CHAPTER 5

Configuring SESM Portal Applications

This chapter describes the configurable attributes and options for the SESM portals. The chapter includes the following topics:

- SESM Portal Application MBeans, page 5-1
- Associating SSGs with Subscriber Requests, page 5-14
- Configuring a Customized SESM Application, page 5-17
- Automatic Service Connections, page 5-19
- Configuring Location Awareness, page 5-21
- Configuring Personal Firewalls, page 5-25

SESM Portal Application MBeans

The SESM installation process uses default values and values you enter during installation to configure the sample portal applications. Read this section if you want to change or fine-tune configuration after installation.

The SESM portal applications use the following MBeans:

- Logger MBean, page 5-2
- ManagementConsole MBean, page 5-3
- SESM MBean, page 5-4
- SESMDemoMode MBean, page 5-6
- DESSMode MBean, page 5-6
- SSG MBean, page 5-7
- AAA MBean, page 5-10
- Firewall MBean, page 5-11
- WebApp MBean, page 5-13

To change attributes in these MBeans, you can either:

- Make changes using the Agent View running on the application management port. For example, use the Agent View for NWSP. You can access the Agent View from the CDAT main window.
- Edit the application MBean configuration file. For example, edit the nwsp.xml file for NWSP.

The installation process configures all three of the sample portal applications (NWSP, WAP, and PDA) using the same default port numbers. These port numbers are:

- Application port—8080
- Application management port—8180

These applications use different MBean configuration files. The files are located in a directory named for the application under the installation directory:

```
nwsp
   config
      nwsp.xml
wap
   config
      wap.xml
pda
   config
      pda.xml
```

Logger MBean

The Logger MBean configures both logging and debugging tools. The logging tool traces business events in the SESM portal. The debugging mechanism produces messages useful to developers in debugging applications. Table 5-1 describes the attributes in the Logger MBean.

Table 5-1 SESM Portal Application—Logger MBean

Attribute Name	Explanation
debug	Turns debugging on or off. That is, it controls whether Log.debug calls executed by the SESM application are displayed in the log file. **Note** Logging remains on regardless of this value. That is, all Log.trace and Log.warning calls executed in the SESM application are written to the log file regardless of the value of the debug attribute. To turn off logging, comment out the entire Logger MBean. Values for this attribute are: • false—The application produces trace messages but not debug messages. The trace messages record business activity performed by the SESM portal. This setting is the normal, recommended setting for production environments. The trace messages provide important information for diagnosing configuration problems. • true—The application produces trace and debug messages. This setting is intended for development environments to debug portal code behavior. The logging of debug messages can affect performance; hence, this setting is not recommended for production environments. The following parameters control the contents of debug messages that the application generates: logFrame, logStack, logThread, debugPatterns, and debugThreads. The following parameters control the types of logging messages produced: trace and warning. Installed default: false
debugPatterns	By specifying one or more patterns, you turn on a filtering mechanism that excludes any message that does not match the pattern. The patterns are file, class, or method names. Pattern matching is based on substring matches. For example, if you specify the pattern RADIUS, the software focuses on RADIUS messages. To specify multiple patterns, separate the patterns using a comma. Installed default: empty, which means that you receive all messages.

Table 5-1 SESM Portal Application—Logger MBean (continued)

Attribute Name	Explanation
debugThreads	Specifies a specific thread name for which to show debugging messages. You can specify multiple thread names, separating them using a comma. For example: 6,13,22. By default, no thread name is specified. Because each user interaction with the SESM web application takes place in a thread named for that user, this parameter can be used to focus the logging trace on a specific user activity. Enter a list of thread names separated by commas. Installed default: empty
debugVerbosity	Specifies the level of detail in debugging messages. When the debug attribute is set to false, this attribute is ignored. Values are MAX, MED, or LOW. Installed default: LOW
logDateFormat	Specifies format of dates in the log file. Installed default: yyyyMMdd:HHmmss.SSS
logFile	Specifies the filename and location for the logging (tracing) of business events performed by the SESM application. The installed default is: *application.log*/*yyyy_mm_dd*.application.log Where: • *application.log*—Is a Java system property. The same system property is used for all log files, so that they are all created in the same directory. See Table 9-1 on page 9-5 for a description of how the start script sets *application.log*. • *yyyy_mm_dd* —Is the year, month, and day that the file was created. • application.log—Is a constant identifying the application log files.
logFrame	Controls whether or not to log the calling member function. Installed default: false
logStack	Controls whether or not to log stack traces. Installed default: false
logThread	Controls whether or not to log thread IDs. Installed default: true
logToErr	Controls whether or not to route log messages to stderr, in addition to the log file. This parameter is useful for monitoring the SESM web application at the command line. Displaying output to stderr is not recommended for production deployments. Installed default: true
trace	Controls whether or not to log trace messages. These messages indicate entry and exit to code points. Installed default: true
warning	Controls whether or not to log warning messages (nonfatal exceptions). Installed default: true

ManagementConsole MBean

The ManagementConsole MBean configures the portal's management console port, including valid user names and passwords for accessing the console. See the "Configuring the ManagementConsole MBean" section on page 3-5 for more information.

SESM MBean

The SESM MBean configures SESM features and options, including the SESM mode.Table 5-2 describes the attributes in the SESM MBean.

Table 5-2 SESM Portal Application—SESM MBean

Attribute Name	Explanation
mode	An SESM portal runs in one of the following modes. • RADIUS—In this mode, the SESM web application communicates with SSG and a RADIUS server. • LDAP—In this mode, the SESM web application communicates with SSG and an LDAP directory. • Demo—In this mode, the SESM web application does not communicate with other components. Rather, it simulates communication by reading data from a Merit flat file. This mode is intended for demonstrations only, when network components such as SSG, RADIUS, or an LDAP directory are not available. The value for mode is a Java system property named: `sesm.mode` This system property is different from most of the other system properties used in the MBean configuration files, in that, by default, the startup script does *not* set this system property. Therefore, the application runs in the mode specified in the MBean configuration file unless you explicitly override that value at run time. The installation program sets the default value to match the type of installation you perform (RADIUS, LDAP, or Demo.) To change the mode, you can: • Reinstall the software. • Edit the MBean configuration files, changing the mode and other attributes, as appropriate. • Use the mode option on the SESM application startup script command line. This command line option provides a way to quickly switch between modes for testing purposes. You might need to alter the start script to access a different set of MBean configuration files for each mode, or use some other method to ensure that the attributes match the mode you are using. The syntax is: – On Solaris: `jetty/bin/startNWSP.sh -mode {Demo | RADIUS | LDAP}` – On Windows: `jetty\bin\startNWSP.cmd {Demo | RADIUS | LDAP}` • The best way to change the SESM mode is to reinstall the software. Several other configuration attributes must be aligned with the mode for SESM to run properly in the selected mode. Also, you might not have all of the appropriate components to run in a mode other than the one you installed. For example, a demo installation does not install the SPE component.
singleSignOn	Enables or disables the single sign-on feature. • true—Subscribers only need to authenticate during a session. Single sign-on offers the following advantages: – Subscribers can stop the browser or navigate away from the SESM portal pages, and then return to the SESM pages later and not be required to reauthenticate. – Subscribers do not need to reauthenticate if SESM automatic memory management clears sessions from the SESM portal. – Point-to-point protocol (PPP) clients do not need to authenticate to the SESM portal. Instead, the SESM portal uses the PPP authenticated identity from SSG. • false—Subscribers are required to reauthenticate for all of the cases described above. Installed default: true

Table 5-2 SESM Portal Application—SESM MBean (continued)

Attribute Name	Explanation
autoConnect	Specifies if SESM should send connection requests to SSG for the services marked for auto connection in the subscriber's profile. Values are: • false—SESM does not send connection requests to SSG • true—SESM sends connection requests to SSG In RADIUS mode, set this attribute to false, because SSG automatically makes the connections immediately after authentication. You do not need SESM to request those connections. In LDAP mode, the SSG performs automatic connections if it obtains a service list from the RDP. If SSG does not obtain the service list from RDP, you should set this attribute to true. The Add Services option, which is set during RDP installation, controls whether or not the RDP returns a service list to SSG. The Add Services option configures RDP to either: • Return a service list to SSG—SSG performs automatic connections for services marked as auto connect in a subscriber's profile. In this configuration, set the autoConnect attribute to false. • Not return a service list to SSG—SSG cannot perform automatic connections. The advantage to this configuration is that it saves memory on the SSG device. In this configuration, set the autoConnect attribute to true.
profileCache Period	Specifies the time in seconds that a service or group object must be idle in the cache before its resources are deallocated from memory. Installed default: 600
sessionCachePeriod	The minimum time in seconds that an SESM session can be in memory without being accessed. If this value is 0 or undefined, the application calculates a value as: profileCachePeriod * 2. Installed default: 1200
confirmMutex Disconnect	Controls the action of the SESM portal if a subscriber is currently connected to a service in a mutually exclusive service group and then selects another service in that group. • true—The SESM portal displays an error message to the subscriber stating that the current service must be disconnected before selecting the newly selected service. • false—The SESM portal sends a request to SSG to disconnect the current service before sending the request to connect to the newly selected service. • Installed default: false
memRequired	The minimum memory that must be available for the application to create a new SESM session or authenticate a subscriber. If this amount of memory is not available, the subscriber receives a "server busy" message. SESM applications include automatic memory management features that constantly work to free unused memory. If this attribute is set correctly, the application does not run out of memory. If this attribute is set too small, the application might run out of memory and terminate abnormally. The installed default is correct for the NWSP application. You might need to adjust the value for customized applications. If subscribers are receiving the server busy message too frequently, increase the amount of memory reserved for the application. This value is set in the startup script. See the "SESM Portal Application Memory Requirements" section on page 9-8 for more information. Installed default: 10485760

SESMDemoMode MBean

The SESMDemoMode MBean configures SESM in demo mode. Table 5-3 describes the attributes in the SESMDemoMode MBean.

Table 5-3 SESM Portal Application—SESMDemoMode MBean

Attribute Name	Explanation
demoDataFile	Specifies the file that contains data for the demo mode. The installed value is: *application.home*/config/demo.txt Where: *application.home* is a Java system property The NWSP start script derives the value for application.home from an expected (installed) directory structure. To change the value of application.home, edit the start script.

DESSMode MBean

The DESSMode MBean configures SPE attributes used by the SESM application. Table 5-4 describes the attributes in the DESSMode MBean.

Table 5-4 SESM Portal Application—DESSMode MBean

Attribute Name	Explanation
tokenCheckInterval	The time in seconds between checking the authorization tokens. Default: 300 seconds
tokenMaxAge	The length of time in seconds a token can remain in cache without being used before it is deleted. Default: 600 seconds
naming	The component in distinguished name (dn) that the LDAP directory uses to allow access to the directory. For example: • cn—Indicates the common name (cn) used in an NDS directory • uid—Indicates the unique identifier (uid) used in an iPlanet directory

SSG MBean

The SSG MBean configures communication between SESM web applications and SSGs. These components communicate using the RADIUS protocol, so this MBean includes RADIUS protocol attributes. The MBean also includes attributes that determine which SSG should handle a subscriber request. Table 5-5 describes the attributes in the SSG MBean.

Table 5-5 SESM Portal Application—SSG MBean

Object	Attribute Name	Explanation
SSG Global attributes The global attributes apply to all SSGs that the SESM web application might communicate with. To determine how an SSG is configured, use the **show run** command on the SSG host.	PORT	The global value for RADIUS ports on the SSG hosts. This value must match the value that was configured on the SSG device using the following command: `ssg radius-helper` *`authenticationPort`* You can create subnet entries in the MBean configuration file to override this global value for specific SSGs.
	TIMEOUTSECS	The number of seconds the SESM web application waits before timing out RADIUS packets that it sends to SSG. You cannot override this global value. Installed default: 5
	RETRIES	The number of times the SESM web application resends a RADIUS packet to SSG if no response is received. You cannot override this global value. Installed default: 3
	SECRET	The global value for the RADIUS protocol shared secret used for communication between the SESM web application and the SSGs. This value must match the value entered on the SSG device using the **ssg radius-helper key** command. You can create subnet entries in the MBean configuration file to override this global value for specific SSGs.
	MASK	The global value for the mask that the SESM web application applies to incoming subscriber IP addresses to derive an IP address for the SSG. You can create subnet entries in the MBean configuration file to override this global value for specific subnets.
	THROTTLE	The global value for the maximum number of simultaneous requests that SESM portals can send to an SSG. The RADIUS protocol queues additional requests and issues them as the SSG returns responses or timeout messages for previous requests. If set correctly, this throttle attribute prevents the situation in which the SSG receives requests at a faster rate than it can handle, causing the SESM application to time out waiting for responses. Set the throttle value according to the ability of the SSG device to process access requests from a client. If the SESM portal times out while waiting for responses from the SSG, try adjusting this value lower. Installed default: 20

Table 5-5 SESM Portal Application—SSG MBean (continued)

Object	Attribute Name	Explanation
SSG global attributes *(continued)*	BUNDLE_LENGTH	The global value for the port bundle length that SSGs use when the port-bundle host key feature is enabled. The port bundle length is the number of bits that SSG uses to indicate bundled slots. For example, a value of 4 indicates 16 bundled slots. This value must match the value used in the following command on the SSG host: `ssg port-map` *`length`* Default: You set this value during installation.
	PORT_BUNDLE_ HOST_KEY_ SWITCH	The global value indicating whether or not the port-bundle host key feature is enabled on the SSGs. If BUNDLE_LENGTH is zero, then the value of this switch is important. • true—The SSGs have port-bundle host key enabled with a 0 bundle length. • false—The SSGs do not have port-bundle host key enabled. • If BUNDLE_LENGTH is non-zero, this switch is ignored, because a nonzero value implies the use of the host key feature.
	MIN_LOCAL_PORT MAX_LOCAL_PORT	Together, these two attributes specify a range of UDP ports for RADIUS protocol requests from the SESM portal application to the SSG. By using these attributes, you restrict the source ports used by NWSP to only the ports in the specified range. For example, you might want to restrict port usage if a firewall separates SESM from other components. In that case, you can configure the firewall to allow traffic through the specified range of ports. You can create subnet entries in the MBean configuration file to override this global value for specific SSGs.

Table 5-5 SESM Portal Application—SSG MBean (continued)

Object	Attribute Name	Explanation

SSG subnet entries
Use subnet entries to override the global values or to map client subnets to specific SSGs when the port-bundle host key feature is not being used.
See the "Associating SSGs with Subscriber Requests" section on page 5-15 for more information about using subnet entries.
	Subnet entries use positional arguments.	The format for a subnet entry is:
		`<Call name="setSubnetAttribute">`
		`<Arg>`*`subnetAddress`*`</Arg>`
		`<Arg>`*`subnetMask`*`</Arg>`
		`<Arg>`*`argumentName`*`</Arg>`
		`<Arg>`*`argumentValue`*`</Arg>`
		`</Call>`
		The call to setSubnetAttribute has four positional arguments:
		1. *subnetAddress* is the subnet for which you are explicitly setting a value, overriding the globally set value.
		2. *subnetMask* is the mask that can be applied to the subscriber's IP address to derive the subnet.
		3. *argumentName* is the argument that you are explicitly setting:
		– PORT—The SSG port for the specified subnet. Overrides the globally-set SSG port.
		– MASK—The mask used on the subscriber's IP address to derive the subnet. Overrides the globally-set mask.
		– SECRET—The shared secret used between SESM and SSG. Overrides the globally-set shared secret.
		– BUNDLE_LENGTH—The host key bundle length used on the SSG. Overrides the globally-set bundle length. Bundle length is the number of bits that SSG uses for the port bundle feature. For example, a value of 4 indicates 16 bundled slots. A value of 0 indicates that the SSG is not using the port-bundle host key mechanism.
		This value must match the value used in the following command on the SSG host:
		`ssg port-map length`
		– IP—Explicitly sets the IP address for the SSG that services the specified *subnetAddress*.
		– THROTTLE—The maximum number of simultaneous requests that SESM portals can send to the SSG. Overrides the globally set throttle value.
		– SESSION_LOCATION and SESSION_BRAND—The location or brand associated with the specified subnet. Valid values are defined as arbitrary properties in the WebApp MBean. See the "Configuring Location Awareness" section on page 5-22 for more information.
		– MIN_LOCAL_PORT and MAX_LOCAL_PORT—The range of UDP ports used by the SESM portal to send messages to the SSG. Overrides the globally set range.
		4. *argumentValue* is the value for *argumentName*.

AAA MBean

The AAA MBean configures communication between an SESM web application and the RADIUS servers, which occurs only when the SESM application is running in RADIUS mode.

Table 5-6 describes the attributes in the AAA MBean.

Table 5-6 SESM Portal Application—AAA MBean

Attribute Name	Explanation
throttle	The maximum number of simultaneous requests that SESM web applications can send to a RADIUS server. This is a RADIUS protocol attribute. The RADIUS protocol queues additional requests and issues them as the server returns responses or timeout messages for previous requests. Installed default: 256
timeOut	The number of seconds the SESM web application waits before timing out RADIUS packets that it sends to the AAA server. Installed default: 4
maxRetries	The number of times the SESM web application resends packets to the AAA server if no response is received. Installed default: 3
primaryIP	The IP address or the host name of the primary AAA server.
primaryPort	The port number that the primary RADIUS server listens on. Default: 1812
secret	The shared secret used between the RADIUS server and the SESM web application. The shared secret must be the same for the primary and secondary servers. It must match the secret specified when you configured SESM as a NAS client on the RADIUS server. Default: `cisco`.
secondaryIP	The IP address or host name of the secondary AAA server. If you are not using a secondary RADIUS server, reenter the primary server.
secondaryPort	The port number that the secondary RADIUS server listens on. If you are not using a secondary server, reenter the primary server. Default: 1812
servicePassword	The password that the SESM web application uses to request service profiles from the RADIUS server. It must match the service password values used in the service profiles in the RADIUS database. Default: `servicecisco`
serviceGroupPassword	The password that the SESM web application uses to request group profiles from the RADIUS server. It must match the service group password values used in the service group profiles in the RADIUS database. Default: `groupcisco`

Firewall MBean

The Firewall MBean configures fields on the NWSP My Firewall page. Table 5-7 describes the attributes in the Firewall MBean.

Firewall Protocols and Applications

The Firewall MBean defines a list of firewall protocols and firewall applications, which are SESM concepts used in a different way than the OSI protocol and application concepts. You can specify ACLs on firewall applications, but not on firewall protocols.

- A firewall protocol defines components used to build the firewall applications. They consist of any Layer 3 or Layer 4 protocol and an optional port. (The combination of a lower layer protocol and a port might define an OSI layer 7 application, such as FTP.) For example, the following are some firewall protocols, shown as they are defined to the Firewall MBean:

  ```
  <Key>ip</Key>
  <Value>ip</Value>

  <Key>tcp</Key>
  <Value>tcp</Value>

  <Key>ftp</Key>
  <Value>tcp, 21</Value>

  <Key>https</Key>
  <Value>tcp,443</Value>

  <Key>imap</Key>
  <Value>tcp,143</Value>
  ```

- The firewall applications are the items that are displayed on the My Firewall page in the Applications/Protocols column. They are the items on which ACLs are applied. A firewall application consists of one or more firewall protocols. For example:

  ```
  <Key>ip</Key>
  <Value>ip</Value>

  <Key>tcp</Key>
  <Value>tcp</Value>

  <Key>ftp</Key>
  <Value>ftp</Value>

  <Key>email</Key>
  <Value>smtp,pop2,pop3,imap</Value>

  <Key>www</Key>
  <Value>http,https</Value>
  ```

SESM includes many predefined firewall protocols and firewall applications. You can see all of these predefined values by accessing the NWSP Agent View. In the Firewall MBean, click in the value column for the read-only attributes AllApplicationDescriptions and AllProtocolDescriptions.

You can use the customProtocols and customApplications attributes in the Firewall MBean to define additional firewall protocols and firewall applications.

Table 5-7 SESM Portal Application—Firewall MBean

Attribute Name	Explanation

customProtocols	Defines additional firewall protocols. Each item in the array consists of two elements:
	• Key—Names the firewall protocol. The name can be anything.
	• Value—The lower layer protocol (OSI Layer 3 or 4 protocol) and an optional port, separated by a comma. The lower layer protocol value must be a protocol that the SSG host is configured to accept.
	For example:
	`<Key>tcp</Key>`
	`<Value>tcp</Value>`
	`<Key>ftp</Key>`
	`<Value>tcp, 21</Value>`
	See the "Firewall Protocols and Applications" section on page 5-11 for a definition and more examples of firewall protocols. Several firewall protocols are predefined in SESM and do not need to be explicitly defined here.

customApplications	Defines additional firewall applications. Each item in the array consists of two elements:
	• Key—Names the firewall application. The name can be anything.
	• Value—A list of firewall protocols that comprise the application, separated by commas. Valid values are the SESM predefined and custom firewall protocols.
	To see a list of all defined protocols, open the portal's Agent View management console and click in the value column of the AllProtocolDescriptions attribute, a read-only attribute in the Firewall MBean.
	`<Key>ftp</Key>`
	`<Value>ftp</Value>`
	`<Key>www</Key>`
	`<Value>http,https</Value>`
	See the "Firewall Protocols and Applications" section on page 5-11 for a definition and more examples of firewall applications.

displayApplications	Specifies the firewall applications that appear on the NWSP My Firewall page, in the Applications/Protocols column. Items in this list must be defined as predefined or custom firewall applications. To see a list of all defined applications, open the portal's Agent View management console and click in the value column of the AllApplicationsDescriptions attribute, a read-only attribute in the Firewall MBean. **Note** The text that represents an application on the My Firewall page is defined in the portal application's resource bundles. See the "Configuring the NWSP My Firewall Page" section on page 5-27 for more information.

Table 5-7 SESM Portal Application—Firewall MBean (continued)

Attribute Name	Explanation
direction	Specifies direction (in or out) for the default access control direction in the ACLs created by SESM. See the "Creating Subscriber-Configured Personal Firewalls" section on page 5-29 for more information about created ACLs. Value values for direction are: • in—Upstream, from the subscriber • out—Downstream, to the subscriber All connections have a return path. A block on in also affects traffic traveling in the opposite direction, and vice-versa. For any ACL, the choice of whether to control the in or out direction is a matter of preference.
returnOption	Sets the return option for TCP applications. Recommended values are: permit and default. Default refers to the Permit/Deny All Else button on the My Farewell page. Default: permit **Note** You can alter the My Firewall JSP to add a button allowing the subscriber to choose the TCP return option. The JSP contains commented-out code for an ipPermission button, which you could copy to implement a return TCP permission button.

WebApp MBean

The WebApp MBean configures options of the SESM portal application, including:

- Attributes that control the behavior of the application
- Attributes that control captive portal service redirections handled by NWSP
- Context parameters, which are used by an application for any arbitrary reason. The nwsp.xml file contains an example of using context parameters to control web page content based on location.

Table 5-8 describes the attributes in the WebApp MBean.

Table 5-8 SESM Portal Application—WebApp MBean

Attribute Name	Explanation
confirmAtServiceLogon	Controls whether or not the application prompts the user for confirmation before it acts on a request to start a service. Default: FALSE
confirmAtServiceLogoff	Controls whether or not the application prompts the user for confirmation before it acts on a request to log off. Default: TRUE
confirmAtAccountLogoff	Controls whether or not the application prompts the user for confirmation before it acts on a request to log off of the SESM application. Default: TRUE
sessionTimeOut	The number of seconds of inactivity allowed before the application closes a session. This value overrides the timeout value in the nwsp.jetty.xml file. Default: 7200

Table 5-8 SESM Portal Application—WebApp MBean (continued)

Attribute Name	Explanation
credentialMaxLength	Controls the maximum length of user names and passwords. Default: 30
serviceNotGivenURI defaultURI serviceSubscriptioURI serviceStartURI serviceLogonURI	These attributes are related to the captive portal solution. See Table 11-4 on page 11-17 for explanations of these attributes.
addDimension entries	You can create arbitrary attributes and associate them with subscriber requests in the manner described for location awareness in the "Configuring Location Awareness" section on page 5-21.

Associating SSGs with Subscriber Requests

A typical SESM deployment consists of multiple SSGs. The installation process configures communication with one SSG when you choose the appropriate options. This section describes how to configure communication with additional SSGs. It includes the following topics:

- Setting SSG Global and Subnet Entries, page 5-14
- Using Port-bundle Host Key with Identical SSG Configurations, page 5-15
- Using Port-bundle Host Key with Varying SSG Configurations, page 5-16
- Specifically Mapping SSGs to Subscriber Subnets, page 5-16

Setting SSG Global and Subnet Entries

You can set the attributes that associate an SSG with subscriber requests globally, by client subnet, or for a specific client IP address, as follows:

- Global attribute elements—A global setting applies to all SSGs. For example, a global shared secret setting means that all SSGs are configured using the same secret. The global attributes are: PORT, SECRET, MASK, and BUNDLE_LENGTH.
- Subnet attribute elements—The subnet attributes apply to a specific subnet and override the global attribute value. The subnet attributes are optional; if any of them are not specifically coded, the global attribute value is used. Subnet attributes that you can supply are: PORT, SECRET, MASK, BUNDLE_LENGTH, and IP. The IP attribute is the IP address of the SSG for a specified subnet.

  You can also specify some optional session information in a subnet entry, using the SESSION_LOCATION and SESSION_BRAND attributes.
- A specific client IP address can be specified in a subnet element.

Using Port-bundle Host Key with Identical SSG Configurations

The easiest way to associate the correct SSG with each subscriber request is to use the port-bundle host key feature on all SSGs, and configure certain attributes identically on all of the SSG hosts. We recommend using the port-bundle host key feature unless you require backward compatibility with SSD Release 2.5(1).

Note To use the port-bundle host key feature, the SSG device must be running Cisco IOS Release 12.2(2)B or later and the SSG port-bundle host key feature must be configured appropriately.

When the port-bundle host key feature is enabled on an SSG, the SSG replaces the subscriber IP address in the request with a software token (or key) when it forwards the request to SESM. The SESM application uses this key in its responses to SSG, and the SSG does an internal translation to an actual host object.

The key is a unique combination of an SSG IP address from a range of IP addresses and a port number from a range of port numbers, as follows:

IP_address:*port*

The IP address and port ranges are configured on each SSG. The key uniquely identifies each subscriber currently logged on to SESM, even when multiple subscribers are using the same IP address.

To use the port-bundle host key feature to associate SSGs, follow these procedures:

1. Enable and configure the port-bundle host key feature on all of the SSGs, as described in the Configuring the Host Key Port Bundle Feature on SSG, page F-2.
2. Configure the same values on all of the SSG hosts for the following attributes:
   - Port—The SSG port on the SSG host. Specify the port that SSG uses to listen for RADIUS requests from an SESM application. Configure this value on the SSG device using the following command:

     ```
     ssg radius-helper authenticationPort
     ```

   - Shared secret—The shared secret used for communication between SSG and an SESM application. Configure this value on the SSG device with the following command:

     ```
     ssg radius-helper key
     ```

   - Port bundle length—The number of bits that SSG uses for port bundling when the port-bundle host key feature is enabled. This value must be 0 or 4. Configure this value on the SSG device with the following command:

     ```
     ssg port-map length
     ```

3. When the SESM installation program prompts you, enter the globally-configured values in Step 2. These values are saved as global elements in the SSG MBean, as the following example illustrates.

Example Using Port-Bundle Host Key

When the port-bundle host key feature is enabled and configured, you can set all parameters globally.

```
<Configure name="com.cisco.aggbu:name=SSG">
<Call name="setGlobalAttribute"><Arg>PORT</Arg><Arg>1812</Arg></Call>
<Call name="setGlobalAttribute"><Arg>SECRET</Arg><Arg>cisco</Arg></Call>
<Call name="setGlobalAttribute"><Arg>MASK</Arg><Arg>255.255.255.255</Arg></Call>
<Call name="setGlobalAttribute"><Arg>BUNDLE_LENGTH</Arg><Arg>4</Arg></Call>
</Configure>
```

In this example, all SSGs are configured to use a port of 1812 and a shared RADIUS secret of `cisco`. The BUNDLE_LENGTH of 4 indicates that port-bundle host key is configured on all SSGs.

The MASK attribute specifies the mask that SESM applies to the client (source) IP address in a received message to determine the client's subnet, and, from that, the SSG IP address. However, when a host key is used, the client (source) IP address is the SSG IP address. The SESM installation program provides the default mask of 255.255.255.255.

Using Port-bundle Host Key with Varying SSG Configurations

If port-bundle host key is enabled on all SSGs, but some are configured differently, you can configure the global case and then specifically configure exceptions. For example, if all but one SSG is assigned the same shared secret, you can configure the shared secret attribute globally, and then add one subnet entry to configure the different secret for the single SSG.

The installation program lets you provide one set of SSG global attribute values and one subnet entry. It records these attribute values in the <Configure name="SSG"> section of the application MBean configuration file, as illustrated in the following example.

Example Using Port-bundle Host Key with One Noncomplying SSG

In this example, port-bundle host key is enabled on all SSGs. In addition, all SSGs are using the same port, secret, and client IP address mask, except that one SSG uses a different port. In this case, you can set all parameters globally, and then use one subnet entry to define:

- The client subnet being serviced by the SSG that uses the nonconforming port.
- The port value that overrides the globally-set port value.

In the following example, the SSG that services subnet 10.1.1.0 uses port 1245.

```
<Configure name="com.cisco.aggbu:name=SSG">
<Call name="setGlobalAttribute"><Arg>PORT</Arg><Arg>1812</Arg></Call>
<Call name="setGlobalAttribute"><Arg>SECRET</Arg><Arg>cisco</Arg></Call>
<Call name="setGlobalAttribute"><Arg>MASK</Arg><Arg>255.255.255.255</Arg></Call>
<Call name="setGlobalAttribute"><Arg>BUNDLE_LENGTH</Arg><Arg>4</Arg></Call>
<Call name="setSubnetAttribute"><Arg>10.1.1.0</Arg><Arg>255.255.255.0</Arg><Arg>PORT
</Arg><Arg>1245</Arg></Call>
</Configure>
```

Specifically Mapping SSGs to Subscriber Subnets

Each request arriving at an SESM web application contains a source, or client, IP address. SESM uses this client IP address to determine which SSG should handle each request.

- If the configuration file explicitly provides an SSG IP address for a subnet or a specific client IP address, SESM uses that SSG. You code an explicit IP address in a <subnet> element. The MASK value in the subnet element specifies whether the element applies to a subnet or to a specific subscriber IP address. The <IP> parameter in the subnet element specifies the SSG IP address.

  For example, the following subnet entry explicitly sets the SSG IP address to 10.6.7.1 for subnet 10.2.0.0:

  ```
  <Call name="setSubnetAttribute">
  <Arg>10.2.0.0</Arg><Arg>255.255.0.0</Arg><Arg>IP</Arg><Arg>10.6.7.1</Arg></Call>
  ```

- If an explicit IP address for the SSG is not provided, SESM masks the subscriber's IP address to determine the SSG that should handle the request.

Use masking as follows:

- If port-bundle host key is enabled—The port-bundle host key feature replaces the original client IP address with the IP address of the SSG. (The port bundle key appended to the address preserves a unique identity for each subscriber). Since the client IP address is the SSG IP address, a global setting for MASK of 255.255.255.255 correctly results in the client IP address being used as the SSG IP address.
- If the SSG uses the first IP address in a particular set of client subnets—Specify the mask that SESM web application can apply to the client IP address to derive the SSG IP address. For example, if, for all 10.x.0.0 client subnets, the SSG IP address is 10.x.0.1, you would specify a subnet of 10.0.0.0 and a mask of 255.0.0.0.
- If the SSG IP is the first IP in all client subnets—You can set a global value for mask. For example, for all subscriber addresses x.y.z.n, if the SSG always has an IP address of x.y.0.1, then use a global mask of 255.255.0.0.

Note Set the widest global or subnet mask possible. Each SSG IP address consumes some resources on the machine where the SESM application is running. (Each one uses an open file descriptor.) For example, even when the SSG is using port-bundle host key, a mask of 255.255.255.0 is desirable so that the SESM uses a single SSG IP address rather than 254 different SSG IP addresses. A mask of 255.255.255.255 is the least efficient, but it is the default setup.

Example Mapping Client Subnets to SSGs

In this example, port-bundle host key is not being used. In this case, you must explicitly define the mapping from subscriber subnet to the SSG IP address.

```
<Configure name="com.cisco.aggbu:name=SSG">
<Call name="setGlobalAttribute"><Arg>PORT</Arg><Arg>1645</Arg></Call>
<Call name="setGlobalAttribute"><Arg>SECRET</Arg><Arg>cisco</Arg></Call>
<Call name="setGlobalAttribute"><Arg>MASK</Arg><Arg>255.255.255.255</Arg></Call>
<Call name="setGlobalAttribute"><Arg>BUNDLE_LENGTH</Arg><Arg>0</Arg></Call>
<Call name="setSubnetAttribute"><Arg>10.1.1.0</Arg><Arg>255.255.255.0</Arg><Arg>IP
</Arg><Arg>10.21.1.2</Arg></Call>
<Call name="setSubnetAttribute"><Arg>10.1.2.0</Arg><Arg>255.255.255.0</Arg><Arg>IP
</Arg><Arg>10.21.2.2</Arg></Call>
<Call name="setSubnetAttribute"><Arg>10.1.3.0</Arg><Arg>255.255.255.0</Arg><Arg>IP
</Arg><Arg>10.21.3.2</Arg></Call>
<Call name="setSubnetAttribute"><Arg>10.1.4.0</Arg><Arg>255.255.255.0</Arg><Arg>IP
</Arg><Arg>10.21.4.2</Arg></Call>
</Configure>
```

Configuring a Customized SESM Application

The Cisco SESM is a collection of components for creating specialized Java 2 Platform, Enterprise Edition (J2EE) web server applications. J2EE provides a framework for using various Java-based components to develop multi-tiered applications. The multi-tiered application (as opposed to the 2-tiered client server application) provides many opportunities for isolating and controlling functional pieces of a large application. For more information about the J2EE development platform, see:

http://java.sun.com/j2ee/

SESM Application Definition

A Cisco SESM application consists of the following:

- SESM servlets and classes—The SESM API defines the SESM classes, including the configurable MBeans, used to implement the application functionality.
- ConfigAgent—The ConfigAgent is a Cisco developed MBean that configures other MBeans. It configures MBeans that are registered with the JMX server by applying parameter values from .xml files. Because .xml files are easily maintained and changed by system administrators, applications that use ConfigAgent are highly configurable without recompiling. Chapter 4 in this guide explains all of the configurable parameters in all of the MBeans.
- Java Server Pages (JSPs)—JSPs offer a way to deliver dynamic content in web pages. Web developers at the deployment site can control their subscriber's SESM experience through the JSPs. The *Cisco Subscriber Edge Services Manager Web Developer Guide* provides instructions for defining and compiling JSPs.
- Images—Images are used by the JSPs and control the look and feel and branding aspects of an SESM application. The *Cisco Subscriber Edge Services Manager Web Developer Guide* provides instructions for changing images and incorporating them into the JSPs.

SESM Application Names

The SESM application name that you use for a customized application is arbitrary, but it must match in all of the following locations:

- The name of the application-specific subdirectory under the installation directory. For example, the directory that holds all application specific information for the NWSP application is:

  ```
  <installDir>nwsp
  ```

- Application parameter inside the application startup script. In the installed scripts, the application name is hard coded on the line that calls the generic start script. For example, for the NWSP application on Windows NT, the call line is:

  ```
  call "%SCRIPTDIR%start.cmd" nwsp %PORTNO%
  ```

- Name of the application's configuration file in the `jetty` subdirectory. For example, for the NWSP application, the configuration filename is:

  ```
  nwsp.jetty.xml
  ```

An application name in the startup script tells the ConfigAgent which configuration file to open. The application name is passed to ConfigAgent by the application startup scripts. The application name might also be used in other ways. For example, you can configure the parameter that defines the Jetty Server log filename to incorporate the application name in the log filename.

Creating Configuration Files and Startup Scripts

Application developers at your site might make changes to the delivered NWSP sample application, producing a customized application. Customized applications require their own set of configuration files, although the files might be very similar to those provided for the sample application.

To create the required configuration files and startup scripts for a customized SESM application that will run in a Jetty server, follow these steps:

Step 1 Create a configuration file for the new application in the container's config directory. You can copy the nwsp.jetty.xml file and appropriately rename it. For example:

```
jetty
    config
        newApplication.jetty.xml
```

Step 2 Edit the new file.

Step 3 Create a startup script for the new application by copying the startNWSP script and appropriately renaming the copy. For example:

```
jetty
    bin
        startNewApplication
```

Step 4 Edit the new file, changing the application name and the port number parameters.

Step 5 Copy the nwsp directory structure, and rename the nwsp objects appropriately. For example, copy:

```
nwsp
    config
        nwsp.xml
    docroot
    docs
```

Step 6 See the *Cisco Subscriber Edge Services Manager Web Developer Guide* for information about customizing the JSPs, images, and other components. That guide also describes how to update the docroot folder, recompile affected components, and edit the web.xml file.

Automatic Service Connections

An automatically connected service is a service that SSG connects immediately after the subscriber authenticates, without requiring the subscriber to explicitly select the service. This section describes two topics related to automatic connections:

- Configuring Automatic Services, page 5-19
- Subscriber Experiences with Automatic Connections, page 5-20

Configuring Automatic Services

In general, if a service is marked as an auto connect service, the SSG performs the automatic connection after the subscriber authenticates. There is a special case with SESM in LDAP mode in which SESM is involved with automatic connection.

Configuring a Service for Automatic Connection

A subscriber profile specifies services for automatic connection. The subscriber profile also controls whether or not the service is hidden or not. If an auto connect service is hidden, it does not appear in the service list displayed on a service connection page.

In RADIUS mode, to configure a service for automatic connection, use the Account-Info A attribute in the subscriber profile. See Table C-6 on page C-11 for more information.

In LDAP mode, to configure a service for automatic connection:

- Subscribers can use the web portal's self-management features to select and deselect the auto connect feature for a service.
- Administrators can use CDAT to maintain subscriber profiles. See the *Cisco Distributed Administration Tool Guide* for information.

Configuring SESM to Request Automatic Connections in LDAP Mode

In LDAP mode, the SSG performs automatic connections if it has the service list. If SSG does not have the service list, the SESM application can perform the automatic connections. During RDP installation, the Add Services option configures RDP to either:

- Return a service list to SSG—In this case, RDP includes the subscriber's service list and related information in replies to SSG, and SSG performs automatic connections for services marked for auto connection in the subscriber's profile.

  The service information consumes memory on the SSG host.
- Not return a service list to SSG—In this case, SSG cannot perform automatic connections. The advantage to this configuration is that it saves memory on the SSG host.

  In this case, you can configure the SESM application to perform automatic connections. The following line in the application MBean configuration file (for example, nwsp/config/nwsp.xml) controls whether the SESM web application performs automatic connections:

  ```
  <Set name="autoConnect" type="boolean">false</Set>
  ```

  Change the value to `true` to enable automatic connections by the SESM web application.

To change the setting of the RDP service list option, reinstall RDP.

Subscriber Experiences with Automatic Connections

This section describes the behavior of the SESM portal application regarding automatically connected services.

Connection Status for Auto Connect Services

The status page in an SESM portal shows the status for all services, including automatically connected services. In NWSP, the selection page includes service status indicators for each service listed. Hidden services are not listed. See the "Configuring a Service for Automatic Connection" section on page 5-19 for an explanation of a hidden service.

Immediately after logging in, the service status for auto connect services might display as not connected. This happens if the service indicators display before the connection is completed. Proxy and tunnel services, for example, can take a while to connect. If the subscriber refreshes the window or selects the status window, the automatically connected services display with a connected status.

Pop-Up Window for Auto Connect Services

If the subscriber's home URL is set to an autoconnect service, the pop-up window for the service might appear before the connection completes. If this occurs, the following message appears in the pop-up window:

```
Page cannot be displayed.
```

The URL is correct. If the subscriber waits a short time and resubmits the request using the URL already displayed in the window, the service pages appear.

Changing the Auto Connect Property for a Service

In LDAP mode, a subscriber can use the SESM self-management features to select or deselect the auto connect property. These changes are recorded immediately in the LDAP directory, but the change is not effective immediately. Changes are not visible in SESM until the cache timeout period in RDP elapses.

For example, a subscriber might select the auto connect property for a service, log out of SESM, log back in, and notice that the service was not automatically connected. Caching in the RDP causes this delay.

Caching in RDP improves system performance. The deployer can turn off caching or reduce the cache period, but those actions impact performance.

Disconnecting Auto Connect Services

A subscriber can disconnect an auto connected service at any time. The disconnected status persists as long as the subscriber remains authenticated. The SESM single sign-on option affects whether a subscriber remains authenticated across SESM sessions. If the subscriber has to reauthenticate after an SESM session expires, the SSG reconnects all auto connect services.

An SESM session might expire, for example, because the subscriber closed the browser or navigated away from the SESM pages. When an SESM session expires:

- With single sign-on, subscribers are not required to reauthenticate.
- Without single sign-on, subscribers are required to reauthenticate when they navigate back to the SESM portal application. As a result of the reauthentication, SSG reconnects the auto connect services.

We recommend running SESM portal applications with single sign-on turned on.

Configuring Location Awareness

This section describes the various ways that an SESM application can implement and use location awareness. The section includes the following topics:

- Overview of Location Awareness, page 5-22
- Location Awareness in the NWSP Application, page 5-22
- Configuring Location Awareness Using IP Addresses, page 5-23
- Configuring Arbitrary Attribute Values, page 5-24
- Demonstrating Location Awareness in NWSP, page 5-25

Overview of Location Awareness

An SESM portal application can determine the location of a subscriber in the following ways:

- The SESM deployer can associate specific locations to IP addresses. The IP address is that of the subscriber (subscriber subnet) or, if port-bundle host key feature is configured on the SSG, that of the SSG that is handling the subscriber requests. To implement this method of location awareness, configure the locations in the SSG MBean in the portal configuration file. The "Configuring Location Awareness Using IP Addresses" section on page 5-23 describes this procedure.

  The SESM core model uses the configured location to set the "LOCATION" attribute in the SESMSession object created for the subscriber. The location is thus available for use in any way the application developer chooses. See the *SESM Web Developer Guid*e for more information about the SESMSession object.

The application developer can use the following methods to control and present content in the JSPs based on the location:

- User shape mechanism—The application can use the location dimension in the user shape. The location dimension can determine resources to use in the returned JSPs. See the *Subscriber Edge Services Manager Web Developer Guide* for more information about the user shape mechanism.
- Arbitrary attributes—SESM offers a way to use the configuration file to associate attribute values to locations. This method of assigning attribute values is configured in the portal configuration file, in the WebApp MBean. The "Configuring Arbitrary Attribute Values" section on page 5-24 describes this procedure.

  The SESM core model constructs a reference table holding all of the configured attributes and associated values. These attributes are thus available for use in any manner the application developer chooses. See the *SESM Web Developer Guid*e for more information about getting dimensions that are configured with the addDimension calls.

Location Awareness in the NWSP Application

The NWSP application shows location awareness capabilities in the following ways:

- In locationDimension.jsp, NWSP uses the location to change the look of the banner used on the NWSP logon page. The location determines which city name appears in the NWSP logo. The nwsp/docroot directory includes subdirectories for three locations: london, paris, and newyork.
- In initUser.jsp, NWSP uses attributes based on location to help determine the initial URL for an Internet service pop-up window. NWSP determines the initial URL as follows:
  - If the subscriber request was captured by the SESM Captive Portal application, the subscriber's initial URL request is used.
  - Otherwise, if a location in an addDimension call matches the LOCATION attribute from the SESMSession object, the URL associated with the location is used.
  - Otherwise, if the subscriber profile includes a non-blank H attribute, that URL is used.

Configuring Location Awareness Using IP Addresses

To configure an SESM portal application to determine location based on IP addresses, use the following procedure:

Step 1 Edit the application MBean configuration file. For example, edit nwsp.xml.

Step 2 In the SSG MBean in the configuration file, use SSG subnet entries with the SESSION_LOCATION attribute, as follows:

```
<Call name="setSubnetAttribute"><Arg>ipAddress</Arg><Arg>mask</Arg>
    <Arg>SESSION_LOCATION</Arg><Arg>location</Arg></Call>
```

Where:

- *ipAddress* and *mask* indicate one of the following:
  - A range of subscriber IP addresses (a subnet)
  - A specific IP address—The IP address is that of the client, or, if port-bundle host key is configured on the SSG, one of the SSG IP addresses specified in the port-bundle host key port map configuration.
- *location* is the location you want to associate with *ipAddress*. Any value is acceptable, but it must match your intended uses. For example:
  - If you plan to use locations as a dimension in the user shape, the configured location values must match subdirectory names in the portal application docroot directory. The NWSP application, for example, contains the following subdirectories:

```
nwsp
   docroot
      london
      newyork
      paris
```

  - If you plan to associate arbitrary attributes to locations, the configured location values must match locations you define in addDimension calls. The NWSP application, for example, assigns a URL to a location named london.

Note The user shape mechanism and the addDimension calls are different features and are not related. The user shape mechanism has no dependencies on any values defined in the addDimension calls.

See Table 5-5 on page 5-7 for more information about formatting subnet entries.

Step 3 For the location determination to be meaningful, the SESM portal application must use the "LOCATION" attribute in the SESMSession object in some way. In the NWSP application, the location is a dimension in the user shape and determines the image used in the NWSP banner. See the *Cisco Subscriber Edge Services Manager Web Developer Guide* for information about setting and using the location attribute in the locationDimension.jsp.

Example 1—Location Associated with Subscriber IP Addresses

The following example associates locations with subscriber subnets. The example associates a different subscriber network with each of the three example locations defined in Step 2. In the NWSP application, when subscribers from the 144.0.0.0 network point their browsers to the NWSP URL, they receive a page containing the words New York under the NWSP logo.

```
<Call name="setSubnetAttribute"><Arg>10.0.0.0</Arg><Arg>255.0.0.0</Arg>
    <Arg>SESSION_LOCATION</Arg><Arg>london</Arg></Call>
<Call name="setSubnetAttribute"><Arg>1.0.0.0</Arg><Arg>255.0.0.0</Arg>
    <Arg>SESSION_LOCATION</Arg><Arg>paris</Arg></Call>
<Call name="setSubnetAttribute"><Arg>144.0.0.0</Arg><Arg>255.0.0.0</Arg>
    <Arg>SESSION_LOCATION</Arg><Arg>newyork</Arg></Call>
```

Example 2—Location Associated with SSG IP Address

When the port-bundle host key feature is configured on the SSG, location must be associated with an SSG IP address, rather than the subscriber's IP address. In the following example, the IP address is an SSG source IP address included in the port mappings during port-bundle host key configuration.

```
<Call name="setSubnetAttribute"><Arg>10.52.199.20</Arg><Arg>255.255.255.255</Arg>
    <Arg>SESSION_LOCATION</Arg><Arg>london</Arg></Call>
```

Configuring Arbitrary Attribute Values

To configure an SESM portal application to assign values to arbitrary attributes, use the following procedure:

Step 1 Edit the application MBean configuration file. For example, edit nwsp.xml.

Step 2 In the WebApp MBean in the configuration file, use addDimension calls to add a new attribute and associate values with that attribute. The format for an addDimension call is:

```
<Call name="addDimension">
      <Arg type="int">attributeID</Arg>
      <Arg>attributeValue</Arg>
      <Arg>attributeResult</Arg>
```

An example from nwsp.xml is:

```
<Call name="addDimension">
      <Arg type="int">1</Arg>
      <Arg>london</Arg>
      <Arg>http:\\www.london.com</Arg>
```

Where:

- *attributeID* identifies a new attribute type. Use the same *attributeID* for all entries associated with the same attribute. For example, the nwsp.xml file defines three location attributes, all using the *attributeID* of 1. To add additional locations, also use the *attributeID* of 1. To add a new arbitrary attribute, use a different attributeID.
- *attributeValue* names the attribute. For example, the nwsp.xml includes the attribute names london, paris, and newyork.
- *attributeURL* defines a URL that you want to associate with the *attributeValue*. For example, the nwsp.xml file defines URLs for london, paris, and newyork.

Demonstrating Location Awareness in NWSP

To demonstrate configuration-based location awareness in NWSP, use the following procedure:

Step 1 Install SESM in Demo mode.

Step 2 Edit the following lines in nwsp.xml to include a specific IP addresses for two different client machines that are available for the demonstration.

```
<Call name="setSubnetAttribute"><Arg>NEED_REAL_IP_ADDRESS</Arg><Arg>255.0.0.0</Arg>
    <Arg>SESSION_LOCATION</Arg><Arg>london</Arg></Call>
<Call name="setSubnetAttribute"><Arg>NEED_REAL_IP_ADDRESS</Arg><Arg>255.0.0.0</Arg>
    <Arg>SESSION_LOCATION</Arg><Arg>paris</Arg></Call>
```

Step 3 (Optional) Edit the following lines in nwsp.xml to change the URLs associated with the london and paris locations.

```
<Call name="addDimension">
      <Arg type="int">1</Arg>
      <Arg>london</Arg>
      <Arg>http://www.london.com</Arg>
    </Call>
    <Call name="addDimension">
      <Arg type="int">1</Arg>
      <Arg>paris</Arg>
      <Arg>http://www.paris-france.org/</Arg>
    </Call>
```

Step 4 Save the nwsp.xml file.

Step 5 Start NWSP using the NWPS startup script.

Step 6 Open browsers on each of the client systems.

Step 7 From each browser, go to the SESM URL. For example, go to http:\\serverName:8080.

Step 8 Notice the images in the banners on each browser. One should say London; the other should say Paris.

Step 9 On a third machine, repeat steps 7 through 9. The banner should not include a city name, because the third browser’s IP address is not associated with any location in the configuration file.

Step 10 From one of the browsers, connect to an Internet service (if the Internet service was not automatically configured.) When an Internet connection occurs, a service pop-up window appears, attempting to go to the URL in the addDimension call. For example, the browser displaying London in the banner attempts to go to www.london.com.

Note If you are using the Captive Portal application, the browser’s original request is honored instead of this location-based attribute.

Configuring Personal Firewalls

This section describes how to configure the SESM personal firewall feature. Topics are:

- Overview of SESM Personal Firewalls, page 5-26
- Configuring the NWSP My Firewall Page, page 5-27

Overview of SESM Personal Firewalls

The SESM firewall feature provides a way for subscribers to restrict or permit traffic to and from their connection by making choices on a web portal page. The portal page presents a list of applications that are available for firewall protection. The SESM deployer configures the list of applications using the Firewall MBean.

Deployers can also configure firewall controls for subscribers which cannot be changed by the subscriber. Administrators use CDAT to configure these controls.

Required Deployment Options

These firewall features are supported only when SESM is running in LDAP mode with an RDP that is running in default (non-Proxy) mode.

Underlying Technology

The underlying technology for the SESM personal firewall feature is extended access control lists (ACLs) added as attributes in subscriber profiles in an LDAP directory.

The ACLs are stored in the subscriber profiles as standard RADIUS attribute with number 26 (vendor specific attribute), subattribute number 1 (Cisco AV-pair). A subscriber profile might have many ACL entries, which together determine which traffic is permitted and denied on the connection.

The ACLs are added to the profile in two ways:

- When a subscriber configures firewall settings from the SESM portal, the portal creates the appropriate ACLs to support the subscriber's choices. The created ACLs are grouped by application, with one ACL per chosen protocol and control direction (upstream or downstream). The ACLs allow traffic to and from *any* source and destination IP address, for a given protocol and port number. (The subscriber does not have the means to enter specific IP addresses when configuring a personal firewall.)
- In the case of deployer imposed firewall settings, the administrators manually create the correctly formatted ACLs and enter them in CDAT. The ACLs entered in CDAT can use the full range of ACL options as described in the Cisco IOS documentation.

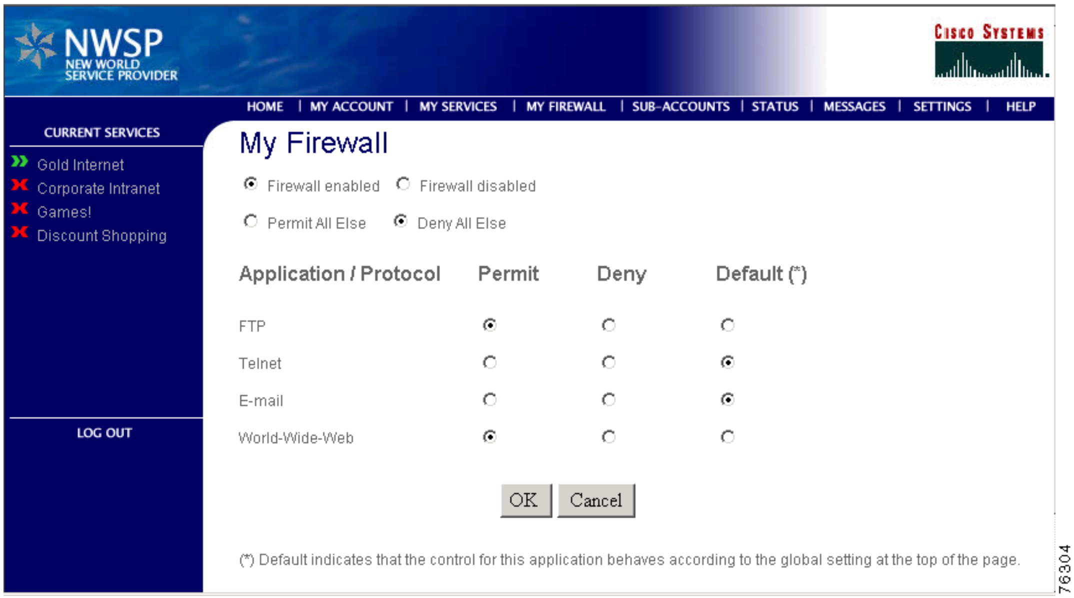
SESM and SSG implement the firewall as follows:

- The subscriber logs into the SESM portal.
- The logon request is accepted by SESM and passes through the SSG to RDP.
- During authentication processing, RDP obtains the subscriber profile from the directory and adds all of the profile information, including the ACLs, in the access request it sends back to the SSG.
- The SSG applies the ACLs against traffic to and from the subscriber's connection.

Configuring the NWSP My Firewall Page

Figure 5-1 shows the My Firewall page.

Figure 5-1 My Firewall Page in NWSP


NWSP
NEW WORLD SERVICE PROVIDER
CISCO SYSTEMS
HOME | MY ACCOUNT | MY SERVICES | MY FIREWALL | SUB-ACCOUNTS | STATUS | MESSAGES | SETTINGS | HELP
CURRENT SERVICES
Gold Internet
Corporate Intranet
Games!
Discount Shopping
LOG OUT
OK
Cancel
76304

My Firewall

● Firewall enabled ○ Firewall disabled

○ Permit All Else ● Deny All Else

Application / Protocol	Permit	Deny	Default (*)
FTP	●	○	○
Telnet	○	○	●
E-mail	○	○	●
World-Wide-Web	●	○	○

(*) Default indicates that the control for this application behaves according to the global setting at the top of the page.

Installed Default Setup of My Firewall Page

The default state of a subscriber profile is one in which no ACLs are defined. If the subscriber profile has no ACL attributes defined, then the first time the subscriber goes to the My Firewall page, the settings are:

- Firewall disabled is selected
- Deny all else is selected
- All applications are set to default

Changing the My Firewall Settings

This section describes how SESM determines the initial display on the My Firewall page and how to change it.

Firewall Enabled/Disabled Button

The Firewall Enabled/Disabled button is set to:

- Enabled if there are any ACLs in the subscriber profile.

  The ACLs in the subscriber profile could be the result of subscriber activity on this page or from administrators entering administrative ACLs in CDAT.
- Disabled if there are no ACLs in the subscriber profile.

The initial state of a subscriber profile is no ACLs. ACLs in the profile can be removed by:

- The deployer, by removing the ACL attributes using CDAT.
- The subscriber, by clicking the Disabled button. This deletes all ACLs from the profile, including any administrative ACLs that were created by the deployer.

Note We recommend removing this radio button from the My Account page for deployments that want to offer both subscriber and administrative firewall settings. See the "Restrictions" section on page 5-30 for more information.

Permit/Deny All Else Button

The Permit/Deny All Else button always initially appears with Deny All Else chosen.

Application/Protocol List

The Application/Protocol field on the My Firewall page is configured by the deployer as follows:

- The applications that appear in the list are configured in the Firewall MBean. See the "Firewall MBean" section on page 5-11 for more information.
- The displayed text that represents an application in the list is configured as a resource bundle in the portal application's directory. For example, for NWSP, resources are in:

  nwsp/docroot/WEB-INF/classes/messages[_*locale*].properties.

  The portal searches its resource bundles for the resource *firewallAppName*Description, where *firewallAppName* is the application defined in the Firewall MBean. If a matching resource is not found, then *firewallAppName* is displayed on the My Firewall page. For example, consider the following firewall application:

  www

  The portal searches for a resource named wwwDescription, and displays the text in the appropriate language on the My Firewall page. (In the installed files, this is World-Wide-Web for the en locale.) If the wwwDescription resource does not exist, then www appears on the My Firewall page.

The displayed state of the Permit/Deny/Default buttons for each application is set by the SESM portal application. For each application:

- If no ACLs exist or if only one ACL exists in the subscriber's profile for an application, the Default button is turned on. In a typical production deployment, most applications initially appear in the default state, because there are no specific ACLs in the subscriber profiles.
- If an application has more than one ACL in the subscriber profile:
  - If all ACLs have the same permission (that is, all are Permit or all are Deny), then that radio button is turned on for that application.
  - Otherwise, if some ACLs specify permit and others deny, then the Default button is turned on for that application.

Sample My Firewall Page Settings and Resulting ACLs

Suppose the subscriber clicks the following buttons on the My Firewall page (see Figure 5-1):

- Firewall Enabled
- Deny All Else

- Application/Protocol settings:
  - FTP default
  - Telnet permit
  - E-mail default
  - World-Wide-Web permit

The ACLs that support the above application settings, as viewed in CDAT, are:

```
Cisco_AV:ip:inacl#138=permit tcp any any eq 443
Cisco_AV:ip:inacl#196=deny ip any any
Cisco_AV:ip:outacl#196=deny ip any any
Cisco_AV:ip:inacl#128=permit tcp any any eq 23
Cisco_AV:ip:outacl#129=permit tcp any any established
Cisco_AV:ip:inacl#138=permit tcp any any eq 80
```

This configuration sets ACLs on the in (upstream) path. It also sets an ACL on TCP for the out (downstream) path for TCP, allowing a return path only for established connections. This means that a return path only exists for connections that the user has started and it blocks connections that are attempted to be started from outside.

Creating Subscriber-Configured Personal Firewalls

Subscribers create their personal firewalls by clicking radio buttons on the My Firewall page. The new ACLs do not take effect until a subscriber reauthenticates (logs out and logs in again). Also, the RDP cache must be refreshed, which by default takes 10 minutes. Due to the possibility of just having missed a refresh, the minimum guaranteed time is double the cache refresh time.

The ACLS that SESM creates from input on the My Firewall page are referred to here as application ACLs. In SESM Release 3.1(5), all ACLs created from input on the My Firewall page allow all addresses in both the source and destination fields.

The ACLs created by SESM are in the following form:

*direction*acl#*ACLnumber*=*permission protocol* any any eq *portNumber*

Where:

- *direction* is in or out, depending on the value in the direction attribute in the Firewall MBean.
- acl# is a required constant.
- *ACLnumber* is in the range from 110 to 196. SESM assigns the ACL number when it creates a new ACL.
- *permission* is one of the following values:
  - permit
  - deny
- *protocol* is the configured protocol for the application, as defined in the Firewall MBean. Examples are tcp, udp, ip, and so on.
- “any any”specifies that all source and all destination IP addresses are subject to the control being defined in this ACL.

Note Finer control is intended for future releases.

- *portNumber* is the port number related to the protocol, as defined in the Firewall MBean.

Creating Deployer-Imposed Firewalls

This section describes how to configure and use the administrative firewall feature. It includes the following topics:

- Restrictions, page 5-30
- Removing the Disable Button from the My Firewall Page, page 5-30
- Entering ACLs in CDAT, page 5-31
- ACL Format for CDAT Entries, page 5-31

Restrictions

Deployer imposed firewalls can be used in conjunction with the subscriber self-configured firewalls, with the following restrictions:

- You should customize the NWSP My Firewall page to remove the Disable button.

  The Disable button removes all ACLs from the subscriber profile, including the ACLs that were entered by administrators.

Warning **By using the Disable button, a subscriber can delete the deployer-imposed restrictions on the account.**

- You should test the ACLs before moving them to a production environment.

  In SESM Release 3.1(5), deployer imposed firewalls are implemented by entering the correctly formatted ACLs in CDAT. CDAT does not analyze or validate your ACL entry.

  The RDP validates RADIUS attributes before it adds the attributes to the authentication message returned to SSG. The RDP stops processing a profile if it finds an attribute that is incorrectly formatted.

Warning **An incorrectly formatted ACL entered through CDAT can prevent a subscriber from logging into the SESM portal.**

- You should create ACLs using ACL numbers in the range from 100 to 109.

  The ACL numbers from 100 to 109 are reserved for administrator use. By using these numbers, you ensure that these ACLs are processed first, making them the highest priority.

  If you create ACLs in CDAT using ACL numbers in the range from 110 to 196, (the ACLs reserved for use by the subscriber self-configured ACLs), you risk the following:

  – You might interfere with the personal firewall settings created by the subscriber.

  – You provide the opportunity for the subscriber to reverse your settings.

Removing the Disable Button from the My Firewall Page

The Disable button on the My Firewall page deletes all ACLs from the subscriber profile.

- If you are using administrative firewalls in combination with subscriber-configured firewalls, remove this button from a production deployment to ensure that subscribers can not delete administrative firewalls.
- If you are not planning to use administrative firewalls, leave this button to provide subscribers with an easy way to remove ACLs, and also reduces the load on the SSG.

To remove the Disable Button from the My Firewall page in NWSP, use the following procedure:

Step 1 Make sure a JDK is installed.

Step 2 Edit the nwsp/docroot/pages/firewallBody.jsp.

Step 3 Comment out lines 51 through 66.

Step 4 Recompile the JSP as described in "Recompiling a Customized JSP" section on page 10-8 or precompile the JSP using the precompile script in:

```
tools
    bin
        precompile
```

Entering ACLs in CDAT

To enter deployer-imposed ACLs, use the following procedure:

Step 1 Start the CDAT application.

Step 2 Access the subscriber or group profile.

Step 3 Enter the ACLs in the Local RADIUS attribute field, using the format described in the following section.

Step 4 If a subscriber is currently logged into an SESM session, the new ACLs do not take effect until the subscriber reauthenticates (logs out and logs in again). Also, the RDP cache needs to be refreshed, which by default takes 10 minutes. Due to the possibility of just having missed a refresh, the minimum guaranteed time is double the cache refresh time.

ACL Format for CDAT Entries

This section describes the format of the firewall entries in the Local RADIUS attribute field in CDAT. The general format for the Local RADIUS attribute field is:

attribute:*value*

In the case of the firewall ACL entries:

- *attribute* is Cisco_AV
- *value* is the ACL whose format is described below

The format of the ACLs entered by administrators is:

Cisco_AV:ip:*direction*acl#*ACLnumber*=*permission protocol source destination*

Where:

- *direction* is one of the following:
  - in
  - out
- acl# is a required string
- *ACLnumber* is in the range from 100 to 109. The numbers indicate priority in the ACL evaluation. ACLs with the lowest numbers are analyzed first. The order is important because ACL processing stops when the first match occurs.

  ACLs whose numbers are in the range 100 to 109 will have higher priority than any ACLs created by subscribers using the My Firewall page. (The range of ACL numbers reserved for use by the My Firewall page is 110 to 196.)

  ACLs whose numbers are in the range 100 to 109 cannot be modified by the subscriber (because the My Firewall page will not modify ACLs whose numbers are in that range), although the subscriber can delete those ACLs along with all others with the Disable Firewall button.

Note If you intend to use both the deployer-imposed ACLs and the subscriber ACLs in a production deployment, you should modify the My Firewall page to remove the Disable button. See the "Removing the Disable Button from the My Firewall Page" section on page 5-30.

- *permission* is one of the following values: permit or deny
- *protocol* is the configured protocol for the application, as defined in the Firewall MBean. Examples are tcp, udp, ip, and so on.
- *source* and *destination* are in the form:

  {any | *IPaddress mask*} [*portOperator portNumber*]

  where *portOperator* values are: lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range). The range operator requires two port numbers. All other operators require one port number.

In the following examples, the first one, with ACL number 100, was set by the deployer. The other s were generated by SESM based on actions from the My Firewall page.

```
Cisco_AV:ip:inacl#100=deny tcp any 10.0.0.0 0.0.0.0 eq 80
Cisco_AV:ip:outacl#196=deny ip any any
Cisco_AV:ip:inacl#128=permit tcp any any eq 23
Cisco_AV:ip:outacl#129=permit tcp any any established
Cisco_AV:ip:inacl#138=permit tcp any any eq 80
```

Note There is an implicit deny at the end of an ACL list. When an ACL list exists, only explicitly permitted traffic is permitted.

More Access Control List Information

The SESM firewall feature creates extended ACLs. For more information about ACL formats and processing, refer to the Cisco IOS documentation on extended ACLs. The following references point to documentation for Cisco IOS Release 12.2:

- Configuration Guide—In the *Configuring IP Services* guide, see the "Filtering IP Packets Using Access Lists" section. The online link is:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt1/1cfip.htm#xtocid14

- Command reference—In the *Cisco IOS IP Command Reference, Volume 1 of 3, Addressing and Services*, see the "IP Services Commands" section. The online link is:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipras_r/1rfip1.htm