Chapter 22

Installing and Configuring Enterprise Service Portals

This chapter describes how to install and configure the enterprise service portals, and contains the following sections:

- Before You Install an Enterprise Service Portal on page 333
- Installing Enterprise Service Portals on page 334
- Writing an Application to Allow a Machine to Provide Public IP Addresses for NAT on page 343
- Configuring an Enterprise Service Portal Audit Plug-In on page 344

Before You Install an Enterprise Service Portal

Before you install the enterprise service portal:

- Identify the machine on which you want to install the application.

  If you plan to use Enterprise Manager Portal and NAT Address Management Portal, which work together but serve different purposes, you must install both portals. You can install these portals on the same or different machines.

- Install a Web application server on the machine on which you want to install the enterprise service portal.

  We provide the JBoss Web application server in the SRC software distribution. For information about installing this software, see *SRC-PE Getting Started Guide, Chapter 38, Installing Web Applications*.

- If you use JBoss or another Web application server that performs load balancing, you must configure the Web application server to use *sticky sessions* to process requests to the enterprise service portal.

Sticky sessions are sessions between a server and client in which information is preserved between different transactions in an activity. When a server establishes a session for an activity with a particular client, the Web application server preserves session information by sending subsequent requests from the client to the same server. For enterprise service portals, use of sticky sessions ensures that the Web application server always routes requests from IT managers to the same instance of the enterprise service portal that they logged into.

For information about configuring sticky sessions for the Web application server, see the documentation for your Web application server.

- Determine how you will identify the SAE that manages a subscriber who connects to the SRC network through an enterprise service portal (see *Identifying the SAE* on page 319). If you will use a network information collector (NIC) for this purpose, configure a NIC that takes the distinguished name (DN) of an access and returns the corresponding SAE reference (for more information about the NICs, see *SRC-PE Network Guide, Chapter 9, Locating Subscriber Information with the NIC*).

- Install the sample data from the SRC software distribution (see *SRC-PE Getting Started Guide, Chapter 34, Defining an Initial Configuration on a Solaris Platform*).

- In the directory, create any new namespaces for the enterprise service portals you will install. For information about namespaces, see ***Chapter 21, Planning Deployment for Enterprise Service Portals***. To create a namespace, you can copy one of the enterprise service portal configurations included with the same data to another location in the directory.

Installing Enterprise Service Portals

Tasks to install an enterprise service portal are:

1. Preparing the Web Applications for Customization on page 335
2. Configuring Connections to the Directory on page 335
3. (Enterprise Manager Portal only) Configuring Deployment Settings for Enterprise Manager Portal on page 337
4. Deploying the Enterprise Service Portals on page 343
5. Configuring the URL for an Enterprise Service Portal on page 343

After you install an enterprise service portal:

- If you use a machine to administer public IP addresses in conjunction with NAT Address Management Portal, write an application to handle the interaction between the machine and this portal. See *Writing an Application to Allow a Machine to Provide Public IP Addresses for NAT* on page 343.

- If you use Enterprise Manager Portal, NAT Address Management Portal, or an application that uses a configuration file based on the easp_conf template, see *Configuring an Enterprise Service Portal Audit Plug-In* on page 344.

Preparing the Web Applications for Customization

When customizing the Web applications, copy the WAR files to a temporary folder and work in that folder.

To copy the WAR file to a temporary folder:

1. Login as `root` or another authorized user.
2. Create a temporary folder in which you will work on the WAR file. For example:

   mkdir tempWar

3. Access the temporary folder. For example:

   cd tempWar

4. Copy the WAR file to the temporary folder.

   cp /cdrom/cdrom0/webapp/<filename>

   <filename>—Name of the WAR file; for example, *entmgr.war*

Configuring Connections to the Directory

To configure a connection between the Web application and the directory that contains the configuration for the enterprise service portal:

1. Access the temporary folder to which you copied the WAR file.

   cd tempWar

2. Extract the *boot.props* file from the WAR file.

   jar xvf <filename> WEB-INF/boot.props

   <filename>—Name of the WAR file; for example, *entmgr.war*

3. Edit the *boot.props* file with any text editor; use the following property descriptions as guidelines.
4. Replace the *boot.props* file in the WAR file.

   jar uvf <filename> WEB-INF/boot.props

Initialization Properties for Enterprise Service Portals

In the boot properties file for an enterprise service portal, you can modify the following fields.

Config.java.naming.provider.url

- URL of the primary directory in URL string format.
- Value—ldap:// < host > : < portNumber > /
  - < host > —IP address or name of the host that supports the directory
  - < portNumber > —Number of the TCP port
- Default—ldap://127.0.0.1:389/

Config.java.naming.security.credentials

- Password that the Web application server uses to authenticate and authorize access to the directory.
- Value— < password >
- Guidelines—The password can be encoded in base64 and not visible in plain text. To use an encoded value, use the format {BASE64} < encoded-value > .
- Default—ent

Config.java.naming.security.principal

- DN that contains the username that the Web application server uses to authenticate and authorize access to the directory.
- Value—DN of the object that contains the username
- Default—*cn = ent-admin, o = operators, o = umc*

Config.net.juniper.smgt.des.backup_provider_urls

- Redundant directories that store configuration information.
- Value—List of URLs in URL string format separated by semicolons (see description for the property Config.java.naming.provider.url)
- Default—ldap://127.0.0.1:389/; ldap://127.0.0.1:389/

Config.net.juniper.smgt.des.<propertySuffix>

- Set of properties that specify how the Web application interacts with the directory.
- Value—See *SRC-PE Getting Started Guide, Chapter 37, Distributing Directory Changes to SRC Components on a Solaris Platform*.
- Default—See *SRC-PE Getting Started Guide, Chapter 37, Distributing Directory Changes to SRC Components on a Solaris Platform*.

Config.net.juniper.smgt.lib.config.staticConfigDN

- Root of the static configuration properties.
- Value—DN of the object that contains the username
- Default—*ou = staticConfiguration, ou = configuration, o = Management, o = umc*

Config.EASP.namespace

- Location of the enterprise service portal's configuration in the directory.
- Value—Path, relative to the root of the static configuration properties, that defines the location
- Guidelines—If you are using the enterprise service portals we provide, use the defaults, which match the locations of the configurations in the sample data.
- Default—Depends on the enterprise service portal:
  - Sample Enterprise Service Portal—/EASP
  - Enterprise Manager Portal—/EASP/ENT-MGR
  - NAT Address Management Portal—/EASP/NAT-ADDR

Configuring Deployment Settings for Enterprise Manager Portal

You configure deployment settings for Enterprise Manager Portal. You do not need to configure deployment settings for the sample Enterprise Service Portal or NAT Address Management Portal.

To configure deployment settings for Enterprise Manager Portal:

1. Access the temporary folder to which you copied the WAR file.

   cd tempWar

2. Extract the *web.xml* file from the WAR file.

   jar xvf entmgr.war WEB-INF/web.xml

3. Edit the *web.xml* file in the *entmgr.war* file with any text editor; use the following property descriptions as guidelines.

   This file specifies which applications Enterprise Manager Portal displays and specifies how to generate e-mails when IT managers request public IP addresses through this enterprise service portal.

4. Replace the *web.xml* file in the WAR files.

   jar uvf entmgr.war WEB-INF/web.xml

Deployment Properties for Enterprise Manager Portal

In the *web.xml* deployment properties file for Enterprise manager Portal, you can modify the following fields.

showBasicBandwidthOnDemand

- Whether or not the enterprise service portal displays basic bandwidth-on-demand (BoD) features.
- Value
  - True—Displays the basic BoD features
  - False—Hides the basic BoD features

- Guidelines—Specify True if you want to provision basic BoD with a JUNOS routing platform. When enabled, service providers can offer basic BoD services to IT managers as service options that affect all traffic on an access link, including customizing the amount of bandwidth provided to meet their traffic requirements.

  To make class of service (CoS) services available, BoD services and basic BoD services must be enabled. If both are enabled, IT managers must select a basic BoD service before they can subscribe to BoD services.

- Default—True

showBandwidthOnDemand

- Whether or not the enterprise service portal displays BoD features.
- Value
  - True—Displays the BoD features
  - False—Hides the BoD features
- Guidelines—Specify True if you want to provision BoD with a JUNOS routing platform. To make CoS services available, BoD services and basic BoD services must be enabled. If both are enabled, IT managers must select a basic BoD service before they can subscribe to BoD services.
- Default—True

showFirewall

- Whether or not the enterprise service portal displays firewall features.
- Value
  - True—Displays the firewall features
  - False—Hides the firewall features
- Guidelines—Specify True if you want to provision firewall services with a JUNOS routing platform.

  If you set showFirewall to True and statelessFirewall to False, the portal provides support for stateful firewalls on JUNOS routing platforms.

- Default—True

statelessFirewall

- Whether or not the enterprise service portal displays stateless firewall features.
- Value
  - True—Displays the stateless firewall features
  - False—Hides the stateless firewall features

- Guidelines—Specify True if you want to provision firewall services on a JUNOS routing platform. The showFirewall field must also be set to True.

  When you set statelessFirewall to True, the Firewall tab but not the Application tab appears in Enterprise Manager Portal.

  You can configure either stateless firewalls or stateful firewalls from Enterprise Manager Portal. If you set showFirewall to True and statelessFirewall to False, the portal provides support for stateful firewalls on JUNOS routing platforms.
- Default—True

showNat

- Whether or not the enterprise service portal displays NAT features.
- Value
  - True—Displays the NAT features
  - False—Hides the NAT features
- Guidelines—Specify True if you want to provision NAT services with a JUNOS routing platform. If this property is set to True, the enterprise service portal always displays the firewall features, regardless of the value of the showFirewall property.
- Default—True

showSchedule

- Whether or not the enterprise service portal displays scheduling features for services.
- Value
  - True—Displays the scheduling features
  - False—Hides the scheduling features
- Default—True

showVpn

- Whether or not the enterprise service portal displays VPN features.
- Value
  - True—Displays the VPN features
  - False—Hides the VPN features
- Guidelines—Specify True if you want to provision VPNs with a JUNOS routing platform. If you set this property to True, you must also set the showBandwidthOnDemand property to True.
- Default—True

showExtranet

- Whether or not the enterprise service portal displays VPN extranet features.
- Value
  - True—Displays the VPN extranet features
  - False—Hides the VPN extranet features
- Guidelines—Specify True if you want to provision VPN extranets with a JUNOS routing platform. If you set this property to True, you must also set the showVPN property to true.
- Default—True

junoseCompatibleBoD

- Whether or not the enterprise service portal can be used to configure BoD services on JUNOSe routers.
- Value
  - True—Provides configuration for BoD services on JUNOSe routers
  - False—Does not provide configuration for BoD services on JUNOSe routers
- Guidelines—If set to true, this field allows BoD services to be configured for JUNOSe routers as well as JUNOS routing platforms. This setting limits the configuration for IP protocol, source IP address, source port or port range, destination IP address, and destination port or port range for a BoD rule to one each for JUNOS routing platforms as well as JUNOSe routers. The online help indicates that users can specify one value for these fields if **junoseCompatibleBoD** is set to True, and that users can specify more than one value for these fields if **junoseCompatibleBoD** is set to False.

  Consider that if both JUNOS routing platforms and JUNOSe routers exist in an enterprise's network, IT managers who are using the enterprise service portal to configure their SRC-managed environment do not know which routers are JUNOSe routers and which are JUNOS routing platforms.

- Default—False

machineReadableNotifications

- Format of the e-mails that indicate that public addresses have been requested or released for a particular access link.
- Value
  - True—E-mails contain XML code and will be handled by a machine.
  - False—E-mails contain ordinary text and will be handled by a human administrator.
- Default—False

renotificationInterval

- Minimum time between e-mails that notify the service provider about outstanding requests for IP addresses.
- Value—Number of seconds in the range 1–2147483647
- Guidelines—For actual SRC implementations that use a human administrator, we recommend a value of 86400 seconds (1 day). For demonstrations of the SRC software that use a human administrator, we recommend a value of 240 seconds. For actual SRC implementations that use machines, the value depends on how you design an application to handle the e-mails; a value of 600 seconds (10 minutes) may be a good starting point.
- Default—120
- Example—200

addressManagerUrl

- URL of NAT Address Management Portal that the service provider uses to manage public IP addresses for enterprises. This value is included in the e-mails about IP addresses.
- Value—URL in the format

  http://<host>:<port><path>

  - <host>—Name or IP address of the machine on which you install the Web application for NAT Address Management Portal
  - <port>—TCP/UDP port for HTTP traffic
  - <path>—Path to location of the Web application
- Default—http://example.com:8080/nataddr/AddressManager

mail.smtp.host

- SMTP mail server that Enterprise Manager Portal uses to send e-mails about requests for or release of public IP addresses.
- Value—Name or IP address of the mail server
- Default—mailhost

notificationFrom

- Sender's address in e-mails that Enterprise Manager Portal sends about public IP addresses.
- Value—Text string that specifies the sender's name and e-mail address in XML format
- Guidelines—Be sure to use the correct XML escape sequences for any special characters in the value.
- Default—"Enterprise Portal" <entMgrPortal@example.com >

notificationTo

- Human administrator or machine to which Enterprise Manager Portal should send e-mails about requests for or release of public IP addresses.
- Value—Text string that specifies the name and e-mail address of the human administrator or machine in XML format
- Guidelines—Be sure to use the correct XML escape sequences for any special characters in the value.
- Default—"Public IP Address Manager" <ipManager@example.com >

notificationSubject

- Text used for the subject of e-mails about requests for or release of public IP addresses.
- Value—Text string that specifies the subject of the e-mail in XML format
- Guidelines—This value is not used if you configure e-mails to be machine-readable notifications. Be sure to use the correct XML escape sequences for any special characters in the value.
- Default—An IP request or release needs your attention.

renotificationSubject

- Text used for the subject of reminders to administrators about requests for or release of public IP addresses.
- Value—Text string that specifies the subject of the e-mail in XML format
- Guidelines—This value is ignored if you configure e-mails to be machine-readable notifications. Be sure to use the correct XML escape sequences for any special characters in the value.
- Default—REMINDER: An IP request or release still needs your attention.

notificationText

- Text that appears in the body of the e-mail.
- Value—Text string in XML format that specifies the body of the e-mail message
- Guidelines—This text and the URL appear in the body of the message if you specify that the e-mails are not machine-readable notifications. Otherwise, the URL appears in the subject, and the body is an XML document indicating which access needs attention. Be sure to use the correct XML escape sequences for any special characters in the value.
- Default—Please click on the link in this e-mail to go to a Web page where you will be able to fulfill a customer's request for public IP addresses, or acknowledge a customer's release of public IP addresses.

maxIpPoolSize

- Maximum number of public IP addresses that you can include in the pool that is used for the dynamic source NAT service.
- Value—Integer in the range 0–2147483647
- Guidelines—Configure this property if you want to provide NAT addresses through NAT Address Management Portal. Consult the JUNOS documentation for information about the maximum for each JUNOS routing platform.
- Default—32

Deploying the Enterprise Service Portals

The way you deploy the enterprise service portals depends on your Web application server.

If you are using a Web application server other than JBoss, see the documentation for your Web application server for information about the deployment.

For information about installing the enterprise service portal inside the JBoss Web application server, see *SRC-PE Getting Started Guide, Chapter 38, Installing Web Applications*.

Configuring the URL for an Enterprise Service Portal

By default, the name of the WAR file determines the URL that you use to access the enterprise service portal. For example, if the name of the WAR files is *entmgr.war*, the URL for the enterprise service portal is http://<host>:<port>/entmgr.

- <host>—Name or IP address of the machine on which you install the enterprise service portal
- <port>—TCP/UDP port for HTTP traffic

If you want use a different URL, you must modify the relevant configuration file for your Web application server. For information about this task, see the documentation for your Web application server.

Writing an Application to Allow a Machine to Provide Public IP Addresses for NAT

If you use Enterprise Manager Portal and NAT Address Management Portal, and you use a machine to administer public IP addresses that you provide to enterprises.

To use a machine to administer public IP addresses:

1. Write an application that handles:
   - E-mails from Enterprise Manager Portal
   - XML messages that NAT Address Management Portal uses to communicate with the software that manages the IP addresses

For information about the XML messages, see *NAT Address Management Portal* on page 320.

2. Install the application that you created in Step 1on a machine that contains the software for managing IP addresses.

Configuring an Enterprise Service Portal Audit Plug-In

The SRC software provides a sample event listener, DefaultAuditEventListener. You can use the sample listener, customize it, or use the information in the sample to create another audit plug-in. The sample event listener is in the SRC software distribution in the directory */SDX/doc/ent/plugindoc/net/juniper/smgt/ent/plugin*. The sample listener sends output to a log file. See the documentation for the plug-in in the SRC software distribution in the folder */SDX/doc/ent/plugindoc* or on the Juniper Networks Web site at

http://www.juniper.net/techpubs/software/management/sdx/api-index.html

If you create an audit plug-in, you add the plug-in class to the WAR file for the enterprise service portal.

Table 34 shows the common information that is provided by every enterprise service portal audit plug-in event.

Table 34: Common Audit Plug-In Information

Information	Description
Manager DN	Distinguished name that identifies the manager's profile in the directory; for example: *cn = unimgr, enterprisename = jnpr, ou = local, retailername = default, o = users, o = umc*
Manager principle	Manager's fully qualified log-in principle for logging in to the enterprise portal. For example, the equivalent principle for the Manager DN above is: unimgr@jnpr/local.default
Operation time	Time when the corresponding operation was successfully completed.

Table 35 describes the events that an audit plug-in listener can listen for and the information reported in those events.

Table 35: Events Reportable to the Audit Plug-In

Event	IT Manager Action That Initiates Event	Information Reported
ManagerLoginEvent	Logs in to an enterprise service portal.	Common information only.
ManagerLogoutEvent	Logs out of an enterprise service portal.	Common information only.
SubscribeAuditEvent	Subscribes to a service.	Common information plus: ■ DN of the new subscription object in the directory. ■ Attributes of the new subscription, including sspState, sspAction, and parameterSubstitution.
UnsubscribeAuditEvent	Unsubscribes from a service.	Common information plus: ■ DN of the subscription object removed from the directory. ■ Attributes of the removed subscription, including sspState, sspAction, and parameterSubstitution.
SubscriberUpdateAuditEvent	Changes the parameterSubstitution attribute of a subscriber object, such as adding or removing a substitution from the IT manager's enterprise object.	Common information plus: ■ DN of the subscriber object that is changed. ■ Attributes changed in the operation, including the old values and new values of the attributes.

SubscriptionUpdateAuditEvent	Changes the parameterSubstitution attribute of a subscription object; suspends, resumes, activates, or deactivates a subscription.	Common information plus:
		■ DN of the subscription object that is changed.
		■ Old and new values of the changed attributes:
		  ■ parameterSubstitution attribute when subscriber object is changed.
		  ■ sspState attribute when subscription is suspended or resumed.
		  ■ sspAction attribute when subscription is activated or deactivated.

Table 35: Events Reportable to the Audit Plug-In (continued)

Event	IT Manager Action That Initiates Event	Information Reported
ServiceOpStateAuditEvent	Changes the operational state of a session. **NOTE:** Because changing the operational state of the session—such as dynamically activating or deactivating a subscription session—does not change the directory entry, the change is not persistent, and the subscription session returns to its administrative state after the subscriber's interface is restarted. Changes to the administrative state of a subscription are reported with the SubscriptionUpdateAuditEvent.	Common information plus: ■ DN of the subscriber that owns the subscription session. The subscriber must be a leaf in the subscriber tree in the enterprise scenario. ■ DN of the subscription object where the subscription session comes from. ■ Operational state of the session after the IT manager's action.
ExportAuditEvent	Exports a VPN.	Common information plus: ■ DN of VPN that is exported. ■ DN of the subscriber to which the VPN is exported.
UnexportAuditEvent	Cancels the export of a VPN.	Common information plus: ■ DN of VPN for which export is canceled. ■ DN of the subscriber for which export of the VPN was canceled.