CHAPTER 3

Installing Components

This chapter describes how to install the Cisco Subscriber Edge Services Manager (SESM) software and bundled components, including SPE. It includes the following topics:

- Preparing for SESM Installation, page 3-1
- Obtaining the SESM Installation File and License Number, page 3-6
- Performing SESM Installation, page 3-7
- Installation and Configuration Parameters, page 3-10
- Installation Results, page 3-20
- Post-Installation Procedures, page 3-21

Preparing for SESM Installation

This section describes prerequisites to installing SESM. It includes the following topics:

- Installation Platform Requirements, page 3-1
- RAM and Disk Space Requirements, page 3-2
- Java Software Considerations, page 3-2
- SSG and RADIUS Considerations, page 3-4
- LDAP Directory Configuration Requirements, page 3-4

Installation Platform Requirements

This section describes platform requirements for installing the SESM components.

Solaris Platform Requirements

You must have the following hardware and operating system software to install the SESM software on Sun Solaris platforms:

- Sun Ultra10 or Sun E250 (or later version)
- Solaris Version 2.6 (or later version) operating system

Windows NT Platform Requirements

You must have the following hardware and software to install the SESM software on Windows NT platforms:

- Pentium III (or equivalent) processor
- Windows NT Version 4.0, Service Pack 5 (or later version)

RAM and Disk Space Requirements

Table 3-1 shows RAM and disk space requirements for a single instance of each component in SESM. These requirements are approximately the same on the Sun Solaris and the Windows NT platforms.

Table 3-1 RAM and Disk Space Requirements

Component Name	Disk Space (MB)	RAM
Jetty server	1.1	The Jetty server provides the J2EE application environment in which the NWSP and CDAT applications execute. The application memory needs specified for NWSP and CDAT, below, include Jetty server usage.
SESM and the NWSP application	9.1	RAM requirements increase relative to the number of instances running and the specific load. The following numbers are approximations: • In RADIUS mode, the NWSP application requires 17k bytes per subscriber. • In DESS mode, the NWSP application requires more. • In DESS mode, the cache adds to the memory requirements. See the "DESS Attributes" section on page 4-37 for cache size information.
RDP	2.4	32 MB. The RDP memory requirements do not expand based on load. RDP never requires more than 32 MB of RAM.
DESS	1.9	N/A
CDAT	4.9	RAM requirements increase proportionally to the number of objects stored in the directory. For most directory sizes, the 64 MB requirements of the operating system (OS) and other system software should be sufficient for heavily populated directories.

Java Software Considerations

A JRE Version 1.2.2 is bundled in the installation image. The installation process installs this bundled version if it cannot find a suitable version on the installation platform.

This section describes the SESM requirements regarding the Java Runtime Environment (JRE) and the Java Development Kit (JDK). The section includes the following topics:

- Solaris Patch Requirements, page 3-3
- Installing the Bundled JRE, page 3-3
- Specifying an Existing JRE or JDK, page 3-3

- Specifying the JRE or JDK in the Startup Scripts, page 3-3
- Obtaining a JDK for SESM Web Development, page 3-4

Solaris Patch Requirements

On older Solaris platforms, you might need to apply Solaris operating system upgrades (patches). To determine if the machine requires patches, go to the Sun Microsystems Java site and start the process of dowloading the JRE Version 1.2.2. After you log in, you a list of download options appears, including the necessary patches for your operating system version. You should also download the README file, which contains instructions on how to apply the patches.

Installing the Bundled JRE

The installation program determines for itself whether or not to install the bundled JRE Version 1.2.2 by doing the following:

1. It searches for a JDK Version 1.2.2 that is already installed.
2. Failing that, it searches for a JRE Version 1.2.2 or later that is already installed.
3. Failing that, it installs and uses the bundled JRE Version 1.2.2.

To search for an existing JDK or JRE, the installation program looks in the following locations:

- On Windows NT, it looks in the NT Registry for a referenced location.
- On Solaris, it looks in well-known locations. See the "Searching for an Existing JDK or JRE" section on page 7-4 for a list of these locations.

Specifying an Existing JRE or JDK

On Windows NT and Solaris, you can explicitly specify the location of a pre-installed JDK or JRE 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 downloaded SESM image.

location is the path name for the JRE or JDK directory. For example, /usr/java1.2.

Specifying the JRE or JDK in the Startup Scripts

The installation process sets the location of the JDK or JRE in the startup files for NWSP, CDAT, and RDP.

If you change the location of the JDK or JRE after installation, make the corresponding change in the following two startup files:

- Generic startup script—This common script starts the NWSP application, CDAT, and any other customized SESM applications.
- RDP startup script

Table 3-2 shows the path names of the startup scripts that you need to change.

Table 3-2 Startup Script Names

Platform	Generic Startup Script	RDP Startup Script
Solaris	jetty/bin/start.sh	rdp/bin/runrdp.sh
Windows	jetty\bin\start.cmd	rdp\bin\runrdp.cmd

Obtaining a JDK for SESM Web Development

A Java Development Kit (JDK) Version 1.2.2 or later must be installed on any system that will be used by web developers to create or modify the Java Server Pages (JSPs) for a customized SESM application. You can obtain JDK Version 1.2.2 or later from the Sun Java web page:

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

On systems that will be used to customize an SESM application, we recommend that you install the JDK before you install SESM. In that way, the SESM installation program uses the JDK in the application startup scripts, rather than a JRE. The JDK is necessary for recompiling the changed JSPs. See the "Recompiling a Customized JSP" section on page 7-5 for more information.

If you install the JDK after installing SESM, then you must:

- Edit the SESM application start script to use the JDK.
- Ensure that the JDK_HOME environment variable points to the directory into which you installed the JDK.

SSG and RADIUS Considerations

The SESM installation program does not attempt to communicate with SSGs or RADIUS servers. Therefore, SSGs and RADIUS servers do not need to be configured and running for you to install SESM components.

However, you should be prepared to provide correct communication information about those network components during the installation. Otherwise, you must manually edit the configuration files at a later time for the SESM application to work correctly.

The installation program updates configuration files with information that you provide about communicating with SSGs and RADIUS servers. Table 3-5 on page 3-11 describes the configuration information that the installation program prompts you for.

LDAP Directory Configuration Requirements

If you are installing SESM in DESS mode, the installation program establishes communication with your LDAP directory, if possible.

Required Configurations

For communication to occur, perform the following LDAP installation and configuration tasks *before* you run the SESM installation program:

Step 1 Install the LDAP directory.

Step 2 Enable the **Allow Clear Text Passwords** attribute if your LDAP directory is the NDS eDirectory. An SESM deployment in DESS mode does not work on NDS without the cleartext password attribute enabled.

You can enable the cleartext password attribute in NDS by using the freely downloadable ConsoleOne application from Novell.

The clear text password attribute is a property of the LDAP Group object of a server. The LDAP Group object stores the configuration data for a defined LDAP group within the directory tree. The **Allow Clear Text Passwords** attribute allows transmission of bind requests that include passwords over nonencrypted connections. By default, only passwords exchanged over SSL connections are encrypted.

See the NDS documentation for more information about the cleartext password option.

Step 3 Create a container in the LDAP hierarchy for SESM data. The container consists of an LDAP organization and organizational unit. For more information about how SESM data is organized in the LDAP object hierarchy, see the *Cisco Distributed Administration Tool Guide*.

If you intend to load the sample data that comes with CDAT, you might want to name the container to match the contents of the sample data file. Alternatively, you can edit the sample data file before you load it to match the names you use. The sample data uses the following names:

- organization: `cisco`
- organizational unit: `sesm`

Step 4 Create the following administrator accounts. They can be the same accounts, but they do not have to be the same.

- A directory-wide administrator that has permission to extend the directory schema.
- An SESM administrator that has permission to add objects to the SESM container (the organization and organizational unit that you created to hold SESM data).

Advantages to a Running LDAP Directory During SESM Installation

The LDAP directory does not need to be configured and running on the network for you to complete the Cisco SESM installation. However, it is advantageous if the directory is configured and running. If the installation program can communicate with the LDAP directory using the communication parameters that you provide, it can perform the following required tasks:

- Extend the directory schema with DESS extensions. These extensions are the LDAP classes and attributes that will hold the SESM subscriber profiles, service profiles, and policy information.
- Install top-level RBAC objects that are required before administrators can log into CDAT to create additional RBAC objects.

If the installation program does not perform these tasks, you must do them at a later time before running an SESM web application or CDAT.

Dependencies among the SESM Components

You can install all SESM components together on the same machine (a typical installation), or you can install some components separately in a distributed manner (a custom installation). Table 3-3 describes components that must be installed together on the same machine.

Table 3-3 Component Dependencies in a Distributed Installation

SESM Mode	Component Dependencies
RADIUS mode	• NWSP requires a J2EE server (for example, jetty) on the same machine.
DESS mode	• NWSP requires a J2EE server (for example, jetty) and the DESS component on the same machine. • CDAT requires a J2EE server (for example, jetty) and the DESS component on the same machine. • RDP requires the DESS component on the same machine.

Obtaining the SESM Installation File and License Number

The installation images for SESM are available from the product CD-ROM or from the Cisco web site. It includes the following topics:

- Obtaining a License Number, page 3-6
- Downloading from the Cisco Web Site, page 3-7
- Uncompressing the Image, page 3-7

Obtaining a License Number

The SESM installation program installs evaluation and licensed versions of SESM:

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

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

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

Downloading from the Cisco Web Site

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

Step 1 Open a web browser and go to:

http://www.cisco.com

Step 2 Click the **Login** button. Provide 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.

Uncompressing the Image

Copy and uncompress the tar or zip file to a temporary directory. When you uncompress the file, the results are:

- The installation executable file—A .bin or .exe file, depending on the platform you are using.
- Files used for a silent mode installation—These are .iss and .properties files. See the "Installing Using Silent Mode" section on page 3-9 for information about silent mode.

Table 3-4 shows the names of the compressed and executable files.

Table 3-4 Installation Image File Names

Platform	Compressed File Name	Executable Installation File Name
Solaris	sesm_sol.tar	sesm_sol.bin
Windows NT	sesm_win.zip	sesm_win.exe

Performing SESM Installation

This section describes how to install SESM. It includes the following topics:

- Installation Privileges, page 3-8
- Installation Modes, page 3-8
- Installing Using GUI Mode, page 3-8
- Installing Using Console Mode, page 3-9
- Installing Using Silent Mode, page 3-9

Installation Privileges

You must log on as a privileged user to perform the installation. In addition, you must have write privileges to the directory in which you intend to load the solution components.

The installation program writes to parts of the file system or Windows registry that are only accessible to a privileged user. The outcome of the installation is unpredictable if you are not privileged.

Log on as a privileged user as follows:

- On Solaris—Run the installation program as root.
- On Windows NT—Run the installation program as a member of the Administrators group.

Installation Modes

You can install SESM using the following installation modes:

- GUI mode—An interactive installation method that communicates with you by displaying interactive windows. You use the mouse and the keyboard to provide input during the installation.

  To run the installation in GUI mode, execute the installation image. No special arguments are required.
- Console mode—A text-only, question and answer interactive installation method.

  To run the installation in console mode, use the `-console` argument on the command line when you execute the installation image.
- Silent mode—A text-only noninteractive method. This mode, also known as batch mode, is useful for multiple installs. Before you start the installation process, you prepare files that contain your installation and configuration information. The installation program obtains all input from the response file.

  To run the installation in silent mode, use the `-option` *fileName* argument on the command line when you execute the installation image.

The following sections provide more details about performing an installation in these modes.

Installing Using GUI Mode

GUI mode is the default installation mode. To run in this mode, execute the installation image. No options are required.

- On Solaris, change directories to the location of the installation image, and enter the image name. For example:

  ```
  solaris> sesm_sol.bin
  ```

- On Windows NT, double-click the installation image file name. Alternatively, open a command prompt window, change directories to the location of the image, and enter the image name. For example:

  ```
  C:\> sesm_win.exe
  ```

Installing Using Console Mode

To run in console mode, use the `-console` option on the command line.

- On Solaris, change directories to the location of the installation image, and enter the following command:

  ```
  solaris> sesm_sol.bin -console
  ```

- On Windows NT, open a command prompt window, change directories to the location of the image, and enter the following command:

  ```
  C:\> sesm_win.exe -console
  ```

Installing Using Silent Mode

To run in silent mode, you must first prepare the configuration information normally gathered during the installation process in two files:

- InstallShield properties file (.iss file)—This file defines values related to the installation process. It includes the name of the .properties file. This file is specified as an argument on the command line when you start the installation process.
- Java system properties file (.properties file)—This file defines values related to application configuration.

Examples of the .iss and .properties files are included in the installation download. You must modify both files to match your requirements before you start the installation.

To prepare for silent mode:

Step 1 Open the .properties and .iss files in any text editor.

Note Before you begin, you might need to obtain write access to the files.

Step 2 Edit the values for each parameter in the file. Table 3-5 on page 3-11 describes each parameter. Save and close the file.

Step 3 To turn on the installation logging feature for a silent mode installation, open the .iss file in any text editor. Remove the first pound sign (#) from the following line:

# -log # @all

Step 4 Save and close the file.

To run in silent mode, use the `-options` option on the command line, as follows:

```
imageName -options issFileName
```

Where:

imageName is the name of the downloaded installation image.

issFileName is the name of the install shield properties file you prepared.

For example:

- On Solaris, change directories to the location of the installation image, and enter the following command:

  ```
  solaris> sesm_sol.bin -options mysesm.iss
  ```

- On Windows NT, open a command prompt window, change directories to the location of the image, and enter the following command:

  ```
  C:\> sesm_win.exe -options mysesm.iss
  ```

Installation and Configuration Parameters

Table 3-5 describes the installation and configuration parameters that you enter during the installation process. You can use the Value column in the table to record your planned input values.

You can change the value of any configuration parameter later by editing configuration files, as described in Chapter 4. You cannot change the values of the general installation parameters identified in the first part of the table.

Table 3-5 SESM Installation and Configuration Parameters

Category	Input Summary	Explanation	Value
General installation parameters	Installation type and license number	Choose the type of installation: • RADIUS Evaluation—Choose this option to evaluate SESM in a RADIUS deployment. You do not need a license number and there is no expiration time associated with the evaluation. • DESS Evaluation—Choose this option to evaluate SESM in a DESS deployment. You do not need a license number and there is no expiration time associated with the evaluation. • Licensed—If you purchased an SESM license, choose this option and enter the license number provided by Cisco. **Note** Obtain your SESM license number from the License Certificate shipped with the CD-ROM or otherwise provided to you by your Cisco account representative. The installation program interprets the license number you enter and proceeds to install either RADIUS or DESS mode components, whichever matches the license you purchased. A RADIUS mode license will not allow you to install the DESS mode components. The licensenum.txt file in your root installation directory records your license number and the software version number you installed. This information is important when you access Cisco technical support for this product.	
	License agreement	Read the displayed license agreement to ensure that you agree with the terms of the license. You must accept the agreement to proceed with installation.	

	Installation directory	**Note** You must have write privileges to the installation directory.
		To specify the installation directory, you can do any of the following:
		• Accept the displayed default installation directory
		• Click **Browse** to find a location
		• Type the directory name in the box.
		The default installation directories are:
		• On Solaris:
		`/opt/cisco/sesm`
		• On Windows NT:
		`C:\Program Files\cisco\sesm`	

Table 3-5 SESM Installation and Configuration Parameters (continued)

Category	Input Summary	Explanation	Value
General installation parameters *(continued)*	Setup type	Select one of the following: • **Typical**—Installs and configures all components on the same workstation. If you are installing a RADIUS mode deployment, a typical installation includes the following components: – NWSP—Includes the SESM core model. – Jetty If you are installing a DESS mode deployment, a typical installation includes the following components: – NWSP—Includes the SESM core model. – Jetty – DESS – RDP – CDAT See the “Software Component Descriptions” section on page 1-18 for a description of what you are installing with each of these components. • **Custom**—Allows you to choose the components to install and configure from a checklist. Choose this option to: – Install the NWSP application without the Jetty server (because you want to use a different J2EE server) – Reinstall one of the components – Distribute the solution components among different workstations. See the “Dependencies among the SESM Components” section on page 3-6 for a list of components that must be installed on the same workstation. • **Demo**—Installs and configures the NWSP application in DEMO mode. Use this option to demonstrate the capabilities of SESM when other network components, such as SSG, are not available. The difference between a demo installation and a typical installation is the contents of the configuration files. In addition, a demo mode installation does not install the DESS component.	

Table 3-5 SESM Installation and Configuration Parameters (continued)

Category	Input Summary	Explanation	Value

Web server configuration	NWSP port number	Specify the port on which the NWSP application's web server will listen for HTTP requests from subscribers. The installation program updates the application startup script to use this value.
		The displayed default is port 8080.
		Tips Change this value to 80 if you plan to use captive portal mode.
		Tips Each web server running on the same machine must listen on its own unique port. If another web server or another instance of the NWSP application is listening on 8080, change this value.
		The application startup script uses the application port number to derive two other port numbers:
		• A secure socket listener (SSL) port is derived as follows:
		`application port - 80 + 443`
		When the application port is 8080, the SSL port is:
		`8080 - 80 + 443 = 8443`
		• A management console port is derived as follows:
		`application port + 100`
		When the application port is 8080, the management port is:
		`8080 + 100 = 8180`	

	Run captive portal	Choose this option to configure the captive portal application. **Note** If you do not choose this option, the installation program installs the captive portal application but does not configure it. The captive portal application runs on the same web server with the NWSP application. It captures the original URL that was requested by the subscriber and forwards it to the SESM web application along with the redirect. The SESM web application can then honor the subscriber's originally requested URL after authentication occurs.	

Table 3-5 SESM Installation and Configuration Parameters (continued)

Category	Input Summary	Explanation	Value
Note The following section applies only if you choose the captive portal option in the previous section.			
Captive portal configuration	Host	Enter the host name or IP address for the host of the captive portal application. This installation program installs the captive portal application on the same machine with the NWSP application.	
	Port	Enter 80, the port number on which the captive portal application's web server will listen. This installation program configures the captive portal application to run in the same J2EE container with the NWSP application. Therefore, the port number must match the port number used for the NWSP port.	

	URI	Enter the URI of the SESM web application's home page (that is, the page you want the subscriber to see first). The URI is appended to the NWSP host and port entered previously to create the URL to which the captive portal application redirects the subscriber's browser.
		For example, the URI for the NWSP application is:
		`/decorate/pages/home.jsp`
		The leading slash is required.
		Continuing the example, if the NWSP host name is myhost and the NWSP port is 80, the captive portal application would redirect an unauthenticated subscriber to the following URL:
		`myhost:80/decorate/pages/home.jsp`
		The URI indicates the directory structure of the NWSP application's files within the J2EE container's directory. The URI is location-independent. You can deploy your SESM web application on many host machines, and, although the host and port would change for each host machine, the URI would not change.	

Note If you are installing SESM in Demo mode, you are finished with the installation.			

Table 3-5 SESM Installation and Configuration Parameters (continued)

<table>
<tr><th>Category</th><th>Input Summary</th><th>Explanation</th><th>Value</th></tr>
<tr><td rowspan="3">SESM to SSG communication
<b>Tips</b> You can use a <b>show run</b> command on the SSG host to determine how SSG is configured.</td><td>SSG port number</td><td>Specify the port that SSG uses to listen for RADIUS requests from an SESM application. This value must match the value that was configured on the SSG host with the following command:
<code>ssg radius-helper <i>authenticationPort</i></code>
The default value is 1812.</td><td></td></tr>
<tr><td>SSG shared secret</td><td>Specify the shared secret used for communication between SSG and an SESM application. This value must match the value that was configured on the SSG host with the following command:
<code>ssg radius-helper key <i>secret</i></code>
The default value is <code>cisco</code>.</td><td></td></tr>
<tr><td>SSG port bundle size</td><td>Enter the number of bits that SSG uses for port bundling when the host key feature is enabled. This value must match the value that was configured on the SSG host with the following command:
<code>ssg port-map <i>length</i></code>
The value must be 0 or 4.
A value of 0 indicates that the SSG is not using the host key and port bundle mechanism.
<b>Note</b> The host key feature is introduced in Cisco IOS Release 12.2(2)B. If you are using an earlier release, use a value of 0 in this field.
The default value is 0.</td><td></td></tr>
<tr><td colspan="4">When the port bundle size is 0, you must map SSGs to client subnets. The following category of parameters lets you map one client subnet for one SSG. You must manually edit the configuration file to:
• Map additional non-host key SSGs,
• Add more client subnets to this SSG, or
• Override the global values you specified in the previous category.
See the “Associating SSGs and Subscriber Requests” section on page 4-27 for more information.</td></tr>
<tr><td rowspan="3">One non-host key SSG</td><td>SSG address</td><td>Enter the host name or IP address of the SSG host.</td><td></td></tr>
<tr><td>Client subnet</td><td>Enter one client subnet address handled by this SSG. For example, 177.52.0.0.</td><td></td></tr>
<tr><td>Subnet mask</td><td>Enter the mask that can be applied to subscriber IP addresses to derive their subnet. For example, 255.255.0.0.</td><td></td></tr>
<tr><td colspan="4"><b>Note</b> If you are installing SESM in DESS mode, skip the following two categories and continue with the “Directory server information” category.</td></tr>
</table>

Table 3-5 SESM Installation and Configuration Parameters (continued)

Category	Input Summary	Explanation	Value
SESM to RADIUS server communication	Primary AAA server IP	Enter the IP address or the host name of the primary RADIUS server.	
	Primary AAA server port	Enter the port number on the primary RADIUS server host that the RADIUS server listens on. The default is 1812.	
	Secondary AAA server IP	Enter the IP address or the host name of the secondary RADIUS server. If you are not using a secondary RADIUS server, enter the same value used for the primary server.	
	Secondary AAA server port	Enter the port number on the secondary RADIUS server host that the RADIUS server listens on. If you are not using a secondary RADIUS server, enter the same value used for the primary server.	
	Shared secret	Enter the shared secret used between the RADIUS server and SESM. If you are using a primary and a secondary server, the shared secret must be the same for both servers. The default value is `cisco`.	
Service Password	RADIUS service password	Enter the password that the SESM application uses to request service and group profiles from RADIUS. This password must match the value that was configured on the SSG host with the following command: `ssg service-password` *`password`* The service-password value must be the same on all of your SSGs. The default value is `servicecisco`.	
Note If you are installing SESM in RADIUS mode, you are finished with the installation.			
Directory server information	Directory address	Enter the IP address or the host name of the system where the directory server is running.	
	Directory port	Enter the port on which the directory server listens.	
	Directory admin user	Enter a user ID that has permissions to extend the directory schema. The default value is cn=admin, ou=sesm, o=cisco.	
	Directory admin password	Enter the password for the directory administrator.	
Note The installation program attempts to access the directory server, using the information you just provided. If access is unsuccessful, the installation program displays a window with the header “Warning—Please confirm these options.” You should verify the information you entered and also verify that the directory server is currently running. If the directory is not running, you can continue the installation of DESS components by clicking the **Ignore** button on the warning window. However, if you click **Ignore**, the installation program can not update the directory for SESM use. You must perform the updates at some later time before running SESM web applications or CDAT. See the “Extending the Directory Schema and Installing Initial RBAC Objects” section on page 4-40 for instructions.			

Table 3-5 SESM Installation and Configuration Parameters (continued)

Category	Input Summary	Explanation	Value
Directory container information	Directory container	Enter the organization and organizational unit that will hold the SESM service, subscriber, and policy information. Use the following format: ou=*orgUnit*,o=*org* For example, the installation program's default values are: ou=sesm,o=cisco The above defaults are the values used in the sample data file that comes with CDAT.	

	Directory user ID	Enter a user ID that has permissions to access and create objects in the organization and organizational unit named above. Use the following format:
		cn=*userID*,ou=*orgUnit*,o=*org*
		For example, the default values are:
		cn=admin,ou=sesm,o=cisco	

	Directory password	Enter the password associated with the directory user ID.	
Note The installation program attempts to access the container using the information you just provided. If it is unsuccessful, a warning message appears, as described in the previous note.			
CDAT	CDAT port number	Enter the port number on which the CDAT web server will listen. The default is 8081.	

Table 3-5 SESM Installation and Configuration Parameters (continued)

Category	Input Summary	Explanation	Value
RDP Configures RDP to SSG communication	IP address	Enter the IP address or host name of the RDP. ⚠ **Caution** This value must be a real IP address to which the NRP can route. You cannot use the values localhost or 127.0.0.1.	
	Port number	Enter the port on which the RDP will listen. The default is 1812.	
	Shared secret	Enter the shared secret to be used for communication between SSG and RDP. It must be a different value from the shared secret used for RDP to RADIUS communication. The default is `cisco`.	
	Service password	Enter the password that RDP uses to request service profiles from the directory. This password must match the value that was configured on the SSG host with the following command: `ssg service-password` *`password`* The service-password value must be the same on all of your SSGs. The default value is `servicecisco`.	
	Next hop password	Enter the password that SSG uses to request next hop tables from RDP. This password must match the value that was configured on the SSG host with the following command: `ssg next-hop download` *`nextHopTableName password`* The service-password value must be the same on all of your SSGs. The default is `nexthopcisco`.	
	Proxy mode	Choose this option to run RDP in proxy mode. RDP has two modes: • Proxy mode—In this mode, RDP forwards authentication requests to a RADIUS server. RDP uses the DESS API to send authorization requests to the directory. • Non-proxy mode—In this mode, RDP performs authentication based on information it obtains from the directory. RDP uses the DESS API to send authorization requests to the directory.	

Table 3-5 SESM Installation and Configuration Parameters (continued)

Category	Input Summary	Explanation	Value
RDP *(continued)*	Add services	Choose this option if you want SSG to perform automatic connections to services when a subscriber's profile includes the autoconnect attribute. When you choose this option, RDP includes the subscriber's service list and related information in replies to SSG. This service information consumes memory on the SSG host—the node route processor (NRP). Do not choose this option if space is a consideration on the NRPs. Instead, you can configure the SESM application to initiate automatic connections. See the "autoConnect" section on page 4-22 for more information.	
If you choose Proxy mode for RDP, then the installation process prompts you for the following RADIUS server information.			
RDP to RADIUS communication	Primary AAA server IP	Enter the IP address or the host name of the primary RADIUS AAA server that you want RDP to communicate with.	
	Primary AAA server port	Enter the port number on the primary RADIUS server host that the RADIUS server listens on.	
	Secondary AAA server IP	Enter the IP address or the host name of the secondary RADIUS server. If you are not using a secondary RADIUS server, enter the same value used for the primary server.	
	Secondary AAA server port	Enter the port number on the secondary RADIUS server host that the RADIUS server listens on. If you are not using a secondary RADIUS server, enter the same value used for the primary server.	
	Shared secret	Enter the shared secret used between RDP and the RADIUS server. The shared secret must be the same for both servers. The default is `cisco`.	

Table 3-5 SESM Installation and Configuration Parameters (continued)

Category	Input Summary	Explanation	Value
The installation program installs the components on your system. When it is finished installing the files, it displays an additional window about modifications to the LDAP directory.			
LDAP directory modifications	Extend schema	Choose this option if you want the installation program to apply the DESS schema extensions to the LDAP directory. These extensions include the dess and auth classes and attributes. For more information about the extensions, see the *Cisco Distributed Administration Tool Guide*. If you do not choose this option, you must extend the directory schema later, before running the SESM application in DESS mode and before logging into CDAT to create objects in the directory. See "Extending the Directory Schema and Installing Initial RBAC Objects" section on page 4-40 for more information. **Note** If you are installing DESS in multiple locations, you only need to extend the schema one time.	
	Install RBAC	Choose this option if you want the installation program to load the top-level RBAC objects. If you do not choose this option, you must install RBAC objects later, before running an SESM application in DESS mode and before logging into CDAT to create objects in the directory. See "Extending the Directory Schema and Installing Initial RBAC Objects" section on page 4-40 for more information. **Note** If you are installing DESS in multiple locations, you only need to extend the schema one time.	

Installation Results

The Cisco SESM installation directory contains the following subdirectories and files:

- _uninst—This subdirectory contains the utility to uninstall the components you just installed. To uninstall, run the executable file in this directory.
- captiveportal—This directory contains the captive portal web application to execute on the Jetty server.
- jetty—This directory contains the following subdirectories:
  - bin—Contains start scripts for Jetty server applications
  - config—Contains configuration files that control Jetty servlets
  - lib—Contains the Jetty server class libraries.
- lib—This directory contains the SESM libraries and the docs subdirectory, which contains the Java application documentation.
- licensenum.txt—This file contains the license number that you used during installation and the version number of the SESM software that you installed.

- nwsp—This directory contains the following subdirectories:
  - config—Contains configuration files for the NWSP application.
  - docroot—Contains the Web application, including libraries, JSPs, images, and a J2EE configuration file.
- redist—This directory contains libraries from other companies that Cisco is redistributing. It includes the Jasper JSP framework, the JMX framework, and the JAXP XML parser framework. It also includes test tools.

When you install SESM in DESS mode, the installation directory contains the following additional directories:

- rdp—This directory contains startup scripts, configuration files, and libraries for the RADIUS/DESS Proxy Server.
- cdat—This directory contains configuration files and libraries for CDAT.
- dess-auth—This directory contains the DESS and AUTH libraries, DESS schema, and sample data.

Post-Installation Procedures

This section outlines the steps to take after you successfully complete an installation.

Step 1 Perform all configuration activities listed in Table 1-3 on page 1-15 (RADIUS mode) or Table 1-5 on page 1-18 (DESS mode).

Step 2 Add configuration information for additional SSGs, if the host key feature is not used.

The SESM installation program caters to use of a single SSG or multiple SSGs with the host key feature. For multiple SSG support without the host key feature, you must configure the SSG to client subnet mapping. See the "Associating SSGs and Subscriber Requests" section on page 4-27 for instructions.

Step 3 Start the NWSP web application with the startNWSP script in the jetty bin directory. See Chapter 5, "Running SESM Components" for information about this script.

Step 4 Start a web browser. See the "Supported Browsers" section on page 6-1. Access the NWSP application as described in the "Accessing the NWSP Application" section on page 6-1.

See the "Customizing the NWSP Application" section on page 6-2 for information about customizing the NWSP application.