

Chapter 17

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 295
- Installing Enterprise Service Portals on page 296
- Writing an Application to Allow a Machine to Provide Public IP Addresses for NAT on page 305
- Configuring an Enterprise Service Portal on page 306
- Configuring an Enterprise Service Portal Audit Plug-In on page 316

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 SDX software distribution. For information about installing this software, see *SDX Getting Started Guide, Chapter 11, 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 SDX network through an enterprise service portal (see *Identifying the SAE* on page 281). 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 NICs, see *SDX Network Guide: SAE, Juniper Networks Routers, and NIC, Chapter 5, Locating Subscriber Information*).
- Install the sample data from the SDX software distribution (see *SDX Getting Started Guide, Chapter 6, Defining an Initial Configuration*).
- In the directory, create any new namespaces for the enterprise service portals you will install. For information about namespaces, see *Chapter 16, 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 297
2. Configuring Connections to the Directory on page 297
3. (Enterprise Manager Portal only) Configuring Deployment Settings for Enterprise Manager Portal on page 299
4. Deploying the Enterprise Service Portals on page 305
5. Configuring the URL for an Enterprise Service Portal on page 305

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 305.
- 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* on page 306.

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.smgmt.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.smgmt.des.<propertySuffix>

- Set of properties that specify how the Web application interacts with the directory.
- Value—See *SDX Getting Started Guide, Chapter 14, Distributing Directory Changes to SDX Components*.
- Default—See *SDX Getting Started Guide, Chapter 14, Distributing Directory Changes to SDX Components*.

Config.net.juniper.smgmt.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 SDX-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 SDX implementations that use a human administrator, we recommend a value of 86400 seconds (1 day). For demonstrations of the SDX software that use a human administrator, we recommend a value of 240 seconds. For actual SDX 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 *SDX Getting Started Guide, Chapter 11, 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 282*.

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

Configuring an Enterprise Service Portal

Follow the configuration instructions in this section for:

- Enterprise Manager Portal
- NAT Address Management Portal
- An application that uses a configuration file based on the `easp_conf` template

Tasks to configure an enterprise service portal are:

1. Accessing the Configuration Files on page 306
2. Configuring Connections to the Subscriber Directory on page 307
3. Configuring Connections to the Service Directory on page 310
4. Configuring Search Bases for Each Directory on page 312
5. Configuring the Logging Properties on page 314
6. (Optional) Configure a NIC proxy if you use a NIC to identify the SAEs that manage subscribers. See Configuring a NIC Proxy on page 314.
7. (Optional) Configure directory eventing if you use directory eventing to identify the SAEs that manage subscribers. See Configuring Directory Eventing for SAE Identification on page 315.
8. Exporting the Configuration to the Directory on page 316

If you use an enterprise service portal audit plug-in with your application, also complete the following task:

- Configuring an Enterprise Service Portal Audit Plug-In on page 316

Accessing the Configuration Files

Use SDX Configuration Editor to configure properties for enterprise service portals. For information about using SDX Configuration Editor, see *SDX Getting Started Guide, Chapter 17, Using SDX Configuration Editor*.

To access the enterprise service portal configuration:

1. Start SDX Configuration Editor.
2. Import the sample data from the directory.
3. Open the folder called enterprise service portal.
4. Open the file for the enterprise service portal that you want to configure.

Configuring Connections to the Subscriber Directory

To configure the connections to the directory that contains information about subscribers:

1. Click the LDAP tab in the configuration file.

The LDAP pane appears.

The screenshot shows the LDAP configuration interface. The 'User Data' section is expanded, revealing the following fields and their values:

- Server Address: 127.0.0.1
- Server Port: 389
- Authentication DN: cn=ent-admin,o=operators,o=umc
- Password: *** (with a 'Show' button)
- Enable SNMP Monitoring: No
- Secured LDAP protocol: [checked] (with a 'Disable' button)
- Filter for loading subscriptions: Subscriber Reference Filter
- Session Usage Refresh Time Interval: 900

Below the 'User Data' section, there are two collapsed sections: 'Service Data' and 'Search Base'.

2. Expand the entry called User Data, and configure the properties for the directory that contains information about subscribers.
3. Save the file.

Server Address

- List of subscriber directories. The first entry is the primary directory, and the rest are backup directories.
- Value—Space-separated list of IP addresses or names of hosts that support subscriber directories
- Guidelines—If one directory contains both subscribers and services, be sure to use the same value for this field in both the User Data entry and the Service Data entry.
- Default—127.0.0.1
- Property name—ent.repository.ldap.subscriber.server.address

Server Port

- Port number for the subscriber directory servers. The primary host and all backup directory hosts must use this port.
- Value—TCP port
- Guidelines—If one directory contains both subscribers and services, be sure to use the same value for this field in both the User Data entry and the Service Data entry.
- Default—389
- Property name—ent.repository.ldap.subscriber.server.port

Authentication DN

- DN for authentication with the subscriber directory.
- Value—DN
- Default—*cn = ent-admin, o = operators, o = umc*
- Property name—ent.repository.ldap.subscriber.manager.authDN

Password

- Password for authentication with the subscriber directory.
- Value—Text string
- Default—ent
- Property name—ent.repository.ldap.subscriber.manager.password

Enable SNMP Monitoring

- Whether or not information about enterprise service portal directory connections to the SNMP directory connection table if an SDX SNMP agent is running on the same host as the enterprise service portal.
- Value
 - Yes—Enable SNMP monitoring.
 - No—Do not enable SNMP monitoring.
- Default—No
- Property name—ent.repository.ldap.subscriber.des.enable_sysman

Secured LDAP Protocol

- Security protocol that the enterprise service portal uses to connect to the subscriber directory.
- Value—ldaps
- Default—ldaps
- Property name—ent.repository.ldap.subscriber.manager.security.protocol

Filter for Loading Subscriptions

- Filter that the SAE uses when it loads sample enterprise data from the subscriber directory.
- Value—One of the following filters:
 - Subscriber Reference Filter—The SAE runs a search based on the subscriberRef attribute in the umcServiceProfile object class, which is the base object class of the service profile hierarchy. The subscriberRef attribute contains a DN that points to the parent of the subscriber object.
 - Subscription Objectclass Filter—The SAE performs a one-level search with the directory entry, which represents the subscriber folder as the base DN. The search filter is (objectClass = sspServiceProfile). This method can be slow if you have a large number of subscription entries within the subscriber folder subtree.
- Guidelines—If you use a directory that does not search efficiently for large numbers of subscribers, specify the Subscriber Reference Filter. Otherwise, use the Subscription Objectclass Filter.
- Default—Subscription Objectclass Filter
- Property name—ent.repository ldap.subscriber.server.loadSubscriptionFilter

Session Usage Refresh Time Interval

- How often the enterprise service portal contacts the SAE to obtain updates for usage data. The SAE obtains this data from the router.
- Value—Number of seconds in the range 0 to 2147483647
- Guidelines—If you specify a lower value than the default, you may cause a denial-of-service attack on the router.
- Default—900
- Example—1200

Configuring Connections to the Service Directory

To configure the connections to the directory that contains information about subscribers:

1. Click the LDAP tab in the configuration file.

The LDAP pane appears.

The screenshot shows the LDAP configuration interface. It is divided into sections: 'User Data' (expanded), 'Service Data' (collapsed), and 'Search Base' (collapsed). The 'Service Data' section is currently visible, containing the following fields:

- Server Address: 127.0.0.1
- Server Port: 389
- Authentication DN: cn=ent-admin,o=operators,o=umc
- Password: *** (with a 'Show' button)
- Enable SNMP Monitoring: No
- Secured LDAP protocol: (with a 'Disable' button)
- Enable Directory Eventing: Yes
- Polling Interval: 60

2. Expand the entry called Service Data, and configure the properties for the directory that contains information about subscribers.
3. Save the file.

Server Address

- List of service directories. The first entry is the primary directory, and the rest are backup directories.
- Value—Space-separated list of IP addresses or names of hosts that support service directories
- Guidelines—If one directory contains both subscribers and services, be sure to use the same value for this field in both the User Data entry and the Service Data entry.
- Default—127.0.0.1
- Property name—ent.repository.ldap.service.server.address

Server Port

- Port number for the service directory servers. The primary host and all backup directory hosts must use this port.
- Value—TCP port number
- Guidelines—If one directory contains both subscribers and services, be sure to use the same value for this field in both the User Data entry and the Service Data entry.
- Default—389
- Property name—ent.repository.ldap.service.server.port

Authentication DN

- DN for authentication with the service directory.
- Value—DN
- Default—*cn = ent-admin, o = operators, o = umc*
- Property name—ent.repository.ldap.service.manager.authDN

Password

- Password for authentication with the service directory.
- Value—Text string
- Default—ent
- Property name—ent.repository.ldap.service.manager.password

Enable SNMP Monitoring

- Whether or not to add Information about enterprise service portal directory connections to the SNMP directory connection table if an SDX SNMP agent is running on the same host as the enterprise service portal.
- Value—Yes or No
- Default—No
- Property name—ent.repository.ldap.service.des.sysman

Secured LDAP protocol

- Whether or not the enterprise service portal uses a security protocol to connect to the service directory.
- Value—LDAPS
- Guidelines—If the connection to the directory is secure, click Enable to enforce use of LDAPS. Click Disable if the connection to the directory is not secure.
- Default—ldaps
- Property name—ent.repository.ldap.service.manager.security.protocol

Enable Directory Eventing

- Whether or not enterprise service portal uses directory eventing to identify the SAE that manages a subscriber.
- Value
 - Yes—Enterprise service portal uses directory eventing to identify the SAE.
 - No—Enterprise service portal does not use directory eventing to identify the SAE.
- Guidelines—Set this property to Yes if you use directory eventing to identify the SAE that manages a subscriber. Set this property to No for NAT Address Management Portal, and for other enterprise service portals if you use a NIC to identify the SAE that manages a subscriber.
- Default—Yes
- Property name—ent.repository ldap.service.des.enable_eventing

Polling Interval

- Time between polls that the enterprise service portal sends to the directory to obtain changes to the addresses of the SAEs' external interfaces.
- Value—Number of seconds in the range 15–2147483647
- Guidelines—Use the default value unless the response time of the directory is unacceptably long. In this case, use a higher value than the default. Do not use a lower value than the default.
- Default—60
- Property name—ent.repository ldap.service.des.pollinginterval

Configuring Search Bases for Each Directory

You configure the base DN's of information that the enterprise service portal uses in each directory.

To configure the search bases (the base DN's in the directory that store particular types of information):

1. Click the LDAP tab in the configuration file.

The LDAP pane appears.

The screenshot shows the LDAP configuration interface. It has a tree view on the left with three main sections: 'User Data', 'Service Data', and 'Search Base'. The 'Search Base' section is expanded, showing a list of properties with corresponding text input fields:

- Subscribers
- Services
- Global Parameters
- Operators
- Service Scopes
- Network

- Expand the entry called Search Base, and configure the properties under this entry.
- Save the file.

Subscribers

- Base DN of subscribers in the directory.
- Value—DN
- Default—*o = users, o = umc*
- Property name—`ent.repository.subscribers.base.dir`

Services

- Base DN of services in the directory.
- Value—DN
- Default—*o = services, o = umc*
- Property name—`ent.repository.services.base.dir`

Global Parameters

- Base DN of the global parameters for policies in the directory.
- Value—DN
- Default—*o = parameters, o = umc*
- Property name—`ent.repository.parameters.base.dir`

Operators

- Base DN of operators in the directory.
- Value—DN
- Default—*o = operators, o = umc*
- Property name—`ent.repository.managers.base.dir`

Service Scopes

- Base DN of service scopes in the directory.
- Value—DN
- Default—*o = scopes, o = umc*
- Property name—ent.repository.scopes.base.dir

Network

- Base DN of networks in the directory.
- Value—DN
- Default—*o = network, o = umc*
- Property name—ent.repository.network.base.dir

Configuring the Logging Properties

To configure logging properties:

1. Click the Logging tab in the configuration file.

The Logging pane appears.

2. Configure the logging properties.

You can see default settings for logging in this file. For information about configuring logging, see *SDX Monitoring and Troubleshooting Guide, Chapter 2, Configuring Logging for SDX Components*.

3. Save the file.

Configuring a NIC Proxy

If you use a NIC to identify the SAEs that manage subscribers, configure a NIC proxy for the enterprise service portal. Do not configure a NIC proxy for NAT Address Management Portal, because it does not need to identify the SAEs that manage subscribers.

To configure a NIC proxy:

1. Click the SAE Resolution tab in the configuration file.
2. Expand the entry called NIC Proxy, and configure the properties under this entry.

For information about configuring NIC proxies, see *SDX Network Guide: SAE, Juniper Networks Routers, and NIC, Chapter 7, Configuring Applications to Communicate with an SAE*.

3. Save the file.

Configuring Directory Eventing for SAE Identification

For SDX implementations that use five or fewer SAEs, you can configure the enterprise service portal to use directory eventing to identify the SAEs that manage subscribers. Do not configure this feature for NAT Address Management Portal, because it does not need to identify the SAEs that manage subscribers. To configure directory eventing for SAE identification:

1. Click the SAE Resolution tab in the configuration file.

2. Expand the entry called Polling-based SAE Resolution, and configure the properties under this entry.
3. Save the file.
4. Be sure that the property `ent.feedback.urlupdateinterval` is configured in the SAE configuration (see *Modifying the SAE Property File* on page 43).

SAE Keepalive Check Interval in Seconds

- Time interval at which the enterprise service portal polls the SAE.
- Value—Number of seconds in the range 0–2147483647
- Guidelines—Specify a value that exceeds the interval at which the SAE updates the address of its external interface (configured in the property `ent.feedback.urlupdateinterval` in SAE properties).
- Default—5400
- Example—6000
- Property name—`ent.saewatchdog_timeout`

SAE References

- DN of the subtree that contains the addresses of the external interface of remote SAEs.
- Value—DN
- Default—`ou = sspadmurls, o = servers, o = umc`.
- Property name—`ent.feedback.admin.baseDN`

Exporting the Configuration to the Directory

For information about exporting the configuration to the directory, see *SDX Getting Started Guide, Chapter 17, Using SDX Configuration Editor*. Enterprise service portal configurations are exported to *l = EASP, ou = staticConfiguration, ou = Configuration, o = Management, o = umc*.

Configuring an Enterprise Service Portal Audit Plug-In

The SDX 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 SDX software distribution in the directory `/SDX/doc/ent/plugin/doc/net/juniper/smg/ent/plugin`. The sample listener sends output to a log file. See the documentation for the plug-in in the SDX software distribution in the folder `/SDX/doc/ent/plugin/doc` 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 31 shows the common information that is provided by every enterprise service portal audit plug-in event.

Table 31: Common Audit Plug-In Information

Information	Description
Manager DN	Distinguished name that identifies the manager's profile in the directory; for example: <i>cn = unimgr, enterprisename = jnpr, ou = local, retailername = default, o = users, o = umc</i>
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: <i>unimgr@jnpr/local.default</i>
Operation time	Time when the corresponding operation was successfully completed.

Table 32 describes the events that an audit plug-in listener can listen for and the information reported in those events.

Table 32: 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: <ul style="list-style-type: none"> ■ DN of the new subscription object in the directory. ■ Attributes of the new subscription, including <code>sspState</code>, <code>sspAction</code>, and <code>parameterSubstitution</code>.

Table 32: Events Reportable to the Audit Plug-In (continued)

Event	IT Manager Action That Initiates Event	Information Reported
UnsubscribeAuditEvent	Unsubscribes from a service.	Common information plus: <ul style="list-style-type: none"> ■ 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: <ul style="list-style-type: none"> ■ 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: <ul style="list-style-type: none"> ■ DN of the subscription object that is changed. ■ Old and new values of the changed attributes: <ul style="list-style-type: none"> ■ parameterSubstitution attribute when subscriber object is changed. ■ sspState attribute when subscription is suspended or resumed. ■ sspAction attribute when subscription is activated or deactivated.
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: <ul style="list-style-type: none"> ■ 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: <ul style="list-style-type: none"> ■ 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: <ul style="list-style-type: none"> ■ DN of VPN for which export is canceled. ■ DN of the subscriber for which export of the VPN was canceled.

Overview of Configuration for an Enterprise Service Portal Audit Plug-In

You must configure the properties for an enterprise service portal audit plug-in in configuration for an enterprise service portal. If you use the sample or create a plug-in based on the sample, use SDX Configuration Editor to configure the plug-in. If you customize the plug-in to use additional API properties, use an LDAP browser or SDX Admin to customize the plug-in.

Configuring the Sample Enterprise Service Portal Audit Plug-In

Use SDX Configuration Editor to configure properties for an enterprise service portal audit plug-in, also referred to as the Enterprise Access Service Portal (EASP) audit plug-in, based on the sample.

Before you configure the properties, define the Java class for the plug-in. You can also configure the Java logging utility provided by JDK 1.4 to record the log messages. For more information about this utility, see

<http://java.sun.com/j2se/1.4.1/docs/api/java/util/logging/FileHandler.html>

To configure the audit plug-in:

1. Start SDX Configuration Editor.

For information about using SDX Configuration Editor, see *SDX Getting Started Guide, Chapter 17, Using SDX Configuration Editor*.

2. Import the SDX system configuration from the directory.
3. Open a file for an enterprise service portal:
 - *ENT-MGR.xml* in the *EASP* folder
 - *NAT-ADDR.xml* in the *EASP* folder
 - File that uses the *easp_conf* template
4. Click the EASP Audit Plug-In tab.

The EASP Audit Plug_In pane appears.

EASP Audit Plugin	
<input type="checkbox"/> Audit Plugin	
Plug-in Class	net.juniper.smg.ent.plugin.DefaultAuditEventListener
Log Destination	audit%g.log
Maximum File Size	100000
Log File Count	3
Log File Append Mode	Append <input checked="" type="checkbox"/>

5. Use the following descriptions to complete the fields in the Audit Plug-in area.
6. Save the file.
7. Export the SDX system configuration from the directory.



NOTE: You can also use SDX Admin to modify Enterprise Service Portal audit plug-in properties. See *Configuring a Customized Enterprise Service Portal Audit Plug-In* on page 320.

Plug-in Class

- Fully qualified name of the Java class for the Enterprise Service Portal audit plug-in event listener. If you implement your own plug-in event listener, set this property to the Java class of your listener. This property is mandatory for all Enterprise Service Portal audit plug-ins.
- Value—Text string
- Default—net.juniper.smg.ent.plugin.DefaultAuditEventListener
- Property name—Plugin.EASPAudit.class

Log Destination

- Path to the log file (relative to the folder where you installed the Enterprise Service Portal audit plug-in) and the pattern of the filename.
- Value—Text string, with the following special characters:
 - /—Separator for names in the path
 - %t—System’s temporary folder
 - %h—Current user’s home folder
 - %g—Generated number for this log file
 - %u—Unique number for this log file
 - %%—Percent sign
- Default—audit %g/log
- Property name—Plugin.EASPAudit.log.file.pattern

Maximum File Size

- Maximum number of bytes that the event listener can write to a file.
- Value—Number of bytes in the range 0–2147483647
- Default—10000
- Property name—Plugin.EASPAudit.log.file.limit

Log File Count

- How many log files the event listener should use.
- Value—Integer in the range 0–2147483647

- Default—3
- Property name—Plugin.EASPAudit.log.file.count

Log File Append Mode

- Whether or not the event listener should add to or replace the exiting information in the log file.
- Value
 - Append—Event listener should add new information to existing information.
 - Overwrite—Event listener should replace existing information.
- Default—Append
- Property name—Plugin.EASPAudit.log.file.append

Configuring a Customized Enterprise Service Portal Audit Plug-In

If you have customized the Enterprise Service Portal audit plug-in to use additional properties in the API, you must configure the plug-in with an LDAP browser or SDX Admin. To do so:

1. Start the LDAP browser or SDX Admin.
2. Access the file *I = EASP, ou = StaticConfiguration, ou = Configuration, o = Management, o = umc*.
3. Find the section that contains the properties with the prefix Plugin.EASPAudit.
4. Modify the existing properties in the file.

Each field description in the previous section includes a property name for the existing properties.

5. Add the properties that you included in the customized portal; be sure to include the prefix Plugin.EASPAudit for each property.
6. Specify appropriate values for the custom properties.
7. Save the file.