Sun Java System Portal Server 7.1 Configuration Guide

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 819–5025–10
March 2007

070918@18741

Contents

Preface

The Sun Java™ System Portal Server 7.1 Configuration guide explains how to install and configure Portal Server on different scenarios.

Who Should Use This Book

This guide is meant for administrators and other individuals installing and using this version of the product.

Before You Read This Book

Before you read this book, see the *Sun Java System Portal Server 7.1 Release Notes*.

Default Paths and File Names

The following table describes the default paths and file names used in this Guide.

TABLE P–1 Default Paths and File Names

Term	Description
PortalServer-base	Represents the base installation directory for a previous version of Portal Server . The software default base installation and product directory depends on your specific platform: Solaris™ systems `/opt`
PortalServer7–base	Represents the base installation directory for this version of Portal Server . The software default base installation and product directory depends on your specific platform: Solaris systems `/opt`

TABLE P–1 Default Paths and File Names *(Continued)*

Term	Description
AccessManager-base	Represents the base installation directory for Sun Java System Access Manager. The Access Manager default base installation and product directory depends on your specific platform: Solaris systems: `/opt/SUNWam`
DirectoryServer-base	Represents the base installation directory for Sun Java System Directory Server. Refer to the product documentation for the specific path name.
ApplicationServer-base	Represents the base installation directory for Sun Java System Application Server. Refer to the product documentation for the specific path name.
WebServer-base	Represents the base installation directory for Sun Java System Web Server. Refer to the product documentation for the specific path name.

Related Third-Party Web Site References

Third-party URLs are referenced in this document and provide additional, related information.

Note – Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Documentation, Support, and Training

The Sun web site provides information about the following additional resources:

- Documentation (`http://www.sun.com/documentation/`)
- Support (`http://www.sun.com/support/`)
- Training (`http://www.sun.com/training/`)

Typographic Conventions

The following table describes the typographic conventions that are used in this book.

TABLE P–2 Typographic Conventions

Typeface	Meaning	Example
`AaBbCc123`	The names of commands, files, and directories, and onscreen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% you have mail.`
`AaBbCc123`	What you type, contrasted with onscreen computer output	`machine_name%` **`su`** `Password:`
aabbcc123	Placeholder: replace with a real name or value	The command to remove a file is `rm` *filename*.
AaBbCc123	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the *User's Guide*. A *cache* is a copy that is stored locally. Do *not* save the file. **Note:** Some emphasized items appear bold online.

Shell Prompts in Command Examples

The following table shows the default UNIX® system prompt and superuser prompt for the C shell, Bourne shell, and Korn shell.

TABLE P–3 Shell Prompts

Shell	Prompt
C shell	`machine_name%`
C shell for superuser	`machine_name#`
Bourne shell and Korn shell	`$`
Bourne shell and Korn shell for superuser	`#`

◆ ◆ ◆ CHAPTER 1

Installing Sun Java System Portal Server 7.1

Sun Java™ System Portal Server 7.1 can be installed using the Installer in two modes: Configure Now mode or Configure Later mode. If you install in the Configure Now mode, the installation and configuration take place simultaneously.

Note – For the default installation of Portal Server, the user should be the root user. A non-root user can install Portal Server in the Configure Later mode.

This chapter contains information about installing Sun Java System Portal Server 7.1 in the Configure Now mode.

This chapter contains the following topics:

Checking Hardware and Software Requirements

This section contains the requirements for installing Sun Java System Portal Server 7.1.

Note – The installation instructions are specific to the Solaris platform. Refer to the Installation guide for Windows if you are installing Portal Server on the Windows.

Hardware and Operating System Requirements

The following table lists hardware and operating system requirements:

TABLE 1–1 Hardware and Operating System Requirements

Component	Platform Requirement
Supported platforms	Sun Blade™ or comparable workstation or server
Operating system	Solaris™ 9 or Solaris 10 on SPARC
	Solaris 9 or Solaris 10 on x86
	Red Hat Enterprise Linux 3.0 Update 3 or 4.0 on x86
	Windows
	Note: Portal Server 7.1 on Windows can only be used as a developer platform or an evaluation platform. It can not be used as a deployment platform.
RAM	1.5 Gbytes for regular deployment on Sun Java System Web Server
	2.0 Gbytes for regular deployment on Sun Java System Application Server
Disk space	1 Gbyte for Portal Server and associated applications
Swap space	Twice the amount of physical memory, for example, 2.0 Gbytes RAM and 4.0 Gbytes swap space.

Before Installing on Linux

- Remove the link `/usr/share/bdb/db.jar` before installation, if it exists.
- Check `ant` already exists on the system by running the following command:

  ```
  rpm -qa | grep ant
  ```

  If a version of `ant` below 1.6 is installed, remove it by running the following command:

  ```
  rpm -e ant-older-version ant-libs-older-version
  ```

  You need to use the version of ant `sun-ant-1.6.5-2` to install or deploy Portal Server. When you run the installer, it is automatically installed at `/opt/sun/bin/ant`.

Software Requirements

Portal Server requires the following stack components:

- Sun Java System Directory Server 6
- Sun Java System Access Manager 7 installed in legacy mode not in realm mode.

Portal Server requires Access Manager, Directory Server, and a web container for its installation and configuration. If you are performing a fresh install, Access Manager and Directory Server do not have to be installed before Portal Server is installed. Access Manager, Directory Server, and Portal Server can be installed at the same time. If Access Manager and Directory Server are installed already, point the Portal Server installation and configuration to the existing Directory Server and Access Manager servers.

- Sun Java System Web Server 6.x or Sun Java System Application Server 8.x.

Note – Access Manager must be installed in legacy mode before installing Portal Server 7.1.

For detailed instructions for installing the stack components, see the *Sun Java Enterprise System 5 Installation Reference for UNIX*.

Miscellaneous Checks

1. If the system on which you installed Portal Server does not have direct connectivity to the internet, an HTTP proxy needs to be specified. For example, for Sun Java System Application Server, specify the following in the `domain.xml` file:

   ```
   <jvm-options>-Dhttp.proxyHost=proxy-host</jvm-options>
   <jvm-options>-Dhttp.proxyPort=proxy-port</jvm-options>
   <jvm-options>-Dhttp.nonProxyHosts="portalserver-host"</jvm-options>
   ```

   For Web Server 7.0, add this options to `server.xml` of the configuration in which portal is deployed. For IBM WebSphere, add this to the `server.xml` of the node in which portal is deployed. For WebLogic, add this to `startWeblogic.sh/startManagedWeblogic.sh` depending on whether the portal is to be installed on administrator server or managed server.

   Where, *proxy-host* is the fully qualified domain name of the proxy host, *proxy-port* is the port on which the proxy is run, and *portalserver-host* is the fully qualified domain name of the Portal Server software host.
2. Execute the command `prtconf | grep Memory` to check RAM.
3. Use the command `swap -l` to see how much swap space your machine has. To temporarily increase your swap space by 4 Gbytes, you can use the following instructions:

   ```
   mkfile 4g /swap-filename
   swap -a /swap-filename
   ```

where *swap-filename* is an empty file to be used as a swap area.

Installing Portal Server 7.1

Some post installation configuration tasks require you to use values that you entered during the installation. Keep these values available for configuration.

Note – If you install Portal Server on a root local zone, install shared components in global zone.

If you install Portal Server on Sparse local zone, install shared components and Message Queue in global zone if you use Application Server as a web container. If you use Web Server as the web container, install only shared components in global zone.

▼ To Install Sun Java System Portal Server 7.1

1. **From the installation location, go to the *OS-arch* directory, where *OS-arch* can be `Solaris_sparc`, `Solaris_x86`, or `Linux_x86`.**

2. **Run `./installer` to invoke the wizard to install the software.**

3. **In the Welcome screen, click Next.**

4. **In the Software License Agreement screen, read the agreement and click Yes, Accept License.**

5. **The Choose Software Components screen appears. Select Portal Server 7.1.**

   When this option this selected, the following components are selected by default:

   - The Directory Preparation Tool
   - Service Registry 3.1
   - Access Manager 7.1 and related sub components of Identity Management and Policy Services
   - Directory Server Enterprise Edition 6.0 including the Directory Server Core
   - Java DB 10.2

6. **Select the other software components that you want to install.**

   - To install Secure Remote Access (SRA) services, select Portal Server Secure Remote Access 7.1. When you select this option, the Gateway, Netlet Proxy, and the Rewriter Proxy are selected by default.
   - To install Application Server, select Application Server Enterprise Edition 8.2 . When you select this option, the Domain Administration Server, Command Line Administration Tool, and Sample Applications for the Application Server are selected by default. The Application Server High Availability Session Store 4.4 and Sun Java System Message Queue 3.7 UR1 are also selected by default.

Note – Select this option if you need EJB container for portal.

- To install Web Server, select the Sun Java System Web Server 7.0. When you select this option, the Web Server CLI, Web Server Core, and Web Server Samples are selected by default.

Note – Select this option if you require only Web Applications.

- To install multilingual support for the selected Java ES components, select Install Multilingual Packages for Selected Component(s).

Note – If J2SE-SDK or any shared components require upgrade, the installer displays the corresponding screens. By default, installer upgrade them with the latest version in the installer disk.

7 The Shared Component Upgrades Requires screen is displayed if any one of the shared components requires upgrading. Click Next to upgrade these shared components.

8 On the Specify Installation Directories page, specify the installation directory for the software. The following are the default locations. Use the Browse button to change the default location. Click Next.

Access Manager	`/opt`
Application Server	`/opt/SUNWappserver`
Application Server: Data and Configuration	`/var/opt/SUNWappserver`
Directory Server	`/opt/SUNWdsee`
Directory Preparation Tool	`/opt/SUNWcomds`
Web Server	`/opt`
Web Server Instance	`/var/opt/SUNWwbsvr7`
Service Registry	`/opt`
Portal Server	`/opt`

The Verify System Requirements screen is displayed. The installer verifies each of the listed system requirements and displays OK if the requirements are met. If the installer indicates that all the requirements are met, the System Ready for Installation message appears. Click Next to continue with the installation. In case any of the requirements are not met, a text indicating the same appears with the following options: View Reports and Check Again. The View Report

option provides the details about the requirements that are not met. It is recommended that you address these issues. After the requirements are met, click the Check Again option to verify whether the requirements are met.

Click Next to continue the installation.

The Choose a Configuration Type screen is displayed.

9 Select Configure Now, and click Next.

The installer only supports adding one portal and one instance only. For any other configuration, the Configure Later option must be selected. If the Configure Now option is selected, after the packages are installed, the configuration starts immediately.

Select Configure Now, and click Next.

The Custom Configuration screen is displayed.

10 Service Registry 3.1 and Java DB are not configured during the installation. It can be configured after the installation. Click Next.

The Specify Administrator Account Preferences screen is displayed.

11 Enter the Administrator ID and password. Type the password, and click Next.

You are also provided with an option to select different administrator accounts for each product.

The Specify Common Server Settings screen is displayed.

12 Specify the following server settings:

Host Name, DNS Domain Name, and Host IP Address
: Host name, domain, and IP address of the system. The installer automatically displays these values.

System User and Group
: System user name and group ID. For Solaris 10 OS and Linux, the default is `root` for system user name and `root` for group ID. For Solaris 9 OS, the default is `root` for system user name and `other` for group ID.

Note – Values you enter here appear as default values during the rest of the installation.

---

13 If you have selected Web Server as a component to install, the Choose Configuration Type screen is displayed. You have an option to configure administration instance as a server or as a node. By default, configure administration instance as server is selected. Click Next.

14 If you have selected Web Server as a component to install, the Web Server: Specify Administration Server Settings and Web Server: Specify Instance Settings screens are displayed. Provide the information for Web Server, and click Next.

Note – Specify the Runtime Unix user ID as `root`.

You need to specify the following details for the Web Server: Specify Administration Server Settings screen:

Server Host	The default value is automatically created by joining the values that you provided for Host Name and DNS Domain Name under Common Server Settings. The value has the format `hostname.domainname`.
SSL Port	The default value is `8989`.
HTTP Port	Port on which Web Server listens for HTTP connections. The default is `8800`.
Runtime User ID	User ID that the default instance of Web Server uses to run on the system. The default is `root`.

You need to specify the following details for the Web Server: Specify Instance Settings screen:

Server Name	A host and domain value that resolves to the local host. The value has the format `hostname.domainname`.
HTTP Port	Port on which Web Server listens for HTTP connections. The default value is `80`.
Runtime UNIX User ID	An existing non-root user. If you are installing Access Manager or Portal Server, set this value to `root` and set the Runtime Group to `other`. You can change these values after installation. For other servers, the Runtime User ID should be a non-root user. The default value is `webservd`.
Document Root Directory	Location where Web Server stores content documents. For Solaris OS, the default value is `/var/opt/SUNWwbsvr7/docs`. For Linux and HP-UX, the default value is `/var/opt/sun/webserver7/docs`.

15 The High Availability Session Store (HADB): Specify Configuration Data screen is displayed. The Installer displays the default values. This screen is displayed only if you have selected Application Server as a component to install. Click Next.

HADB Management Port

Port on which the HADB management listens. The default value is `1862`.

HADB Resource Directory
: Location where HADB stores resource contents. The default value is `/var/opt`.

HADB Administrator Group
: The UNIX group (GID) in which the default instance of HADB runs as a user. The default value is `other`.

Automatically start HADB when system starts
: Choose this option to direct the installer to configure HADB to start automatically when the system restarts. By default, this is selected.

Allow Group Management
: Choose this option when you want HADB to be managed by the HADB Administration Group. If this parameter is set to `yes`, all members belonging to the group (`HADB_DEFAULT_GROUP`) can run and manage HADB. By default, it is set to `No`.

The Application Server: Domain Administration Server screen is displayed.

16 Provide or change values in the installer pages as needed and click Next.

The installer displays the default values. This screen is displayed only if you have selected Application Server as a component to install.

Admin Port	Port on which Application Servers administrative server listens for connections. By default, it is `4849`.
JMX Port	The default is `8686`.
HTTP Port	The default value is `8080`. If the installer detects that the default port is used, an alternative value is suggested.
HTTPS Port	The default is `8181`.
Master Password	SSL certificate database password, used for asadmin operations such as Domain Administration Server startup and Node Agent startup. The default value is the Administrator Password you provided under Common Server Settings.

The Application Server: Node Agent screen is displayed.

17 Specify the details and click Next.

This screen displays only if you have selected Application Server as a component to install.

Admin Host Name	Host name for administration server which the node agent can connect to.
Admin User Name	User ID of the Application Server admin user. The default value is the Administrator User ID you provided under Common Server Settings. If you chose to use a single administrator account, this field is not present.

Password	Password for the Application Server admin user. There is no default value. If you chose to use a single administrator account, this field is not present.
Master Password	SSL certificate database password, used for asadmin operations such as Domain Administration Server startup and Node Agent startup. There is no default value.
Admin Port	Port on which Application Servers node agent listens for connections. Provides access to the administration tools. The default value is 4849.
Node Agent Name	Name of the local node. The default value is the local host name

The Application Server: Configure Load Balancing Plugin screen is displayed.

18 Specify the details and click Next.

This screen displays only if you have selected Application Server as a component to install.

Web server that the load balancing plugin will use
: You can select either Sun Java System Web Server or Apache Web Server. HP-UX does not support Apache Web Server.

Web server installation directory
: Installation directory for Web Server or Apache HTTP Server.

  The default value is:

  - Solaris OS: `/opt/SUNWwbsvr7`
  - Linux and HP-UX: `/opt/sun/webserver7`

Web Server instance directory
: Installation directory for Web Server or Apache HTTP Server.

  The default value is:

  - Solaris OS: `/var/opt/SUNWwbsvr7`
  - Linux and HP-UX: `/var/opt/sun/webserver7`

The Directory Server: Specify Instance Creation Information screen is displayed.

19 Specify the information for Directory Server instance creation and click Next.

Instance Directory	Location of new instance.
Directory Instance Port	The default value is 389.
Directory Instance SSL Port	The default value is 636.

Directory Manager DN	Distinguished Name (DN) of the user who has unrestricted access to Directory Server. The default value is `cn=Directory Manager`.
System User	The default value is `root`.
System Group	The default value is `root`.
Directory Manager Password	Password for the directory manager.
Suffix	Initial directory suffix managed by this instance. The default value is formed by the segments of the fully qualified domain name for the current host. For example, if you install on `siroe.sub1.example.com`, the default value is `dc=sub1,dc=example,dc=com`.

For more information, see "Directory Server Configuration Information" in *Sun Java Enterprise System 5 Installation Reference for UNIX*.

The Access Manager: Specify Configuration Information screen is displayed.

20 Specify the information for the Access Manager configuration and click Next.

Install type	Indicates the level of interoperability with other components. You have a choice of Realm mode (version 7 style) or Legacy mode (version 6 style). Default option is Legacy mode. You must use Legacy mode if you are installing Access Manager with Portal Server, Messaging Server, Calendar Server, Delegated Administrator, or Instant Messaging. The default value for Legacy mode is Enabled. The default for Realm mode is Disabled.

Note – Portal Server supports Realm mode only if Sun Java System Directory Server is used as a user repository and Access Manager SDK is configured as the datastore plugin for the Realm mode. If you select the Configure Now option for the Realm mode, the installer does this by default.

Administrator User ID	Access Manager's top-level administrator. This user has unlimited access to all entries managed by Access Manager. The default name, `amadmin`, cannot be changed. This ensures that the Access Manager administrator role and its privileges are created and mapped properly in Directory Server, allowing you to log into Access Manager immediately after installation.
Administrator Password	Password of the `amadmin` user. The value must have at least eight characters.

LDAP User ID	Bind DN user for LDAP, Membership, and Policy services. This user has read and search access to all Directory Server entries. The default user name, `amldapuser`, cannot be changed.
LDAP Password	Password of the `amldapuser` user. This password must be different from the password of the `amadmin` user. It can be any valid Directory Service password.
Password Encryption Key	A string that Access Manager uses to encrypt user passwords. For security purposes, it is recommended that the password encryption key be 12 characters or longer.

Note – `amAdmin` and `amldapuser` password should be different.

For more information, see the "Access Manager Configuration Information" in *Sun Java Enterprise System 5 Installation Reference for UNIX*.

Note – Portal Server supports installing Access Manager in the Realm mode or in the Legacy mode.

The Access Manager: Choose Deployment Container screen is displayed.

21 You can select either Sun Java System Web Server or Sun Java System Application Server. Select the option, and click Next.

For more information about configuring Web Server, see the "Web Server Configuration Information" in *Sun Java Enterprise System 5 Installation Reference for UNIX* in *Sun Java Enterprise System 5 Installation Reference for UNIX*.

For more information about configuring Application Server, see the *Sun Java Enterprise System 5 Installation Reference for UNIX*

The Access Manager: Specify Sun Java System Application Server screen is displayed.

22 Specify the details and click Next.

This screen is displayed only if you have selected Sun Java System Application Server as the web container for Access Manager.

Secure Server Instance Port	Specify whether the value for Instance Port refers to a secure port. A secure port uses the HTTPS protocol. A non-secure port uses HTTP.
Secure Administration Server Port	Specify whether the value for Administrator Port is a secure port. A secure port uses the HTTPS protocol. A non-secure port uses HTTP.

The Access Manager: Specify Web Container for Running Access Manager Services screen is displayed.

23 Specify the details for Access Manager and click Next.

Host Name	Fully qualified domain name of the host on which you are installing.
Services Deployment URI	Uniform Resource Identifier (URI) prefix for accessing the HTML pages, classes, and Java Archive (JAR) files associated with the Identity Management and Policy Services Core subcomponent. The default value is `amserver`. Do not enter a leading slash.
Common Domain Deployment URI	URI prefix for accessing the common domain services on the web container. The default value is `amcommon`. Do not enter a leading slash.
Cookie Domain	The names of the trusted DNS domains that Access Manager returns to a browser when Access Manager grants a session ID to a user. A leading dot (.) is required for each domain in the list. The default value is the current domain, prefixed by a dot (.).
Password Deployment URI	URI that determines the mapping that the web container running Access Manager will use between a string you specify and a corresponding deployed application. The default value is `ampassword`. Do not enter a leading slash.
Console Protocol	Specify whether the console uses a secure or unsecure port. A secure port uses the HTTPS protocol. A non-secure port uses HTTP. The default is HTTP.

The Access Manager: Choose Access Manager Console screen is displayed.

Note – This screen is displayed only if you select the Legacy mode to install Access Manager.

---

24 By default, Deploy New Console is selected. Click Next.

Administration Console	Choose Deploy new console to deploy the console into the web container of the host on which Access Manager is being installed. Choose Use existing console to use an existing console that is deployed on a remote host.
Console Deployment URI	URI prefix for accessing the HTML pages, classes, and JAR files associated with the Access Manager Administration Console subcomponent.The default value is `amconsole`.

Console Host Name	Fully qualified domain name for the server hosting the existing console. This value is not needed if you are deploying a new console. You can edit the field only if you are using an existing console.
Console Port	Port on which the existing console listens for connections. Permitted values are any valid and unused port number, in the range 0 (zero) through 65535.

The Access Manager: Choose Directory Server Instance screen is displayed.

25 Use the Directory Server Instance that you just created. Click Next.

Note – If you choose to use an existing instance instead of the default, the alternate instance must already be configured.

The Access Manager: Specify Directory Server Data screen is displayed.

---

26 You can select Yes or No for the option: Is Directory Server is Provisioned with User Data. By default, No is selected. If you select Yes, you need to provide the related information. Click Next.

27 If you have selected Application Server as the deployment container for Access Manager, the Specify Sun Java System Application Server Information screen is displayed. Click Next.

Secure Server Instance Port	This protocol specifies whether the value for Server Instance port refers to a secure port. A secure port uses the `HTTPS` protocol. A non-secure port uses `HTTP`.

The Portal Server: Specify Web Container Deployment Information screen is displayed.

28 Specify the Web Container deployment information and click Next.

Portal Access URL	The default is *host name:port/portal1*.
Portal ID	The default is `portal1`.
Search ID	The default is `search1`.
Deployment URI	The default is `/portal`.
Portal Instance ID	The default is `hostname-8080`.

Select the Enable Secure Remote Access option, if you wish to enable Secure Remote Access. Select Developer Sample, Enterprise Sample, and Community Sample if you wish to configure samples.

The Portal Server: Secure Remote Access screen is displayed. The Portal Server: Secure Remote Access: Configure Gateway screen is displayed.

29 Enter the following information and click Next.

Gateway Protocol	It is https by default.
Portal Server Domain Name	Portal Server domain name.
Gateway Domain	Gateway domain.
Gateway Port	It is 443 by default.
Gateway Profile Name	It is `default` by default.
Log User Password	The user password

30 Specify the details and click Next.

Protocol	Protocol (HTTP or HTTPS) the gateway uses to communicate. In most cases the gateway should use `HTTPS`.
Host Name, Subdomain, and Domain	The name, subdomain, and domain name of the machine on which the Gateway proxy resides. By default, the system values are used.
Host IP Address and Access Port	The host IP address on which the Gateway Proxy resides. By default, the IP address is the IP address of the system and port is `443`.
Gateway Profile Name	The gateway profile name. By default, the gateway profile name is `default`.

The Portal Server: Secure Remote Access: Configure Netlet Proxy screen is displayed.

31 Specify the following information for the Netlet Proxy.

Host Name, Subdomain, and Domain	The name, subdomain, and domain name of the machine on which the Netlet proxy resides. By default, the system values are used.
Host IP Address and Access Port	The host IP address on which the Netlet Proxy resides. By default, the IP address is the IP address of the system and port is `10555`.
Gateway Profile Name	The gateway profile name. By default, the gateway profile name is `default`.

Click Next.

The Portal Server: Secure Remote Access: Configure Rewriter Proxy screen is displayed.

32 Specify the following information to install the Rewriter Proxy.

Host Name, Subdomain, and Domain	The host name, subdomain, and domain name of the machine on which the Rewriter Proxy resides. By default, the system values are used.
Host IP Address and Access Port	The Host IP address and access port of the machine on which the Rewriter Proxy resides. By default, the IP address is the IP address of the system and port is `10443`.
Gateway Profile Name	The gateway profile name. By default, the gateway profile name is `default`.

Click Next.

The Portal Server: Secure Remote Access: Specify Certificate Information screen is displayed.

33 Specify the following certificate information for the Secure Remote Access.

Organization, Division, City/Locality, State/Province
: The organization name, division, city, and state information.

Country Code
: The country code in two character format.

Certificate Database Password
: The certificate database password must be at least eight characters.

Click Next.

34 The Ready to Install screen is displayed. Specify whether you are ready to install by clicking Install.

Verifying the Portal Server 7.1 Installation

Verify the Portal Server installation by doing the following:

- Accessing the samples.
- Accessing the Portal Server administration console.
- Verifying the Gateway port and running the Portal Server in secure mode.

▼ To Verify Sun Java System Portal Server 7.1 Installation

1 **Start Directory Server, web container, and gateway.**

2 **Access Portal Server. For example, type the URL in the browser.**

http`://`*host.domain-name*`:`*port*`/`*portal-URI*

The welcome page appears. The page displays a short description of Portal server and links to sample portals that you selected for installation. Click on one of the links and access the anonymous portal desktop for the sample portal. If the sample portal desktop displays without exception, your Portal Server installation was successful.

3 **Type** *http*`://`*host.domain-name*`:`*port*`/psconsole`**.**

4 **Verify whether Java DB process is running.**

```
netsatat -an | grep 1527
```

If Java DB is not running, start Java DB. For more information, refer to "To Start and Stop Java DB" on page 40

5 **Check whether the common agent container is running.**

On the Solaris platform, type the following:

```
/usr/share/bin/cacaoadm status
```

On the Linux platform, type the following:

```
/opt/sun/cacao/bin/cacaoadm status
```

If the common agent container is not running, restart it.

On the Solaris platform, type the following:

```
/usr/share/bin/cacaoadm stop
/usr/share/bin/cacaoadm start
```

On the Linux platform, type the following:

```
/opt/sun/cacao/bin/cacaoadm stop
/opt/sun/cacao/bin/cacaoadm start
```

Note – By default, common agent container creates a self-signed CA cert and uses it to sign the server cert of the Cacao agent. The subject DN of this server cert is CN=*hostname*_agent (or CN=*hostname*_default_agent on MS Windows). When this default server cert is to be replaced by another server cert signed by the CA of the user's choice, the subject DN of the new server cert must be kept the same as the original one for Portal Server administration to continue function without interruption.

6 Verify whether Directory Server is running using the following commands:

```
netstat -an | grep 389
```

If it is not running, start the Directory Server using the following command:

```
cd /opt/SUNWdsee/ds6/bin
./dsadm start /var/opt/SUNWdsee/dsins1
```

7 Verify whether the Application Server or Web Server is running using the following command:

For Web Server:

```
netstat -an | grep 80
```

For Application Server:

```
netstat -an | grep 8080
```

If it is not running, start the server using the following command:

For Application Server:

/ApplicationServer_base/`Appserver/bin/asadmin`
`    start-domain --user` *admin* `domain1`

For Web Server:

`/var/opt/SUNWwbsvr7/https-`*host.domain-name*`/bin/startserv`

8 Run the following command to check if the gateway is running on the specified port (the default port is 443):

```
netstat -an | grep 443
```

If the gateway is not running, do the following:

PortalServer-base`/bin/psadmin provision-sra -u amadmin -f` *amadmin-password-file* `--gateway-profile gateway-profile --enable`

PortalServer-base`/bin/psadmin start-sra-instance -u amadmin -f` *amadmin-password-file* `--instance-type gateway --instance-name` *gateway-instance-name*

a. Create a file and add the `amadmin` password in plaint text.

b. **Also view the log files. The log file name is picked up from the property called** `debug.com.sun.portal.handler.java.util.logging.FileHandler.pattern` **in the** `platform.conf` **file.**

9 **Run the Portal Server in secure mode by typing the gateway URL in your browser:**

`https://`*gateway-machine-name*`:`*443*

If you chose a different port number other than the default port (443) during installation, you need not specify that port number.

Uninstalling Portal Server

Use the following procedure to uninstall Portal Server.

▼ To Uninstall Portal Server

1 **As a root user, log in to the machine where you installed Portal Server.**

2 **Change directories to:**

- `/var/sadm/prod/SUNWentsys5/` on Solaris.
- `/var/sadm/prod/sun-entsys5/` on Linux.

3 **Type** `./uninstall` **to uninstall Portal Server.**

The Sun Java Enterprise System Uninstall Wizard is displayed.

4 **Select the components to uninstall and select Next.**

If you are uninstalling the Secure Remote Access component, you are asked to provide the portal administrator, Access Manager administrator, and LDAP passwords.

5 **Select Uninstall to uninstall the software.**

Installing Community Samples to an Organization Other Than the Community Sample Organization

▼ To Install Community Samples to an Organization Other Than the Community Sample Organization

1 **Create a custom directory for the configuration files.**

```
mkdir /tmp/mydir
```

2 **Copy the sample configuration files,** `input.properties` **and** `password.properties`**, in** *PortalServer-base*`/samples/portals/shared` **to the directory you created and remove the** `.template` **extension.**

```
cp /opt/SUNWportal/samples/portals/shared/input.properties.template
/tmp/mydir/input.properties
   cp /opt/SUNWportal/samples/portals/shared/password.properties.template
/tmp/mydir/password.properties
```

3 **Edit the** `input.properties` **file and replace all the tokens that begin and end with % with the appropriate Portal Server settings.**

```
ps.config.location=/etc/opt/SUNWportal
ps.portal.id=portal1
ps.access.url=http://domain-name:80/portal
ps.webapp.uri=/portal
ps.profiler.email=
ps.profiler.smtp.host=
search.access.url=http://domain-name:80/search1/search
search.id=search1
am.admin.dn=uid=amAdmin,ou=People,dc=sun,dc=com
default.org.dn=dc=sun,dc=com
```

4 **Edit the** `password.properties` **file and replace tokens that begin and end with % with the appropriate administration password value.**

```
amadminPassword=adminpassword
amldapuserPassword=amldapuserpassword
userManagementPassword=%USER_MANAGEMENT_PASSWORD%
```

Note – The `userManagementPassword` is used for only enterprise sample communications tab setup.

---

5 **The organization name CommunitySample is hardcoded in the community sample ant configuration file. Edit the** `/opt/SUNWportal/samples/portals/community/build.xml` **file and replace CommunitySample in the following line with your organization name:**

```
<property name="orgName" value="CommunitySample"/>
```

6 **The organization name CommunitySample is hardcoded in the par** `DPMapping.properties` **file. Edit the** `/opt/SUNWportal/par-src/community_sample/dp/DPMapping.properties` **file and replace CommunitySample in the following line with your organization name:**

```
organization=o=CommunitySample,dpnode
```

7 **The organization name CommunitySampleis hardcoded in the JSP file. Edit the** `/opt/SUNWportal/par-src/community_sample/pbfiles/templateBaseDir/community_sample /Login/content.jsp` **file and replace CommunitySample with your organization name.**

8 **The user, test, is hardcoded in the community sample setup files. Edit the following files and replace the user, test, with your user name:** `/opt/SUNWportal/samples/portals/community/setup/CommunitySampleConfigRequest.xml` **and** `/opt/SUNWportal/samples/portals/community/setup/CommunitySampleSRAConfigRequest.xml`**.**

9 **The user,** `commauthlessanonymous` **is hardcoded in the community configuration and JSP files. Edit the following files and replace the user** `commauthlessanonymous` **with your user name.**

- `/opt/SUNWportal/samples/portals/community/build.xml`
- `/opt/SUNWportal/samples/portals/community/setup/ CommunitySampleConfigRequest.xml`
- `/opt/SUNWportal/samples/portals/community/setup/ CommunitySamplePortalRequest.input`

10 **Install the Community Sample by running the following command:**

```
/usr/sfw/bin/ant -buildfile /opt/SUNWportal/samples/portals/community/build.xml
-Dconfig.location=/tmp/mydir -logfile /tmp/mydir/community_sample_install.log
```

Working With the Windows Platform

The details provided in the Configuration guide, such as default directories and commands are specific to the Solaris platform. You can use the same commands for Solaris, Linux, and HP-UX. If you install Portal Server on the Windows platform, a .bat extension is required with all the commands.

EXAMPLE 1–1 Running the psconfig command

The `psconfig` command is run as follows on the Solaris platform:

`PortalServer-base/SUNWportal/bin/psconfig --config` *configuration-xml-file*

When you run the psconfig command on the Windows platform, use the command as follows:

`JES-installer-base/portal/bin/psconfig.bat --config` *configuration-xml-file*

where `JES-installer-base` is the directory where you installed Java ES components. For example, if `C:/PROGRA~1/Sun/JavaES5` is the directory where you installed Java ES components, you need to run the psconfig command as follows:

`C:/PROGRA~1/Sun/JavaES5/portal/bin/psconfig.bat --config` *configuration-xml-file*

EXAMPLE 1–2 Running the psadmin commands

All the commands of Portal Server are run from the `/opt/SUNWportal/bin` directory. The `/opt/SUNWportal` is the default installation directory of Portal Server.

The command to display help on the Solaris platform is run as follows:

```
/opt/SUNWportal/bin psadmin --help
```

On the Windows platform, use the command as follows:

PortalServer_base`/portal/bin psadmin.bat --help`

EXAMPLE 1–3 Running the common agent container admin command

The command to start common agent container on the Solaris platform is as follows:

```
/usr/share/bin/cacaoadm start
```

On the Windows platform, use the command as follows:

JES_installer_base`/share/cacao_2/bin/cacaoadm.bat start`

The default installation directories of Java ES Components change based on the operating system. While running a command, you need to change the directories. In the Configuration guide, the information provided is specific to the Solaris platform. If you are using Windows, Linux, or HP-UX platform, refer to the following table for the default directories.

TABLE 1–2 Default Directories on LINUX, HP/UX, and Windows

Product Name	*LINUX / HP-UNIX*	*Windows*
Access Manager	/opt/sun/identity	*JES_installer_base*/identity
Access Manager configuration directory	/etc/opt/sun/identity/config	*JES_installer_base*/identity/config
Access Manager data directory	/var/opt/sun/identity	*JES_installer_base*/identity/data
Application Server install directory	/opt/sun/appserver	*JES_installer_base*/appserver
Application Server instance directory	/var/opt/sun/appserver/domains/domain1	*JES_installer_base*/appserver/domains/domain1
Application Server docroot	/var/opt/sun/appserver/domains/domain1/docroot	*JES_installer_base*/appserver/domains/domain1/docroot
WebServer install directory	/opt/sun/webserver7	*JES_installer_base*/webserver7
WebServer docroot	/var/opt/sun/webserver7/https-instancename/docs	*JES_installer_base*/webserver7/https-instancename/docs
Directory Server product directory	/opt/sun/ds6	*JES_installer_base*/DSEE/ds6
Directory Server instance directory	/var/opt/sun/dsins1	*JES_installer_base*/DSEE/var/DSInstance
Portal Server product directory	/opt/sun/portal	*JES_installer_base*/portal
Portal Server configuration directory	/etc/opt/sun/portal	*JES_installer_base*/portal/config
Portal Server data directory	/var/opt/sun/portal	*JES_installer_base*/portal/data
Common agent container product directory	/opt/sun/cacao	*JES_installer_base*/share/cacao_2
Common agent container configuration directory	/etc/opt/sun/cacao/instances/default	*JES_installer_base*/share/cacao_2/etc/cacao/instances/default
Registry lib directory	/opt/sun/srvc-registry/lib	*JES_installer_base*/srvc-registry/lib
MFWK lib directory	/opt/sun/mfwk/share/lib	*JES_installer_base*/share/mfwk/lib
MFWK bin directory	/opt/sun/mfwk/bin	*JES_installer_base*/share/mfwk/lib

TABLE 1–2 Default Directories on LINUX, HP/UX, and Windows *(Continued)*

Derby lib directory	/opt/sun/javadb/lib	*JES_installer_base*/javadb/lib
Webnfs lib directory	/opt/sun/webnfs	*JES_installer_base*/share/webnfs
Ant Home directory	/opt/sun	*JES_installer_base*/share/ant
Ant lib directory	/opt/sun/share/lib	*JES_installer_base*/share/ant/lib
Shared lib directory	/opt/sun/share/lib	*JES_installer_base*/share/lib
Private lib directory	/opt/sun/private/share/lib	*JES_installer_base*/share/lib
Java home	/usr/jdk/entsys-j2se	*C:/Java*/JDK15~3.0_0
JDMK lib directory	/opt/sun/jdmk/5.1/lib	*JES_installer_base*/share/lib
JAX lib directory	/opt/sun/share/lib	*JES_installer_base*/share/lib
NSS lib directory	/opt/sun/private/lib	*JES_installer_base*/share/lib
JSS Jar directory	/opt/sun/private/lshare/lib	*JES_installer_base*/share/lib

◆ ◆ ◆ CHAPTER 2

Managing Java DB for Portal Server

This chapter includes the following:

Introduction to Java DB

By default, the Sun Java System Portal Server software uses the Java™ DB to store configuration and membership for the collaboration feature. It is used by the desktop. Java DB is also used by wiki, fileshare and survey portlet applications. The Portal Server software installs and configures the database.

Tip – For information on switching to enterprise-scale databases, see this article.

The Portal Server software does not manage the Java DB process; it must be manually started and stopped using the Java DB `NetworkServerControl` class (see "To Start and Stop Java DB" on page 40 for more information). The default database user name is `portal` and the password is a random string generated during installation. On a production system, change the credentials to secure the system.

Database Configuration

The Portal Server software components use Java DB through Java EE JDBC resources. When a new portal instance is created, the Portal Server software creates one JDBC resource for each component that accesses the database. In other words, there is one resource per component, per Portal Server instance.

The resource configuration can be modified using the web container console or command line interface. The database URL for the Java DB community database is of the form `jdbc:derby://host[:port]/component_`*portal-ID*. When connecting to Java DB using third-party tools, use the driver `org.apache.derby.jdbc.ClientDriver`. This driver is in the JAR file `/opt/SUNWjavadb/lib/derbyclient.jar`.

Starting, Stopping, and Disabling the Java DB

There are two portal components that use the relational database: community membership and configuration and portlet applications, such as wiki, survey, and filesharing. By default, Portal Server uses Java DB. After the installation, Portal Server can be configured to switch to Oracle. In that case, you need to shut down the Java DB database. Java DB should also be stopped if community features and the portlet application are not used in the deployed portal.

For each portal component using relational database, a separate database instance is configured with default userid and password. After the installation, you are recommended to change the default password and the access permissions of the properties files containing them. For this release of the Portal Server software, see the release notes for more information on how to change the password.

▼ To Start and Stop Java DB

1. **Set the classpath. The** `derby.jar`**,** `derbytools.jar`**, and** `derbynet.jar` **files must be in your** `classpath`**. By default, these JAR files are installed into** `/opt/SUNWjavadb/lib` **directory.**

2. **Set the system property** `derby.system.home` **to** *PortalServer-DataDir*`/derby`**.**

3. **Stop and start the database using Java DB** `NetworkServerControl` **class.**

   For example, type:

   - `java -Dderby.system.home=`*PortalServer-DataDir*`/derby org.apache.derby.drda.NetworkServerControl start` to start the database.
   - `java -Dderby.system.home=`*PortalServer-DataDir*`/derby org.apache.derby.drda.NetworkServerControl shutdown` to stop the database.

Note – By default, the Application Server's instance of Java DB uses the same port as Portal's (the Java DB default port of 1527). If you wish to run the Application Server's instance of Java DB, change the port from 1527 to some other value.

If the Java DB process remains connected to a terminal, it will quit when the terminal exits, when the user logs out, or when the system in restarted. To detach the Java DB process from the terminal on UNIX-based systems, use the `nohup` command. On Windows system, make the Java DB process a Windows service.

After the installation, Portal Server software can be configured to switch to Oracle. In that case, Java DB need not be running. It can also be stopped if use of Java DB is disabled for desktop and the portlet applications (such as wiki, fileshare, surveys) are not used in the deployed portal.

▼ To Disable Use of Java DB by Desktop

The Portal Desktop uses the database (Java DB or Oracle) to get community membership and configuration for users. If you are not using the Community Feature, this is not required. To prevent the Portal Desktop from getting user membership and configuration from the database, perform the following steps.

1. **Log in to the Portal Server host as root and go to** *PortalServer-DataDir*`/portals/`*portal-ID*`/config/` **directory.**

2. **Edit the** `communitymc.properties` **file and remove the** `jdo` **entry from the** `manager.contributors` **list.**

   Note – If this change is applied, the community sample does not function properly.

3. **Restart the web container.**

◆ ◆ ◆ CHAPTER 3

Configuring Sun Java System Portal Server in the Configure Later Mode After Installation

Sun Java System Portal Server 7.1 can be installed using the Java ES installer in two modes: Configure Now mode or Configure Later mode. If you select the Configure Now option, the installation and configuration take place simultaneously. If you select the Configure Later mode, you need to run the `psconfig` command to configure Portal Server after installation.

This chapter contains the following topics:

Understanding the `psconfig` Command

When you run the `psconfig` command, you specify a configuration XML file. You can customize the configuration XML file based on your requirements. Sample configuration XML files are provided at the *PortalServer-base*`/samples/psconfig` directory. To know more about the files that you need to customize, read the *PortalServer-base*`/SUNWportal/samples/psconfig/ReadMe.txt`. To customize the files, you modify values and replace the tokens.

The syntax of the `psconfig` command is as follows:

`psconfig --config` *configuration-xml-file*

The location of the `psconfig` utility is *PortalServer-base*`/SUNWportal/bin`.

The subsequent sections in this chapter contain information about customizing a sample configuration XML file if the sample configuration XML files do not meet your requirements.

Creating a Custom Configuration XML File

If a sample configuration file does not suit your desired setup and if a custom configuration XML file must be constructed, follow the instructions in this section. Sample configuration XML files are provided at the *PortalServer-base*/samples/psconfig directory. In order to set up your custom configuration file, you must follow this process:

1. Construct the required basic configuration file XML file. For more information, refer to "Constructing the Required Basic XML File" on page 44.

   This basic configuration is required to make the portal psadmin command usable.
2. Construct the <ComponentsToConfigure> element depending on which components are to be configured on this host. See "Configuring Portal Server Components" on page 45 for more information.
3. Construct the following configuration information based on the components to configure on this host:

   "Configuring Basic Portal Server" on page 46
   "Configuring a Sample Portal" on page 46
   "Configuring Web Container" on page 47
   "Configuring Search Server " on page 48
   "Configuring Secure Remote Access" on page 49
   "Configuring Gateway" on page 49
   "Configuring Netlet Proxy" on page 50
   "Configuring Rewriter Proxy" on page 51
4. Run the ./psconfig --config *configuration-xml-file* command.

Constructing the Required Basic XML File

This section describes the overall Portal Server, header/footer, shared components, and the Access Manager elements in the configuration file. See the example2.xml file.

▼ To Construct the Required Basic XML File

1 Edit the example2.xml file.

2 In the example2.xml file, replace the following tokens with the actual values.

@HOST.DOMAIN@	The host and domain name of the machine on which configuration is occurring
@AMADMIN.PASSWORD@	Administrator's password for the Access Manager instance with which Portal Server is to be configured

`@AMLDAPUSER.PASSWORD@`	Internal LDAP user password for the Access Manager instance with which Portal Server is to be configured
`@DIRMGR.PASSWORD@`	Administrator's password of the Directory Server with which Portal Server is to be configured

3 Modify the following values in the file as needed.

`PortalServerConfiguration xsi:noNamespaceSchemaLocation`
If Portal Server is installed in a non-default location, then change this location to the non-default location.

`SharedComponents JCIFSLibDir`
If Netfile utility is required, install the optional JCIFS package and specify the `lib` directory path name.

`SharedComponents JChardet`
Install the optional JChardet package and specify the `lib` directory path name.

`AccessManager InstallationDirectory ProdDir, DataDir, ConfigDir`
Specify the installation path name of Access Manager if Access Manager was not installed in the default location.

`PortalConfiguration InstallationDirectory ProdDir, DataDir, ConfigDir`
Specify the installation path name of Portal Server if Portal Server was not installed in the default location.

Configuring Portal Server Components

Portal Server components that can be installed and configured across different nodes include the core Portal Server , Secure Remote Access (SRA), Gateway, Netlet Proxy, and Rewriter Proxy. The `<ComponentsToConfigure>` element is constructed based on which components are configured on this host.

▼ To Configure Portal Server Components

- **Include the following in the configuration XML file.**

```
<ComponentsToConfigure>
        <component>portalserver</component>
        <component>gateway</component>
        <component>netletproxy</component>
        <component>rewriterproxy</component>
</ComponentsToConfigure>
```

To exclude components, remove the corresponding `<component>` element.

Configuring Basic Portal Server

This section explains how to configure a basic Portal Server.

▼ To Configure Basic Portal Server

1 **Open the configuration XML file.**

2 **Replace the following tokens in the configuration XML file.**

`@HOST.DOMAIN@`	The host and domain name of the machine on which Portal Server is to be configured.
`@PORT@`	Web container port at which Portal Server has to be deployed.

3 **Modify the following values in the configuration XML file.**

`PortalConfiguration PortalServer PortalAccessURL` (optional)
If the DEPLOY URI is not the default, change `/portal` to the changed URI value.

`PortalConfiguration PortalServer PortalWebappURI` (optional)
If the DEPLOY URI is not the default, change `/portal` to the changed URI value. Ensure that both `PortalAccessURL` and `PortalWebappURI` are specified in the configuration XML file.

`PortalConfiguration PortalServer PortalID`
Change `portal1` to the required portal ID, which should be unique.

`PortalConfiguration PortalServer Instance InstanceID`
Change `myInstance` to the required instance ID, which should be unique.

`PortalConfiguration PortalServer SearchServerID` (optional)
Specifies which Search Server this portal samples are configured with. This is needed only if samples are configured.

Configuring a Sample Portal

Portal Server software three types of sample portals: the Developer Sample, Enterprise Sample, and Community Sample. Each sample is created under its own sub-org for ease of management. You can configure any of the samples or all of the samples.

▼ To Configure a Sample Portal

- **Include the following in the configuration XML file.**

```
<PortalConfiguration>
        <PortalServer
            .
```

```
            .
            .
        >
            <SamplePortal>
                <Sample Name="DeveloperPortal"/>
                <Sample Name="EnterprisePortal"/>
                <Sample Name="CommunityPortal"/>
            </SamplePortal>
            .
            .
            .
        </PortalServer>
</PortalConfiguration>
```

Configuring Web Container

The Web container configuration varies with the container to be configured. In the configuration XML file, there is one `<WebContainerProperties>` element specified for the web container under the `<PortalServer><Instance>` element and one under the `<SearchServer>` element.

▼ To Configure the Web Container

1 Open the configuration XML file.

- For Web Server, open `example1.xml`, examples 3 to 9, `example13.xml`, or `example17.xml`.
- For Application Server, open the `example14.xml` file.

2 Replace the tokens with actual values.

For Web Server:

`@HOST.DOMAIN@`	The host and domain name of the machine on which the Portal Server instance is to be configured
`@PORT@`	Web Server port
`@INSTANCENAME@`	Web Server instance name
`@ADMIN.PORT@`	Web Server administration port
`@PASSWORD@`	Web Server administrator's password

For Application Server:

`@HOST.DOMAIN@`	The host and domain name of the machine on which the Portal Server instance is to be configured
`@PORT@`	Application Server port

`@ADMIN.PORT@`	Application Server administration port
`@PASSWORD@`	Application Server administrator's password
`@MASTER.PASSWORD@`	Application Server master password if specified

3 **Modify the following values in the configuration XML file as needed.**

For Application Server:

`WebContainerInstallDir`
If Application Server is installed at a non-default location insert the installation path name.

`WebContainerDomainName, WebContainerInstanceDir, WebContainerDocRoot`
If deploying to a non-default Application Server domain insert the appropriate name.

`WebContainerInstanceName`
Instance name within the Application Server domain. The `server` is the name of the first instance which is created by default at the same time the Application Server 8.1 domain is created. This can be changed to the name of any other created instance within that domain.

Configuring Search Server

The Search Server is deployed to a specific web container instance which is defined by a `<WebContainerProperties>` element. Multiple Search servers can be specified by having multiple `<SearchServer>` elements within a `<PortalConfiguration>` section, each with a unique ID. A Portal Server can be associated with a specific search server by specifying the `SearchServerID` attribute within the `<PortalServer>` element.

▼ To Configure Search Server

- **In the configuration XML file, include the `SearchServerID` attribute within the `<PortalServer>` element.**

```
<PortalConfiguration>
        <SearchServer SearchServerID="search1">
            <WebContainerProperties
                .
                .
                .
            />
        </SearchServer>
        <PortalServer
            SearchServerID="search1">
        </PortalServer>
</PortalConfiguration>
```

Configuring Secure Remote Access

The SRA core component can only be installed and configured on the same node as the Portal Server component. The Portal Server and SRA core components have to be configured at the same time. So the SRA core component cannot be configured on a host that already has an existing Portal Server.

▼ To Configure Secure Remote Access

1 **Add Secure remote access support to Portal Server by adding the** `<component>sracore</component>` **to the** `<ComponentsToConfigure>` **section.**

2 **Add the following section to the** `<PortalConfiguration>` **section.**

```
<PortalConfiguration>
        .
        .
        .
        <SecureRemoteAccessCore
            GatewayProtocol="https"
            PortalServerDomain="@DOMAIN@"
            GatewayPort="@GATEWAY.PORT@"
            GatewayProfileName="default"
        LogUserPassword="@SRA.LOGUSER.PASSWORD@"/>
</PortalConfiguration>
```

3 **Replace the tokens with actual values.**

`@DOMAIN@`	Domain name of the machine on which Portal Server is to be configured
`@GATEWAY.PORT@`	Port on which Gateway is to run
`@SRA.LOGUSER.PASSWORD@`	SRA log user password

4 **Modify the** `GatewayProfileName` **value if the default profile will not be used.**

Configuring Gateway

This section explains how to configure Gateway with Portal Server.

▼ To Configure Gateway

1. **Open the `example10.xml` file.**

2. **Replace the following tokens with actual values.**

`@HOST.DOMAIN@`	The host and domain name of the machine on which Gateway is to be configured
`@GATEWAY.PORT@`	Port on which Gateway will run
`@IPADDRESS@`	IP address of the machine on which Gateway will run
`@PSHOST.DOMAIN@`	The host and domain name of the machine on which the Portal Server instance is to be configured
`@PORT@`	Port on which the Portal Server instance will run
`@SRA.LOGUSER.PASSWORD@`	SRA log user password
`@SRA.CERTDB.PASSWORD@`	SRA certificate database password

3. **Modify the following values as needed.**

`Gateway Profile`	Change if the default profile will not be used
`Gateway SRAInstance StartInstance`	Change if start on installation is not required
`CertificateInformation`	Change attributes in this section accordingly

Configuring Netlet Proxy

This section explains how to configure the Netlet proxy.

▼ To Configure Netlet Proxy

1. **Open the `example11.xml` file.**

2. **Replace the tokens with the actual values.**

`@HOST.DOMAIN@`	The host and domain name of the machine on which Netlet Proxy will be configured
`@NETLET.PROXY.PORT@`	Port on which Netlet Proxy will run
`@IPADDRESS@`	IP address of the machine on which Netlet Proxy will run
`@PSHOST.DOMAIN@`	The host and domain name of the machine on which the Portal Server instance will be configured

`@PORT@`	Port on which the Portal Server instance will run
`@SRA.LOGUSER.PASSWORD@`	SRA log user password
`@SRA.CERTDB.PASSWORD@`	SRA certificate database password

3 Modify the following values as needed.

`NetletProxy Profile`	Change if the default profile will not be used
`NetletProxy SRAInstance StartInstance`	Change if start on installation is not required
`CertificateInformation`	Change attributes in this section accordingly

Configuring Rewriter Proxy

This section explains how to configure Rewriter Proxy.

▼ To Configure Rewriter Proxy

1 Open the `example12.xml` file.

2 Replace the tokens with the actual values.

`@HOST.DOMAIN@`	The host and domain name of the machine on which Rewriter Proxy will be configured
`@REWRITER.PROXY.PORT@`	Port on which Rewriter Proxy will run
`@IPADDRESS@`	IP address of the machine on which Rewriter Proxy will run
`@PSHOST.DOMAIN@`	The host and domain name of the machine on which portal instance will be configured
`@PORT@`	Port on which Portal Server instance runs
`@SRA.LOGUSER.PASSWORD@`	SRA log user password
`@SRA.CERTDB.PASSWORD@`	SRA Certificate database password

3 Modify the following values as needed.

`RewriterProxy Profile`
Change if the default profile is not to be used

`RewriterProxy SRAInstance StartInstance`
Change if start on install is not required

`CertificateInformation`
Change attributes in this section accordingly

◆ ◆ ◆ CHAPTER 4

Installing Portal Server 7.1 on Web Containers

This chapter explains how to install Portal Server 7.1 on Sun Java System Web Server and Sun Java System Application Server on different scenarios, such as SSL installation and non-root installation. This chapter also explains how to install Portal Server on IBM WebSphere and BEA WebLogic. This chapter includes the following sections:

Installing Portal Server 7.1 on Web Server 7.0

This section contains the following Portal Server 7.1 installation procedures on Web Server 7.0:

- Default installation
- SSL installation and post installation
- Configuring Portal Server 7.1 on 64–bit Web Server 7.0 instance
- Installing Portal Server 7.1 as a non-root user

Installing Portal Server on Sun Java System Web Server

Portal Server can be installed on Sun Java System Web Server using the Java ES installer. Sun Java System Web Server can be selected as component to install. Later you can select Sun Java System Web Server as the web container to install Portal Server using the Java ES installer.

For more information on the default installation procedure, see Chapter 1, "Installing Sun Java System Portal Server 7.1."

Installing Portal Server on Sun Java System Web Server 7.0 in the SSL Mode

The secure socket layer (SSL) mode enables a user to access Portal Server using the `https` protocol. The `https` protocol ensures secured communication between the user and Portal Server. In this scenario, you need to create a secured Web Server instance. After creating a secured Web Server instance, you direct the Portal Server web container to the secured Web Server instance.

This section describes following procedures:

- Create a new configuration instance
- Create a request certificate
- Generate a server certificate
- Add the Server Certificate to the Certificate Database
- Add `root ca` to the Certificate Database
- Enable SSL on the Listener

▼ To Create a New Configuration Instance

Before You Begin Install Web Server 7.0 on Node 1.

1. **Log in to the Web Server 7.0 administrator console.**

   `https://`*node1.domain-name***`:8989`**

2. **Select New Configuration under the Configuration Tasks option.**

3. **Type the following values:**

   - Configuration name: **`node1`**
   - Server name: **`node1.`***domain-name*
   - Hosts: **`node1.`***domain-name*
   - Server user: **`root`**
   - Port: **`8200`**

4. **Move the node from the Available list box to the Selected list box.**

5. **Click Finish.**

6. **Start the server configuration and access it.**

   `http://`*node1.domain-name***`:8200`**

To Create a Request Certificate

1 Run the following command.

WebServer_base/SUNWwbsvr7/bin/wadm create-cert-request
--user=*admin* --host=*node1.domain-name*
--port=*8989* --echo=*true* --rcfile=*rcfile* --config=*node1* --token=*internal*
--server-name=*node1.domain-name* --org=*org* --locality=*locality* --state=*state*
--country=*country*

2 Type the token values.

- Pin: *password*
- Administrator user password: *password*

The request certificate is created.

3 Send the request certificate to the Certificate Authority for approval.

To Add the Server Certificate to the Certificate Database

1 Add the Server Certificate, `servercert`, to the certificate database.

WebServer_base/SUNWwbsvr7/bin/wadm install-cert --user=*admin*
--password-file=*password* --host=*node1.domain-name*
--port=*8989* --ssl=*true*
--rcfile=*rcfile1*
--echo=*true* --token=*internal* --config=*node1*
--cert-type=*server*
--file-on-server=*true* --nickname=*servercert* *WebServer_base*/SUNWwbsvr7/bin/servercert

2 Type the token values.

- Pin: *password*
- Administrator user password: *password*

To Add the Root CA Certificate to the Certificate Database

1 Add the `root ca` certificate to the database.

WebServer_base/SUNWwbsvr7/bin/wadm install-cert --user=*admin* --password-file=*ps*
--host=*node1.domain-name* --port=*8989* --ssl=*true*
--rcfile=*rcfile1* --echo=*true* --token=internal --config=*node1*
--cert-type=*ca* --file-on-server=*true* --nickname=*rootca*
root-CA-file-path

2 Type the token values.

- Pin: *password*

- Administrator user password: *password*

3 **Restart the server configuration.**

▼ To Enable SSL on the Listener

1 **Access the Web Server 7.0 administrator console.**
`https://`*node1.domain-name*`:8989`

2 **Select New Configuration on the Tasks page.**

3 **Select Edit Configuration.**

4 **Select Virtual Servers.**

5 **Select http-listener1.**

6 **Click the Security tab.**

7 **Select Security option.**

8 **Click Apply and Close.**

9 **Click the Deploy button.**

10 **Restart the servers.**
WebServer_base`/SUNWwbsvr7/bin/stopserv`
WebServer_base`/SUNWwbsvr7/bin/startserv`

11 **Verify the SSL instance by accessing the following URL.**
`https://`*node1.domain-name*`:8200`

Configuring Portal Server 7.1 on a 64–bit Web Server 7.0 Instance

Portal Server 7.1 supports 64–bit Web Server 7.0 on the following platforms:

- Solaris 10 SPARC
- Solaris 9 SPARC
- Solaris 10 amd64 (Opteron based systems)

While you install Portal Server using the Java ES installer, it is installed in the 32–bit mode. If you need to install Portal Server in 64–bit mode, you need to install it in two sessions:

- In the first session, you need to install the components, such as Web Server 7.0, Directory Server, and Access Manager.
- In the second session, you need to install Portal Server and configure it to support 64–bit mode.

▼ To Configure Portal Server 7.1 on a 64–bit Web Server 7.0 Instance

1. **Install Web Server 7.0, Directory Server, and Access Manager using the Java ES installer.**
2. **Start the Directory Server instance.**
3. **Ensure that the Web Server 7.0 administrator server is running.**

   `https://`*node1.domain-name*`:8989`**
4. **Ensure that the Web Server instance is running.**

   `http://`*node1.domain-name*`:80`**
5. **Configure Web Server to support 64–bit mode.**

```
WebServer_base/SUNWwbsvr7/bin/wadm set-config-prop
--user=admin --port=8989 --password-file=passfile
-config=host_name platform=64

WebServer_base/bin/wadm set-thread-pool-prop
-user=admin --port=8989 --password-file=passfile
-config=host_name stack-size=261144

WebServer_base/bin/wadm deploy-config
-user=admin --password-file=passfile
-port=8989 --restart=true host_name
```

6. **Ensure that the web container instance and administrator server are running.**

   `https://`*node1.domain-name*`:8989`**

   `http://`*node1.domain-name*`:80`**
7. **Install Portal Server 7.1 in the Configure Now mode using the Java ES installer.**

Switching Portal Server Installation From 64–bit Mode to 32–bit Mode

If you have installed Portal Server in 64–bit mode, you can use the following procedure to convert Portal Server to support 32–bit mode. After configuring Portal Server to support 32–bit mode, you need to manually configure the search server.

▼ To Switch Portal Server Installation From 64–bit Mode to 32–bit Mode

1. **Start the Directory Server instance.**
2. **Ensure that the Web Server administrator server is running.**
3. **Ensure that Web Server instance is running.**
4. **Configure Web Server to support 32–bit mode.**

```
WebServer_base/SUNWwbsvr7/bin/wadm set-config-prop
--user=admin --port=8989 --password-file=passfile
--config=host_name platform=32

WebServer_base/bin/wadm set-jvm-prop
--user=admin --port=8989 --password-file=passfile
--config=host_name
ative-library-path-prefix="/PortalServer_base/SUNWportal/lib
```

5. **Remove all compiled JSPs for the Portal desktop.**

```
rm -rf /var/opt/SUNWportal/portals/PORTAL_ID/desktop/compiled/_jsps/*
```

```
WebServer_base/bin/wadm
deploy-config --user=admin --password-file=
passfile --port=8989
--restart=true host_name
```

6. **Stop and start the Web Server instance.**

▼ To Configure the Search Setup from 64–bit Mode to 32–bit Mode

1. **Go to the Search Server directory.**

```
cd /var/opt/SUNWportal/searchservers/searchserver_name/db
```

2. **Remove the unwanted files.**

```
rm -rf _*
```

3. **Edit the `search.conf` file.**

```
vi /var/opt/SUNWportal/searchservers/search1/config/search.conf
```

4. **Set the `search-platform` property to 32.**
5. **Stop and start the Web Server instance.**

Switching Portal Server Installation From 32–bit Mode to 64–bit Mode

If you have installed Portal Server in 32–bit mode, then you can use the following procedure to convert Portal Server to support 64–bit mode. After configuring Portal Server to support 64–bit mode, you need to manually configure the search server.

▼ To Switch Portal Server Installation From 32–bit Mode to 64–bit Mode

1 Start the Directory Server instance.

2 Ensure that the Web Server 7.0 administrator server is running.

3 Ensure that Web Server instance is running.

```
WebServer_base/SUNWwbsvr7/bin/wadm
set-config-prop --user=admin --port=8989
--password-file=passfile
--config=host_name platform=64

WebServer_base/SUNWwbsvr7/bin/wadm
set-thread-pool-prop --user=admin --port=8989
--password-file=passfile
--config=host_name stack-size=261144

WebServer_base/SUNWwbsvr7/bin/wadm
set-jvm-prop --user=admin --port=8989
--password-file=passfile --config=
host_name native-library-path-prefix=
"/PortalServer_base/SUNWportal/lib/sparcv9" (amd64 for x86)

WebServer_base/SUNWwbsvr7/bin/wadm
delete-jvm-options --user=admin --port=8989
--password-file=passfile --config=
host_name "-Xms512M -Xmx768M -Xss128k"

WebServer_base/SUNWwbsvr7/bin/wadm
create-jvm-options --user=admin --port=8989
--password-file=passfile --config=
host_name "-Xms512M -Xmx768M -Xss512k"
```

4 Remove all compiled JSPs for the Portal desktop.

```
rm -rf /var/PortalServer_base/SUNWportal/portals/PORTAL_ID/desktop/compiled/_jsps/*

WebServer_base/SUNWwbsvr7/bin/wadm deploy-config
--user=admin --password-file=
```

passfile `--port=`*8989* `--restart=`*true*
host_name

To Switch the Search Setup From 32–bit Mode to 64–bit Mode

1. **Go to the Search Server directory and delete the unwanted files.**

   ```
   cd /var/SUNWportal/searchservers/searchserver_name/db
   rm -rf _*
   ```

2. **Edit the `search.conf` file.**

   ```
   vi /var/opt/SUNWportal/searchservers/search1/config/search.conf
   ```

3. **Set the `search-platform` property to 64.**

4. **Stop and start the Web Server instance.**

Installing Portal Server 7.1 as a Non-Root User

If you do not have administrator privileges for the machine where you install Portal Server, use the following procedure to install Portal Server.

To Install Portal Server 7.1 as a Non-Root User

1. **Install the Directory Server using the Java ES installer.**

   During installation, provide the username and group information whenever prompted.

2. **As the non-root user, start Directory Server and verify whether it is running.**

   ```
   ps -aef | grep slapd
   ```

3. **Install web container as the non-root user using the Java ES installer.**

4. **Install Access Manager.**

   For more information on installation steps, see the *Technical Note: Installing Access Manager to Run as a Non-Root User*.

5. **Install Portal Server in the Configure Later mode.**

6. **During installation, provide the non-root user information whenever prompted.**

7. **Change the ownership and access rights of `SUNWportal` to the User ID and Group of the non-root user.**

```
chown -R Userid:Group /PortalServer_base/SUNWportal
chown -R Userid:Group /etc/SUNWportal
chown -R Userid:Group /var/SUNWportal
chmod -R 755 /PortalServer_base/SUNWportal
chmod -R 755 /etc/SUNWportal
chmod -R 755 /var/SUNWportal
```

8. **Restart the web container.**

▼ To Create a New Portal Server Instance as a Non-Root User

1. **Create a web container instance as a non-root user.**
2. **Telnet as a non-root user and run the `psadmin create-instance` command.**
3. **Telnet as the root user and run the `chown -R psuser:portal /var/opt/SUNWportal/portals/myPortal/` command.**
4. **Telnet as a non-root user and restart the web container instance.**

▼ To Create a New Search Server in Web Server Non-Root Install

1. **Create a Web Server instance using the Web Server 7.0 administration console as a non—root user.**
2. **Create a search server.**
3. **Log in as a root user into the machine and change the search server instance.**

   `chown -R nonrootuser.nonroot /var/opt/SUNWportal/searchservers/`*search-server-id*

   For the Linux platform, use the following command: `chown -R nonrootuser.nonroot /var/opt/sun/portal/searchservers/`*search-server-id*.

4. **Change permissions of the search instance.**

   `chmod -R og+rX /var/opt/SUNWportal/searchservers/`*search-server-id*

   For the Linux platform, use the following command: `chmod -R og+rX /var/opt/sun/portal/searchservers/`*search-server-id*

5. **Restart Web Server as the non-root user.**

Installing Portal Server 7.1 on Application Server 8.2

This section explains how to install Portal Server as Application Server 8.2 as the web container.

Default Installation

You can install Portal Server with Application Server as the web container. You need to select Application Server as a component to install in the Java ES installer, and later select Application Server as the web container for Portal Server. For more information on default installation, see the "To Install the Portal Server Software" in Chapter 1, "Installing Sun Java System Portal Server 7.1."

SSL Installation on an Application Server Instance

You can install Portal Server in SSL mode which ensures a secure communication. You need to create a SSL-enabled instance of Application Server. You can install Portal Server using the Java ES installer, and point to the instance of the Application Server as the web container.

▼ To Create an Application Server Instance on SSL Mode

1. **Install Application Server and Directory Server using the Java ES installer.**

2. **Add valid certificates to the Application Server.**

   The certificate database is available in the `/var/SUNWappserver/domains/domain1/config` directory. The database files are `key3.db` and `cert8.db`.

3. **Change to the `config` directory.**

   ```
   cd /var/SUNWappserver/domains/domain1/config
   ```

4. **Create a password file, `password`, and specify the password.**

5. **Create a certificate signing request.**

   ```
   certutil -R -s "CN=node1.domain-name,OU=People,O=Portal,
   L=location,ST=state,C=country" -o certreq.pem -g 512
   -d  /var/SUNWappserver/domains/domain1/config -f password -a
   ```

   This command creates a certificate request in the `certreq.pem` file. The `certutil` utility is located in the `/usr/sfw/bin` directory.

   a. **Send this certificate request to a Certificate Management Server (CMS) for approval.**

b. After the certificate is approved, paste the contents of the approved certificate in a flat file on the Application Server machine. For example, the `servercert.pem` file.

c. Add this certificate to the database.

d. Change to the `config` directory of the Application Server.

```
cd /var/ApplicationServer_base/SUNWappserver/domains/domain1/config
```

Note – The `servercert.pem` file is also in the `config` directory.

---

e. Run the command:

```
certutil -A -n servercert -t "u,u,u" -d
ApplicationServer_base/SUNWappserver/domains/domain1/config -a -i servercert.pem
-f password
```

f. Add `root ca` to the database.

```
certutil -A -n rootca -t "TCu,TCu,TCuw" -d
ApplicationServer_base/SUNWappserver/domains/domain1/config -a -i
path_to_root_ca -f password
```

6 Log in to administrator console of the Application Server.

`https://`*host.domain-name*`:4849`

7 Select Configuration -> server-config -> HTTP Service -> HTTP Listeners -> http-listener-2.

Perform the following tasks:

- Verify whether the security is enabled.
- Verify whether the certificate nickname is `servercert`.
- Enable SSL3.
- Enable Transport Layer Security (TLS).
- Select the All Cipher suites checkbox.

8 Restart the Application Server.

Because the Application Server is SSL enabled, you start the Java ES installer, Portal Server will not communicate with Application Server. You need to install `root ca` in the Java Development Kit (JDK) keystore of the hostname.

9 Install `root ca` in the JDK keystore of the hostname.

```
cd /usr/jdk/entsys-j2se/jre/lib/security
/usr/jdk/entsys-j2se/jre/bin/keytool -keystore
cacerts -keyalg RSA -import -trustcacerts -alias hostname
-storepass store-password -file root-ca-CA
```

10 **Invoke the Java ES installer and select Access Manager and Portal Server.**

11 **Specify valid protocol and port values wherever prompted.**

▼ To Install Portal Server on a Non-Default Application Server 8.2 Instance

If you install Portal Server on Application Server using the Java ES installer, Portal Server is installed on a default instance of the Application Server on port `8080`. This procedure describes to create a non-default Application Server instance and install Portal Server on it.

1 **Run the Java ES installer to install Directory Server and Application Server.**

2 **Start Directory Server and Application Server.**

3 **Create a node agent,** `nodeagent`**.**

ApplicationServer_base`/SUNWappserver/bin/asadmin start-node-agent --user` *admin* `--password` *password* `--savemasterpassword=`*true nodeagent*

4 **Start the node agent.**

ApplicationServer_base`/SUNWappserver/bin/asadmin start-node-agent --user` *admin* `--password` *password nodeagent*

5 **Create the server instance** *server-instance* **on port 38080.**

ApplicationServer_base`/SUNWappserver/bin/asadmin create-instance --user` *admin* `--password` *password* `--node agent=`*nodeagent* `--port=`*38080 server-instance*

6 **Start the server instance.**

ApplicationServer_base`/SUNWappserver/bin/asadmin start-instance --user` *admin* `--password` *password server-instance*

7 **Start the Java ES installer and install Access Manager and Portal Server in the Configure Later mode.**

8 **Modify the** `amsamplesilent` **file and configure Access Manager.**

On Solaris platform, the `amsamplesilent` file is located at the *AccessManager_base*`/SUNWam/bin` directory. In Linux, the file is located at the *AccessManager_base*`/SUN/identity/bin` directory.

9 **Run the** `amconfig` **command.**

See Appendix for more details on the `amconfig` file.

10 **Restart the server instance.**

11 **Access the administrator console of the Access Manager.**

`http://host.domain-name:38080/amconsole`

12 **Modify the** `example14.xml` **file.**

See Appendix for more details on the `example14.xml` file.

13 **Configure the common agent container.**

PortalServer_base`/SUNWportal/bin/psconfig --config` *example14.xml*

14 **Restart Directory Server, Access Manager, Application Server, and Portal Server.**

▼ To Convert Portal Server to the Secure Mode on Application Server 8.2

If you have already installed Directory Server, Access Manager, Web Server, and Portal Server on Application Server 8.2, use this procedure to convert Portal Server installation to the secure mode. In the Secure mode, the communication between the user and Portal Server is through the `https` protocol.

1 **Install Directory Server, Access Manager, Web Server, Portal Server, and Application Server 8.2.**

2 **Create a password file** `password` **and specify the password that has been provided for Application Server.**

3 **Create a certificate signing request.**

`certutil -R -s "CN=`*HOSTNAME*`.domain-name,OU=`*People*`,O=`*Portal*`,L=`*Location*`,ST=`*State*`,C=`*Country*`" -o` *certreq.pem* `-g` *512* `-d /var/opt/SUNWappserver/domains/domain1/config -f` *password* `-a`

This command creates a certificate request in the `certreq.pem` file. The `certutil` file is present in the `/usr/sfw/bin` directory.

4 **Send the certificate signing request to the CMS.**

5 **Paste the contents of the approved certificate in an empty file on the Application Server machine.**

For example, the file name is `servercert.pem`.

6 **Add this certificate in the database.**

a. **Change to the** `config` **directory of Application Server.**

`cd /var/opt/SUNWappserver/domains/domain1/config`

b. Run the command the following.

```
certutil -A -n servercert -t "u,u,u" -d
/var/opt/SUNWappserver/domains/domain1/config -a -i servercert.pem -f password
```

7 Add the CMS `root ca` to the database.

```
certutil -A -n rootca -t "TCu,TCu,TCuw" -d
/var/opt/SUNWappserver/domains/domain1/config -a -i path-to-cert -f password
```

8 Log in to the administrator console of Application Server.

`https://`*hostname.domain-name*`:4849`**

9 Click Configurations -> server-config -> HTTP Service -> HTTP Listeners -> http-listener-2.

Perform the following tasks:

- Verify whether the security is enabled.
- Verify whether the certificate nickname is `servercert`.
- Enable SSL3.
- Enable TLS.
- Select Cipher Suites option.

10 Restart the Application Server.

11 Log in to the Access Manager administrator console.

`http://`*host.domain-name:8080*`/amconsole`**

a. Change success URLs to `https://`*host.domain-name:8181*`/portal`.

b. In the Service Configuration, change the platform server list from `https://`*host:8080*`|01` to `http://`*host*`:8181|01`.

12 Open the `AMConfig.properties` file.

The `AMConfig.properties` file is located in the *AccessManager_base*`/SUNWam/lib` directory.

13 Change `com.iplanet.am.server.protocol` to `https`. Add `com.sun.identity.liberty.authnsvc.url=` `https://`*host.domain-name:8181*`/amserver/Liberty/authnsvc`.

```
com.iplanet.am.server.protocol=https
com.iplanet.am.server.host=host.domain-name
com.iplanet.am.server.port=8181
com.iplanet.am.console.protocol=https
com.iplanet.am.console.host=host.domain-name
com.iplanet.am.console.port=8181
com.iplanet.am.profile.host=host.domain-name
com.iplanet.am.profile.port=8181
```

```
com.iplanet.am.naming.url=https://host.domain-name:8181
/amserver/namingservice
com.iplanet.am.notification.url=https://host.domain-name:8181
/amserver/notificationservice
com.sun.identity.liberty.interaction.wspRedirectHandler=
https://host.domain-name:8181/amserver/WSPRedirectHandler
com.sun.identity.loginurl=https://host.domain-name:8181
/amserver/UI/Login
com.sun.identity.liberty.authnsvc.url=
https://host.domain-name:8181/amserver/Liberty/authnsvc
```

14 Restart Directory Server, Access Manager, Application Server, and Portal Server.

Installing Portal Server 7.1 on BEA WebLogic 8.1

If you want to install Portal Server on BEA WebLogic, you need to install the components in different session.

- Install Directory Server and Application Server or Web Server using the Java ES Installer in the Configure Now mode.
- Install Access Manager using the Java ES installer in the Configure Later mode.
- Install Portal Server using the Java ES installer in the Configure Now or Configure Later mode

---

Note – Portal Server administration console does not work with WebLogic.

Installing Portal Server on BEA WebLogic 8.1

▼ To Install BEA WebLogic 8.1, Directory Server, and Access Manager

1 Install BEA WebLogic 8.1.

2 Create the WebLogic domain and start the administrator server.

```
/usr/local/bea/user_projects/domains/domain1/startWebLogic.sh
```

3 Access the administrator server of BEA WebLogic.

`http://`*host.domain-name*`:7001`

4 Install Directory Server, Java DB 10. 2 and Web Server using the Java ES installer in the Configure Now mode.

5 Start Directory Server instance.

▼ To Install Access Manager on a WebLogic Administrator Server

1 Install Access Manager in the Configure Later mode using the Java ES installer.

a. Customize the `amsamplesilent` file.

The `amsamplesilent` file is located in the following directories:

- Solaris: */AccessManager_base*`/SUNWam/bin`
- Linux: */AccessManager_base*`/sun/identity/bin`

Set the values in the `amasamplesilent` file as follows:

- `DEPLOY_LEVEL = 1`
- `SERVER_NAME` =*AM_HOSTNAME without FQDN*
- `SERVER_HOST = $SERVER_NAME.domain-name`
- `SERVER_PORT = 7001`
- `ADMIN_PORT = 7001`
- `DS_HOST` =*DS_HOSTNAME with FQDN*
- `DS_DIRMGRPASSWD` = *Directory Manager Password*
- `ROOT_SUFFIX` = *root suffix of Access Manager*
- `ADMINPASSWD` = *AM_PASSWORD*
- `AMLDAPUSERPASSWD` = *LDAP_PASSWORD*
- `COOKIE_DOMAIN` =.domain-name
- `AM_ENC_PWD` =*any string of 12 characters*
- `NEW_OWNER = root`
- `NEW_GROUP` = `other` (`root` for the Solaris 10 release and `linux` and `other` for the Solaris 9 release)
- `PAM_SERVICE_NAME = other`
- `WEB_CONTAINER = WL8`
- `BASEDIR` =*Access Manager install directory*
- `AM_REALM = disabled`
- `WL8_HOME` =*WebLogic Install Directory.*, for example, `/usr/local/bea`.
- `WL8_PROJECT_DIR = user_projects`
- `WL8_DOMAIN` = *Domain name.*, for example, `mydomain`)
- `WL8_CONFIG_LOCATION = $WL8_HOME/$WL8_PROJECT_DIR/domains`
- `WL8_SERVER` =*Instance name.* For example, `myserver`

- WL8_PROTOCOL = $SERVER_PROTOCOL
- WL8_HOST = $SERVER_HOST
- WL8_PORT = $SERVER_PORT
- WL8_SSLPORT = $ADMIN_PORT
- WL8_ADMIN =*Administrator name of WebLogic.* For example, weblogic.
- WL8_PASSWORD =*WebLogic administrator password.*
- WL8_JDK_HOME = $WL8_HOME/jdk142_05 for 8.1 sp4 or $WL8_HOME/jdk/142_08 for 8.1sp5

b. Run the *AccessManager_base*/bin/amconfig -s amsamplesilent **script.**

The amsamplesilent file is located in the following directories:

- Solaris: /*AccessManager_base*/SUNWam/bin
- Linux: /*AccessManager_base*/sun/identity/bin

c. Edit the startweblogic.sh **and** startManagedweblogic.sh **scripts and add the following to the classpath:** /opt/SUNWjavadb/lib/derbyclient.jar**.**

For Linux, the derbyclient.jar file is located at the /opt/sun/javadb/lib directory.

d. In the startweblogic.sh **and** startManagedweblogic.sh **scripts, remove the following classpaths:** *AccessManager_base*/SUNWam/lib/jaxrpc_1.0/jaxrpc-api.jar **and** *AccessManager_base*/SUNWam/lib/jaxrpc_1.0/jarpc-ri.jar**.**

e. In the startweblogic.sh **and** startManagedweblogic.sh **scripts, add the following classpaths:** *AccessManager_base*/SUNWam/lib/jaxrpc-api.jar**,** *AccessManager_base*/SUNWam/lib/jaxrpc-impl.jar**, and** *AccessManager_base*/SUNWam/lib/jaxrpc-spi.jar**.**

f. (Optional) For Linux, remove the following classpaths: *AccessManager_base*/identity/lib/jaxrpc_1.0/jaxrpc-api.jar **and** *AccessManager_base*/identity/lib/jaxrpc_1.0/jarpc-ri.jar **from the** startweblogic.sh **and** startManagedweblogic.sh **scripts.**

g. For Linux, add the following classpaths: *AccessManager_base*/identity/lib/jaxrpc-api.jar**,** *AccessManager_base*/identity/lib/jaxrpc-impl.jar**, and** *AccessManager_base*/identity/lib/jaxrpc-spi.jar

2 Restart WebLogic and access the following URL.

http://*host.domain-name***:7001/amconsole**

▼ To Install Portal Server on a WebLogic Administrator Server in the Configure Now Mode

1 Install Portal Server in the Configure Now mode using the Java ES installer.

2 Choose WebLogic as the web container for Portal Server.

Note – In the Portal Server web container panel, ensure that the Managed Server option is not selected. Also, ensure that both the administrator and server ports are `7001`.

---

3 Restart WebLogic server after the successful installation of Portal Server.

Post Installation Steps

1. Access the WebLogic administrator console.

   `http://`*hostname.domain-name***`:7001/console`**
2. Deploy the portal web applications.
3. Deploy the `portal.war`, `communityportlets.war`, `search.war`, and the remaining web applications.
4. Restart the WebLogic server.

▼ To Install Portal Server on a WebLogic Administrator Server in the Configure Later Mode

1 Install Portal Server in the Configure Later mode using the Java ES installer.

2 Complete the Portal Server installation.

3 Change the example files based on the requirements.

Note – You can use the `example15.xml` file to configure Portal Server and search server on WebLogic. In the `example15.xml` file, make sure both the Port and web container administrator port are set to `7001` and web container managed server is set to `false`.

---

4 Configure the common agent container.

PortalServer_base`/bin/psconfig --config` *example15.xml*

The `psconfig` utility is located in the *PortalServer_base*`/SUNWportal/bin` directory on the Solaris platform. For Linux, it is in the */PortalServer_base*`/sunportal/bin` directory.

The example files are located in the *PortalServer_base*`/samples/psconfig` directory for the Solaris platform and *PortalServer_base*`/samples/psconfig` directory for Linux.

Post-Installation Steps

1. Access the WebLogic administrator console.

   `http://`*hostname.domain-name*`:7001/console`
2. Deploy the portal web applications.
3. Deploy `portal.war`, `communityportlets.war`, `search.war`, and the remaining web applications.
4. Restart the WebLogic server.

Installing Portal Server 7.1 on a BEA WebLogic 8.1 Managed Server

You can create a managed server in WebLogic and use the managed server as the web container of Portal Server. You can install Access Manager on a managed server or administrator server of WebLogic.

To install Portal Server on a managed server of WebLogic, you need to:

- Create a managed server.
- Install Portal Server on the managed server in the Configure Now or Configure Later mode.

▼ To Install Portal Server on a WebLogic Managed Server

Before You Begin Install Access Manager on the administrator server of WebLogic 8.1.

1 Start the WebLogic administrator server.

2 Add the IP address of the machine, which has the administrator server of the domain in the *BEAWebLogic_base*`/weblogic81/common/nodemanager/nodemanager.hosts` file.

By default, the `nodemanager.hosts` file is located at the *WebLogic_base*`/usr/local/bea` directory.

3 Start the WebLogic node manager with the IP address of the host as the first argument and the port number on which you want the node manager to run as the second argument.

For example, *WebLogic_base*`/weblogic81/server/bin/startNodeManager.sh` *192.192.10.12 7878*

4 Log in to the WebLogic administrator console.

5 Select Machines.

6 Select Configure a New Machine.

7. **Type a machine name and click Create.**
8. **Select the Node Manager tab.**
9. **Specify the IP address of the host in the listen address and specify the port on which the Node Manager is running.**
10. **Select Servers in the left pane to create a new managed server.**
11. **Select Configure a New Server.**
12. **Specify the server name and machine name and specify the listen port of the managed server.**
13. **Start the managed server from the WebLogic administration console.**

▼ To Install Portal Server on a Managed Server in the Configure Now Mode

Before You Begin

- Install Access Manager in the WebLogic administrator server.
- Install Directory Server.

1. **Install Portal Server in the Configure Now mode using the Java ES installer.**
2. **Select the WebLogic container in the WebLogic container panel.**
3. **Specify the administrator port as `7001` and the server port as the port of the managed server instance.**
4. **Select Managed Server option.**
5. **Restart WebLogic server after the successful installation of Portal Server.**

▼ To Install Portal Server on a Managed Server in the Configure Later Mode

Before You Begin

- Install Access Manager in the WebLogic administrator server.
- Install Directory Server.

1. **Install Portal Server in the Configure Later mode using the Java ES installer.**
2. **Complete the Portal Server installation.**

3 **Change the example files depending on your requirements.**

For WebLogic, you can use the `example15.xml` file to configure Portal Server and Search Server. In the `example15.xml` file, ensure that the Port is set to port of the managed server, web container administrator port is set to `7001`, and web container managed server is set to `true`.

4 **Configure the common agent container.**

PortalServer_base`/bin/psconfig --config` *example15.xml*

The `psconfig` utility is located in the *PortalServer_base*`/bin` directory. It is located in the *PortalServer_base*`/SUNWportal` directory. For Linux, this utility is located in the *PortalServer_base*`/sun/portal` directory. It is located in the *PortalServer_base*`/samples/psconfig` directory for Solaris. It is located in the *PortalServer_base*`/samples/psconfig` directory for Linux.

Note – For more information on the appropriate sample, see the *PortalServer_base*`/samples/psconfig/README.txt` file.

---

5 **Restart WebLogic server after the successful installation of Portal Server.**

▼ To Install Access Manager on a BEA WebLogic Managed Server

In this section, you install Access Manager on a managed server of BEA WebLogic.

1 **Install BEA WebLogic 8.1 using the installer.**

2 **Create WebLogic domain and start administrator server.**

`/usr/local/bea/user_projects/domains/domain1/startWebLogic.sh`

3 **Access the administrator server of BEA WebLogic.**

`http://`*host.domain-name***`:7001`**

4 **Create a managed server.**

5 **Start the Java ES installer. Install Directory Server, Java DB 10. 2 and Web Server in the Configure Now mode.**

6 **Start the Directory Server instance.**

7 **Install Access Manager in the Configure Later mode.**

8 **Customize the `amsamplesilent` file.**

The amsamplesilent file is located in the following directories:

- Solaris platform: /*AccessManager_base*/SUNWam
- Linux platform: /*AccessManager_base*/sun/identity

Set the values in the amasamplesilent file as follows:

- DEPLOY_LEVEL = 1
- SERVER_NAME =*AM_HOSTNAME without FQDN*
- SERVER_HOST = $SERVER_NAME.domain-name
- SERVER_PORT =*MANAGED_SERVER_INSTANCE_PORT*
- ADMIN_PORT = 7001
- DS_HOST =*DS_HOSTNAME with FQDN*
- DS_DIRMGRPASSWD =*Directory Manager Password*
- ROOT_SUFFIX = *root suffix of Access Manager*
- ADMINPASSWD =*AM_PASSWORD*
- AMLDAPUSERPASSWD =*LDAP_PASSWORD*
- COOKIE_DOMAIN = *.domain-name*
- AM_ENC_PWD =*any string of 12 characters*
- NEW_OWNER = root
- NEW_GROUP = other (root for the Solaris 10 release and Linux and other for the Solaris 9 release)
- PAM_SERVICE_NAME = other
- WEB_CONTAINER = WL8
- BASEDIR = *Access Manager install directory.*, for example, /opt
- AM_REALM = disabled
- WL8_HOME =*WebLogic install directory.*, for example, /usr/local/bea)
- WL8_PROJECT_DIR = user_projects
- WL8_DOMAIN = *Domain name.*, for example, mydomain
- WL8_CONFIG_LOCATION = $WL8_HOME/$WL8_PROJECT_DIR/domains
- WL8_SERVER = *Instance name.*, for example, myserver
- WL8_PROTOCOL = $SERVER_PROTOCOL
- WL8_HOST = $SERVER_HOST
- WL8_PORT = $SERVER_PORT
- WL8_SSLPORT = $ADMIN_PORT
- WL8_ADMIN = *Administrator name of WebLogic.*, for example, weblogic
- WL8_PASSWORD = *WebLogic administrator password*

- `WL8_JDK_HOME` = `$WL8_HOME/jdk142_05` for WebLogic 8.1 service pack 4 or `$WL8_HOME/jdk/142_08` for WebLogic 8.1 service pack 5

9. **Run the following command.**

   AccessManager_base`/bin/amconfig -s amsamplesilent`

10. **Log in to the WebLogic administrator console.**

11. **Deploy the Access Manager war files, such as** `amserver.war`, `ampassword.war`, `amconsole.war`, **and** `amcommon.war` **available in the** *AccessManager_base* **directory.**

    a. **In the scripts, remove the following classpaths:**
    AccessManager_base`/SUNWam/lib/jaxrpc_1.0/jaxrpc-api.jar` **and**
    AccessManager_base`/SUNWam/lib/jaxrpc_1.0/jarpc-ri.jar`**.**

    b. **In the scripts, add the following classpaths:**
    AccessManager_base`/SUNWam/lib/jaxrpc-api.jar`,
    AccessManager_base`/SUNWam/lib/jaxrpc-impl.jar`**, and**
    AccessManager_base`/SUNWam/lib/jaxrpc-spi.jar`**.**

    c. **(Optional) For Linux, remove the following classpaths:**
    AccessManager_base`/identity/lib/jaxrpc_1.0/jaxrpc-api.jar` **and**
    AccessManager_base`/identity/lib/jaxrpc_1.0/jarpc-ri.jar` **from the** `startweblogic.sh` **and** `startManagedweblogic.sh` **scripts.**

    d. **(Optional) Add the following classpaths:**
    AccessManager_base`/identity/lib/jaxrpc-api.jar`,
    AccessManager_base`/identity/lib/jaxrpc-impl.jar`**, and**
    AccessManager_base`/identity/lib/jaxrpc-spi.jar`

12. **Restart WebLogic server and access the administrator console.**

    `http://`*host.domain-name*`:`***managed-server-port*`/amconsole`**

▼ To Install Portal Server in the Configure Now Mode on a WebLogic Managed Server Where Access Manager is Installed on a Managed Server

1. **Create a managed server.**

2. **Install Access Manager on the managed server.**

3 **Set** `-Dcom.iplanet.am.serverMode=false` **in the** `startManagedWebLogic.sh` **script if the managed server instance Portal Server is different from the managed server instance of Access Manager. Otherwise, set** `-Dcom.iplanet.am.serverMode=true`**.**

4 **Run the** `/usr/local/bea/domains/mydomain/startManagedWeblogic.sh` **script.**

5 **Start the Java ES installer and install Portal Server in the Configure Now mode.**

6 **Choose WebLogic container in the WebLogic container panel.**

7 **Specify the administrator port as** `7001` **and the server port as the port of the managed server instance.**

8 **Select Managed Server option.**

9 **Restart WebLogic server after the installation of Portal Server.**

▼ To Install Portal Server in the Configure Later Mode on a WebLogic Managed Server Where Access Manager is Installed on a Managed Server

1 **Create a managed server.**

2 **Install Access Manager on the managed server.**

3 **Install Portal Server in the Configure Later mode using the Java ES installer.**

4 **Change the example files based on your requirements.**

For WebLogic, you can use the `example15.xml` file to configure Portal Server and search server. In the `example15.xml` file, ensure that the Port is set to the port of the managed server, the web container administrator port is set to `7001`, and the web container managed server is set to `true`.

5 **Configure the common agent container.**

PortalServer_base`/bin/psconfig --config` *example15.xml*

Note – For more information on the required sample, see the *PortalServer_base*`/samples/psconfig/README.txt` file.

---

6 **Restart WebLogic server after the successful installation of Portal Server.**

▼ To Install `psconsole` on Web Server 7.0

The `psconsole` of Portal Server can be installed only on Web Server or Application server. If you install Portal Server on any of the compatible web containers, such as BEA WebLogic or IBM WebSphere, you need to install `psconsole` on Web Server or Application Server.

1. **Start the Web Server 7.0 administrator server and instance.**

   WebServer_base`/admin-server/bin/startserver`
   WebServer_base`/https-host.domain-name:80/bin/startserv`

2. **Deploy the** *PortalServer_base*`/SUNWportal/admin/psconsole.war` **file on the Web Server 7.0 using the administrator console.**

   a. **Log in to the administrator console.**

   b. **Click the Deployment Pending link.**

   c. **Select Deploy.**

   d. **Select Configurations.**

   e. **Select the configuration in which the** `psconsole.war` **file is to be deployed.**

   f. **Click the java tab.**

   g. **Type** `/usr/lib/cacao/lib/cacao_cacao.jar` **to the Class Path Suffix text box and click Save.**

3. **Access** `psconsole`**.**

   `http://host.domain-name:80/psconsole`

Installing Portal Server 7.1 on an IBM WebSphere Server 5.1.1.6

This section includes procedures to install Portal Server on WebSphere 5.1.1.6 in the following scenarios:

- Installing Portal Server on IBM WebSphere 5.1.1.6 Using in the Configure Now Mode
- Installing Portal Server on IBM WebSphere 5.1.1.6 Using the Configure Later Mode
- Installing psconsole on Web Server 7.0

Note – Portal Server administration console (psconsole) is supported only on Sun Java System Web Server 7.0 and Sun Java System Application Server 8.2.

▼ To Install Portal Server on IBM WebSphere 5.1.1.6 in the Configure Now Mode

1. **Install IBM WebSphere 5.1.1.6.**

2. **Start the IBM WebSphere server.**

3. **Start the Java ES installer. Select Directory Server and Web Server 7.0, and install the components in the Configure Now mode.**

4. **Start the Directory Server instance.**

   DirectoryServer_base`/SUNWdsee/ds6/bin/dsadm start`
   DirectoryServer_base`/SUNWdsee/dsins1`

5. **Start the Java ES installer. Install Access Manager in the Configure Later mode.**

6. **Configure Access Manager on the IBM WebSphere container by modifying the following values in the** `amsamplesilent` **file.**

   The `amsamplesilent` file is located at in the following directories:

   - Solaris platform: `/`*AccessManager_base*`/SUNWam`
   - Linux platform: `/`*AccessManager_base*`/sun/identity`
   - Default: *AccessManagerSample_Location*`/bin`

   Set values in the `amasamplesilent` file as follows:

   - `DEPLOY_LEVEL=1`
   - `SERVER_NAME=`*AM_HOSTNAME without FQDN*
   - `SERVER_HOST=$SERVER_NAME.domain-name`
   - `SERVER_PORT=9080`
   - `ADMIN_PORT=9090`
   - `DS_HOST=`*DS_HOSTNAME with FQDN*
   - `DS_DIRMGRPASSWD=`*Directory Manager Password*
   - `ROOT_SUFFIX=`*root suffix of Access Manager*
   - `ADMINPASSWD=`*AM_PASSWORD*
   - `AMLDAPUSERPASSWD=`*LDAP_PASSWORD*

- COOKIE_DOMAIN=.doamin-name
- AM_ENC_PWD=*string*
- NEW_OWNER=root
- NEW_GROUP=other (root for the Solaris 10 release and Linux and other for the Solaris 9 release)
- PAM_SERVICE_NAME=other
- WEB_CONTAINER=WAS5
- BASEDIR= *Directory where Access Manager is installed.*, for example, */AccessManager_base*/SUNWam
- AM_REALM=disabled
- WAS51_HOME=/WebSphere_base/WebSphere/AppServer
- WAS51_JDK_HOME=/AccessManager_base/WebSphere/AppServer/java
- WAS51_CELL=*Usually hostname without FQDN.* Please check it in your install.
- WAS51_NODE=*Usually hostname without FQDN.* Please check it in your install.
- WAS51_INSTANCE=server1
- WAS51_PROTOCOL=$SERVER_PROTOCOL
- WAS51_HOST=$SERVER_NAME
- WAS51_PORT=9080
- WAS51_SSLPORT=9081
- WAS51_ADMIN=admin
- WAS51_ADMINPORT=9090

7 Run the amsamplesilent **script.**

The amsamplesilent file is located in the following directories

- Solaris platform: */AccessManager_base*/SUNWam
- Linux platform: */AccessManager_base*/sun/identity

8 Verify if Access Manager is functioning properly.

http://*host.domain-name***:9080/amconsole**

9 Install Portal Server in the Configure Now mode using the Java ES installer.

10 Restart IBM WebSphere after the successful installation of the Portal Server.

11 Access the portal.

http://host.domain-name:9080/portal

▼ To Install Portal Server on IBM WebSphere 5.1.1.6 Using the Configure Later Mode

1. **Install IBM WebSphere 5.1.1.6 server.**

2. **Start IBM WebSphere.**

3. **Install Directory Server and Web Server 7.0 in the Configure Later mode using the Java ES installer.**

4. **Start the Directory Server instance.**

   /DirectoryServer_base`/SUNWdsee/ds6/bin/dsadm start`
   `/var/`*DirectoryServer_base*`/SUNWdsee/dsins1`

5. **Install Access Manager in the Configure Later mode using the Java ES installer.**

6. **Configure Access Manager on IBM WebSphere container using the following values in the `amsamplesilent` file.**

   The `amsamplesilent` file is located at:

   - Solaris: */AccessManager_base*`/SUNWam`
   - Linux: */AccessManager_base*`/sun/identity`
   - Default: *AccessManagerSample_Location*`/bin`

   The values in the `amasamplesilent` file is as follows:

   - `DEPLOY_LEVEL=1`
   - `SERVER_NAME=`*AM_HOSTNAME without FQDN*
   - `SERVER_HOST=$SERVER_NAME.sun-name`
   - `SERVER_PORT=9080`
   - `ADMIN_PORT=9090`
   - `DS_HOST=`*DS_HOSTNAME with FQDN*
   - `DS_DIRMGRPASSWD=`*Directory Manager Password*
   - `ROOT_SUFFIX=`root suffix of Access Manager
   - `ADMINPASSWD=`*AM_PASSWORD*
   - `AMLDAPUSERPASSWD=`*LDAP_PASSWORD*
   - `COOKIE_DOMAIN=`*.domain-name*
   - `AM_ENC_PWD=`*any string*
   - `NEW_OWNER=root`

- NEW_GROUP=other (root for the Solaris 10 release and Linux and other for the Solaris 9 relesae)
- PAM_SERVICE_NAME=other
- WEB_CONTAINER=WAS5
- BASEDIR=*Directory where Access Manager is installed.*, for example: */AccessManager_base*/SUNWam
- AM_REALM=disabled
- WAS51_HOME=/WebSphere_base/WebSphere/AppServer
- WAS51_JDK_HOME=/WebSphere/AppServer/java
- WAS51_CELL=*Usually hostname without FQDN.* Please check it in your install.
- WAS51_NODE=*Usually hostname without FQDN.* Please check it in your install.
- WAS51_INSTANCE=server1
- WAS51_PROTOCOL=$SERVER_PROTOCOL
- WAS51_HOST=$SERVER_NAME
- WAS51_PORT=9080
- WAS51_SSLPORT=9081
- WAS51_ADMIN=admin
- WAS51_ADMINPORT=9090

7 **Run the** *AccessManager_base*/SUNam/bin/amconfig -s *AccessManager_base*/SUNam/bin/amsamplesilent **script.**

For Solaris, the amsamplesilent file is available in the */AccessManager_base*/SUNWam directory. For Linux, it is available in the *AccessManager_base*/sun/identify directory.

8 **Verify if Access Manager is functioning properly.**

http://*host.domain-name*:**9080/amconsole**

9 **Install Portal Server in the Configure Later mode using the Java ES installer.**

10 **Modify the example files based on your requirements.**

For IBM WebSphere, you can use the example16.xml file.

11 **Configure the common agent container.**

PortalServer_base/bin/psconfig --config *example16.xml*

◆ ◆ ◆ CHAPTER 5

Installing Access Manager and Portal Server on Different Nodes

When you install Portal Server using the installer, Access Manager is installed on the node where you install Portal Server. However, you can install Access Manager and Portal Server on two different nodes. In this scenario, you need to install Directory Server, Access Manager, and a web container on one node. On the other node, you need to install Portal Server, Access Manager SDK (AMSDK) and a web container. You can install Portal Server in the Configure Now mode or in the Configure Later mode.

This chapter explains the following tasks:

Installing Access Manager and Portal Server on Different Nodes

This section explains how to install Directory Server, Access Manager, and Web Server on Node 1 and Access Manager SDK, Web Server, and Portal Server on Node 2 in the Configure Now and Configure Later modes.

▼ To Install Access Manager and Portal Server on Different Nodes in the Configure Now Mode

1 **Install Directory Server, web container, and Access Manager on Node 1.**

2 **Start the Directory Server and web container instance.**

Note the Access Manager encryption password used on Node 1.

3. **On Node 2, install Portal Server, Access Manager SDK, and a web container in the Configure Now mode.**

4. **Provide the Node 1 details in the Java ES installer.**

   Note – Provide the same encryption key that is used for Access Manager on Node 1. If you have not noted the encryption key, examine the `/etc/opt/SUNWam/amconfig.properties` file on Node 1.

5. **Start the web container instance on Node 2 after the successful installation of Portal Server.**

▼ To Install Access Manager and Portal Server on Different Nodes in the Configure Later Mode

1. **Install Directory Server, web container, and Access Manager on Node 1.**

2. **Start the Directory Server and web container instance.**

   Note – Note the Access Manager encryption password used on Node 1.

3. **On Node 2, install Access Manager SDK and a web container in the Configure Now mode.**

4. **Provide the Node 1 details wherever required.**

   Note – Provide the same encryption key that is used for Access Manager on Node 1. If you have not noted the encryption key, you can examine the `/etc/opt/SUNWam/amconfig.properties` file on Node 1.

5. **Install Portal Server on Node 2 in the Configure Later mode.**

6. **Modify the `example.xml` file, which is available in the** */PrtalServer_base*`/SUNWportal/samples/psconfig` **directory based on the requirement.**

7. **Configure the common agent container.**

   PortalServer_base`/SUNWportal/bin/psconfig --config` *example.xml*

◆ ◆ ◆ CHAPTER 6

Installing and Configuring a Gateway With Portal Server

Configuring a gateway to access Portal Server allows you to access Portals using a secure protocol, `https`. If you have Portal Server installed in an Intranet, you can access Portals from another network through Gateway using Internet. Gateway handles the user requests through the secure protocol.

This chapter includes the following sections:

Configuring Gateway During Installation

This section contains the following procedures:

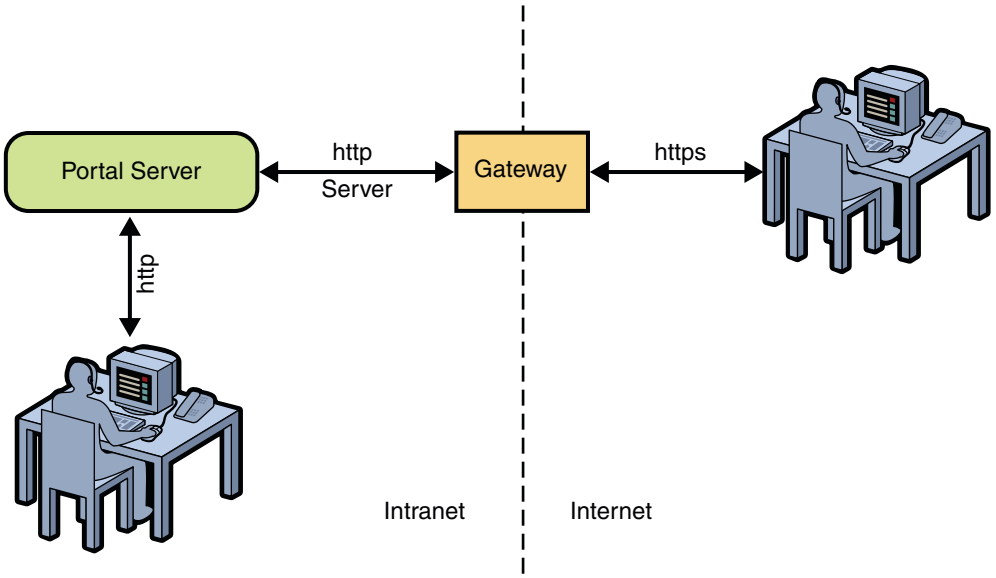

FIGURE 6–1 Portal Server with Gateway

Configuring a Portal Server and a Gateway on a Single Node

This section describes how to configure a Portal Server and a Gateway on a single node in the Configure Now and Configure Later modes.

Using the Configure Now mode, you can configure a Gateway while installing Portal Server, where the Gateway is configured with other components. You can also configure the Gateway using the Configure Later mode, where you need to manually configure Gateway using the `psconfig` command after installing Portal Server.

▼ To Configure Portal Server on a Single Node using the Configure Now Mode

1. **Select the Gateway option displayed with Sun Java System Portal Server Secure Remote Access 7.1 when you install Sun Java System Portal Server 7.1.**
2. **Enter Directory Server, Access Manager, and web container information in the Java ES installer screens.**
3. **Start Directory Server and web container instance after a successful installation of Portal Server.**

4 **Start the gateway.**

PortalServer_base/SUNWportal/bin/psadmin switch-sra-status -u *admin-user-name* -f *password-file* on

PortalServer_base/SUNWportal/bin/psadmin provision-sra -u *admin-user-name* -f *password-file* --gateway-profile *gateway_profile* --enable

PortalServer_base/SUNWportal/bin/psadmin start-sra-instance -u *admin-user-name* -f *password-file* -N default -t gateway

▼ To Configure Portal Server on a Single Node using the Configure Later Mode

1 **Select Sun Java System Portal Server 7.1, Directory Server, and web container in the Java ES installer.**

2 **Select the Gateway option displayed with Sun Java System Portal Server Secure Remote Access 7.1.**

3 **Install the components using the Java ES installer in the Configure Later mode.**

4 **Ensure that Directory Server, web container instance, and web container administrator server are running.**

5 **Modify the** `example7.xml` **file.**

The `example7.xml` file is located in the *PortalServer_base*/SUNWportal/samples/psconfig directory.

6 **Configure common agent container.**

PortalServer_base/SUNWportal/bin/psconfig --config *example7.xml*

7 **Start the Gateway.**

PortalServer_base/SUNWportal/bin/psadmin switch-sra-status -u *admin-user-name* -f *password-file* on

PortalServer_base/SUNWportal/bin/psadmin provision-sra -u *admin-user-name* -f *password-file* --gateway-profile *gateway_profile* --enable

PortalServer_base/SUNWportal/bin/psadmin start-sra-instance -u *admin-user-name* -f *password-file* -N default -t gateway

Configuring Portal Server and Gateway on Separate Nodes

This section describes how to configure Portal Server and Gateway on separate nodes in the Configure Now and Configure Later modes.

Using the Configure Now mode, you can configure a Gateway while installing the Portal Server, where the Gateway is configured with other components. You can also configure the Gateway using the Configure Later mode, where you need to manually configure Gateway using the `psconfig` command after installing Portal Server.

Ensure that the following ports are opened whenever you configure a Gateway or perform any administrator console or command line operations that involve Gateway.

- 11162 : JMX Port (TCP)
- 11161 : SNMP Adapter Port (UDP)
- 11163 : Commandstream Adapter Port (TCP)
- 11164: RMI Connector Port (TCP)

▼ To Configure Portal Server and Gateway on Separate Nodes in the Configure Now Mode

This procedure requires two nodes: Node 1 and Node 2.

1 Install Portal Server and Directory Server in the Configure Now mode on Node 1.

Note – Select Enable SRA for Portal while installing the Portal Server.

---

2 (Optional) Set SRA status to `Enabled` on Node 1, if the Enable SRA for Portal is not selected while installing.

PortalServer_base`/SUNWportal/bin/psadmin switch-sra-status -u` *admin_user* `-f` *password_file* `on`

3 Start the Java ES installer and install Access Manager SDK and Gateway on Node 2 in the Configure Now mode.

Note – Use the same password encryption key on both the nodes.

---

4 Enable Gateway profile on Node 1.

PortalServer_base`/SUNWportal/bin/psadmin provision-sra -u` *admin_user* `-f` *password_file* `--gateway-profile` *gateway_profile* `--enable`

5 **Start the SRA instance on Node 2.**

PortalServer_base/SUNWportal/bin/psadmin switch-sra-status -u *admin-user-name* -f *password-file* on

PortalServer_base/SUNWportal/bin/psadmin provision-sra -u *admin-user-name* -f *password-file* --gateway-profile *gateway_profile* --enable

PortalServer_base/SUNWportal/bin/psadmin start-sra-instance -u *admin-user-name* -f *password-file* -N default -t gateway

▼ To Configure Portal Server and Gateway on Separate Nodes in the Configure Later Mode

1 **Install Portal Server and Directory Server on Node 1 in the Configure Now mode.**

2 **Install AMSDK on Node 2 in the Configure Now mode using the Java ES installer.**

Note – Use the same password encryption key on both the nodes.

---

3 **Install Gateway on Node 2 in the Configure Later mode using the Java ES installer.**

4 **Enable Gateway profile on Node 1.**

PortalServer_base/SUNWportal/bin provision-sra -u *admin_user* -f *password_file* --gateway-profile *gateway_profile* --enable

5 **Modify the** `example10.xml` **file.**

The `example10.xml` file is located in the *PortalServer_base*/SUNWportal/samples/psconfig directory.

6 **Configure common agent container.**

PortalServer_base/SUNWportal/bin/psconfig --config *example10.xml*

7 **Start the Gateway.**

PortalServer_base/SUNWportal/bin/psadmin switch-sra-status -u *admin-user-name* -f *password-file* on

PortalServer_base/SUNWportal/bin/psadmin provision-sra -u *admin-user-name* -f *password-file* --gateway-profile *gateway_profile* --enable

PortalServer_base/SUNWportal/bin/psadmin start-sra-instance -u *admin-user-name* -f *password-file* -N default -t gateway

▼ To Install Gateway on a Non-Default Instance of Application Server

1. **Install Directory Server and Application Server.**
2. **Start Directory Server and Application Server.**
3. **Create a node agent.**

   `asadmin create-node-agent --user` *admin* `--password` *password* `--savemasterpassword=true` *node1*
4. **Start the node agent.**

   `./asadmin start-node-agent --user` *admin* `--password` *password node1*
5. **Create non default server instance.**

   `./asadmin create-instance --user` *admin* `--password` *password* `--nodeagent node1 server1`
6. **Start the instance.**

   `./asadmin start-instance --user` *admin* `--password` *password* `server1`
7. **Install Access Manager in the Configure Later mode.**
8. **Edit the `amsamplesilent` file.**
9. **Restart Directory Server, Application Server, and Access Manager.**
10. **Check if Access manager is up and running.**
11. **Invoke installer and install Portal Server in the Configure Later mode.**
12. **Edit the `example14.xml` file and configure common agent container.**

    `./psconfig --config` *example14.xml*

Installing the Gateway with Portal Server in the SSL Mode

Installing the Gateway with Portal Server in SSL mode allows the user, in the same Intranet where Portal Server is installed, to access Portals through a secure protocol.

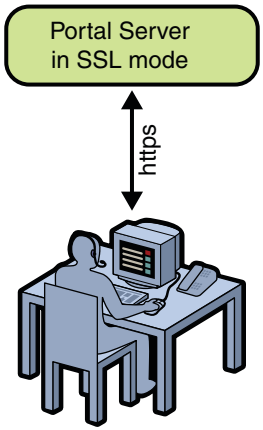

FIGURE 6–2 Portal Server in the SSL mode

To Install Gateway with Portal Server in SSL

1. **Import the root Certificate Authority (CA) to the certificate database.**

   ```
   cd /usr/jdk/entsys-j2se/jre/lib/security
   /usr/jdk/entsys-j2se/jre/bin/keytool -keystore
   cacerts -keyalg RSA -import -trustcacerts -alias
   alias-name -storepass store-password -file
   file-name-path
   ```

2. **Start the Java ES installer and install the Gateway and Access Manager SDK.**

3. **Create a certificate signing request.**

   a. **Run the following command:**

      ```
      PortalServer_base/SUNWportal/bin/certadmin -n default
      ```

   b. **Select Option 2 in the command-line interface.**

   c. **Type the details and save the certificate request in a file.**

4. **Get this certificate signed by the Certificate Authority.**

   The Certificate Authority will be the Portal Server Administrator.

5. **Create a file on the Gateway node, and paste the certificate response.**

6 **Add the signed certificate to the certificate database of Gateway.**

   a. **Run the following command:**
      PortalServer_base/SUNWportal/bin/certadmin -n default

   b. **Select Option 4 in the command-line interface.**

7 **Add the Root Certificate Authority to the certificate database.**

   a. **Run the following command:**
      PortalServer_base/SUNWportal/bin/certadmin -n default

   b. **Select Option 3 in the command-line interface.**

   c. **Provide the path for the Root Certificate Authority.**
      The following message is displayed, "Successfully added."

8 **Restart the Gateway.**

   PortalServer_base/SUNWportal/bin/psadmin switch-sra-status -u *admin-user-name* -f *password-file* on

   PortalServer_base/SUNWportal/bin/psadmin provision-sra -u *admin-user-name* -f *password-file* --gateway-profile *gateway_profile* --enable

   PortalServer_base/SUNWportal/bin/psadmin start-sra-instance -u *admin-user-name* -f *password-file* -N default -t gateway

Creating a Gateway Instance

You can also create an instance of Gateway. This allows the user to contact any one of the Gateway instances and access Portals.

▼ To Create a Gateway Instance

1 **Log in to Portal Server administrator console.**

2 **Click the Secure Remote Access tab.**

3 **Click New Profile.**

4 **Type the new profile name and select the Copy Profile Data From option. Click OK.**

   The following message is displayed: "New profile is successfully created. Please change the relevant ports in the new profile so that they do not clash with those in the existing profiles."

5 **Click OK.**

The Profile screen is displayed.

6 **Click the new profile created and change the port of the instance so that it does not clash with any ports that are in use.**

You need to change both the `http` and `https` port numbers.

7 **Click OK.**

Configuring Personal Digital Certificate (PDC) Authentication

This section describes how to configure a digital certificate for a Gateway.

▼ To Configure Personal Digital Certificate Authentication

Before You Begin

- Ensure that the Gateway and Portal Server are up and running.

1 **Edit the `AMConfig.properties` file on the Portal Server node.**

The `AMConfig.properties` file is located in the *AccessManager_base*`/SUNWam/config` directory.

a. **Add the following line in the `AMConfig.properties` file.**

```
com.iplanet.authentication.modules.cert.gwAuthEnable=yes
```

2 **Import the certificates to the certificate database of the Gateway.**

3 **Import the Root Certificate Authority on the Gateway machine.**

4 **Add the Root Certificate Authority to the Gateway profile.**

a. **Run the following command:**

PortalServer_base`/SUNWportal/bin/certadmin -n` *gateway-profile-name*

b. **Select Option 3 in the command-line interface.**

You are prompted to provide the certificate path. When you provide a valid path, the certificate is added. You will get a message that the certificate is added successfully.

5. **Generate a Certificate Signing Request for submitting to the Certificate Authority.**

   a. **Run the following command:**
   PortalServer_base/SUNWportal/bin/certadmin -n *gateway-profile-name*

   b. **Select Option 2 in the command-line interface.**

   c. **Enter values when prompted.**

   d. **Save the request in a file.**

6. **Submit the Certificate Signing Request to a Certificate Authority and get it approved.**

7. **Save the certificate response on a file after Certificate Authority has signed it.**

8. **Import the certificate response file.**

   a. **Run the following command:**
   PortalServer_base/SUNWportal/bin/certadmin -n *gateway-profile-name*

   b. **Select Option 4 in the Certadmin menu.**

   c. **Provide the location of the certificate response file.**

9. **Import the Root CA certificate on the Portal Server machine.**

```
./certutil -A -n rootca -t "TCu,TCu,TCuw"
-d /var/opt/SUNWappserver/domains/domain1/config
 -a -i rootca-path
```

10. **Register Certificate as an Authentication module.**

    a. **Log in to amconsole as the administrator.**

    b. **Click the Identity Management tab.**

    c. **Select the Organization.**

    d. **Select Services in the View drop-down list.**

    e. **Verify whether the Certificate is displayed in the left pane under the Authentication Modules option.**

    f. **Click Add if the Certificate Service is not displayed in the left pane.**

g. **Select Certificate in the right pane.**
   Certificate is displayed under the Authentication Modules option.

h. **Click OK.**
   Certificate is displayed under the Authentication Modules option in the left pane.

11 **Allow Certificate Authentication to trust any remote host.**

a. **Log in to amconsole as the administrator.**

b. **Click the Identity Management tab.**

c. **Select the Organization.**

d. **Select Services in the View drop-down list.**

e. **Click the Arrow button displayed with the Certificate option.**

f. **Select the None option displayed in the Trusted Remote Hosts list box.**

g. **Click Remove.**

h. **Type `Any` in the text box displayed with the Trusted Remote Hosts list box.**

i. **Click Add, and click Save in the right panel.**

12 **Add Certificate as a required enforcement criterion.**

a. **Log in to amconsole as the administrator.**

b. **Click the Identity Management tab.**

c. **Select the Organization.**

d. **Select Services in the View drop-down list.**

e. **Click the Arrow button that is displayed with the Authentication Configuration option.**
   The Service Instance screen appears.

f. **Click New in the Service Instance screen.**
   The New Service Instance List screen appears.

g. **Enter the service instance name as `gatewaypdc`.**

h. Click Submit.
The Service Instance List screen appears.

i. Click `gatewaypdc` option.
The gatewaypdc Show Properties screen appears.

j. Click the Edit link.

k. Click Add.
The Add Authentication Modules pop-up window appears.

l. Select `Cert` as the Module Name.

m. Select `Required` for Enforcement Criteria.

n. Click OK.
The Authentication Modules pop-up window appears.

o. Click OK and close the pop-up window.

13 Add a dynamic user.

a. Log in to amconsole as the administrator.

b. Click the Arrow button displayed with Core option in the Identity Management tab.

c. Select `gatewaypdc` in the Organization Authentication Modules list box.

d. Select Dynamic from the User Profile drop-down list.

e. Click Save.

14 Add Gateway host in the Portal Server administration console.

a. Log in to Portal Server administration.

b. Click Secure Remote Access.

c. Click the Gateway profile.
The Profile screen appears.

d. Click the Security tab.
The Security Options screen appears.

e. Add the Gateway host name in the Certificate-enabled Gateway Hosts list box.

f. Click Add and click Save.

15 Restart the server.

Note – This is mandatory because the `Amconfig.Properties` is updated.

---

16 Restart the Gateway profile.

17 Install the client certificate issued by the Certificate Authority into the browser.
Access the PDC enabled Gateway.

18 Install the client certificate to the JVM keystore.

a. Click Start > Settings > Control Panel > Java.

b. Add the following parameters in the Applet Run Time parameters:

```
-Djavax.net.ssl.keyStore=keystore-path
 -Djavax.net.ssl.keyStorePassword=password
 -Djavax.net.ssl.keyStoreType=type
```

19 Add portal services to the dynamic user created.

a. Log in to Access Manager administrator console as the administrator.

b. Click the Identity Management tab.

c. Select the Organization.

d. Select Users in the View drop-down list.

e. Add Services to the dynamic user created.

20 Add a dynamic user to the Distinguished Name (DN).

a. Log in to the Portal Server administrator console.

b. Click Portals > Portal name.

c. Add the dynamic user to the DN.

d. Change the Parent Container to JSPTabContainer.

e. **Change Desktop Type of the user to developer_sample, enterprise_sample, or community_sample.**

Installing Load Balancer Plugin and Gateway for Portal Server

This section explains how to install Load Balancer Plugin and Gateway for Portal Server. A Load Balancer handles multiple Portal Server instances. If any one of the Portal Server instances goes down, the Load Balancer automatically redirects the user to the other available Portal Server instance.

A Load Balancer can be installed behind the Gateway or in front of the Gateway. If the Load Balancer is installed behind the Gateway, the user accesses the Portal Server instances through the Gateway. The end user contacts the Gateway. If the Load Balancer is installed in front of the Gateway, the user accesses the Portal Server instances through the Load Balancer.

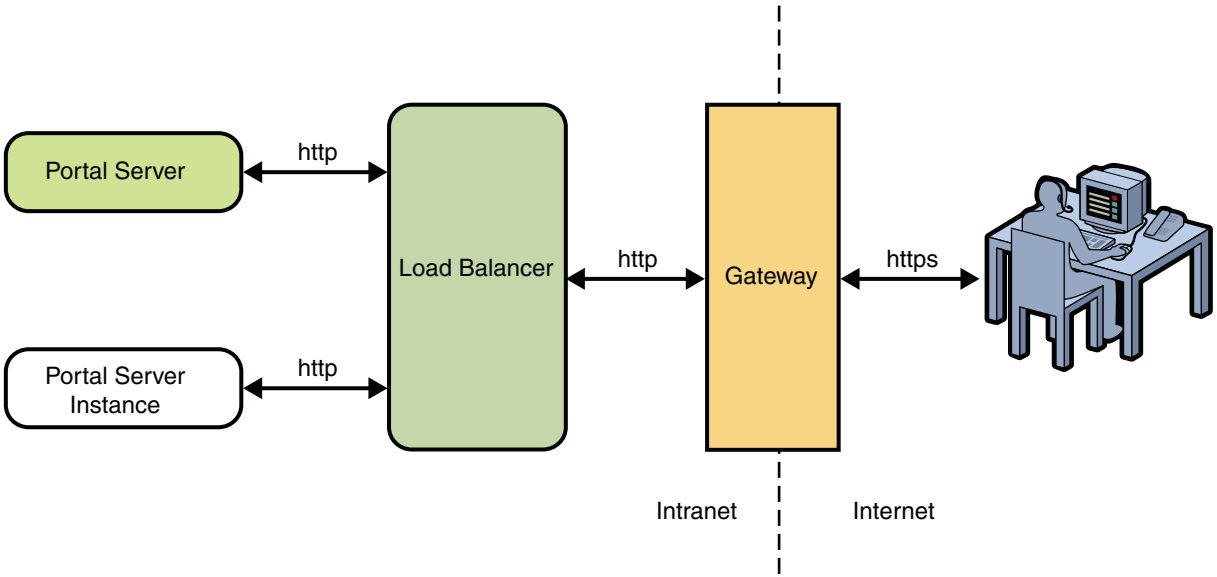

FIGURE 6–3 Portal Server with Load Balancer

This section explains the following:

- "To Install Load Balancer Plugin for Portal Server" on page 99
- "To Install Gateway in Front of the Load Balancer " on page 100

▼ To Install Load Balancer Plugin for Portal Server

This task requires the following:

- Two nodes: Node 1 and Node 2.
- Two Portal Server instances on Node 1 and Node 2.

1 Install the Load Balancer plugin that is available with the Application Server using the Java ES installer.

Note – Select Web Server as a component to install with the Load balancer plugin.

---

2 Edit the `Loadbalancer.xml` file.

The `Loadbalancer.xml` file is located in the *WebServer_base*`/SUNWwbsvr/https-`*node3*`/config/Loadbalancer.xml` directory.

A sample `Loadbalancer.xml` file is displayed as follows:

```
<!DOCTYPE Load Balancer PUBLIC "-//Sun Microsystems Inc.
//DTDSun ONE Application Server 7.1//EN"
"sun-Load Balancer_1_1.dtd">
<Load Balancer>
<cluster name="cluster1">
<!--
Configure the listeners as space seperated URLs like
listeners="http://host:port https://host:port" For example:
<instance name="instance1" enabled="true"
disable-timeout-in-minutes="60"
listeners="http://node1.domain-name:80"/>
<instance name="instance1" enabled="true"
disable-timeout-in-minutes="60"
listeners="http://node2.domain-name:80"/>
-->
<instance name="instance1" enabled="true"
disable-timeout-in-minutes="60"
listeners=""/>
<web-module context-root="/portal" enabled="true"
disable-timeout-in-minutes="60"
error-url="sun-http-lberror.html" />
<web-module context-root="/psconsole" enabled="true"
disable-timeout-in-minutes="60"
error-url="sun-http-lberror.html" />
<health-checker url="/" interval-in-seconds="10"
timeout-in-seconds="30" />
</cluster>
<property name="reload-poll-interval-in-seconds"
value="60"/>
<property name="response-timeout-in-seconds"
```

```
value="30"/>
<property name="https-routing" value="true"/>
<property name="require-monitor-data" value="false"/>
<property name="active-healthcheck-enabled"
value="false"/>
<property name="number-healthcheck-retries"
value="3"/>
<property name="rewrite-location" value="true"/>
</Load Balancer>
```

3 Restart the Web Server and access Portal through the Load Balancer.

▼ To Install Gateway in Front of the Load Balancer

This procedure requires three nodes: Node 1, Node 2, and Node 3.

In this procedure, you do the following:

- Installs Portal Server, Secure Remote Access, Directory Server, Access Manager, and Application Server on Node 1.
- Installs Load Balancer on Node 2.
- Installs Gateway on Node 3.

1 Install Portal Server with Secure Remote Access, Directory Server, Access Manager, and Application Server on Node 1.

2 Install Load Balancer on Node 2.

Load Balancer plugin is available with Application Server 8.2.

Note – Select Web Server as a component to install with Load Balancer.

---

3 Log in to Access Manager administration console on Node 1.

`http://node1:8080/amconsole`

a. Select Services in the in the View drop-down list.

b. Click Administration.

c. Add Load Balancer Fully Qualified Domain Name in the organization aliases.

`http://`*node2.domain-name***`:8080`**

d. Add the Load Balancer URL in the platform service.

`http://`*node1.domain-name***`:8080|`***01*

e. **Click Core.**

f. **Change Default Success Login URL to** `http://`*node1.domain-name*`:8080/portal/dt` **from** `http://`*node2.domain-name*`:8080/portal/dt`**.**

4 **Edit the** `AMConfig.properties` **file.**

The `AMConfig.properties` file is located in the *AccessManager_base*`/SUNWam/Config` directory.

a. **Change** `com.sun.identity.server.fqdnMap` *LB-FQDN]=LB-FQDN* **line in the** `AMConfig.properties` **file with the fully qualified domain name of Load Balancer.**

5 **Restart Portal Server and Application Server on Node 1.**

6 **Log in to Access Manager administrator console and Portal through the Load Balancer.**

`http:`*node2.dommain-name***`:8080/amconsole`**

`http:`*node2.dommain-name***`:8080/portal/dt`**

7 **Install Gateway on Node 3.**

8 **Provide appropriate Portal Server, Access Manager, and Directory Server values in the Installation panels.**

Note – Do not provide any values of the Load Balancer.

The Gateway is installed successfully.

Gateway can be installed in the Configure Later mode also. Change the `example10.xml` file. Set the `PortalAccessURL` as the Load Balancer URL. Set the `PrimaryPortalHost` as the portal where the first portal is installed. This is used to set up trust between two common agent containers. After modifying the `example10.xml` file, run the `psconfig` command to configure Portal Server.

9 **Configure the Gateway to direct to the Load Balancer instead of Portal Server on Node 3.**

a. **Set** `ignoreServerList=true` **in the** `platform.conf.default` **file.**

The `platform.conf.default` file is located in the *PortalServer_base*`/SUNWportal` directory.

b. **Replace Portal host and port information with Load Balancer host and port in the** `platform.conf.default` **file.**

The `platform.conf.default` file is located in the *PortalServer_base*`/SUNWportal` directory.

c. **Replace Portal host and port information with Load Balancer host and port in the `AMConfig-default.properties` file on Node 3.**

   The `AMConfig-default.properties` file is located in the *AccessManager_base*`/SUNWam` directory.

d. **Log in to Portal Server administrator console.**

   `http://`*node1.domain-name*`:8080/psconsole`

e. **Click Secure Remote Access > *gw448*.**

f. **Enter the Load Balancer URL in the Portal Server(s) list displayed in the right panel.**

   `http://`*node2.domain-name*`:8080`

g. **Add the Load Balancer URL in the URLs to which User Session Cookie is Forwarded list.**

h. **Click the Security tab.**

i. **Add the Load Balancer URL for Access Manager console and Access Manger server in the Non-authenticated URLs list.**

   `http://`*node2.domain-name*`:8080/amconsole`

   `http://`*node2.domain-name*`:8080/amserver`

j. **Configure the `enableSRAforPortal.xml` file.**

   `PortalServer_base/SUNWportal/bin/psadmin provision-sra` *enableSRAforPortal.xml*

10 **Restart Gateway.**

Installing and Creating Instances of Netlet and Rewriter Proxies

This section explains how to install Netlet Proxy and Rewriter Proxy. This section also explains how to create a second instance of Netlet and Rewriter proxies using the `psadmin` command.

This section includes the following:

To Install Netlet Proxy in the Configure Now Mode

1. **Invoke the Java ES installer.**
2. **Select Netlet Proxy in the Components Selection screen and proceed with the installation.**
3. **Specify the Host IP Address, Access Port (default: 10555), and the Profile Name to which the Netlet Proxy instance needs to be associated in the Portal Server: Secure Remote Access: Configure Netlet Proxy panel.**
4. **Verify whether the Netlet Proxy instance is running.**

   `netstat -an | grep` *PORT*

To Install Netlet Proxy in the Configure Later Mode

1. **Install Netlet Proxy in the Configure Later mode using the Java ES installer.**
2. **Modify the** `example11.xml` **with the appropriate values.**

   The attributes within `<NetletPoxy profile=`*profilename*`>...</NetletProxy>` tags need to be changed.
3. **Configure** `example11.xml`**.**

   PortalServer_base`/SUNWportal/bin/psconfig --config` *example11.xml*
4. **Start Netlet Proxy.**

To Create a Second Instance of Netlet Proxy Using the `psadmin` Command

1. **Install Netlet Proxy in the Configure Later mode using the Java ES installer.**
2. **Configure common agent container by modifying the** `example2.xml` **file.**
3. **Configure the common agent container.**

   PortalServer_base`/SUNWportal/bin/psconfig --config example2.xml`
4. **Copy the** `NLPConfig.properties.template` **file to a temporary location.**

   `cp` *PortalServer_base*`/SUNWportal/template/sra/NLPConfig.properties.template /tmp`

5 **Modify the values for an existing profile.**

6 **Create a Netlet Proxy instance.**

`psadmin create-sra-instance -u` *admin-user-name* `-f` *PASSWORDFILE* `-S` */tmp/NLPConfig.properties.template* `-t` *nlproxy*

7 **Start Netlet Proxy.**

▼ To Install Rewriter Proxy in the Configure Now mode

1 **Invoke the Java ES installer.**

2 **Select Rewriter Proxy in the Components Selection screen, and proceed with the installation.**

3 **Specify the Host IP Address, Access Port (default: 10443), and the Profile Name to which this Rewriter Proxy instance needs to be associated in the Portal Server: Secure Remote Access: Configure Rewriter Proxy screen.**

4 **Check whether the Rewriter Proxy instance is running:**

`netstat -an | grep` *PORT*

▼ To Install Rewriter Proxy in the Configure Later Mode

1 **Install Rewriter Proxy in the Configure Later mode using the Java ES installer.**

2 **Modify the `example11.xml` file with the appropriate values.**

The attributes within the `<RewriterPoxy profile=`*profilename*`>...</RewriterProxy>` tags need to be changed for Rewriter proxy.

3 **Configure the common agent container.**

PortalServer_base`/SUNWportal/bin/psconfig --config` *example11.xml*

4 **Start Rewriter Proxy.**

▼ To Create a Second Instance of Rewriter Proxy Using the `psadmin` Command

1. **Install Rewriter Proxy in Configure Later mode using the Java ES installer.**
2. **Configure common agent container by modifying the `example2.xml` file.**
   PortalServer_base`/SUNWportal/bin/psconfig --config` *example2.xml*
3. **Copy the `RWPConfig.properties.template` file to a temporary location.**
   `cp` *PortalServer_base*`/SUNWportal/template/sra/RWPConfig.properties.template` */tmp*
4. **Modify the values for an SRA profile.**
5. **Create a Rewriter Proxy.**
   PortalServer_base`/SUNWportal/bin/psadmin create-sra-instance -u` *admin-user-name* `-f` *PASSWORDFILE* `-S` */tmp*`/RWPConfig.properties.template -t` *rwproxy*
6. **Start Rewriter Proxy.**

◆ ◆ ◆ CHAPTER 7

Creating Multi-Portal Instances

You can create a new Portal Server or an instance of a Portal Server using the same Access Manger and Directory Server that you used to create the first or existing Portal Server instance. Creating a new Portal Server helps you to create Portal Severs for different purposes, for example, for different departments of an organization. Creating a new Portal Server instance enables you to cluster portal instances so that the user can access other instances if one Portal Server instance is down.

Note – When you create a new portal or Portal Server instance, you need to ensure that Portal Server, Access Manager, and Directory Server on the first installation are running.

This chapter contains the following sections:

Creating a New Portal

After creating a Portal Server installation on a node, you can create another Portal Server installation on the same node or different nodes using the same Access Manager and Directory Server. This new Portal Server installation is empty. You can use the sample portals provided to customize the portal for your specific needs. For example, you could create portals for different departments of an organization but still use the same Access Manager and Directory Server.

This section explains about creating a new portal installation on the same node or different node depending on your first Portal Server installation.

Creating a New Portal on the Same Node

When you create a new portal on the same node where you have the first Portal Server installation, you need to create a web container instance. Then, you need to duplicate the `Webcontainer.properties` file that is available in the Portal Server installation directory and modify the `Webcontainer.properties` file to direct to the new web container instance. Finally, you can run the `psadmin create-portal` sub command to create the new portal.

This section explains how to create a new portal on different web containers, such as Sun Java System Web Server, Sun Java System Application Server, IBM WebSphere, and BEA Web Logic.

▼ To Create a New Portal on a New Configuration of Web Server 7.0

Before You Begin Ensure the following:

- The first Portal Server installation is up and running.
- Access Manager Administrator console is accessible.
- Web Server 7.0 is installed in the default directory.

1 Create a new configuration of Web Server 7.0 on the same node where first portal is up and running.

2 Name the configuration `secondportal` and assign the port `8100`.

3 Copy the *PortalServer_base*`/SUNWportal/template/Webcontainer.properties.SJSWS7` file to a *PortalServer_base*`/SUNWportal/bin/secondportal.properties` file.

4 Edit the following properties in the `secondportal.properties` file.

- `Host=`*hostname.domain*
- `Port=8100`
- `Scheme=`http
- `WebContainerType=SJSWS7`
- `WebContainerInstallDir=`/opt/SUNWwbsvr7
- `WebContainerInstanceName=`*secondportal*
- `WebContainerDomainName=`*secondportal*
- `WebContainerDocRoot=`/var/SUNWwbsvr7/docs
- `WebContainerAdminHost=`*hostname.domain*
- `WebContainerAdminPort=`8989
- `WebContainerAdminScheme=`https
- `WebContainerAdminUid=`*admin*

5 Create the new portal.

PortalServer_base`/SUNWportal/bin/psadmin create-portal -u` *amadmin* `-f` *ps_password* `-p` *secondportal* `--uri` */portal* `-w` *secondportal.properties*

Note – The `ps_password` file contains the Access Manager password.

6. **Restart the web container.**

7. **Verify whether the new portal has been created.**

   PortalServer_base`/SUNWportal/bin/psadmin list-portals -u` *amadmin* `-f` *ps_password*

To Create a New Portal on a New Domain of Application Server 8.2

1. **Create a new domain,** `seconddomain`**, on port 8100.**

   /ApplicationServer_base`/appserver/bin/asadmin create-domain --adminport` *4850* `--adminuser` *admin* `--instanceport` *8100 seconddomain*

2. **Start the new domain.**

   /ApplicationServer_base`/appserver/bin/asadmin start-domain --user` *admin seconddomain*

3. **Copy the** *PortalServer_base*`/SUNWportal/template/Webcontainer.properties.SJSAS81` **file to a** *PortalServer_base*`/SUNWportal/bin/secondportal.properties` **file.**

4. **Edit the following properties in the** `secondportal.properties` **file.**

   - `Host=`*hostname.domain*
   - `Port=`8100
   - `Scheme=`http
   - `WebContainerType=`SJSAS81
   - `WebContainerInstallDir=`/opt/SUNWappserver/appserver
   - `WebContainerInstanceName=`server
   - `WebContainerDomainName=`*seconddomain*
   - `WebContainerInstanceDir=`/var/opt/SUNWappserver/domains/*seconddomain*
   - `WebContainerDocRoot=`/var/opt/SUNWappserver/domains/*seconddomain*/docroot
   - `WebContainerAdminHost=`*hostname.domain*
   - `WebContainerAdminPort=`4850
   - `WebContainerAdminScheme=`https
   - `WebContainerAdminUid=`*admin*
   - `WebContainerAdminPassword=`*ApplicationServer admin password*
   - `WebContainerMasterPassword=`*ApplicationServer master password*

5. **Create the new portal.**

   PortalServer_base`/SUNWportal/bin/psadmin create-portal -u` *amadmin* `-f` *ps_password* `-p -secondportal --uri` */portal* `-w` *secondportal.properties*

6. **Restart the web container.**

7. **Verify that the new portal has been created.**

   PortalServer_base`/SUNWportal/bin/psadmin list-portals -u` *amadmin* `-f` *ps_password*

▼ To Create a New Portal on a New Domain of BEA WebLogic 8.1 Service Pack 5

1. **Create a WebLogic domain,** `seconddomain` **running on port** `7002`**.**

2. **Create a managed server,** `7022server`**, running on port** `7022`**.**

3. **Go to the** *WebLogic_base*`/user_projects/domains/seconddomain` **directory and start the managed server.**

   ```
   ./startWeblogic.sh
   ```

   ```
   ./startManagedWeblogic.sh 7022server
   ```

4. **Copy the** *PortalServer_base*`/SUNWportal/template/Webcontainer.properties.BEAWL8` **file to a** *PortalServer_base*`/SUNWportal/bin/secondportal.properties` **file.**

5. **Edit the following properties in the** `secondportal.properties` **file.**

   - `Host=`*hostname.domain*
   - `Port=`*7022*
   - `Scheme=`http
   - `WebContainerType=`BEAWL8
   - `WebContainerInstallDir=`/usr/local/bea/weblogic81
   - `WebContainerInstanceName=`*7022server*
   - `WebContainerInstanceDir=`/usr/local/bea/user_projects/domains/*seconddomain*
   - `WebContainerDocRoot=`*LEAVE BLANK*
   - `WebContainerAdminHost=`*hostname.domain*
   - `WebContainerAdminPort=`7002
   - `WebContainerAdminScheme=`http
   - `WebContainerAdminUid=`*admin userid*
   - `WebContainerAdminPassword=`*admin passwd*
   - `WebContainerJDKDir=`/usr/local/bea/jdk142_08
   - `WebContainerManagedServer=true`

     The value is `false`, if new portal is installed on the administrator server itself.

6 **Create the new portal.**

PortalServer_base/SUNWportal/bin/psadmin create-portal -u *amadmin* -f *ps_password* -p *secondportal* --uri */portal* -w *secondportal.properties*

7 **Restart the web container.**

8 **Verify that the new portal has been created.**

PortalServer_base/SUNWportal/bin/psadmin list-portals -u *amadmin* -f *ps_password*

▼ To Create a New Portal on a New Domain of WebSphere 5.1.1.6

1 **Create a WebSphere domain and start the domain.**

2 **Copy the** *PortalServer_base*/SUNWportal/template/Webcontainer.properties.IBMWAS5 **to a** *PortalServer_base*/SUNWportal/bin/secondportal.properties **file.**

3 **Edit the following properties in the** secondportal.properties **file.**

- Host=*hostname.domain*
- Port=9080
- Scheme=http
- WebContainerType=
- WebContainerInstallDir=/optM/WebSphere/Express51/AppServer
- WebContainerInstanceName=*server1*
- WebContainerDomainName=*LEAVE BLANK*
- WebContainerInstanceDir=*LEAVE BLANK*
- WebContainerDocRoot=*LEAVE BLANK*
- WebContainerAdminHost=*hostname.domain*
- WebContainerAdminPort=9090
- WebContainerAdminScheme=http
- WebContainerAdminUid=*admin userid*
- WebContainerAdminPassword=*admin passwd*
- WebContainerJDKDir=/opt/IBM/WebSphere/Express51/AppServer/java
- WebContainerDeployCell=*Usually hostname without FQDN. Please check it in your install.*
- WebContainerDeployNode=*Usually hostname without FQDN. Please check it in your install.*

4 **Create the new portal.**

PortalServer_base/SUNWportal/bin/psadmin create-portal -u *amadmin* -f *ps_password* -p *second-portal* --uri */portal* -w *second-portal.properties*

5 **Restart the web container.**

6 **Verify that the new portal is created.**

PortalServer_base/SUNWportal/bin/psadmin list-portals -u *amadmin* -f *ps_password*

Creating a New Portal on a Remote Node

This section explains how to create a new portal on a remote node. When you create a new portal on a remote node, you should install Access Manager SDK (AMSDK) and a compatible web container. When you install AMSDK, you need to provide the details of Access Manager and Identity Server that you installed for the Portal Server installation. You need to install Portal Server in the Configure Now or Configure Later mode. All the procedures that are explained in this section use the web container of the first portal installation for the second portal installation on a remote node.

Note – When you install AMSDK, provide the same encryption key, am password, and LDAP password that are used for Access Manager on Node 1.

After you install AMSDK and the web container, you can use any one of the following options to create a new portal:

- Using Portal Server in the Configure Now Mode: When you create a new portal in the Configure Now mode, you can create only one portal on a node. The installer prevents you from creating another portal on a node where you already have a portal.
- Using Portal Server in the Configure Later Mode: When you create a new portal in the Configure Later mode, you can create several portals on the same node. You need to create web container instances and change the example files. You can create portals by running the `psconfig` command.
- Using the `psadmin` command: Using the `psadmin` command, you can create several portals on the same node. You need to create web container instances, and run the `psadmin create-portal` sub command.

▼ To Create a New Portal on Web Server 7.0 in the Configure Now Mode

Before You Begin Ensure the following:

- Portal Server, Access Manager, and Common Agent Container are up and running on the first node. Execute the following command:
  `PortalServer-base/SUNWportal/bin/psadmin list-portals -u` *user-name* `-f` *admin-password*
- Access Manager Administrator console is accessible.
- A web container is installed at the default location.

1. **Run the Java ES installer.**
2. **Select Web Server 7.0, Access Manager SDK, and Portal Server and run it in the Configure Now mode.**

   In the Installer panels, provide the details about the Directory Server and Access Manager of the first Portal Server installation.
3. **Change the name of the Portal.**

   For example, the first portal will be `portal1`, so change the name of the second portal to `portal2`.
4. **Complete the installation.**

▼ To Create a New Portal on Web Server 7.0 in the Configure Later Mode

Before You Begin Ensure the following:

- Portal Server, Access Manager, and Common Agent Container are up and running on the first node. Execute the following command on Node 1:
  `PortalServer-base/SUNWportal/bin/psadmin list-portals -u` *user-name* `-f` *admin-password*

1. **Install Access Manager SDK and Web Server 7.0 in the Configure Now mode using the Java ES installer.**

   In the installer pages, provide the details about the Directory Server and Access Manager of the first Portal Server installation.
2. **Start the Web Server 7.0 administrator server.**

   WebServer_base`/admin-server/bin/startserv`
3. **Start the Web Server 7.0 instance configuration.**

   WebServer_base`/https-`*hostname.domain*`/bin/startserv`
4. **Use the installer to install Portal Server in the Configure Later mode.**

5 **Modify the example files accordingly.**

For Web Server 7.0, you can use one of the following example files depending on the requirements:

- `example1.xml`
- `example3.xml`
- `example4.xml`
- `example5.xml`
- `example6.xml`
- `example7.xml`
- `example8.xml`
- `example9.xml`
- `example13.xml`
- `example17.xml`

6 **Complete the Portal Server installation.**

PortalServer_base`/bin/psconfig --config` *examplefile*

▼ To Create a New Portal on Web Server 7.0 Using the `psadmin` Command

Before You Begin Ensure the following:

- Portal Server, Access Manager, and Common Agent Container are up and running on the first node. Execute the following command on Node 1:
  `PortalServer-base/SUNWportal/bin/psadmin list-portals -u` *user-name* `-f` *admin-password*

1 **Install Access Manager SDK and Web Server 7.0 in the Configure Now mode using the Java ES installer.**

2 **Start the Web Server 7.0 administrator server.**

WebServer_base`/admin-server/bin/startserv`

3 **Start the Web Server 7.0 instance.**

WebServer_base`/https-`*hostname.domain*`/bin/startserv`

4 **Install Portal Server in the Configure Now mode using the Java ES installer.**

5 **Configure the common agent container and Java DB.**

PortalServer_base`/bin/psconfig --config` *example2.xml*

6 **Verify whether the common agent container is working properly.**

PortalServer_base`/SUNWportal/bin/psadmin list-portals -u` *amadmin* `-f` *ps_password*

7. **Copy the** *PortalServer_base*`/SUNWportal/template/Webcontainer.properties.SJSWS7` **file to a** *PortalServer_base*`/SUNWportal/bin/secondportal.properties` **file.**

8. **Edit the following properties in the** `secondportal.properties` **file.**

   - `Host=hostname.domain`
   - `Port=80`
   - `Scheme=http`
   - `WebContainerType=SJSWS7`
   - `WebContainerInstallDir=/opt/SUNWwbsvr7`
   - `WebContainerInstanceName=`*hostname.domain*
   - `WebContainerDomainName=`*hostname.domain*
   - `WebContainerDocRoot=/var/opt/SUNWwbsvr7/docs`
   - `WebContainerAdminHost=`*hostname.domain*
   - `WebContainerAdminPort=8989`
   - `WebContainerAdminScheme=https`
   - `WebContainerAdminUid=`*admin*
   - `WebContainerAdminPassword=`*Webserver7.0 admin password*

9. **Create the new portal.**

   PortalServer_base`/SUNWportal/bin/psadmin create-portal -u` *amadmin* `-f` *ps_password* `-p` *secondportal* `--uri` */portal* `-w` *secondportal.properties*

   Note – The `ps_password` file contains the Access Manager password.

10. **Restart the web container.**

11. **Verify that the new portal has been created.**

    PortalServer_base`/SUNWportal/bin/psadmin list-portals -u` *amadmin* `-f` *ps_password*

▼ To Create a New Portal on Application Server 8.2 in the Configure Now Mode

Before You Begin Ensure the following:

- Portal Server, Access Manager, and Common Agent Container are up and running on the first node. Execute the following command on Node 1:
  `PortalServer-base/SUNWportal/bin/psadmin list-portals -u` *user-name* `-f` *admin-password*

1. **Start the Java ES installer and select Application Server 8.2, Access Manager SDK, and Portal Server and install them in the Configure Now mode.**

2. **Provide the Access Manager host and the Directory Server host information.**

3 **Change the name of the portal.**

For example, first portal will be `portal1`. Change the second portal name to `portal2`.

▼ To Create a New Portal on Application Server 8.2 in the Configure Later Mode

Before You Begin Ensure the following:

- Portal Server, Access Manager, and Common Agent Container are up and running on the first node. Execute the following command on Node 1:
  `PortalServer-base/SUNWportal/bin/psadmin list-portals -u` *user-name* `-f` *admin-password*

1 **Install Access Manager SDK and Application Server 8.2 in the Configure Now mode using the Java ES installer.**

2 **Start the Application Server 8.2 administrator server.**

ApplicationServer_base`/appserver/bin/asadmin start-domain --user` *admin_user* `--password` *admin_password domain-name*

3 **Install Portal Server in the Configure Later mode using the Java ES installer.**

4 **Complete the Portal Server installation.**

PortalServer_base`/bin/psconfig --config` *example7.xml*

▼ To Create a New Portal on Application Server 8.2 Using the `psadmin` Command

Before You Begin Ensure the following:

- Portal Server, Access Manager, and Common Agent Container are up and running on the first node. Execute the following command on Node 1:
  `PortalServer-base/SUNWportal/bin/psadmin list-portals -u` *user-name* `-f` *admin-password*

1 **Install Access Manager SDK and Application Server 8.2 in the Configure Now mode using the Java ES installer.**

2 **Start the Application Server 8.2.**

ApplicationServer_base`/appserver/bin/asadmin start-domain --user` *admin_user* `--password` *admin_password domain-name*

3 **Run the installer and install Portal Server software in the Configure Later mode.**

4. **Configure common agent container and Java DB.**

   PortalServer_base`/bin/psconfig --config` *example2.xml*

5. **Verify that the common agent container is working properly.**

   PortalServer_base`/SUNWportal/bin/psadmin list-portals -u` *amadmin* `-f` *ps_password*

6. **Copy the** *PortalServer_base*`/SUNWportal/template/Webcontainer.properties.SJSWS7` **file to a** *PortalServer_base*`/SUNWportal/bin/secondportal.properties` **file.**

7. **Edit the following properties in the** `secondportal.properties` **file.**

   - `Host=`*hostname.domain*
   - `Port=`8080
   - `Scheme=`http
   - `WebContainerType=`SJSAS81
   - `WebContainerInstallDir=`/opt/SUNWappserver/appserver
   - `WebContainerInstanceName=`server
   - `WebContainerDomainName=`domain1
   - `WebContainerInstanceDir=`/var/opt/SUNWappserver/domains/domain1
   - `WebContainerDocRoot=`/var/opt/SUNWappserver/domains/domain1/docroot
   - `WebContainerAdminHost=`*hostname.domain*
   - `WebContainerAdminPort=`4849
   - `WebContainerAdminScheme=`https
   - `WebContainerAdminUid=`*admin id*
   - `WebContainerAdminPassword=`*ApplicationServer admin password*
   - `WebContainerMasterPassword=`*ApplicationServer master password*

8. **Create the new portal.**

   PortalServer_base`/SUNWportal/bin/psadmin create-portal -u` *amadmin* `-f` *ps_password* `-p` *secondportal* `--uri` */portal* `-w` *secondportal.properties*

9. **Restart the web container.**

10. **Verify that the new portal has been created.**

    PortalServer_base`/SUNWportal/bin/psadmin list-portals -u` *amadmin* `-f` *ps_password*

▼ To Create a New Portal on WebLogic 8.1 Service Pack 5 in the Configure Now Mode

Before You Begin Ensure the following:

- Portal Server, Access Manager, and Common Agent Container are up and running on the first node. Execute the following command on Node 1:
  `PortalServer-base/SUNWportal/bin/psadmin list-portals -u` *user-name* `-f` *admin-password*

1 Install WebLogic 8.1 Service Pack 5 and create a managed server in a domain.

2 Start the administrator server and managed server.

3 Run the installer and select Access Manager SDK and install in the Configure Later mode.

4 Edit the values in the `amsamplesilent` file.

For Solaris, the `amsamplesilent` file is present in the */AccessManager_base*`/SUNWam/bin` directory. For Linux, it is in the */AccessManager_base*`/sun/identity` directory.

5 Change the following values in the `amsamplesilent` file.

- `DEPLOY_LEVEL=`4
- `SERVER_NAME=`*AccessManager host name without FQDN*
- `SERVER_HOST=`$SERVER_NAME.domain-name
- `SERVER_PORT=`*AccessManager Server Port*
- `ADMIN_PORT=`*Admin port for the web container on which Access Manager resides*
- `DS_HOST=`*DirectoryServer hostname with FQDN*
- `DS_DIRMGRPASSWD=`*Directory Manager password*
- `ROOT_SUFFIX=`*root suffix of AccessManager*
- `ADMINPASSWD=`*AccessManager_password*
- `AMLDAPUSERPASSWD=`*LDAP_password*
- `COOKIE_DOMAIN=`.doamin-name
- `AM_ENC_PWD=`*any string*
- `NEW_OWNER=`root
- `NEW_GROUP=`other

  This value is `root` for the Solaris 10 release and Linux, and `other` for the Solaris 9 release.
- `PAM_SERVICE_NAME=`other
- `WEB_CONTAINER=`WL8
- `BASEDIR=`*Directory where Access Manager SDK is installed.*

  For example, */AccessManager_base*`/SUNWam`
- `CONSOLE_HOST=`*FQDN of host where Portal needs to be installed*

- CONSOLE_PORT=*Port where second Portal needs to be installed, which is the port of the managed server*
- CONSOLE_PROTOCOL=*$SERVER_PROTOCOL*
- AM_REALM=disabled
- WL8_HOME=/usr/local/bea
- WL8_PROJECT_DIR=user_projects
- WL8_DOMAIN=mydomain
- WL8_CONFIG_LOCATION=$WL8_HOME/$WL8_PROJECT_DIR/domains
- WL8_SERVER= myserver

  Name of the managed server on which second Portal needs to be installed.
- WL8_INSTANCE=$WL8_HOME/weblogic81
- WL8_PROTOCOL=$SERVER_PROTOCOL
- WL8_HOST=*FQDN of the node on which second Portal needs to be installed*
- WL8_PORT=*Port where the second Portal needs to be installed, which is the port of the managed server*
- WL8_SSLPORT=*Weblogic ADMIN_PORT*
- WL8_ADMIN=weblogic
- WL8_PASSWORD=*weblogic admin password*
- WL8_JDK_HOME=$WL8_HOME/jdk142_08

6 Run the following command:

AccessManager_base/SUNWam/bin/amconfig -s
AccessManager_base/SUNWam/bin/amsamplesilent

For Linux, the amsamplesilent utility is available in the /*AccessManager_base*/sun/identity directory.

7 Run the installer again and install portal in the Configure Now mode.

8 Change the name of the portal.

For example, if the first portal is portal1, change name of the second portal to portal2.

▼ To Create a New Portal on WebLogic 8.1 Service Pack 5 in the Configure Later Mode

Before You Begin Ensure the following:

- Portal Server, Access Manager, and Common Agent Container are up and running on the first node. Execute the following command on Node 1:
  `PortalServer-base/SUNWportal/bin/psadmin list-portals -u` *user-name* `-f` *admin-password*

1 Install WebLogic 8.1 Service Pack 5 and create a managed server in a domain.

2 Start the WebLogic administrator server and managed server.

3 Start the Installer and select Access Manager SDK and install it in the Configure Later mode.

4 Edit values in the `amsamplesilent` file.

For Solaris, the `amsamplesilent` file is present in the */AccessManager_base*`/SUNWam/bin` directory. For Linux, it is in the */AccessManager_base*`/sun/identity` directory.

5 Change the following values in the `amsamplesilent` file.

- `DEPLOY_LEVEL=4`
- `SERVER_NAME=`*AccessManager_host name without FQDN*
- `SERVER_HOST=`*$SERVER_NAME.domain-name*
- `SERVER_PORT=`*AccessManager_server_port*
- `ADMIN_PORT=`*Admin port for the web container on which Access Manager resides*
- `DS_HOST=`*DirectoryServer hostname with FQDN*
- `DS_DIRMGRPASSWD=`*Directory Manager Password*
- `ROOT_SUFFIX=`*root suffix of Access Manager*
- `ADMINPASSWD=`*AccessManager Password*
- `AMLDAPUSERPASSWD=`*LDAP Password*
- `COOKIE_DOMAIN=.domain-name`
- `AM_ENC_PWD=`*any string*
- `NEW_OWNER=`root
- `NEW_GROUP=`other

  (This value is `root` for the Solaris 10 release and Linux, and `other` for the Solaris 9 release)
- `PAM_SERVICE_NAME=`other
- `WEB_CONTAINER=`WL8
- `BASEDIR=`*Directory where Access Manager SDK is installed.*
- `CONSOLE_HOST=`*FQDN of host where Portal needs to be installed*
- `CONSOLE_PORT=`*Port where second Portal needs to be installed, which is the port of the managed server*

- CONSOLE_PROTOCOL=$SERVER_PROTOCOL
- AM_REALM=disabled
- WL8_HOME=/usr/local/bea
- WL8_PROJECT_DIR=user_projects
- WL8_DOMAIN=mydomain
- WL8_CONFIG_LOCATION=$WL8_HOME/$WL8_PROJECT_DIR/domains
- WL8_SERVER=myserver*name of the managed server on which second Portal needs to be installed*
- WL8_INSTANCE=$WL8_HOME/weblogic81
- WL8_PROTOCOL=$SERVER_PROTOCOL
- WL8_HOST=*FQDN of the node on which second Portal needs to be installed*
- WL8_PORT=*Port where the second Portal needs to be installed, which is the port of the managed server*
- WL8_SSLPORT=*Weblogic admin port*
- WL8_ADMIN="weblogic"
- WL8_PASSWORD=*weblogic admin password*
- WL8_JDK_HOME=$WL8_HOME/jdk142_08

6 Run the following command:

AccessManager_base/SUNWam/bin/amconfig -s
AccessManager_base/SUNWam/bin/amsamplesilent

For Linux, the amsamplesilent utility is available in the /*AccessManager_base*/sun/identity directory.

7 Run the installer and install portal in the Configure Later mode.

8 Complete the portal Server installation.

PortalServer_base/bin/psconfig --config *example15.xml*

▼ To Create a New Portal on WebLogic 8.1 Service Pack 5 Using the psadmin Command

Before You Begin Ensure the following:

- Portal Server, Access Manager, and Common Agent Container are up and running on the first node. Execute the following command on Node 1:
  PortalServer-base/SUNWportal/bin/psadmin list-portals -u *user-name* -f *admin-password*

1. **Install Weblogic 8.1 Service Pack 5 and create a managed server.**

2. **Start the administrator server and the managed server.**

3. **Run the installer. Select Access Manager SDK and install it in the Configure Later mode.**

4. **Edit the values in the `amsamplesilent` file.**

   For Solaris, the `amsamplesilent` file is present in the */AccessManager_base*`/SUNWam/bin` directory. For Linux, it is in the */AccessManager_base*`/sun/identity` directory.

5. **Change the following values in the `amsamplesilent` file.**

   - `DEPLOY_LEVEL=4`
   - `SERVER_NAME=`*AccessManager_hostname without FQDN*
   - `SERVER_HOST=`*$SERVER_NAME.domain-name*
   - `SERVER_PORT=`*AccessManager_server_port*
   - `ADMIN_PORT=`*Admin port for the web container on which Access Manager resides*
   - `DS_HOST=`*DirectoryServer_hostname with FQDN*
   - `DS_DIRMGRPASSWD=`*Directory Manager Password*
   - `ROOT_SUFFIX=`*root suffix of Access Manager*
   - `ADMINPASSWD=`*AccessManager_password*
   - `AMLDAPUSERPASSWD=`*LDAP_password*
   - `COOKIE_DOMAIN=`*.domain-name*
   - `AM_ENC_PWD=`*any string*
   - `NEW_OWNER=`root
   - `NEW_GROUP=`other

     This value is `root` for Solaris 10 and Linux, and `other` for Solaris 9.
   - `PAM_SERVICE_NAME=`other
   - `WEB_CONTAINER=`WL8
   - `BASEDIR=`*Directory where Access Manager SDK is installed.*
   - `CONSOLE_HOST=`*FQDN of host where Portal needs to be installed*
   - `CONSOLE_PORT=`*Port where second Portal needs to be installed, which is the port of the managed server*
   - `CONSOLE_PROTOCOL=`$SERVER_PROTOCOL
   - `AM_REALM=`disabled
   - `WL8_HOME=`/usr/local/bea
   - `WL8_PROJECT_DIR=`user_projects

- `WL8_DOMAIN=`mydomain
- `WL8_CONFIG_LOCATION=`$WL8_HOME/$WL8_PROJECT_DIR/domains
- `WL8_SERVER=myserver`*name of the managed server on which second Portal needs to be installed*
- `WL8_INSTANCE=`$WL8_HOME/weblogic81
- `WL8_PROTOCOL=`$SERVER_PROTOCOL
- `WL8_HOST=`*FQDN of the node on which second Portal needs to be installed*
- `WL8_PORT=`*Port where the second Portal needs to be installed, which is the port of the managed server*
- `WL8_SSLPORT=`*Weblogic ADMIN_PORT*
- `WL8_ADMIN=`"weblogic"
- `WL8_PASSWORD=`*weblogic admin password*
- `WL8_JDK_HOME=`$WL8_HOME/jdk142_08

6 Run the following command:

AccessManager_base`/SUNWam/bin/amconfig -s`
AccessManager_base`/SUNWam/bin/amsamplesilent`

For Linux, the `amsamplesilent` utility is available in the `/`*AccessManager_base*`/sun/identity` directory.

7 Run the installer and install portal in the Configure Later mode.

8 Configure common agent container and Java DB.

PortalServer_base`/bin/psconfig --config` *example2.xml*

9 Verify that common agent container is functioning properly.

PortalServer_base`/SUNWportal/bin/psadmin list-portals -u` *amadmin* `-f` *ps_password*

10 Edit the following properties in the `secondportal.properties` file.

- `Host=hostname.domain`
- `Port=`*port on which second Portal needs to be installed*
- `Scheme=`http
- `WebContainerType=`BEAWL8
- `WebContainerInstallDir=`/usr/local/bea/weblogic81
- `WebContainerInstanceName=`*name of the managed server on which second Portal needs to be installed*
- `WebContainerInstanceDir=`/usr/local/bea/user_projects/domains/newdomain

- `WebContainerDocRoot=`*Leave Blank*
- `WebContainerAdminHost=`*hostname.domain*
- `WebContainerAdminPort=`*port of admin server*
- `WebContainerAdminScheme=http`
- `WebContainerAdminUid=`*admin userid*
- `WebContainerAdminPassword=`*admin password*
- `WebContainerJDKDir=`/usr/local/bea/jdk142_08
- `WebContainerManagedServer=true`

  `false` if new portal is installed on administrator server itself.

11 Create the new portal.

PortalServer_base`/SUNWportal/bin/psadmin create-portal -u amadmin -f` *ps_password* `-p` *secondportal* `--uri /portal -w` *secondportal.properties*

12 Restart the web container.

13 Verify that the new portal is created.

PortalServer_base`/SUNWportal/bin/psadmin list-portals -u` *amadmin* `-f` *ps_password*

▼ To a Create a New Portal on WebSphere 5.1.1.6 in the Configure Now Mode

Before You Begin Ensure the following:

- Portal Server, Access Manager, and Common Agent Container are up and running on the first node. Execute the following command on Node 1:
  `PortalServer-base/SUNWportal/bin/psadmin list-portals -u` *user-name* `-f` *admin-password*

1 Install WebSphere.

2 Start WebSphere.

3 Start the Java ES installer and select Access Manager SDK and install it in the Configure Later mode.

4 Edit the values in the `amsamplesilent` file

For Solaris, the `amsamplesilent` file is present in the */AccessManager_base*`/SUNWam/bin` directory. For Linux, it is in the */AccessManager_base*`/sun/identity` directory.

5 Change the following values in the `amsamplesilent` file.

- DEPLOY_LEVEL=4
- SERVER_NAME=*AccessManager_hostname without FQDN*
- SERVER_HOST=$SERVER_NAME.domain-name
- SERVER_PORT=*AccessManager_server_port*
- ADMIN_PORT=*Admin port of the web container on which Access Manager resides*
- DS_HOST=*DirectoryServer with FQDN*
- DS_DIRMGRPASSWD=*Directory Manager Password*
- ROOT_SUFFIX=*root suffix of Access Manager*
- ADMINPASSWD=*AccessManager Password*
- AMLDAPUSERPASSWD=*LDAP_Password*
- COOKIE_DOMAIN=.domain-name
- AM_ENC_PWD=any string
- NEW_OWNER=root
- NEW_GROUP=other

  (This value is root for Solaris 10 and Linux, and other for Solaris 9.
- PAM_SERVICE_NAME=other
- WEB_CONTAINER=WAS5
- BASEDIR=*Directory where Access Manager SDK is installed.*
- CONSOLE_HOST=*FQDN of host where Portal needs to be installed*
- CONSOLE_PORT=*Port where second Portal needs to be installed, which is the port of the managed server*
- CONSOLE_PROTOCOL=$SERVER_PROTOCOL
- AM_REALM=disabled
- WAS51_HOME=/*Websphere_base*/WebSphere/AppServer
- WAS51_JDK_HOME=/*Websphere_base*/WebSphere/AppServer/java
- WAS51_CELL=*Usually hostname without FQDN. Please check it in your install.*
- WAS51_NODE=*Usually hostname without FQDN. Please check it in your install.*
- WAS51_INSTANCE=*server1*
- WAS51_PROTOCOL=*$SERVER_PROTOCOL*
- WAS51_HOST=*$SERVER_NAME*
- WAS51_PORT=*$SERVER_PORT*
- WAS51_SSLPORT=9081
- WAS51_ADMIN=*admin*
- WAS51_ADMINPORT=*ADMIN_PORT*

6 **Run the following command:**

AccessManager_base/SUNWam/bin/amconfig -s
AccessManager_base/SUNWam/bin/amsamplesilent

For Linux, the amsamplesilent utility is available in the /*AccessManager_base*/sun/identity directory.

7 **Start the Java ES installer again and install portal on the Configure Now mode.**

8 **Change the name of the portal.**

For example, if the first portal is portal1, then change the name of the new portal to portal2.

▼ To Create a New Portal on WebSphere 5.1.1.6 in the Configure Later Mode

Before You Begin Ensure the following:

- Portal Server, Access Manager, and Common Agent Container are up and running on the first node. Execute the following command on Node 1:
  PortalServer-base/SUNWportal/bin/psadmin list-portals -u *user-name* -f *admin-password*

1 **Install Websphere.**

2 **Start the Websphere.**

3 **Run the installer and select Access Manager SDK, and install in the Configure Later mode.**

4 **Edit the values in the** amsamplesilent **file.**

For Solaris, the amsamplesilent file is present in the /*AccessManager_base*/SUNWam/bin directory. For Linux, it is in the /*AccessManager_base*/sun/identity directory.

5 **Change the following values in the** amsamplesilent **file.**

- DEPLOY_LEVEL=4
- SERVER_NAME=*AccessManager host name without FQDN*
- SERVER_HOST=*$SERVER_NAME.domain-name*
- SERVER_PORT=*AccessManager server port*
- ADMIN_PORT=*Admin port for the web container on which Access Manager resides*
- DS_HOST=*DirectoryServer with FQDN*
- DS_DIRMGRPASSWD=*DirectoryManager Password*
- ROOT_SUFFIX=*root suffix of AccessManager*

- ADMINPASSWD=*AccessManager_password*
- AMLDAPUSERPASSWD=*LDAP_password*
- COOKIE_DOMAIN=.domain-name
- AM_ENC_PWD=*any string*
- NEW_OWNER=root
- NEW_GROUP=other

  This value is root for the Solaris 10 release and Linux, and other for the Solaris 9 release.
- PAM_SERVICE_NAME=other
- WEB_CONTAINER=WAS5
- BASEDIR=*Directory where Access Manager SDK is installed.*
- CONSOLE_HOST=*FQDN of host where Portal needs to be installed*
- CONSOLE_PORT=*Port where second Portal needs to be installed, which is the port of the managed server*
- CONSOLE_PROTOCOL=*$SERVER_PROTOCOL*
- AM_REALM=disabled
- WAS51_HOME=/*Websphere_base*/WebSphere/AppServer
- WAS51_JDK_HOME=/*Websphere_base*/WebSphere/AppServer/java
- WAS51_CELL=*Usually hostname without FQDN. Please check it in your install.*
- WAS51_NODE=*Usually hostname without FQDN. Please check it in your install.*
- WAS51_INSTANCE=*server1*
- WAS51_PROTOCOL=*$SERVER_PROTOCOL*
- WAS51_HOST=*$SERVER_NAME*
- WAS51_PORT=*$SERVER_PORT*
- WAS51_SSLPORT=*9081*
- WAS51_ADMIN=*"admin"*
- WAS51_ADMINPORT=*$ADMIN_PORT*

6 Run the following command:

AccessManager_base/SUNWam/bin/amconfig -s
AccessManager_base/SUNWam/bin/amsamplesilent

For Linux, the amsamplesilent utility is available in the /*AccessManager_base*/sun/identity directory.

7 Start the installer again and install portal on the Configure Later mode.

8 **Complete the Portal Server installation.**

PortalServer_base`/bin/psconfig --config` *example16.xml*

▼ To Create a New Portal Using the `psadmin` Command

Before You Begin Ensure the following:

- Portal Server, Access Manager, and Common Agent Container are up and running on the first node. Execute the following command on Node 1:
  `PortalServer-base/SUNWportal/bin/psadmin list-portals -u` *user-name* `-f` *admin-password*

1 **Install WebSphere.**

2 **Start the WebSphere.**

3 **Start the installer. Select Access Manager SDK and install in the Configure Later mode.**

4 **Edit the values in the `amsamplesilent` file.**

For Solaris, the `amsamplesilent` file is present in the `/`*AccessManager_base*`/SUNWam/bin` directory. For Linux, it is in the `/`*AccessManager_base*`/sun/identity` directory.

5 **Change the following values in the `amsamplesilent` file.**

- `DEPLOY_LEVEL=4`
- `SERVER_NAME=`*AccessManager without FQDN*
- `SERVER_HOST=`*$SERVER_NAME.domain-name*
- `SERVER_PORT=`*AccessManager admin password*
- `ADMIN_PORT=`*Admin port for the web container on which Access Manager resides*
- `DS_HOST=`*DirectoryServer hostname with FQDN*
- `DS_DIRMGRPASSWD=`*Directory Manager Password*
- `ROOT_SUFFIX=`*root suffix of Access Manager*
- `ADMINPASSWD=`*AccessManager Password*
- `AMLDAPUSERPASSWD=`*LDAP_password*
- `COOKIE_DOMAIN=`.domain-name
- `AM_ENC_PWD=`any string
- `NEW_OWNER=`root
- `NEW_GROUP=other`

  This value is `root` for Solaris 10 and Linux, and `other` for Solaris 9.
- `PAM_SERVICE_NAME=`other

- `WEB_CONTAINER=`WAS5
- `BASEDIR=`*Directory where Access Manager SDK is installed.*
- `CONSOLE_HOST=`*FQDN of host where Portal needs to be installed*
- `CONSOLE_PORT=`*Port where second Portal needs to be installed, which is the port of the managed server*
- `CONSOLE_PROTOCOL=`*$SERVER_PROTOCOL*
- `AM_REALM=`disabled
- `WAS51_HOME=`/*Websphere_base*/WebSphere/AppServer
- `WAS51_JDK_HOME=`/*Websphere_base*/WebSphere/AppServer/java
- `WAS51_CELL=`*Usually hostname without FQDN. Please check it in your install.*
- `WAS51_NODE=`Usually hostname without FQDN. Please check it in your install.
- `WAS51_INSTANCE=server1`
- `WAS51_PROTOCOL=`*$SERVER_PROTOCOL*
- `WAS51_HOST=`*$SERVER_NAME*
- `WAS51_PORT=`*$SERVER_PORT*
- `WAS51_SSLPORT=`9081
- `WAS51_ADMIN=`*"admin"*
- `WAS51_ADMINPORT=`*$ADMIN_PORT*

6 **Run the following command:**

AccessManager_base`/SUNWam/bin/amconfig -s`
AccessManager_base`/SUNWam/bin/amsamplesilent`

For Linux, the `amsamplesilent` utility is available in the `/`*AccessManager_base*`/sun/identity` directory.

7 **Start the installer again and install Portal Server in the Configure Later mode.**

8 **Configure Common Agent Container and Java DB.**

PortalServer_base`/bin/psconfig --config` *example2.xml*

9 **Verify that common agent container is functioning properly.**

PortalServer_base`/SUNWportal/bin/psadmin list-portals -u` *amadmin* `-f` *ps_password*

10 **Copy the** *PortalServer_base*`/SUNWportal/template/Webcontainer.properties.IBMWAS5` **to** *PortalServer_base*`/SUNWportal/bin/secondportal.properties` **file.**

11 **Edit the following properties in the** `secondportal.properties` **file.**

- `Host=`*hostname.domain*
- `Port=`*9080*
- `Scheme=`http
- `WebContainerType=`IBMWAS5
- `WebContainerInstallDir=`*/Websphere_base*/IBM/WebSphere/Express51/AppServer
- `WebContainerInstanceName=`*server1*
- `WebContainerDomainName=`Leave Blank
- `WebContainerInstanceDir=`*Leave Blank*
- `WebContainerDocRoot=`*Leave Blank*
- `WebContainerAdminHost=`*hostname.domain*
- `WebContainerAdminPort=`9090
- `WebContainerAdminScheme=http`
- `WebContainerAdminUid=`*admin userid*
- `WebContainerAdminPassword=`*admin password*
- `WebContainerJDKDir=`*/Websphere_base*/IBM/WebSphere/Express51/AppServer/java
- `WebContainerDeployCell=`*Usually hostname without FQDN. Please check it in your install.*
- `WebContainerDeployNode=`*Usually hostname without FQDN. Please check it in your install.*

12 Create the new portal.

PortalServer_base`/SUNWportal/bin/psadmin create-portal -u` *amadmin* `-f` *ps_password* `-p` *secondportal* `--uri` */portal* `-w` *secondportal.properties*

13 Restart the web container.

14 Verify that the new portal is created.

PortalServer_base`/SUNWportal/bin/psadmin list-portals -u` *amadmin* `-f` *ps_password*

Deploying Sample Content to a New Portal

When you create a new portal, it does not have any sample portal deployed in it. However, you can deploy sample portals such as community sample, enterprise sample, and developer sample to the new portal.

▼ To Deploy a Sample Content to a New Portal

1. **Copy the** */PortalServer-base*`/SUNWportal/samples/portals/shared/input.properties.template` **file to the** `/var/opt/SUNWportal/tmp/input.properties` **file.**

   In the Linux platform, copy to the `/var/opt/sun/portal/tmp/input.properties` file.

2. **Edit the** `input.properties` **file that you created in the** `/var/opt/SUNWportal/tmp` **directory with the following values.**

   - ps.config.location=/etc/opt/SUNWportal
   - ps.portal.id=*new portal id*
   - ps.access.url=*access url of the new portal.*
   - ps.webapp.uri=*access uri of the new portal.*
   - ps.profiler.email=admin@domain.com

     Optional. You can leave this value empty.
   - ps.profiler.smtp.host=host.domain

     Optional. You can leave this value empty.
   - search.access.url=http://host.domain:port/search1/search
   - search.id=search1
   - am.admin.dn=uid=amAdmin,ou=People,dc=domain,dc=com
   - default.org.dn=dc=domain,dc=com

3. **Copy the** */PortalServer-base*`/SUNWportal/samples/portals/shared/password.properties.template` **file to the** `/var/opt/SUNWportal/tmp/password.properties` **file.**

   In the Linux platform copy the file to the `/var/opt/sun/portal/tmp/password.properties` directory.

4. **Edit the** `/var/opt/SUNWportal/tmp/password.properties` **file and set proper passwords.**

   - amadminPassword=*%AMADMIN_PASSWORD%*
   - amldapuserPassword=*%AMLDAPUSER_PASSWORD%*
   - userManagementPassword=*%USER_MANAGEMENT_PASSWORD%*

     You can ignore this value if you are not setting up Communication channels.

5. **Run the following command.**

   ```
   export JAVA_HOME=/usr/jdk/entsys-j2se
   ```

6. **Run the following command to deploy all the portals.**

   ```
   /usr/sfw/bin/ant -buildfile
   /PortalServer-base/SUNWportal/samples/portals/build.xml -Dconfig.location
   /var/opt/SUNWportal/tmp/ -logfile /var/opt/SUNWportal/tmp/log-file.txt
   ```

7. **(Optional) Run the following command if you wish to deploy only the developer portal.**

   ```
   /usr/sfw/bin/ant -buildfile
   /PortalServer-base/SUNWportal/samples/portals/developer/build.xml
   -Dconfig.location /var/opt/SUNWportal/tmp/ -logfile
   /var/opt/SUNWportal/tmp/log-file.txt
   ```

8. **(Optional) Run the following command if you wish to deploy only the enterprise portal.**

   ```
   /usr/sfw/bin/ant -buildfile
   /PortalServer-base/SUNWportal/samples/portals/enterprise/build.xml
   -Dconfig.location /var/opt/SUNWportal/tmp/ -logfile
   /var/opt/SUNWportal/tmp/log-file.txt
   ```

9. **(Optional) Run the following command if you wish to deploy only the community portal.**

   ```
   /usr/sfw/bin/ant -buildfile
   /PortalServer-base/SUNWportal/samples/portals/community/build.xml
   -Dconfig.location /var/opt/SUNWportal/tmp/ -logfile
   /var/opt/SUNWportal/tmp/log-file.txt
   ```

10. **(Optional) Run the following command if you wish to deploy only the welcome portal.**

    ```
    /usr/sfw/bin/ant -buildfile
    /PortalServer-base/SUNWportal/samples/portals/welcome/build.xml -Dconfig.location
    /var/opt/SUNWportal/tmp/ -logfile /var/opt/SUNWportal/tmp/log-file.txt
    ```

11. **Restart the web container.**

Creating a Portal Server Instance

This section explains how to create a new instance of Portal Server. When you install Portal Server, it creates an instance of Portal Server on the default instance of the web container. For example, if you install Portal Server on Sun Java System Web Server, a Portal Server instance is created on the default instance of Web Server that listens to the port `80`. You can also create several instances of the web container and create instances of the Portal Server that are already installed. A new instance of Portal Server that you create will have all the portals that are deployed on your first Portal Server.

After creating instances of Portal Server, you can use clustering or load balancing to serve the users effectively. Portal Server instances can be created on a node where you installed Portal Server or on a remote node where you installed a web container, AMSDK, and Portal Server packages.

Creating a Portal on the Same Node

This section explains how to create a Portal Server instance on different web containers on the same node where you installed Portal Server. When you create a Portal Server instance, you can create the instance on a new configuration or a new domain of the web container. You can also create a Portal Server instance on the existing configuration or domain of the web container where you have installed Portal Server.

This section explains the following:

- Creating a Portal Instance on a New Configuration of Web Server 7.0
- Creating a Portal Instance on a New Domain of Application Server 8.2
- Creating a Portal Instance on a New Instance of Application Server 8.2
- Creating a Portal Instance on a Managed Server of WebLogic 8.1 Service Pack 5
- Creating a Portal Instance on a Managed Server of WebLogic 8.1 Service Pack 5 on which Portal Instance Exists

▼ To Create a New Portal Instance on a New Configuration of Web Server 7.0

Before You Begin Ensure the following:

- Portal Server is installed. Name of the first portal is `portal1`.
- Access Manager administrator console is running.
- Web containers are installed under the default directories.

1. **Create a new configuration of Web Server 7.0 on the same node where Portal Server is installed. Specify the name of the configuration as `secondinstance` and the port as `8100`.**

2. **Start the new configuration. Ensure that the Web Server administrator console is running.**

3. **Copy the *PortalServer_base*`/SUNWportal/template/Webcontainer.properties.SJSWS7` to a *PortalServer_base*`/SUNWportal/bin/secondportal.properties` file.**

4. **Edit the following properties in the `secondportal.properties` file.**
   - `Host=`*hostname.domain*
   - `Port=`*8100*
   - `Scheme=http`

- `WebContainerType=SJSWS7`
- `WebContainerInstallDir=/WebServer_base/SUNWwbsvr7`
- `WebContainerInstanceName=`*`secondinstance`*
- `WebContainerDomainName=`*`secondinstance`*
- `WebContainerDocRoot=`*`/var/SUNWwbsvr7/docs`*
- `WebContainerAdminHost=`*`hostname.domain`*
- `WebContainerAdminPort=`*`8989`*
- `WebContainerAdminScheme=`*`https`*
- `WebContainerAdminUid=`*`admin`*
- `WebContainerAdminPassword=`*`Webserver_admin_password`*

5 **Create the new portal instance.**

PortalServer_base`/SUNWportal/bin/psadmin create-instance -u` *amadmin* `-f` *ps_password* `-p` *portal1* `-w` *secondportal.properties*

The `ps_password` file contains the Access Manager password

6 **Restart the web container.**

7 **Verify that the new portal instance has been created.**

PortalServer_base`/SUNWportal/bin/psadmin list-portals -u` *amadmin* `-f` *ps_password*

8 **Access the new Portal Server instance.**

`http://`*`hostname.domain-name`***`:8100/`***`portal1`*

▼ To Create a Portal Instance on a New Domain of Application Server 8.2

Before You Begin Ensure the following:

- Portal Server is installed on Application Server. Name of the first portal is `portal1`.
- Access Manager is installed on Application Server.
- Application Server is installed in the default directory.

1 **Create a domain,** `seconddomain`**, and a server instance on the port** `8100`**.**

/ApplicationServer_base`/appserver/bin/asadmin create-domain --adminport` *4850* `--adminuser admin --instance-port` *8100 seconddomain*

2 **Start the new domain,** *seconddomain***.**

3 **Copy the** *PortalServer_base*`/SUNWportal/template/Webcontainer.properties.SJSAS81` **file to a** *PortalServer_base*`/SUNWportal/bin/secondinstance.properties` **file.**

4 **Edit the following properties in the** `secondinstance.properties` **file.**

- `Host=`*hostname.domain*
- `Port=`*8100*
- `Scheme=http`
- `WebContainerType=SJSAS81`
- `WebContainerInstallDir=`*/ApplicationServer_base*/SUNWappserver/appserver
- `WebContainerInstanceName=server`
- `WebContainerDomainName=`*seconddomain*
- `WebContainerInstanceDir=/var/SUNWappserver/domains/seconddomain`
- `WebContainerDocRoot=/var/SUNWappserver/domains/seconddomain/docroot`
- `WebContainerAdminHost=`*hostname.domain*
- `WebContainerAdminPort=4850`
- `WebContainerAdminScheme=https`
- `WebContainerAdminUid=`*admin*
- `WebContainerAdminPassword=`*Application Server administrator password*
- `WebContainerMasterPassword=`*Application Server master password*

5 Create the new Portal Server instance.

PortalServer_base`/SUNWportal/bin/psadmin create-instance -u` *amadmin* `-f` *ps_password* `-p` *portal1* `-w` *secondinstance.properties*

6 Restart the web container.

7 Verify that the new portal has been created.

PortalServer_base`/SUNWportal/bin/psadmin list-portals -u` *amadmin* `-f` *ps_password*

8 Access the new portal instance.

`http://`*hostname.domain.com***`:8100/`***portal*

9 Restart the common agent container.

On the Solaris platform:

```
/usr/share/bin/cacaoadm stop
/usr/share/bin/cacaoadm start
```

On the Linux platform:

```
/opt/sun/cacao/bin/cacaoadm stop
/opt/sun/cacao/bin/cacaoadm start
```

▼ To Create a Portal Instance on a New Instance of Application Server on Which a Portal Instance Exists

Before You Begin Ensure the following:

- Portal Server is installed on Application Server. Name of the first portal is `portal1`.

- Access Manager is installed on Application Server.
- Application Server is installed in the default directory.

1 Create a node agent, `nodeagent1`, in the same domain in which the first Portal Server instance exists.

ApplicationServer_base`/appserver/bin/asadmin`
`create-node-agent --host` *hostname.domain*
`--port` *4849* `--user` *ApplicationServer_admin_user*
`--password` *ApplicationServer_admin_password* *nodeagent1*

2 Create an instance in the node agent.

ApplicationServer_base`/appserver/bin/asadmin`
`create-instance --host` *hostname.domain*
`--port 4849 --user` *ApplicationServer_admin_user*
`--password` *ApplicationServer_admin_password*
`--nodeagent` *nodeagent1* `--systemproperties HTTP_LISTNER_PORT=`*3870* *server2*

3 Start the node agent and the instance.

ApplicationServer_base`/appserver/bin/asadmin`
`start-node-agent --user` *admin* `--password` *password* *nodeagent1*

ApplicationServer_base`/appserver/bin/asadmin`
`start-instance --port` *4849* `--user` *admin* `--password` *password* *server2*

Note – When you start the instance after starting the node agent, the start-instance CLI may fail stating that the server instance is already started. In this case, ignore the message. This is due to the server instance being started while starting the node agent. This behavior is controlled by the `start-servers-in-startup` attribute, located in the `domain.xml` and if it is set to true, all the server instances which are not running are started during node-agent startup.

---

4 Copy the *PortalServer_base*`/SUNWportal/template/Webcontainer.properties.SJSAS81` to a *PortalServer_base*`/SUNWportal/bin/secondinstance.properties` file.

5 Edit the following properties in the `secondinstance.properties` file.

- `Host=`*hostname.domain*
- `Port=`*3870*
- `Scheme=http`
- `WebContainerType=SJSAS81`
- `WebContainerInstallDir=/`*ApplicationServer_base*/SUNWappserver/appserver
- `WebContainerInstanceName=`*server2*
- `WebContainerDomainName=`*domain1*
- `WebContainerInstanceDir=`*ApplicationServer_base*/nodeagents/node1/server2
- `WebContainerDocRoot=`*ApplicationServer_base*/nodeagents/node1/server2/docroot

- `WebContainerAdminHost=`*hostname.domain*
- `WebContainerAdminPort=`*admin port of domain1*
- `WebContainerAdminScheme=https`
- `WebContainerAdminUid=`*admin id*
- `WebContainerAdminPassword=`*ApplicationServer admin password*
- `WebContainerMasterPassword=`*ApplicationServer master password*

6. **Create the new Portal Server instance.**

   PortalServer_base`/SUNWportal/bin/psadmin create-instance -u` *amadmin* `-f` *ps_password* `-p portal1 -w` *secondinstance.properties*

7. **Restart the web container.**

8. **Verify that the new portal instance has been created.**

   PortalServer_base`/SUNWportal/bin/psadmin list-portals -u` *amadmin* `-f` *ps_password.*

9. **Access the new Portal Server instance.**

   `http://`*hostname.domain.com***`:`***3870/portal*

To Create a Portal Instance on a Managed Server in a New Domain of WebLogic 8.1 Service Pack 5

Before You Begin Ensure the following:

- Portal Server is installed on WebLogic. Name of the first portal is `portal1`.
- Access Manager is installed on WebLogic.
- WebLogic is installed in the default directory.

1. **Create a WebLogic domain,** `seconddomain` **on the port** `7002`**.**

2. **Create a managed server,** `7022server`**, on the port** `7022`**.**

3. **Go to the** *WebLogic_base*`/user_projects/domains/seconddomain` **directory and run the following scripts.**

   ```
   ./startWeblogic.sh
   ```

   ```
   ./startManagedWeblogic.sh 7022server
   ```

4. **Copy the** *PortalServer_base*`/SUNWportal/template/Webcontainer.properties.BEAWL8` **file to a** *PortalServer_base*`/SUNWportal/bin/secondinstance.properties` **file.**

5. **Edit the following properties in the** `secondportal.properties` **file.**

   - `Host=`*hostname.domain*

- `Port=`*7022*
- `Scheme=`*http*
- `WebContainerType=BEAWL8`
- `WebContainerInstallDir=/usr/local/bea/weblogic81`
- `WebContainerInstanceName=`*7022server*
- `WebContainerInstanceDir=`/usr/local/bea/user_projects/domains/*seconddomain*
- `WebContainerDocRoot=`LEAVE BLANK
- `WebContainerAdminHost=`*hostname.domain*
- `WebContainerAdminPort=`7002
- `WebContainerAdminScheme=`http
- `WebContainerAdminUid=`*admin userid*
- `WebContainerAdminPassword=`*admin passwd*
- `WebContainerJDKDir=`/usr/local/bea/jdk142_08
- `WebContainerManagedServer=`true

  The value is `false` if new Portal Server is installed on administrator server itself.

6 Create the new portal instance.

PortalServer_base`/SUNWportal/bin/psadmin create-instance -u` *amadmin* `-f` *ps_password* `-p` *portal1* `-w` *secondinstance.properties*

7 Restart the web container.

8 Verify that the new portal instance has been created.

PortalServer_base`/SUNWportal/bin/psadmin list-portals -u` *amadmin* `-f` *ps_password*.

9 Access the new Portal Server instance.

`http://`*hostname.domain.com*`:`***instance-port*`/`***portal*

▼ To Create a Portal Instance on a Managed Server Instance of WebLogic 8.1 Service Pack 5 on Which Portal Instance Exists

Before You Begin Ensure the following:

- Portal Server is installed on WebLogic. Name of the first Portal is `portal1`.
- Access Manager is installed on WebLogic.
- WebLogic is installed in the default directory.

1 Create a new WebLogic Server instance, `7022server`, on the port `7022`.

2 **Go to the** *WebLogic_base*`/user_projects/domains/seconddomain` **directory and run the following scripts:**

```
./startWeblogic.sh
```

```
./startManagedWeblogic.sh 7022server
```

3 **(Optional) You can also follow these steps to create a new portal instance on WebLogic 8.1 Service Pack 5:**

a. **Start the WebLogic Administrator Server.**

b. **Start the WebLogic node manager with the IP address of the host as the first argument and the port number on which you want the node manager to run as the second argument.**

c. **Add the IP address of the node in the** */bea_install*`/weblogic81/common/nodemanager/nodemanager.hosts` **file.**

d. **Log in to the WebLogic administrator console.**

e. **Click Machines.**

f. **Click Configure a New Machine.**

g. **Specify a machine name and click Create.**

h. **Click the Node Manager tab.**

i. **Specify the IP Address of the host in the listen address and specify the port on which the Node Manager is running.**

j. **Click on Servers in the left pane to create a new managed server.**

k. **Click on configure a new server.**

l. **Specify the server name and Listen Port of the managed server.**

m. **Start the managed server from the console.**

4 **Copy the** *PortalServer_base*`/SUNWportal/template/Webcontainer.properties.BEAWL8` **file to a** *PortalServer-base*`/SUNWportal/bin/secondinstance.properties` **file.**

5 **Edit the following properties in the** `secondinstance.properties` **file.**

- `Host=`*hostname.domain*
- `Port=`*7022*

- `Scheme=`http
- `WebContainerType=`BEAWL8
- `WebContainerInstallDir=`/usr/local/bea/weblogic81
- `WebContainerInstanceName=`*7022server*
- `WebContainerInstanceDir=`/usr/local/bea/user_projects/domains/*seconddomain*
- `WebContainerDocRoot=`LEAVE BLANK
- `WebContainerAdminHost=`*hostname.domain*
- `WebContainerAdminPort=`7002
- `WebContainerAdminScheme=`http
- `WebContainerAdminUid=`*admin userid*
- `WebContainerAdminPassword=`*admin passwd*
- `WebContainerJDKDir=`/usr/local/bea/jdk142_08
- `WebContainerManagedServer=`true

  The value is `false` if new Portal is installed on administrator server itself.

6 Create the new Portal instance.

PortalServer_base`/SUNWportal/bin/psadmin create-instance -u` *amadmin* `-f` *ps_password* `-p portal1 -w` *secondinstance.properties*

Note – If Portal Server is on the same port as Access Manager, then the `Dcom.iplanet.am.serverMode` in `startWeblogic.sh` or `startManagedWeblogic.sh` should be `true`, else it should be `false`. Before restarting the web container, edit the `startWeblogic.sh` or `startManagedWeblogic.sh` appropriately.

---

7 Restart the web container.

8 Verify that the new portal instance.

PortalServer_base`/SUNWportal/bin/psadmin list-portals -u` *amadmin* `-f` *ps_password*.

9 Access the new Portal Server instance.

`http://`*hostname.domain.com*`:`*instance-port*`/portal`

Creating a Portal Server Instance a Remote Node

This section explains how to create a Portal Server instance on a remote node. In this scenario, you have Portal Server installed on a node. You are creating an instance of Portal Server on another node. You need to install AMSDK, web container, and Portal Server packages on the

node where you wish to install Portal Server instance. Then, you need to run the `psadmin create-instance` command to create a new Portal Server instance.

Note – When you install AMSDK, provide the same encryption key, am password, and LDAP password that are used for Access Manager on Node 1.

This section explains the following:

- Creating a portal instance on Web Server 7.0 on a Remote Node
- Creating a portal instance on WebLogic 8.1 Service Pack 5 on a Remote Node
- Creating a portal instance on WebSphere 5.1.1.6 on a Remote Node

▼ To Create a New Portal Instance on Web Server 7.0 on a Remote Node

Before You Begin Ensure the following:

- Portal Server, Access Manager, and Common Agent Container are up and running on the first node. Execute the following command on Node 1: `PortalServer-base/SUNWportal/bin/psadmin list-portals -u` *user-name* `-f` *admin-password*
- Ensure that the Access Manager is accessible.
- Web Server 7.0 is installed in the default directory.
- The system date on the second instance node should be same as the system date on the first instance node. System dates should be in sync. To achieve this, run the `rdate` *first_instance_node_fqdn* command on the second instance node.

1 Start the installer and install Access Manager SDK and Web Server 7.0 in the Configure Now mode.

In the installer panel, provide the details of the Identity Server and Access Manager that you installed in the first node.

2 Start the Web Server 7.0 administrator server.

WebServer_base`/admin-server/bin/startserv`

3 Start the Web Server 7.0 instance.

WebServer_base`/https-`*hostname.domain*`/bin/startserv`

4 Stat the installer and install Portal Server in the Configure Later mode.

5 Configure the common agent container and Java DB.

PortalServer_base`/bin/psconfig --config` *example2.xml*

6. **Verify that the common agent container is functioning properly.**

   PortalServer_base`/SUNWportal/bin/psadmin list-portals -u` *amadmin* `-f` *ps_password*

7. **Copy the** *PortalServer_base*`/SUNWportal/template/Webcontainer.properties.SJSAS81` **file to a** *PortalServer_base*`/SUNWportal/bin/secondinstance.properties` **file.**

8. **Edit the following properties in** `secondinstance.properties` **file.**

   - `Host=`*hostname.domain*
   - `Port=`*80*
   - `Scheme=`http
   - `WebContainerType=`SJSWS7
   - `WebContainerInstallDir=`*/WebServer_base*/SUNWwbsvr7
   - `WebContainerInstanceName=`*hostname.domain*
   - `WebContainerDomainName=`*hostname.domain*
   - `WebContainerDocRoot=`/var/SUNWwbsvr/docs
   - `WebContainerAdminHost=`*hostname.domain*
   - `WebContainerAdminPort=`8989
   - `WebContainerAdminScheme=`https
   - `WebContainerAdminUid=`*administrator id*
   - `WebContainerAdminPassword=`*WebServer administrator password*

9. **Create the new portal instance.**

   PortalServer_base`/SUNWportal/bin/psadmin create-portal -u` *amadmin* `-f` *ps_password* `-p` *secondportal* `-w` *secondinstance.properties*

10. **Restart the web container.**

11. **Verify that the new Portal Server instance has been created.**

    PortalServer_base`/SUNWportal/bin/psadmin list-portals -u` *amadmin* `-f` *ps_password*

12. **Access the second Portal Server instance.**

    `http://`*hostname.domain***`.com:`***instance-port/portal*

▼ To Create a Portal Instance on WebLogic 8.1 Service Pack 5 on a Remote Node

Before You Begin Ensure the following:

- Portal Server, Access Manager, and Common Agent Container are up and running on the first node. Execute the following command on Node 1:
  `PortalServer-base/SUNWportal/bin/psadmin list-portals -u` *user-name* `-f` *admin-password*

1. **Install WebLogic 8.1 Service Pack 5 and create a managed server, `7022server` on Port 7022.**

2. **Go to the *WebLogic_base*`/user_projects/domains/mydomain` directory and run the following scripts:**

   ```
   ./startWeblogic.sh
   ```

   ```
   ./startManagedWeblogic.sh 7022server
   ```

3. **Start the installer, select Access Manager SDK and install it in the Configure Later mode.**

4. **Edit the values in the `amsamplesilent` file.**

   For Solaris, the `amsamplesilent` file is present in the */AccessManager_base*`/SUNWam/bin` directory. For Linux, it is in the */AccessManager_base*`/sun/identity` directory.

5. **Change the following values in the `amsamplesilent` file.**

   - `DEPLOY_LEVEL=4`
   - `SERVER_NAME=`*AccessManager host name without FQDN*
   - `SERVER_HOST=$SERVER_NAME.domain.com`
   - `SERVER_PORT=`*AccessManager server port*
   - `ADMIN_PORT=`*Admin port for the web container on which Access Manager resides*
   - `DS_HOST=`*Directory Server HOSTNAME with FQDN*
   - `DS_DIRMGRPASSWD=`*Directory Manager Password*
   - `ROOT_SUFFIX=`*root suffix of Access Manager*
   - `ADMINPASSWD=`*AccessManger Password*
   - `AMLDAPUSERPASSWD=`*LDAP password*
   - `COOKIE_DOMAIN=.domain.com`
   - `AM_ENC_PWD=`*any string*
   - `NEW_OWNER=root`
   - `NEW_GROUP=other`

     This value is `root` for Solaris 10 and Linux, and `other` for Solaris 9
   - `PAM_SERVICE_NAME=other`
   - `WEB_CONTAINER=WL8`
   - `BASEDIR=`*Directory where Access Manager SDK is installed*

     For example, */AccessManager_base*`/SUNWam`
   - `CONSOLE_HOST=`*FQDN of host where Portal needs to be installed*
   - `CONSOLE_PORT=`*Port where new Portal needs to be installed, which is the port of the managed server*

- `CONSOLE_PROTOCOL=$SERVER_PROTOCOL`
- `AM_REALM=disabled`
- `WL8_HOME=/usr/local/bea`
- `WL8_PROJECT_DIR=user_projects`
- `WL8_DOMAIN=mydomain`
- `WL8_CONFIG_LOCATION=$WL8_HOME/$WL8_PROJECT_DIR/domains`
- `WL8_SERVER=myserver`

  Name of the managed server on which second Portal needs to be installed.
- `WL8_INSTANCE=$WL8_HOME/weblogic81`
- `WL8_PROTOCOL=$SERVER_PROTOCOL`
- `WL8_HOST=`*FQDN of the node on which second Portal needs to be installed*
- `WL8_PORT=`*Port where the new Portal needs to be installed, which is the port of the managed server*
- `WL8_SSLPORT=`*Weblogic ADMIN_PORT*
- `WL8_ADMIN=`*weblogic*
- `WL8_PASSWORD=`*weblogic admin password*
- `WL8_JDK_HOME=$WL8_HOME/jdk142_08`

6 Run the following command:

AccessManager_base`/SUNWam/bin/amconfig -s`
AccessManager_base`/SUNWam/bin/amsamplesilent`

For Linux, the `amsamplesilent` utility is available in the `/`*AccessManager_base*`/sun/identity` directory.

7 Run the installer again and install Portal Server in the Configure Later mode.

8 Configure the common agent container and Java DB.

PortalServer_base`/bin/psconfig --config` *example2.xml*

9 Verify that the common agent container is working properly.

PortalServer_base`/SUNWportal/bin/psadmin list-portals -u` *amadmin* `-f` *ps_password*

10 Edit the following properties in the `secondinstance.properties` file.

- `Host=hostname.domain`
- `Port=`*Port on which new Portal needs to be installed*
- `Scheme=http`
- `WebContainerType=BEAWL8`

- `WebContainerInstallDir=/usr/local/bea/weblogic81`
- `WebContainerInstanceName=`*Name of the managed server on which second instance of Portal needs to be installed*
- `WebContainerInstanceDir=/usr/local/bea/user_projects/domains/mydomain`
- `WebContainerDocRoot=`*Leave Blank*
- `WebContainerAdminHost=`*hostname.domain*
- `WebContainerAdminPort=`*Port of admin server*
- `WebContainerAdminScheme=http`
- `WebContainerAdminUid=`*admin id*
- `WebContainerAdminPassword=`*admin password*
- `WebContainerJDKDir=/usr/local/bea/jdk142_08`
- `WebContainerManagedServer=true`

  The value is `false`, if new Portal is installed on administrator server itself.

11 Create the new instance of Portal Server.

PortalServer_base`/SUNWportal/bin/psadmin create-instance -u` *amadmin* `-f` *ps_password* `-p` *portal1* `-w` *secondinstance.properties*

Note – `Dcom.iplanet.am.serverMode` in `startWeblogic.sh` or `startManagedWeblogic.sh` should be set to `false`.

---

12 Restart the web container.

13 Verify that the new portal instance is created.

PortalServer_base`/SUNWportal/bin/psadmin list-portals -u amadmin -f` *ps_password*

14 Access the second portal instance.

`http://`*hostname.domain.com*`:`*instance-port*`/portal`

▼ To Create a Portal Instance on WebSphere 5.1.1.6 on a Remote Node

Before You Begin Ensure the following:

- Portal Server, Access Manager, and Common Agent Container are up and running on the first node. Execute the following command on Node 1:
  `PortalServer-base/SUNWportal/bin/psadmin list-portals -u` *user-name* `-f` *admin-password*

1 Install WebSphere.

2. **Start the WebSphere.**

3. **Run the Java ES installer, select Access Manager SDK and install in the Configure Later mode.**

4. **Edit the values in the `amsamplesilent` file.**

   For Solaris, the `amsamplesilent` file is present in the */AccessManager_base*`/SUNWam/bin` directory. For Linux, it is in the */AccessManager_base*`/sun/identity` directory.

5. **Change the following values in the `amsamplesilent` file:**

   - `DEPLOY_LEVEL=4`
   - `SERVER_NAME=`*AccessManager_hostname without FQDN*
   - `SERVER_HOST=$SERVER_NAME.domain.com`
   - `SERVER_PORT=`*AccessManager_admin_port*
   - `ADMIN_PORT=`*Admin port for the web container on which Access Manager resides*
   - `DS_HOST=`*DirectoryServer_hostname with FQDN*
   - `DS_DIRMGRPASSWD=`*Directory Manager Password*
   - `ROOT_SUFFIX=`*root suffix of AccessManager*
   - `ADMINPASSWD=`*AccessManager_password*
   - `AMLDAPUSERPASSWD=`*LDAP_password*
   - `COOKIE_DOMAIN=.domain.com`
   - `AM_ENC_PWD=`*any string*
   - `NEW_OWNER=root`
   - `NEW_GROUP=other`

     This value is `root` for Solaris 10 and Linux, and `other` for Solaris 9.
   - `PAM_SERVICE_NAME=other`
   - `WEB_CONTAINER=WL8`
   - `BASEDIR=`*Directory where Access Manager SDK is installed.*

     For example, */Access_Manager_base*`/SUNWam`.
   - `CONSOLE_HOST=`*FQDN of host where Portal needs to be installed*
   - `CONSOLE_PORT=`*Port where new Portal needs to be installed, which is the port of the managed server*
   - `CONSOLE_PROTOCOL=$SERVER_PROTOCOL`
   - `AM_REALM=disabled`
   - `WAS51_HOME=/Websphere_base_dir/Websphere/AppServer`
   - `WAS51_JDK_HOME=/Websphere_base_dir/WebSphere/AppServer/java`

- WAS51_CELL=*usually hostname without FQDN. Please check it in your install.*
- WAS51_NODE=*usually hostname without FQDN. Please check it in your install.*
- WAS51_INSTANCE=server1
- WAS51_PROTOCOL=$SERVER_PROTOCOL
- WAS51_HOST=$SERVER_NAME
- WAS51_PORT=$SERVER_PORT
- WAS51_SSLPORT=9081
- WAS51_ADMIN=*admin*
- WAS51_ADMINPORT=$ADMIN_PORT

6 **Run the following command:**

AccessManager_base/SUNWam/bin/amconfig -s
AccessManager_base/SUNWam/bin/amsamplesilent

For Linux, the amsamplesilent utility is available in the /*AccessManager_base*/sun/identity directory.

7 **Run the installer again and install Portal Server in the Configure Later mode.**

8 **Configure the common agent container and Java DB.**

PortalServer_base/bin/psconfig --config *example2.xml*

9 **Verify that common agent container is working properly.**

PortalServer_base/SUNWportal/bin/psadmin list-portals -u *amadmin* -f *ps_password*

10 **Copy the** *PortalServer_base*/SUNWportal/template/Webcontainer.properties.IBMWAS5 **file to a** *PortalServer_base*/SUNWportal/bin/secondinstance.properties **file.**

11 **Edit the following properties in the** secondinstance.properties **file.**

- Host=*hostname.domain*
- Port=9080
- Scheme=http
- WebContainerType=IBMWAS5
- WebContainerInstallDir=/*Websphere_base*/IBM/WebSphere/Express51/AppServer
- WebContainerInstanceName=*server1*
- WebContainerDomainName=*Leave Blank*
- WebContainerInstanceDir=*Leave Blank*
- WebContainerDocRoot=*Leave Blank*

- `WebContainerAdminHost=`*hostname.domain*
- `WebContainerAdminPort=9090`
- `WebContainerAdminScheme=http`
- `WebContainerAdminUid=`*admin userid*
- `WebContainerAdminPassword=`*admin passwd*
- `WebContainerJDKDir=/`*Websphere_base*/IBM/WebSphere/Express51/AppServer/java
- `WebContainerDeployCell=`*usually hostname without FQDN. Please check it in your install.*
- `WebContainerDeployNode=`*usually hostname without FQDN. Please check it in your install.*

12 Create the new instance of Portal Server.

PortalServer_base`/SUNWportal/bin/psadmin create-instance -u` *amadmin* `-f` *ps_password* `-p` *portal1* `-w` *secondinstance.properties*

13 Restart the web container.

14 Verify that the new Portal Server instance is created.

PortalServer_base`/SUNWportal/bin/psadmin list-portals -u` *amadmin* `-f` *ps_password*

15 Access the second Portal Server instance.

`http://`*hostname.domain*`:`*instance-port*`/`*portal URI*

Setting Up Administrator Console and Command-Line Interface on a Remote Host

This section explains how to set up Portal Server administrator console or command-line interface on a remote host. In this scenario, you can install Portal Server on a node and can set up administrator console or command-line interface on another node. On the node where you set up administrator console or command-line interface, you need to install a web container and Portal Server packages. You need to install Portal Server packages in the Configure Later mode.

The `psconsole` of Portal Server can be installed only on Web Server or Application server. If you install Portal Server on any of the compatible web containers, such as BEA WebLogic or IBM WebSphere, you need to install `psconsole` on Web Server or Application Server.

To Set Up an Administrator Console on a Remote Host on Web Server 7.0

1. **Install Portal Server 7.1 on Node 1 in the Configure Now mode.**
2. **Install Web Server on Node 2 in the Configure Now mode.**
3. **Install Portal Server in the Configure Later mode on Node 2.**
4. **Create the following directory structure in your current directory.**

   ```
   mkdir -p WEB-INF/classes/
   ```

   ```
   mkdir -p WEB-INF/lib/
   ```

5. **Create a property file,** `WEB-INF/classes/pasconnect.properties`**, with the property value pair** `pas.host=`*node1.domain.com*.
6. **Copy the** `cacao_cacao.jar` **file into the** `WEB-INF/lib` **directory.**

   The `cacao_cacao.jar` file is located in the following directories:

   - For Solaris platform: `/usr/lib/cacao/lib`
   - For Linux platform: `/`*cacao_base*`/sun/cacao/share/lib`
7. **In the** `psconsole.war` **file, add the following content.**

   ```
   jar -uvf /PortalServer_base/SUNWportal/admin/psconsole.war WEB-INF
   ```

8. **Deploy the updated** `psconsole.war` **file to the Web Server instance.**

To Set Up an Administrator Console on a Remote Host on Application Server 8.2

1. **Install Portal Server 7.1 on Node 1 in the Configure Now mode.**
2. **Install Application Server 8.2 on Node 2 in the Configure Now mode.**
3. **Install Portal Server in the Configure Later mode on Node 2.**
4. **Stop the common agent container on node 2.**

   ```
   /usr/lib/cacao/bin/cacaoadm stop
   ```

5 **Run the following command on Node 2:**

```
/usr/lib/cacao/bin/cacaoadm create-keys -f
```

6 **Start the common agent container on Node 2 .**

```
/usr/lib/cacao/bin/cacaoadm start
```

7 **Create the following directory structure in your current directory.**

```
mkdir -p WEB-INF/classes/
```

```
mkdir -p WEB-INF/lib/
```

8 **Create a property file,** `WEB-INF/classes/pasconnect.properties`**, with the property value pair** `pas.host=`*node1.domain.com*.

9 **Copy the** `cacao_cacao.jar` **file into the** `WEB-INF/lib` **directory.**

The `cacao_cacao.jar` file is located in the following directories:

- For Solaris platform: `/usr/lib/cacao/lib`
- For Linux platform: */cacao_base*`/sun/cacao/share/lib`

10 **In the** `psconsole.war` **file, add the following content.**

```
jar -uvf /PortalServer_base/SUNWportal/admin/psconsole.war WEB-INF
```

11 **Deploy the updated** `psconsole.war` **file to the Application Server instance.**

12 **Add the following in the** `/domains/domain1/server.policy` **file.**

```
grant {
permission java.util.PropertyPermission "*","read,write";
permission java.lang.RuntimePermission "writeFileDescriptor";
permission java.lang.RuntimePermission "createClassLoader";
permission java.io.FilePermission "\${/}-", "read,write,execute,delete";

// Used by psconsole app
permission java.security.SecurityPermission "insertProvider.SunSASL";
permission java.security.SecurityPermission "insertProvider.SunJSSE";
permission java.lang.RuntimePermission "getProtectionDomain";

};
```

13 **Restart the Application Server instance.**

Note – Step 12 is not required if the security manager is disabled for the Application Server domain where psconsole is deployed. This is achieved by commenting out the following JVM option for security policy in the `domain.xml` file.

```
<jvm-options>-Djava.security.policy=${com.sun.aas.instanceRoot}
/config/server.policy</jvm-options>
```

▼ To Setup Command-Line Interface on a Remote Host on Web Server 7.0 or Application Server 8.2

1. **Install the Portal Server 7.1 on Node 1 in the Configure Now mode.**
2. **Install Web Server 7.0 or Application Server 8.2 on Node 2 in the Configure Now mode.**
3. **Install Portal Server 7.1 on Node 2 in the Configure Later mode.**
4. **In the** *PortalServer_base*`/SUNWportal/samples/psconfig/example2.xml` **file, replace tokens with the node information for Node 2.**
5. **Run the following command:**

   PortalServer_base`/SUNWportal/bin/psconfig --config` *example2.xml*
6. **In the** `pasconnect.properties` **file, change the property value as** `pas.host=`*node1.domain.com*.

   The `pasconnect.properties` file is located in the following directories:

   - For Solaris platform: `/etc/opt/SUNWportal`
   - For Linux platform: `/etc/SUNWportal`

◆ ◆ ◆ CHAPTER 8

Installing and Configuring Portal Server 7.1 in High Availability Scenarios

In a high availability scenario, many Portal Server instances and Access Manager instances exist. An end user accesses any of the Portal Server instances. When a Session Fail Over occurs, the user automatically gets redirected to an available Portal Server instance. This chapter covers various high availability scenarios.

This chapter contains the following scenarios:

Installing Portal Server and Access Manager in a High Availability Scenario with Berkeley Database

This section explains how to install Portal Server and Access Manager in a high availability scenario using Berkeley database. Berkeley database is installed when you install Access Manager. In a high availability scenario, Berkeley database is used to store session variables of the user.

In the procedures in this section, you do the following:

- Install Directory Server, Application Server, Access Manager, and Portal Server on Node 1 and Node 2.
- Install a Portal Server instance on Node 2. (The portal ID for Node 1 and Node 2 are the same.)
- Install a Load Balancer on Node 3.

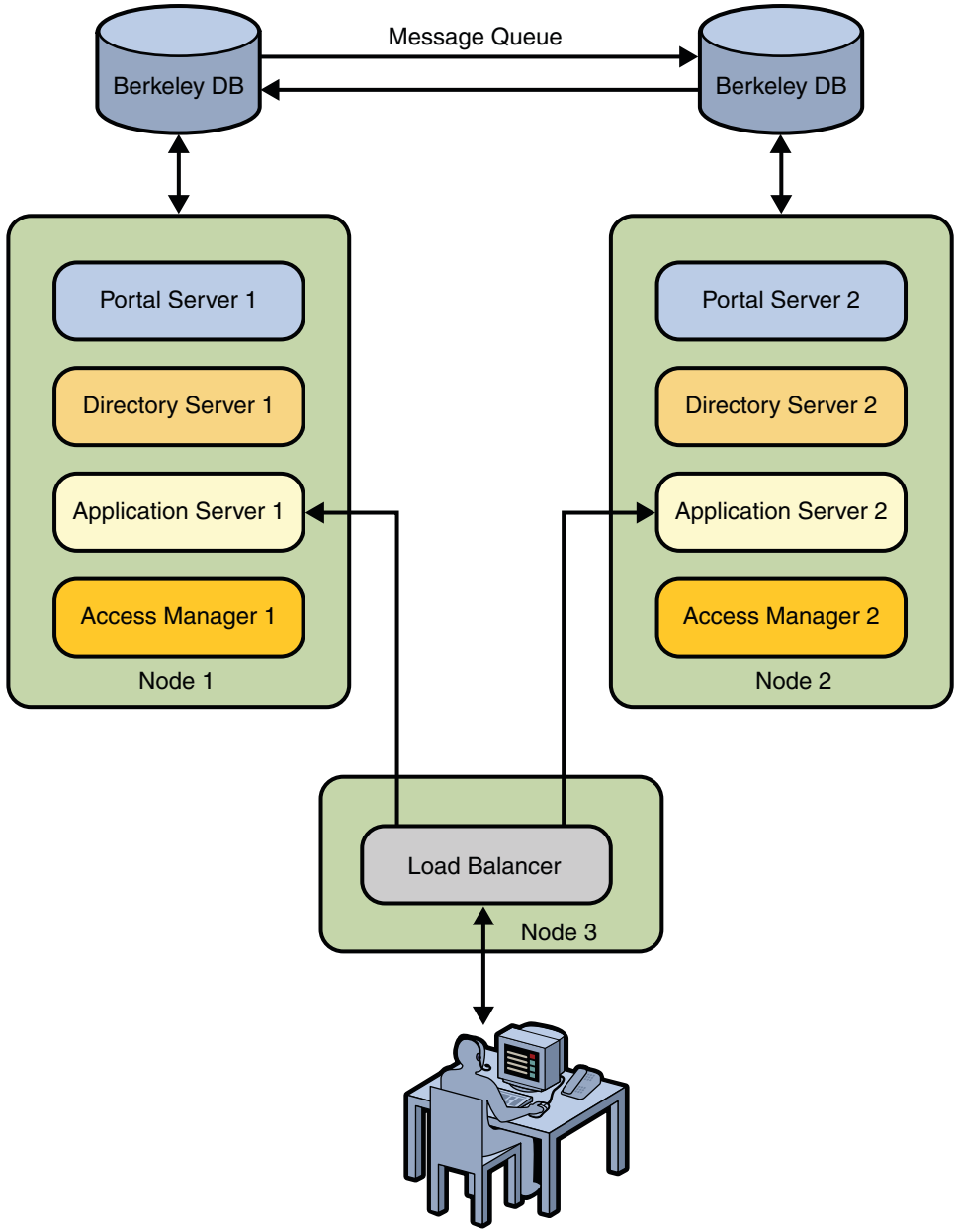

FIGURE 8–1 Portal Server With Berkely Database

▼ To Install Portal Server and Access Manager in a High Availability Scenario with Berkeley Database

These instructions require the following:

- Directory Server on Node 1 is not in the multi master replication (MMR) mode. Only one instance of Directory Server exists.
- Access Manager on Node 1 is installed in Legacy mode. The data can be stored only in Directory Server.

1. **On Node 1, install Directory Server, Access Manager, and Application Server.**

2. **Verify whether Access Manager is installed properly by accessing amconsole.**

   `http://`*node1.domain-name***`:8080/amconsole`**

3. **Log in to `amconsole` on Node 1. In the Organization Aliases List, add the Fully Qualified Domain Name (FQDN) of Node 2.**

4. **Click Service Configuration and click Platform in the right panel.**

5. **In the Platform Server List, add the following.**

   `http://`*node2.domain-name***`:8080|02`**

6. **On Node 2, run the Java ES installer to install Access Manager.**

   On the page that asks whether Directory Server is already provisioned with data, select Yes and proceed with installing Access Manager.

   Note – Ensure that the password encryption key on Node 2 is the same as the password encryption key on Node 1. The password encryption key should be the same for the LDAP internal password on both of the nodes.

   ---

7. **On Node 2, start Application Server and verify whether Access Manager is installed properly by accessing amconsole.**

   `http://`*node2.domain-name***`:8080/amconsole`**

8. **In a text editor, open the `AMConfig.properties` file on Node 1 and Node 2.**

   The file is located in the *AccessManager_base*`/SUNWam/config` directory.

   a. **Edit the `com.iplanet.am.cookie.encode` property to be `false`.**

   b. **Edit `com.sun.identity.server.fqdnMap`***Node3.domain-name***`=isserver.mydomain.com` with the Fully Qualified Domain Name of the Load Balancer.**

▼ To Install the Load Balancer on Node 3

1 Install the Load Balancer plugin on Node 3 that is provided with Application Server 8.2. Select Web Server as a component to install with the Load Balancer plugin.

2 In a text editor, open the `loadbalancer.xml` file on Node 3.

This file is located in the *WebServer_base*`/SUNWwbsvr7/https-`*Node3*`/config` directory.

3 Edit the file so that the Load Balancer balances the load between the two Access Manager instances.

Edit the listeners with the appropriate values.

A sample `loadbalancer.xml` which balances the load on Portal Server and Access Manager instances on Node 1 and Node 2 is as follows:

```
<!DOCTYPE loadbalancer PUBLIC
"-//Sun Microsystems Inc.//DTD Sun ONE Application Server 7.1//
EN" "sun-loadbalancer_1_1.dtd">
<loadbalancer>
<cluster name="cluster1">
<!--
Configure the listeners as space seperated URLs like
listeners="http://host:port https://host:port" For example:
<instance name="instance1" enabled="true"
disable-timeout-in-minutes="60"
listeners="http://localhost:80
https://localhost:443"/>
-->
<instance name="instance1" enabled="true"
disable-timeout-in-minutes="60"
listeners="http://node1.domain-name:8080"/>
<instance name="instance2" enabled="true"
disable-timeout-in-minutes="60"
listeners="http://node2.domain-name:8080"/>
<web-module context-root="/portal" enabled="true"
disable-timeout-in-minutes="60" error-url="sun-http-lberror.html" />
<web-module context-root="/psconsole" enabled="true"
disable-timeout-in-minutes="60" error-url="sun-http-lberror.html" />
<web-module context-root="/amserver" enabled="true"
disable-timeout-in-minutes="60" error-url="sun-http-lberror.html" />
<web-module context-root="/amconsole" enabled="true"
disable-timeout-in-minutes="60" error-url="sun-http-lberror.html" />
<web-module context-root="/ampassword" enabled="true"
disable-timeout-in-minutes="60" error-url="sun-http-lberror.html" />
<web-module context-root="/amcommon" enabled="true"
disable-timeout-in-minutes="60" error-url="sun-http-lberror.html" />
<web-module context-root="/" enabled="true"
```

```
disable-timeout-in-minutes="60" error-url="sun-http-lberror.html" />
<health-checker url="/" interval-in-seconds="10" timeout-in-seconds="30" />
</cluster>
<property name="reload-poll-interval-in-seconds" value="60"/>
<property name="response-timeout-in-seconds" value="30"/>
<property name="https-routing" value="true"/>
<property name="require-monitor-data" value="false"/>
<property name="active-healthcheck-enabled" value="false"/>
<property name="number-healthcheck-retries" value="3"/>
<property name="rewrite-location" value="true"/>
</loadbalancer>
```

4 **Start the Web Server.**

5 **On Node 1 and Node 2, start Access Manager, Directory Server, and Application Server .**

▼ To Configure Session Failover with Message Queue and Berkeley Database

1 **Edit the Application Server** `domain.xml` **file on Node 1 and Node 2 to add locations of the** `jms.jar` **file and** `imq.jar` **file.**

```
<JAVA javahome="/usr/jdk/entsys-j2se"
server-classpath="/usr/share/lib/imq.jar:/usr/share/lib/jms.jar: ....?
```

Note – When you create a Message Queue instance, do not use the default Message Queue instance that starts with Application Server or the guest user for Message Queue.

---

2 **Start Message Queue on Node 1 and Node 2.**

`/bin/imqbrokerd -tty -name` *mqins* `-port` *7777* `&`

where *mqins* is the Message Queue instance name.

3 **Add a user to this message queue.**

`imqusermgr add -u` *amsvrusr* `-p` *secret12* `-i` *mqins* `-g` *admin*

where *amsvrusr* is the name of the new user that is used instead of guest.

4 **Inactivate the guest user.**

`imqusermgr update -u` *guest* `-i` *mqins* `-a` *false*

5 **Create an encrypted file for the message queue on Node 1 and Node 2.**

`./amsfopasswd -f` */AccessManager_base/*`SUNWam/.password -e` *password-file*

6 **Edit the** `amsfo.conf` **file on both the nodes.**

A list of sample entries in `amsfo.conf` file is displayed as follows:

```
AM_HOME_DIR=/opt/SUNWam
AM_SFO_RESTART=true
LUSTER_LIST=node1.domain-name:7777,node2.domain-name:7777
DATABASE_DIR="/tmp/amsession/sessiondb"
DELETE_DATABASE=true
LOG_DIR="/tmp/amsession/logs"
START_BROKER=true
BROKER_INSTANCE_NAME=amsfo
BROKER_PORT=7777
BROKER_VM_ARGS="-Xms256m -Xmx512m"
USER_NAME=amsvrusr
PASSWORDFILE=$AM_HOME_DIR/.password
AMSESSIONDB_ARGS=""
lbServerPort=8080
lbServerProtocol=http
lbServerHost=node3.domain-name
SiteID=10
```

7 **Configure** `amsfo.conf` **on Node 1.**

AccessManager_base`/SUNWam/bin/amsfoconfig`

After running the script, the following output is displayed:

```
Session Failover Configuration Setup script.
============================================================
============================================================
Checking if the required files are present...
============================================================

Running with the following Settings.
-----------------------------------------------
Environment file: /etc/opt/SUNWam/config/amProfile.conf
Resource file: /opt/SUNWam/lib/amsfo.conf
         -----------------------------------------------
Using /opt/SUNWam/bin/amadmin

Validating configuration information.
Done...

Please enter the LDAP Admin password:
(nothing will be echoed): password1
Verify: password1
Please enter the JMQ Broker User password:
(nothing will be echoed): password2
Verify: password2
```

```
Retrieving Platform Server list...
Validating server entries.
Done...

Retrieving Site list...
Validating site entries.
Done...

Validating host: http://amhost1.example.com:7001|02
Validating host: http://amhost2.example.com:7001|01
Done...

Creating Platform Server XML File...
Platform Server XML File created successfully.

Creating Session Configuration XML File...
Session Configuration XML File created successfully.

Creating Organization Alias XML File...
Organization Alias XML File created successfully.

Loading Session Configuration schema File...
Session Configuration schema loaded successfully.

Loading Platform Server List File...
Platform Server List server entries loaded successfully.

Loading Organization Alias List File...
Organization Alias List loaded successfully.

Please refer to the log file /var/tmp/amsfoconfig.log for additional
information.
################################################################
Session Failover Setup Script. Execution end time 10/05/05 13:34:44
################################################################
```

8 Edit the `amsessiondb` script with the default path and directory of the following:

```
JAVA_HOME=/usr/jdk/entsys-j2se/
IMQ_JAR_PATH=/usr/share/lib
JMS_JAR_PATH=/usr/share/lib
BDB_JAR_PATH=/usr/share/db.jar
BDB_SO_PATH=/usr/lib
AM_HOME=/opt/SUNWam
```

9 Start and stop the Message Queue instance running on port 7777.

AccessManager_base`/SUNWam/bin/amsfo start`

AccessManager_base`/SUNWam/bin/amsfo stop`

10 **Restart Access Manager, Directory Server, Application Server, and Web Server on all the nodes.**

11 **Log in to the** `amconsole` **through Load Balancer.**
`http://`*node3.domain-name*`:80/amconsole`

12 **Stop the Application Server on Node 1.**
The session is handled by Access Manager on Node 2.

▼ To Install Portal Server on Node 1

1 **Invoke the Java ES installer and install Portal Server on Node 1 in the Configure Now mode.**

2 **Access Portal Server to verify the installation.**
`http://`*node1.domain-name*`:8080/portal`

3 **Create a Portal Server instance on Node 2.**

▼ To Create a Portal Server Instance on Node 2

1 **Invoke the Java ES installer, and install Portal Server in the Configure Now mode.**

2 **Copy** `example2.xml` **to a temporary directory to make a backup of the original file.**
`cp` *PortalServer_base*`/SUNWportal/samples/psconfig/example2.xml` */tmp-directory*

3 **Edit the original** `example2.xml` **file to replace the tokens with the machine information for Node 1.**

4 **Configure Portal Server using the** `example2.xml` **file as the configuration XML file.**
PortalServer_base`/SUNWportal/bin/psconfig --config` *example2.xml*

5 **Copy the** `Webcontainer.properties` **template file to Portal Server installation** `bin` **directory.**
`cp` *PortalServer_base*`/SUNWportal/template/Webcontainer.properties`
`\`*PortalServer_base*`/SUNWportal/bin`

6 **Modify the** `WebContainer.properties` **file as per your requirements.**
`vi` *PortalServer_base*`/SUNWportal/bin/WebContainer.properties`

Refer to the Creating Multi-Portal for more information about changing the `WebContainer.properties` file.

7 **Create a Portal Server instance.**

PortalServer_base/SUNWportal/bin/psadmin create-instance -u *amadmin* -f *ps_password* -p *portal1* -w Webcontainer.properties

8 **Restart Directory Server, Application Server, Access Manager, and Portal Server on Node 1 and Node 2.**

9 **Restart Web Server on Node 3.**

10 **Access the portal through the Load Balancer.**

You can verify the node to which the portal is connected by tracking the access logs of the container. After you log in to the portal, kill the Application Server on the node to which it is connected. Then, click any of the links on the desktop to maintain the session and automatically connect to Node 2.

Configuring HADB for Session Fail Over

▼ To Configure HADB for Session Fail Over

Before You Begin

- All nodes are in the same subnet.
- Servers are installed with the latest OS patch level.
- Name resolution of all servers is correct on each server, either through the hosts file or DNS.
- The fully qualified hostname is the first entry after the IP address in the /etc/hosts file. The other machine details are also entered in hosts file.
- Any previously installed Java Enterprise System components are removed from the system before starting the installation procedure.
- Installation happens in a shared memory configuration.

1 **Check the physical memory of the nodes.**

```
prtconf | grep Mem
```

2 **Calculate the value of the** shminfo_shmmax **parameter.**

shminfo_shmmax = (Server's Physical Memory in MB / 256 MB) * 10000000

For example, if the physical memory is 512 MB, the value of the shminfo_shmmax parameter is 20000000.

3 **Add the following parameter to the** /etc/system **configuration file.**

```
set shmsys:shminfo_shmmax=0x40000000
set shmsys:shminfo_shmseg=20
```

```
set semsys:seminfo_semmni=16
set semsys:seminfo_semmns=128
set semsys:seminfo_semmnu=1000
```

4 **Reboot the server.**

5 **Set up secure shell (ssh).**

The secure shell is used by the HADB component of the Sun Application Server Enterprise Edition to exchange file information between the server nodes in the application server cluster. Additionally, the HADB utility commands can operate on multiple server nodes at the same time to keep them in sync.

Note – Root ssh login is required between servers without the need for password authentication. This is achieved by enabling non-console root login and configuring the ssh certificates.

---

6 **Check and implement the following steps on each application server cluster node to ensure successful installation, configuration, and operation of the software.**

7 **Ensure that the hostname has a fully qualified domain name in the `/etc/hosts` file as the first entry after the IP address.**

For example, 10.10.10.2 as 1.example.com as1 loghost

8 **Check that hostname lookup and reverse lookup is functioning correctly.**

9 **Check the contents of the `/etc/nsswitch.conf` file hosts entry.**

```
cat /etc/nsswitch.conf | grep hosts
```

10 **Allow non-console root login by commenting out the `CONSOLE=/dev/console` entry in the `/etc/default/login` file.**

```
cat /etc/default/login | grep "CONSOLE="
```

11 **If you need to enable remote root ftp, comment out the `root` entry in the `/etc/ftpd/ftpusers` file.**

```
cat /etc/ftpd/ftpusers | grep root
```

12 **Permit ssh root login. Set `PermitRootLogin` to yes in the `/etc/ssh/sshd_config` file, and restart the ssh daemon process.**

```
cat /etc/ssh/sshd_config | grep PermitRootLogin
/etc/init.d/sshd stop
/etc/init.d/sshd start
```

13 **Generate the ssh public and private key pair.**

```
ssh-keygen -t dsa
```

Note – When running the ssh-keygen utility program, do NOT enter a passphrase and press Return. Otherwise, whenever ssh is used by the Application Server, the passphrase will be prompted for — breaking the automated scripts.

14 **Generate the keys on all Application Server nodes before proceeding to the next step where the public key values are combined into the** `authorized_keys` **file.**

15 **Copy all the public key values to each server's** `authorized_keys` **file. Create the** `authorized_keys` **file on one server and then copy that to the other servers.**

```
root@as1# cd ~/.ssh
root@as1# cp id_dsa.pub authorized_keys.as2
root@as1# scp as2.example.com:/.ssh/id_dsa.pub authorized_keys.as2
root@as1# cat authorized_keys.as2 >> authorized_keys
root@as1# rm authorized_keys.as2
root@as1# scp authorized_keys as2.example.com:/.ssh/authorized_keys
```

16 **Verify that ssh functions correctly between the Application Server nodes without the need for a password to be entered.**

17 **Create node agents on the two server on Host A , Host B, and Host C.**

18 **Create the cluster.**

19 **Create a server instance for each server at the DAS.**

20 **Start the ma on all the nodes.**

```
cd /opt/SUNWhadb/4/bin; ./ma &
```

21 **Create the ha cluster on Host A.**

```
asadmin configure-ha-cluster --user admin --devicesize 256 --hosts HostB,HostC
pscluster
```

Installing Portal Server on an Application Server Cluster

This section explains how to install Portal Server 7.1 in an Application Server cluster environment. In a cluster environment, a primary node exists where Portal Server is installed. A cluster is created in the primary node. One or more secondary nodes exist where instances of Portal Server are created. The user accesses the portal through a load balancer. In such an environment, if any of the servers installed on any node goes down, the load balancer automatically redirects the user to the other available Portal Server instances.

Note – If Portal Server is installed on a clustered environment, any deployment or undeployment of container specific files should be done on the primary instance, where DAS is installed.

▼ To Install Portal Server on Application Server Cluster

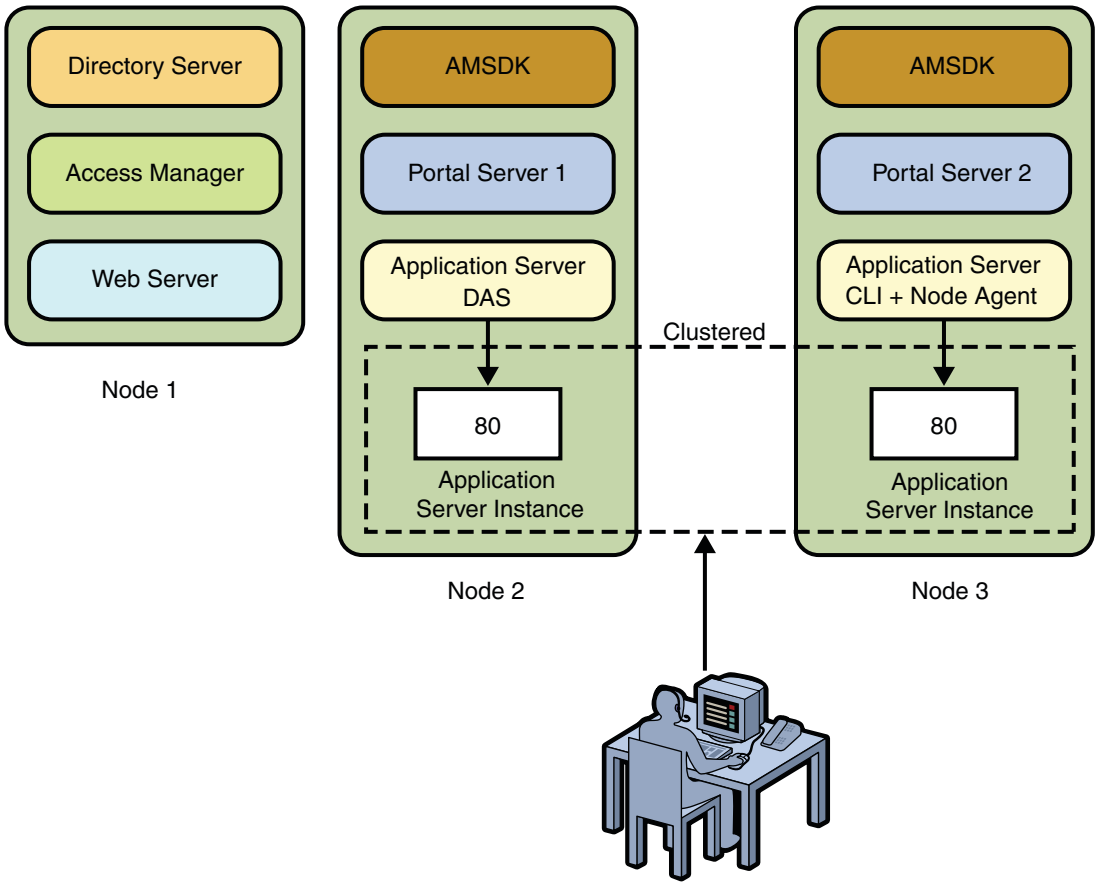

FIGURE 8–2 Portal Server on Application Server Cluster

1 **On Node 1, install Access Manager, Web Server, and Directory Server using the Java ES installer. Directory Server is in the MMR (Multi Master Replication) mode. Access Manager and Directory Server must be in the HA Configuration mode.**

2 **Verify whether Access Manager is installed properly.**

`http://`*node1.domain-name:80*`/amconsole`

3 **Install Portal Server on Node 2.**

▼ Install Portal Server on Node 2

1 **Install Application Server and Access Manager SDK using the Java ES installer in the Configure Now mode.**

Note – Select the Application Server components, such as Domain Application Server (DAS) and Command-Line Interface.

---

2 **Start Domain Application Server.**

ApplicationServer_base`/SUNWappserver/sbin/asadmin start-domain --user` *admin domain1*

3 **Create a node agent, for example** `ps1`**.**

ApplicationServer_base`/SUNWappserver/sbin/asadmin create-node-agent --user` *admin ps1*

4 **Start the node agent.**

ApplicationServer_base`/SUNWappserver/sbin/asadmin start-node-agent --user` *admin ps1*

5 **Create a cluster, for example** `pscluster`**.**

ApplicationServer_base`/SUNWappserver/sbin/asadmin create-cluster --user` *admin pscluster*

Creating a cluster creates a configuration, namely `pscluster-config`.

6 **Create an Application Server instance, for example** `server1–ps1`**.**

ApplicationServer_base`/SUNWappserver/sbin/asadmin create-instance --user` *admin* `--cluster` *pscluster* `--nodeagent` *ps1* `--systemproperties HTTP_LISTENER_PORT=80` *server1-ps1*

7 **Start the Application Server instance.**

ApplicationServer_base`/SUNWappserver/sbin/asadmin start-instance --user` *admin server1-ps1*

8 **Using the Java ES installer, install Portal Server in the Configure Later mode.**

9 **Create a Portal Server instance by modifying the `example14.xml` file with the installation parameters.**

Also, set the `WebcontainerInstanceName` attribute to the Application Server Cluster, `pscluster`. Set the host name as the primary host, `node1.domain-name`.

PortalServer_base`/SUNWportal/bin/psconfig --config example14.xml`

10 **Delete the `com.sun.portal.instance.id` option from the `pscluster` configuration, and add it to the `server1`–`ps1` instance.**

ApplicationServer_base`/SUNWappserver/sbin/asadmin delete-jvm-options --user` *admin* `--target` *pscluster* `"-Dcom.sun.portal.instance.id=ps1-80"`

ApplicationServer_base`/SUNWappserver/sbin/asadmin create-system-properties --user` *admin* `--target server1-ps1 com.sun.portal.instance.id=`*ps1-80*

ps1–80 is the name of the instance specified in the configuration file.

▼ To install Portal Server on Node 3

1 **Install Application Server's node agent and command-line interface and Access Manager SDK in the Configure Now mode using the Java ES installer.**

Note – Configure the Application Server's node agent to use *node1.domain-name* as the Domain Application Server.

The Java ES installer creates a node agent, `node3`.

---

2 **Install Portal Server in the Configure Later mode using the Java ES installer.**

3 **Configure Access Manager SDK to use Access Manager Directory Server installed on `node1.domain-name`.**

4 **Start the node agent.**

ApplicationServer_base`/SUNWappserver/sbin/asadmin start-node-agent --user` *admin* *node3*

5 **Create an Application Server instance, `ps2`–`80`.**

ApplicationServer_base`/SUNWappserver/sbin/asadmin create-instance --user` *admin* `--cluster` *pscluster* `--nodeagent` *node3* `--systemproperties HTTP_LISTENER_PORT=80` *ps2-80* `--host` *node2*

6 **Start the Application Server instance.**

7. **Delete `ps_util.jar` Classpath from the Application Server instance.**

   Creating a Portal Server instance verifies whether the Application Server instance is not already been configured for a Portal Server instance. It does it by checking the `ps_util.jar` class path. For instances that are part of Application Server cluster the configuration and applications are automatically deployed. So, the `create-instance` sub command fails.

   a. **Log in to Application Server.**

   b. **Click Configuration > pscluster-config > JVM Settings.**

   c. **In the Classpath Suffix list box, delete** *PortalServer_base*`/SUNWportal/lib/ps_util.jar`**.**

8. **Configure the common agent container by modifying the `example2.xml` file with the deployment values.**

   PortalServer_base`/SUNWportal/bin/psconfig --config example2.xml`

9. **Create a `Webcontainer.properties.ps2` file by modifying the `Webcontainer.properties.SJSAS81` file with the newly create instance parameters, such as host, port, scheme, and file paths.**

   The `Webcontainer.properties.SJSAS81` file is located at the *PortalServer_base*`/SUNWportal/template` directory.

10. **Create a Portal Server instance in the newly created Application Server instance.**

    PortalServer_base`/SUNWportal/bin/psadmin create-instance -u` *amadmin* `-f` *password* `--portal myPortal --instance` *ps2-80* `--webconfig` *Webcontainer.properties.ps2*

11. **Add the `com.sun.portal.instance.id` to the `server1`–`ps1` instance.**

    ApplicationServer_base`/SUNWappserver/sbin/asadmin create-system-properties --user` *admin* `--target` *ps2-80* `com.sun.portal.instance.id=`*ps2-80* `--host` *node1*

    ps2–80 is the name of the default instance specified in the configuration file.

▼ To Display the Default WSRP Portlets in the WSRP tab of Portal Desktop

When you configure Portal Server on Application Server cluster, the default portlets are not displayed on the WSRP tab of the desktop. Do the following to get portlets displayed on the WSRP tab.

1. **Create a producer with the portlets that you want to add to the WSRP tab.**

2. **Configure a consumer with the producer.**

3 **Add the consumer to the WSRPSamplesTabPanel container.**

For more information on how to create and configure a producer, see *Technical Note: Web Services for Remote Portlets for Sun Java System Portal Server 7.1*.

Note – You can also do the following to display the defaults portlets on the WSRP tab:

a. Create a producer with Bookmark, JSP Remote, Notepad, and Weather portlets.
b. Configure a consumer with the producer.
c. Copy the producer entity ID after configuring the producer.
d. Go to Manage Channels and Container.
e. Under Developer Sample, select the WSRPSamplesTabPanel container.

   This container displays Bookmark, JSP Remote, Notepad, and Weather portlets.
f. Select the portlet and paste the producer entity ID to the Producer Entity ID field.

▼ To Configure Portlet Session Failover on Application Server 8.2

Before You Begin The portal instances should be clustered and HADB should be installed.

1 **Undeploy the `portal.war` from the Application Server 8.2 DAS (administration server), and add the <distributable/> tag in the `WEB-INF/web.xml` of `portal.war`. Refer to the sample `web.xml` file displayed below:**

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE web-app PUBLIC "-//Sun Microsystems, Inc.//DTD Web Application 2.3//EN
" "http://java.sun.com/dtd/web-app_2_3.dtd">
<web-app>
<display-name>Sun Java Enterprise System Portal Server Desktop Web Application</
display-name>
<description>Provides a user customizable interface for content that is aggregat
ed from Portlet applications</description>
<distributable/>
<context-param>
<param-name>desktop.configContextClassName</param-name>
<param-value>com.sun.portal.desktop.context.PropertiesConfigContext</param-value>
```

2 **Add the same <distributable/> tag to the `web.xml` of the `portlet.war` which is used for storing session variable.**

3 **Ensure that the Availability option is selected for both `portal.war` and the `portlet.war` files.**

   a. **Log in to administration console of Application Server.**

b. Click Web applications -> portal.

c. Select the Availability option in the right panel.

Clustering in Portal Server 7.1 on BEA WebLogic 8.1 Service Pack 4 and Service Pack 5

This section explains about clustering Portal Server 7.1 on BEA WebLogic 8.1 Service Pack 4 and Service Pack 5.

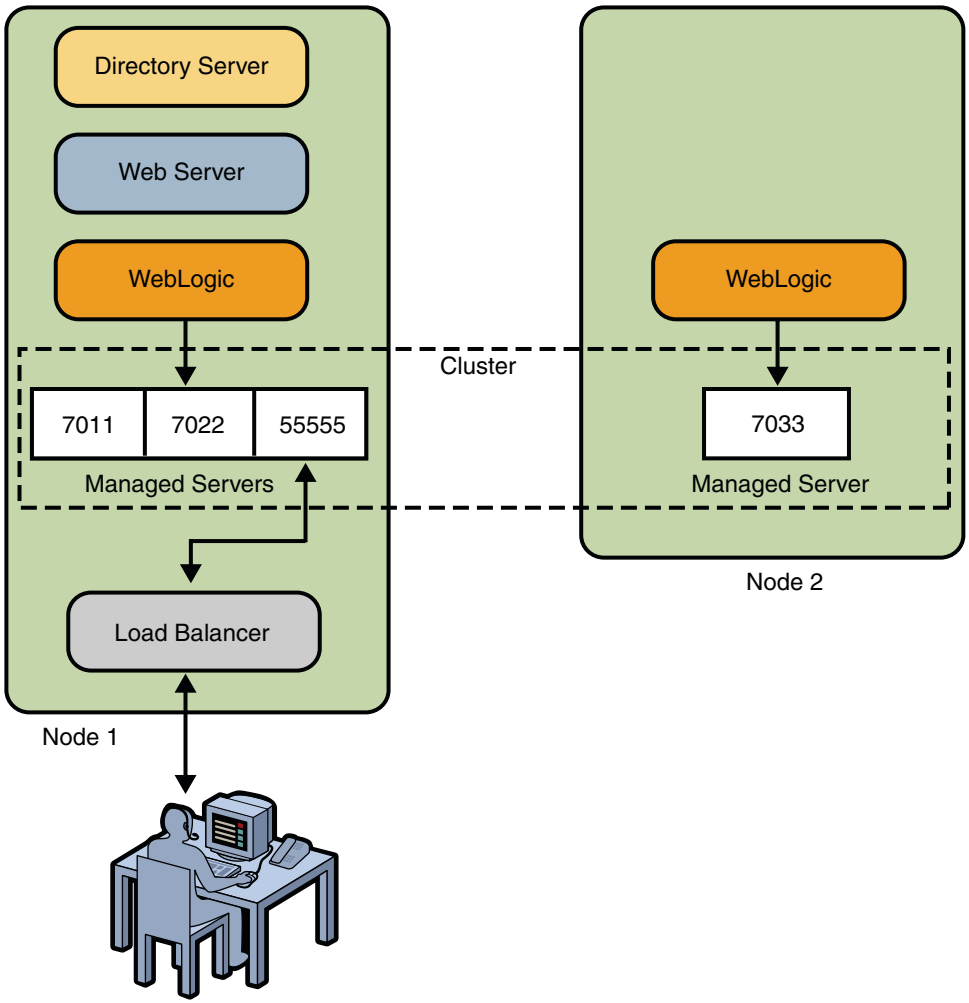

FIGURE 8–3 Portal Server on WebLogic Cluster Environment

▼ To Cluster Portal Server 7.1 on WebLogic 8.1 Service Pack 4

In this section, you do the following:

- Install Directory Server and Web Server on Node 1. (`psconsole` of Sun Java System Portal Server does not support WebSphere and WebLogic.)
- Install BEA WebLogic 8.1 Service Pack 4 or WebLogic 8.1 Service Pack 5 using Sun Java Development Kit.

- Create a node agent on Node 1 on the port 5555.
- Create three managed servers on the following ports of the node agent: port 7011, port 7022, and port 55555. The first two managed servers are used for creating the Portal Server instances. The third managed server is used as proxy server for load balancing.
- Create a BEA WebLogic managed server on Node 2.
- Create a node agent and managed server on Node 2 using the Administrator Server on Node 1.
- Install Access Manager on Administrator Server on Node 1.
- Install Portal Server on port 7011 of Node 1. Creates an instance of Portal Server on the managed servers created on Node 1 and Node 2.
- Configure a cluster and a load balancer.
- Install a Gateway on Node 3.

Before You Begin

- Ensure that the node on which you perform the task has a BEA license for clustering to work.
- Ensure that all clustered nodes are in the same subnet.

1 **Run the BEA WebLogic 8.1 installer to install BEA WebLogic 8.1.**

2 **Run the script** `quickStart.sh` **after a successful installation.**

Bea-base`/weblogic81/common/bin/quickStart.sh`

3 **Click Create a New Domain Configuration or Extend an Existing One.**

The installation panel appears.

4 **Enter** `admin` **and the** `admin` **password.**

Leave the other defaults as they are.

5 **Click Finish to complete the installation.**

6 **To start WebLogic, run the** `startWeblogic.sh` **script.**

Bea-base`/user_projects/domains/mydomain/startWeblogic.sh`

7 **Access the Administrator server.**

`http://`*node1.domain-name*`:7001/console`**

By default, the administrator server of WebLogic is created on port 7001.

▼ To Create a Node Agent on Node 1

This procedure creates a node agent on the port 5555, which is the default port for node agents. A node agent is required to create managed servers.

1 **Log in to the administrator server.**

`http://`*node1.domain-name*`:7001/console`**

2 **Click Machines and click Configure a New Machine.**

3 **Enter a name for the node agent, and click Create. For example,** `node_1`**.**

By default, the node agent runs on the port 5555. If you need any other port, enter the port number in the Node Manager tab.

4 **On Node 1, start the node agent.**

Bea-base`/weblogic81/server/bin/startNodeManager.sh` *node1-ip-address* `5555`

▼ To Create WebLogic Managed Servers on Node 1

This procedure creates managed servers on port 7011, port 7022, and port 55555. The first two managed servers are used for creating Portal Server instances. The last one is used as a proxy server to set up the load balancer.

1 **Log in to the administrator server.**

`http://`*node1.domain-name*`:7001/console`**

2 **Click Servers, and click Configure a New Machine.**

3 **Enter a name for the managed server. For example,** `node1_7011`**.**

4 **Select node_1 from the Machine list box.**

5 **Enter the Listen Port as** `7011`**, and click Create.**

6 **To start the managed server, click the Control tab and click Start the Server.**

7 **(Optional) You can also start the managed server using the command-line interface.**

bea_base`/user_projects/domains/mydomain/startManagedWeblogic.sh node1_7011`

8 **Use steps 2 through 5 to create a managed server named** `node1_7022` **with a listen port of** `7022`**.**

9 **Start the second managed server.**

10 **Use steps 2 through 5 to create a managed server named** `proxy` **with a listen port of** `55555`**.**

This managed server is used for the proxy settings.

11 **Start the third managed server.**

▼ To Create a Node Agent on Node 2

This procedure creates a node agent on port 5555 on Node 2 using the administrator console installed in Node 1.

1 **Install BEA WebLogic on Node 2.**

2 **Log in to the administrator server of Node 1.**

`http://`*node1.domain-name*`:7001/console`**

3 **Click Machines and click Configure a New Machine.**

4 **Enter** `node_2` **for the node agent name, and click Create.**

5 **In the Listen Address field, enter the IP address of Node 2.**

6 **On Node 2, start the node agent.**

Bea-base`/weblogic81/server/bin/startNodeManager.sh` *node2-ip-address* `5555`

7 **In the** `nodemanager.Hosts` **file of Node 2, add the IP address of Node 1.**

Bea-base`/weblogic81/common/nodemanager.Hosts`

You need to do this to ensure that Node 2's node agent can accept commands from the administrator server on Node 1.

▼ To Create WebLogic Managed Servers on Node 2

This procedure creates a managed server on Node 2 on the port 7033 using the administrator console installed on Node 1.

1 **Log in to the administration server.**

`http://`*node1.domain-name*`:7001/console`**

2 **Click on Servers, and click Configure a New Machine.**

3 **Enter a name for the managed server. For example,** `node2_7033`**.**

4. **Select** `node_2` **from the Machine list box.**
5. **Enter the Listen Address as the IP address of Node 2.**
6. **Enter the Listen Port as** `7022`**, and click Create.**
7. **Click the Control tab and click Start the Server.**
8. **(Optional) You can also start the managed server using the command-line interface on Node 2.**
   bea_base`/user_projects/domains/mydomain/startManagedWeblogic.sh` *node2_7033*

▼ To Install Access Manager on Administrator Server

This procedure installs Access Manager on the Administrator server (BEA WebLogic 8.1 Administrator Server) on Node 1. By default, the Administrator Server port is 7001.

1. **Install Directory Server and Web Server using the Java ES installer.**
2. **Install Access Manger in the Configure Later mode.**
3. **Run** `amsamplesilent`**.**
   AccessManager_base`/SUNWam/amconfig -s amsamplesilent`
4. **Change the values in** `amsamplesilent` **accordingly.**
5. **Access amconsole and verify whether Access Manager is running.**
   `http://`*node1.domain-name*`:7001/amconsole`

▼ To Install Portal Server 7.1 on Node 1

This procedure installs Portal Server 7.1 on port 7011 of the managed server on Node 1.

1. **Install Portal Server 7.1 using the Java ES installer.**
2. **In the installer, select Managed Server while installing.**
3. **Access the portal.**
   `http://`*node1.domain-name*`:7011/portal/dt`

   The Portal Welcome page appears.

To Create an Instance of Portal Server 7.1 on Node 1

This procedure creates an instance of Portal Server on port 7022 of the managed server on Node 1.

1. **Modify the `Webcontainer.properties` file in BEA WebLogic to change the values corresponding to the managed server `node1_7022`.**

2. **Create an instance of Portal Server.**

   PortalServer_base`/SUNWportal/bin/psadmin create-instance -u` *amadmin* `-f` *password* `-p` *portal1* `-w webcontainer.properties.BEAWL8`

3. **Restart the managed server named `node1_7022`.**

4. **Access the portal.**

   `http://`*node1.domain-name*`:7022/portal/dt`

   The Portal Welcome page appears.

To Create an Instance of Portal Server 7.1 on Node 2

This procedure creates an instance of Portal Server on port 7033 of the managed server on Node 2.

1. **Install Portal Server 7.1 and Access Manager SDK in the Configure Later mode using the installer.**

2. **Modify the `amsamplesilent` script with appropriate values. Ensure that `DEPLOY_LEVEL` is set as 4.**

   The `amsamplesilent` script is located in the *AccessManager_base*`/SUNWam/bin` directory.

3. **Run the `amsamplesilent` script.**

   AccessManager_base`/SUNWam/bin/amconfig -s amsamplesilent`.

4. **Copy the `example15.xml` file to a temporary directory and modify it with appropriate values.**

   The `example15.xml` file is located in the *PortalServer_base*`/SUNWportal/samples/psconfig` directory.

5. **Configure Portal Server using the `example15.xml` as the configuration XML file.**

   PortalServer_base`/SUNWportal/bin/psconfig --config example15.xml`

6. **Modify the `webcontainer.properties` file in BEA WebLogic to change the values corresponding to the managed server `node1_7033`.**

7 **Create a Portal Server instance.**

PortalServer_base/SUNWportal/bin/psadmin create-instance -u *amadmin* -f *password* -p *portal1* -w webcontainer.properties.BEAWL8

8 **Restart the managed server** node1_7033**.**

9 **Access the portal.**

http://*node1.domain-name***:7033/portal/dt**

The Portal Welcome page appears.

▼ To Configure a Cluster

This procedure configures a cluster for the three managed server that were created: node1_7011, node1_7022, and node2_7033.

1 **Log in to the administrator server.**

http://*node1.domain-name***:7001/console**

2 **Click Cluster and click Configure a New Cluster.**

3 **Enter a cluster name and cluster address.**

Enter the cluster name as new_cluster and enter the cluster address as *node1.domain-name*.

4 **Select Default Load Algorithm as** round robin**, and click Create.**

5 **Click the Server tab, and select** node1_7011**,** node1_7022 **and** node1_7033 **and drag them into the list box.**

6 **Stop and restart all of the servers.**

Each time you change the cluster configuration you must stop and restart all of the servers in the cluster.

7 **Select the Monitoring tab.**

After a successful configuration of cluster, the following is displayed.

```
Number of servers configured for this cluster: 2
Number of servers currently participating in this cluster: 2
```

▼ To Install Proxy Servlet for Load Balancing

This procedure creates a proxy server `.war` file for load balancing.

1 Telnet to Node 1.

2 Create files `web.xml` and `weblogic.xml` in the new `proxy/WEB-INF` directory.

```
mkdir -p proxy/WEB-INF
cd proxy/WEB-INF
```

3 Add the following contents to the `web.xml` file.

```
<!DOCTYPE web-app PUBLIC "-//Sun Microsystems, Inc.//DTD Web Application 2.3
//EN? "http://java.sun.com/dtd/web-app_2_3.dtd"><web-app>

<servlet>
        <servlet-name>HttpClusterServlet</servlet-name>
        <servlet-class>weblogic.servlet.proxy.HttpClusterServlet</servlet-class>
        <init-param>
                <param-name>WebLogicCluster</param-name>
                <param-value>HOST.DOMAIN:7011|HOST.DOMAIN:7022</param-value>
        </init-param>
</servlet>

<servlet-mapping>
        <servlet-name>HttpClusterServlet</servlet-name>
        <url-pattern>/</url-pattern>
</servlet-mapping>

<servlet-mapping>
        <servlet-name>HttpClusterServlet</servlet-name>
        <url-pattern>*.jsp</url-pattern>
</servlet-mapping>

<servlet-mapping>
        <servlet-name>HttpClusterServlet</servlet-name>
        <url-pattern>*.htm</url-pattern>
</servlet-mapping>

<servlet-mapping>
        <servlet-name>HttpClusterServlet</servlet-name>
        <url-pattern>*.html</url-pattern>
</servlet-mapping>

</web-app>
```

4 **Add the following contents to the** `weblogic.xml` **file.**

```
<!DOCTYPE weblogic-web-app PUBLIC "-//BEA Systems,
 Inc.//DTD Web Application 8.1//
EN" "http://www.bea.com/servers/wls810/dtd/weblogic810-web-jar.dtd">
<weblogic-web-app>
        <context-root>/</context-root>
</weblogic-web-app>
```

5 **Change directories to the** `proxy` **directory.**

6 **Run the following command:**

```
/usr/jdk/jdk1.5.0_01/bin/jar cvf proxy.war WEB-INF
```

7 **Access the administrator console.**

`http://`*node1.domain-name*`:7001/console`**

8 **Click Server > Configure a New Server.**

9 **Enter the new server name as proxy and the listen port as 55555, and click Apply.**

10 **Click Deployment in the left pane, click Web Applications Module, and click Deploy New.**

11 **Select** `proxy.war` **from the** `node1.domain` **and deploy it on the independent server named** `proxy`**.**

▼ To Deploy `.war` Files on the Cluster

This procedure deploys all `.war` files on the cluster. Redeployment of all the `.war` files needs to be done on the cluster.

1 **Log in to administrator server.**

2 **Click Web Application Modules.**

3 **For each Portal Web Application module, click the Target tab, select All Servers in the Cluster option, and click Apply.**

4 **Click Services > JDBC > Connection Pools.**

5 **For each connection pool related to Portal Server, click the Target tab, select All Servers in the Cluster option, and click Apply.**

6 **Click Services > JDBC > Data Source.**

7 **For each data source related to Portal Server, click the Target tab, select All Servers in the Cluster option, and click Apply.**

8 **Restart all servers.**

▼ To Install Gateway on the Gateway Host

1 **Install Gateway on Node 3.**

2 **Enter the load balancer URL, `http://`*node1/domain-name*`:55555/portal`, as the portal URL while installing gateway.**

3 **Log in to gateway and access `developer/developer`.**

If the proxy is working, the URL changes to the following:
`https://`*GWhost*`:443/http://`*node1.domain-name*`:55555/portal/dt`

Setting Up Portlet Session Failover on BEA WebLogic 8.1 Service Pack 5

In this scenario, more than two Portal Server instances are clustered. The user accesses a portlet from a Portal Server instance. The user can set session variables in the portlet. In case of a failover of a Portal Server instance that the user accesses, the user automatically gets directed to the other Portal Server instance, and the session variables are retained.

This section explains about setting up a portlet session failover on BEA WebLogic 8.1 Service Pack 5.

▼ To Set up Portlet Session Failover on BEA WebLogic 8.1 Service Pack 5

Before You Begin Two or more portal instances should already be clustered. To cluster Portal Server instances, refer to "Clustering in Portal Server 7.1 on BEA WebLogic 8.1 Service Pack 4 and Service Pack 5" on page 169.

1 **Undeploy the `portal.war` from the managed servers using the WebLogic administrator console.**

2 **Add the following into the `weblogic.xml` file of `portal.war`:**

```
<session-descriptor>
<session-param>
```

```
<param-name>PersistentStoreType</param-name>
<param-value>replicated</param-value>
</session-param>
</session-descriptor>
```

Both `portal.war` and the `portlet` which is used for session failover should have the `session-descriptor` set in the `weblogic.xml` file.

After the modification, the content of the `weblogic.xml` file of `portal.war` is as follows:

```
<!DOCTYPE weblogic-web-app PUBLIC "-//BEA Systems, Inc.//DTD Web Application 8.1
//EN" "http://www.bea.com/servers/wls810/dtd/weblogic810-web-jar.dtd">
<weblogic-web-app>
<reference-descriptor>
<resource-description>
<res-ref-name>jdbc/communitymc</res-ref-name>
<jndi-name>jdbc/communitymc</jndi-name>
</resource-description>
</reference-descriptor>
<session-descriptor>
<session-param>
<param-name>PersistentStoreType</param-name>
<param-value>replicated</param-value>
</session-param>
</session-descriptor>
<virtual-directory-mapping>
<local-path>/opt/SUNWam/public_html</local-path>
<url-pattern>/online_help/*</url-pattern>
</virtual-directory-mapping>
</weblogic-web-app>
```

3 **Deploy the `portal.war` onto the Portal Server instance using the BEA WebLogic administrator console.**

4 **Add the same `session-descriptor` into the `weblogic.xml` file of the portlet to be used for session failover.**

Note – If the `weblogic.xml` file does not exist, create it under `WEB-INF`.

---

5 **Deploy the portlet through the `psconsole` and add the portlet to the desktop.**

6 **Set session variables in the portlet and bring down the Portal Server instance which it uses to access the desktop.**

The session variables will be retained after you start accessing another Portal Server instance.

Replacing Java DB With Oracle Database

Java DB is used as a default database for Portal Server. This section explains how to replace Java DB with the Oracle database. Using this, you can ensure high availability and scalability. This procedure is divided into the following tasks:

1. Setting Up General Requirements
2. Preparing Oracle

▼ To Prepare the Database

1 Prepare the Database.

a. Install RDBMS or identify the RDBMS that already exists on the system.

b. Create a database instance (tablespace in case of Oracle) to be used for collaboration.

c. Create the database user account or accounts.

2 Establish appropriate privileges for the user accounts.

a. Locate the JDBC driver.

b. Add JDBC driver to the web container's JVM classpath.

c. Add JVM option:

```
-Djdbc.drivers=<JDBC_DRIVER_CLASS>
```

3 Configure Community Membership and Configuration.

a. Configure communitymc database configuration file by running the following scripts:

portal-data-dir`/portals/`*portal-id*`/config/portal.dbadmin`

b. Remove the Java DB specific property in the `communitymc.properties` file.

portal-data-dir`/portals/`*portal-id*`/config/communitymc.properties`

4 Load the schema onto the database.

5 Edit the `jdbc/communitymc` JDBC resource to point to the new database.

Note – On some of the web containers, you might need to edit the corresponding JDBC connection pool instead of the JDBC resource.

6 Configure and install portlet applications.

a. Locate the portlet applications.

portal-data-dir/portals/*portal-id*/portletapps

b. Configure portlet applications to use the new database by editing `tokens_xxx.properties`**.**

c. Using the administration console or command-line tool provided by the web container, create a JDBC resource for the application using the values from the `tokens_xxx.properties`**.**

Resource JNDI Name	`jdbc/DB_JNDI_NAME`
Resource Type	`javax.sql.DataSource`
Datasource Classname	`DB_DATASOURCEA`
User	`DB_USERU`
Password	`DB_PASSWORDS`
URL	`DB_URL`

Note – Some of the web containers might require you to set up a connection pool prior to setting up the JDBC resource.

d. Undeploy existing portlets that use the Java DB Database as a datastore.

e. Deploy the newly configured portlet applications.

▼ To Prepare the Oracle Database

1 Prepare Oracle.

a. Install Oracle 10g Release 2.

b. Create a database instance named `portal` **(the SID is** `portal`**).**

c. Log in to Oracle Enterprise Manager (`http://`*hostname*`:5500/em`) as SYSTEM.

d. Create a tablespace `communitymc_`*portal-id* **for example,** `communitymc_portal1`**.**

Note – For Wiki, FileSharing, and Surveys portlets, the tablespace and user accounts are created during the deployment of the Oracle configured portlet.

---

e. Create a user account with the following information:

Username:	`portal`
Password:	`portal`
Default Tablespace	`communitymc_portal-id`
Assign roles	`CONNECT` and `RESOURCE`

2 Prepare the web container for the New Database

a. Locate the Oracle JDBC driver `ojdbc14.jar`**.**

```
$ORACLE_HOME/jdbc/lib/ojdbc14.jar
```

Alternatively, you can download the JDBC driver from the Oracle web site. Ensure that you download the version that is compatible with the Oracle RDBMS you use.

b. Using the administration console or the CLI, add the JDBC driver `ojdbc14.jar` **to the JVM classpath by adding the following JVM option:**

```
-Djdbc.drivers=oracle.jdbc.OracleDriver
```

- *For Web Server 7.0:*
  a. Log in to Web Server 7 administrator console.
  b. Click the Configuration tab and select the respective configuration.
  c. Click the java tab and add the location of the ojdbc14.jar to the classpath suffix.
  d. Click the JVM Settings tab.
  e. Replace any existing `-Djdbc.drivers` entry as below:

     ```
     -Djdbc.drivers=oracle.jdbc.OracleDriver
     ```

  f. If the `-Djdbc.drivers` entry does not exit, add the following:

     ```
     -Djdbc.drivers=oracle.jdbc.OracleDriver
     ```

  g. Click Save.
  h. Click Deploy Pending and deploy the changes.
- *For Application Server 8.2*
  a. Log in to Application Server administrator console.
  b. Click Configurations > server-config (Admin Config) > JVM Settings > Path Settings > Path Settings.

c. Add the location of the ojdbc14.jar to the classpath suffix.

d. Click the JVM Settings tab.

e. Replace any existing `-Djdbc.drivers` entry as below:

```
-Djdbc.drivers=oracle.jdbc.OracleDriver
```

f. If the `-Djdbc.drivers` entry does not exit, add the following:

```
-Djdbc.drivers=oracle.jdbc.OracleDriver
```

g. Click Save.

3 Configure Community Membership and Configuration.

a. Edit the `communitymc` file database configuration file.

```
% vi portal-data-dir/portals/portal-id/config/portal.dbadmin
db.driver=oracle.jdbc.OracleDriver
db.driver.classpath=JDBC-driver-path/ojdbc14.jar
url=jdbc:oracle:thin:@oracle-host:oracle-port:portal
```

b. Remove or comment out the following property from the `communitymc` configuration file.

```
% vi portal-data-dir/portals/portal-id/config/communitymc.properties
#javax.jdo.option.Mapping=derby
```

c. Load community schema onto the Oracle database.

```
% cd portal-data-dir/portals/portal-id/config
% ant -Dportal.id=portal-id -f config.xml configure
```

d. Edit the JDBC and `communitymc` JDBC resource to point to Oracle.

- *For Web Server 7.0*

  a. Log in to the Web Server administration console.

  b. Click the Configuration tab and select the respective configuration.

  c. Click the java tab > Resources and add a new JDBC resource.

  d. Click `jdbc/communitymc` and edit the Datasource Class Name.

  e. Set the `Datasource classname` to `oracle.jdbc.pool.OracleDataSource`

  f. Set the following properties: user: `portal` and password: `portal`.

  g. Delete the following derby properties: Database Name, Port Number, and Server Name.

  h. Add the following property: url: `jdbc:oracle:thin:@oracle-host:oracle-port:portal`

  i. Click Save.

  j. Click Deploy Pending and deploy the changes.

- *For Application Server*
  a. Log in to the Application Server administration console.
  b. Click Resources > JDBC > Connection Pools > communitymcPool
  c. Set the `Datasource classname` to `oracle.jdbc.pool.OracleDataSource`
  d. Set the following properties: user: `portal` and password: `portal`.
  e. Delete the following derby properties: Database Name, Port Number, and Server Name.
  f. Add the following property: url: `jdbc:oracle:thin:@oracle-host:oracle-port:portal`
  g. Click Save.

4 Configure and install Portlet applications.

a. Run the `filesharing` script.

portal-data-dir`/portals/`*portal-id*`/portletapps/filesharing`

b. Configure `tokens_ora.properties` to load information when initially loading the schema.

`DB_ADMIN_DRIVER_CLASSPATH`	`$ORACLE_HOME/jdbc/lib/ojdbc14.jar`
DB_JNDI_NAME	OracleFileSharingDB
`DB_ADMIN_URL`	`jdbc:oracle:thin:@<ORACLE_HOST>:<ORACLE_PORT>:portal`
`DB_ADMIN_USER`	`<ORACLE_SYSTEM_USER>`
`DB_ADMIN_PASSWORD`	`<ORACLE_SYSTEM_PASSWORD>`
`DB_URL`	`jdbc:oracle:thin:@<ORACLE_HOST>:<ORACLE_PORT>:portal`
`DB_USER`	`portalfs`
`DB_PASSWORD`	`portalfs`
`DB_DRIVER_JAR`	`$ORACLE_HOME/jdbc/lib/ojdbc14.jar`
`DB_TABLESPACE_NAME`	`Filesharingdb_<PORTAL_ID>`
`DB_TABLESPACE_DATAFILE`	`filesharingdb_<PORTAL_ID>`
`DB_TABLESPACE_INIT_SIZE`	100M

c. Using the administration console or the command-line tool provided by the web container, create the JDBC resource using the values from the `tokens_ora.properties`.

- *For Web Server 7.0:*

a. Create a JDBC Resource with the following properties:

Resource JNDI Name	`jdbc/OracleFilesharingDB` This value must match `DB_JNDI_NAME` in `tokens_ora.properties`.
Datasource Class Name	`oracle.jdbc.pool.OracleDataSource` This value must match `DB_DATASOURCE` in `tokens_ora.properties`.
User	`portalfs` This value must match `DB_USER` in `tokens_ora.properties`.
Password	`portalfs` This value must match `DB_PASSWORD` in `tokens_ora.properties`.
URL	`jdbc:oracle:thin:@<ORACLE_HOST>:<ORACLE_PORT>:portal` This value must match `DB_URL` in `tokens_ora.properties`.

- *For Application Server:*

a. Create a new connection pool with the following properties:

Name	`OracleFilesharingDBPool` This value must match `DB_JNDI_NAME` in `tokens_ora.properties`.
Resource Type	`javax.sql.DataSource`
Datasource Class Name	`oracle.jdbc.pool.OracleDataSource` This value must match `DB_DATASOURCE` in `tokens_ora.properties`.

b. In the Properties list, delete all the default properties and add the following:

User	`portalfs` This value must match `DB_USER` in `tokens_ora.properties`.
Password	`portalfs` This value must match `DB_PASSWORD` in `tokens_ora.properties`.

URL `jdbc:oracle:thin:@<ORACLE_ HOST>:<ORACLE_PORT>:portal`

This value must match `DB_URL` in `tokens_ora.properties`.

c. Create a JDBC resource with the following value:

Resource JNDI Name `jdbc/OracleFilesharingDB`

This value must match `DB_JNDI_NAME` in `tokens_ora.properties`.

Connection Pool `OracleFilesharingDBPool`

This value must match the pool that is created in the previous step.

d. Add the available target to the Selected list. Click OK.

d. Undeploy existing portlets that use Java DB Database as a datastore.

```
/opt/SUNWportal/bin/psadmin undeploy-portlet -u \
uid=amadmin,ou=people,dc=acme,dc=com -f password-file \
-p portal-id -i portal-instance-id
```

e. Deploy the newly configured file sharing portlet.

```
cd portal-data-dir/portals/portal-id/portletapps/filesharing
ant -Dapp.version=ora
```

This `ant` command performs several tasks including regenerating the war image, loading up the schema onto the database, and deploying the newly built portlet. If the `ant` command fails and you want to unload schema, use the following command:

```
ant -Dapp.version=ora unconfig_backend
```

Note – During deployment provide the Access Manager administrator password.

If the `ant -Dapp.version=ora` command fails with the following error, "Error: Password file does not exist or is not readable," run `ant deploy` from command line to deploy the portlet.

---

f. Repeat this procedure for the other portlet applications, such as Surveys and Wiki.

◆ ◆ ◆ CHAPTER 9

Configuring the Communication Channels

This chapter provides information on the communication channels for Sun Java System Portal Server, starting with general descriptive information, moving to an explanation of the state of the communication channels after installation but before configuration, and finally leading into a description of various steps for configuring the communication channels according to a site's needs.

The information provided on configuration makes up the bulk of this chapter and includes administrator and end-user configuration. End users can edit the configuration of each channel directly from the Portal Desktop by clicking the edit button accessible in each channel. This gives end users access to an edit page (or edit pages) that allows editing of specific server configuration information and that allows editing of specific features, such as the number of address book entries visible in the Address Book channel, visible to the end user in the channel.

Administrators can limit or extend end users' editing options. Administrators can pre-configure channels to work without the need for end-user server configuration. For more information, see "Administrator Proxy Authentication: Eliminating End-User Credential Configuration" on page 210.

Since administrators can design the edit page for each channel, they can select which specific features end users can edit. For more information, see "Application Preference Editing: Configuring Communication Channel Edit Pages" on page 205.

If a site has more than one instance of a particular application available, administrators can allow end users to configure a second channel on their Portal Desktops. An example of this would be two or more instances of a mail application. For more information, see "Enabling End Users to Set Up Multiple Instances of a Communication Channel Type" on page 209.

This chapter includes the following sections:

Overview of the Communication Channels

The Sun Java System Portal Server product offers four communication channels that are accessible by end users directly in Portal Desktop. These channels allow end users access to corresponding applications, such as a mail application, to enable end users to organize, schedule, and communicate more effectively and efficiently.

The four communication channels are:

Address Book Channel	The Address Book channel displays address book entries for end users to view. To access the address book in order to create and edit address book entries, first click Launch Address Book.
Calendar Channel	The Calendar channel displays calendar events and tasks for end users to view. To access the calendar application in order to create new tasks and events, first click Launch Calendar.
Instant Messaging Channel	The Instant Messaging Channel displays the presence status of other users with access to Sun Java™ System Instant Messenger. These contacts are from a list end users have created within the Instant Messenger application. Initiate a chat from the channel by clicking a presence status icon, which is one method of invoking Instant Messenger. To get presence updates directly from the channel, reload Portal Desktop. To receive presence updates as they occur, view contacts' presence status from Instant Messenger by invoking the application; therefore, click Instant Messenger.
Mail Channel	The Mail channel displays mail messages sent to end users for them to view. To access the mail application in order to read and compose messages, click Launch Mail.

Supported Software for the Communication Channels

The Sun Java System Portal Server software supports the following resource server platforms for the Communication Channels:

- Sun Java System Messaging Server 5.2, 6.0, 6 2006Q4
- Sun Java System Calendar Server 5.1.1, 6.0, 6 2006Q4
- Sun Java System Instant Messaging Server 6.1, 6 2006Q2
- IBM Lotus Notes 5.0.6
- Microsoft Exchange Server 2000

The Installer and the Communication Channels

The Sun Java System Portal Server installer performs several tasks involving the communication channels. General communication channel configuration tasks are also handled by the installer. More detailed configuration is then required by administrators and end users depending up the needs of the site and of the individuals.

Sun Java System Portal Server Installer Tasks

The Sun Java System Portal Server Installer:

- Installs the following packages, `SUNWpsso`, `SUNWpsap`, `SUNWpsmp` , `SUNWpscp`, and `SUNWiimps` which are deployed to the default Sun Java System Portal Server instance. Therefore, the installer does not install the communication channels on all of the Sun Java System Portal Server instances. For information on multi-server deployments, see "Multiple Instance Deployments" on page 191.
- Creates the channels, Address Book, Calendar, Instant Messaging, and Mail. The installer places channels for Sun Java System servers into the My Front Page Tab panel container for the sample organization. Therefore, the communication channels are installed only when the sample portal is installed. Microsoft Exchange Server and IBM Lotus Notes server are not automatically placed in a container. An administrator would need to add these channels to a container, if desired.

  The default configurations for the Calendar and Mail channels work after only basic configuration by end users; therefore, they do not require further configuration by administrators. The Address Book and Instant Messaging channels require further configuration by both administrators and end users.
- Creates and configures the single sign-on (SSO) Adapter service which enables single sign-on with the Sun Java System Calendar Server and Sun Java System Messaging Server.

Multiple Instance Deployments

If your Sun Java System Portal Server deployment involves multiple instances, you must manually deploy the communication channels to each additional instance of Sun Java System Portal Server and restart each instance. To deploy, type:

portal-server-base`/SUNWportal/bin/deploy redeploy --instance` *instance-name* `--deploy_admin_password` *deploy-admin-password*

where:

instance-name is the name for that particular non-default instance

deploy-admin-password is the administrator password for the web container. The web container administrator password is required only when the web container is Sun Java System Application Server or BEA WebLogic Server. If you include the password when using Sun Java System Web Server or IBM WebSphere Application Server, the password is ignored.

"Multiple Instance Deployments" on page 191 lists the commands for manually deploying communication channels to two non-default Sun Java System Portal Server instances and for restarting those instances, where `myinstance1` and `myinstance2` are non-default Sun Java System Portal Server instance names and `Admin` is the web container's administrator password.

EXAMPLE 9–1 Deploying Communication Channels to a Non-Default Instance

```
portalServer-base/SUNWportal/bin/deploy redeploy --instance myinstance1
-deploy_admin_password Admin
portalServer-base/SUNWportal/bin/deploy redeploy -instance myinstance2
--deploy_admin_password Admin
```

Configuration Tasks for the Communication Channels

The following are the high-level tasks involved in setting up the communication channels. Not all tasks are applicable to all sites. You must determine whether your site's business requirements make the task necessary.

- "Enabling Access to Mail and Calendar Applications" on page 193
- "Configuring the Services for the Default Organization" on page 194
- "Configuring the Address Book Service Defaults" on page 202
- "Application Preference Editing: Configuring Communication Channel Edit Pages" on page 205
- "Enabling End Users to Set Up Multiple Instances of a Communication Channel Type" on page 209
- "Administrator Proxy Authentication: Eliminating End-User Credential Configuration" on page 210
- "Configuring a Read-Only Communication Channel for the Authentication-Less Portal Desktop" on page 214
- "Configuring Microsoft Exchange Server or IBM Lotus Notes" on page 218
- "Configuring the Mail Provider to Work with an HTTPS Enabled Sun Java System Messaging Server" on page 237

If you already have Sun Java System Messaging Server and Sun Java System Calendar Server installed either on the same server or on different servers, specify the respective URL when you create a channel.

Enabling Access to Mail and Calendar Applications

Both Messaging Server and Calendar Server verify the Internet Protocol (IP) address of the host where the browser requests a login session ID. If the IP address differs from the host IP address where the session ID is issued, Messaging Server and Calendar Server reject the session with a session timeout message.

You must change the value of the parameter that enables and disables an IP security check to allow the user to access mail through Portal Server. The parameter that specifies whether to restrict session access to the login IP address, is:

`service.http.ipsecurity`

▼ To Disable `ipsecurity` for Messaging Server

To disable `ipsecurity` for Messaging Server, perform the following steps in the command line on the machine running the mail server.

1. **Log in to the Messaging Server.**
2. **Type the following command:**

   MessagingServer-base `/sbin/server5/msg-`*messaging-server-hostname* `/configutil -o service.http.ipsecurity -v no`
3. **Change to root using the `su` command.**
4. **Stop Messaging Server using this command**

   MessagingServer-base `/sbin/server5/msg-`*messaging-server-hostname* `/stop-msg`
5. **Start Messaging Server using this command:**

   MessagingServer-base `/sbin/server5/`*msg-messaging-server-hostname* `/start-msg`

▼ To Disable `ipsecurity` for Calendar Server

To disable `ipsecurity` for Calendar Server, perform the following steps in the command line on the machine running the Calendar Server:

1. **Log in to the Calendar Server.**
2. **Assuming calendar server is installed in `/opt/SUNWics5`, type the following:**

   `cd /opt/SUNWics5/cal/config/`

3 **Edit the `ics.conf` file and set `ipsecurity` to `no`. For example:**

```
service.http.ipsecurity = "no"
```

4 **Assuming calendar server is installed in `/opt/SUNWics5`, restart Calendar Server by typing:**

```
/opt/SUNWics5/cal/sbin/stop-cal
```

```
/opt/SUNWics5/cal/sbin/start-cal
```

Refresh or re-authenticate to the Portal Desktop, and verify that the "Launch Calendar" link works.

Configuring the Services for the Default Organization

After the communication channels have been installed, the Instant Messaging and Address Book channels require more detailed configuration as explained subsequently. The Calendar and Mail channels have sample or default settings that can work without further configuration by an administrator.

If site-specific issues exist for any of the communication channels, including the Calendar and Mail channels, configuration by an administrator might be necessary before the channels work according to the needs of your site.

The following sections provide important information relating to the configuration of the communication channels.

- "Configuring the Address Book Channel" on page 202

End-User Configuration

Unless you configure the communication channels with proxy authentication, end users must go to each channel's edit page by clicking the edit button in the respective communication channel to further configure the channel. For more information, see "Administrator Proxy Authentication: Eliminating End-User Credential Configuration" on page 210 .

CAUTION—Undetected Error: Missing Launch Link

If a client port number is entered incorrectly for any of the communication channels, end users do not receive an error message. The error manifests itself by not displaying the launch link for the respective channel, a result that does not help end users to identify the root cause of the problem.

Both administrators and end users can enter an incorrect client port number, but since end users can edit only the client port number for the Calendar and Mail channels, those are the only channels where this problem can occur.

CAUTION—Undetected Error: Missing Channel

Various situations can cause end users *not* to see a communication channel and *not* to see an error message explaining the problem. The cause might be a misconfigured template or configuration name, which doesn't allow the template or configuration to be found. A communication channel does not display when any of the following conditions is true:

- The SSOAdapter template is not found.
- The SSO Adapter configuration is not found.
- The `display.template` file is not found.

HTTPS Enabled

This applies to the Mail Channel only. If the Mail channel is connected to a more secure HTTP-enabled messaging server instead of the basic HTTP-enabled messaging server, you need to make some security-related adjustments for the Mail channel to work as intended. For more information, see "Configuring the Mail Provider to Work with an HTTPS Enabled Sun Java System Messaging Server" on page 237.

Configuring the Instant Messaging Channel

Sun Java System Instant Messengeris installed during the installation of Sun Java System Portal Server if the Enable IM in Sun Java System Portal Server option is selected.

While the Instant Messaging Portal channel is designed to work right out of the box, other configuration might be necessary depending upon your site's needs. Therefore, after following the steps in "Instant Messaging Channel" on page 196 see "Additional Configuration for the Instant Messaging Channel" on page 198 to determine if any of that section's subsections apply to your installation.

The Instant Messaging channel is based on a Sun Java System Portal Server content provider called `IMProvider`. The `IMProvider` is an extension of the `JSPProvider` in the Portal Server. As an extension of the `JSPProvider`, `IMProvider` uses the JSP files to generate the content page and the edit page for the Instant Messaging channel. The JSP files are also used to generate the pages used to launch the Instant Messenger. The `IMProvider` also defines an instant messaging-specific tag library and this tag library is used by the JSP files. The JSP files and the tag library use the channel properties that are defined by the `IMProvider`.

For more information on Sun Java SystemInstant Messenger, see *Instant Messaging Administrator's Guide*.

Administrators and end users can access information about Sun Java System Instant Messengerby visiting the URL used in the `codebase` property for the Instant Messaging Channel configuration.

Instant Messaging Channel

▼ To Configure the Instant Messaging Channel

1. **From an Internet browser, log into the Sun Java System Portal Server administration console at** `http://`*hostname:port* `/psconsole`**, for example** `http://psserver.company22.example.com:80/psconsole`

2. **Click the Identity Management tab to display the View drop down list in the navigation pane (the lower left frame).**

3. **Select Services in the View drop down list to display the list of configurable services.**

4. **Under the Sun Java System Portal Server Configuration heading, click the arrow next to Portal Desktop to bring up the Portal Desktop page in the data pane (the lower right frame).**

5. **Click the Manage Channels and Containers.**

6. **Scroll down to the Channels heading and click Edit Properties next to IMChannel to display the Instant Messenger service panel, which includes Basic Properties.**

   The following is a partial list of the properties displayed in the Edit IMChannel page with example values provided for each property.

Property	Example Value
`authMethod`	`idsvr`
`authUsernameAttr`	`uid`
`clientRunMode`	`plugin`
`codebase`	`imapplet.example.com`
`contactGroup`	`My Contacts`
`mux`	`imserver.example.com`
`muxport`	`49909`

Property	Example Value
netletRule	IM
password	(not applicable when idsvr is used for authmethod)
port	49999
server	imserver.example.com
username	(not applicable when idsvr is used for authmethod)

7 In the text field next to each property you want to input, enter the desired value. The following describes the properties and the type of information to enter as a value.

Property	Value
authMenthod	Two values are possible, idsvr or ldap. The idsvr value enables Single Sign-On to work. It also removes the username and password fields from the Instant Messenger channel edit page The value idsvr is usually preferable, to indicate that the authentication method to be used is the Sun Java System Portal Server authentication method.
authUsernameAttr	Enter the name of the attribute to use for the user name when authenticating using the idsvr authentication method.
clientRunMode	Enter the method for running the Instant Messaging client: plugin or jnlp (used for Java Web Start).
codebase	Enter the URL prefix from which the Instant messaging client is downloaded.
contactGroup	Enter the name of the contact group that is displayed in the Instant Messaging channel.
mux	Enter the hostname of the Sun Java System Instant Messaging Multiplexor to be used when the channel launches the Instant Messaging client.
muxport	Enter the port number associated with the Sun Java System Instant Messaging Multiplexor. The default port number is 49909.
netletRule	Enter the name of the netlet rule that is used with the Instant Messaging client when using the Secure Remote Access (SRA) gateway.

Property	Value
password	Enter the password to use when authenticating using the LDAP method. When stored in the display profile, this property is obfuscated using the `AMPasswordUtil` class.
port	Enter the port number associated with the Sun Java System Instant Messaging Server to be used by the channel. The default port number is 49999.
server	Enter the hostname of the Sun Java System Instant Messaging Server to be used by the channel.
username	Enter the username to use when authenticating using the LDAP method.

8 Scroll as needed and click Save.

Additional Configuration for the Instant Messaging Channel

The following sections provide information for additional configuration of the Instant Messaging Channel.

Allowing Multiple Organizations

When a Sun Java System Portal Server instance serves multiple organizations but uses a single server additional steps must be taken.

Portal Server and Sun Java System Portal Server allow administrators to set up users with the same User ID (`uid`) across an organization. For example, an organization could have two suborganizations that each have an end user named `enduser22`. This creates a conflict when these two end users attempt to access their respective accounts through the channel.

To avoid this potential conflict, one set of JSP launch pages per organization must be created to contain a pass-in-the-parameter domain set to the value of the organization's attribute `sunPreferredDomain`. The default launch pages are:

```
/etc/opt/SUNWportal/desktop/default/IMProvider/jnlpLaunch.jsp
```

```
/etc/opt/SUNWportal/desktop/default/IMProvider/pluginLaunch.jsp
```

Inserting Instant Messenger Links in an Organization

By default Instant Messenger links are added to the Application channel, which provides the links to launch various applications, in the default organization. The Instant Messenger links allows end users to launch the Instant Messenger from the Application channel. You need to add Instant Messenger links manually if:

- You want to add these links for another organization.
- You do not have the sample portal installed.
- You are using the `AppProvider` for another channel.

The contents for the Instant Messenger links are in the file *PortalServer-base* `/SUNWportal/samples/InstantMessaging/dp-IMChannel.xml`. The `dp-IMChannel.xml` file also contains the sample `IMChannel` .

Edit a copy of the file `dp-IMChannel.xml` to add the Instant Messenger links information to the display profile for another organization and install the file using the `psadmin` command as follows:

▼ Inserting Instant Messenger Links

1 Change to the following directory:

PortalServer-base `/SUNWportal/bin/`

2 Create a copy of the `dp-IMChannel.xml` file as follows:.

```
cp dp-IMChannel.xml newfile.xml
```

3 To modify the Application channel, type the following `psadmin` command:

```
psadmin modify -u
                    ADMIN_DN -w
                    PASSPHRASE -d
                    ORG_DN -m newfile.xml
```

where:

ADMIN_DN - Replace with LDAP administrator DN. For example: `psadmin`

PASSPHRASE - Replace with the administrator's password.

ORG_DN - Replace with the DN of the Organization where the links are to be added. For example: `o=example.com, o=isp`

The URL for launching the Instant Messenger using Java Plug-in is a reference to the Instant Messaging channel with a launch argument. For example:

```
/portal/dt?action=content&provider=IMChannel&launch=plugin&username=sam
```

The URL for launching the Instant Messenger applet with Java Web Start is:

```
/portal/imlaunch?channel=IMChannel&launch=jnlp&username=sam
```

Enabling Secure Mode in Sun Java Server Portal Server

Netlet facilitates secure communication between the Instant Messenger and the server.

Note – The Instant Messaging channel automatically uses the secured mode when accessed through the Secure Remote Access gateway. The Instant Messaging channel does not use the secured mode when it is not accessed through the gateway.

To enable the secure mode, you need to add the Netlet Rule.

To add the Netlet Rule:

▼ Adding the Netlet Rule

1. **From an Internet browser, log into the Portal Server administration console at** `http://`*hostname:port* `/psconsole`**, for example** `http://psserver.company22.example.com:80/psconsole`
2. **Click the Identity Management tab to display the View drop down list in the navigation pane.**
3. **Select Services in the View drop down list to display the list of configurable services.**
4. **Scroll down to SRA Configuration and select Netlet.**
5. **Click the arrow icon beside Netlet. The Netlet Rules are displayed in the right panel.**
6. **Click Add under Netlet Rules.**
7. **Type `IM` in the Rule Name field.**

   Note – The Netlet rule name can be different. You can configure the Instant Messaging channel to use a different Netlet rule.

8. **Remove the default value in the URL field and leave the field blank.**
9. **Select the Download Applet check box and enter the following string:**

   $IM_DOWNLOAD_PORT:$IM_HOST:$IM_PORT

   For example:

   49916:company22.example.com:80

   where:

   IM_DOWNLOAD_PORT. The port on which Instant Messaging resources are downloaded using Netlet.

IM_HOST. The host name of the web container serving Instant Messenger. For example: company22.example.com

IM_PORT. The port number of the web container serving the Instant Messenger. For example, 80.

10 **Select the default value in the Port-Host-Port List and click Remove.**

11 **In the Client Port field, Enter the local host port on which Netlet runs. For example:** `49916`**.**

12 **Enter the Instant Messaging Multiplexor host name in the Target Host(s) field.**

13 **Enter the Instant Messaging Multiplexor port in the Target Port(s) field.**

Note – The values for Netlet Port, Instant Messaging Host, and Instant Messaging Port should be the same as the Instant Messaging service attributes mentioned in the Instant Messenger service panel as discussed in the final steps of "Instant Messaging Channel" on page 196.

---

14 **Click Add to List.**

15 **Click Save to save the Netlet Rule.**

Disallowing Users from Launching Instant Messenger

You can remove the ability for users to use the Instant Messaging channel by removing the channel from the user\qs display profile. For example, to remove the sample IMChannel that is automatically installed, do the following:

▼ Disallowing Users from Launching Instant Messenger

1 **From an Internet browser, log into the Portal Server administration console at** `http://`*hostname:port* `/psconsole`**, for example** `http://psserver.company22.example.com:80/psconsole`

2 **Click the Identity Management tab to display the View drop down list in the navigation pane.**

3 **Select Services in the View drop down list to display the list of configurable services.**

4 **Click the arrow icon next to the Portal Desktop service.**

5 **Click the Manage Channels and Containers Link.**

6 **Select the check box to the left of the IMChannel channel.**

7 Scroll as needed and click Delete to delete the channel.

Configuring the Address Book Channel

For the Address Book channel to work, you need to configure the defaults for the Address Book service. Because the AddressBookProvider is not pre-configured, channels the user creates based on the AddressBookProvider do not appear on the user's Desktop or on the Content link unless the AddressBookProvider has been configured.

Note – Creating channels based on the other communications channels in the pre-populated, user-defined channels set may result in the created channel displaying the message: `Please specify a valid configuration`. Although the other Communication Channels are defined to a sufficient extent to appear on the user's Desktop, they require additional administrative tasks to ascertain which backend service to use.

Additionally, the communication channels require the desktop user to specify back-end credentials (such as username and password) after the administrative tasks are completed. The desktop user can specify these values in the channel by using the channel's Edit button.

Note – The `userDefinedChannels` set might need to be administered on a per-installation basis, because this set includes references to back-end services that might not apply to your particular setup. For example, all Lotus Providers in this set refer to interaction with Lotus back-end services for the communication channels. These do not apply if no one in the Portal Server user base uses Lotus backend services.

Configuring the Address Book Service Defaults

This section provides information about single sign-on (SSO) Adapter templates. These templates globally affect the display of the communication channels on users' portal Desktops. To alter the display profile of users for the communication channels, you need to edit or create SSO Adapter templates and configurations.

▼ To Configure the Address Book Service Defaults

1 From an Internet browser, log into the Portal Server administration console at `http://`*hostname:port* `/psconsole`**, for example** `http://psserver.company22.example.com:80/psconsole`

2 Click the Service Configuration tab to display the list of configurable services in the navigation pane.

3. **Scroll down the navigation pane to the Single Sign-on Adapter Configuration heading and click the arrow next to the item SSO Adapter, which brings up the SSO Adapter page in the data pane.**

4. **Click New under SSO Adapter Configuration to add an SSO adapter configuration.**
   The New Configuration page appears.

5. **Type a configuration name and select SUN-ONE-ADDRESS-BOOK from the menu.**

6. **Click Next.**
   The Configuration Properties page appears.

7. **Modify the properties as needed.**

8. **Scroll down the SSO Adapter page and click Save.**

9. **When done, click Save.**

Configuring End-User Channel Settings

▼ To Configure End-User Channel Settings

1. **Log into the Desktop as the new user:**

   a. **From an Internet browser, go to:**

      `http://` *hostname*`.domain:port/portal/dt, for example`
      `http://psserver.company22.example.com:80/portal/dt`

   b. **Enter the user ID and password.**

   c. **Click Login.**

2. **Click the Edit button of each channel to configure the server settings.**

   - To configure the Mail channel settings:

     Server Name. Enter the host name of the mail server. For example, `mailserver.example.com`.

     IMAP Server Port. Enter the mail server port number.

     SMTP Server Name. Enter the name of the Domain Name Server (DNS) of the outgoing mail—Simple Mail Transfer Protocol (SMTP)— server.

     Client Port. Enter the port number configured for HTTP service.

     User Name. Enter the mail server user name.

User Password. Enter the mail server user password.

When sending a message place a *copy in Sent Folder.* Check this box to store copies of your outgoing messages in the Sent folder.

Finished. Click this button to save the mail configuration.

Cancel. Click this button to close the window without saving the configuration details.

- To configure Address Book channel settings:

  The IMAP user ID and Password are the same as the User Name and User Password entered when configuring the mail channel settings. For details, refer to the previous bulleted item,"Configuring the Address Book Service Defaults" on page 202

  User Name. Enter your User Name.

  Password. Enter you Password.

  Finished. Click this button to save the server information.

  Cancel. Click this button to close the window without saving the details.

- To configure the Calendar channel settings:

  Server Name. Enter the calendar server host name. For example, `Calserver.example.com`.

  Server Port. Enter the calendar server port number.

  User Name. Enter the calendar server user name.

  User Password. Enter the calendar server user password.

  Finished. Click this button to save the calendar configuration.

  Cancel. Click this button to close the window without saving the details.

- To configure the Instant Messaging channel settings:

  Contact List. Select the desired contact list whose contacts will be displayed in the Instant Messaging Channel.

  Launch Method. Select the desired launch method: `Java Plugin` or `Java Web Start`.

  Server. Enter the Sun Java System Instant Messaging Server name. For example:`IMserver.example.com`

  Server Port. Enter the Sun Java System Instant Messaging Server port number. For example:`49999`

  Multiplexor. Enter the Multiplexor name, which must be the same machine as the Sun Java System Instant Messenger server. For example: `IMserver.example.com`

  Multiplexor Port. Enter the Multiplexor port number. For example:`49909`

  User Name. (This field only appears when the authentication method is set to the Sun Java System Portal Server authentication method, `idsvr`) Enter the Sun Java System Instant Messenger user name.

User Password. (This field only appears when the authentication method is set to the Sun Java System Portal Server authentication method, `idsvr`) Enter the Sun Java System Instant Messenger user password.

Finished. Click this button to save the Sun Java System Instant Messaging Server configuration.

Cancel. Click this button to close the window without saving the details.

The Address Book, Calendar, and Mail channels each have display options that the user can set and the administrators cannot by default overwrite. After logging into the Portal Desktop, the user can change the display options for a channel by clicking the edit button in the panel for that channel. The display options are clearly marked and easily changed.

In Address Book, a display option that users can change is the Number of Entries option; in Calendar, a display option that users can change is the Display Day View option; in Mail, a display option that users can change is the Number of Headers option.

Changes made by users to the default communication channels display options take precedence. Any future changes made by administrators do not automatically take effect, and a new channel added by administrators is not automatically accessible by users.

Application Preference Editing: Configuring Communication Channel Edit Pages

You can configure the edit pages that end users see after they click the edit button in a communication channel's tool bar for the Address Book, Calendar, and Mail channels. The Instant Messaging channel does not use application preference editing. For information about configuring the Instant Messaging Channel's edit page, see Sun Java System Portal Server 7.1 Desktop Customization Guide.

For the three communication channels that allow application preference editing, you can change which options are available for end users to edit, what names and wording accompany those options, and how the options are formatted. Configuration of the communication channels edit pages can be performed in the display profile, various HTML templates, and an SSO Adapter template. You might also need to access an SSO Adapter configuration. These items together are involved in the configuration of the edit pages.

This section gives a brief explanation of application preference editing. Other chapters in this guide and the Sun Java System Portal Server 7.1 Desktop Customization Guide provide a more complete explanation of the template files and the display profile, including how they interact with each other and how you can access and edit them.

Display Profile Attributes for the Edit Pages

The communication channels have two collections in their display profile for creating the edit pages. They are `ssoEditAttributes` and `dpEditAttributes`.

You can edit these collections by accessing the Sun Java System Portal Server administration console. Either download the display profile to edit the XML code before uploading it back to the directory server, or edit specific properties in these collections using only the administration console.

The `ssoEditAttributes` collection controls the editing of the attributes contained by the SSO Adapter service, such as `user name` and `user password`. `dpEditAttributes` controls the editing for the display profile attributes, such as `sort order` and `sort by`, which are options that by default end users can edit.

Therefore, these collections list the attributes that can be edited and also contain information on the type of input and the header for the input string to use. For example:

```
<String name="uid" value="string|User Name:"/>
<String name="password" value="password|User Password:"/>
```

The name in the collection must match the name of the corresponding display profile SSO Adapter attribute. The value portion of the item contains two pieces of information separated by the "`|`" character. The first part of the value string specifies the attribute's display type. The second part of the attribute's value string specifies the text that is displayed next to the item.

The list below specifies how the type relates to a corresponding HTML GUI item:

- string—Creates a text field where alphanumeric characters can be entered
- password— Creates a password field where the input is replaced with "*"
- check—Creates a checkbox
- select—Creates a select box. Every select item must have a corresponding collection with a list of values and display text

For every select display type, you must have a corresponding collection that lists the value to be returned and the display value for the option. The collection name must be made up of the name value for the attribute and the text `SelectOptions` . For example, for the `sortOrder` attribute in the `MailProvider`, the collection name is `sortOrderSelectOptions`:

```
<Collection name="sortOrderSelectOptions" advanced="false" merge="replace"
lock="false" propagate="true">
        <String name="top" value="Most recent at top"/>
        <String name="bottom" value="Most recent at bottom"/>
</Collection>
```

HTML Templates for the Edit Pages

Nine HTML templates are used to create edit pages for the communication channel providers. The templates are generic, to correspond to specific browser GUI types, and they primarily relate to specific HTML inputs in the edit pages.

The `edit-start.template` and the `edit-end.template` are exceptions. They contain most of the HTML that is used for page layout. "HTML Templates for the Edit Pages" on page 207 contains a description of each template name and how it relates to the GUI types. Some of the templates are used to start, end and separate the attributes. These templates are available for each of the communication channels at:

`/etc/opt/SUNWportal/desktop/default/`*ChannelName_Provider* `/html`

For example, the templates for the Calendar channel edit pages can be accessed at:

```
/etc/opt/SUNWportal/desktop/default/CalendarProvider/html
```

TABLE 9–1 Templates for the Communication Channel Edit Pages

Template	Description
edit-start.template	Provides the starting HTML table for the edit page.
edit-checkbox.template	Provides a generic template for checkbox items.
edit-separate.template	Separates the display profile attributes from the SSO attributes.
edit-end.template	Ends the HTML table for the edit page.
edit-password.template	Provides a generic template for password items.
edit-string.template	Provides a generic template for text items.
edit-select.template	Provides a generic template for a select item.
edit-selectoption.template	Provides a generic template for a select option. This way the option can also be generated dynamically from the display profile.
edit-link.template	Provides a template to generate the link so the user can edit their client's display attributes.

A Display Profile Example

This example demonstrates how certain SSO Adapter attributes work together with their corresponding display profile attributes to give end users the ability to change the entries for specific features in a communication channel's edit page, thereby changing how the communication channels are configured and displayed on their Portal Desktops.

The SSO Adapter template in "A Display Profile Example" on page 207 is for a sample mail channel. The SSO Adapter template contains two merged attributes:

- uid—User ID

- password—User password

A `merged attribute` is an attribute that end users can specify. Administrators decide which attributes are merged so that end users can edit them.

EXAMPLE 9–2 Sample SSO Adapter Template

```
default|imap:///&configName=MAIL-SERVER-TEMPLATE
    &encoded=password
    &default=protocol
    &default=clientProtocol
    &default=type
    &default=subType
    &default=ssoClassName
    &default=smtpServer
    &default=clientPort
    &default=host
    &default=port
    &merge=username
    &merge=userpassword
    &clientProtocol=http
    &type=MAIL-TYPE
    &subType=sun-one
    &ssoClassName=com.sun.ssoadapter.impl.JavaMailSSOAdapter
    &smtpServer=example.sun.com
    &clientPort=80
    &host=company22.example.com
    &port=143
```

"A Display Profile Example" on page 207 contains the channel's display profile XML fragment for the channel's `ssoEditAttributes`.

After you set an attribute to `merge` in an SSO Adapter template, you can edit that attribute in the display profile to reconfigure how the attribute is displayed to end users in an edit page and how end users can edit it.

Administrators edit the proper display profile collection to define how end users are queried for the necessary information. In this example, administrators could replace `UserName` with the question, `What is your user name?` The use of the `string` attribute display type before the "`|`" symbol is the most likely choice. However, an administrator can change this to the `password` type or to another type.

EXAMPLE 9–3 Sample Mail Channel Display Profile XML Fragment

```
<Channel name="SampleMailChannel" provider="MailProvider">
<Properties>
<Collection name="ssoEditAttributes">
    <String name="username" value="string|User Name:"/>
    <String name="userpassword" value="password|User Password:"/>
</Collection>
```

For this example, in the Mail channel edit page, end users see text fields titled:

- User Name:
- User Password:

Enabling End Users to Set Up Multiple Instances of a Communication Channel Type

End users or administrators can create multiple types of communication channels . To create multiple types of communication channels, end users need to use the Create a new channel link found on the Content page.

Administrators can create multiple channels for an organization, role, or group. After administrators have made multiple instances of a particular component available, such as a second instance of the address book component, they can allow end users to configure a second Address Book channel on their Portal Desktops.

You can create an SSO Adapter template for each new communication channel type or they can use one SSO Adapter template and create multiple SSO Adapter configurations for each channel. For more information, see the SSO Adapter documentation in .

Depending on the amount of configuration done by the administrator, the end users may not need to enter as many configuration settings. Administrators can configure these settings by using the application preference editing feature. See "Application Preference Editing: Configuring Communication Channel Edit Pages" on page 205.

To create two Address Book channels, you make each refer to a different SSO adapter template. You can then add both Address Book channels to the visible page you just came from. Likewise, you can create one SSO Adapter template and two SSO Adapter configurations (dynamic). The SSO Adapter template would define the server settings as user definable values (`merge`) and the SSO Adapter configuration would then specify those server settings.

▼ To Configure the Address Book for Different Servers

To configure the address book for different servers where end users can configure the servers as needed:

1. **Specify the server information as user definable, merge, in the SSO Adapter template. For more information, see .**

2. **In the channel's display profile , specify which attributes can be edited.**`ssoEditAttributes` **collection. For more information, see** **"Application Preference Editing: Configuring Communication Channel Edit Pages" on page 205** **and for specific information about the display profile, see the** *Sun Java System Portal Server 7.1 Desktop Customization Guide***.**

Administrator Proxy Authentication: Eliminating End-User Credential Configuration

You can enable administrator proxy authentication for the Address Book, Calendar, and Mail channels. If you extend support for proxy authentication between the Sun Java System Sun Java System Portal Server and Sun Java System Messaging Services (Sun Java System Messaging Server and Calendar Server), end users do not have to visit a channel's edit page to enter their user name and user password credentials. An administrator's credentials are used instead of an end-user's credentials, and they are stored in the SSO Adapter template.

Within the template, the administrator's User ID is stored as a value for the `proxyAdminUid` attribute while the administrator's password is stored as a value for the `proxyAdminPassword` attribute. Every time a user launches a channel, these values are used to make a connection between a channel and its respective back-end server. A naming attribute for the user is also sent to the back-end server. For more information on naming attributes for administrator proxy authentication, see the `userAttribute` property in "Overview of How to Configure Proxy Authentication" on page 211.

Proxy authentication cannot be configured for Sun Java System Instant Messaging Server, Microsoft Exchange Server, or IBM Lotus Notes server.

Note – Enabling administrator proxy authentication disables the end-user credential configuration for the associated Address Book, Calendar, or Mail channel. A message will be displayed in the channel.

CAUTION—Potential for Multiple End Users to be Directed to One Mail Account

Portal Server and Sun Java System Portal Server allow administrators to set up users with the same User ID across an organization. For example, the organization could have two suborganizations that each have an end user named `enduser22` .

If administrator proxy authentication is enabled for a Sun Java System communication channel, and the end user naming attribute is set to the default, `uid`, both users could potentially access the same back-end user account.

Administrator proxy authentication enables administrators to change the user naming attribute in the SSO Adapter template. For example, you can change the attribute to an attribute that is unique for each employee, such as employee number, to ensure that portal end users access the correct back-end server account.

Overview of How to Configure Proxy Authentication

To enable administrator proxy authentication for the Address Book, Calendar, and Mail channels, you use the Sun Java System Portal Server administration console to access the SSO Adapter templates. Then you need to access the Sun Java System communication servers. Specifically, you need to:

- Edit SSO Adapter Templates.

  In the SSO Adapter Templates, you edit the strings that apply to the Address Book, Calendar, and Mail channels. One of the distinguishing factors of the strings is the protocol used:

  - The Address Book channel uses the LDAP protocol
  - The Calendar channel uses the HTTP protocol
  - The Mail channel uses the IMAP or POP protocol.

  Access Sun Java System Sun Java System Messaging Server to enable proxy authentication for the Address Book and Mail channels.
- Access Sun Java System Calendar Server to enable proxy authentication for the Calendar channel.

▼ To Edit SSO Adapter Templates For Enabling Administrator Proxy Authentication

1 **From an Internet browser, log into the Sun Java System Portal Server administration console at** `http://`*hostname:port*`/psconsole`**, for example**
`http://psserver.company22.example.com:80/psconsole`

2 **Click the Service Configuration tab to display the list of configurable services in the navigation pane.**

3 **Select SSO Adapter to display the page for configuring the SSO Adapter in the data pane.**

4 **Click the string for the channel that you want to enable with administrator proxy authentication.**

5 **Click in the configuration description field.**

6 **Delete and key in the necessary information for administrator proxy authentication:**

"Overview of How to Configure Proxy Authentication" on page 211 describes the properties that need to be edited in the SSO Adapter Template to enable support for administrator proxy authentication.

Property	Value	Description
`enableProxyAuth`	`true` | `false`	The value associated with this attribute is a flag to indicate if proxy authentication is enabled or not. If `true`, the SSO Adapter and Application Adapter perform proxy authentication. For example, `&enableProxyAuth=true`
`proxyAdminUid`	(configurable)	The value associated with this attribute is the administrator's user name. For example, `&proxyAdminUid=ServiceAdmin`
`proxyAdminPassword`	(configurable)	The value associated with this attribute is the administrator's user password. For example, `&proxyAdminPassword=mailpwd`

Property	Value	Description
`userAttribute`	(configurable)	The value associated with this attribute is the user's naming attribute. This value is mapped to an attribute on the user's record (the user's entry in the directory). A typical record has several attributes, including the User ID (`uid`) and employee number. By default, the naming attribute is set to `uid`. For example, `&userAttribute= uid` By editing the SSO Adapter template, you can map the naming attribute to another attribute, such as employee number.
The preceding four properties appear in the SSO Adapter template string again. You can set the configuration of the properties to `default` or `merge`. In the following examples, they are all set to default.		
Property	Value	Example
`enableProxyAuth`	default	&default=`enableProxyAuth`
`proxyAdminUid`	default	&default=proxyAdminUid
`proxyAdminPassword`	default	&default=proxyAdminPassword
`userAttribute`	default	&default=userAttribute

▼ To Set Up Sun Java System Messaging Server for Administrator Proxy Authentication

1. **Log in to the Sun Java System Messaging Server software host and become super user.**
2. **Type the following code:**

   MessagingServer-base **/***msg-instance-name* **`/configutil -o service.http.allowadminproxy -v yes`**

3. **Restart the Sun Java System Messaging Server.**

   See the *Sun Java System Messaging Server Administrator's Guide* for detailed instructions on running `configutil` and restarting the server.

▼ To Set Up Calendar Server for Administrator Proxy Authentication

1. **Log in to the Sun Java System Calendar Server software host and become super user.**

2. **Open the following file with the editor of your choice:**

   CalendarServer-base`/cal/bin/config/ics.conf`

3. **Set the following attribute as shown:**

   ```
   service.http.allowadminproxy = "yes"
   ```

4. **Restart the calendar server.**

   See the *Calendar Server Administrator's Guide* for detailed instructions on restarting the server.

Configuring a Read-Only Communication Channel for the Authentication-Less Portal Desktop

The authentication-less (authless anonymous) Portal Desktop supports read-only communication channels.

Read-Only Communication Channels Facts and Considerations

You can configure read-only access to Address Book, Calendar, and Mail channels for the authless anonymous Portal Desktop. End users can access the information in a read-only communication channel by simply accessing the Portal Desktop; therefore, by entering the following URL in an Internet browser:

```
http://hostname.domain:port/portal/dt, for example
http://psserver.company22.example.com:80/portal/dt
```

Without logging in, end users an access any read-only communication channels that administrators have configured. End users are usually prevented from editing these channels, however. For more information about the authentication-less Portal Desktop, including enabling anonymous log in, see the Sun Java System Portal Server 7.1 Desktop Customization Guide.

The calendar channel is the communications channel most commonly shared by multiple users. The following steps are for configuring a read-only calendar channel. In this example, the calendar being shared belongs to user *library*. The public read-only calendar is titled *Library Schedule*.

Note – The following calendar set up demonstrates one possible approach. For more information about setting up users for the Sun Java System Calendar Server, see the `create` *userid* option of the `csuser` command in the *Sun Java System Calendar Server Administrator's Guide*.

To Set Up a Calendar User

1. **Create a calendar user by issuing a command such as the following:**

   ```
   csuser -g Library -s Admin -y libadmin -l en -m libadmin@library.com -c
   librarySchedule create libadmin
   ```

   Where user **`libadmin`** has a given name of **`Library`**, surname of **`Admin`**, password of **`libadmin`**, preferred language of **`en`** (English), email address of **`libadmin@library.com`** , and calendar ID of **`librarySchedule`**.

2. **Set the access permissions to world readable for:**

   ```
   libadmin:librarySchedule
   ```

   You can set the access permissions using the `cscal` utility or the end user can do this using Calendar Express.

To Configure a Read-Only Communication Channel

1. **Configure the settings for the end user—which in this case is authless anonymous—and create a calendar SSO adapter configuration.**

   a. **From an Internet browser, log on to the Sun Java System Portal Server administration console at** `http://` *hostname:port* `/psconsole`**, for example** `http://psserver.company22.example.com:80/psconsole`

   b. **Click the Identity Management tab to display the View drop down list in the navigation pane.**

   c. **Click Users in the View drop down list.**

   d. **Scroll down as needed to the authless anonymous user and click the accompanying arrow to bring up the authlessanonymous page in the data pane.**

      Now you can add the SSO Adapter service to the authless anonymous user.

   e. **Click Services in the View drop down list within the authlessanonymous page to display the available services.**

f. Click Add.

g. Click the checkbox for SSO Adapter.

h. Click Save.

2 Create a calendar SSO Adapter configuration for the authless anonymous user.

a. If not already logged in, log into the Sun Java System Portal Server administration console.

b. Click the Identity Management tab to display the View drop down list in the navigation pane.

c. Select Services in the View drop down list to display the list of configurable services.

d. Click the arrow next to SSO Adapter to display the SSO Adapter page in the data pane.

e. In the blank configuration description field, type in a group-oriented SSO Adapter configuration string (with a User ID and password). A typical configuration has been provided subsequently for your reference. The attributes available in this string can vary depending upon how you configured the Sun Java System Portal Server SSO Adapter template. By default the SSO Adapter template expects the user to specify the following information:

- host
  - port
    - client port
    - uid
    - password

    If the configuration description field is not blank when you get to it, select all the text in the field and delete it before entering a string in the following format:

    `default|undef://?` *uid:password@host:port* `/?configName=`*configuration-name*`&configDesc=`*configuration-description*

    For example:

    ```
    default|undef://?libadmin:libadmin@example.com:3080/?configName=
    sunOneCalendar_librarySchedule&configDesc=SUN-ONE-CALENDAR
    ```

f. Click Add.

g. Click Save.

3 Create a new calendar channel for the authless anonymous user that is based on the newly created SSO Adapter configuration.

a. Log in to the Sun Java System Portal Server administration console.

b. Click the Identity Management tab to display the View drop down list in the navigation pane.

c. Click Users in the View drop down list.

d. Scroll down to the authless anonymous user, and click the accompanying arrow.

The authlessanonymous page appears in the data pane.

e. Click Portal Desktop in the View drop down list.

The Edit link is displayed.

f. Click the Edit link.

g. Click the Channel and Container Management link.

h. Scroll down to the Channels section and click New.

i. Enter a name in the Channel Name field. For example:

```
LibraryScheduleChannel
```

j. Choose the correct provider from the provider drop down list. For this example the correct provider is Calendar Provider.

k. Click OK, which returns you to the Channel and Container Management page.

Now you can edit the channel properties.

l. Scroll down to the Channels section and click Edit Properties next to your newly created channel. For example:

```
LibraryScheduleChannel
```

m. Edit fields as appropriate. For example:

- title: Library Schedule
  - description: Library Schedule
    - ssoAdapter: sunOneCalendar_librarySchedule
    - loadSubscribedCalendars: false (no checkmark)
    - is editable: false (no checkmark)

n. **Scroll as needed and click Save.**

4 **Add the new calendar channel to Portal Desktop of the Authless Anonymous user:**

a. **Near the top of the page, click Top, which returns you to the Channel and Container Management page.**

b. **Scroll down the Container Channels section and click the link for the container that you want to add the new channel to. For example,** `MyFrontPageTabPanelContainer`**. Do not click the accompanying Edit Properties link.**

c. **Under the Channel Management heading, click the name of the channel you just created.**
For example, `LibraryScheduleChannel`, in the Ready For Use list.

d. **Add the channel to the Available to End Users on the Content Page list or to the Visible on the Portal Desktop list.**
Click the Add button above the list for which you want to add the channel.

e. **Scroll back up the page to click Save under the Channel Management heading.**

f. **Restart the web container.**

Configuring Microsoft Exchange Server or IBM Lotus Notes

Besides supporting Sun Java System Messaging Server and Sun Java System Calendar Server for the communication channels, Sun Java System Portal Server also supports Microsoft Exchange Server and IBM Lotus Notes server.

▼ To Configure Microsoft Exchange 5.5 Server for Address Book, Calendar, and Mail

1 **Log into your Primary Domain Controller (PDC) as an administrator of the domain.**

2 **Select Start, Programs, Administrative Tools, User Manager for Domains and create an account with user name MAXHost.**

3 **Select Groups and add MAXHost to the groups, Administrators, and Domain Admins.**

4 **Ensure that MAXHost can log on locally to the** `MAIL_HOST`**, Domain Controllers, and** `MAX_HOST`**.**

5 **Set the password.**

6. **Log in to your Exchange 5.5 (`MAIL_HOST`) as MAXHost.**

7. **Go to Start, Programs, Microsoft Exchange, Microsoft Exchange Administrator.**

8. **For each end user, set permissions to the mailbox.**

9. **To enable the permissions tab, go to Tools, Options, Permissions, and enable Show Permissions Page for All Objects.**

10. **Double-click on the user name.**

11. **Select the permissions tab and select Add from the permissions page to add MAXHost and leave role as User.**

    Repeat steps 9 through 11 for each user who accesses the communication channels.

12. **Unzip the `ocxhost.zip` file located in the following directory:**

    PortalServer-base/SUNWportal/export.

    When unzipping the file, you see the following file format:

    ```
    Archive: ocxhost.zip
    creating: ocxhost
    creating: ocxhost/international
    inflating:ocxhost/international/ocxhostEnglishResourceDll.dll
    inflating:ocxhost/ocxhost.exe
    ```

13. **Register ocxhost as follows:**

    a. **Locate the `ocxhost.exe`.**

    b. **Select Start and Run.**

    c. **Type the following in the Run window:**

       `ocxhost.exe /multipleuse`

14. **To set the properties of ocxhost utility:**

    a. **Configure the necessary DCOM settings for the ocxhost utility using the `dcomcnfg` utility. That is:**

       i. **Select Start and Run.**

ii. Type `dcomcnfg` and select OK.

iii. In the Distributed COM Configuration Properties dialog box:

iv. Select Default Properties tab:

- Check the Enable Distributed COM on the computer check box.
  - Set the default Authentication Level to Connect.
    - Set the default Impersonation Level to Identify.

v. Select the Applications tab.

vi. Double-click the `ocxhost` utility in the Properties dialog.

The `ocxhost` properties window is displayed.

vii. Check Run Application on this Computer under the Location tab.

viii. Set Use custom access permissions, Use custom launch permissions, and Use custom configuration permissions under the Security tab.

ix. Select Edit for the Access, Launch, and Configuration settings and ensure that the following users are included in the Access Control List (ACL):

- Interactive
  - Everyone
    - System

x. Select a User under the Identity tab in the `ocxhost` properties window.

xi. Select Browse and locate the MAXHost.

xii. Enter the password and confirm the password.

xiii. Select OK.

The `ocxhost` DCOM component is now configured and ready to communicate with the Exchange Servers.

▼ To Configure Microsoft Exchange 2000 Server for Address Book, Calendar, and Mail

To set up Portal Server to access Calendar data from an Exchange Server 2000 environment in a complex Windows 2000 Domain configuration, install `ocxhost.exe` on a dedicated System (called `MAX_HOST`).

Examples of a complex Domain configuration can be:

- A configuration that includes an Exchange Server that is a Cluster and front-end, and a back-end Exchange Server.
- A configuration in which a Windows user and Exchange Mailbox of the same end user are in different Domains.

Installing `ocxhost.exe` on a dedicated machine is useful for two reasons:

- It allows easier troubleshooting if a user cannot access his calendar from the portal.
- It allows a more restrictive security setup if a firewall exists between the Portal Server and the Windows Domain.

The following instructions assume that:

`MAX_HOST`

is the name of the dedicated Windows 2000 System running Outlook 2000 and where `ocxhost.exe` is installed.

`MAIL_HOST`

is the Exchange Server on which the mailboxes of the end users reside.

PORTAL

is the Java Enterprise System Portal Server 7 2005Q3

DOMAIN

is the Windows Domain with `MAX_HOST` and `MAIL_HOST`

When setting up the dedicated Windows 2000 System (`MAX_HOST`) note the following requirements and assumptions:

- Windows 2000 Server SP3 or Windows 2000 Professional.
- Microsoft Outlook 2000 with CDO enabled.
- The Operating System and Outlook 2000 is installed. Assign an IP Address and bring the new Host in the same Domain as the Exchange Server.

1 Create a User MAXhost in the Domain.

a. Log into your Host (`MAX_HOST`) as an administrator of the domain.

b. Select Start, Programs, Administrative Tools, Active Directory Users and Computers and create an domain account with user name MAXHost.

c. Select User->Properties->Member of and add the group Administrators (local)

d. **Ensure that MAXHost can log on locally to the `MAIL_HOST` and `MAX_HOST`.**

e. **Set the password.**

2 **Configure Outlook for MAXHost user.**

a. **Log in to your `MAX_HOST` System as Domain user MAXHost**

b. **Configure the Outlook Profile for the user MAXHost by starting Outlook (refer to Microsoft Documentation if required).**

c. **Close Outlook after completing the Outlook setup for MAXHost user.**

Note – Outlook may not run concurrently with `ocxhost.exe`.

---

3 **Configure Microsoft Exchange Server for Address Book, Calendar, and Mail.**

a. **Log in to your Exchange 2000 Server (`MAIL_HOST`) as MAXHost.**

b. **If you are using an Exchange 2000 Front-End Server, log in to your front-end Server as MAXHost.**

c. **Go to Start, Programs, Microsoft Exchange, Active Directory Users and Computers.**

d. **For each end user, set permissions to the mailbox.**

e. **Select View->Advanced Features**

f. **Double-click on the user name.**

g. **Select the Exchange Advanced tab and select Mailbox Rights.**

h. **Add MAXHost and give MAXHost full access.**

Repeat steps "Configuring Microsoft Exchange Server or IBM Lotus Notes" on page 218 through "Configuring Microsoft Exchange Server or IBM Lotus Notes" on page 218 for each user who access the communication channels.

4 **Install `ocxhost.exe` on the `MAX_HOST`.**

a. **Log in to `MAX_HOST` as domain user MAXhost.**

b. **Unzip the `ocxhost.zip` file located in the following directory:**

PortalServer-base`/SUNWportal/export.`

When unzipping the file, you see the following file format:

- `Archive: ocxhost.zip`
  - `creating: ocxhost`
    - `creating: ocxhost/international`
    - `inflating:ocxhost/international/ocxhostEnglishResourceDll.dll`
    - `inflating:ocxhost/ocxhost.exe`

c. Register `ocxhost` as follows:

i. Locate the `ocxhost.exe` file.

ii. Select Start and Run.

iii. Type `ocxhost.exe /multipleuse` and select OK.

Note – Perform this registration only once. Each time this command is executed the DCOM settings described in the next step are cleared and need to be reconfigured.

---

d. Configure the necessary DCOM settings for the `ocxhost` utility using the `dcomcnfg` utility.

e. Select Start and Run.

f. Type `dcomcnfg` and select OK.

g. In the Distributed COM Configuration Properties dialog box select Default Properties tab and use the following settings:

- Check the Enable Distributed COM on the computer check box.
  - Set the default Authentication Level to Connect.
    - Set the default Impersonation Level to Identify.

h. Select the Applications tab.

i. Double-click the `ocxhost` utility in the Properties dialog.

The `ocxhost` properties window is displayed.

j. Check Run Application on this Computer under the Location tab.

k. Set Use custom access permissions, Use custom launch permissions and Use custom configuration permissions under the Security tab.

l. Select Edit for the Access, Launch, and Configuration settings and ensure that the following users are included in the Access Control List (ACL):

- Interactive
  - Everyone
    - System

m. Select a User under the Identity tab in the `ocxhost` properties window.

n. Select Browse and locate the MAXHost.

o. Enter the password and confirm the password.

p. Select OK.

The `ocxhost` DCOM component is now configured and ready to communicate with the Exchange Servers. It is launched by RPC call when the first access from the Portal Server occurs.

5 Change MAXHost users group.

For security reasons you may want to remove the domain user from the Administrators group:

a. Log out and log in again as Administrator on `MAX_HOST`.

b. Remove the user MAXHost from local Administrators group, (and assign it to Domain User Group).

Note – Do not use a firewall should between the Portal and the MAX_HOST.

(RPC calls using dynamic ports are used for the communication from Portal Server to `ocxhost.exe`.)

Do not use a firewall between the `MAX_HOST` and the `MAIL_HOST`.

▼ To Configure Microsoft Exchange 2003 Server for Address Book, Calendar, and Mail

To set up Portal Server to access Calendar data from an Exchange Server 2003 environment in a complex Windows 2000 Domain configuration, install `ocxhost.exe` on a dedicated System (called `MAX_HOST`).

Examples of a complex Domain configuration can be:

- A configuration that includes an Exchange Server that is a Cluster and front-end, and a back-end Exchange Server.

- A configuration in which a Windows user and Exchange Mailbox of the same end user are in different Domains.

Installing `ocxhost.exe` on a dedicated machine is useful for two reasons:

- It allows easier troubleshooting if a user cannot access his calendar from the portal.
- It allows a more restrictive security setup if a firewall exists between the Portal Server and the Windows Domain.

The following instructions assume that:

`MAX_HOST`

is the name of the dedicated Windows 2000 System running Outlook 2000 and where `ocxhost.exe` is installed.

`MAIL_HOST`

is the Exchange Server on which the mailboxes of the end users reside.

PORTAL

is the Java Enterprise System Portal Server 7.1

DOMAIN

is the Windows Domain with `MAX_HOST` and `MAIL_HOST`

When setting up the dedicated Windows 2000 System (`MAX_HOST`) note the following requirements and assumptions:

- Windows 2000 Server SP3 or Windows 2000 Professional.
- Microsoft Outlook 2000 with CDO enabled.
- The Operating System and Outlook 2000 is installed. Assign an IP Address and bring the new Host in the same Domain as the Exchange Server.

1 Create a User MAXhost in the Domain.

a. Log into your Host (`MAX_HOST`) as an administrator of the domain.

b. Select Start, Programs, Administrative Tools, Active Directory Users and Computers and create an domain account with user name MAXHost.

c. Select User->Properties->Member of and add the group Administrators (local)

d. Ensure that MAXHost can log on locally to the `MAIL_HOST` and `MAX_HOST`.

e. Set the password.

2. **Configure Outlook for MAXHost user.**

   a. **Log in to your `MAX_HOST` System as Domain user MAXHost**

   b. **Configure the Outlook Profile for the user MAXHost by starting Outlook (refer to Microsoft Documentation if required).**

   c. **Close Outlook after completing the Outlook setup for MAXHost user.**

   Note – Outlook may not run concurrently with `ocxhost.exe`.

3. **Configure Microsoft Exchange Server for Address Book, Calendar, and Mail.**

   a. **Log in to your Exchange 2003 Server (`MAIL_HOST`) as MAXHost.**

   b. **If you are using an Exchange 2003 Front-End Server, log in to your front-end Server as MAXHost.**

   c. **Go to Start, Programs, Microsoft Exchange, Active Directory Users and Computers.**

   d. **For each end user, set permissions to the mailbox.**

   e. **Select View->Advanced Features**

   f. **Double-click on the user name.**

   g. **Select the Exchange Advanced tab and select Mailbox Rights.**

   h. **Add MAXHost and give MAXHost full access.**

   Repeat steps "Configuring Microsoft Exchange Server or IBM Lotus Notes" on page 218 through "Configuring Microsoft Exchange Server or IBM Lotus Notes" on page 218 for each user who access the communication channels.

4. **Install `ocxhost.exe` on the `MAX_HOST`.**

   a. **Log in to `MAX_HOST` as domain user MAXhost.**

   b. **Unzip the `ocxhost.zip` file located in the following directory:**

   PortalServer-base`/SUNWportal/export`.

   When unzipping the file, you see the following file format:

   - `Archive: ocxhost.zip`
     - `creating: ocxhost`

- `creating: ocxhost/international`
- `inflating:ocxhost/international/ocxhostEnglishResourceDll.dll`
- `inflating:ocxhost/ocxhost.exe`

c. Register `ocxhost` as follows:

i. Locate the `ocxhost.exe` file.

ii. Select Start and Run.

iii. Type `ocxhost.exe /multipleuse` and select OK.

Note – Perform this registration only once. Each time this command is executed the DCOM settings described in the next step are cleared and need to be reconfigured.

---

d. Configure the necessary DCOM settings for the `ocxhost` utility using the `dcomcnfg` utility.

e. Select Start and Run.

f. Type `dcomcnfg` and select OK.

g. In the Distributed COM Configuration Properties dialog box select Default Properties tab and use the following settings:

- Check the Enable Distributed COM on the computer check box.
  - Set the default Authentication Level to Connect.
    - Set the default Impersonation Level to Identify.

h. Select the Applications tab.

i. Double-click the `ocxhost` utility in the Properties dialog.

The `ocxhost` properties window is displayed.

j. Check Run Application on this Computer under the Location tab.

k. Set Use custom access permissions, Use custom launch permissions and Use custom configuration permissions under the Security tab.

l. Select Edit for the Access, Launch, and Configuration settings and ensure that the following users are included in the Access Control List (ACL):

- Interactive
  - Everyone

- System

m. Select a User under the Identity tab in the `ocxhost` properties window.

n. Select Browse and locate the MAXHost.

o. Enter the password and confirm the password.

p. Select OK.

The `ocxhost` DCOM component is now configured and ready to communicate with the Exchange Servers. It is launched by RPC call when the first access from the Portal Server occurs.

5 Change MAXHost users group.

For security reasons you may want to remove the domain user from the Administrators group:

a. Log out and log in again as Administrator on `MAX_HOST`.

b. Remove the user MAXHost from local Administrators group, (and assign it to Domain User Group).

Note – Do not use a firewall should between the Portal and the MAX_HOST.

(RPC calls using dynamic ports are used for the communication from Portal Server to `ocxhost.exe`.)

Do not use a firewall between the `MAX_HOST` and the `MAIL_HOST`.

▼ To Set Up SSO Adapter for Calendar

Set up SSO Adapter for Calendar if you are using a dedicated Server for `ocxhost.exe` (MAX_HOST).

1 Create an SSO Adapter template.

a. Log in to the Access Manager administration console.

b. Select the Service Configuration Tab.

c. Select SSOAdapter.

d. Select New.

e. **Enter a name for your new template and select the existing EXCHANGE-CALENDAR from the list.**

f. **Select Next.**

g. **In the line for the ocxHost enter the dns-name or IP-Address of the system were** `oxchost.exe` **resides, in this case MAX_HOST.**

h. **Select Save.**

2 **Create an SSO Adapter configuration for your organization.**

a. **From the Identity Management tab, select your organization.**

b. **Select Services from the scroll down menu**

c. **Select SSOAdapter.**

d. **Under SSO Adapter Configurations, select New.**

e. **Enter a name for the configuration and select the previously created Template.**

f. **Select Next.**

g. **Modify the properties as needed.**

You can provide a default Host name which is your MAIL_HOST (DNS name or IP-Address), or you can leave it blank

h. **Select Save and note the message Changes Saved.**

▼ To Uninstall `ocxhost.exe`

Unregister ocxhost as follows:

1 **Locate the** `ocxhost.exe` **utility.**

2 **Select Start and Run.**

3 **Type the following in the Run window:**

```
ocxhost.exe /unregserver
```

4 **Delete the files** `ocxhost.exe` **and** `ocxhostEnglishResourceDll.dll`

▼ To Configure Lotus Domino Server for Address Book, Calendar, and Mail

1. **Open the Lotus Administrator by selecting Start, Programs, Lotus Applications, and Lotus Administrator.**
2. **Go to Administration, Configuration, Server, Current Server Documents.**
3. **In the Security tab, set the following settings:**
   a. **Under Java/COM Restrictions, set Run restricted Java/Javascript/COM and Run unrestricted Java/Javascript/COM to *.**
   b. **Under Security Settings, set:**
      - Compare Notes Public keys against those stored in Directory to No.
        - Allow anonymous Notes connections to No.
          - Check Passwords on Notes IDs to Disabled.

   c. **Under Server Access, set Only allow server access to users listed in this Directory to No.**
   d. **Under Web Server Access, set Web Server Authentication to More Name Variations with lower security.**
4. **In the Ports tab:**
   a. **Select the Notes Network Ports tab and ensure that TCPIP is ENABLED.**
   b. **Select Internet Ports tab and the Web tab.**
      i. **Ensure that TCP/IP port status is Enabled.**
      ii. **Under Authentication options, ensure that Name and password and Anonymous are Yes.**
      iii. **Select the Directory tab and ensure that:**
         - TCP/IP port status is Enabled.
           - Authentication options items Name and Password and Anonymous are Yes.
             - SSL port status is Disabled.

      iv. **Select the Mail tab and ensure that:**
         - TCP/IP port status is Enabled.
           - Authentication options Name and Password and Anonymous are set as follows:

Mail (IMAP)	Mail (POP)	Mail (SMTP Inbound)	SMTP (Outbound)
Name and Password	Yes	Yes	No
Anonymous	N/A	N/A	Yes

v. **Select the IIOP tab and ensure that:**

- TCP/IP port status is Enabled.
  - Authentication options items Name and Password and Anonymous are Yes.
    - TCP/IP port number is not set to `0`. It should be `63148`.
    - SSL port status is Disabled.

c. **Select the Internet Protocols tab and the IIOP sub-tabs. Ensure that the Number of threads is at least 10.**

5 **Save and close.**

6 **Restart the server by typing the following in the Domino server console:**

```
restart server
```

Restarting the server enables the settings to take effect.

7 **Enable DIIOP server by typing the following command in the console:**

```
load diiop
```

8 **Check to see if `diiop_ior.txt` has been generated at location:**

```
C:\\Lotus\\Domino\\Data\\domino\\html\\diiop_ior.txt
```

9 **Enable HTTP service by typing the following command in the console:**

```
load http
```

- If another service is using port 80, the HTTP service does not start. Stop the service running on port 80 and retype the following in the console: **`load http`**

  Or

  - Use the existing service. To do this, copy the `diiop_ior.txt` file into the root or home directory of the web server running on port 80. You can include both the HTTP service and the DIIOP service in the `notes.ini` file to ensure that both services start when you start the server.

▼ To Configure Portal Server to Access Lotus Notes

To access a Lotus Notes system using the Sun Java System Portal Server Mail and Calendar channels, you must add another file to the Sun Java System Portal Server. This file is called `NCSO.jar`. It must be obtained from the Lotus Notes product CD or the IBM web site.

This file is available with the Domino Designer and Domino Server products from IBM in the `domino\\java` subdirectory. It is also available in a Web download from the following Web site:

```
http://www-10.lotus.com/ldd/toolkits
```

1 **Go to the Lotus Domino Toolkit link and then to the Java/Corba R5.0.8 update link.**

Note – The download file, which performs the extraction of this file and other files, is an `.exe` file.

---

2 **Place the `NCSO.jar` file in the global class path of the web container (web server or application server) as described in the subsequent sections about each of the four possible web containers. For three of the four web containers, the `NCSO.jar` file is placed in `/usr/share/lib`. The following table summarizes the steps that follow.**

The table outlines the process of placing the JAR file in the global class path by indicating where the `NCSO.jar` file can be placed: in the System Classpath or in the Portal WAR. The table also indicates if special instructions are needed. If so, they are included later in this section.

Web Container	System Classpath	Portal WAR	Special Instructions
Sun Java System Web Server	Yes	Yes	N/A
Sun Java System Application Server	Yes	Yes	N/A
BEA WebLogic Server	Yes	No	How to update system classpath
IBM WebSphere Application Server	No	Yes	How to prune JAR file

The following instructions are provided for each web container:

Note – To complete the following steps for your web container, you must have administrative rights to it. Also you should have access to the web container documentation to obtain detailed information on various web container processes and commands.

For more information concerning the Sun Java System web containers, see *Sun Java System Application Server Administrator's Guide* or *Sun Java System Sun Java System Web Server, Enterprise Edition Administrator's Guide*.

Sun Java System Web Server

▼ To Configure Lotus Notes with the Sun Java System Web Server

1. **Place the `NCSO.jar` in the following Sun Java System Portal Server directory:**
   `/usr/share/lib`
2. **Update the web container class path to include:**
   `/usr/share/lib/NCSO.jar`
   a. **Launch the Sun Java System Web Server administration console.**
   b. **Select the Sun Java System Web Server instance.**
   c. **Click Manage.**
   d. **Select the Java tab.**
   e. **Select the JVM Path Settings.**
   f. **Add `/usr/share/lib/NCSO.jar` to the classpath suffix.**
   g. **Select ok**
   h. **Select Apply**
3. **Restart the Sun Java System Web Server . Though often not mandatory, this practice is a good one.**

▼ Optional Placement of the `NCSO.jar` file

1. **Place the `NCSO.jar` file in the following directory:**
   PortalServer-base`/SUNWportal/web-src/WEB-INF/lib`
2. **Redeploy the web application with the following command:**
   PortalServer-base`/SUNWportal/bin/deploy redeploy`
3. **Restart the web container.**

Sun Java SystemApplication Server

▼ To configure Lotus Notes with Sun Java System Application Server

1. **Place the `NCSO.jar` in the following Sun Java System Portal Server directory:**
   `/usr/share/lib`
2. **Update the web container class path to include `/usr/share/lib/NCSO.jar` using the Sun Java System Application Server administration console.**
   a. **Launch the Sun Java System Application Server administration console.**
   b. **Select the domain.**
   c. **Select the server instance.**
   d. **Select the JVM Settings tab in the server instance view.**
   e. **Select Path Settings under the JVM Settings tab.**
   f. **Add `/usr/share/lib/NCSO.jar` in the Classpath Suffix list.**
   g. **Select Save.**
   h. **Select Apply Changes under the General tab of the instance.**
   i. **Select Restart.**

▼ Optional Placement of the `NCSO.jar` File

1. **Place the `NCSO.jar` file in the following directory:**
   PortalServer-base`/SUNWportal/web-src/WEB-INF/lib`
2. **Redeploy the web application with the following command:**
   PortalServer-base`/` **`SUNWportal/bin/deploy redeploy`**
   Where *PortalServer-base* represents the directory in which the Sun Java System Portal Server was originally installed.
3. **Restart the web container.**

To Configure Lotus Notes With BEA WebLogic Server

1. **Place the `NCSO.jar` in the following Sun Java System Portal Server directory:**

   `/usr/share/lib`

2. **Update the web container class path to include `/usr/share/lib/NCSO.jar` using the command line.**

   a. **Change directories to the web container install directory:**

      WebContainer-base `/bea/wlserver6.1/config`

      Where *WebContainer-base* represents the directory in which the web container was originally installed.

   b. **Change directories to the directory that contains the domain instance:**

      `mydomain`

   c. **Edit the `startWebLogic.sh` file using the editor of your choice.**

   d. **Add `/usr/share/lib/NCSO.jar` to the end of the CLASSPATH.**

      Note – The `startWebLogic.sh` file may contain multiple CLASSPATH definitions. Locate the last definition of the variable and add the following string to the very end of the CLASSPATH:

      `/usr/share/lib/NCSO.jar`

   e. **Restart the web container.**

Configuring Lotus Notes For IBM WebSphere

1. **Prune the classes under `org/w3c/dom/` and `org/xml/sax/` from the `NCSO.jar` file and rejar.**

   The classes should include the following:

   - `org/w3c/dom/Document.class`
     - `org/w3c/dom/Node.class`
     - `org/xml/sax/InputSource.class`
     - `org/xml/sax/SAXException.class`

       You can perform this task in many ways. Two examples are provided here. Follow the method that suits you best:

     - The following method requires you to manually unjar and rejar the file:

a. Download and place the file in the following directory:

`/tmp/ncsoprune/work`

b. Unjar the file while it is in that directory.

c. Remove the preceding four classes.

d. Rejar the file.

- The following method requires you to run a script that automates the jar and unjar logic.

a. Download and place the file in the following directory:

`/tmp/ncsoprune/work`

b. Run the following script:

```
!/bin/ksh JAR=/usr/j2se/bin/jar JAR_FILE=NCSO.jar RM=/usr/bin/rm BASE_DIR=
/tmp/ncsoprune WORK_DIR=${BASE_DIR}/work
cd to director of jar file cd $WORK_DIR # unjar $JAR xvf $JAR_FILE
prune classes $RM $WORK_DIR/org/w3c/dom/Document.class
$RM $WORK_DIR/org/w3c/dom/Node.class
$RM $WORK_DIR/org/xml/sax/InputSource.class $RM
$WORK_DIR/org/xml/sax/SAXException.class
jar $JAR cvf $BASE_DIR/$JAR_FILE META-INF com lotus org
```

2 **Place the re-jarred `NCSO.jar` file in the following directory:**

PortalServer-base`/SUNWportal/web-src/WEB-INF/lib`

3 **Redeploy the web application with the following command:**

PortalServer-base`/ SUNWportal/bin/deploy redeploy`

Where *PortalServer-base* represents the directory in which the Sun Java System Portal Server was originally installed.

4 **Restart the web container.**

▼ To Create a New User Under the Default Organization

1 **From an Internet browser, log on to the Sun Java System Portal Server administration console at** `http://`*hostname:port*`/psconsole`**, for example**
`http://psserver.company22.example.com:80/psconsole`

2 **Click the Identity Management tab to display the View drop down list in the navigation pane.**

3 **Select Users in the View drop down list to display the User page.**

4. **Click New to display the New User page in the data pane.**

5. **Select the services to be assigned to the user.**
   Select at a minimum Portal Desktop and SSO Adapter.

6. **Enter the user information.**

7. **Click Create.**
   The new user's name appears in the Users list in the navigation pane.

Configuring the Mail Provider to Work with an HTTPS Enabled Sun Java System Messaging Server

The Mail channel automatically supports the HTTP protocol, but not the more secure HTTPS protocol. If your Sun Java System Messaging Server is enabled for HTTPS, however, you can follow the steps in this section to configure the Mail provider to work properly with the Sun Java System Messaging Server. These steps do not apply to Microsoft Exchange Server and IBM Lotus Notes server.

Web Container Facts and Considerations

In terms of configuring the mail provider for HTTPS for Sun Java System Messaging Server, the steps regarding the web container differ depending upon which web container you are using: Sun Java System Web Server, Sun Java System Application Server, BEA WebLogic Server, or IBM WebSphere Application Server. Regardless of which web container you use, you need administrative rights to it.

You should refer to the web container documentation for information on initializing a trust database, adding certificates, and restarting the web container. For more information on these tasks and other security-related issues concerning the Sun Java System web containers, see *Sun Java System Application Server Administrator's Guide to Security* or *Sun Java System Sun Java System Web Server, Enterprise Edition Administrator's Guide*.

▼ To Configure the Mail Provider to Work with an HTTPS Enabled Sun Java System Messaging Server

1. **Initialize the trust database for the web container running Sun Java System Portal Server. For more information, refer to the proper documentation as discussed in the preceding paragraph.**

2. **Install the SSL certificate for the Trusted Certificate Authority (TCA) if it is not already installed.**

3. **Restart the web container. Even though restarting is not mandatory, this practice is a good one.**

4 **Add a new SSO Adapter template specifically for HTTPS. The name of the template used in this example is `SUN-ONE-MAIL-SSL`, which is descriptive since the security protocol, SSL, is included in the name.**

Note – You can configure an SSO Adapter template and related SSO Adapter configurations in many ways. The steps presented subsequently explain a typical configuration. They describe how to create a new template and a new configuration since this is a safer practice than simply editing existing templates and configurations.

If you are comfortable with the editing option, then proceed in that manner. If you change the name of the SSO Adapter template and SSO Adapter configuration as part of the edits you make, you also need to change the SSO Adapter name by editing the properties of the Mail channel.

The two items you would need to edit in the SSO Adapter template or SSO Adapter configuration are:

- `clientProtocol`
- `clientPort`

In creating a new SSO Adapter Template for this example, the `clientProtocol` attribute is set as a `default` attribute. Therefore, it appears in an SSO Adapter template not in an SSO Adapter configuration. The `clientProtocol` attribute must be changed from `http` to `https`. The edited template fragment for this attribute appears as follows:

```
clientProtocol=https
```

For this example, the `clientPort` attribute is set as a `merge` attribute. Therefore, it appears in an SSO Adapter configuration (see "Web Container Facts and Considerations" on page 237). If the `clientPort` attribute were set as a `default` attribute, it would appear in an SSO Adapter template. The client port should be changed to a port reserved exclusively for HTTPS. Here port `443` is used since the HTTPS protocol uses this port number as the default. The edited template fragment for this attribute appears as follows:

```
&clientPort=443
```

---

a. **From an Internet browser, log into the Sun Java System Portal Server administration console at `http://` *hostname:port* `/psconsole`, for example**
`http://psserver.company22.example.com:80/psconsole`

b. **Click the Service Configuration tab to display the list of configurable services in the navigation pane.**

c. **Click the arrow next to SSO Adapter to bring up the SSO Adapter page in the data pane.**

d. **Type a template name and select an existing template from the menu.**

e. **Click Next.**

f. **The Template Properties page appears.**

g. **Modify the properties as needed.**

"Web Container Facts and Considerations" on page 237 is a typical configuration which has been provided for your reference. The template you enter probably has different information. For example, you probably enter a different value for the `configName` property type unless you want to use the name `SUN-ONE-MAIL-SSL` . Furthermore, the attributes you set as `default` and `merge` probably differ from this example, depending upon the needs of your site.

h. **When done, click Save.**

```
default|imap:///?configName=SUN-ONE-MAIL-SSL &encoded=password
&default=protocol &default= clientProtocol &default=type &default=subType
&default=enableProxyAuth &default=proxyAdminUid &default=proxyAdminPassword
&default=ssoClassName &merge=host &merge=port &merge=uid &merge=password
&merge=smtpServer &merge=clientPort &clientProtocol=https &enableProxyAuth=false
&proxyAdminUid=[PROXY-ADMIN-UID] &proxyAdminPassword=[PROXY-ADMIN_PASSWORD
&type=MAIL-TYPE &subType=sun-one &    ssoClassName=
com.sun.ssoadapter.impl.JavaMailSSOAdapter
&default=enablePerRequestConnection &enablePerRequestConnection=false

                              If more than one string that begins with the IMAP protocol
exists, this is acceptable.
```

5 **Add a new SSO Adapter configuration specifically for HTTPS.**

The name of the configuration used in this example is `sunOneMailSSl`, because it is similar to the name used for the respective SSO Adapter template.

Note – See the Note from the preceding step, "Web Container Facts and Considerations" on page 237.

---

a. **From an Internet browser, log on to the Sun Java System Portal Server administration console at** `http://` *hostname:port* `/psconsole`**, for example** `http://psserver.company22.example.com:80/psconsole`

b. **Click the Identity Management tab to display the View drop down list in the navigation pane.**

c. **Click Services in the View drop down list.**

d. **Scroll down the navigation pane to the Single Sign-on Adapter configuration heading and click the arrow next to SSO Adapter to bring up the SSO Adapter page in the data pane.**

e. **Click in the blank configuration description field—which is just above the Add and Remove buttons.**

f. **Click New under SSO Adapter Configuration to add an SSO adapter configuration.**

g. **The New Configuration page appears.**

h. **Type a configuration name and select an SSO Adapter template from the menu.**

i. **Click Next.**

j. **The Configuration Properties page appears.**

k. **Modify the properties as needed.**

l. **When done, click Save.**

6 **Add a new Mail channel to Portal Desktop.**

"Web Container Facts and Considerations" on page 237 and "Web Container Facts and Considerations" on page 237 explained how to create a new SSO Adapter template and SSO Adapter configuration to create a new channel. In this step you make the channel available to end users.

Choose a descriptive name for the new channel. The example name chosen here is `SunOneMailSSLChannel`.

a. **From an Internet browser, log on to the Sun Java System Portal Server administration console at** `http://` *hostname:port* `/psconsole`**, for example** `http://psserver.company22.example.com:80/psconsole`

b. **Click the Identity Management tab to display the View drop down list in the navigation pane.**

c. **Select Services in the View drop down list to display the list of configurable services.**

d. **Under the Sun Java System Portal Server Configuration heading, click the arrow next to Portal Desktop to bring up the Portal Desktop page in the data pane**

e. **Scroll as needed and click the Manage Channels and Containers link.**

f. **Scroll down to the Channels heading and click New.**

g. **In the Channel Name field, type your site's name for the new channel. For example,** `SunJavaMailSSLChannel`**.**

h. **In the Provider drop down menu, select MailProvider.**

i. **Click OK, which returns you to the Channel and Container Management Web page where the channel you just created now exists.**

j. **Scroll down to the Channels heading and click Edit Properties next to the name of the channel you just created, which for this example is** `SunOneMailSSLChannel`**.**

k. **Scroll down to the title field, select and delete any words that currently exist, for example** `mail`**, and type a provider title. A possible name is** `SSL Mail Account`**.**

l. **In the description field, select and delete any words that currently exist, for example** `mail`**, and type a provider description. The same example is used here for description as for the title in the preceding substep:** `SSL Mail Account`**.**

m. **Scroll down the page; select and delete any words that currently exist in the SSO Adapter field, for example** `sunOneMail` **; and type the same SSO Adapter configuration name used in** **"Web Container Facts and Considerations" on page 237** **, which for this example is** `sunOneMailSSL`**.**

n. **Scroll down and click Save.**

o. **Scroll back up the page to click the word** `top`**, which is the first item following the words** `Container Path`**.**

p. **Scroll down to the Container Channels heading and click the link for the container that you want to add the new channel to. For example,** `MyFrontPageTabPanelContainer`**. Do not click the accompanying Edit Properties link.**

q. **Scroll down to the Channel Management heading, scroll as needed in the Ready For Use frame, and click the name of your newly created channel to select it.**

   Remember, for this example the channel name is `SunOneMailSSLChannel` .

r. **Add the channel to the Available to End Users on the Content Page list or to the Visible on the Portal Desktop list.**

   Click the Add button above the list for which you want to add the channel.

s. **Scroll back up the page and click Save under the Channel Management heading.**

   You should now be able to log in and use an HTTPS enabled messaging server.

Configuring Instant Messaging Server

After installing Instant Messaging server, you need to manually configure it for Portal Server.

▼ To Configure Instant Messaging Server

1 Install Instant Messaging Server.

2 Run the following command to configure Instant Messaging server.

Instant-Messaging-server-base`/SUNWiim/configure`

The Instant Messaging configurator appears.

3 Type the following values in the configurator pages:

Components	Select the following components: Instant Messaging Server, Instant Messenger Resources Identity Server, and Instant Messaging Service.
Server Components	Select these options.
Client components	
Use Access Manager for Single—Sign-on	Select these options.
Use Access Manager for Policy	
User ID	Type the user ID and group ID. For example, in Solaris 10, these values are root and root respectively.
Group ID	
Runtime Directory	The default value of runtime directory is `/var/opt/SUNWiim`.
Domain Name	Type the domain name.
XMPP port	By default, it is 522.
Multiplexed XMPP port	By default, it is 4522.
Disable Server	Do not select this option.
Ldap hostname	It is `machine-name.host-name`.
Ldap Port Number	By default, it is 389.
Base dn	By default, it is dc=sun,dc=com.
Bind dn	By default, it is cn=Directory Manager.
Bind Password	Type the password.

Enable E-mail Integration	Select this option.
Smtp server	Provide the domain name.
Enable E-Mail Archiving	Select this option.
Deploy Messenger Resources	Provide the details.
Codebase Web Administration URL	
Web Administrator User Id	
Web Administrator User Password	
Deploy IM HTTP Gateway	Provide the details.
Context Root	
Web Administration URL	
Web Administrator User Id	
Web Administrator User Password	
Enable Calendar Agent	Select this option if you wish to enable the calendar agent.
Start Services After Successful Configuration	Select these options.
Start Services When System start	

4 Click Done.

▼ To Configure Instant Messaging Server in Portal Server

1 Log in to Portal Server desktop.

2 Click the Edit button displayed with the Instant Messaging portlet.

The Instant Messaging portlet is displayed in the Edit mode.

3 Provide the following details.

Launch Method	The launch method can be Java Plugin or Java Web Start.
Server Hostname	The fully qualified domain name of the machine where you installed Messaging Server.
Server Port	The port on which the Messaging Server is running.

◆ ◆ ◆ CHAPTER 10

Setting Up Federated Search

The Federated Search feature enables users to submit a search query to multiple search engines concurrently and have the search results displayed in a unified format. The Federated Search feature provides a single interface for the user to post a search query to both a web meta-repository, such as google.com and an internal directory system such as a local personnel directory. The search results from these two different sites are presented to the user in a single web page.

Note – Federated google search will work only if the customer has an existing google client key, because new keys are no longer being issued.

Setting Up Federated Search

▼ To Set Up Federated Search

1 **Set up sample federated databases:**

   a. **From a terminal window, log in to the host where search server is installed.**

   b. **Type the following:**

      ```
      cd /opt/SUNWportal/sdk/search
      ```

   c. **Modify the `sampledbs.soif` file to change google clientKey value to be your downloaded license key, and modify databaseurl, providerurl, rdmserverurl, and other url values, accordingly.**

      Use the SOIF file syntax. The number in curly brackets ({ }) following the attribute is the number of characters you enter for that attribute's value.

d. Type the following:

`cd /var/opt/SUNWportal/searchservers/`*search-server*

`./run-cs-cli rdmgr -y root /opt/SUNWportal/sdk/search/sampledbs.soif`

`./run-cs-cli rdmgr -y root -U` to verify that the soif entries containing the configurations for sample federated databases in the `sampledbs.soif` are in the root db.

2 Add `googleapi.jar` and `oracledriver.jar` to the web container's class path:

On the Application Server:

`cp` *google-api-install-directory*`/googleapi/googleapi.jar /var/opt/SUNWappserver/domains/domain1/applications/j2ee-modules/`*search-server-ID*`/WEB-INF/lib/googleapi.jar`

On the Web Server:

`cp /google-api-install-directory/googleapi/googleapi.jar /var/opt/SUNWwbsvr7/https-`*host*`.`*domain*`/webapp/`*host*`.`*domain*`/`*search-server-ID*`/WEB-INF/lib`

3 Restart the web container.

▼ To Test Federated Search

1 Use the `rdmserver` front-end by:

a. Go to http://*host-name*.red.iplanet.com/*search-server-ID*/testrdm.html

b. Select "rd-request" for Type, select "search" for "Query Language."

c. Enter a federated db such as "google" for "Database."

d. Enter a query such as "java" for "Scope".

e. Click "Submit GET."

f. Verify that search results are returned.

2 Use the Search channel by modifying Search channel JSPs, such as `dbMenu.jsp`, `results.jsp`, and `searchOnly.jsp` to add federated databases to the database list and view attributes for federated search results.

◆ ◆ ◆ APPENDIX A

Appendix

Content of the `ampsamplesilent` File

```
# Copyright 2005 Sun Microsystems, Inc. All rights reserved.

#

# Sun Microsystems, Inc. has intellectual property rights relating to

# technology embodied in the product that is described in this document.

# In particular, and without limitation, these intellectual property rights

# may include one or more of the U.S. patents listed at

# http://www.sun.com/patents and one or more additional patents or pending

# patent applications in the U.S. and in other countries.

#

# U.S. Government Rights - Commercial software. Government users are subject

# to the Sun Microsystems, Inc. standard license agreement and applicable

# provisions of the FAR and its supplements.

#

# Use is subject to license terms.

#

# This distribution may include materials developed by third parties.Sun,
```

```
# Sun Microsystems and the Sun logo are trademarks or registered trademarks
# of Sun Microsystems, Inc. in the U.S. and other countries.
#
# Copyright 2005 Sun Microsystems, Inc. Tous droits rservs.
# Sun Microsystems, Inc. dtient les droits de proprit intellectuels relatifs
# technologie incorpore dans le produit qui est dcrit dans ce document.
# En particulier, et ce sans limitation, ces droits de proprit
# intellectuelle peuvent inclure un ou plus des brevets amricains lists
# adresse http://www.sun.com/patents et un ou les brevets supplmentaires
# ou les applications de brevet en attente aux Etats - Unis et dans les
# autres pays.
#
# L'utilisation est soumise aux termes du contrat de licence.
#
# Cette distribution peut comprendre des composants dvelopps par des
# tierces parties.
#
# Sun, Sun Microsystems et le logo Sun sont des marques de fabrique ou des
# marques dposes de Sun Microsystems, Inc. aux Etats-Unis et dans
# d'autres pays.


###############################################################################
###
### Access Manager common deployment variables. The variables in the common
```

```
### section, as well as those in the container specific sections must be

### set to the proper values for the amconfig script to successfully

### configure or deploy Access Manager.

###

### DEPLOY_LEVEL is a numeric value corresponding to the type of installation

### which should be performed. See supported values below.

###

### DEPLOY_LEVEL possible values

### 1 = Full install

### 2 = Console only install

### 3 = SDK only install

### 4 = SDK only with container config

### 5 = Federation common domain install

### 6 = Server only install

### 7 = Container config

### 8 = Distributed Auth

### 9 = Client SDK

### 10 = AM Single War

### 11 = Full uninstall

### 12 = Uninstall console only

### 13 = Uninstall SDK

### 14 = Uninstall SDK and unconfig container

### 15 = Uninstall Federation

### 16 = Uninstall server
```

```
### 17 = Uninstall container config

### 18 = Uninstall Distributed Auth

### 19 = Uninstall Client SDK

### 21 = Redeploy console password services common

### 26 = Undeploy console password services common

###

### SERVER_PROTOCOL is the protocol (http or https) used by the web

### container instance on which the Access Manager server has been or

### will be deployed.

###

### SERVER_NAME is the name of the host on which

### the Access Manager server (/amserver) has been or will be deployed.

###

### SERVER_HOST is the fully qualified domain name of the host on which

### the Access Manager server (/amserver) has been or will be deployed.

###

### SERVER_PORT is the port on SERVER_HOST on which the Access Manager

### server has been or will be deployed.

###

### ADMIN_PORT is the port on which the administration

### instance will listen for connections.

###
### ADMIN_PORT default values are:

### 4849 => Application Server 8.x
```

```
### 7001 => WebLogic 8.x

### 9080 => Websphere 5.1

### 8989 => Webserver 7.0

###

### DS_HOST is the fully qualified domain name of the host on which the

### directory server is running.

###

### DS_HOST is the fully qualified domain name of the host on which the

### directory server is running.

###

### DS_DIRMGRPASSWD is the password for the directory manager.

###

### ROOT_SUFFIX is the initial or root suffix of the directory server.

###

### ADMINPASSWD, the amadmin password, and AMLDAPUSERPASSWD, the amldapuser

### password, must be set to different values

###

### COOKIE_DOMAIN contains the name(s) of the trusted DNS domain(s) that

### Access Manager returns to a browser when it grants a session ID to a user.

###

### AM_ENC_PWD is the password encryption key. In a multiserver installation,

### this parameter must have the same value as the other servers. By default,

###

### AM_ENC_PWD is set to "" which means that Access Manager will generate a
```

```
### random password encryption key.
###
### NEW_OWNER is the user which will have ownership of the Access Manager
### files.
###
### NEW_GROUP is the group which corresponds to NEW_OWNER. Solaris 8 and 9
### installations using root as NEW_OWNER should set this parameter to other.
### Solaris 10 and Linux installations using root as NEW_OWNER should set
### NEW_GROUP to root as the same default value.
###
### PAM_SERVICE_NAME is the name of the PAM service from the PAM
### configuration/stack that comes with the OS and is used for the Unix
### authentication module (normally 'other' for Solaris or 'password' for
### Linux)
###
### WEB_CONTAINER is the web container on which Access Manager will be
### configured and/or deployed. See supported values below.
###
### WEB_CONTAINER values can be:
### AS8 => Application Server 8.1
### WAS5 => IBM WebSphere 5.x
### WL8 => BEA WebLogic 8.x
### WS6 => Sun Web Server 6.x
### WS => Sun Web Server
```

```
################################################################################

DEPLOY_LEVEL=1

SERVER_PROTOCOL=http

# The following entries contain sample values!

# These should be modified for your specific installation

# and then uncommented (remove the # from the line)

#

SERVER_NAME=servername

SERVER_HOST=$SERVER_NAME.domain.com

SERVER_PORT=38080

ADMIN_PORT=4849

DS_HOST=domain.com

DS_DIRMGRPASSWD=dmpassword

ROOT_SUFFIX="dc=ROOT_SUFFIX,dc=com"

ADMINPASSWD=ampassword

AMLDAPUSERPASSWD=password

COOKIE_DOMAIN=.domain.com

AM_ENC_PWD="passwordpassword"

NEW_OWNER=root

NEW_GROUP=root

PAM_SERVICE_NAME=root

WEB_CONTAINER=AS8

################################################################################
```

```
### DISTAUTH_PROTOCOL is the protocol (http or https) used by the web
### container instance on which the Distributed Authentication web
### application has been or will be deployed.
###
### DISTAUTH_HOSTNAME is the fully qualified host where a distributed
### authentication server is located.
###
### DISTAUTH_PORT is the port on DISTAUTH_HOST on which the distributed
### authentication server has been or will be deployed.
###
### APPLICATION_USER is the user name for the application.
###
### APPLICATION_PASSWD is the users password for the application.
###
### AM_ENC_SECRET sets the password encryption secret key from the Server.
###
### AM_ENC_LOCAL sets the password encryption key.
###
### DEBUG_LEVEL is used to configure the debug service. Possible values
### are: error | warning | message
###
### DEBUG_DIR is directory where the debug files will be created.
###
################################################################################
```

```
DISTAUTH_PROTOCOL=http

#DISTAUTH_HOST=distAuth_sample.com

#DISTAUTH_PORT=80

#APPLICATION_USER=username

#APPLICATION_PASSWD=11111111

#AM_ENC_SECRET=""

#AM_ENC_LOCAL=""

DEBUG_LEVEL=error

DEBUG_DIR=/var/opt/SUNWam/logs

################################################################################

### SSL_PASWORD is used when a container is automatically restarted

################################################################################

SSL_PASSWORD="sample"

################################################################################

### BASEDIR is the directory in which the Access Manager jars, libraries,

### utilities, etc. will be installed.

###

### PLATFORM_DEFAULT indicates /opt on Solaris and /opt/sun on Linux.

###

### To use a base directory other than the default, set the BASEDIR variable

### below to the directory you want to use.
```

```
################################################################################

BASEDIR=/space/AM

################################################################################

### CONSOLE_HOST is the fully qualified domain name of the host on which

### the Access Manager Console has been or will be deployed.

###

### CONSOLE_PORT is the port on CONSOLE_HOST on which the Access Manager

### console has been or will be deployed.

###

### CONSOLE_PROTOCOL is the protocol (http or https) used by the web

### container instance on which the Access Manager console has been or

### will be deployed.

################################################################################

CONSOLE_HOST=$SERVER_HOST

CONSOLE_PORT=$SERVER_PORT

CONSOLE_PROTOCOL=$SERVER_PROTOCOL

################################################################################

### CONSOLE_REMOTE should be set to true if the Access Manager console

### is or will be running on a different web container instance than the

### the Access Manager server.

################################################################################

CONSOLE_REMOTE=false

################################################################################
```

```
### SERVER_DEPLOY_URI is the URI prefix for accessing content associated
### with the Access Manager server and Access Manager 7.0 administration
### console.
###
### CONSOLE_DEPLOY_URI is the URI prefix for accessing content associated
### with the Access Manager 6.3 administration console.
###
### PASSWORD_DEPLOY_URI is the URI prefix for accessing content associated
### with the Access Manager password reset module.
###
### COMMON_DEPLOY_URI is the URI prefix for accessing content associated
### with the Access Manager common domain services.
###
### DISTAUTH_DEPLOY_URI is the URI prefix for accessing content associated
### with the Distributed Authentication web application.
###
### CLIENT_DEPLOY_URI is the URI prefix for accessing content associated
### with the Client SDK.
################################################################################
SERVER_DEPLOY_URI=/amserver
CONSOLE_DEPLOY_URI=/amconsole
PASSWORD_DEPLOY_URI=/ampassword
COMMON_DEPLOY_URI=/amcommon
DISTAUTH_DEPLOY_URI=/amdistauth
```

```
CLIENT_DEPLOY_URI=/amclient

############### Configuration for Directory Server ########################

#############################################################################
### DIRECTORY_MODE is a numeric value which determines how Access Manager
### will configure the directory server.
###
### DIRECTORY_MODE possible values
###1 = Default (Fresh new installation of a DIT)
###
###2 = Existing DIT (Naming attributes and object classes are same,
### to load installExisting.ldif and umsExisting.xml. Also
### do the tag swapping.)
###
###3 = Existing DIT Manual(Naming attributes and object classes are
### different, so do NOT load installExisting.ldif and
### umsExisting.xml. Do the tag swapping only. Do NOT delete
### ldif files, and amserveradmin after installation. All the
### ldif files and the services will be loaded manually by the
### user later.)
###
###4 = Existing Multiserver(Only do tag swapping). It will be
### modified later to add more features. Currently it is same
### as option 5.
```

```
###

###5 = Existing upgrade (Only do tag swapping)

###

### DS_PORT is the port on which the directory server on DS_HOST is running.

###

### DS_DIRMGRDN is the DN (distinguished name) of the directory manager,

### the user who has unrestricted access to Directory Server.

###

### USER_NAMING_ATTR is the user naming attribute in the directory server.

###

### ORG_NAMING_ATTR is the organization naming attribute in the directory

### server.

###

### ORG_OBJECT_CLASS is the organization object class.

###

### USER_OBJECT_CLASS is the user object class.

###

### DEFAULT_ORGANIZATION is the default organization name.

################################################################################

DIRECTORY_MODE=1

DS_PORT=389

DS_DIRMGRDN="cn=Directory Manager"

USER_NAMING_ATTR=uid

ORG_NAMING_ATTR=o
```

```
ORG_OBJECT_CLASS=sunismanagedorganization

USER_OBJECT_CLASS=inetorgperson

DEFAULT_ORGANIZATION=


############### Required for Active Directory Configuration ###############

###############################################################################

### To store service schema and services in a different datastore namely,

### Active Directory Support, change the values here.

### CONFIG_AD set to true if AD is chosen as configuration data store.

### Active Directory schema will be loaded.

###############################################################################


CONFIG_AD="false"

CONFIG_SERVER=$DS_HOST

CONFIG_PORT=$DS_PORT

CONFIG_ADMINDN="cn=dsameuser,ou=DSAME Users"

CONFIG_ADMINPASSWD="$ADMINPASSWD"


###############################################################################

### JAVA_HOME is the JDK installation directory. This value of this

### parameter will be the JDK which will be used by Access Manager

### utilities (for example, the amadmin script).

###############################################################################

JAVA_HOME=/usr/jdk/entsys-j2se
```

```
################################################################################
### AM_REALM indicates whether realm mode should be enabled.
### If AM_REALM is set to disabled, then Access Manager will operate in
### compatiblity mode to use Access Manager 6.x directory information.
################################################################################
AM_REALM=disabled

################################################################################
### PLATFORM_LOCALE is the locale of Access Manager.
################################################################################
PLATFORM_LOCALE=en_US

XML_ENCODING=ISO-8859-1

################################################################################
### NEW_INSTANCE should be set to true when deploying Access Manager to
### a new user-created web container instance.
################################################################################
NEW_INSTANCE=false

############### Required for Application Server 8.x ######################

################################################################################
### AS81_HOME is the directory which contains the Application Server 8.1
### utilities (bin) directory. The default value for Linux installations
```

```
### should be /opt/sun/appserver.
###
### AS81_PROTOCOL is the protocol (http or https) which is being used
### by the Application Server instance.
###
### AS81_HOST is the fully qualified domain name on which the Application
### Server instance listens for connections.
### If using Distributed Authentication this should be set to the same
### value as DISTAUTH_HOST.
###
### AS81_PORT is the port on which the Application Server instance will
### listen for connections.
###
### AS81_ADMINPORT is the port on which the Application Server administration
### instance will listen for connections.
###Default for Application Server is 4849
###
### AS81_ADMIN is the user ID of the Application Server administrator.
###
### AS81_ADMINPASSWD is the password of the Application Server administrator.
###
### AS81_INSTANCE is the name of the Application Server instance on which
### Access Manager will be configured and/or deployed.
###
```

```
### AS81_DOMAIN is the name of the Application Server domain in which the
### Application Server instance exists.
###
### AS81_INSTANCE_DIR is the path to the directory where the Application
### Server instance stores its files. The default value for Linux
### installations is /var/opt/sun/apppserver/domains/domain1.
###
### AS81_DOCS_DIR is the document root of the Application Server instance
### on which Access Manager will be configured and/or deployed. The default
### value for Linux installations is
### /var/opt/sun/appserver/domains/domain1/docroot.
###
### AS81_ADMIN_IS_SECURE (true / false) specifies whether the Application
### Server administration instance is using SSL. By default this should be
### set to true.
#############################################################################

AS81_HOME=/space/AS/appserver
AS81_PROTOCOL=$SERVER_PROTOCOL
AS81_HOST=$SERVER_HOST
#AS81_HOST=$DISTAUTH_HOST
AS81_PORT=$SERVER_PORT
AS81_ADMINPORT=$ADMIN_PORT
AS81_ADMIN=admin
AS81_ADMINPASSWD="password"
```

```
AS81_INSTANCE=server1

AS81_DOMAIN=domain1

AS81_INSTANCE_DIR=/space/AS/nodeagents/node1/server1

AS81_DOCS_DIR=/space/AS/nodeagents/node1/server1/docroot

AS81_ADMIN_IS_SECURE=true


############### Required for BEA WebLogic 8.1.x ################################


###############################################################################

### WL8_HOME is the installation directory for WebLogic 8.1.

###

### WL8_PROJECT_DIR is the name of the WebLogic projects directory.

###

### WL8_DOMAIN is the name of the WebLogic domain in which Access Manager will

### be configured and/or deployed.

###

### WL8_CONFIG_LOCATION should be set to the parent directory of the

### directory where the WebLogic start script (by default startWebLogic.sh)

### exists for the domain on which Access Manager is being deployed

###

### WL8_SERVER is the name of the WebLogic server instance in which

### Access Manager will be configured and/or deployed.

###

### WL8_INSTANCE is the directory under which the WebLogic libraries

### and utility classes reside.
```

```
###
### WL8_PROTOCOL is the protocol (http or https) which is being used by the
### WebLogic instance.
###
### WL8_HOST is the hostname on which the WebLogic instance is listening
### for connections.
### If using Distributed Authentication this should be set to the same
### value as DISTAUTH_HOST.
###
### WL8_PORT is the port on which the WebLogic instance is listening
### for HTTP connections.
###Default for WebLogic is 7001
###
### WL8_SSLPORT is the port on which the WebLogic instance is listening
### for HTTPS connections.
###Default for WebLogic is 7002
###
### WL8_ADMIN is the username for the WebLogic administrator.
###
### WL8_PASSWORD is the password for the WebLogic administrator.
###
### WL8_JDK_HOME is the base directory of the JDK in which WebLogic is
### running.
#############################################################################
```

```
WL8_HOME=/usr/local/bea

WL8_PROJECT_DIR=user_projects

WL8_DOMAIN=mydomain

WL8_CONFIG_LOCATION=$WL8_HOME/$WL8_PROJECT_DIR/domains

WL8_SERVER=myserver

WL8_INSTANCE=$WL8_HOME/webLogic81

WL8_PROTOCOL=$SERVER_PROTOCOL

WL8_HOST=$SERVER_HOST

#WL8_HOST=$DISTAUTH_HOST

WL8_PORT=$SERVER_PORT

WL8_SSLPORT=$ADMIN_PORT

WL8_ADMIN="webLogic"

WL8_PASSWORD="$ADMINPASSWD"

WL8_JDK_HOME=$WL8_HOME/jdk142_04


############### Required for IBM WebSphere 5.1 ################################


#############################################################################

### WAS51_HOME is the WebSphere 5.1 installation directory.

###

### WAS51_JDK_HOME is the base directory of the WebSphere JDK.

###

### WAS51_CELL is the name of cell in which the WebSphere instance resides.

###
```

```
### WAS51_NODE is the name of node on which the WebSphere instance resides.
###
### WAS51_INSTANCE is the name of the WebSphere instance on which Access
### Manager will be configured and/or deployed.
###
### WAS51_PROTOCOL is the protocol (http or https) which is being used by the
### WebSphere instance.
###
### WAS51_HOST is the hostname on which the WebSphere instance is listening
### for connections.
### If using Distributed Authentication this should be set to the same
### value as DISTAUTH_HOST.
###
### WAS51_PORT is the port on which the WebSphere instance is listening
### for HTTP connections.
###Default for WebSphere is 9080
###
### WAS51_SSLPORT is the port on which the WebSphere instance is listening
### for HTTPS connections.
###
### WAS51_ADMIN is the username for the WebSphere administrator.
###
### WAS51_ADMINPORT is the port on which the WebSphere administration
### instance will listen for connections.
```

```
###Default for WebSphere is 9090

#############################################################################

WAS51_HOME=/opt/WebSphere/AppServer

WAS51_JDK_HOME=/opt/WebSphere/AppServer/java

WAS51_CELL=$SERVER_NAME

WAS51_NODE=$SERVER_NAME

WAS51_INSTANCE=server1

WAS51_PROTOCOL=$SERVER_PROTOCOL

WAS51_HOST=$SERVER_NAME

#WAS51_HOST=$DISTAUTH_HOST

WAS51_PORT=$SERVER_PORT

WAS51_SSLPORT=9081

WAS51_ADMIN="admin"

WAS51_ADMINPORT=$ADMIN_PORT

############### Required for Web Server ##############################

#############################################################################

### WS_INSTANCE is the name of the Web Server instance on which Access

### Manager will be configured and/or deployed. The value of this parameter

### should correspond to a directory beneath WS61_HOME. The default for WS6.x

### is https-$SERVER_HOST. For WS7.x the default is $SERVER_HOST.

###

### WS_CONFIG is the name of the Web Server configuration.

###
```

```
### WS_HOME is the Web Server instance directory. The default value
### for Linux installations is /var/opt/sun/webserver7/$WS_INSTANCE.
###
### WS_PROTOCOL is the protocol (http or https) which is being used by
### the Web Server instance.
###
### WS_HOST is the fully qualified domain name on which the Web Server
### instance is listening for connections.
### If using Distributed Authentication this should be set to the same
### value as DISTAUTH_HOST.
###
### WS_PORT is the port on which WS_INSTANCE will listen for connections.
###Default for Webserver is 80
###
### WS_ADMINPORT is the port on which the Web Server administration
### instance will listen for SSL connections.
###Default for Webserver is 8989
###
### WS_ADMIN is the user ID of the Web Server administrator.
###
### WS_PASSWORD is the password for the Webserver administrator (defaults to
### the same value as the amadmin password).
###
#############################################################################
```

```
WS61_INSTANCE=https-$SERVER_HOST

WS61_HOME=/opt/SUNWwbsvr

WS61_PROTOCOL=$SERVER_PROTOCOL

WS61_HOST=$SERVER_HOST

WS61_PORT=$SERVER_PORT

WS61_ADMINPORT=$ADMIN_PORT

WS61_ADMIN="admin"


WS_INSTANCE=$SERVER_HOST

WS_CONFIG=$SERVER_HOST

WS_HOME=/var/opt/SUNWwbsvr7

WS_PROTOCOL=$SERVER_PROTOCOL

WS_HOST=$SERVER_HOST

#WS_HOST=$DISTAUTH_HOST

WS_PORT=$SERVER_PORT

WS_ADMINPORT=$ADMIN_PORT

WS_ADMIN="admin"

WS_ADMINPASSWD=$ADMINPASSWD


###############################################################################
```

Content of the *example14.xml* File

```
<?xml version = "1.0" encoding = "UTF-8"?>

<PortalServerConfiguration xmlns:xsi="http://www.w3.org/2001
/XMLSchema-instance"

xsi:noNamespaceSchemaLocation="file:///opt/SUNWportal
/lib/psconfig.xsd" SchemaVersion="1.0">

<Configure ConfigurationHostName="hostname"
 SystemUser="root" SystemGroup="root" Validate="true">

<SharedComponents

JavaHome="/usr/jdk/entsys-j2se"

CacaoProdDir="/usr/lib/cacao"

CacaoConfigDir="/etc/cacao/instances/default"

SharedLibDir="/usr/share/lib"

PrivateLibDir="/usr/share/lib"

JDMKLibDir="/opt/SUNWjdmk/5.1/lib"

NSSLibDir="/usr/lib/mps/secv1"

JSSJarDir="/usr/share/lib/mps/secv1"

WebNFSLibDir="/opt/SUNWebnfs"

DerbyLibDir="/opt/SUNWderby/lib"

AntLibDir="/usr/sfw/lib/ant"

AntHomeDir="/usr/sfw"

RegistryLibDir="/opt/SUNWsrvc-registry/lib"

MFWKLibDir="/opt/SUNWmfwk/lib"

MFWKBinDir="/opt/SUNWmfwk/bin"

JAXLibDir="/opt/SUNWjax/share/lib"

/>
```

```
<AccessManager>

<InstallationDirectory

ProdDir="/opt/SUNWam"

DataDir="/var/opt/SUNWam"

ConfigDir="/etc/opt/SUNWam/config"

ConfigFile="AMConfig.properties"

/>

<UserCredentials

AdministratorUID="amadmin"

AdministratorUserPassword="ampassword"

LDAPUserId="amldapuser"

LDAPUserIdPassword="password"

DirectoryManagerDn="cn=Directory Manager"

DirectoryManagerPassword="dmpassword"/>

</AccessManager>

<PortalConfiguration>

<InstallationDirectory

ProdDir="/opt/SUNWportal"

DataDir="/var/opt/SUNWportal"

ConfigDir="/etc/opt/SUNWportal"/>

<ComponentsToConfigure>

<component>portalserver</component>

<component>sracore</component>

<component>netletproxy</component>
```

```
<component>rewriterproxy</component>

</ComponentsToConfigure>

<SearchServer SearchServerID="mySearch">

<WebContainerProperties

Host="hostname"

Port="38080"

Scheme="http"

WebContainerInstallDir="/opt/SUNWappserver/appserver"

WebContainerInstanceName="server1"

WebContainerDomainName="domain1"

WebContainerInstanceDir="/var/opt/SUNWappserver/nodeagents/node1/server1"

WebContainerDocRoot="/var/opt/SUNWappserver/nodeagents/node1/docroot"

WebContainerAdminHost="hostname"

WebContainerAdminPort="4849"

WebContainerAdminScheme="https"

WebContainerAdminUid="admin"

WebContainerAdminPassword="password"

WebContainerMasterPassword="password"

WebContainerType="SJSAS81"

/>

</SearchServer>

<PortalServer PortalAccessURL="http://hostname:38080/portal"

PortalID="myPortal"

PortalWebappURI="/portal"
```

```
SearchServerID="mySearch">

<SamplePortal>

<Sample Name="DeveloperPortal"/>

<Sample Name="EnterprisePortal"/>

<Sample Name="CommunityPortal"/>

</SamplePortal>

<Instance InstanceID="myInstance">

<WebContainerProperties

Host="hostname"

Port="38080"

Scheme="http"

WebContainerInstallDir="/opt/SUNWappserver/appserver"

WebContainerInstanceName="server1"

WebContainerDomainName="domain1"

WebContainerInstanceDir="/var/opt/SUNWappserver/nodeagents/node1/server1"

WebContainerDocRoot="/var/opt/SUNWappserver/nodeagents/node1/docroot"

WebContainerAdminHost="hostname"

WebContainerAdminPort="4849"

WebContainerAdminScheme="https"

WebContainerAdminUid="admin"

WebContainerAdminPassword="password"

WebContainerMasterPassword="password"

WebContainerType="SJSAS81"
```

```
/>

</Instance>

</PortalServer>

<SecureRemoteAccessCore

GatewayProtocol="https"

PortalServerDomain="domain.com"

GatewayPort="443"

GatewayProfileName="default"

LogUserPassword="password"/>

<NetletProxy Profile="default">

<SRAInstance

Protocol="https"

Host="hostname"

Port="10555"

IPAddress="10.12.147.222"

LogUserPassword="password"

StartInstance="true"/>

</NetletProxy>

<RewriterProxy Profile="default">

<SRAInstance

Protocol="https"

Host="hostname"

Port="10443"

IPAddress="10.12.147.222"
```

```
LogUserPassword="password"

StartInstance="true"/>

</RewriterProxy>

<CertificateInformation

Organization="Organization"

Division="Software"

CityOrLocality="City"

StateProvince="State"

CountryCode="Countrt"

CertificateDatabasePassword="password"/>

</PortalConfiguration>

</Configure>

</PortalServerConfiguration>
```

Index

D

E

H

I

J

L

M

N

O

P

R

S

T

U

V

W

X