial number available.

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