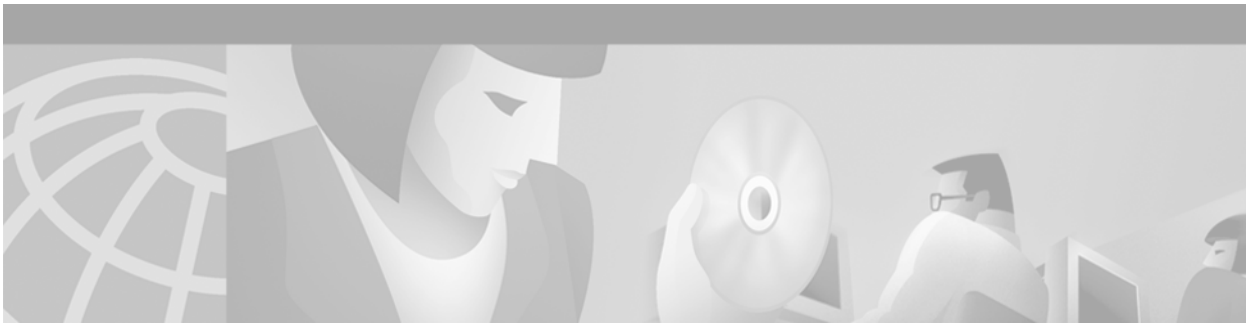

Release Notes for the Cisco Subscriber Edge Services Manager, Release 3.1(3)

April 2002

These release notes contain important information regarding the Cisco Subscriber Edge Services Manager (Cisco SESM) Release 3.1(3).

Note For information about obtaining a license number, see the "Obtaining a License Number" section on page 6.

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(3) 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(3) 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.

SESM-SPE includes two additional supporting applications:

- Cisco Distributed Administration Tool (CDAT)—A web-based interface for administrators that manages data in the SPE extensions to the LDAP directory.
- 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 components—For SESM running in LDAP mode, SPE components 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:

- Sun Ultra10 or Sun E250 running Sun Solaris Version 2.6 (or later version)
- Windows NT and Windows 2000
- Linux—Red Hat Linux Version 7.1 and SuSE Linux

SSG Devices

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(3):

- 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 12.1(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
- The SSG TCP redirect feature must be configured appropriately

Port-bundle Host Key Compatibility

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

New and Changed Information

This section describes new features introduced in SESM Release 3.1(3).

New Features for RADIUS and LDAP Mode

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

- The New World Service Provider (NWSP) web portal application detects the subscriber's device (for example, PC or WAP phone) and serves content customized for the device.
- Two new sample web portal applications demonstrate how SESM might be used for service selection on specific devices:
  - The Personal Digital Assistant (PDA) application is designed for handheld devices.
  - The Wireless Application Protocol (WAP) application is designed for mobile phones.
- SESM and SSG can support authentication based on three credentials rather than the standard two.
- SESM portals can support mutually exclusive service selection, which restricts a subscriber to connecting to only one service at a time in a configured group of services.
- The SESM single sign-on feature now supports non-PPP clients. When single sign-on is enabled, a subscriber remains authenticated even if the SESM session terminates, as long as the host object remains in the SSG. For example, subscribers might close their browsers, but remain connected to services. When they reopen the browser, they do not need to reauthenticate.
- SESM captive portal feature supports four redirection types offered by the SSG TCP redirect feature:
  - Unauthenticated user redirections
  - Service redirections
  - Initial logon redirection
  - Advertising redirection

Additional New Features for LDAP Mode

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

- The RDP server includes an optional configuration option that restricts it to servicing a configured list of clients (SSGs).
- The CDAT application includes support for new fields and options. See the "Cisco Subscriber Edge Services Manager Web Developer Guide" section on page 14.
- Passwords stored in the LDAP directory are encrypted.
- Deployers can impose limits on the number of subaccounts that can be created within a main account.

Enhanced Web-Application Software

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

- The SESM web application components are more fully modularized, separating the presentation components into easy-to-customize JSP pages and the processing logic into a set of preprogrammed Java servlets.
- Support for internationalization and localization is extended. The SESM web-application software is more fully internationalized and additional language-specific properties files are added to the resource bundles.
- Three additional JSP tag libraries minimize the need for Java coding in the JSP pages. The new tag libraries are: Iterator, Navigator, and Shape.
- For easier development and testing, the SESM web application software includes a set of test “decorator” servlets that allow the developer to easily simulate various user profiles, brands, devices, and locales.

New SESM Deployment Option

This release introduces support for a new deployment option, whereby the SESM application is deployed without the SSG enabled on the edge router. In this deployment, the SESM application does not provide support for service selection, but it can be used as a subscriber management system. This deployment option is only possible when SESM is operating in LDAP mode, with support for the self-care features.

Self-care can enable features such as:

- Subscriber selected PVCs
- Personal Firewalls

These features will be fully demonstrated in a future SESM release.

A new input panel in the SESM installation program allows the installer to choose whether to deploy the SESM application in a network with an SSG. The check box defaults to Yes, as most installations will continue to take advantage of the SSG features. If you do not want to make use of SSG features in your deployment, uncheck the box. In this release, this deployment option only makes sense in LDAP mode.

This feature has not yet been fully validated and does not appear in the SESM documentation set.

Installation Notes

The following sections highlight some important installation information.

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

Obtaining a License Number

The SESM installation program provides for two types of installation:

- Evaluation—You can install 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-3.1.3-pkg-sol.tar
- For Linux platforms: sesm-3.1.3-pkg-linux.tar
- For Windows platforms: sesm-3.1.3-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(1)

Web Portal Development

An SESM Release 3.1(1) portal application works in an SESM Release 3.1(3) deployment with some modifications. To help you with the migration process, a modified version of NWSP from SESM Release 3.1(1) is included with SESM Release 3.1(3) in a subdirectory called nwsp311. The nwsp311 application was precompiled using SESM Release 3.1(3) libraries. The nwsp311 application code contains comments explaining all required modifications.

Captive Portal Configuration

To configure the SSG TCP redirect feature to work with the sample SESM captive portal solution, the captive portal server must be the IP address of the SESM Captive Portal application. This is different from how you configured SSG to work with the captive portal solution in SESM Release 3.1(1). In Release 3.1(1), the SSG captive portal server was the IP address of the NWSP application.

LDAP Mode Deployments

The SPE directory extensions contain new fields. You can use options in the SESM installation program to load the new extensions.

Note You must first delete the old extensions. If you are using the NDS eDirectory, you must reinstall the directory.

Upgrading from the Service Selection Dashboard Release 3.0(1)

The Cisco Service Selection Dashboard (SSD) Release 3.0(1) is essentially the same as SESM Release 3.1(1) in RADIUS mode. An SSD Release 3.0(1) web application works in an SESM RADIUS mode deployment. Some changes were made in the XML Document Type Definition (DTD)

for the MBean configuration files. Therefore, there are slight differences in the configuration files from those that were installed for SSD Release 3.0(1). There are a few new optional configuration parameters. Some Java APIs were deprecated, and the NWSP sample application was improved.

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

Upgrading from SSD Release 2.5(1)

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

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

If you are currently using SSD Release 2.5(1) or earlier, see the "Upgrading from SSD Release 2.5(1)" section in *Release Notes for Cisco Subscriber Edge Services Manager Release 3.1(1)* for migration information. The online location is:

http://www.cisco.com/univercd/cc/td/doc/solution/sesm/sesm_311/rnsesm31.htm

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 for caveat CSCuk27495 in the "Caveats" section on page 11.

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(3) 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. This console displays the currently set values for all attributes in the XML configuration files and is useful for development environments.

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

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

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

```
name="management.portno"/></Set>
<Call name="start"/>
</Configure>
```

Cisco SESM Security

Cisco SESM Release 3.1(3) 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 5, “Running SESM Components,” in the *Cisco Subscriber Edge Services Manager and Subscriber Policy Engine Installation and Configuration Guide* for more details about memory requirements.

Caveats

Table 1 describes known problems in SESM Release 3.1(3).

Table 1 Caveats in SESM Release 3.1(3)

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.
	CSCuk28781	If a home URL does not contain the complete URL information, the resulting popup homepage that the subscriber sees after logging in the next time is malformed. Workaround: Instead of entering a URL such as www.cisco.com, enter the complete URL as in http://www.cisco.com.
	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 was not subscribed to the service group. Workaround: Do not define services in a service group as auto-logon in a user group.
	CSCuk31416	For the RDP component, if you configure the service and group passwords to be the same, then service connections always fail. Workaround: Ensure that the RDP is configured so that the service and group passwords are unique.
	CSCuk32513	When the RDP component is used in a deployment in which the SSG is in RADIUS proxy mode, authentication failures result in an Access Reject message returned from the RDP to the SSG without the Proxy attribute (33) present. In this instance, the SSG ignores this response and does not reply to the originating client. Workaround: None
	CSCuk32279	Display-related issues exist with the Service List page if the service list includes a service group with a service that is no longer valid. A service could be invalid because it is misconfigured in the RADIUS server database, or in LDAP mode, because it was deleted by an administrator using the CDAT interface. After the SSG host object is cleared and the user logs in again, this problem is resolved. Workaround: Try to ensure that all users are unsubscribed from the service that you wish to delete before deleting it.

Table 1 Caveats in SESM Release 3.1(3) (continued)

Category	Caveat	Description
General Issues *(continued)*	CSCuk32591	For Proxy and Tunnel service types, if a subscriber decides to enter or change a service username and password for a subscribed service, the changes have no effect. Workaround: If this occurs, the subscriber must unsubscribe and then resubscribe to the affected service.
	CSCuk32619	On the Linux platform, the SESM portal application stop scripts (for example, stopNWSP) sometimes fail. Workaround: After running the stop script, manually verify if the process stopped. If it is not stopped, use native Linux commands to manually kill the relevant process.
	CSCuk32607	In LDAP mode, the Next Hop Gateway functionality for a service does not work. Workaround: Manually bind services on the edge router using Cisco IOS CLI commands.
	CSCuk32606	Authentication or session logon with a WAP device fails if the subscriber is subscribed to any services that do not have a defined service route. Workaround: Ensure that all services required by WAP-based subscribers have service routes defined in the service profile.
	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.
Install Issues	CSCuk27495	If you are installing SESM from the SESM product CD-ROM onto a Windows NT platform, the installation application fails because it tries to write to the CD's partition, which is read-only. Workaround: Copy the installation file to your Windows NT platform and execute the local copy to install SESM.
	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.

Table 1 Caveats in SESM Release 3.1(3) (continued)

Category	Caveat	Description
Install Issues *(continued)*	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 and Subscriber Policy Engine Installation and Configuration Guide* for further details, including a list of the well-known directories.
	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
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 1 Caveats in SESM Release 3.1(3) (continued)

Category	Caveat	Description
CDAT Issues *(continued)*	CSCuk32405	A known problem in iPlanet Version 5.0 affects the CDAT application. The problem is that removing an attribute does not fully remove it. For more information, see the following locations regarding iPlanet Bug 554309: http://docs.iplanet.com/docs/manuals/directory/50sp1/relnotes.html#19127 http://docs.iplanet.com/docs/manuals/directory/50sp1/relnotes.html. This issue has an impact on the CDAT application in the following situation. If the InetOrgPerson is set to UID, and an administrator removes Poolname or Primary Service, it causes an exception and unexpected behavior in the CDAT application. If you change the Poolname or Primary Service to a value other than a null string, this problem does not occur. Workarounds: Either: • Do not remove the Poolname or Primary Service. • Apply the iPlanet Version 5.0 SP1 patch or upgrade to iPlanet Version 5.1.
	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 information about SESM Release 3.1(3) that does not appear in the *Cisco Subscriber Edge Services Manager Web Developer 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 when it is requested. 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 (Figure 1). 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.

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

Step 1 In the directory where the SESM software is installed, create a directory called tools/bin and make tools/bin your current directory.

Step 2 Using a text editor, create a shell script by copying and pasting the script in Figure 1 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 some time.

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 as the paths used in the script are all full path names. If you do 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(3) 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_3.1.3

# 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

# Manifest for JAR file
MANIFESTV=$APPDIR/manifest.mfv

# 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/docroot/WEB-INF/lib/sesm.jar:\
$APPDIR/docroot/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/docroot\
 -webapp $APPDIR/docroot

# 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/docroot/WEB-INF/lib/com.cisco.sesm.contextlib.jar:\
$INSTALLDIR/lib/lib/com.cisco.sesm.lib.jar:\
$APPDIR/docroot/WEB-INF/lib/sesm.jar -d $CLASSESDIR\
 `find $SRCDIR -name '*.java' -print`

# Update the manifest file for the jar file
MANIFEST=$APPDIR/manifest.mf
LABEL="`whoami`, `uname -a`, `date`"
sed -e "s/Implementation-Version:.*/Implementation-Version: $LABEL/g"\
 <$MANIFEST >$MANIFESTV

# Create the jar file
JARFILE=$APPDIR/docroot/WEB-INF/lib/jsp.jar
echo "Creating jsp.jar ..."
cd $CLASSESDIR
rm -f $JARFILE
$JDKDIR/bin/jar cvf0m $JARFILE $MANIFESTV\
 `find . -type f -print | sed -e 's=^\./=='`

# Modify web.xml
XMLSRC=$APPDIR/docroot/WEB-INF/web.recompile.xml
XMLDEST=$APPDIR/docroot/WEB-INF/web.xml
if fgrep -s PRE_COMPILE $XMLSRC
then
echo "Updating web.xml ..."
rm -f $XMLDEST
sed -e  "/PRE_COMPILE/r $XMLINC" $XMLSRC\
        | sed -e 's=JASPER:==' > $XMLDEST
```

```
chmod a-w $XMLDEST
fi

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

echo "Done."
```

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 and Subscriber Policy Engine 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.