Sun™ ONE Portal Server 6.0 can be deployed on a Sun™ ONE Application Server using it as its web application container.

This supplement contains the following sections:

- What is New in the Sun ONE Portal Server 6.0 to Support (Run on) Sun ONE Application Server
- Hardware and Software Requirements
- Installing Sun ONE Application Server
- Installing the Sun ONE Portal Server Software
- Installing Secure Remote Access
- Installing the Sun ONE Portal Server into a Secure Application Server Instance
- Setting Up the Sun ONE Portal Server to Use Secure External LDAP Directory Server
- Setting Up LDAP Replication for the Sun ONE Portal Server
- Known Problems and Limitations
- How to Report Problems
- Where to Find More Information
Familiarity with Sun ONE Portal Server 6.0 Release Notes, Sun ONE Portal Server 6.0 Installation Guide, and Sun ONE Portal Server 6.0 Administrator’s Guide are recommended before using this supplement. The installation information only describes the procedure for installing the Sun ONE Portal Server with default settings and includes the sample desktop.

About This Document

This section provides details about this document. It contains the following topics:

- Typographic Conventions
- Command-Line Prompts

Typographic Conventions

This is a three column table. The first column gives the typeface, the second its meaning and the third an example. This information is also detailed after the table.

<table>
<thead>
<tr>
<th>Typeface</th>
<th>Meaning</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>AaBbCc123</td>
<td>The names of commands, files, and directories; on-screen computer output</td>
<td>Edit your .login file. Use ls -a to list all files. machine_name% You have mail.</td>
</tr>
<tr>
<td>AaBbCc123</td>
<td>What you type, when contrasted with on-screen computer output</td>
<td>machine_name% su Password:</td>
</tr>
<tr>
<td>AaBbCc123</td>
<td>Book titles, new words or terms, words to be emphasized or glossary terms.</td>
<td>Read Chapter 6 in the User’s Guide. These are called class options. You must be superuser to do this.</td>
</tr>
<tr>
<td>AaBbCc123</td>
<td>Command-line variable; replace with a real name or value</td>
<td>To delete a file, type rm filename.</td>
</tr>
</tbody>
</table>

NOTE The settings on your web browser may differ from these.
Monospaced Font

Monospaced font is used for any text that appears on the computer screen or text that you should type. It is also used for file names, distinguished names, functions, and examples.

Bold Monospaced Font

Bold monospaced font is used to represent text within a code example that you should type. For example, you might see something like this:

```
$ dpadmin list -n TemplateTableContainer -u "uid=amAdmin,ou=people,o=sesta.com,o=isp" -w joshua -d "o=sesta.com,o=isp"
```

In this example, `dpadmin list` is what you would type on the command line to list part of a display profile.

Italicized Font

Italicized font is used to represent text that you enter using information that is unique to your installation (for example, variables). It is used for server paths and names and account IDs.

Square or Straight Brackets

Square (or straight) brackets [] are used to enclose optional parameters. For example, in this document you will see the usage for the `par` command described as follows:

```
par import -r uid -p password -a [-d] [-v] parfile [dn|global]
```

The presence of `[-d]`, `[-v]`, and `[dn|global]` indicates that there are optional parameters that may be added to the `par` command.

Command-Line Prompts

Command-line prompts (for example, % for a C-Shell, or $ for a Korn or Bourne shell) Vary according to the operating system environment you are using. However, you should enter the command as it appears in the document unless specifically noted otherwise.
What is New in the Sun ONE Portal Server 6.0 to Support (Run on) Sun ONE Application Server

This section summarizes enhancements implemented in Sun ONE Portal Server 6.0 so that it can be deployed on the Sun ONE Application Server.

The visible changes are in the Portal Server install script. The script asks you which deployment type you are using. Once you select Sun ONE Application Server, the install script sets up the appropriate default directories and adds a number of .war files that facilitate running the Portal Server on a Sun ONE Application Server.

Since you are using the Sun ONE Application Server, the install script needs to know what the Application Server directory is (/opt/SUNWappserver7, the default) and what the Application Server instance (server1) is. The Portal Server installation summary lists the deployment information related to the application server.

Overview of Products

A portal is a doorway or entry point to an aggregate of pieces of information. What the end user sees when visiting a portal is a set of HTML pages called a desktop. This desktop is made up of an aggregate of channels. Each channel displays a specific type of information. A channel is an area on the portal desktop; it can be small area showing something like stock quotes, it can be a container that aggregates other channels, or it can be the complete page.

The Sun ONE Portal Server 6.0 provides a portal that is flexible, versatile, customizable, and extensible. An administrator can manage users and content from a single administration console. The administrator can choose how a user logs in and what a user sees. The organization a user belongs to and what a user’s role is determine what content is visible to a user, as well as what services and applications are available. The content may be a mix of XML, HTML, RSS, WSDL, and JavaServer Pages™ (JSP™) or something that the administrator has created by extending the public APIs.

The Sun ONE Application Server is a Java™ application server that enables deployment of web applications, such as the Sun ONE Portal Server, and web services. The Sun ONE Application Server implements the J2EE™ platform specification and supports servlets, JSPs, Enterprise JavaBeans™ (EJB™), and other platform services. In addition, the Sun ONE Application Server allows you to use the Sun ONE Web Server to serve up static HTML and image files as well as JSPs and servlets.
Hardware and Software Requirements

Before installing the Sun ONE Portal Server software, ensure that your system meets the following requirements:

- Hardware Requirements
- Software Requirements
- Operating System Requirements, including patches

Hardware Requirements

For a new installation of the software, your system must meet the following minimal hardware requirements:

- 1 450 MHz CPU or better
- 512 Mbytes of RAM
- 1 Gbyte of hard drive swap space
- 1 Gbyte of disk space

Software Requirements

The software discussed here is required for a successful installation of the Sun ONE Portal Server software. Other versions of these software products are not supported.

- Sun ONE Application Server 7.0
- iPlanet™ Directory Server Access Management Edition 5.1a, included with the Portal Server installation.
- Java™ Development Kit (JDK™) 1.4.1_01, which is installed with S1AS

Space Requirements

These requirements are the ones that are checked for in the Portal Server installation script. This is a three column table. The first column lists the directory, the second the size in megabytes, and the third adds relevant comments.
Hardware and Software Requirements

Operating System Requirements

The Sun ONE Portal Server software requires at least a user distribution of the Solaris™ 8 or Solaris 9 software as the operating system. Solaris 8 requires the following operating system patches as well for a successful installation of the product:

- 109326-03
- 108434-03
- 108827-34
- 112438-01

Table 1  Space Requirements

<table>
<thead>
<tr>
<th>Directory</th>
<th>Size</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>/etc/opt</td>
<td>200 MB</td>
<td></td>
</tr>
<tr>
<td>/var/opt</td>
<td>200 MB</td>
<td>Add more for extended logging.</td>
</tr>
<tr>
<td>/usr</td>
<td>50 MB</td>
<td>If installing JDK 1.3.1_04.</td>
</tr>
<tr>
<td>Application server base directory</td>
<td>50 MB</td>
<td>If using migration tools.</td>
</tr>
<tr>
<td>DS_BASEDIR (/usr/ldap)</td>
<td>300 MB</td>
<td>For Directory Server.</td>
</tr>
<tr>
<td>Application server base directory</td>
<td>200 MB</td>
<td>For Portal Server only.</td>
</tr>
<tr>
<td>Application server base directory</td>
<td>500 MB</td>
<td>For Secure Remote Access on the same machine as the Portal Server software.</td>
</tr>
<tr>
<td>BASEDIR (/opt)</td>
<td>100 MB</td>
<td>For Secure Remote Access support on the machine that has the Portal Server software when the gateway is on a separate machine.</td>
</tr>
</tbody>
</table>
Installing Sun ONE Application Server

These are the minimum required patches. The last two digits of the patch number are the minor revision number. If updates to the patch have been released, install the most recent patch revision (the one with the higher revision number). Typically, these patches are made obsolete when a new patch is released and only the most recent patch is available at the SunSolve site. Please review the readme for each patch to find out what dependencies or patches may be required.

Installing Sun ONE Application Server

The Sun ONE Application Server needs to be installed before you install the Sun ONE Portal Server software. Use the standard Sun ONE Application Server install instructions.

Note the values you enter during the install.

1. Log in with root privileges to the server on which to install the SUN ONE Application Server software.

2. Change directories to the directory where the Sun ONE Application Server installer is. For example, if you have downloaded and extracted the application server installation files to /temp/sun-appserver7, type

   # cd /temp/sun-appserver7

3. Start the install.

   To run the GUI-based installation program, run the setup program without any options as follows:

   # ./setup

   To run the terminal-based, interactive installation program, run the setup program with the -console option. For example:

   # ./setup -console

4. To continue the installation, accept the license agreement

5. Specify the installation directory for the application server and create the directory if necessary. The default is /opt/SUNWappserver7.
6. Specify the application server components to install. The components available are:
   - Application Server
   - Sample Applications
   - Pointbase Server
   - Admin Client
   - Support for Sun ONE Studio 4, Enterprise Edition for Java
   - Java 2 SDK 1.4.0_02

7. Specify the product configuration directory for the application server and create the directory if necessary. The default is /etc/opt/SUNWappserver7.

8. Specify the default server directory for the application server and create the directory if necessary. The default is /var/opt/SUNWappserver7.

9. Specify the admin user name and password. The default user name is admin.

10. Specify the admin server port. The default is 4848.

11. Specify the HTTP server port. The default is 80. Port specified must not be used by other applications or the installation terminates.

12. Confirm the settings and proceed with the install.

   The installation successful message displays.

13. To upgrade the license, type “yes” to proceed to the upgrade license screen, and enter the license key at the prompt.

To run the Sun ONE Application Server, change directories to the directory containing the application server administration utility. For example if application server was installed in the default installation directory of /opt/SUNWappserver7, the admin utility is in /opt/SUNWappserver7/bin. From this directory, enter the following to start the application server:

```
# ./asadmin start-appserv
```

**NOTE** The Sun ONE Application Server needs to be running for the Sun ONE Portal Server software installation.
Installing the Sun ONE Portal Server Software

After you download the software into /tmp/ps, unzip it and run the tar extract command. For the Sun ONE Portal Server 6.0, type:

```
# gunzip -dc ps-6.0-sl-us.sparc-sun-solaris.tar.gz | /usr/bin/tar xvf -
```

This installation example only gives the procedure for installing the Sun ONE Portal Server with default settings, which includes the sample desktop.

**NOTE**  
Do not use this procedure if you are planning to run the portal server on an SSL-enabled application server instance. To run the portal server on an SSL-enabled application server, you should secure the application server instance before you install the Sun ONE Portal Server software. See “Installing the Sun ONE Portal Server into a Secure Application Server Instance,” on page 15 for information.

The installation script sets the parameters needed. You supply the Sun ONE Application Server password and Portal Server passphrase to complete the install.

**NOTE**  
The Sun ONE Portal Server software can only be installed in the default directory.

1. Go to the directory where the portal server software is, then type the install command:

   ```
   # ./pssetup
   ```

2. After you have accepted the licensing agreement, select option 1, Install Portal Server.

3. Select option 1, Sun ONE Application Server, as the deployment type.

4. This installs the portal server with these defaults.

**Application Server summary**

```
Directory: /opt/SUNWappserver7
Domain: /var/opt/SUNWappserver7/domains/domain1
```
5. Accept the default settings if they are correct, otherwise change as necessary.
6. Enter the password for the Sun ONE Application Server and confirm it.
7. Enter a passphrase for the portal server and confirm it.
   The install script finishes installing the portal server.
8. Check the `/var/sadm/install/logs/pssetup.pid/setup.log` file for errors.
9. Stop and restart the application server.
10. Test the portal server installation by launching the portal desktop in a browser by using:

   http://full-hostname:listen-port/portal/dt

   If the sample desktop displays without any exception, then your portal server installation is good.

Installing Secure Remote Access

After you download the software into /tmp/ps-sra, unzip it and run the tar extract command. For the Sun ONE Portal Server 6.0 with Secure Remote Access (SRA) for the Sun ONE Application Server, type:

   # gunzip -dc ps-sra-6.0-s1-us.sparc-sun-solaris8.tar.gz | /usr/bin/tar xvf -


1. Go to the directory where the portal server software is, then type the install command:

   # ./pssetup

   a. When installing the Sun ONE Portal Server software portion, make the same selections as described in the Installing the Sun ONE Portal Server Software section.

   b. After installing the portal server software, stop and restart the Sun ONE Application Server before installing the gateway.

   c. When installing the gateway on the same server as the portal server software, the base directory can be anything; using the /opt/SUNWappsolver7 directory as the base directory is not necessary.

   d. After installing the gateway, you need to restart the portal server and the gateway.

2. For each gateway profile, in the mime mappings there is an entry similar to:

   JAVASCRIPT=application/x-javascript

   Replace this entry with:

   JAVASCRIPT=application/x-javascript:text/javascript

   This is so the admin console works properly through the gateway.
3. After doing this change, the profile has to be saved and the gateway restarted.

4. Go to the /var/opt/SUNWappserver7/domains/domain1/server1/config directory and modify the server.policy file. The correct lines are:

   ```
   permission java.net.SocketPermission "*", "connect, accept, listen, resolve"
   
   permission java.io.FilePermission "<<ALL FILES>>", "read, write, execute, delete"
   ```

   This is needed for NetFile to work.

   Some of the files are placed in different directories when using Secure Remote Access with the Sun ONE Application Server software.

   The rewriter samples are accessed from a web browser using `portal_server_URL/portal/samples/rewriter`. These samples are described in the Sun One Portal Server, Secure Remote Access Administrator’s Guide, which lists their location as `portal_server_URL/rewriter`.

   The MIME types configuration file is now in the `InstallDir/SUNWps/samples/config/netfile` directory. In a Sun ONE Portal Server installation not using the Sun ONE Application Server software, the MIME type configuration file is in the `InstallDir/SUNWam/servers/instance_name/config` directory.

---

**NOTE**

The Sun ONE Application Server console is not accessible through the gateway.

The SRA gateway and SRA NetFile do not work if the Portal Server software is configured for session failover.

---

**Setting Additional Parameters for Gateway Reliability**

When running the Sun ONE Portal Server with Secure Remote Access, you should configure your implementation as follows to achieve optimal performance:

- Set up notifications between the Portal Server instance and the gateway in open mode.
- Set the Java -Dhttp.keepAlive option to false on the Portal Server and the gateway.
• Set the notification threadpool size to 200.

Perform the following configure your implementation.

1. Go to the /opt/SUNWappserver7/domains/domain1/server1/config directory and modify the AmConfig.properties file to set the notification threadpool size for the application server. At the top of the file just below the following lines:

Sun, Sun Microsystems, the Sun logo, and iPlanet * are trademarks or registered trademarks of Sun Microsystems, * Inc. in the United States and other countries.

Add the following lines to set the threadpool size to 200:

/*Notification Thread Pool Size*/
com.iplanet.am.notification.threadpool.size=200

2. Log into the Sun ONE Portal Server administration console with user name amadmin and the passphrase you entered during the installation.

3. Select Service Management in the View menu.

4. Select SRAP Configuration and then Gateway.

5. Select the default server and click Edit.

6. Check the Enable HTTP Connections checkbox.

7. In the HTTP Port field, type 80 and Click Save.

8. Log in to the Sun ONE Application Server administration console as administrator (admin) by entering http://fullservername:port in your browser’s web address field. The default port is 4848. Use the password you entered at installation.

9. Select the application server Instance on which you installed the Identity Server.

10. Click JVM Settings and then JVM Options.

11. In the JVM Option field, enter the following string:

-Dhttp.keepAlive=false

12. Click Add and then Save.

13. Select the application server instance on which you will install the Sun ONE Portal Server software.

The right pane shows that the configuration has changed.
14. Click Apply Changes.

15. Click Restart.

The application server should automatically restart.

16. On the server in which the gateway is installed, go to the 
   /opt/SUNWps/bin/perf directory and enter the following to run a script that 
   will set tuning parameters for the Sun ONE Portal Server: Secure Remote 
   Access product:
   
   ./srpperftune

17. Go to the /opt/SUNWam/lib directory and modify the AmConfig.properties 
   file to set the notification threadpool size for the gateway. At the top of the file 
   just below the following lines:

   Sun, Sun Microsystems, the Sun logo, and iPlanet 
   * are trademarks or registered trademarks of Sun Microsystems, 
   * Inc. in the United States and other countries.

   Add the following lines to set the threadpool size to 200:

   /*Notification Thread Pool Size*/
   com.iplanet.am.notification.threadpool.size=200

18. Go to the /opt/SUNWps/bin directory and modify the gateway file to set the 
    -Dhttp.keepAlive option to false and to increase the settings for the -Xms 
    and -Xmx heap size options. By default, the srpperftune script sets the -Xms 
    and -Xmx heap size options to 1024. In the line defining the CMD settings 
    options, increase the default values defined for -Xms and -Xmx options to 
    2048 and add the string -Dhttp.keepAlive=false. For example, the correct 
    lines would be

    CMD="$JAVA_HOME/bin/java -server -Xms2048M -Xmx2048M 
    -XX:+OverrideDefaultLibthread -XX:ThreadStackSize=128 
    -XX:MaxPermSize=128M -XX:PermSize=128M -XX:MaxNewSize=256M 
    -XX:NewSize=256M -Dhttp.keepAlive=false -classpath $CLASSPATH 
    $DEFINES $PROXY_DEFINES $INSTANCE_DEFINES 
    com.sun.portal.netlet.eproxy.EProxy"

19. Go to the /etc/opt/SUNWps directory and modify the 
    platform.conf.default file and set the gateway.protocol parameter to http 
    and gateway.port parameter to port 80 as follows:

    gateway.protocol=http
    gateway.port=80
20. Restart the gateway for the changes to take effect by typing the following command:

```
InstallDir/SUNWps/bin/gateway -n default start
```

*default* is the default gateway profile that is created during installation.

## Installing the Sun ONE Portal Server into a Secure Application Server Instance

Setting up the Sun ONE Portal Server to run on an SSL-enabled Sun ONE Application Server instance is a two-step procedure. First, secure the application server instance into which you will install the portal server. Then install the Sun ONE Portal Server software.

### To Secure the Application Server Instance

1. Log in to the Sun ONE Application Server administration console as administrator (admin) by entering `http://fullservername:port` in your browser’s web address field. The default port is 4848. Use the password you entered at installation.

2. Select the application server Instance on which you installed or will install the Identity Server.

   The right pane shows that the configuration has changed.

3. Click Apply Changes.

4. Click Restart.

   The application server should automatically restart.

5. In the left pane, click Security under the application server instance on which you installed or will install the Identity Server.

6. Click the Manage Database tab.

7. Click Create Database if it is not selected.

8. Enter the new database password and confirm it, then click the OK button.

   Ensure that you write down the database password for later use.
9. Once the Certificate Database has been created, click the Certificate Management tab.

10. Click the Request link if it is not selected.

11. Enter the Request data for the certificate as follows:
   a. Select if this is a new certificate or a certificate renewal.
      Many certificates expire after a set period of time, such as six months or a year. Some CAs will automatically send you a renewal.
   b. Specify how you want to submit the request for the certificate.
      • If the CA expects to receive the request in an email message, check CA Email and enter the email address of the CA. For a list of CAs, click List of available certificate authorities.
      • If you are requesting the certificate from an internal CA that is using the Sun ONE Certificate Server, click CA URL and enter the URL for the Certificate Server. This URL should point to the certificate server’s program that handles certificate requests.
   c. Select the cryptographic module for the key-pair file you want to use when requesting the certificate from the drop-down list.
   d. Enter the password for your key-pair file.
      This is the password you specified in Step 8.
   e. Enter your identification information.
      In the Common Name field, enter the full name of the server including the port number, for example myserver1.sesta.com:80. In the Locality and State or Province fields, spell out your location completely. Abbreviations, such as CA for California, will not work.

12. Click OK button, you will see a message such as:

   --BEGIN NEW CERTIFICATE REQUEST---
   afajsdlwqeroidsdai234rlkqwkelkasijlasnvnkbslajowijalsdkfalsdfldasf
   alsfjwoeirjoi2ejowdnlkswnvnpofijwoeijfwiepwerfoiqrjepwpfrwl
   --END NEW CERTIFICATE REQUEST--

13. Copy all of this text to a file. Click OK.

   Ensure that you get the Root CA certificate.
14. You will receive an e-mail certificate response containing the certificate, such as:

```
--BEGIN CERTIFICATE---
afaisdlwqeroidaoi234rlkqwelkasjlasndkbnbsljalsdjkjfasdf
alsfjawoeirjoi2ejowdnlkswnwofijwowieiffwepwerioqernoierwprwfrwl
--END CERTIFICATE--
```

15. Copy this text into your clipboard, or save the text into a file.

16. Go the Sun ONE Application Server administration console and click on Install link.

17. Select Certificate for This Server.

18. Enter the Certificate Database password in the Key Pair File Password field. It is the same password you entered in Step 8.

19. Paste the certificate into the provided text field, Message text (with headers), or enter the filename in the Message is in this file text box. Select the appropriate radio button.

20. Click OK button.

The browser displays the certificate, and provides a button to add the certificate.

21. Click Add Server Certificate.

22. Install the Root CA Certificate in the same manner described in Step 9 through Step 21. In Step 17, select Certificate for Trusted Certificate Authority instead.

23. Once you have completed installing both certificates, expand HTTP Server node in the left pane

24. Select HTTP Listeners under HTTP Server.


The browser displays the socket information.

26. Change the value of the port used by http-listener-1 from the value entered in Step 11 of “Installing Sun ONE Application Server,” on page 7 to a more appropriate value such as 443.

27. Select SSL/TLS Enabled.

29. Specify the Return server.
   This should match the common name specified in Step 11.
30. Click Save.
31. Select the application server instance on which you will install the Sun ONE Portal Server software.
   The right pane shows that the configuration has changed.
32. Click Apply Changes.
33. Click Restart.
   The application server should automatically restart.

To Install the Sun ONE Portal Server to Run as SSL

Once the Sun ONE Application Server instance is secured, install the Sun ONE Portal Server software as follows:

1. Go to the directory where the portal server software is, then type the install command:

   # ./pssetup

2. After you have accepted the licensing agreement, select option 1, Install Portal Server.
3. Select option 1, Sun ONE Application Server, as the deployment type.
4. Do not accept the default settings by entering n at the prompt.
5. Enter the application server password and server passphrase and hit return to accept the default values for each prompt except the Run SSL on <hostname>? y/[n] prompt. Do not accept the default value of n. Enter y at this prompt to use SSL.
6. At the What port should be used to access the portal server? [443] prompt, enter the port number that was entered as the http-listener1 in Step 26 of “To Secure the Application Server Instance,” on page 15.
7. Review the values that will be used for the install and if they are correct accept them.
8. Log in to the Sun ONE Application Server administration console as administrator (admin) by entering http://fullservername:port in your browser’s web address field. The default port is 4848. Use the password you entered at installation.

9. Select the application server instance on which you installed or will install the Sun ONE Identity Server. The right pane shows that the configuration has changed.

10. In the left pane, click Security under the application server instance on which you installed the Identity Server/Portal Server.

11. Select the JVM Settings Tab in the right pane.

12. Select the JVM Options link.

13. Type -Djava.protocol.handler.pkgs=com.iplanet.services.comm into JVM Option text field and click Add.

14. Click Save.

15. In the Sun ONE Application Server administration console, select the application server instance on which Identity Server is running. The right pane shows that the configuration has changed.

16. Click Apply Changes.

17. Click Restart button.

The application server should automatically restart.

18. Open the AMConfig.properties file in a text editor. By default, the location of this file is the /opt/SUNWappserver7/SUNWam/lib directory.

19. Set property com.iplanet.am.admin.cli.certdb.dir to APP_SERVER_INSTANCE_DIR/config. For example, /opt/SUNWappserver7/domains/domain1/server1/config.

20. Set property com.iplanet.am.admin.cli.certdb.prefix to empty.

For example, this line will have the following value by default com.iplanet.am.admin.cli.certdb.prefix=https-<fqdn>-<hostname>-. Change it to com.iplanet.am.admin.cli.certdb.prefix=.


22. Restart the Sun ONE Application Server Instance from command line. It should prompt you for password. Enter the Certificate Database password.
Setting Up the Sun ONE Portal Server to Use Secure External LDAP Directory Server

In the default install, the Sun ONE Portal Server, the iPlanet Directory Server Access Management Edition, and the Sun ONE Directory Server software are all running on the same host. However, depending on the performance, security, and integration requirements of your deployment, you might want to run the directory server on a separate, external host and have the portal server access the directory over a secure connection using SSL. In order to access the directory server over a secure connection, the Sun ONE Application Server must be configured to trust the certificate authority that signed the directory’s certificate. To set up this configuration, perform the tasks described in the following sections:

• “To Configure the Directory Server to Run in SSL,” on page 20
• “To Configure the Sun ONE Application Server to Trust the CA on the Directory Server Certificate,” on page 24

To Configure the Directory Server to Run in SSL

1. Verify that both the Directory Server (ns-slapd process) and the Admin Server (ns-httpd process) are started and running.

2. As root, in a terminal window start the directory server console by typing:
   
   `/usr/ldap/startconsole`

3. In the login window that is displayed, enter `admin` as the user name and the passphrase for the Directory Server.

4. In the left pane of the console, expand the directory until you see the Directory Server instance under Server Group.

5. Select Directory Server instance and click Open.

6. Select Tasks and then Manage Certificates.

   The first time you perform this task, you’ll be asked to create a certificate database by entering a password. Make a note of this password as you will need it later to start up the Directory Server.
6. Click Request.
   The Certificate Request Wizard appears. Follow the wizard and complete the steps to generate a certificate request. The request is sent to a Certificate Management Server (CMS) for approval. The CMS returns the real certificate. Save a copy of the certificate request by copying the request data to a file.

7. After the certificate request is sent to the CMS, have the administrator of the CMS approve the request and send back the approved certificate.

8. Get the generated certificate for the DS and the CMS certificate.
   Since the CMS generated the certificate for DS, the CMS will also have to be trusted by importing its certificate as a root CA.

9. Select Manage Certificates, Server Certificates and then click Install.
   The Certificate Install Wizard appears.

10. Copy and paste the approved certificate data from Step 7 into the text area and follow the steps of the wizard to install the certificate.
    When the certificate is successfully installed, the certificate displays as a line item on the Server Certificates tab.

11. Select Manage Certificates and CA Certificates, and then click Install.
    Copy and paste the CMS certificate data into the text area and follow the steps of the wizard to install the certificate.

12. Click Close to close the Manage Certificates window.

13. Select Configuration.

14. In the right pane, select Settings.

15. Verify or specify a valid port number in the Encrypted port field and click Save.
    The default is 636.

16. Click Encryption, check the Enable SSL for this server and Use the cipher family: RSA checkboxes and click Save.

17. Restart the Directory Server and supply the certificate database password entered in Step 5.
    Your Directory is now listening on port 636 (default) for SSL connections.
To Configure iPlanet Directory Server Access Management Edition to Communicate with the Directory Server Using SSL

1. Initialize a new certificate DB using the certutil tool located in DSAME_BASEDIR/SUNWam/bin. Enter the following command to create and initialize the new certificate DB:

```bash
#!/bin/ksh
#

export
LD_LIBRARY_PATH=<DSAME_BASEDIR>/SUNWam/lib/solaris/sparc:$LD_LIBRARY_PATH
certutil -N -d <cert-db-dir> -P <cert-db-prefix>
```

2. Enter the password to protect the database. Use a prefix that reflects the instance of iPlanet Directory Server Access Management Edition that you are configuring.

3. Install the CMS certificate in step 5 in the previous section as a root CA in the certificate database. Use the following command:

```bash
#!/bin/ksh
#

export
LD_LIBRARY_PATH=<DSAME_BASEDIR>/SUNWam/lib/solaris/sparc:$LD_LIBRARY_PATH
cd <DSAME_BASEDIR>/SUNWam/bin
./certutil -A -n "Root CA - Sun" -t "CTu,CTu,CTu" -h "internal" -P https-servername.domain.com-servername- -d <cert-db-dir> -i $(1:-/u/xinyang/tmp4/rootca.txt)
```

4. List the CMS certificate info in the certificate database. Use the following command:

```bash
#!/bin/ksh
#

export
LD_LIBRARY_PATH=<DSAME_BASEDIR>/SUNWam/lib/solaris/sparc:$LD_LIBRARY_PATH
```
cd <DSAME_BASEDIR>/SUNWam/bin
if [ $# -eq 0 ];then
 ./certutil -L -P https-servername.domain.com-servername- -d <cert-db-path>
else
 ./certutil -L -P https-servername.domain.com-servername- -d <cert-db-path> -n "Root CA - Sun"
fi

5. Open the <DSAME_BASEDIR>/lib/AMConfig.properties file with a text editor and change the following three lines from
com.iplanet.am.directory.ssl.enabled=false
com.iplanet.am.directory.host=<hostname>.domain.com
com.iplanet.am.directory.port=<DS no SSL port#>

to
com.iplanet.am.directory.ssl.enabled=true
com.iplanet.am.directory.host=<hostname where iDS SSL active>.domain.com
com.iplanet.am.directory.port=<iDS SSL port#, default 636>

6. Change the following two lines to point to the newly created certificate DB path and prefix specified in Step 1:
com.iplanet.am.admin.cli.certdb.dir=<cert-db-dir>
com.iplanet.am.admin.cli.certdb.prefix=<cert-db-prefix>

7. Open the <DSAME_BASEDIR>/SUNWam/config/ums/serverconfig.xml file and change the following line from
<Server name="Server1" host="hostname.red.iplanet.com" port="389" type="Simple" />

to
<Server name="Server1" host="hostname.red.iplanet.com" port="636" type="SSL" />

8. Save the changes and restart the Application Server.

9. Verify that SSL is working by issuing the following amadmin command:
#!/bin/ksh
#
export PATH=<DSAME_BASEDIR>/SUNWam/bin:$PATH
export LD_LIBRARY_PATH=<DSAME_BASEDIR>/SUNWam/lib:$LD_LIBRARY_PATH

$cd <DSAME_BASEDIR>/SUNWam/servers/rootca amadmin --runasdn "uid=amAdmin,ou=People,o=iplanet.com,o=isp" --password 11111111 --verbose --deleteservice ${1:-asdfkj}

If SSL authentication passed (and AMConfig.properties is configured to log all messages), you should see the following message:

****************************************************
11/29/2002 02:06:42:408 PM PST: Thread[main,5,main]
Start JSS initialization

NOTE To monitor the log in a separate terminal window, enter

tail -f /var/opt/SUNWam/debug/amJSS


If you the admin console displays, you have successfully configured SSL between iPlanet Directory Server Access Management Edition and the Directory Server.

To Configure the Sun ONE Application Server to Trust the CA on the Directory Server Certificate

1. Login into the Sun ONE Application Server admin console as the administrator.

2. In the left pane, click Security.

3. In the right pane, select the Certificate Management tab.

4. If a certificate database has not been initialized or created yet, initialize a new certificate DB by providing a key pair file password. Reconfirm the password and click OK to create the certificate DB.

5. In Certificate Management tab, click Install.

6. Check the button next to Trusted Certificate Authority (CA).
7. Enter the password for the key pair file and copy and paste the certificate data for the CA into the Message text field.

8. Provide the full path to the CA certificate file in the Message is in this file: field.

9. Click OK to install the certificate for the CA.

10. Restart application server to make the change effective.

Setting Up LDAP Replication for the Sun ONE Portal Server

The main reason for using LDAP replication for your Sun ONE Portal Server is to provide higher availability.

This procedure requires that you install the iPlanet Directory Server 5.1 software on all the machines you want to use for replication, then set up the replication. Next, you install the Sun ONE Application Server and Portal Server software. The Sun ONE Application Server and Portal Server software can be installed on the machines to be used for replication or on separate machines. Before using the portal server software, you need to update a number of configuration files.

The following instructions are for setting up two machines: one machine with Sun ONE Portal Server software (ps-server) including LDAP and one machine with just LDAP (x-ldap-server). Replication is set up between the two machines and LDAP failover is set up on the machine with the Sun ONE Portal Server software.

For more details and other replication set ups, see Chapter 8, Managing Replication in the iPlanet Directory Server 5.1 Administrator’s Guide.

These instructions assume that the default values are used except where specifically noted.

On both machines, install the directory server.

1. In a terminal window on the machine that will have the portal server installation, as root, go to the directory where the portal server software is and type:

   # ./pssetup

2. Select 2, Install Directory Server only.

3. Remember the password.
To Set Up Replication on the Sun ONE Portal Server Machine

1. As root, in a terminal window start the directory server console by typing:
   
   `#/usr/ldap/startconsole`

2. In the login window that is displayed, enter `admin` as the user name and the passphrase you choose earlier.

3. In the left pane of the console, expand the directory.


5. In the right pane, click Open.
   
   A pop-up window is displayed.

6. Select the Configuration tab.

7. Expand Replication in the left pane.

8. Select Replication.

9. Check Enable Changelog check box in the right pane.

10. Click Use default button in the right pane.
    
    The default directory value is entered in the Changelog database directory text field.

11. Click Save.

12. Select userRoot in the left pane.

13. Check Enable Replica check box in the right pane.

14. Select Multiple Master.

15. Enter a number (1-255) in the Replica ID box. This number needs to be unique for each master.

16. Click Save.

17. In the tool bar, click Object and select New Replication Agreement.

18. Enter a name (you can use the name of the `x-ldap-server`) for the replication agreement. Add a brief description.

19. Click Next.
20. Select Other and insert the fully qualified distinguished name of the machine to be connected to with the port number (default 389).

21. Click OK.

22. For Bind as, use cn=Directory Manager and insert the password for the directory server on the \textit{x-ldap-server} machine being connected to.

23. Click Next.

24. Click Next again.

25. Select Do Not Initialize Consumer and click Next.

   The replication agreement is displayed.

26. Click Done if it is correct.

27. Click OK.

To Set Up Replication on the Dedicated LDAP Machine

1. As \texttt{root}, in a terminal window start the directory server console by typing:

   \texttt{#/usr/ldap/startconsole}

2. In the login window that is displayed, enter \texttt{admin} as the user name and the passphrase you chose earlier.

   The console is displayed.

3. In the left pane of the console, expand the directory.

4. Select Directory Server (\texttt{x-ldap-server}).

5. In the right pane, click Open.

   A pop-up window is displayed.

6. Select the Configuration tab.

7. Expand the Replication in the left pane.

8. Select Replication.

9. Check Enable Changelog check box in the right pane.
10. Click Use default button in the right pane.
   The default directory value is entered in the Changelog database directory text field.

11. Click Save.

12. Select userRoot in the left pane.

13. Check Enable Replica check box in the right pane.

14. Select Multiple Master.

15. Enter a number (1-255) in the Replica ID box. This number needs to be unique for each master.

16. Click Save.

17. In the tool bar, click Object and select New Replication Agreement.

18. Enter a name (you can use the name of the ps-server) for the replication agreement. Add a brief description.

19. Click Next.

20. Select Other and insert the fully qualified distinguished name of the machine to be connected to with the port number (default 389).

21. Click OK.

22. For Bind as, use cn=Directory Manager and insert the password for the directory server on the ps-server machine being connected to.

23. Click Next.

24. Click Next again.

25. Select Initialize consumer now and click Next.
   The replication agreement is displayed.

26. Click Done if it is correct.

27. Click OK.

**NOTE**
To check replication status, select the Status tab. Select Replication Status in the left pane. The right pane displays the name of your replication agreement. You may need to click the Refresh button if you are using multiple replication agreements.
28. In this set up the Sun ONE Portal Server machine’s LDAP is a consumer of this LDAP and this LDAP is a consumer of the portal server machine’s LDAP. So for each additional consumer portal server machine, repeat Steps 20 to 30.

29. Stop each LDAP that has been initialized (Step 25), then restart. For example, log into the supplier machine (*ps-server*) as *root* and type:

```
# /usr/ldap/slapd-servername/stop-slapd
# /usr/ldap/slapd-servername/start-slapd
```

**NOTE**

To check replication on the consumer, start the directory server console, expand the directory in the left pane and select Directory Server. Click Open and select the Directory tab on the pop-up window. Expand the entry for the root suffix (default *isp*). Note that there are few nodes. After installing Sun ONE Application Server and Portal Server software, and starting replication, check *isp* again. If replication is set up correctly, there should be many nodes.

---

**Adding More Suppliers**

When making the replication agreements, each master must have an agreement with every other master. Any supplier you initialize, you need to restart.

**To Configure the Sun ONE Portal Server Software**

These instructions assume that the default values are used excepted where specifically noted.

1. Install the Sun ONE Application Server. Follow the install instructions in “Installing Sun ONE Application Server,” on page 7.

2. Install the Sun ONE Portal Server software as described in the “Installing the Sun ONE Portal Server Software,” on page 9 with the following changes:

   a. Do not accept the default values.
      A series of questions about installation values are asked.

   b. Respond to the question:
      
      Use an existing Directory Server? y/[n] y
c. Respond to the question:

What is the directory manager password?

by typing the password for the directory server on this machine and confirming it.

3. After the Sun ONE Portal Server software is installed, go to the Sun ONE Application Server console. Expand the hierarchy in the left pane and select the server that the portal server software is running on (server1). Select the General tab and click Stop.

4. Stop and restart the amserver.

```bash
#/etc/init.d/amserver stop
#/etc/init.d/amserver start
```

5. In a terminal window, restart the Sun ONE Application Server by typing:

```bash
#/opt/SUNWappserver7/bin/asadmin start-appserv
```

6. Test the portal server installation by launching the portal desktop in a browser by using:

```
http://full-hostname:listen-port/portal/dt
```

If the sample desktop displays without any exceptions, then your Sun ONE Portal Server installation is good.

7. Go to the BASEDIR/config/ums/serverconfig.xml file (the default is /opt/SUNWappserver7/SUNWam/config/ums/serverconfig.xml). Set the configuration to point to the local LDAP.

a. Copy the Server1 line right below itself.

b. Edit the lines so they have these values:

```xml
<Server name="Server1" host="full-ps-servername" port="389" type="SIMPLE" />
<Server name="Server2" host="x-ldap-fullservername" port="389" type="SIMPLE" />
```

c. If you have multiple suppliers, add similar lines for each one.

```xml
<Server name="Server3" host="x-ldap-fullservername2" port="389" type="SIMPLE" />
```

8. Go to the BASEDIR/lib/AmConfig.properties file (the default is /opt/SUNWappserver7/SUNWam/lib/AmConfig.properties).

a. Check that this line is correct:

```
com.iplanet.am.directory.host=full-ps-servername
```
b. Change `com.iplanet.am.replica.enable=false` to `com.iplanet.am.replica.enable=true`.

c. If appropriate, change
   `com.iplanet.am.session.failover.enabled=false` to `com.iplanet.am.session.failover.enabled=true`.

9. Return to the Sun ONE Application Server console. Expand the hierarchy in the left pane and select the server that the Sun ONE Portal Server software is running on (server1). Select the General tab and click Stop.

10. Stop and restart the amserver.
    
    ```
    # /etc/init.d/amserver stop
    # /etc/init.d/amserver start
    ```

11. In a terminal window, restart the Sun ONE Application Server by typing:
    
    ```
    # /opt/SUNWappserver7/bin/asadmin start-appserv
    ```

12. Log into the Sun ONE Portal Server administration console with user name amadmin and the passphrase you entered during the installation.

13. Select User Management in the View menu and click on the organization name link in the navigation pane.

14. Select Services in the Show menu.

15. Click on the Properties arrow next to LDAP Authentication in the navigation pane.

16. Check that the Primary LDAP box only has the `full-ps-servername` listed. If you have multiple LDAP servers, the Primary LDAP box should list localhost or `full-ps-servername` | `full-ps-servername`:389.

17. To the Secondary LDAP box Add the `x-ldap-fullservername` to the list.

18. Click Save to save the configuration.

19. If you have a number of portal server installations, complete Step 20 to Step 24. If not, you are finished.

20. Return to the root level by clicking root suffix (default `isp`) in the location pane.

21. In the View menu, select Service Management.

22. Click on the Properties arrow next to Platform.
23. Check that the Server List has all of the portal server machines listed using the `full-ps-servername` for each server.

24. Click Save.

**Known Problems and Limitations**

The following table contains a list of current bugs with workarounds. In this three column table, the first column lists the bug IDs; the second column describes the bug; and the third column provides the available workarounds.

<table>
<thead>
<tr>
<th>Bug ID</th>
<th>Description</th>
<th>Workarounds</th>
</tr>
</thead>
<tbody>
<tr>
<td>4786641</td>
<td>Redeploy of portal web application fails during imports.</td>
<td>Some characters, the colon (:), the asterisk (<em>), and the backslash (), cause errors if you use them in the command syntax unless you use escape characters to set them off. The possibilities for using escape characters vary depending upon what platform you use and whether you use singlemode or multimode. The characters for all arguments to the command line need to be escaped if they include the colon (:), the asterisk (</em>), and the backslash (). Putting &quot; around the password operand solved the problem but this is not a general solution since &quot; could be part of the password itself.</td>
</tr>
<tr>
<td>4788255</td>
<td>SRA Data Migration: <code>srapGatewayConfig.xml</code> file not created.</td>
<td>The exported gateway config xml file is found to have some namespace violations with regards to jdk1.4. Set the namespace aware flag to false as it does not cause any harm.</td>
</tr>
<tr>
<td>4803270</td>
<td>Intermittent system error occurs when adding channels using the Admin Console.</td>
<td>Reload the console page.</td>
</tr>
</tbody>
</table>
Problem:
Portal Server cannot be installed into an application server instance or domain whose name contains a dash or a space, for example, Default-Server or Default Server. If you try to install into an application server instance or domain with a dash or space in the name, the installation script returns the error message Invalid response! and prompts for the application server domain or application server instance name again.

Solution:
Install portal on an instance or in a domain that does not have a dash or space in its name.

Troubleshooting
The debug logs for the Portal Server software are in the /var/opt/SUNWam/debug directory. The debug logs for the Secure Remote Access software are in the /var/opt/SUNWps/debug directory.

How to Report Problems
If you have problems with Sun ONE Portal Server 6.0, contact Sun ONE customer support using one of the following mechanisms:
• Sun ONE online support Web site at
http://www.sun.com/service/support

After selecting Sun ONE software support, Online Support Center and Product Tracker are available for logging problems.

- The telephone dispatch number associated with your maintenance contract

So that we can best assist you in resolving problems, please have the following information available when contacting customer support:

- Description of the problem, including the situation where the problem occurs and its impact on the operation
- Machine type, operating system version, and product version, including any patches and other software that might be affecting the problem
- Detailed steps on the methods used to reproduce the problem
- Any error logs or core dumps

Where to Find More Information

In addition to this guide, Sun ONE Portal Server comes with supplementary information for administrators as well as documentation for developers. Use the following URL to see all the Sun ONE Portal Server documentation:

http://docs.sun.com/prod/slportalsrv

Listed below are the additional documents that are available:

- Sun ONE Portal Server 6.0 Release Notes
- Sun One Portal Server 6.0 Deployment Guide
- Sun ONE Portal Server 6.0 Installation Guide
- Sun ONE Portal Server 6.0 Administrator’s Guide
- Sun ONE Portal Server 6.0 Desktop Customization Guide
- Sun ONE Portal Server 6.0 Developer’s Guide
- Sun ONE Portal Server 6.0 Migration Guide