



Troubleshooting Sun Java System Portal Server Secure Remote Access 7



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

Part No: 819-6447

Copyright 2006 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. 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 U.S. 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.

This distribution may include materials developed by third parties.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, the Solaris logo, the Java Coffee Cup logo, docs.sun.com, Java, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

Products covered by and information contained in this publication are controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical or biological weapons or nuclear maritime end uses or end users, whether direct or indirect, are strictly prohibited. Export or reexport to countries subject to U.S. embargo or to entities identified on U.S. export exclusion lists, including, but not limited to, the denied persons and specially designated nationals lists is strictly prohibited.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 2006 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. Tous droits réservés.

Sun Microsystems, Inc. détient les droits de propriété intellectuelle relatifs à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et ce sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plusieurs brevets américains ou des applications de brevet en attente aux États-Unis et dans d'autres pays.

Cette distribution peut comprendre des composants développés par des tierces personnes.

Certains composants de ce produit peuvent être dérivés du logiciel Berkeley BSD, licenciés par l'Université de Californie. UNIX est une marque déposée aux États-Unis et dans d'autres pays; elle est licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, le logo Solaris, le logo Java Coffee Cup, docs.sun.com, Java et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux États-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux États-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui, en outre, se conforment aux licences écrites de Sun.

Les produits qui font l'objet de cette publication et les informations qu'il contient sont régis par la législation américaine en matière de contrôle des exportations et peuvent être soumis au droit d'autres pays dans le domaine des exportations et importations. Les utilisations finales, ou utilisateurs finaux, pour des armes nucléaires, des missiles, des armes chimiques ou biologiques ou pour le nucléaire maritime, directement ou indirectement, sont strictement interdites. Les exportations ou réexportations vers des pays sous embargo des États-Unis, ou vers des entités figurant sur les listes d'exclusion d'exportation américaines, y compris, mais de manière non exclusive, la liste de personnes qui font objet d'un ordre de ne pas participer, d'une façon directe ou indirecte, aux exportations des produits ou des services qui sont régis par la législation américaine en matière de contrôle des exportations et la liste de ressortissants spécifiquement désignés, sont rigoureusement interdites.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFACON.

Contents

Troubleshooting Sun Java System Portal Server 7 Secure Remote Access	5
Technical Note Revision History	5
Portal Server 7 and Components Configuration Requirements	5
Troubleshooting Secure Remote Access	6
Log Files Location	6
Troubleshooting Issues	12
Best Practices Checklist	15
Known Issues and Limitations	17
How to Report Problems and Provide Feedback	17
Additional Sun Resources	18
Sun Welcomes Your Comments	18

Troubleshooting Sun Java System Portal Server 7 Secure Remote Access

This Technical Note describes issues you may encounter while administering Sun Java System Portal Server 7 Secure Remote Access and how to troubleshoot them. This note also includes a list of best practices and information on the log files locations and all its configurable parameters.

This Technical Note contains the following sections:

- [“Technical Note Revision History”](#) on page 5
- [“Portal Server 7 and Components Configuration Requirements”](#) on page 5
- [“Troubleshooting Secure Remote Access”](#) on page 6
- [“Best Practices Checklist”](#) on page 15

Technical Note Revision History

TABLE 1 Revision History

Revision Date	Details
June 2006	Initial release.

Portal Server 7 and Components Configuration Requirements

The following table lists the supported configuration matrix for Portal Server 7.

TABLE 2 Supported Configuration for Solaris 9 and Solaris 10 on SPARC and x86, and Red Hat Linux

Operating System	Web Container	Browser Client	Portal Server Console
Solaris 10, SPARC	<ul style="list-style-type: none"> ■ Sun Java System Application Server 8.1 ■ Sun Java System Web Server 6.1 SP5 ■ BEA Weblogic 8.1 SP4 ■ IBM WebSphere 5.1.1.5 Advanced Edition 	<ul style="list-style-type: none"> ■ Mozilla 1.4 ■ Internet Explorer 6.0 	<ul style="list-style-type: none"> ■ Sun Java Enterprise System Application Server 8.1 ■ Sun Java Enterprise System Web Server 6.1SP5
Solaris 9 SPARC	<ul style="list-style-type: none"> ■ Sun Java System Application Server 8.1 ■ Sun Java System Web Server 6.1 SP5 ■ BEA Weblogic 8.1 SP4 ■ IBM WebSphere 5.1.1.5 Advanced Edition 	<ul style="list-style-type: none"> ■ Mozilla 1.4 ■ Internet Explorer 6.0 	<ul style="list-style-type: none"> ■ Sun Java Enterprise System Application Server 8.1 ■ Sun Java Enterprise System Web Server 6.1SP5
Solaris 9 on x86	Sun Java Enterprise System Web Server 6.1SP5	Mozilla 1.4	Sun Java Enterprise System Web Server 6.1SP5
Linux Red Hat 3.0 on x86	<ul style="list-style-type: none"> ■ Sun Java Enterprise System Application Server 8.1 ■ BEA WebLogic 8.1 SP4 ■ Sun Java Enterprise System Web Server 6.1SP5 	<ul style="list-style-type: none"> ■ Mozilla 1.4 ■ Internet Explorer 6.0 	<ul style="list-style-type: none"> ■ Sun Java Enterprise System Application Server 8.1 ■ BEA WebLogic 8.1 SP4 ■ Sun Java Enterprise System Web Server 6.1SP5 on Linux RH 3.0,x86ux 2.1

Troubleshooting Secure Remote Access

Log Files Location

The following table lists the location of all the log files and the various log file names associated with the Secure Remote Access components.

TABLE 3 Log Files Location

Component Name	Log Configuration Filename and Location	Log File Location
----------------	---	-------------------

TABLE 3 Log Files Location (Continued)

Portal Instance	<p><PS_DATA_DIR>/portals/ <PORTAL_ID>/config/ PSLogConfig.properties</p> <p>For example /var/opt/SUNWportal/ portals/myPortal/ config/ PSLogConfig.properties</p>	<p><PS_DATA_DIR>/portals/ <PORTAL_ID>/logs/<instance ID>.</p> <p>For example, /var/opt/SUNWportal/portals /myPortal/logs/myInstance/ portal.0.0.log.</p> <p>By default, only one file is created</p>
Portlet Applications	<p><PS_DATA_DIR>/portals/ <PORTAL_ID>/config/ PSLogConfig.properties</p> <p>For example, /var/opt/SUNWportal/portals/ myPortal/config/ PSLogConfig.properties.</p>	<p><PS_DATA_DIR>/portals/ <PORTAL_ID>/logs/<instance ID>. For example, /var/opt/SUNWportal/portals/ myPortal/logs/myInstance/.</p> <p>By default, only one file is created - portal.0.0.log. The content logged through PortletContext.log() gets appended to this file.</p>
Search Webapp	<p><PS_DATA_DIR>/searchserver/ <SEARCH_ID>/config/ SearchLogConfig.properties</p> <p>For example, /var/opt/SUNWportal/ searchserver/mySearch/config/ SearchLogConfig.properties.</p>	<p><PS_DATA_DIR>/searchserver/<SEARCH_ID>/ config/SearchLogConfig.properties.</p> <p>By default, three files are created:rdmserver.0.0.log, rdm.0.0.log, rdmgr.0.0.log.</p> <p>For example, /var/opt/SUNWportal/ searchserver/mySearch/logs/.</p>
Administration CLIs	<p><PS_CONFIG_DIR>/ PSAdminLogConfig.properties</p> <p>For example, /etc/opt/SUNWportal/ PSAdminLogConfig.properties.</p>	<p><PS_DATA_DIR>/logs/admin. /var/opt/SUNWportal/logs/admin/.</p> <p>By default, only one file is created portal.admin.cli.0.0.log.</p>
Portal Administration Server	<p><PS_CONFIG_DIR>/ PSAdminLogConfig.properties</p> <p>For example, /etc/opt/SUNWportal/ PSAdminLogConfig.properties.</p>	<p><PS_DATA_DIR>/logs/admin/. For example, /var/opt/SUNWportal/logs/admin/ .</p> <p>By default, only one is created portal.0.0.log.</p>
Administration Console	<p><PS_DATA_DIR>/portals/ <PORTAL_ID>/config/ PSLogConfig.properties</p> <p>For example, /var/opt/SUNWportal/portals/ myPortal/config/ PSLogConfig.properties.</p>	<p><PS_DATA_DIR>/logs/admin/. For example, /var/opt/SUNWportal/logs/admin/ By default, only one file is created portal.admin.console.0.0.log.</p>

TABLE 3 Log Files Location (Continued)

Gateway	<p><PS_CONFIG_DIR>/ platform.conf.<profile></p> <p>For example, /etc/opt/SUNWportal/ platform.conf.default .</p>	<p>PS_DATA_DIR>/logs/sra/<profile>/. For example, /var/opt/SUNWportal/logs/sra/default/.</p> <p>By default, only one file is created portal.gateway.0.0.log .</p>
Netlet proxy	<p><PS_CONFIG_DIR>/ platform.conf.<profile></p> <p>For example, /etc/opt/SUNWportal/ platform.conf.<profile> .</p>	<p><PS_DATA_DIR>/logs/sra/<profile>. For example, /var/opt/SUNWportal/logs/sra/default/ .</p> <p>By default, only one file is created portal.nlproxy.0.0.log .</p>
Rewriter proxy	<p><PS_CONFIG_DIR>/ platform.conf.<profile></p> <p>For example, /etc/opt/SUNWportal/ platform.conf.<profile> .</p>	<p><PS_DATA_DIR>/logs/ sra/<profile>.</p> <p>For example, /var/opt/SUNWportal/ logs/sra/default/ .</p> <p>By default, only one file is created portal.rwproxy.0.0.log .</p>
Rewriter	<p>/var/opt/SUNWportal/logs/ sra/<PROFILE_NAME>/</p> <p>The log settings for the particular gateway instance can be configured by modifying the /etc/opt/SUNWportal/ platform.conf.PROFILE_NAME file.</p>	<p>The log files corresponding to each of the above properties are:</p> <ul style="list-style-type: none"> ■ portal.rewriter.original.gateway.0.0.log ■ portal.rewriter.rest.gateway.0.0.log ■ portal.rewriter.rewritten.gateway.0.0.log ■ portal.rewriter.rulesetinfo.gateway.0.0.log ■ portal.rewriter.unaffected.gateway.0.0.log ■ portal.rewriter.uriinfo.gateway.0.0.log

Configurable Parameters of a Log Configuration file

You can use the instructions in this section to do the following:

- Set a separate file for the logger
- Set a level for the logger
- Specify a handler for the logger
- Set the format for the logger

EXAMPLE 1 A separate file can be set for the logger as follows:

`LOGGER_NAME.separatefile=true`. For example,
`debug.com.sun.portal.desktop.separatefile=true`.

EXAMPLE 2 The level for the logger can be set as follows:

`LOGGER_NAME.level=LEVEL_NAME`. For example, `debug.com.sun.portal.level=FINE`.

EXAMPLE 3 A handler can be specified for the logger as follows:

LOGGER_NAME.handler=HANDLER_NAME. For example,
`debug.com.sun.portal.handler=java.util.logging.FileHandler.`

EXAMPLE 4 A Formatter can be specified for the logger as follows:

LOGGER_NAME.handler.HANDLER_NAME.formatter=FORMATTER_NAME. For example,
`debug.com.sun.portal.handler.java.util.logging.FileHandler.formatter=com.sun.portal.log.common.PortalLogFormatter.`

Viewing the Log Files List

The following table describes the list of options to view log files of the Secure Remote Access components.

TABLE 4 Component Logs List Command

Component	Command
Gateway	<code>psadmin list-loggers -u adminUser -f passwordfile --component gateway --sra-instance profile</code>
Netletproxy	<code>psadmin list-loggers -u adminUser -f passwordfile --component nlproxy --sra-instance profile</code>
Rewriterproxy	<code>psadmin list-loggers -u adminUser -f passwordfile --component rwproxy --sra-instance profile</code>

Logging Command Line Options

The following three commands are used for logging files for Secure Remote Access components:

- `list-loggers` — Lists all the loggers.
- `set-logger` — Sets the level for the logger and also the separate file for the logger.
- `reset-logger` — Resets the log level and log file to *root* logger.

Psadmin List-Loggers Command Options

Use this table to review the options available for the `list-loggers` command.

TABLE 5 List-Loggers Command Line Options List

Option	Description
--adminuser -u <i>userName</i>	Specify the name of the administrator.
--passwordfile -f <i>password-filename</i>	Specify the administrator password in the password file.
--component -m <i>component-type</i>	Specify the component type. The valid values are <code>portal</code> , <code>search</code> , <code>pas</code> , <code>gateway</code> , <code>n1proxy</code> , and <code>rwproxy</code> .
--portal -p <i>portal-ID</i>	Specify the portal ID. This is required only if the component type is <code>portal</code> .
--instance -i <i>portal-instance-name</i>	Specify the portal server instance. This is required only if the component-type is <code>portal</code> .
--searchserver -s <i>search-server-ID</i>	Specify the search server ID. This is required only if the component type is <code>search</code> .
--sra-instance <i>sra-instance</i>	Specify the SRA instance name. This is required only if the component type is either <code>gateway</code> , <code>n1proxy</code> , or <code>rwproxy</code> .
--detail	Displays detailed information about loggers listed. It includes level, handler information, filename, and filehandler.

Psadmin Set-Logger Command Options

TABLE 6 Set-Logger Command Line Options List

Option	Description
--adminuser -u <i>userName</i>	Specify the name of the administrator.
--passwordfile -f <i>password-filename</i>	Specify the administrator password in the password file.
--component -m <i>component-type</i>	Specify the component type. The valid values are <code>portal</code> , <code>search</code> , <code>pas</code> , <code>gateway</code> , <code>n1proxy</code> , and <code>rwproxy</code> .
--logger -o <i>loggerName</i>	Specify the name of the logger.
--level -L <i>level</i>	Specify the level.
--portal -p <i>portal-ID</i>	Specify the portal ID. This is required only if the component-type is <code>portal</code> .
--instance -i <i>portal-instance-name</i>	Specify the portal server instance. This is required only if the component type is <code>portal</code> .
--searchserver -s <i>search-server-ID</i>	Specify the search server ID. This is required only if the component type is <code>search</code> .

TABLE 6 Set-Logger Command Line Options List (Continued)

Option	Description
<code>--sra-instancesra-instance-name</code>	Specify the SRA instance name. This is required only if the component type is either <code>gateway</code> , <code>nproxy</code> , or <code>rwproxy</code> .
<code>--file -F</code>	Specify if the logger is to be logged to a separate file.
<code>--stack-trace -T</code>	This option can be specified only if <code>--file</code> option is specified. Specifies whether the stack trace should be printed in the log file. If this option is specified, the <code>--parent</code> option cannot be specified. The default is <code>false</code> . If you specify <code>true</code> , then the stack trace is printed in the log file.
<code>--parent -P</code>	This option can be specified only if <code>--file</code> option is specified. Specifies whether the log data should be printed in the parent log file of the current logger. If this option is specified, <code>--stack-trace</code> option cannot be specified. The default is <code>false</code> , if you do not specify the option, the log data is printed only in the current logger's log file. If you specify <code>true</code> , the log data is printed in the parent log file and also in the current logger's log file.

Psadmin Reset-Logger Command Options

TABLE 7 Reset-Logger Command Line Options List

Option	Description
<code>--adminuser -u userName</code>	Specify the administrators name.
<code>--passwordfile -f password-filename</code>	Specify the administrator password in the password file.
<code>--component -m component-type</code>	Specify the component type. The valid values are <code>portal</code> , <code>search</code> , <code>pas</code> , <code>gateway</code> , <code>nproxy</code> , and <code>rwproxy</code> .
<code>--logger -l loggerName</code>	Specify the name of the logger.
<code>--portal -p portal-ID</code>	Specify the portal ID. This is required only if the <code>component-type</code> is <code>portal</code> .
<code>--instance -i portal-instance-name</code>	Specify the portal server instance. This is required only if the <code>component-type</code> is <code>portal</code> .
<code>--searchserver -s search-server-ID</code>	Specify the search server ID. This is required only if the <code>component-type</code> is <code>search</code> .
<code>--sra-instancesra-instance-name</code>	Specify the SRA instance name. This is required only if the <code>component-type</code> is either <code>gateway</code> , <code>nproxy</code> , or <code>rwproxy</code> .

Frequently Asked Questions on Logging

When a separate file is created, what is the name of the new file?

When a separate file is created, the filename is the same as the logger name except `debug.com.sun`. For example, if a separate file is set for the logger `debug.com.sun.portal.desktop`, the file name will be `portal.desktop.0.0.log`.

What is the format used to log the content in the file?

The format to log the content is:

```
|DATETIME|LOG_LEVEL|PRODUCT_ID|LOGGER NAME|KEY VALUE PAIRS|MESSAGE|
```

When is the stack trace logged?

The logging of stack trace is determined by the `stacktrace` property. This value is applicable only if the format is `PortalLogFormatter.debug.com.sun.portal.stacktrace=false`. If the value is false, the stack trace is logged only if the levels is either `SEVERE` or `WARNING`. If the value is `true`, the stack trace is always logged.

Troubleshooting Issues

This section describes issues that you may encounter while administrating the Portal Server Secure Remote Access component. It also includes the solution or workaround to resolve the issue.

Problem: Gateway does not display a confirmation message after you enter the start up command.

Solution: Although no confirmation messages is displayed, Gateway may be running. To verify if gateway is running, use `netstat -an | grep <port number>` and verify if the port is listening.

Problem: Gateway does not work when Netletproxy and Rewriterproxy are enabled in the Gateway profile in the psconsole.

Solution: Verify if Netletproxy and Rewriterproxy are running.

Problem: Cacao sends a timestamp check failed exception.

Solution: Ensure that the date and time is the same on both the nodes, when Gateway is installed on a remote node.

Problem: Gateway login problem due to cookies.

Solution: This issue occurs when the `com.ipplanet.encode` property is not the same as the `AMConfig.properties` file on all the nodes; Access Manager, Portal Server, and Gateway nodes. Ensure that the password encryption key properties are the same too on both the nodes.

Problem: Netlet and Proxylet do not work.

Solution: This issue can occur if the `enableSRAforPortal.xml` file is not loaded. Ensure the file is in the installation directory: `/opt/SUNWportal/export/request`. To initialize this file, execute the `amadmin` command.

Problem: Unable to start or stop Gateway.

Solution: Try restarting cacao. To restart cacao, enter the `/usr/lib/cacao/bin/cacaoadmin start` or `stop` command.

Problem: Failed to initialize OLE.

This issue occurs if an application failed to initialize OLE.

Solution: Try running the applet again with appropriate administrative privileges.

Problem: Error installing DLL file.

This issue occurs when the registration of the OCX control fails.

Solution: Verify if the `java.io.tmp` directory exists and is writable. You can retrieve the value of `java.io.tmp` from the Java console.

Problem: Registering OCX ctrl.

This issue can occur if the DLL file is not written to the `java.io.tmpdir` location on the user's hard drive.

Solution: Try running the applet again with appropriate administrative privileges.

Problem: Unable to read proxy setting information.

This error occurs when the system fails to read the proxy settings of the browser.

Solution: Close all instances of the browser and try again.

Problem: Failed to configure browser proxy settings.

This error occurs when the browser proxy settings fails to get modified.

Solution: Close all instances of the browser and try modifying the proxy setting again. If you are using Mozilla, allocate sufficient cache memory.

Problem: Error trying to restore browser proxy settings.

This error occurs when trying to restore the original browser proxy settings.

Solution: The proxy settings must be restored manually by the user.

Problem: Unable to write to the disk.

This error occurs when the application fails to write to the specified location.

Solution: Ensure that the location has appropriate write permissions.

Problem: Problem displaying User Interface. Unknown error.

The user interface is not displayed due to this error.

Solution: Verify if the JVM installation is successfully installed and running else reinstall the JVM.

Problem: Session Timeout. Please login again.

Solution: Logon to the desktop again to resolve this error.

Problem: Bad Request.

This error occurs when Gateway does not accept a particular request.

Solution: It could be a network issue, try again later.

Problem: Access to this resource denied.

This error occurs when Gateway does not have appropriate privileges to fulfill the request.

Problem: Not found error.

This error occurs when the requested page cannot be located.

Solution: Verify if the URL is correct and try accessing the page again.

Problem: Gateway Service Unavailable.

This error occurs when Proxylet is unable to establish contact with Gateway.

Solution: Try again later.

Problem: Netlet is unable to bind to port.

Solution: Ensure that the values for the client bind IP address in NetletProvider is correct and start Netlet again.

Best Practices Checklist

This section lists some of the best practices you can adopt while you execute and administer Gateway in your environment.

Gateway Best Practices

- To start or stop Watchdog, you could use the **psadmin sra-watchdog** command.
- To change the password of amService-srapGateway agent, log into AMConsole and select Agents > SRA Log User Password, and change the password. Gateway verifies the credentials of an user using the amService-srapGateway agent.
- To view the logs of the Gateway, use the psconsole. From the PSCconsole, select the Secure Remote Access tab and click Logging. Select Gateway, Netletproxy, or Rewriterproxy to view the logs.
- When configuring Gateway on a separate node, ensure that the local Directory Server is running and the security directory is copied from the Portal Server node.
- The certificate database for Gateway is located at `/etc/opt/SUNWportal/cert`.
- When Gateway is configured to access multiple Access Managers and Portal Servers, the respective entries of each Access Manager and Portal Server instance must be appended to the non-authenticated URLs list.
- You can use one of these methods to change the Gateway configuration:
 - Change the parameters in the `platform.conf.<instance>` file.
 - Using the psconsole, change the Gateway profile.
- The **chroot** command is deprecated and is not supported in Portal Server 7.
- The Access Manager encryption key password must match the Access Manager SDK install on the Gateway node, with Access Manager installed on the remote node.
- When Portal Server and Gateway are installed on different domains, the domain entries should be present under the Cookie Domain List in the AMConsole under Service Configuration.
- On the Portal Server node, you can view both the `AMConfig-default.properties` and `AMConfig.properties` files at `/etc/opt/SUNWPortal/`. This file is specific to Netletproxy and Rewriterproxy.
- To create the Gateway profile:
 1. Create a new Gateway profile using the psconsole. Ensure the https and http port numbers you use is not currently used by another application.
 2. Run the **psadmin** command to create an instance by modifying an appropriate template.
- Ensure that the SRA Core is installed during the Portal Server installation, else Gateway does not get installed.
- SRA Core cannot be installed in a separate session from an open Portal Server.

- Proxylet does not work when Portal Server is installed in the SSL mode.

Proxylet Best Practices

This section lists some of the best practices you can adopt while administering Proxylet in your environment.

Proxylet supports WPAD protocol

Use the following procedure to add the application URLs to the Proxylet console.

1. Login to psconsole.
2. From Manage Channels and Containers for Proxylet, select the Appurls link.
3. Click the New Property button, and select a string type.
4. Enter a short name for the URL in the Name field and the actual URL in the Value field. Application URLs override the default settings.

Deployment Options

You can choose to deploy Proxylet for the entire enterprise domain which completely eliminates the need to use Rewriter or use Proxylet only for applications that cannot be configured using the Rewriter.

Option 1 — Deploying Proxylet in an Enterprise Domain

1. Add a rule to the Proxylet Rules field for enterprise domain. For example, **enterprise domain: proxylethost: proxyletport**. The Proxylet channel displays a link.
2. Launch Proxylet by default. Clicking the link downloads Proxylet and reloads the portal desktop page. Using the rules defined in Step 1, the portal desktop page is displayed through the Proxylet.

Option 2 — Deploying Proxylet for Selected Applications

1. Add multiple rules to the Proxylet Rules field for each of the application domain and sub-domain. For example, **application domain: proxylethost: proxyletport**.
2. Add application URLs to the appurls collection property of Proxylet Channel properties. The Proxylet channel displays the application URLs.
3. Click any one of the URLs to download the Proxylet and redirect the browser to the selected application.

Customizing Proxylet

From the psconsole, use the Custom PAC file field to write a customized PAC file logic that is appropriate to your working environment. Proxylet configures the end users browser with the custom PAC file. If the custom PAC file is configured, then the Rule field is ignored.

You can use a customized launch pad for starting applications instead of using the Proxylet Channel. The format of the URL is as follows:

- Proxylet Servlet URL?
- `command=loadApp` or `loadJWSApp`
- `&followUp=Application URL`
- `&portalurl=portalsever desktop URL`
- `&propertyfile=name of property file`

Netlet Best Practices

- You can configure a Netlet static rule using the `psconsole`, Netlet starts automatically when the user logs onto the desktop.
- Users can configure dynamic rules using the Netlet channel.

Known Issues and Limitations

See the Sun Java System Portal Server Release Notes at the following URL to find out about known problems: http://docs.sun.com/app/docs/coll/entsysrn_05q1

How to Report Problems and Provide Feedback

If you have problems with Communications Express, contact Sun customer support using one of the following mechanisms:

- Sun Software Support services online at <http://www.sun.com/service/sunone/software>.
This site has links to the Knowledge Base, Online Support Center, and ProductTracker, as well as to maintenance programs and support contact numbers.
- 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 you contact support:
- Description of the problem, including the situation where the problem occurs and its impact on your 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 you have used to reproduce the problem
- Any error logs or core dumps

Additional Sun Resources

Useful Sun Java System information can be found at the following Internet locations:

- Sun Java System Documentation
<http://docs.sun.com/prod/java.sys>
- Sun Java System Professional Services
<http://www.sun.com/service/sunps/sunone>
- Sun Java System Software Products and Service
<http://www.sun.com/software>
- Sun Java System Software Support Services
<http://www.sun.com/service/sunone/software>
- Sun Java System Support and Knowledge Base
<http://www.sun.com/service/support/software>
- Sun Support and Training Services
<http://training.sun.com>
- Sun Java System Consulting and Professional Services
<http://www.sun.com/service/sunps/sunone>
- Sun Java System Developer Information
<http://developer.sun.com>
- Sun Developer Support Services
<http://www.sun.com/developers/support>
- Sun Java System Software Training
<http://www.sun.com/software/training>
- Sun Software Data Sheets
<http://www.sun.com/software>

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. To share your comments, go to <http://docs.sun.com> and click Send Comments. In the online form, provide the full document title and part number. The part number is a 7-digit or 9-digit number that can be found on the book's title page or in the document's URL. For example, the part number of this book is 819-6447.