



Installing SESM

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

- [Obtaining the SESM Installation File and License Number, page 2-1](#)
- [Required Installation Privileges, page 2-3](#)
- [Installation Methods, page 2-3](#)
- [Turning On the Installation Logging Feature, page 2-5](#)
- [Installation Parameter Descriptions, page 2-5](#)
- [Installation Results, page 2-20](#)
- [Post-Installation Configuration Tasks, page 2-21](#)

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. This section includes the following topics:

- [Obtaining a License Number, page 2-1](#)
- [Downloading Software from the Cisco Web Site, page 2-2](#)
- [Uncompressing the Image, page 2-2](#)

Obtaining a License Number

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

- **Evaluation**—The evaluation options do not require a license number and do not have an expiration period. An evaluation installation provides full software functionality. You can install a RADIUS mode evaluation or an LDAP mode evaluation.
- **Licensed**— You must install a licensed version using 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 Software 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** Click **Technical Support**.
- Step 4** In the popup menu, click **Software Center**.
- Step 5** Click **Web Software**.
- Step 6** Click **Cisco Subscriber Edge Services Manager**.
- Step 7** Download the appropriate image based on the platform you intend to use for hosting the SESM web application.
-

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 2-4 for information about silent mode.

[Table 2-1](#) shows the names of the compressed and executable files.

Table 2-1 Installation Image Filenames

Platform	Compressed Filename	Executable Installation Filename
Solaris	<code>sesm-3.1.x-pkg-sol.tar</code>	<code>sesm_sol.bin</code>
Linux	<code>sesm-3.1.x-pkg-linux.tar</code>	<code>sesm_linux.bin</code>
Windows NT	<code>sesm-3.1.x-pkg-win32.zip</code>	<code>sesm_win.exe</code>

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

Installation Methods

You can install SESM using the following installation modes:

- **Installing Using 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.

- **Installing Using 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.

- **Installing Using 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 installations in these modes.

Installing Using GUI Mode

GUI mode is the default installation mode. To run in this mode, execute the installation image. No command line 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 filename. 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. Before you start the installation, you must modify both files to match your requirements.

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 2-2 on page 2-6](#) 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
```

Turning On the Installation Logging Feature

The `-log` option on the installation command line turns on the installation logging feature.

- On Solaris:

```
solaris> sesm_sol.bin -log location @ALL
```

Where:

location can be # to send logging messages to the console or a filename

@ALL indicates to log all messages, which is the recommended procedure

- On Windows NT:

```
C:\> sesm_win.exe -options -log location @ALL
```

Where:

location can be # to send logging messages to the console or a filename

@ALL indicates to log all messages, which is the recommended procedure.

Installation Parameter Descriptions

[Table 2-2](#) 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 2-2 *SESM Installation and Configuration Parameters*

Category	Field	Explanation
General installation parameters	Installation type and license number	<p>Choose the type of installation:</p> <ul style="list-style-type: none"> • RADIUS Evaluation—Choose this option to evaluate SESM in a RADIUS deployment. You do not need a license number, there is no expiration time associated with the evaluation, and the functionality is the same as that of licensed mode. • LDAP Evaluation—Choose this option to evaluate SESM in an LDAP deployment. You do not need a license number, there is no expiration time associated with the evaluation, and the functionality is the same as that of licensed mode. • Licensed—If you purchased an SESM license, choose this option and enter the license number provided by Cisco. <p>The installation program interprets the license number you enter and proceeds to install either RADIUS or LDAP mode components, whichever matches the license you purchased. A RADIUS mode license will not allow you to install the LDAP-specific components, such as CDAT and RDP.</p> <p>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. If you have not yet received a Certificate, choose one of the Evaluation modes.</p> <p>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.</p>
	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	<p>Note You must have write privileges to the installation directory.</p> <p>To specify the installation directory, you can either: accept the displayed default installation directory, click Browse to find a location, or type the directory name in the box.</p> <p>The default installation directories are:</p> <ul style="list-style-type: none"> • On Solaris and Linux: /opt/cisco/sesm_3.1.x • On Windows NT: C:\Program Files\cisco\sesm_3.1.x

Table 2-2 SESM Installation and Configuration Parameters (continued)

Category	Field	Explanation
General installation parameters (continued)	Setup type	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Typical—Installs all of the following components in the same directory on the same machine: <ul style="list-style-type: none"> – Web Applications—Includes the NWSP, WAP, and PDA sample applications and the SESM core model. – Jetty—Includes the Jetty web server, the JMX server, and JNDI. – RDP—Installed only when installation type is LDAP evaluation or LDAP license. – CDAT—If the installation type is RADIUS evaluation or RADIUS license, CDAT includes only the remote management interface. If the installation type is LDAP evaluation or LDAP license, CDAT includes both the remote management and the LDAP directory management interfaces. – SPE—Installed only when installation type is LDAP evaluation or LDAP license. – Bundled SESM RADIUS Server and Proxy RADIUS Server—Installed in the tools directory for all installation types • Custom—Allows you to choose the components to install and configure from a checklist. Choose this option to: <ul style="list-style-type: none"> – Include the SESM captive portal solution in your installation. The captive portal solution supports several types of redirection capabilities for subscriber access management solutions. – Include the SESM web services gateway (WSG) application software in your installation. WSG provides a SOAP-based interface enabling third-party web portals and subscriber management systems to integrate with the SESM and SSG solution. – Reinstall one of the components. – Distribute the SESM components among different workstations. • Demo—Installs and configures the NWSP, WAP, and PDA applications to run in Demo mode. The configuration files are not set up to communicate with an SSG, a RADIUS server, or an LDAP directory. Choose this option when those components are not available. <p>Note If you install SESM in Demo mode and later want to run the portals in RADIUS or LDAP mode, we recommend that you perform another SESM installation in RADIUS or LDAP mode. Otherwise, you must make extensive adjustments to configuration attributes in the MBeans.</p> <p>Demo mode simulates the actions of an SESM deployment in both RADIUS and LDAP modes. It uses a local copy of a Merit RADIUS file to obtain profile information. See the <i>Subscriber Edge Services Manager Solution Guide</i> for more information about installing and using SESM in Demo mode.</p> <p>The difference between a demo installation and a typical installation is the contents of the configuration files. In addition, a demo installation does not install the SPE component.</p>

Table 2-2 SESM Installation and Configuration Parameters (continued)

Category	Field	Explanation
Configuration and Deployment	Web Application Host	<p>Specify the IP address or host name of the host on which the SESM portal applications will run. For Demo mode, you can use the value localhost.</p> <p> Caution For LDAP and RADIUS modes, this value must be a real IP address. You cannot use the values localhost or 127.0.0.1.</p>
	Web Application Port Number	<p>Specify the port on which the container (the J2EE web server) for the SESM portal applications will listen for HTTP requests from subscribers. The installation program updates the application startup scripts for NWSP, WAP, and PDA to use this value. If you want to run these applications simultaneously, you must edit the start scripts to ensure that each application uses a different port.</p> <p>The displayed default value is port 8080.</p> <p>Tip Each web server running on the same machine must listen on its own unique port. If another web server or another instance of the SESM portal application is listening on 8080, change this value.</p> <p>The application startup script uses the application port number to derive two other port numbers:</p> <ul style="list-style-type: none"> A secure socket listener (SSL) port is derived as follows: $\text{application port} - 80 + 443$ <p>When the application port is 8080, the SSL port is:</p> $8080 - 80 + 443 = 8443$ A management console port is derived as follows: $\text{application port} + 100$ <p>When the application port is 8080, the management port is:</p> $8080 + 100 = 8180$
	SSG Deployment Option	<p>Check this option if you are deploying SESM for a solution that uses the SSG. When you choose this option, the installation program configures the SESM components to work with one or more SSGs.</p> <p>Uncheck this option if you are deploying SESM for a self care solution that does not require an SSG component. In this case, the installation program does not prompt for any SSG information. The self care solutions require LDAP evaluation or LDAP license installations.</p>

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

Table 2-2 SESM Installation and Configuration Parameters (continued)

Category	Field	Explanation
SSG details Tip Use the show run command on the SSG host device to determine how SSG is configured.	SSG port number	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 authenticationPort</code> Default: 1812.
	SSG shared secret	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 secret</code> Default: <code>cisco</code> .
	SSG port bundle size	Enter the number of bits that SSG uses for port bundling when the port-bundle 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 length</code> We recommend using the value 4. A value of 0 indicates that the SSG is not using the port-bundle host key mechanism. Note The port-bundle host key feature was introduced in Cisco IOS Release 12.2(2)B. If you are using an earlier release, use a value of 0 in this field. Default: 0.

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 with Subscriber Requests” section on page 5-16](#) for more information.

One non-host key SSG	SSG address	Enter the host name or IP address of the SSG host.
	Client subnet	Enter one client subnet address handled by this SSG. For example, 177.52.0.0.
	Subnet mask	Enter the mask that can be applied to subscriber IP addresses to derive their subnet. For example, 255.255.0.0.

Table 2-2 SESM Installation and Configuration Parameters (continued)

Category	Field	Explanation
Note If you are installing SESM in LDAP mode, skip the following two categories and continue with the “Directory server information” category later in this table.		
RADIUS server details	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. Default: <code>cisco</code> .
Passwords	Service password	Enter the password that the SESM application uses to request service profiles from RADIUS. It must match the service password values used in the service profiles in the RADIUS database. This password must also match the value that was configured on the SSG host with the following command: <code>ssg service-password password</code> The service-password value must be the same on all of your SSGs. Default: <code>servicecisco</code> .
	Service group password	Enter the password that the SESM application uses to request service group profiles from RADIUS. It must match the service group password values used in the service group profiles in the RADIUS database. Default: <code>groupcisco</code> .
Note If you are installing SESM in RADIUS mode, you are finished with the installation of the standard components. If you are selected to install the captive portal solution from the custom installation window, go to the Captive Portal category later in this table.		

Table 2-2 *SESM Installation and Configuration Parameters (continued)*

Category	Field	Explanation
Directory server information	Directory address	Enter the IP address or the host name of the system on which the directory server is running.
	Directory port	Enter the port on which the directory server listens.
	Directory admin user	<p>Enter a user ID that has permissions to extend the directory schema. Use cn or uid as appropriate. For example:</p> <ul style="list-style-type: none"> For NDS, enter: cn=admin, ou=sesm, o=cisco For Sun ONE (or iPlanet), enter: cn=Directory Manager <p>Note The default configuration by the Sun ONE installation process uses cn for the Directory Manager. See the “Sun ONE and iPlanet Installation and Configuration Requirements” section on page B-4 for more information.</p>
	Directory admin password	<p>Enter the password for the directory administrator. This is the password you entered during directory installation and configuration. For example:</p> <ul style="list-style-type: none"> For NDS, enter the password you specified for the admin user during installation. For Sun ONE, enter the password you entered for the Directory Manager user during Sun ONE installation.

Note The installation program attempts to access the directory server, using the information you provided. If access is unsuccessful, the installation program displays a window with the header “Warning—Please confirm these options.” Verify the information you entered and also verify that the directory server is running. If the directory is not running, you can continue the installation of SPE 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 a later time before you run SESM web applications or CDAT. See the [“Extending the Directory Schema and Loading Initial RBAC Objects”](#) section on page 8-3 for instructions.

Table 2-2 SESM Installation and Configuration Parameters (continued)

Category	Field	Explanation
Directory container information	Directory container	<p>Enter the organization and organizational unit that will hold the SESM service, subscriber, and policy information. Use the following format:</p> <pre>ou=orgUnit,o=org</pre> <p>For example, the installation program's default values are:</p> <pre>ou=sesm,o=cisco</pre> <p>The above defaults are the values used in the sample data file that comes with CDAT.</p>
	Directory user ID	<p>Enter a user ID that has permissions to access and create objects in the organization and organizational unit named above. Use cn or uid as appropriate. For example:</p> <ul style="list-style-type: none"> For NDS, the container administrator is the same as the directory administrator you entered on the previous window: <pre>cn=admin,ou=sesm,o=cisco</pre> <ul style="list-style-type: none"> For Sun ONE (or iPlanet), the container administrator is not the same as the directory administrator. You created this container administrator after Sun ONE installation. <pre>uid=yourAdmin,ou=sesm,o=cisco</pre>
	Directory password	Enter the password associated with the directory user ID.
Naming attribute	inetorgPerson	<p>Choose the component in distinguished name (dn) that allows access to the SESM container.</p> <ul style="list-style-type: none"> common name (cn)—NDS, for example, uses cn. unique identifier (uid)—Sun ONE, for example, uses uid for the SESM container. See the “Sun ONE and iPlanet Installation and Configuration Requirements” section on page B-4 for more information. <p>Note The SESM sample data uses cn. If you choose uid, you must edit the sample data before loading it into a Sun ONE or other directory that uses uid. See the “Loading Sample Data” section on page 8-4.</p>

Note The installation program attempts to access the container using the information you provided. If it is unsuccessful, a warning message appears, as described in the previous note.

Table 2-2 SESM Installation and Configuration Parameters (continued)


Category	Field	Explanation
RDP Configures RDP to SSG communication	RDP host	Enter the IP address or host name on which the RDP will run.  Caution Use a routable IP address. Do not use the values localhost or 127.0.0.1.
	Port number	Enter the port on which the RDP will listen. Default: 1812.
	Shared secret	Enter the shared secret to be used for communication between the SSGs and RDP when the restricted client feature is turned off. This value must match the value configured on the SSG host devices, using the following command: <code>radius-server key SharedSecret</code> When the restricted client feature is turned off, the shared secret must be the same on all SSGs. When the restricted client feature is turned on, this attribute is ignored. Instead, you configure a specific shared secret for each client (each SSG). See the “ RDP MBean ” section on page 7-4 for more information. The next set of prompts from the installation program lets you choose whether to turn the restricted client feature on or off. Default: <code>cisco</code> .
	Service password	Enter the password that RDP uses to request service profiles from the directory. This value must match two other configured values: 1. This password must match the value that was configured on the SSG host with the following command: <code>ssg service-password password</code> The service-password value must be the same on all the SSGs that communicate with this RDP server. 2. This value must also match the service password value you entered for the SESM portal. See the SESM “ Passwords ” section on page 2-10. Default: <code>servicecisco</code> .
	Group password	Enter the password that RDP uses to request service group profiles from the directory. This password must match the group password value you entered for the SESM portal. See the SESM “ Passwords ” section on page 2-10. Default: <code>groupcisco</code> .
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: <code>ssg next-hop download nextHopTableName password</code> The service-password value must be the same on all of the SSGs that communicate with this RDP server. Default: <code>nexthopcisco</code> .	

Table 2-2 SESM Installation and Configuration Parameters (continued)

Category	Field	Explanation
RDP Options	Proxy mode	<p>Choose this option to run RDP in proxy mode. RDP has two modes:</p> <ul style="list-style-type: none"> Proxy mode—In this mode, RDP forwards authentication requests to a RADIUS server. RDP uses the SPE API to send authorization requests to the directory. Default (non-proxy) mode—In this mode, RDP performs authentication based on information it obtains from the directory. RDP uses the SPE API to send authorization requests to the LDAP directory.
	Add services	<p>Choose this option if you want the 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. The service information consumes memory on the SSG device.</p> <p>Do not choose this option if space is a consideration on the SSG device. Instead, you can configure the SESM application to initiate automatic connections with the autoConnect attribute in the SESM MBean. See the "SESM MBean" section on page 5-4 for more information.</p>
	Add client	<p>Choose this option if you want to turn on the RDP restricted client feature, which allows RDP to service requests only from a preconfigured list of clients. The RDP clients are SSGs.</p> <p>If you check this option, the installation program prompts for configuration information for one client. You can add more clients by adding elements to the allowedClients attribute in the RADIUSServerSocket MBean.</p> <p>If you do not check this option, the RDP accepts requests from any client (any SSG).</p>

If you choose the RDP Proxy mode option, the installation process prompts you for the following RADIUS server information.

AAA Server Details	Primary IP	Enter the IP address or the host name of the primary AAA server that you want RDP to communicate with.
	Primary port	Enter the port number on the primary RADIUS server host that the RADIUS server listens on.
	Secondary 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 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	<p>Enter the shared secret used between RDP and the RADIUS server. The shared secret must be the same for both servers.</p> <p>Default: <code>cisco</code>.</p>

Table 2-2 SESM Installation and Configuration Parameters (continued)

Category	Field	Explanation
<p>If you choose the RDP Add client option, the installation program prompts you for the following information about one RDP client. You can add more clients by adding elements to the allowedClients attribute in the RDPMBean, RADIUSServerSocket component. See the “RDP MBean” section on page 7-4 for more information.</p>		
RDP Client	Client IP address	Enter the IP address of the SSG.
	Shared Secret	<p>Enter the shared secret used for SSG to RDP communication. This value must match the value configured on the SSG, using the following command:</p> <pre>radius-server key SharedSecret</pre>
<p>If you are performing a Custom installation and you check the Captive Portal item, the installation program prompts you for captive portal configuration information.</p>		
<p>Note The configuration information you enter in the following parameters must match TCP redirect configuration values on the SSG. The easiest way to ensure that values match in both places is to accept all of the default values presented by the installation process. Then configure the SSG based on the example captiveportal/config/ssgconfig.txt file. See Chapter 11, “Deploying a Captive Portal Solution,” for more information.</p>		
Captive Portal Server Configuration	Captive portal host	Enter the IP address or host name on which the captive portal solution will run.
	Captive portal port number	<p>Enter the port number on which the first listener in the captive portal web server will listen.</p> <p>This installation program sets up the captiveportal.jetty.xml file to create seven listeners in the web server, as follows:</p> <ul style="list-style-type: none"> Subscriber redirection listener Initial logon redirection listener Advertising redirection listener Default service redirection listener Three service redirection listeners <p>Later in this installation procedure, you are prompted for a port number for each of these listeners. The port you enter now is used as the default value for the first listener.</p> <p>Note If you use the same port number for more than one listener, some redirections will not work.</p> <p>Default: 8090</p>
	Install Message Portal	<p>Choose this option if you want to install the Message Portal application. The Message Portal application is an example of an SESM portal that provides content for:</p> <ul style="list-style-type: none"> Initial logon redirections Advertising redirections <p>For those redirection types, the default URIs displayed later in this installation procedure refer to pages in the Message Portal application.</p>

Table 2-2 *SESM Installation and Configuration Parameters (continued)*

Category	Field	Explanation
If you choose the Message Portal option above, the installation program prompts you for the following information.		
Message Portal Server Configuration	Message Portal Port Number	Enter the port number on which the Message Portal web server will listen. The Message Portal web server has one listener. Default: 8085
	Redirect after message page	Choose this option if you want the Message Portal application to redirect the subscriber to the originally requested URL after the message duration time elapses. If you do not choose this option, the subscriber must enter an URL to leave the message page. Default: true
Main web server configuration	Host	Enter the host name or IP address of the web server for the NWSP or other application that will respond to: <ul style="list-style-type: none"> Unauthenticated user redirection Default unconnected service redirection Specific unconnected service redirections Error handling due to captive portal misconfiguration (if a port has been used which is not configured for redirection). This value becomes the default value for the serviceportal.host system property in the captiveportal.xml file.
	Port	Enter the port number on which the web server named above will listen. This value becomes the default value for the serviceportal.port system property in the captiveportal.xml file. Default: 8080
Unauthenticated User Redirection	Enable	Check this box to configure unauthenticated user redirections.
	Port In	Enter the port that the web server for the Captive Portal application will listen on for unauthenticated user redirections received from the SSG. The installation program displays the value that you entered earlier in the Captive Portal Port Number field. You can accept this default value. Note You must configure the SSG TCP redirect feature to send unauthenticated user redirections to this port. Default: 8090
	URL Out: Host URL Out: Port URL Out: URI	These fields define the URL to which browsers are redirected for unauthenticated user redirections. The default values reference the NWSP application. <ul style="list-style-type: none"> Host—Enter the name or IP address for the web server that contains the content application for unauthenticated user redirections. Port—Enter the listener port number for this content application. The default is the port number you entered for the NWSP application. URI—The absolute page name you want the subscriber to see. The default is /home, which is the NWSP logon page.


Table 2-2 SESM Installation and Configuration Parameters (continued)

Category	Field	Explanation
Initial Captivation	Enable	Check this box to configure initial logon redirections.
	Port In	Enter the port that the Captive Portal web server will listen on for initial logon redirections. Note You must configure the SSG TCP redirect feature to send initial logon redirections to this port. Default: 8091
	URL Out: Host URL Out: Port URL Out: URI	These fields define the URL to which browsers are redirected for initial logon redirections. The default values reference the Message Portal application. <ul style="list-style-type: none"> • Host—Enter the name or IP address for the web server that contains the content application for initial logon redirections. • Port—Enter the listener port number for this content application. The default is the port number you entered for the Message Portal application. • URI—The absolute page name you want the subscriber to see. The default is /initial, which is the Message Portal greeting page.
	Duration	The length of time that the Message Portal application waits before attempting to redirect the browser to the user's originally requested URL. Default: 15
Advertising Captivation	Enable	Check this box to configure advertising redirections.
	Port In	Enter the port that the Captive Portal web server will listen on for advertising redirections. Note You must configure the SSG TCP feature to send advertising redirections to this port. Default: 8092
	URL Out: Host URL Out: Port URL Out: URI	These fields define the URL to which browsers are redirected for advertising redirections. The default values reference the Message Portal application. <ul style="list-style-type: none"> • Host—Enter the name or IP address for the web server that contains the content application for advertising redirections. • Port—Enter the listener port number for this content application. The default is the port number you entered for the Message Portal application. • URI—The absolute page name you want the subscriber to see. The default is /advertising, which is the Message Portal advertising page.
	Duration	The length of time that the Message Portal application waits before attempting to redirect the browser to the user's originally requested URL. Default: 15

Table 2-2 SESM Installation and Configuration Parameters (continued)

Category	Field	Explanation
Unconnected Service Redirection	Enable	Check this box to configure service redirections, including a default service redirection.
	Default Service Redirect Port In	Enter the port that the Captive Portal web server will listen on for default service redirections. Default service redirections are used for services whose address does not belong to the destination network of any of the specific service redirections. Note You must configure the SSG TCP feature to send default service redirections to this port. Default: 8093
	First Service Redirect Port In	Enter the ports that the Captive Portal web server will listen on for service redirections for Service1, Service2, and Service3.
	Second Service Redirect Port In Third Service Redirect Port In	Note You must configure the SSG TCP feature to send redirections to these ports. Defaults: 8094, 8095, 8096
	URL Out	Enter the URL to which browsers are redirected for any type of service redirection. The default value references the NWSP application, as follows: <ul style="list-style-type: none"> The host and port values are the ones you entered earlier for the service application. The page name is /serviceRedirect, which is a generalized NWSP page. Configuration parameters in nwsp.xml define more specific pages. This installation program assumes that the same URL is used for all service redirections. You can change this default configuration in the captiveportal.xml file. There is no requirement that all service redirections use the same page, port, or application.
Details for Unconnected Service Redirection	Pass Service Names	Choose this option if you want the Captive Portal application to pass the service names to the content application that handles service redirections (NWSP in the default configuration). NWSP uses the service name to connect to the service. If you do not check this option, NWSP displays the page specified in the serviceNotGivenURI attribute in nwsp.xml. (The default installation setting for the serviceNotGivenURI attribute is the NWSP status page.)
	Redirect Service Names	Provide the service name as specified in the service profile. The default values provided in the installation program match services in the sample data installed with SESM.

Table 2-2 SESM Installation and Configuration Parameters (continued)

Category	Field	Explanation
CDAT	CDAT host	Enter the IP address or host name on which the CDAT application will run.  Caution Use a routable IP address. Do not use the values localhost or 127.0.0.1.
	CDAT port number	Enter the port number on which the CDAT web server will listen. The default is 8081.
Links for CDAT main window	Hosts and port numbers for remote SESM applications	The installation program prompts for host names and port numbers of all applications that you did not install during the current session. It uses this information to configure links on the CDAT main window pointing to the management consoles of these remote SESM applications. To skip the prompts for applications that you have not installed on any system or do not want CDAT to manage, click Next . For applications that you installed during the current session, the installation program already has the link information.
The installation program installs the components on your system. When it is finished installing the files, and if it successfully connected to your LDAP directory, it displays the following additional prompts about modifications to the directory.		
LDAP directory modifications	Extend schema	Choose this option if you are installing SESM to run with a new LDAP directory and you want the installation program to apply the SPE schema extensions to the directory. The extensions include the <code>des</code> and <code>auth</code> classes and attributes. For more information about the extensions, see the <i>Cisco Distributed Administration Tool Guide</i> . If you do not choose this option, you must extend the directory schema later, before running the SESM application in LDAP mode and before logging into CDAT to create objects in the directory. See the “Post-Installation Configuration Tasks” section on page 2-21. Note The schema must be extended for each LDAP directory used in the SESM deployment. If multiple instances of SESM using just one LDAP directory exist, then the schema need only be extended in one of the installs where the SPE component is selected.
	Install RBAC	Choose this option if you want the installation program to load the top-level RBAC objects. Some initial top-level rules and roles must be created in the directory before an administrator can log into CDAT and create additional objects. If you do not choose this option, you must install RBAC objects later, before running the SESM application in LDAP mode and before logging into CDAT to create objects in the directory. See the “Post-Installation Configuration Tasks” section on page 2-21. Note The RBAC objects must be installed into each LDAP directory used in the SESM deployment. If multiple instances of SESM using just one LDAP directory exist, then the RBAC objects must only be loaded in one of the installs where the SPE component is selected.

Installation Results

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

- `_jvm`—(Optional) This directory contains the JRE that is shipped with SESM. If your SESM installation directory does not include `_jvm`, it means that the installation program located a suitable JSDK or JRE elsewhere on your system. See the [“Installing the Bundled JRE” section on page 1-3](#).
- `_uninst`—This directory contains the utility to uninstall the components you just installed. To uninstall components, run the executable file in this directory.
- `captiveportal`—This directory exists only if you installed the Captive Portal solution using a Custom installation.
- `cdat`—This directory contains configuration files and libraries for CDAT.
- `dess-auth (LDAP-mode only)`—This directory contains the SPE DESS and AUTH libraries, SPE DESS schema, and sample data. The schema subdirectory contains the `README.SESM.LDIF.html` file, which explains how to manually update the LDAP directory with the SPE schema, load initial RBAC objects, and load sample data.
- `docs`—This directory contains the `apidoc` directory, which holds the Java documentation for the SESM application programmer interface (API).
- `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 class libraries.
- `messageportal`—This directory exists only if you installed the Captive Portal solution using a Custom installation, and chose the Install Message Portal option during the installation.
- `nwsp`, `pda`, and `wap`—These directories contain the following subdirectories:
 - `config`—Contains a configuration file for the portal application and a demo data file.
 - `docs`—Contains the application javadoc files.
 - `webapp`—Contains the Web application, including libraries, JSPs, images, and the `WEB-INF` directory, which includes J2EE configuration files, such as `web.xml` and `web-jetty.xml`.
- `rdp`—This directory contains startup scripts, configuration files, and libraries for the RDP server.
- `redist`—This directory contains libraries from third-party 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.
- `tools`—This directory contains scripts that developers can use to precompile customized SESM JSPs, configure and start the bundled RADIUS server, and configure and start a proxy RADIUS server.
- `licensenum.txt`—This file contains the license number that you used during installation and the version number of the SESM software that you installed.

Post-Installation Configuration Tasks

This section lists some configuration tasks that might be required after you install SESM applications.

-
- Step 1** Install and configure other software components required for your SESM solution, such as RADIUS servers, LDAP directory, and SSGs.
 - Step 2** (LDAP mode only) Update the LDAP directory with SPE schema extensions and load initial RBAC objects if you did not allow the installation program to do these tasks. See the [“Extending the Directory Schema and Loading Initial RBAC Objects”](#) section on page 8-3.
 - Step 3** (LDAP mode only) Optionally load sample data into the LDAP directory. See [“Loading Sample Data”](#) section on page 8-4.
 - Step 4** Add configuration information for additional SSGs, if the SSG port bundle host key feature is not used on the SSGs.

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 with Subscriber Requests”](#) section on page 5-16.
 - Step 5** If you installed the captive portal solution, see the [“Additional Configuration Steps”](#) section on page 11-7 for instructions on configuring an SSG to work with the installed captive portal features.
 - Step 6** If you installed the RDP server and turned on the restricted client feature, you might need to add more SSGs to the RDP’s client list. The installation program accepts information for one client. See the [“Using a Restricted Client List”](#) section on page 7-3.
-

For information about starting SESM portals and logging on, see [Chapter 9, “Running SESM Components.”](#)

For information about configuring a customized SESM portal application, see the [“Configuring a Customized SESM Application”](#) section on page 5-19.

