C H A P T E R **13**

Troubleshooting SESM Installation and Configuration

This chapter provides some help with troubleshooting problems in a Cisco Subscriber Edge Services Manager (SESM) deployment. It includes the following topics:

Diagnosing Problems

This section contains procedural charts that show you how to research a problem and identify the general area of the problem before escalating it to the Cisco Technical Assistance Center. The section includes the following procedures:

Procedures for Troubleshooting SESM Portals

Figure 13-1 shows a procedure for analyzing problems in SESM portal applications. The numbered callouts are keyed to the table that follows the figure.

Diagnosing Problems

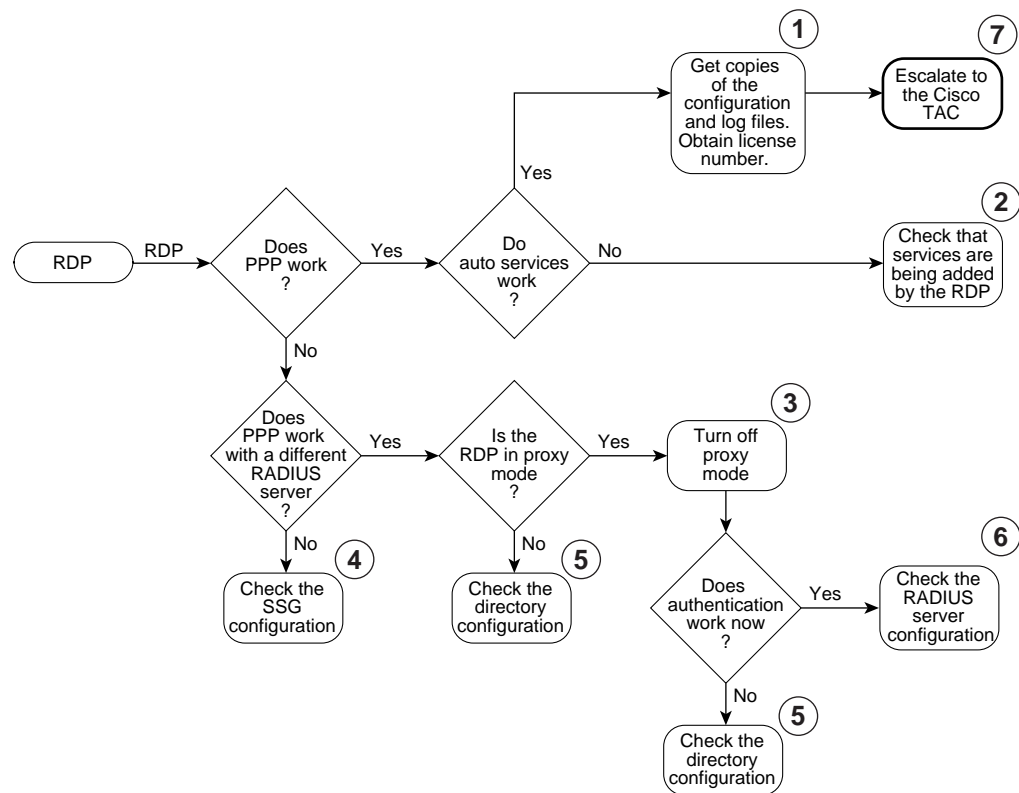*Figure 13-1   Procedures for Troubleshooting SESM Portal Applications*
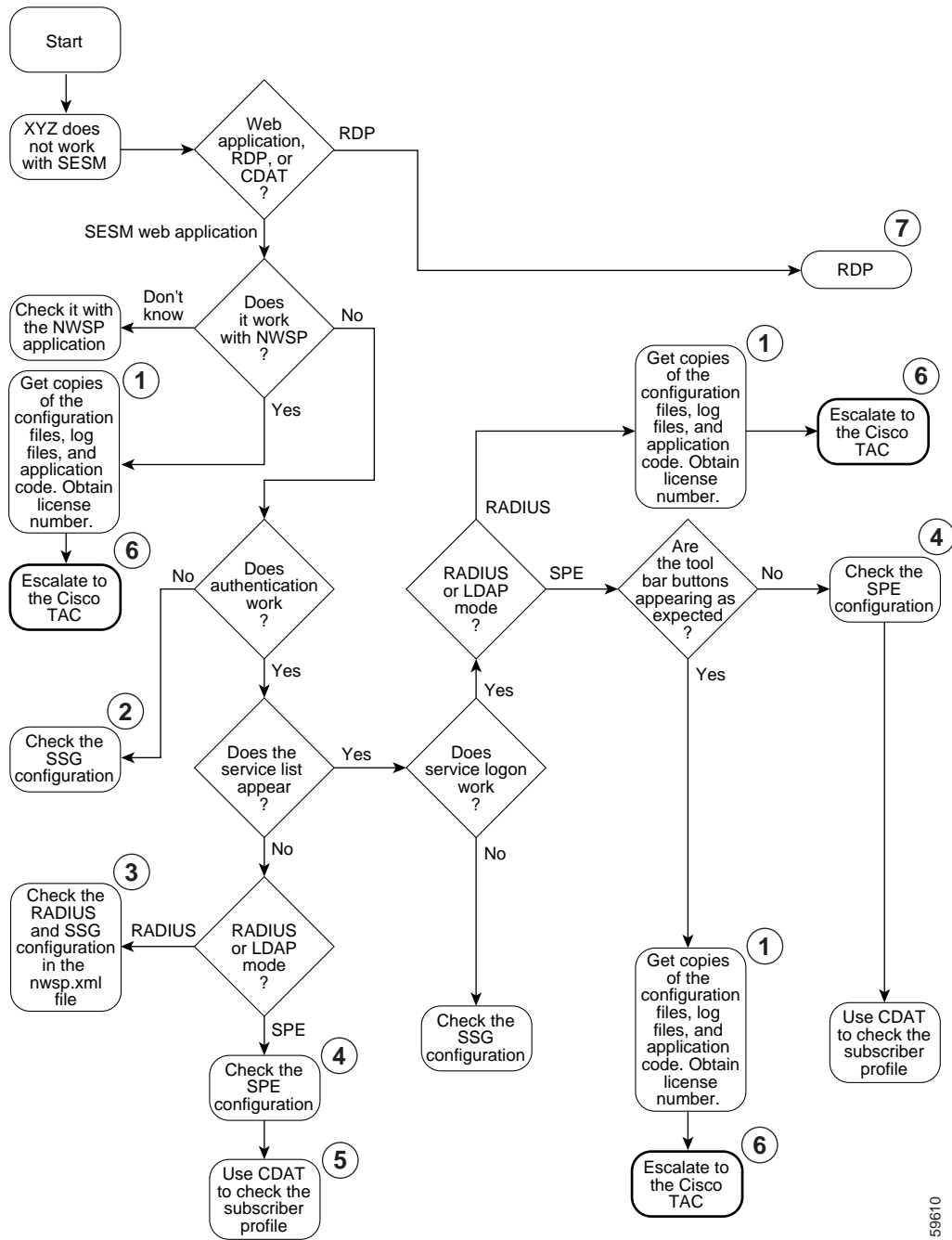
1	See MBean Configuration File Names, page 3-14 , Log File Descriptions, page 13-4 , and Obtaining License and Version Information, page 13-5.
2	See Basic SSG Configuration, page F-1.
3	See SSG MBean, page 5-7 and AAA MBean, page 5-10.
4	See SPE Attributes, page 8-1.

5	Make sure the subscriber is subscribed to services and has the proper privileges to access those services. See the CDAT documentation: http://www.cisco.com/univercd/cc/td/doc/solution/sesm
6	See Obtaining Technical Assistance, page xvi.
7	See Procedures for Troubleshooting RDP, page 13-3.

Procedures for Troubleshooting RDP

Figure 13-2 shows a procedure for analyzing problems in RDP. The numbered callouts are keyed to the table that follows the figure.

Figure 13-2   Procedures for Troubleshooting RDP

1	See MBean Configuration File Names, page 3-14, Log File Descriptions, page 13-4, and Obtaining License and Version Information, page 13-5.
2	See Adding Service Information to Replies, page 7-2.
3	See Changing the RADIUS Data Proxy Mode, page 7-2.
4	See Configuring the SSG for SESM Deployments, page F-1.
5	See Configuring Security Policy Engine for SESM, page 8-1.
6	See the client and server socket components in the RDP MBean, page 7-4and RADIUS Data Proxy MBeans, page 7-3.
7	See Obtaining Technical Assistance, page xvi.

■ **Troubleshooting Aids**

Troubleshooting Aids

This section describes some facilities that might be useful in troubleshooting SESM installation and configuration problems. It includes the following topics:

- Log File Descriptions, page 13-4
- Log File Configuration, page 13-4
- Java Command Line Options, page 13-5
- Obtaining License and Version Information, page 13-5

Log File Descriptions

The SESM log files can help troubleshoot SESM applications and deployments. By changing the configuration of the logging and debugging mechanisms, you can change the amount of detail reported and specify message filtering. Two of the log files have debugging mechanisms in addition to the logging features.

- Jetty HTTP Request log—Contains incoming HTTP requests. You can use this log file to analyze volume and traffic patterns for the web server.
- Jetty log—Contains logging and debugging messages from Jetty. The logging messages record the startup of the Jetty server and all ongoing activity, such as errors trapped by the Jetty server and HTTP errors. If the SESM application fails to start, look at this log. Make sure you monitor this log file for illegal HTTP requests that might indicate attempts to subvert the web server. If you enable debugging, the log file also includes more detailed debugging messages.
- Application log—Contains logging and debugging messages from the SESM application. The logging tool logs SESM web application activity. The debugging mechanism produces messages useful to developers in debugging applications.

You can configure all three of these logs for each SESM portal application and for CDAT. RDP uses only the application log.

Log File Configuration

Table 13-1 shows the MBeans that configure the log files. The MBeans control the level of verbosity in the logs, message filtering, debugging, file location, and file management.

Table 13-1   Configuring the Log Files

Log Type	MBean Name and Reference to More Information	Filename Attribute	Default Log Filename
Request log	Server MBean, page 4-5	RequestLog	*date*.request.log
Jetty log	Log MBean, page 4-3 Debug MBean, page 4-4	filename	*date*.jetty.log
Application log	Logger MBean, page 5-2	logFile	*date*.application.log

To change the location of a log file, change the value of the filename attributes listed in Table 13-1. All of the log filename attributes use the application.home property, which ensures that all logs for an application are located in the same directory. The value for the application.home property is set by the start script at run time. See Table 9-1 on page 9-5, "Java System Properties in Startup Scripts" for more information about the application.home property.

The installed default configuration places all log files for an application into the logs subdirectory under the application home directory. For example:

```
SESMinstallDir
    nwsp
        logs
```

If the logs directory does not exist, it is created at application runtime.

Java Command Line Options

When you execute a startup script that includes the java command, you can specify any Java option on the command line. To specify Java options, use -jvm as an option on the command line. For example, you can add the following option to the command line when you execute the SESM application startup script:

```
-jvm –Djava.compiler=NONE
```

Obtaining License and Version Information

If you purchased SESM, your license number is available on the License Certificate shipped with the product. If you have not purchased SESM, you can install an evaluation copy of the software without a license number. An evaluation installation provides full software functionality. Although the evaluation options do not have an expiration period, you must obtain a license before deploying SESM in a production environment.

The installation program records the license number and the software version you installed in the licensenum.txt file under the installation directory.

Troubleshooting Tips

This section contains some hints that might help you identify and fix problems in SESM. The problems are divided into the following topics:

- JRE and JDK Troubleshooting, page 13-6
- Installation Troubleshooting, page 13-7
- Configuration File Location Troubleshooting, page 13-8
- SESM Configuration Troubleshooting, page 13-8
- RADIUS Configuration Troubleshooting, page 13-9
- SSG Configuration Troubleshooting, page 13-10

JRE and JDK Troubleshooting

If the SESM installation program does not find an appropriate JRE, it installs the bundled JRE. See the section "Installing the Bundled JRE" section on page 1-3.

This section contains the following topics:

- Java Warning and Error Messages at Application Startup, page 13-7
- Searching for an Existing JDK or JRE, page 13-6
- Using a Pre-installed JRE or JDK, page 13-7
- Recompiling a Customized JSP, page 13-7

Searching for an Existing JDK or JRE

The SESM installation program does the following when searching for a valid JDK or JRE:

1. It searches for a JDK Version 1.3.1 that is already installed.
2. Failing that, it searches for a JRE Version 1.3.1 or later that is already installed.
3. Failing that, it installs and uses the bundled JRE Version 1.3.1_03.

In some cases, even though a JRE is installed, the installation program may not find it or finds a different JRE.

On Windows NT, the installation program looks in the NT Registry for the location of a JDK or JRE. It searches for the following:

\Java\1.3.1	\JavaSoft\JRE\1.3.1
\Java\1.3	\JavaSoft\JRE\1.3
\Program Files\JavaSoft\JRE\1.3.1	\Java\JRE\1.3.1
\Program Files\JavaSoft\JRE\1.3	\Java\JRE\1.3

On Solaris and Linux, the installation program looks in the following well-known locations before installing the bundled JRE:

/usr/jdk1.3.1	/usr/java1.3.1	/usr/j2sdk1.3.1	/usr/jre1.3.1
/usr/jdk1_3_1	/usr/java1_3_1	/usr/j2sdk1_3_1	/usr/jre1_3_1
/usr/jdk1.3	/usr/java1.3	/usr/j2sdk1.3	/usr/jre1.3
/usr/jdk1_3	/usr/java1_3	/usr/j2sdk1_3	/usr/jre1_3
/usr/jdk	/usr/java	/usr/j2sdk	/usr/jre
/opt/jdk1.3.1	/opt/java1.3.1	/opt/j2sdk1.3.1	/opt/jre1.3.1
/opt/jdk1_3_1	/opt/java1_3_1	/opt/j2sdk1_3_1	/opt/jre1_3_1
/opt/jdk1.3	/opt/java1.3	/opt/j2sdk1.3	/opt/jre1.3
/opt/jdk1_3	/opt/java1_3	/opt/j2sdk1_3	/opt/jre1_3
/opt/jdk	/opt/java	/opt/j2sdk	/opt/jre

Using a Pre-installed JRE or JDK

On any of the installation platforms, you can specify the location of a pre-installed JRE or JDK by starting the installation process on a command line and specifying the javahome parameter, as follows:

installImageName -is:javahome *location*

Where:

installImageName is the name of the SESM downloaded image.

location is the path name for the JRE or JDK.

Recompiling a Customized JSP

The installed web.xml file points to precompiled versions of the JSPs. It does *not* reference the JSPs in /nwsp/webapp. Thus, changing the JSPs in webapp has no effect if you use the installed web.xml file.

If you do not see changes that you make to a JSP, do either of the following:

- Recompile the page when you run the application—See the *Subscriber Edge Services Manager Web Developer Guide* for procedures.

- Precompile the page before running the application—Run the precompile script in tools/bin.

Java Warning and Error Messages at Application Startup

SESM application startup might produce warning messages and nonfatal error messages. These messages are expected and normal.

- The warning message states that JSPs will not be compiled. You do not need to recompile JSPs to run the NWSP application.

  If you are a Web developer expecting to write new JSPs or change the NWSP JSPs, you must load the Java Development Kit (JDK). To obtain a recent JDK, go to:

  http://java.sun.com/products/j2se

- The nonfatal JIT relocation error message is the result of a problem within the bundled JVM obtained from Sun Microsystems. It does not affect SESM operation. You can ignore this message and all supporting information.

Installation Troubleshooting

This section describes some potential problems that you might encounter during installation.

No X Server for a Solaris Installation

To install SESM on a Solaris server with no X server, use the Silent or Console installation modes.

Incorrect Permissions

The SESM installation program writes to parts of the file system or Windows registry that are only accessible to a privileged user (that is, root on Solaris, or a member of the Administrators group on Windows NT). An SESM installation must be performed by a privileged user who has access to these resources. Otherwise, the outcome of the installation is unpredictable.

Files Not Found

If you receive Java error messages indicating missing files in system level directories (for example, /var, on Solaris), you do not have correct permissions to perform the installation. See the preceding "Incorrect Permissions" section.

Incomplete Installation or Files Installed in Incorrect Directory

On a Solaris system, if you remove the contents of the SESM installation directory using the **rm** command instead of uninstalling SESM using the uninstall utility, then subsequent installations of SESM into the same directory might be adversely affected.

Uninstall SESM using uninstall.bin. If uninstalling is not possible, before reinstalling SESM, delete the vpd.properties file from the home directory of the person who is performing the installation.

Note   If you deploy multiple SESM installations, and you delete the vpd.properties file to recover from removing one of the installations, then you cannot use uninstall.bin to uninstall any of the other installations.

Configuration File Location Troubleshooting

The SESM installation program places the J2EE web server and SESM configuration files in the correct directories as defined in the startup scripts. If the configuration files are moved for any reason, then you must edit the web.xml file to reflect the new locations.

SESM Configuration Troubleshooting

If the SESM software is installed correctly, and all of the configuration files are in the proper location, but the SESM web application does not function, then examine the configuration values in the application MBean configuration file (for example, nwsp/config/nwsp.xml).

Communication with SSG

If the SSG port number or shared secret specified in the SESM application's MBean configuration file does not match actual SSG configuration (as performed on the SSG host), the SSG cannot see the SESM requests or is unable to decrypt the requests because the shared secret does not match. When the shared secret does not match, the SSG returns an Access Reject message.

For more information on SSG configuration, see Appendix F, "Configuring the SSG for SESM Deployments."

Communication with RADIUS Server

If incorrect IP addresses or port numbers are specified in the SESM application's MBean configuration file for the primary and secondary RADIUS servers, the RADIUS servers cannot see the SESM requests.

If the IP addresses and port numbers are correct, the RADIUS server returns an Access Reject when either of the following errors is present:

- The shared secret specified for the RADIUS server in the application's MBean configuration file is not correct.

- The SESM web application is not properly configured as a RADIUS client.

For more information on RADIUS configuration, see Appendix C, "Configuring RADIUS for SESM Deployments."

Out of Memory Exceptions

Out of memory exceptions might indicate that there is not enough Java virtual memory reserved to handle the number of users currently logged on.

The generic startup script sets the Java virtual memory size to 64 MB. To change this value, stop the application, edit the generic start script (start.sh or start.cmd), and restart the application.

Web Server Unavailable

Messages stating that the web server is unavailable might indicate that there is not enough Java virtual memory reserved to handle the number of users currently logged on. Follow the instructions in the "Out of Memory Exceptions" section on page 13-9 to increase Java virtual memory.

RADIUS Configuration Troubleshooting

The RADIUS server must be configured to recognize the following two clients:

- SESM web application

- SSG

If either of these configuration items is incorrect, then the RADIUS server sends Access Reject messages in response to all requests. See the "Configuring RADIUS Clients" section on page C-1 for information on configuring these RADIUS clients.

For service profile requests, the password for service and service group profiles must match those defined for the SSG and the SESM application. This password is used in Access Request messages for profiles, where the profile name is the service or service group name and the password is as defined in the following two locations:

- The servicePassword attribute in the AAA section of the SESM application's MBean configuration file

- The service-password parameter for the SSG

SSG Configuration Troubleshooting

The SSG must have a default network location defined, from which the SESM web application is accessible. Otherwise, client requests never reach the SESM application, and the client browser eventually times out.

The SSG must have the radius-helper parameters configured with the correct port numbers and shared secret so that the SSG can see SESM messages and decrypt them. Because the SSG carries out authentication against the RADIUS server, it must also have the correct values defined for the radius-server parameters.

Considerations for Subscribers Using PDA Devices

This section describes how some characteristics of PDA devices might impact subscriber experiences when accessing the SESM portal.

- PDAs use basic IE browsers, which might lose the port number of the request during redirections. This characteristic might not be noticeable with simple configurations, but it is a problem with the SSG TCP redirection feature. It is therefore important to run the server on the default ports (80 for insecure connections, 443 for secure connections).

- The webapp/decorators/httpSniff.jsp is useful for fine-tuning the recognition of the subscriber device type. This JSP modifies the default behavior of the SESM HttpSniffBean decorator, which influences the shape decoration. See the *Cisco Subscriber Edge Services Manager Web Developer Guide* for more information about decorators.

- If a PDA device does not have an IP address, it cannot use DNS to resolve a requested URL. The result is a "Page Not Found" error.

  PDAs can take between 20 to 60 seconds to get an IP address after the subscriber logs out and reinserts the PC card. If the subscriber reinserts the card immediately and tries to browse, the "Page Not Found" error is returned. However, if the subscriber waits for an IP address before browsing, the browser should be redirected appropriately.

  The simplest way to verify that a PDA has an IP address is to use the WLAN card statistics utility. For example, the Cisco 350 card shows the number of unicast packets received and transmitted. Subscribers should make sure that the count is higher than 0 for received packets before attempting to login.

- PDA browsers cache easily. If a subscriber selects a web site that is cached, the cached page might display even though the subscriber is not authenticated. PDA browsers do not have controls for avoiding this behavior.