Sun Java™ System

Portal Server Secure Remote Access 6 Administration Guide

2004Q2

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

Part No: 817-5317-10

Contents

List of Figures

List of Tables

List of Procedures

About This Guide

This guide explains how to administer the Sun Java™ System Portal Server Secure Remote Access (formerly Sun ONE™ Portal Server, Secure Remote Access)

Sun Java System Portal Server Secure Remote Access (SRA) enables remote users to securely access their organization's network and its services over the internet. Additionally, it gives your organization a secure internet portal, providing access to content, applications, and data to any targeted audience—employees, business partners, or the general public.

SRA runs on the Solaris™ 8.0 and 9.0 Operating Systems. This guide contains instructions for configuring and administering SRA.

This Preface includes the following sections:

- Who Should Read This Guide
- What You Need to Know
- How This Book is Organized
- Document Conventions Used in This Guide
- Where to Find Related Information
- Where to Find This Guide Online

Who Should Read This Guide

This guide assumes that you are a network or system administrator experienced in managing UNIX® systems and TCP/IP networks. You are responsible for installing, configuring and administering SRA.

You need root access to the required machines for installing the various components of SRA. You also need the required administrative privileges to carry out other operations such as configuring users and services.

What You Need to Know

Before you administer SRA, you need to be familiar with the following:

- Basic Solaris administrative procedures
- LDAP
- Sun Java™ System Directory Server
- Sun Java™ System Web Server
- Sun Java™ System Portal Server

You also need the following to be able to write Rewriter rules:

- Understanding of HTML and HTML tags
- A fair knowledge of JavaScript
- Basic knowledge of XML

How This Book is Organized

This book contains the following chapters and appendices:

About This Guide (this chapter)

Chapter 1, "Introduction to Portal Server Secure Remote Access"

This chapter describes the SRA and the relationship between the Sun Java™ System Portal Server product and SRA components. It also provides information on administering and configuring SRA.

Chapter 2, "The Gateway"

This chapter describes Gateway related concepts and information required for the smooth running of the Gateway.

Chapter 3, "Proxylet and Rewriter"

This chapter describes Proxylet and Rewriter. For Rewriter, it provides sample rules and best practices.

Chapter 4, “NetFile”

This chapter describes NetFile and explains its operation.

Chapter 5, “Netlet”

This chapter describes how to use Netlet to run applications securely between users’ remote standard Portal Desktops and the servers running applications on your intranet.

Chapter 6, “Netlet With PDC”

This chapter describes how to configure the client browser’s Java Plugin so that Netlet can be used with PDC.

Chapter 7, “Certificates”

This chapter describes certificate management and explains how to install self-signed certificates or certificates from a Certificate Authority.

Chapter 8, “Configuring URL Access Control”

This chapter describes how to allow or deny access to the end-user through the Gateway for specific URLs.

Chapter 9, “Configuring the Gateway”

This chapter describes how to configure Gateway attributes from the Sun Java™ System Identity Server administration console.

Chapter 10, “Configuring NetFile”

This chapter describes how to configure the NetFile from the Sun Java™ System Identity Server administration console.

Chapter 11, “Configuring Netlet”

This chapter describes how to configure the Netlet attributes from the Sun Java™ System Identity Server administration console.

Chapter 12, “Configuring Proxylet”

This chapter describes how to configure Proxylet from the Sun Java™ System Identity Server administration console.

Chapter 13, “Configuring SSL Accelerators”

This chapter describes how to configure various accelerators for Portal Server Secure Remote Access.

Appendix A, "Log Files"

This appendix lists all the Portal Server Secure Remote Accesslog files and their descriptions.

Appendix B, "Configuration Attributes"

This appendix lists the attributes you set for Portal Server Secure Remote Access on the Sun Java™ System Identity Server administration console.

Appendix C, "Country Codes"

This appendix lists the two-letter country codes that you need to specify during certificate administration.

Glossary

This glossary contains the link to the global glossary for the Sun Java System.

Document Conventions Used in This Guide

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.

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, 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 `xx` command described as follows:

```
xx [options] [action] [component]
```

The presence of `[options]`, `[arguments]`, and `[component]` indicates that there are optional parameters that may be added to the `xx` command.

Command-Line Prompts

Command-line prompts (for example, `%` for a C-Shell, or `$` for a Korn or Bourne shell) are not displayed in the examples. Depending on which operating system environment you are using, you will see a variety of different command-line prompts. However, you should enter the command as it appears in the document unless specifically noted otherwise.

Where to Find Related Information

SRA Documentation

Listed below are additional SRA documents.

- *Portal Server Secure Remote Access Attribute Online Help*
- *Portal Server Secure Remote Access Netlet Online (client) Help*
- *Portal Server Secure Remote Access NetFile Java1 Online (client) Help*
- *Portal Server Secure Remote Access NetFile Java2 Online (client) Help*
- *Portal Server Secure Remote Access Proxylet Online (client) Help*

Portal Server Documentation

The Sun Java™ System Portal Server documentation suite also includes the following:

- *Portal Server Administration Guide*
- *Portal Server Migration Guide*
- *Portal Server Desktop Customization Guide*
- *Portal Server Developer's Guide*

Documents Referenced in This Guide

Other documents referenced in this guide:

- *Identity Server Administration Guide*
- *Sun Crypto Accelerator 1000 Board Installation and User’s Guide*

This guide can be found at:
http://www.sun.com/products-n-solutions/hardware/docs/pdf/816-2450-11.pdf

Related Third-Party Web Site References

You can access the Sun technical documentation online at http://docs.sun.com. You can browse the archive or search for a specific book title or subject.

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 by or in connection with the use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Where to Find This Guide Online

You can access the Sun technical documentation online at http://docs.sun.com. You can browse the archive or search for a specific book title or subject.

Chapter 1

Introduction to Portal Server Secure Remote Access

This chapter describes Sun Java™ System Portal Server Secure Remote Access (formerly Sun ONE™ Portal Server, Secure Remote Access) and the relationship between Sun Java™ System Portal Server (Portal Server) software and Sun Java System Portal Server Secure Remote Access (SRA) components.

This chapter covers the following topics:

- Overview of SRA Software
- SRA Services
- Administering the SRA Product
- Configuring SRA Attributes
- Supported Applications

Overview of SRA Software

SRA software enables remote users to securely access their organization's network and its services over the Internet. Additionally, it gives your organization a secure internet portal, providing access to content, applications, and data to any targeted audience—employees, business partners, or the general public.

SRA software offers browser-based secure remote access to portal content and services from any remote device. It is a cost-effective, secure access solution that is accessible to users from any device with a Java technology-enabled browser, eliminating the need for client software. Integration with Portal Server ensures that users receive secure encrypted access to the content and services that they have permission to access.

SRA software is targeted towards enterprises deploying highly secure remote access portals. These portals emphasize security, protection, and privacy of intranet resources. The SRA architecture is well suited to these types of portals. SRA software enables users to securely access intranet resources through the Internet without exposing these resources to the Internet.

The Gateway, residing in the Demilitarized Zone (DMZ), provides a single secure access point to all intranet URLs, file systems and applications. All other non-SRA services such as Session, Authentication, and the standard PortalDesktop reside behind the DMZ in the secured intranet. Communication from the client browser to the Gateway is encrypted using HTTPS. Communication from Gateway to the server and intranet resources can be either HTTP or HTTPS.

SRA software uses two methods

The Netlet and NetFile applets are downloaded to the client machine, while the support files may reside either on the Gateway or on the Portal Server host.

The Portal Server can function in two modes:

- Open Mode
- Secure Mode

Open Mode

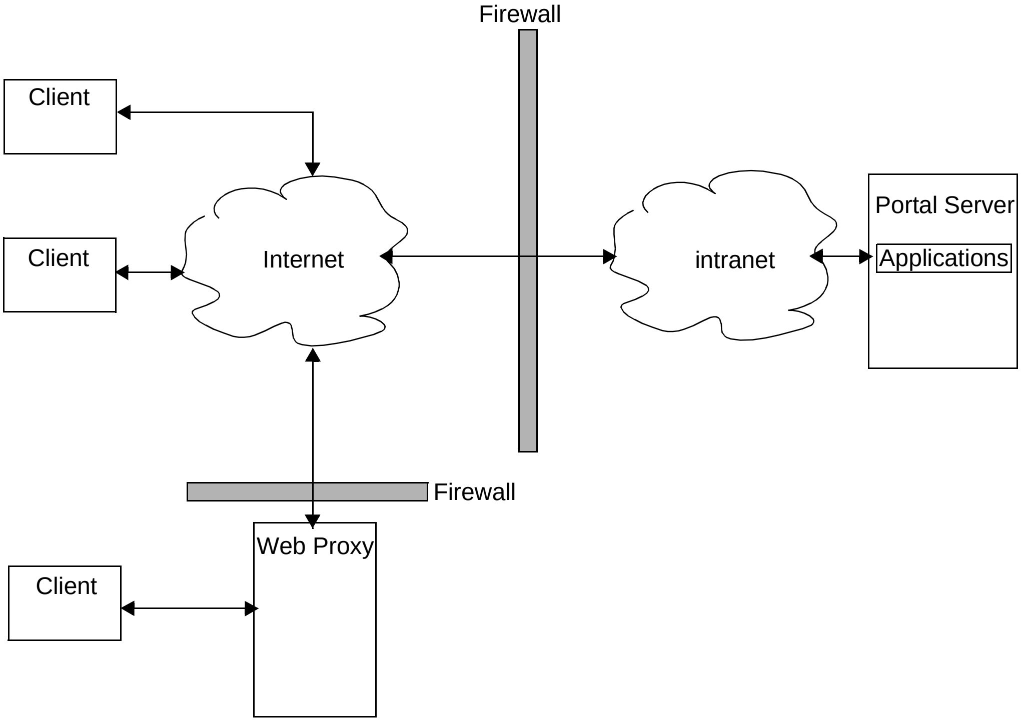
In open mode, Portal Server is installed without SRA software. Although HTTPS communication is possible in this mode, secure remote access is not possible. This means that users cannot access secure remote file systems and applications.

The main difference between an open portal and a secure portal is that the services presented by the open portal typically reside within the demilitarized zone (DMZ) and not within the secured intranet. A DMZ is a small protected network between the public Internet and a private intranet, usually demarcated with firewalls on both ends.

If the portal does not contain sensitive information (deploying public information and allowing access to free applications), then responses to access requests by a large number of users is faster than using secure mode.

Figure 1-1 shows Portal Server in open mode. Here, Portal Server is installed on a single server behind the firewall. Multiple clients access Portal Server across the Internet through the single firewall.

Figure 1-1 The Portal Server in Open Mode



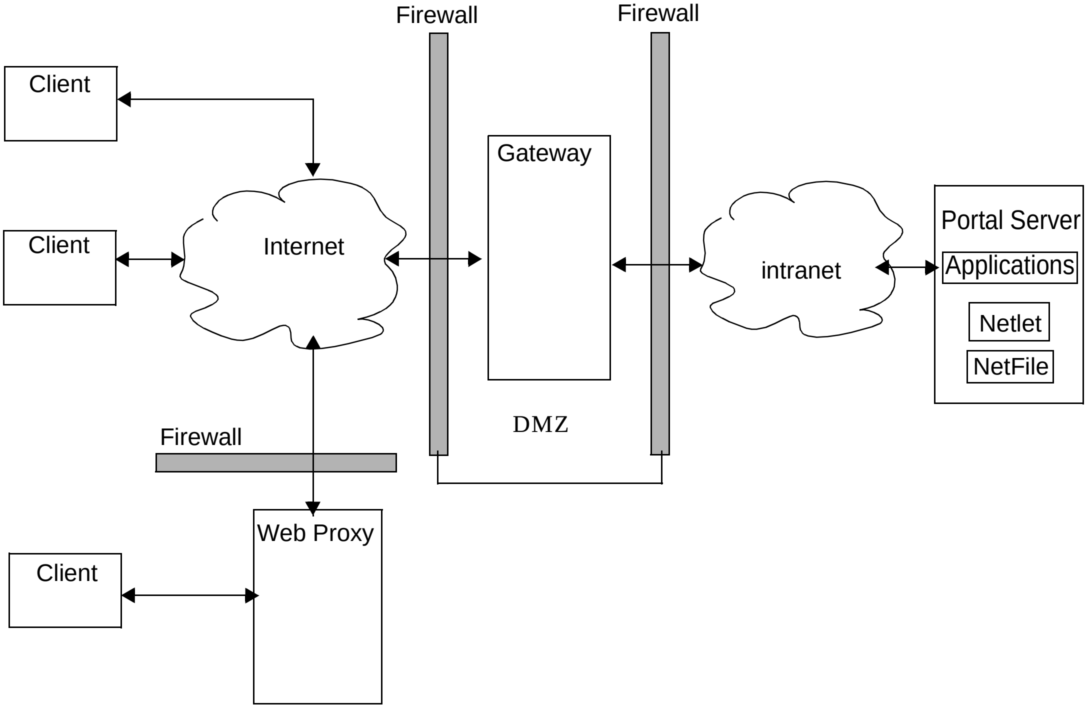
Secure Mode

Secure mode provides users with secure remote access to required intranet file systems and applications.

Gateway resides in the demilitarized zone (DMZ). Gateway provides a single secure access point to all intranet URLs and applications, thus reducing the number of ports to be opened in the firewall. All other Portal Server services such as Session, Authentication, and the standard Portal Desktop reside behind the DMZ in the secured intranet. Communication from the client browser to the Gateway is encrypted using HTTP over Secure Sockets Layer (SSL). Communication from the Gateway to the server and intranet resources can be either HTTP or HTTPS.

Figure 1-2 shows Portal Server with SRA software. SSL is used to encrypt the connection between the client and the Gateway over the Internet. SSL can also be used to encrypt the connection between the gateway and the server. The presence Gateway between the intranet and the Internet extends the secure path between the client and the Portal Server.

Figure 1-2 Portal Server in Secure Mode (with SRA software)



Additional servers and gateways can be added for site expansion. SRA software can be configured in various ways based on the business requirement.

SRA Services

SRA software has five major components:

- Gateway
- Rewriter
- NetFile
- Netlet
- Proxylet

Gateway

The SRA Gateway provides the interface and security barrier between remote user sessions originating from the Internet and your corporate intranet. Gateway presents content securely from internal web servers and application servers through a single interface to a remote user.

The web servers use web-based resources such as HTML, JavaScript and XML to communicate between the client and Gateway. Rewriter is the Gateway component used to make web content available.

The application servers use binary protocol such as telnet and FTP to communicate between the client and Gateway. Netlet which resides on Gateway is used for this purpose. See Chapter 2, "The Gateway" for more detail.

Rewriter

Rewriter enables end-users to browse the intranet and makes links and other URL references on those pages operate correctly. Rewriter prepends the Gateway URL in the location field of the web browser, thereby redirecting content requests through Gateway. See Chapter 3, "Proxylet and Rewriter" for details.

NetFile

NetFile is a file manager application that allows remote access and operation of file systems and directories. NetFile includes NetFile Java™, a Java-based user interface. This is available for Java 1 and Java 2. See Chapter 4, "NetFile" for details.

Netlet

Netlet facilitates the running of popular or company-specific applications on remote desktops in a secure manner. After you implement Netlet at your site, users can securely run common TCP/IP services, such as Telnet and SMTP, and HTTP-based applications such as pcANYWHERE or Lotus Notes. See Chapter 5, "Netlet" for details.

Proxylet

Proxylet is a dynamic proxy server that runs on a client machine. Proxylet redirects a URL to the Gateway. It does this by reading and modifying the proxy settings of the browser on the client machine so that they point to the local proxy server or Proxylet.

Administering the SRA Product

SRA software has two interfaces for administration:

- The Identity Server administration console
- The command-line

Most administration tasks are performed through the web-based Sun Java System Identity Server administration console. The administration console can be accessed locally or remotely from a web browser. However, tasks such as file modification must be administered through the UNIX command-line interface.

Configuring SRA Attributes

You can configure attributes related to SRA at the organization, role, and user levels, with the following exceptions:

- Conflict Resolution Level cannot be set at the user level. It is also not available from the Service Configuration tab. See "Setting Conflict Resolution" on page 35.
- MIME types Configuration File Location attribute can be set only at the organization level. See "Specify the MIME-types Configuration File Location" on page 299.

Values set at the organization level are inherited by all roles and users under that organization. Values set at the user level override the values set at the organization or role levels.

Most attributes can be set from either the Identity Server tab or the Service Configuration tab on the Identity Server. The attributes set at the Service Configuration level serve as a template. Any new organization or user that is created inherits these values by default.

You can make changes to the attribute values at the Service Configuration level. These new values are reflected only when new organizations are added. Changes in the attribute values at the Service Configuration tab do not affect existing organizations or users. See the *Identity Server Administration Guide* for details.

You configure SRA attributes on the Identity Server administration console under SRA Configuration using the following services:

- Access List

  This service allows you to allow or restrict access to specific URLs and to manage the single sign-on feature. See Chapter 8, "Configuring URL Access Control" for more information.

- Gateway

  This service allows you to configure all Gateway related attributes such as proxy management, cookie management, logging, rewriter management, and ciphers. See Chapter 9, "Configuring the Gateway" for more information.

- NetFile

  This service allows you to configure all NetFile related attributes such as common hosts, MIME types, and access to different types of hosts. See Chapter 10, "Configuring NetFile" for more information.

- Netlet

  This service allows you to configure all Netlet related attributes such as Netlet rules, access to required rules, organizations and hosts, and the default algorithm. See Chapter 11, "Configuring Netlet" for more information.

- Proxylet

  This service allows you to configure Proxylet related attributes such as Proxylet Applet Bind IP address and port number. See Chapter 12, "Configuring Proxylet" for more information.

CAUTION The Gateway does not receive notifications for attribute changes that are made while Gateway is running.

Restart Gateway to ensure that updated profile attributes (belonging to the Gateway or any other service) are used by Gateway. See "Using Authentication Chaining" on page 76.

Setting Conflict Resolution

➤ **To Set the Conflict Resolution Level**

1. Log in to the Identity Server administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View drop-down list.
6. Click the arrow next to appropriate service (Access List, NetFile, or Netlet) under SRA Configuration.
7. Select the required level from the Conflict Resolution Level field drop-down list.
8. Click Save at the top or bottom of the NetFile page to record the change.

Supported Applications

SRA software supports the following applications:

- SRA software supports MS Exchange 2000 SP3 installation and MS Exchange 2003 of Outlook Web Access (OWA)..

  The ruleset required for OWA pages is installed out of the box with the name `exchange_2003_owa_ruleset`. To view the case study for OWA see "Ruleset for Outlook Web Access" on page 272.
- iNotes - Notes 5.0.11
- Calendar - Sun ONE Calendar Server Release 5.1.1 and later
- Messenger Express - iPlanet Messaging Server 5.2 and later

Chapter 2

The Gateway

This chapter describes Gateway related concepts and information required for the smooth running of the Gateway. For information on configuring the Gateway, see Chapter 9, “Configuring the Gateway”.

This chapter covers the following topics:

- Overview of the Gateway
- Creating a Gateway Profile
- Understanding the platform.conf File
- Running the Gateway in the chroot Environment
- Restarting Gateway in the chroot Environment
- Creating Multiple Instances of a Gateway
- Starting and Stopping the Gateway
- Restarting the Gateway
- Specifying a Virtual Host
- Specifying a Proxy to Contact the Identity Server
- Using Web Proxies
- Using Automatic Proxy Configuration
- Using a Netlet Proxy
- Using a Rewriter Proxy
- Using a Reverse Proxy with the Gateway
- Obtaining Client Information
- Using Authentication Chaining

- Using Wild Card Certificates
- Disabling Browser Caching
- Customizing the Gateway Service User Interface
- Using Federation Management

Overview of the Gateway

The Gateway provides the interface and security barrier between remote user sessions originating from the Internet and your corporate intranet. The Gateway presents content securely from internal web servers and application servers through a single interface to a remote user.

Creating a Gateway Profile

A gateway profile contains all the information related to gateway configuration, such as the port on which the Gateway listens, SSL options, and proxy options.

When you install a Gateway, if you choose the default values, a default gateway profile called "default" is created. A configuration file corresponding to the default profile exists at:

```
/etc/opt/SUNWps/platform.conf.default
```

where `/etc/opt/SUNWps` is the default location for all the `platform.conf.*` files.

See "Understanding the platform.conf File" on page 40 for more information on the contents of the `platform.conf` file.

You can:

- Create multiple profiles, define attributes for each profile, and assign these profiles to different Gateways as required.
- Assign a single profile to Gateway installations on different machines.

- Assign different profiles to instances of a single Gateway running on the same machine.

CAUTION Do not assign the same profile to different instances of the Gateway running on the same machine. This will cause a conflict since the port numbers will be the same.

Do not specify the same port numbers in the different profiles created for the same Gateway. Running multiple instances of the same Gateway with the same port will cause a conflict.

➤ To Create a Gateway Profile

1. Log in to the Sun Java™ System Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays in the right pane.
4. Click New.

   The Create New Gateway Profile page displays.
5. Enter the name of new gateway profile.
6. Select the profile to use for creating the new profile from the drop-down list.

   By default, any new profile that you create is based on the pre-packaged default profile. If you have created a custom profile, you can select that profile from the drop-down list. The new profile inherits all the attributes of the selected profile.
7. Click Create.

   The new profile is created you are returned to the Gateway page, where the new profile is listed.
8. Restart the Gateway with this gateway profile name if you want the changes to take effect:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

To configure the Gateway, see Chapter 9, “Configuring the Gateway”.

Understanding the platform.conf File

The `platform.conf` file is located by default at:

```
/etc/opt/SUNWps
```

The `platform.conf` file contains the details that the Gateway needs. This section provides a sample `platform.conf` file and describes all the entries.

The advantage of including all the machine-specific details in the configuration file is that a common profile can be shared by Gateways running on multiple machines.

Here is a sample:

```
#

# Copyright 11/28/00 Sun Microsystems, Inc. All Rights Reserved.

# "@(#)platform.conf1.38 00/11/28 Sun Microsystems"

#

gateway.user=noaccess

gateway.jdk.dir=/usr/java_1.3.1_06

gateway.dsame.agent=http://pserv2.iportal.com:8080/sunportal/RemoteConfigS
ervlet

portal.server.protocol=http

portal.server.host=pserv2.iportal.com

portal.server.port=8080

gateway.protocol=https

gateway.host=siroe.india.sun.com

gateway.port=333

gateway.trust_all_server_certs=true

gateway.trust_all_server_cert_domains=false

gateway.virtualhost=siroe1.india.sun.com 10.13.147.81

gateway.virtualhost.defaultOrg=o=root,dc=test,dc=com

gateway.notification.url=/notification

gateway.retries=6

gateway.debug=error
gateway.debug.dir=/var/opt/SUNWps/debug
gateway.logdelimiter=&&
gateway.external.ip=10.12.147.71
gateway.certdir=/etc/opt/SUNWps/cert/portal
gateway.allow.client.caching=true
gateway.userProfile.cacheSize=1024
gateway.userProfile.cacheSleepTime=60000
gateway.userProfile.cacheCleanupTime=300000
gateway.bindipaddress=10.12.147.71
gateway.sockretries=3
gateway.enable.accelerator=false
gateway.enable.customurl=false
gateway.httpurl=http://siroe.india.sun.com
gateway.httpsurl=https://siroe.india.sun.com
gateway.favicon=https://siroe.india.sun.com
gateway.logging.password=ALKJDF123SFLKJJSDFU
portal.server.instance=
gateway.cdm.cacheSleepTime
gateway.cdm.cacheCleanUpTime
```

Table 2-1 lists and describes all the fields in the `platform.conf` file.

Table 2-1 The platform.conf File Properties

Entry	**Default Value**	**Description**
`gateway.user`	noaccess	The Gateway runs as this user. The Gateway must be started as root and after initialization, it loses its root privileges to become this user.
`gateway.jdk.dir`		This is the location of the JDK directory that the Gateway uses.
`gateway.dsame.agent`		This is the URL of the Identity Server that the Gateway contacts while starting up to get its profile.

Table 2-1 The platform.conf File Properties

Entry	Default Value	Description

`portal.server.protocol`
`portal.server.host`
`portal.server.port`
		This is the protocol, host and port that the default Portal Server installation is using.

`gateway.protocol`
`gateway.host`
`gateway.port`
		This is the Gateway protocol, host and port. These values are the same as the mode and port that you specified during installation. These values are used to construct the notification URL.

`gateway.trust_all_server_certs`	true	This indicates whether the Gateway has to trust all server certificates, or only those that are in the Gateway certificate database.
`gateway.trust_all_server_cert_domains`	false	Whenever there is an SSL communication between the Gateway and a server, a server certificate is presented to the Gateway. By default, the Gateway checks if the server host name is the same as the server certificate CN. If this attribute value is set to true, the Gateway disables the domain check for the server certificate that it receives.
`gateway.virtualhost`		If the Gateway machines has multiple hostnames configured, you can specify a different name and identity provider address in this field.

Table 2-1 The platform.conf File Properties

Entry	Default Value	Description

`gateway.virtualhost.defaultOrg=org`		This specifies the default Org to which the user will log into.
		For example suppose the virtual host field entries are the following:
		`gateway.virtualhost=test.com employee.test.com`
		`Managers.test.com`
		with the default org entries as:
		`test.com.defaultOrg = o=root,dc=test,dc=com`
		`employee.test.com.defaultOrg = o=employee,dc=test,dc=com`
		`Manager.test.com.defaultOrg = o=Manager,dc=test,dc=com`
		The user can use `https://manager.test.com` to log into the manager's org instead of `https://test.com/o=Manager,dc=test,dc=com`
		Note: virtualhost and defaultOrg are case sensitive in the `platform.conf file`, but no when using it in the URL.

`gateway. notification.url`		A combination of the Gateway host, protocol and port is used to construct the notification URL. This is used to receive session notification from the Identity Server. Ensure that the notification URL is not the same as any organization name. If the notification URL matches an organization name, a user trying to connect to that organization will get a blank page instead of the login page.
`gateway.retries`		This is the number of times that the Gateway tries to contact the Portal Server while starting up.

Table 2-1 The platform.conf File Properties

Entry	Default Value	Description
`gateway.debug`	`error`	This sets the debug level of the Gateway. The debug log file is located at *debug-directory*`/files`. The debug file location is specified in the `gateway.debug.dir` entry. The debug levels are: error - Only serious errors are logged in the debug file. The Gateway usually stops functioning when such errors occur. warning - Warning messages are logged. message - All debug messages are logged. on - All debug messages are displayed on the console. The debug files are: `srapGateway.`*gateway-profile-name* - Contains the Gateway debug messages. `Gateway_to_from_server.`*gateway-profile-name* - In message mode, this file contains all the requests and response headers between the Gateway and internal servers. To generate this file, change the write permission on `/var/opt/SUNWps/debug` directory. `Gateway_to_from_browser.`*gateway-profile-name* - In message mode, this file contains all the requests and response headers between the Gateway and the client browser. To generate this file, change the write permission on `/var/opt/SUNWps/debug` directory.
`gateway.debug.dir`		This is the directory where all the debug files are generated. This directory should have sufficient permissions for the user mentioned in `gateway.user` to write to files.
`gateway.logdelimiter`		Not used currently.

Table 2-1 The platform.conf File Properties

Entry	Default Value	Description
`gateway.external.ip`		In case of a multi-homed Gateway machine (one with multiple IP addresses), you need to specify the external IP address here. This IP is used for Netlet to run FTP.
`gateway.certdir`		This specifies the location of the certificate database.
`gateway.allow.client.caching`	true	Allow or disallow client caching. If allowed, client browsers can cache static pages and images for better performance (by reduced network traffic). If disallowed, there is higher security as nothing is cached at the client side but there will be a performance drop with the higher network load.
`gateway.userProfile.cacheSize`		This is the number of user profile entries that get cached at the Gateway. If the number of entries exceeds this value, frequent retries occur to cleanup the cache.
`gateway.userProfile.cacheSleepTime`		Sets the sleep time, in seconds, for the cache cleanup.
`gateway.userProfile.cacheCleanupTime`		The maximum time in seconds after which a profile entry can get removed.
`gateway.bindipaddress`		On a multihomed machine, this is the IP address to which the Gateway binds its serversocket. To configure the Gateway to listen to all interfaces, replace the ip address so that the `gateway.bindipaddress=0.0.0.0`
`gateway.sockretries`	3	Not used currently.
`gateway.enable.accelerator`	false	If set to true external accelerator support is allowed.
`gateway.enable.customurl`	false	If set to true the administrator is allowed to specify a custom URL for the Gateway to rewrite pages to.
`gateway.httpurl`		Enter the HTTP reverse proxy URL to set a custom URL for the Gateway to rewrite pages to.

Table 2-1 The platform.conf File Properties

Entry	**Default Value**	**Description**
`gateway.httpsurl`		Enter the HTTPS reverse proxy URL to set a custom URL for the Gateway to rewrite pages to.
`gateway.favicon`		This specifies the URL to which the Gateway will redirect requests for the favicon.ico file. This is used for the "favorite icon" in Internet Explore and Netscape 7.0 and higher's preferences or favorites. If left empty, the Gateway will send a 404 not found message back to browser.
`gateway.logging.password`		This field contains the LDAP password of the user "amService-srapGateway" that gateway uses for creating its application session. This can be either encrypted or in plain text.
`http.proxyHost`		This proxy host is used to contact the Portal Server.
`http.proxyPort`		This is the port for the host used to contact Portal Server.
`http.proxySet`		This property is set to true if a proxy host is required. If the property is set to false,http.proxyHost and http.proxyPort are ignored.
`portal.server.`*instance*		The value of this property is the corresponding /etc/opt/SUNWam/config/AMConfig-*instance-name*.properties file. If the value is default, then it points to AMConfig-default.properties.
`gateway.cdm.cacheSleepTime`		The time out value for cache Client Detection Module responses sent to the Gateway from the Identity Server.
`gateway.cdm.cacheCleanupTime`		The time out value for cache Client Detection Module responses sent to the Gateway from the Identity Server.

Running the Gateway in the chroot Environment

To provide high security in a chroot environment, the chroot directory content must be as minimal as possible. For example, if any programs exist which allow a user to modify a file under the chrooted directory, then chroot will not protect the server against an attacker modifying files under the chroot tree. CGI programs should not be written in an interpreted language, such as bourne shell, c-shell, korn shell or perl, but should be compiled binaries so interpreters do not need to be present under the chroot directory tree.

NOTE The watchdog feature is not supported in the chroot environment.

➤ To Install chroot

1. As root, in a terminal window, copy the following files to an external source such as a computer on the network, a backup tape or a floppy disk.

   `cp /etc/vfstab` *external-device*

   `cp /etc/nsswitch.conf` *external-device*

   `cp /etc/hosts` *external-device*

2. Run the `mkchroot` script from:

   portal-server-install-root`/SUNWps/bin/chroot`

NOTE The `mkchroot` script cannot be terminated by pressing Ctrl-C after execution has begun.

In the event of an error during the execution of the `mkchroot` script, see "Execution Failure of the mkchroot Script" on page 49.

You are prompted for a different root directory (new_root_directory). The script creates the new directory.

In the following examples, `/safedir/chroot` is the new_root_directory.

```
mkchroot version 6.0

Enter the full path name of the directory which will be the chrooted
tree:/safedir/chroot
Using /safedir/chroot as root.
Checking available disk space...done
```

```
mkchroot version 6.0
/safedir/chroot is on a setuid mounted partition.
Creating filesystem structure...dev etc sbin usr var proc opt bin lib tmp
etc/lib usr/platform usr/bin usr/sbin usr/lib usr/openwin/lib var/opt
var/tmp dev/fd done
Creating devices...null tcp ticots ticlts ticotsord tty udp zero conslog
done
Copying/creating etc files...group passwd shadow hosts resolv.conf netconfig
nsswitch.conf
done
Copying binaries..................................done
Copying libraries.....................................done
Copying zoneinfo (about 1 MB)..done
Copying locale info (about 5 MB)..........done
Adding comments to /etc/nsswitch.conf ...done
Creating loopback mount for/safedir/chroot/usr/java1.2...done
Creating loopback mount for/safedir/chroot/proc...done
Creating loopback mount for/safedir/chroot/dev/random...done
Do you need /dev/fd (if you do not know what it means, press return)[n]:
Updating /etc/vfstab...done
Creating a /safedir/chroot/etc/mnttab file, based on these loopback mounts.
Copying SRAP related data ...
Using /safedir/chroot as root.
Creating filesystem structure...........done
mkchroot successfully done.
```

3. Manually mount the Java directory mentioned in the `platform.conf` file to the chroot directory using the following command:

   ```
   mkdir -p /safedir/chroot/java-dir
   ```

   ```
   mount -F lofs java-dir /safedir/chroot/java-dir
   ```

   For Solaris 9, do the following:

   ```
   mkdir -p /safedir/chroot/usr/lib/32
   ```

   ```
   mount -F lofs /usr/lib/32 /safedir/chroot/usr/lib/32
   ```

   ```
   mkdir -p /safedir/chroot/usr/lib/64
   ```

   ```
   mount -F lofs /usr/lib/64 /safedir/chroot/usr/lib/64
   ```

   To mount this directory at system startup, add a corresponding entry in the `/etc/vfstab` file:

   ```
   java-dir - /safedir/chroot/java-dir lofs - no -
   ```

   For Solaris 9:

```
/usr/lib/32 - /safedir/chroot/usr/lib/32 lofs - no -

/usr/lib/64 - /safedir/chroot/usr/lib/64 lofs - no -
```

4. Type the command below to restart the Gateway:

```
chroot /safedir/chroot ./gateway-install-root/SUNWps/bin/gateway start
stopping gateway ... done.
starting gateway ...
done.
```

Execution Failure of the mkchroot Script

In the event of an error during the execution of the `mkchroot` script, the script will restore the files to their initial state.

In the following examples, `/safedir/chroot` is the chroot directory.

If the following error message is encountered:

```
Not a Clean Exit
```

1. Copy the backed up files in step 1 of the procedure To Install chroot, to their original locations, and execute the following commands:

   ```
   umount /safedir/chroot/usr/java1.2

   umount /safedir/chroot/proc

   umount /safedir/chroot/dev/random
   ```

2. Remove the `/safedir/chroot` directory.

Restarting Gateway in the chroot Environment

Follow these steps to start Gateway in a chroot environment whenever the Gateway machine is rebooted.

➤ To Restart Gateway in the chroot Environment

1. Stop Gateway running from the ’/’ directory.

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `stop`

2. Start the Gateway to run from the chroot directory:

   `chroot /safedir/chroot ./`*portal-server-install-root*`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

NOTE The `/safedir/chroot/etc` files (such as `passwd` and `hosts`) need to be administered, just like the `/etc` files, but only include host and account information required by the programs running in the chroot tree.

For example, if you change the identity provider address of the system, also change the file `/safedir/chroot/etc/hosts`.

Creating Multiple Instances of a Gateway

Use the `gwmultiinstance` script to create a new instance of the Gateway. It's preferable to run this script after the gateway profile has been created.

1. Log in as root and navigate to the following directory:

   gateway-install-root`/SUNWps/bin/`

2. Run the multi-instance script:

   ```
   ./gwmultiinstance
   ```

3. Choose one of the following installation options:

```
1) Create a new gateway instance

2) Remove a gateway instance

3) Remove all gateway instances

4) Exit
```

If you chose 1, answer the following questions:

```
What is the name of the new gateway instance?

What protocol will the new gateway instance use? [https]

What port will the new gateway instance listen on?

What is the fully qualified hostname of the portal server?

What port should be used to access the portal server?

What protocol should be used to access the portal server? [http]

What is the portal server deploy URI?

What is the organization DN? [dc=iportal,dc=com]

What is the identity server URI? [/amserver]

What is the identity server password encryption key?


Please provide the following information needed for creating a
self-signed certificate:

What is the name of your organization?

What is the name of your division?

What is the name of your city or locality?

What is the name of your state or province?

What is the two-letter country code?

What is the password for the Certificate Database? Again?


What is the password for the logging user? Again?

Have you created the new gateway profile in the admin console? [y]/n

Start the gateway after installation? [y]/n
```

4. Start the new instance of the Gateway with the new gateway profile name.

   gateway-install-root / SUNWps / bin / gateway -n *gateway-profile-name* start

   where *gateway-profile-name* is the new Gateway instance.

In addition to the gateway profile, the `AMConfig-.`*instance-name*`.properties` file is created in the `/etc/opt/SUNWam/config` directory.

If the `portal.server.instance` property in the `platform.conf` file is present, then the corresponding `AMConfig-`*instance-name*`.properties` file is read by the Gateway. If the `portal.server.instance` property in the `platform.conf file` is not present, then the default AMConfig files (AMConfig.properties) is read by the Gateway.

Creating Multi-homed Gateway Instances

If you are creating multi-homed gateway instances, that is multiple gateways on one Portal Server, you must modify the `platform.conf` file as follows:

```
gatewaybindipaddress = 0.0.0.0
```

Creating Gateway Instances Using the Same LDAP

If you are creating multiple gateway instances that use the same LDAP, after creating the first Gatewayon all subsequent Gateways:

In /etc`/opt/SUNWam/config/`, modify the following areas in `AMConfig-`*instance-name*`.properties` to be in sync with the first installed instance of the Gateway:

1. Replace the key that is used to encrypt and decrypt passwords with the same string used for the first Gateway.

   `am.encryption.pwd=` *`string_key_specified_in gateway-install`*

2. Replace the key that is the shared secret for application auth module

   `com.iplanet.am.service.secret=` *`string_key_specified_in gateway-install`*

3. In `/etc/opt/SUNWam/config/ums` modify the following areas in `serverconfig.xml` to be insync with the first installed instance of Portal-Identity Server:

```
<DirDN> cn=puser,ou=DSAME Users,dc=sun,dc=net</DirDN>
```

`<DirPassword>`*`string_key_specified_in gateway-install`*`</DirPassword>`

```
<DirDN>cn=dsameuser,ou=DSAME Users,dc=sun,dc=net</DirDN>
```

`<DirPassword>`*`string_key_specified_in gateway-install`*` </DirPassword>`

4. Restart amserver services.

Starting and Stopping the Gateway

By default, the Gateway starts as user `noaccess`.

➤ To Start the Gateway

1. After installing the Gateway and creating the required profile, run the following command to start the Gateway:

   gateway-install-root`/SUNWps/bin/gateway -n default start`

   `default` is the default gateway profile that is created during installation. You can create your own profiles later, and restart the Gateway with the new profile. See "Creating a Gateway Profile" on page 38.

   If you have multiple Gateway instances, use:

   gateway-install-root`/SUNWps/bin/gateway start`

This command starts all the Gateway instances configured on that particular machine.

NOTE Restarting the server (the machine on which you have configured instances of the Gateway) restarts all configured instances of the Gateway.

Ensure that there are no old or backed up profiles in the `/etc/opt/SUNWps` directory.

2. Run the following command to check if the Gateway is running on the specified port:

   ```
   netstat -a | grep port-number
   ```

   The default Gateway port is 443.

➤ To Stop the Gateway

1. Use the following command to stop the Gateway:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name stop
   ```

   If you have multiple Gateway instances, use:

   ```
   gateway-install-root/SUNWps/bin/gateway stop
   ```

   This command stops all the Gateway instances that are running on that particular machine.

2. Run the following command to check if the Gateway processes are no longer running:

   ```
   /usr/bin/ps -ef | entsys
   ```

Restarting the Gateway

Normally, you do not need to restart the Gateway. You need to restart only if any of the following events have occured:

- You have created a new profile and need to assign the new profile to the Gateway.
- You have modified some attributes in the existing profile and need the changes to take effect.

➤ To Restart the Gateway with a Different Profile

Restart the Gateway:

```
gateway-install-root/SUNWps/bin/gateway -n new-gateway-profile-name start
```

➤ To Restart the Gateway

In a terminal window, connect as root and do one of the following:

- Start the watchdog process:

```
gateway-install-root/SUNWps/bin/gateway watchdog on
```

This creates an entry in the crontab and the watchdog process is now active. The watchdog monitors all running instances of a Gateway on a particular machine and Gateway port and restarts the Gateway if it goes down.

➤ To Configure the Gateway Watchdog

You can configure the time interval at which the watchdog monitors the status of the Gateway. This time interval is set to 60 seconds by default. To change this, edit the following line in the crontab:

```
0-59 * * * * gateway-install-root/SUNWps/bin/

/var/opt/SUNWps/.gw. 5 > /dev/null 2>&1
```

See the `crontab` man page to configure the `crontab` entries.

Specifying a Virtual Host

A virtual host is an additional hostname that points to the same machine IP and a host name. For example if a host name a.b.c points to the host IP address 192.155.205.133, you can add another host name c.d.e which points to the same IP address.

➤ To Specify a Virtual Host

1. Log in as root and edit the `platform.conf` file of the required Gateway instance:

   `/etc/opt/SUNWps/platform.conf.`*gateway-profile-name*

2. Add the following entries:

   `gateway.virtualhost=`*fully-qualified-gateway-host gateway-ip-address fully-qualified-reverse-proxyhost*

   `gateway.enable.customurl=true` (This value is set to false by default.)

3. Restart the Gateway:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

If these values are not specified, then the Gateway will default to normal behavior.

Specifying a Proxy to Contact the Identity Server

You can specify a host proxy to be used by the Gateway to contact SRA Core (RemoteConfigServlet) that is deployed over the Portal Server. This proxy is used by the Gateway to reach the Portal Server and Identity Server.

➤ To Specify a Proxy

1. From the command-line, edit the following file:

   ```
   /etc/opt/SUNWps/platform.conf.gateway-profile-name
   ```

2. Add the following entries:

   ```
   http.proxyHost=proxy-host
   http.proxyPort=proxy-port
   http.proxySet=true
   ```

3. Restart the Gateway to use the specified proxy for requests made to the server:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Using Web Proxies

You can configure the Gateway to contact HTTP resources using third party web proxies. Web proxies reside between the client and the Internet.

Web Proxy Configuration

Different proxies may be used for different domains and subdomains. These entries tell the Gateway which proxy to use to contact specific subdomains in specific domains. The proxy configuration specified in the Gateway works as follows:

- Creates a list of domains and subdomains along with the required proxies in the Proxies for Domains and Subdomains field in the Gateway service.

  For information on configuring proxies for domains and subdomains, see "Create List of Proxies for Domains and Subdomains" on page 256.

- With the Use Proxy option enabled:

  - The proxies specified in the Proxies for Domains and Subdomains field are used for the specified hosts.

- ❍ To enable direct connections for certain URLs within the domains and subdomains specified in the Proxies for Domains and Subdomains list, specify these URLs in the Do Not Use Web Proxy URLS field.

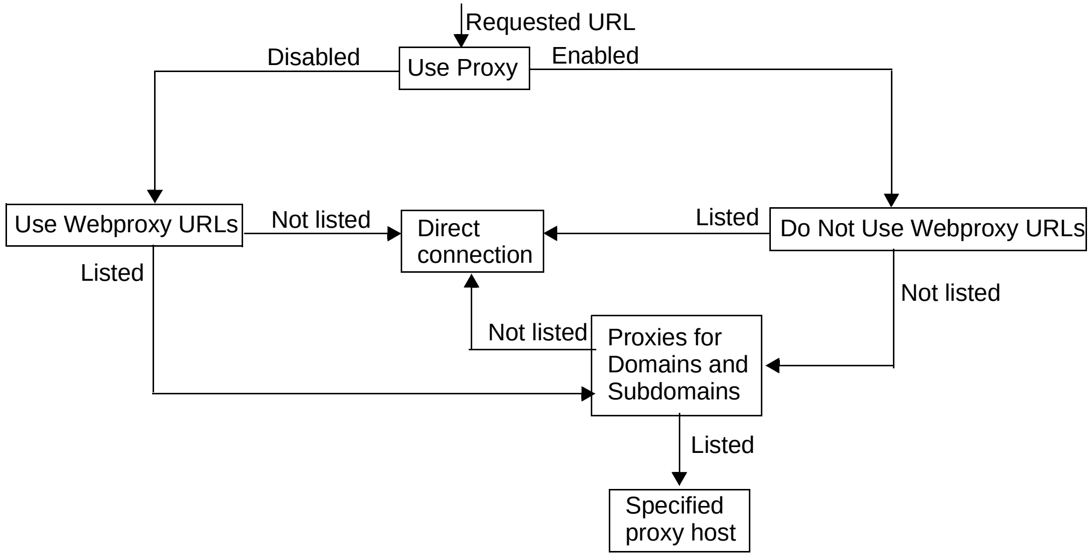
- With the Use Proxy option disabled:

  - ❍ To ensure that proxies are used for certain URLs within the domains and subdomains specified in the Proxies for Domains and Subdomains field, specify these URLs in the Use Webproxy URLs list. Although the Use Proxy option is disabled, a proxy is used to connect to the URLs listed under Use Webproxy URLs. The proxies for these URLs are obtained from the Proxies for Domains and Subdomains list.

To configure the Use Proxy option, see "Enable Usage of Web Proxies" on page 254.

Figure 2-1 shows how the web proxy information is resolved based on the proxy configuration in the Gateway service.

Figure 2-1 Web Proxy Management



In Figure 2-1, if Use Proxy is enabled, and the requested URL is listed in the Do Not Use Webproxy URLs list, the Gateway connects to the destination host directly.

If Use Proxy is enabled, and the requested URL is not listed in the Do Not Use Webproxy URLs list, the Gateway connects to the destination host through the specified proxy. The proxy, if specified, is looked up in the Proxies for Domains and Subdomains list.

If Use Proxy is disabled, and the requested URL is listed in the Use Webproxy URLs list, the Gateway connects to the destination host using the proxy information in the Proxies for Domains and Subdomains list.

If Use Proxy is disabled, and the requested URL is not listed in the Use Webproxy URLs list, the Gateway connects to the destination host directly.

If none of the above conditions are met, and a direct connection is not possible, the Gateway displays an error saying that connection is not possible.

NOTE If you are accessing the URL through the Bookmark channel of the standard Portal Desktop, and none of the above conditions are met, the Gateway sends a redirect to the browser. The browser accesses the URL using its own proxy settings.

Syntax

```
domainname [web_proxy1:port1]|subdomain1 [web_proxy2:port2]|......
```

Example

```
sesta.com wp1:8080|red wp2:8080|yellow|* wp3:8080
```

* is a wild card that matches everything

where,

`sesta.com` is the domain name and `wp1` is the proxy to contact on port 8080.

`red` is a subdomain and `wp2` is the proxy to contact on port 8080.

`yellow` is a subdomain. Since no proxy is specified, the proxy specified for the domain is used, that is, `wp1` on port 8080.

* indicates that for all other subdomains `wp3` needs to be used on port 8080.

NOTE Port 8080 is used by default if you do not specify a port.

Processing the Web Proxy Information

When a client tries to access a particular URL, the host name in the URL is matched with the entries in the Proxies for Domains and Subdomains list. The entry that matches the longest suffix of the requested host name is considered. For example, consider that the requested host name is `host1.sesta.com`

- The Proxies for Domains and Subdomains is scanned for `host1.sesta.com`. If a matching entry is found, the proxy specified against this entry is used to connect to this host.
- Else, the list is scanned for `*.sesta.com`. If an entry is found, the corresponding proxy is used.
- Else, the list is searched for `sesta.com`. If an entry is found, the corresponding proxy is used.
- Else, the list is searched for `*.com`. If an entry is found, the corresponding proxy is used.
- Else the list is searched for `com`. If an entry is found, the corresponding proxy is used.
- Else the list is searched for `*`. If an entry is found, the corresponding proxy is used.
- Else, a direct connection is attempted.

Consider the following entries in the Proxies for Domains and Subdomains list:

```
com p1| host1 p2 | host2 | * p3

sesta.com p4 | host5 p5 | * p6

florizon.com | host6

abc.sesta.com p8 | host7 p7 | host8 p8 | * p9

host6.florizon.com p10

host9.sesta.com p11

siroe.com | host12 p12 | host13 p13 | host14 | * p14

siroe.com | host15 p15 | host16 | * p16

* p17
```

The Gateway internally maps these entries into a table as shown in Table 2-2.

Table 2-2 Mapping of Entries in the Proxies for Domains and Subdomains List

Number	Entry in Proxies for Domains and Subdomains List	Proxy	Description
1	com	p1	As specified in the list.
2	host1.com	p2	As specified in the list.
3	host2.com	p1	Since there is no proxy specified against host2, the proxy for the domain is used.
4	*.com	p3	As specified in the list.
5	sesta.com	p4	As specified in the list.
6	host5.sesta.com	p5	As specified in the list.
7	*.sesta.com	p6	As specified in the list.
8	florizon.com	Direct	See the description for entry 14 for details.
9	host6.florizon.com	–	See the description for entry 14 for details.
10	abc.sesta.com	p8	As specified in the list.
11	host7.abc.sesta.com	p7	As specified in the list.
12	host8.abc.sesta.com	p8	As specified in the list.
13	*.abc.sesta.com	p9	As specified in the list. For all hosts other than `host7` and `host8` under the `abc.sesta.com` domain, `p9` is used as the proxy.
14	host6.florizon.com	p10	This entry is the same as entry 9. Entry 9 indicates a direct connection, whereas this entry indicates that proxy p10 should be used. In a case where there are two entries such as this, the entry with the proxy information is considered as the valid entry. The other entry is ignored.
15	host9.sesta.com	p11	As specified in the list.
16	siroe.com	Direct	Since there is no proxy specified against `siroe.com`, a direct connection is attempted.
17	host12.siroe.com	p12	As specified in the list.
18	host13.siroe.com	p13	As specified in the list.
19	host14.siroe.com	Direct	Since no proxy is specified for `host14`, or for `siroe.com`, a direct connection is attempted.

Table 2-2 Mapping of Entries in the Proxies for Domains and Subdomains List

Number	Entry in Proxies for Domains and Subdomains List	Proxy	Description
20	*.siroe.com	p14	See the description for entry 23.
21	host15.siroe.com	p15	As specified in the list.
22	host16.siroe.com	Direct	Since no proxy is specified for `host16`, of for `siroe.com`, a direct connection is attempted.
23	*.siroe.com	p16	This is similar to entry 20. But the proxies specified are different. In such a case, the exact behavior of the Gateway is not known. Either of the two proxies may be used.
24	*	p17	If no other entry matches the requested URL, `p17` is used as the proxy.

NOTE Instead of separating the proxy entries in the Proxies for Domains and Subdomains list with the | symbol, it may be simpler to have individual entries in the list. For example, instead of an entry such as:

```
sesta.com p1 | red p2 | * p3
```

you can specify it as:

```
sesta.com p1
red.sesta.com p2
*.sesta.com p3
```

This makes it easier to trap repeated entries or any other ambiguities.

Rewriting Based on the Proxies for Domains and Subdomains List

The entries in the Proxies for Domains and Subdomains list are also used by Rewriter. Rewriter rewrites all URLs whose domains match the domains listed in the Proxies for Domains and Subdomains list.

CAUTION The * entry in the Proxies for Domains and Subdomains list is not considered for rewriting. For example, in the sample provided in Table 2-2, entry 24 is not considered.

See Chapter 3, “Proxylet and Rewriter” for information on Rewriter.

Default Domain and Subdomain

When the destination host in the URL is not a fully qualified host name, the default domain and subdomain are used to arrive at the fully qualified name.

Assume that the entry in the Default Domains field of the administration console is:

```
red.sesta.com
```

NOTE You need to have the corresponding entry in the Proxies for Domains and Subdomains list.

In the example above, `sesta.com` is the default domain and the default subdomain is `red`.

If the requested URL is `host1`, this is resolved to `host1.red.sesta.com` using the default domain and subdomain. The Proxies for Domains and Subdomains list is then looked up for `host1.red.sesta.com`.

Using Automatic Proxy Configuration

To ignore the information in the Proxies for Domains and Subdomains list, enable the Automatic Proxy Configuration feature. To configure this, see “Enable Automatic Proxy Configuration Support” on page 258.

Please note the following when using a Proxy Auto Config (PAC) file:

- The `js.jar` must be present in the `$JRE_HOME/lib/ext` directory on the Gateway machine, otherwise the Gateway will not be able to parse the PAC file.
- Gateway fetches the PAC file at bootup from the location specified in the gateway profile Automatic Proxy Configuration File location field. To configure the location, see “Specify Automatic Proxy Configuration File Location” on page 258.
- Portal Server, Gateway, Netlet, Proxylet, and Jchardet use the Rhino software to parse the PAC file. You can install the software from the SUNWrhino package.

This package contains the `js.jar` file which must be present in the `/usr/share/lib directory`. Add this directory to the `webserver/appserver` classpath on the Gateway and Portal Server machine, otherwise the Portal Server, Gateway, Netlet, Proxylet, and Jchardet will not be able to parse the PAC file.

- Gateway uses the URLConnection API to reach this location. If the proxy needs to be configured to reach the, the proxy needs to be configured in the following way.

  a. From the command-line, edit the following file:

  `/etc/opt/SUNWps/platform.conf.`*gateway-profile-name*

  b. Add the following entries:

  `http.proxyHost=`*web-proxy-hostname*

  `http.proxyPort=`*web-proxy-port*

  `http.proxySet=true`

  c. Restart the Gateway to use the specified proxy:

  gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

- If PAC file initialization fails, then the Gateway uses the information in the Proxies for Domains and Subdomains list.
- If "" (empty string) or "null" is returned from the PAC file, then the Gateway assumes that the host does not belong to the intranet. This is similar to the host not being in the Proxies for Domains and Subdomains list.

  If you want the Gateway to use a direct connection to the host, return "DIRECT". See "Example with Either DIRECT or NULL Return" on page 64.
- Gateway only uses the first proxy returned when multiple proxies are specified. It will not try to failover or loadbalance among the various proxies specified for a host.
- Gateway ignores SOCKS proxies and attempts a direct connection and assumes that the host is part of the intranet.
- To specify a proxy to be used to reach any host not part of the intranet, use the proxy type "STARPROXY". This is an extension of the PAC file format and is similar to the entry `* proxyHost:port` in Proxies for Domains and Subdomains section of the gateway profile. See "Example with STARPROXY Return" on page 64

Sample PAC File Usage

The following examples show the URLs listed in the Proxies for Domains and Subdomains list and the corresponding PAC file.

Example with Either DIRECT or NULL Return

Using these proxies for domains and subdomains:

```
*intranet1.com proxy.intranet.com:8080

intranet2.com proxy.intranet1.com:8080
```

the corresponding PAC file is:

```
// Start of the PAC File

function FindProxyForURL(url, host) {

         if (dnsDomainIs(host, ".intranet1.com")) {

             return "DIRECT";

         }

          if (dnsDomainIs(host, ".intranet2.com")) {

              return "PROXY proxy.intranet1.com:8080";

          }

          return "NULL";

}

//End of the PAC File
```

Example with STARPROXY Return

Using these proxies for domains and subdomains:

```
intranet1.com

intranet2.com.proxy.intranet1.com:8080

internetproxy.intranet1.com:80
```

the corresponding PAC file is:

```
// Start of the PAC File

function FindProxyForURL(url, host) {

          if (dnsDomainIs(host, ".intranet1.com")) {

              return "DIRECT";
          }
          if (dnsDomainIs(host, ".intranet2.com")) {
              return "PROXY proxy.intranet1.com:8080;" +
                  "PROXY proxy1.intranet1.com:8080";
          }
          return "STARPROXY internetproxy.intranet1.com:80";
}
//End of the PAC File
```

In this case, if the request is for a host in `.intranet2.com domain`, the Gateway will contact `proxy.intranet1.com:8080`. If proxy.`intranet1.com:8080` is down, the request will fail. the Gateway will not failover and contact `proxy1.intranet1.com:8080`.

Using a Netlet Proxy

Netlet packets are decrypted at the Gateway and sent to the destination servers. However, the Gateway needs to access all Netlet destination hosts through the firewall between the demilitarized zone (DMZ) and the intranet. This requires opening a large number of ports in the firewall. The Netlet proxy can be used to minimize the number of open ports in the firewall.

The Netlet proxy enhances the security between the Gateway and the intranet by extending the secure tunnel from the client, through the Gateway to the Netlet proxy that resides in the intranet. With the proxy, Netlet packets are decrypted by the proxy and then sent to the destination.

The Netlet proxy is useful for the following reasons:

- To add an additional layer of security.
- To minimize the use of extra IP addresses and ports from the Gateway through an internal firewall in a significantly sized deployment environment.
- To restrict the number of open ports between the Gateway and the Portal Server to 1. This port number can be configured during installation.

- To extend the secure channel between the client and the Gateway, up to the Portal Server as shown in the "With a Netlet Proxy Configured" section of Figure 2-2. The Netlet proxy offers improved security benefits through data encryption but may increase the use of system resources. See the *Sun Java Enterprise System Install Guide* for information on installing the Netlet proxy.

You can:

- Choose to install the Netlet proxy on the Portal Server node or on a separate node.
- Install multiple Netlet proxies and configure them for a single Gateway using the administration console. This is useful in load balancing. "Enable and Create a List of Netlet Proxies" on page 239 for details.
- Configure multiple instances of the Netlet proxy on a single machine.
- Point multiple instances of the Gateway to a single installation of the Netlet proxy.
- Tunnel Netlet through a web proxy. To configure this, see "Enable Netlet Tunneling via Web Proxy" on page 259.

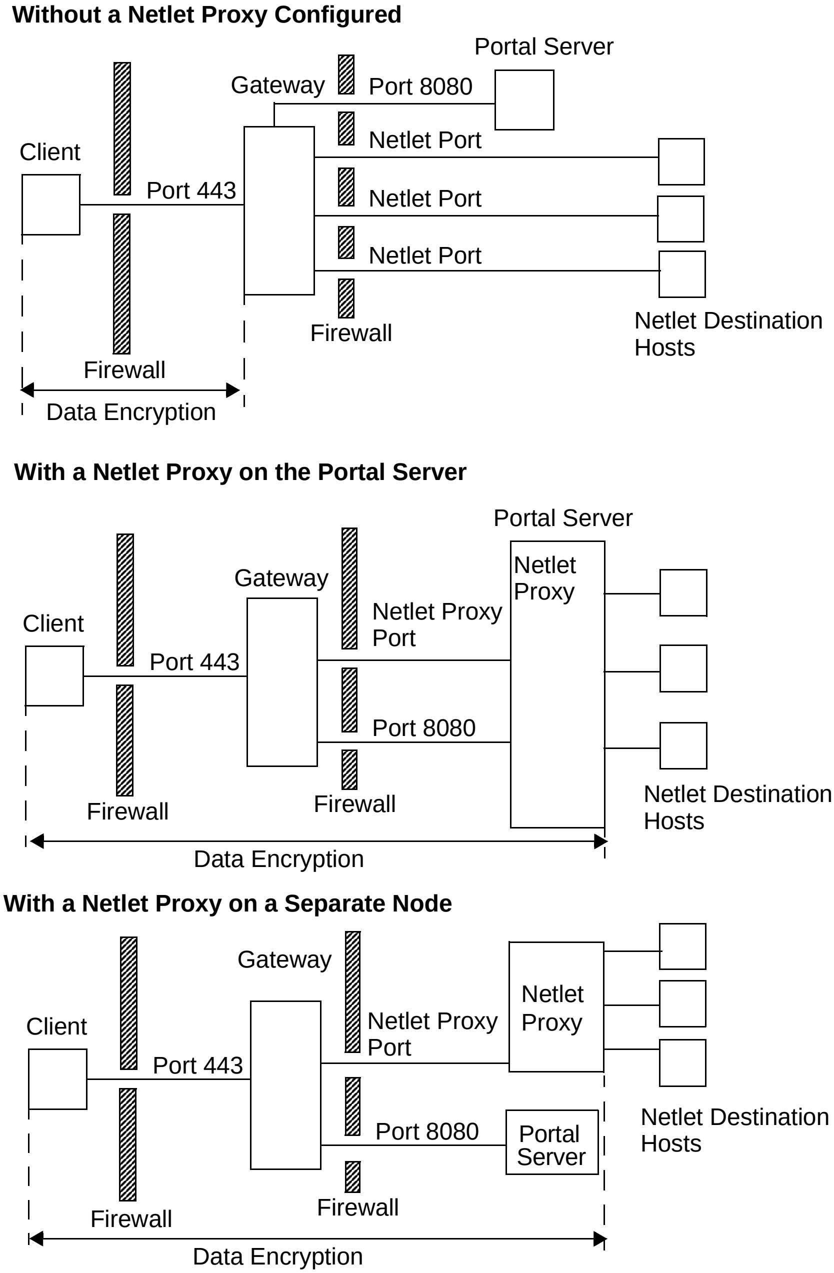
Figure 2-2 shows three sample implementations of the Gateway and the Portal Server with and without a Netlet proxy installed. The components include a client, two firewalls, the Gateway that resides between the two firewalls, Portal Server, and Netlet destination servers.

The first scenario shows the Gateway and Portal Server without a Netlet proxy installed. Here the data encryption extends only from the client to the Gateway. A port is opened in the second firewall for each Netlet connection request.

The second scenario shows the Gateway and Portal Server with a Netlet proxy installed on Portal Server. In this case, the data encryption extends from the client all the way to the Portal Server. Since all Netlet connections are routed through a Netlet proxy, only one port needs to be opened in the second firewall for Netlet requests.

The third scenario shows the Gateway and the Portal Server with a Netlet proxy installed on a separate node. Installing a Netlet proxy on a separate node reduces the load on the Portal Server node. Here again, only two ports need to be opened in the second firewall. One port services requests to the Portal Server, and the other port routes Netlet requests to the Netlet proxy server.

Figure 2-2 Implementation of Netlet Proxy



Creating Instances of a Netlet Proxy

Use the `nlpmultiinstance` script to create a new instance of a Netlet proxy on the Portal Server node or a separate node. It is preferable to run this script after the gateway profile has been created:

1. Log in as root and navigate to the following directory:

   netlet-install-dir`/SUNWps/bin`

2. Run the multi-instance script:

   ```
   ./nlpmultiinstance
   ```

3. Answer the questions asked by the `nlpmultiinstance` script:

   - What is the name of the new netlet proxy instance?
   - If you have a instance configured on this node with the same name, you are asked if you want to use the same configuration for this netlet proxy instance.
   - If you answered yes, answer these two questions:
     - What port will the new netlet proxy instance listen on?
     - Start the netlet proxy after installation?
   - If you answered no, answer the following questions:
     - What protocol will the new netlet proxy instance use?
     - What port will the new netlet proxy instance listen on?
     - What is the name of your organization?
     - What is the name of your division?
     - What is the name of your city or locality?
     - What is the name of your state or province?
     - What is the two-letter country code?
     - What is the password for the certificate Database?
     - What is the password for the logging user?
     - Have you created the new gateway profile in the admin console?
     - If you answered yes, start the netlet proxy after installation?

4. Start the new instance of the netlet proxy with the required gateway profile name:

   ```
   netlet-proxy-install-root/SUNWps/bin/netletd -n gateway-profile-name start
   ```

   where *gateway-profile-name* is the profile name corresponding to the required Gateway instance.

Enabling a Netlet Proxy

You enable a Netlet proxy through the Gateway service under SRA Configuration in the Identity Server administration console. See "Enable and Create a List of Netlet Proxies" on page 239.

Restarting a Netlet Proxy

You can configure a Netlet proxy to restart whenever the proxy is killed accidentally. You can schedule a watchdog process to monitor a Netlet proxy and restart it if it goes down.

You can also restart a Netlet proxy manually.

➤ To Restart a Netlet Proxy

In a terminal window, connect as root and do one of the following:

- Start the watchdog process:

  ```
  netlet-proxy-install-root/SUNWps/bin/netletd watchdog on
  ```

  This creates an entry in the crontab and the watchdog process is now active. The watchdog monitors the Netlet proxy port and brings up the proxy if it goes down.

- Start a Netlet proxy manually:

  ```
  netlet-proxy-install-root/SUNWps/bin/netletd -n gateway-profile-name start
  ```

  where *gateway-profile-name* is the profile name corresponding to the required Gateway instance.

➤ To Configure a Netlet Proxy Watchdog

You can configure the time interval at which the watchdog monitors the status of a Netlet proxy. This time interval is set to 60 seconds by default. To do this, edit the following line in the crontab:

```
0-59 * * * * netlet-install-dir/bin/checkgw /var/opt/SUNWps/.gw 5 > /dev/null 2>&1
```

Using a Rewriter Proxy

Rewriter proxy is installed in the intranet. Instead of trying to retrieve the contents directly, the Gateway forwards all the requests to Rewriter proxy which fetches and returns the contents to the Gateway.

There are two advantages to using a Rewriter proxy:

- If there is a firewall between the Gateway and server, the firewall needs to open only two ports - one between the Gateway and Rewriter proxy, and another between the Gateway and the Portal Server.
- HTTP traffic is now secure between the Gateway and the intranet even if the destination server only supports HTTP protocol (no HTTPS).

If you do not specify a Rewriter proxy, the Gateway component makes a direct connection to intranet computers when a user tries to access one of those intranet computers.

If you are using the Rewriter proxy as a load balancer, be sure that the platform.conf.*instance_name* for Rewriter points to the load balancer URL. Also ensure that the load balancer host is specified in the Portal Servers list.

If you have multiple instances of the Rewriter proxies for each Gateway instance (not necessarily on the portal node). In the platform.conf, rather than a single port entry for the Rewrite proxy, enter the details for each Rewriter proxy in the form of *host-name:port*.

Creating Instances of a Rewriter Proxy

Use the `rwpmultiinstance` script to create a new instance of a Rewriter proxy on the Portal Server node. It is preferable to run this script after the gateway profile has been created.

1. Log in as root and navigate to the following directory:

   rewriter-proxy-install-root/`SUNWps/bin`

2. Run the multi instance script:

   ```
   ./rwpmultiinstance
   ```

3. Answer the questions asked by the script:

   - What is the name of the new rewriter proxy instance?
   - If you have a rewriter proxy instance configured on this node with the same name, you are asked if you want to use the same configuration for this rewriter proxy instance.
   - If you answered yes, answer these two questions:
     - What port will the new rewriter proxy instance listen on?
     - Start the rewriter proxy after installation?
   - If you answered no, answer the following questions:
     - What protocol will the new rewriter proxy instance use?
     - What port will the new rewriter proxy instance listen on?
     - What is the name of your organization?
     - What is the name of your division?
     - What is the name of your city or locality?
     - What is the name of your state or province?
     - What is the two-letter country code?
     - What is the password for the certificate Database?
     - What is the password for the logging user?
     - Have you created the new gateway profile in the admin console?
     - If you answered yes, start the rewriter proxy after installation?

4. Start the new instance of the rewriter proxy with the required gateway profile name:

   rewriter-proxy-install-root`/SUNWps/bin/rwproxyd -n` *gateway-profile-name* `start`

   where *gateway-profile-name* is the profile name corresponding to the required Gateway instance.

Enabling a Rewriter Proxy

Enable a Rewriter proxy through the Gateway service under SRA Configuration in the Identity Server administration console. See "Enable and Create a List of Rewriter Proxies" on page 237.

Restarting a Rewriter Proxy

You can configure to restart Rewriter proxy whenever the proxy is killed accidentally. You can schedule a watchdog process to monitor and restart it if this happens.

You can also restart a Rewriter proxy manually.

➤ To Restart a Rewriter Proxy

In a terminal window, connect as root and do one of the following:

- Start the watchdog process:

  rewriter-proxy-install-root`/SUNWps/bin/rwproxd watchdog on`

  This creates an entry in the crontab and the watchdog process is now active. The watchdog monitors the port and brings up the proxy if it goes down.

- Start manually:

  rewriter-proxy-install-root`/SUNWps/bin/rwproxd -n` *gateway-profile-name* `start`

  where *gateway-profile-name* is the profile name corresponding to the required Gateway instance.

➤ To Configure a Rewriter Proxy Watchdog

You can configure the time interval at which the watchdog monitors the status of the Rewriter proxy. This time interval is set to 60 seconds by default. To do this, edit the following line in the crontab:

```
0-59 * * * * rewriter-proxy-install-root/bin/checkgw /var/opt/SUNWps/.gw 5 >
/dev/null 2>&1
```

Using a Reverse Proxy with the Gateway

A proxy server serves Internet content to the intranet, while a reverse proxy serves intranet content to the Internet. Deployments of reverse proxies can be configured to serve the Internet content to achieve load balancing and caching.

If the deployment has a third-party reverse proxy in front of the Gateway, the response has to be rewritten with the reverse proxy's URL instead of the Gateway's URL. For this, the following configurations are needed.

➤ To Enable a Reverse Proxy

1. Log in as root and edit the `platform.conf` file of the required Gateway instance:

   `/etc/opt/SUNWps/platform.conf.`*gateway-profile-name*

2. Add the following entries:

   `gateway.virtualhost=`*fully-qualified-gateway-host gateway-ip-address fully-qualified-reverse-proxyhost*

   `gateway.enable.customurl=true` (This value is set to false by default.)

   `gateway.httpurl=`*http reverse-proxy-URL*

   `gateway.httpsurl=`*https reverse-proxy-URL*

   `gateway.httpurl` will be used to rewrite the response for the request received at the port which is listed as HTTP port in the gateway profile.

   `gateway.httpsurl` will be used to rewrite the response for the request received at the port which is listed as HTTPS port in the gateway profile.

3. Restart the Gateway:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

If these values are not specified, then the Gateway will default to normal behavior.

Obtaining Client Information

When the Gateway forwards a client request to any internal server, it adds HTTP headers to the HTTP request. You can use these headers to obtain additional client information and detect the presence of the Gateway.

To view the HTTP request headers, set the entry in the `platform.conf` file to `gateway.error=message,` then use the request.getHeader() from the servlet API. The following table lists the information in the HTTP headers

Table 2-3 Information in HTTP Headers

Header.	**Syntax**	**Description**
PS-GW-PDC	X-PS-GW- PDC: true/false	Indicates whether PDC is enabled at the Gateway.
PS-Netlet	X-PS-Netlet:enabled=true/false	Indicates whether Netlet has been enabled or disabled at the Gateway. If it is enabled, then the encryption option is populated, indicating whether the Gateway is running in HTTPS (encryption=ssl) or in HTTP mode (encryption=plain) For example: PS-Netlet: enabled=false Netlet is disabled. PS-Netlet: enabled=true; encryption=ssl Netlet is enabled with the Gateway running in SSL mode. The encryption=ssl/plain is not populated when Netlet is not enabled.
PS-GW-URL	X-PS-GW-URL: http(s)://gatewayURL(:port)	Indicates the URL that the client is connected to. If it is non-standard port (that is the Gateway is in HTTP/HTTPS mode with port not being 80/443), then the ":port" is also populated.

Table 2-3 Information in HTTP Headers

Header.	**Syntax**	**Description**
PS-GW-Rewriting-URL	X-PS-GW-URL: http(s)://gatewayURL(:port)/[SessionInfo]	Indicates the URL that the Gateway rewrites all the pages to. 1. When the browser supports cookies, the value of this header would is the same as the PS-GW-URL header. 2. When the browser does not support cookies: • and if the destination host is in the "User Session to which User Session Cookie is Forwarded" field, the value is the actual URL to which the Gateway rewrites the page to (which includes the encoded SessionID info). • or if the destination host is not in the "User Session to which User Session Cookie is Forwarded” field, then the SessionInfo string will be "$SessionID" Note: As part of response, if the user's Identity Server sessionId changes (like response from authentication page) then the pages are rewritten with that value (and not the value that was previously indicated in the header). For example: • If the browser supports cookies: PS-GW-Rewriting-URL: https://siroe.india.sun.com:10443/ • If the browser does not support cookies, but the endserver is in "User Session to which User Session Cookie is Forwarded" field. PS-GW-Rewriting-URL: https://siroe.india.sun.com:10443/SessIDValCustomEncodedValue/ • If the browser does not support cookies and endserver is not in " User Session to which User Session Cookie is Forwarded" field. PS-GW-Rewriting-URL: https://siroe.india.sun.com:10443/$SessionID
PS-GW-CLientIP	X-PS-GW-CLientIP: *IP*	This is the IP that the Gateway obtained from recievedSocket.getInetAddress().getHostAddress() This gives the client's IP if directly connected to the Gateway. Note: Due to a JSS/NSS bug, this is currently not present.

Using Authentication Chaining

Authentication chaining provides a higher level of security over the regular mechanism of authentication. You can enable users to be authenticated against more than one authentication mechanism.

The procedure described here is only for enabling authentication chaining along with a Personal Digital Certificate (PDC) authentication at the Gateway. For authentication chaining without PDC authentication at the Gateway please refer to the *Identity Server Administration Guide*.

For example, if you chain the PDC, Unix, and Radius authentication modules, the user will have to authenticate against all three modules to access the standard Portal Desktop.

NOTE PDC is always the first authentication module to be presented to the user if it is enabled.

➤ To Add Authentication Modules to an Existing PDC Instance

1. Log in to the Identity Server administration console as administrator.
2. Choose the required organization.
3. Select Services from the View drop-down menu.

   The services are displayed in the left pane.
4. Click the arrow next to Authentication Configuration.

   The Service Instance List displays.
5. Click gatewaypdc.

   The Gatewaypdc properties page displays.
6. Click Edit in front of Authentication Configuration.

   Add Module displays.
7. Select Module Name and set Flag to Required. Option can be blank.
8. Click OK.
9. Click Save after adding one or more modules.
10. Click Save in the gatewaypdc properties page.

11. For the changes to take effect, restart the Gateway:

    ```
    gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
    ```

Using Wild Card Certificates

A wild card certificate accepts a single certificate with a wild card character in the fully-qualified DNS name of the host.

This allows the certificate to secure multiple hosts within the same domain. For example, a certificate for `*.domain.com` can be used for `abc.domain.com`, and `abc1.domain.com`. In fact, this certificate is valid for any host in the `domain.com` domain.

You need to specify a `*` in the fully-qualified host name. For example, if the fully-qualified host name is `abc.florizon.com`, specify it as `*.florizon.com`. The certificate that is generated is now valid for all host names in the `florizon.com` domain.

Disabling Browser Caching

As the Gateway component provides secure access to backend corporate data from any location using just a web browser, it may be necessary that the information not be cached locally by the client.

You can disable caching of pages redirected through the Gateway by modifying the attribute in the `platform.conf` file of the specific Gateway.

Disabling this option can have an impact on the Gateway performance. Every time the standard Portal Desktop is refreshed, the Gateway has to retrieve everything referenced by the page, such as images which may have been previously cached by the browser. However, by enabling this feature, remotely accessing secure content will not leave a cached footprint on the client site. This could outweigh performance implications if the corporate network is being accessed from an Internet cafe or similar remote location that is not under corporate IT control.

➤ To Disable Browser Caching

1. Log in as root and edit the `platform.conf` file of the required Gateway instance:

    ```
    /etc/opt/SUNWps/platform.conf.gateway-profile-name
    ```

2. Edit the following line:

```
gateway.allow.client.caching=true
```

This value is set to `true` by default. Change the value to `false` to disable browser caching at the client side.

3. Restart the Gateway:

gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

Customizing the Gateway Service User Interface

This section discusses the various property files that can be edited.

srapGateway.properties File

You can edit this file for the following purposes:

- Customize the error messages that may appear when the Gateway is running.
  - HTML-CharSets=ISO-8859-1 specifies the character set that was used to create this file.
  - The number in braces (for example, {0}) indicates that the value will be displayed at run time. You can change the label associated with this number, or rearrange the labels as required. Ensure that the label corresponds to the message that will be displayed since the number and the message are associated.
- Customize the log information.

  By default the `srapGateway.properties` file is located under the *portal-server-install-root*`/SUNWps/locale` directory. All messages that appear on the Gateway machine (Gateway related messages) are located in this file, irrespective of the language of the messages.

  If you need to change the language of the messages that appear on the client standard Portal Desktop, copy this file into the respective locale directory, for example *portal-server-install-root*`/SUNWps/locale_en_US`.

srapgwadminmsg.properties File

You can edit this file for the following reasons:

- Customize the labels that appear on buttons for the Gateway service on the administration console.

- Customize the status messages and error messages that appear when you are configuring the Gateway.

Using Federation Management

Federation Management allows users to aggregate their local identities so that they have one network identity. Federation Management uses the network identity to allow users to login at one service provider's site and access other service provider's sites without having to re-authenticate their identity. This is referred to as single sign-on.

Federation management can be configured in open mode and secure mode on the Portal Server. The *Portal Server Administration Guide* describes how to configure federation management in open mode. Before configuring Federation management in secure mode, using Secure Remote Access, ensure that it works in open mode. If you want your users to use Federation Management from the same browser in both open and secure mode, they must clear the cookies and cache from the browser.

Refer to the *Identity Server Customization and API Guide* for detailed information on Federation Management.

Federation Management Scenario

A user authenticates to an initial service provider. Service providers are commercial or not-for-profit organizations that offer web-based services. This broad category can include internet portals, retailers, transportation providers, financial institutions, entertainment companies, libraries, universities, and governmental agencies.

The service provider uses a cookie to store the user's session information in the client browser. The cookie also includes the user's identity provider.

Identity providers are service providers that specialize in providing authentication services. As the administrating service for authentication, they also maintain and manage identity information. Authentication accomplished by an identity provider is honored by all service providers with whom it is affiliated.

When the user attempts to access a service that is not affiliated with the identity provider, the identity provider forwards the cookie to the unaffiliated service provider. This service provider can then access the identity provider called out in the cookie.

However, cookies cannot be read across different DNS domains. Therefore a Common Domain Cookie Service is used to redirect the service provider to the correct identity provider thus enabling single sign-on for the user.

Configuring Federation Management Resources

The Federation resources, the service providers, identity providers, and the Common Domain Cookie Service (CDCS), are configured in the gateway profile based on where they reside. This section describes how to configure three scenarios:

1. when all resources are inside the corporate intranet
2. when all resources are not inside the corporate intranet or the identity provider resides in the Internet
3. when all resources are not inside the corporate intranet or the service provider is a third party residing in the Internet while the identity provider is protected by the Gateway.

Configuration 1

In this configuration the service providers, identity providers and the Common Domain Cookie Service are deployed in the same corporate intranet and the identity providers are not published in the Internet Domain Name Server (DNS). The CDCS is optional.

In this configuration the Gateway points to the service provider, which is the Portal Server. This configuration is valid for multiple instances of the Portal Server.

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab from the administration console.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.
4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Click the Core tab.
6. Select the Enable Cookie Management checkbox to enable cookie management.

7. Scroll to the Portal Server field and enter Portal Server names so that you can use relative URLs like /amserver or /portal/dt listed in the Non-authenticated URLs list. For example:

   http://*idp-host:port*/amserver/js

   http://*idp-host:por*t/amserver/UI/Login

   http://*idp-host:port*/amserver/css

   http://*idp-host:port*/amserver/SingleSignOnService

   http://*idp-host:port*/amserver/UI/blank

   http://*idp-host:port*/amserver/postLogin

   http://*idp-host:port*/amserver/login_images

8. Scroll to the Portal Server field and enter the Portal Server name. For example /amserver.

9. Click Save.

10. Click the Security tab.

11. Scroll to the Non-authenticated URLs list and add the Federation resources. For example:

    /amserver/config/federation

    /amserver/IntersiteTransferService

    /amserver/AssertionConsumerservice

    /amserver/fed_images

    /amserver/preLogin

    /portal/dt

12. Click Add.

13. Click Save.

14. If web proxies are needed to reach the URLs listed in the Non-authenticated URLs list, click the Proxies tab.

15. Scroll to the Proxies for Domains and Subdomains field and enter the necessary web proxies.

16. Click Add.

17. Click Save.

18. From a terminal window, restart the Gateway:

    gateway-install-root/`SUNWps/bin/gateway -n` *gateway-profile-name* `start`

Configuration 2

In this configuration the identity providers, identity providers and the Common Domain Cookie Provider (CDCP) are *not* deployed in the corporate intranet or the identity provider is a third party provider residing the in Internet.

In this configuration the Gateway points to the service provider, which is the Portal Server. This configuration is valid for multiple instances of the Portal Server.

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab from the administration console.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.
4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Click the Core tab.
6. Select the Enable Cookie Management checkbox to enable cookie management.
7. Scroll to the Portal Server field and enter service provider portal server names so that you can use relative URLs like /amserver or /portal/dt listed in the Non-authenticated URLs list.

   `http://`*idp-host:port*`/amserver/js`

   `http://`*idp-host:port*`/amserver/UI/Login`

   `http://`*idp-host:port*`/amserver/css`

   `http://`*idp-host:port*`/amserver/SingleSignOnService`

   `http://`*idp-host:port*`/amserver/UI/blank`

   `http://`*idp-host:port*`/amserver/postLogin`

   `http://`*idp-host:port*`/amserver/login_images`
8. Click Save.
9. Click the Security tab.

10. Scroll to the Non-authenticated URLs list and add the Federation resources. For example:

    ```
    /amserver/config/federation
    /amserver/IntersiteTransferService
    /amserver/AssertionConsumerservice
    /amserver/fed_images
    /amserver/preLogin
    /portal/dt
    ```

11. Click Add.

12. Click Save.

13. If web proxies are needed to reach the URLs listed in the Non-authenticated URLs list, click the Proxies tab.

14. Scroll to the Proxies for Domains and Subdomains field and enter the necessary web proxies.

15. Click Add.

16. Click Save.

17. From a terminal window, restart the Gateway:

    ```
    gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
    ```

Configuration 3

In this configuration the identity providers, identity providers and the Common Domain Cookie Provider (CDCP) are *not* deployed in the corporate intranet or the service provider is a third party provider residing the in Internet and the identity provider is protected by the Gateway.

In this configuration the Gateway points to the identity provider, which is the Portal Server.

This configuration is valid for multiple instances of the Portal Server. This configuration is very unlikely on the Internet, however, some corporate networks may have such a configuration within their intranet, that is the identity provider may reside in a subnet this is protected by a firewall and the service providers are directly accessible from within the corporate network.

1. Log in to the Identity Server administration console as administrator.

2. Select the Service Configuration tab from the administration console.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.
4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Click the Core tab.
6. Select the Enable Cookie Management checkbox to enable cookie management.
7. Scroll to the Portal Server field and enter identity provider portal server so that you can use relative URLs like /amserver or /portal/dt listed in the Non-authenticated URLs list.

   `http://`*idp-host:port*`/amserver/js`

   `http://`*idp-host:port*`/amserver/UI/Login`

   `http://`*idp-host:port*`/amserver/css`

   `http://`*idp-host:port*`/amserver/SingleSignOnService`

   `http://`*idp-host:port*`/amserver/UI/blank`

   `http://`*idp-host:port*`/amserver/postLogin`

   `http://`*idp-host:port*`/amserver/login_images`
8. Click Save.
9. Click the Security tab.
10. Scroll to the Non-authenticated URLs list and add the Federation resources. For example:

    `/amserver/config/federation`

    `/amserver/IntersiteTransferService`

    `/amserver/AssertionConsumerservice`

    `/amserver/fed_images`

    `/amserver/preLogin`

    `/portal/dt`
11. Click Add.
12. Click Save.

13. If web proxies are needed to reach the URLs listed in the Non-authenticated URLs list, click the Proxies tab.
14. Scroll to the Proxies for Domains and Subdomains field and enter the necessary web proxies.
15. Click Add.
16. Click Save.
17. From a terminal window, restart the Gateway:

    ```
    gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
    ```

Chapter 3

Proxylet and Rewriter

This chapter describes Proxylet and Rewriter. These components enable a user to access intranet web pages through the Gateway. They accomplish this by different methods. Proxylet does not parse webpages, as Rewriter does.

This following topics are covered for Proxylet:

- Overview of Proxylet

The following topics are covered for Rewriter:

- Overview of Rewriter
- Character Set Encoding
- Rewriter Usage Scenarios
- Writing Rulesets
- Public Interface (RuleSet DTD)
- Configuring Rewriter in the Gateway Service
- Troubleshooting Using Debug Logs
- Public Interface (RuleSet DTD)
- Working Samples
- Case Study
- Mapping of 6.x RuleSet with 3.0

Overview of Proxylet

Proxylet is a dynamic proxy server that runs on a client machine. Proxylet redirects a URL to the Gateway. It does this by reading and modifying the proxy settings of the browser on the client machine so that they point to the local proxy server or Proxylet.

It supports both HTTP and SSL, inheriting the transport mode from the Gateway. If the Gateway is configured to run on SSL, Proxylet establishes a secure channel between the client machine and the Gateway. Proxylet uses the JSSE API if the client JVM is 1.4 or higher or if the required jar files reside on the client machine. Otherwise it uses the KSSL API.

The domain and subdomain for URLs that are to be directed to the Gateway are specified in the gateway profile. If a URL is not part of a domain that the gateway handles, the request is directed to the Internet. If a particular URL domain is listed in the gateway profile, then Proxylet resets the client proxy settings to point to the Gateway.

Proxylet is enabled from the Identity Server administration console where the client IP address and port are specified. If Proxylet is enabled, it checks the client machine for the following:

- Correct browser permissions
- JVM version 2 (for Netscape browsers)
- The browser is Netscape 7.0, Mozilla 1.4.1, Internet Explorer 5.0 or greater.
- The machine or device can run a server application

If the requirements are met, then a small applet is downloaded and launched on the client machine. If the client does not have JRE 1.3.1 or higher, then JRE is automatically downloaded with Proxylet.

It retrieves the proxy settings from the Proxy Auto Configuration (PAC) file, if it is used, or from the proxy configuration list.

Advantages of Using Proxylet

Unlike Rewriter, Proxylet is an out-of-the-box solution with very little or no post-installation changes. Integration with third party software such as Microsoft Exchange Server is easy. Also there is an increase in the performance of the Gateway as Proxylet does not deal with web content.

Configuring Proxylet

For information on enabling and configuring Proxylet, see Chapter 12, “Configuring Proxylet” on page 317.

Overview of Rewriter

The Rewriter component of SRA allows end-users to browse the intranet by modifying Uniform Resource Identifier (URI) references on web pages so that they point to the Gateway. A URI defines a way to encapsulate a name in any registered name space, and label it with the name space. The most common kinds of URIs are Uniform Resource Locators (URLs). A URL can have various protocols such as http, ftp, mailto, file, and news.

All standard URLs, as specified in RFC-1738 and with protocol either HTTP or HTTPS are recognized and rewritten by Rewriter. The protocols are not case-sensitive. For example, hTtP, HTtp, and httP are all valid. Some sample URLs are listed below:

```
http://www.my.work.com/

http://www.w3.org:8000/imaginary/test

http://www.myu.edu/org/admin/people#andy

http://info.my.org/AboutUs/Index/Phonebook?dobbins

http://www.w3.org/RDB/EMP?where%20name%3Ddobbins

http://info.my.org/AboutUs/Phonebook

http://user:password@abc.com
```

Rewriter supports the rewriting of some basic non-standard URLs which are supported by Internet Explore and Netscape. Information required to convert a non-standard URL to a standard format is taken from the base URL of the page where the URL displays. This information could include:

- protocol
- host name
- port
- path

Rewriter only supports backslashes when they are part of a relative URL.

For example,

`http://abc.sesta.com\index.html` is rewritten,

These URLs would not be rewritten:

`http:\\abc.sesta.com`.

`http:/abc.com`

Character Set Encoding

HTTP standards require that HTTP headers or HTML meta tags specify a character set for web pages. However, sometimes this information is not available. The character set must be known so that encoding for the data is set and the data is displayed as intended by the creator.

Sun Microsystems provides a third-party product to detect the character sets. To enable this product, install the SUNWjchdt package. If the product is installed Rewriter will detect it and use it if necessary.

NOTE Using this product can impact performance, therefore you should install it only when required. Please see the `jcharset_readme.txt` for details on installation, configuration and usage.

Rewriter Usage Scenarios

When a user tries to access intranet web pages through the Gateway, web pages are made available by using Rewriter. Rewriter is used by these components:

- URLScraper
- The Gateway

URLScraper

The URL Scraper provider gets content from the configured URIs and before sending them to the browser, it expands all relative URIs to absolute URIs.

For example, if a user is trying to access the site with content as:

```
<a href="../mypage.html">
```

Rewriter translates this to:

```
<a href="http://yahoo.com/mypage.html">
```

where `http://yahoo.com/test/` is the base URL of the page.

See the *Portal Server Administration Guide* for details on the URLScraper provider.

The Gateway

The Gateway obtains content from internet portals and before sending the content to the browser, it prefixes the Gateway URIs to the existing URI so that subsequent URI requests from the browser can reach the Gateway.

For example, a user who is trying to access an HTML page on an internet machine with content as:

```
<a href="http://mymachine.intranet.com/mypage.html>"
```

Rewriter prefixes this URL with a reference to the Gateway as follows:

```
<a href="https://gateway.company.com/http://mymachine.intranet.com/
mypage.html>"
```

When the user clicks a link associated with this anchor, the browser contacts the Gateway. The Gateway fetches the content of `mypage.html` from `mymachine.intranet.com`.

The Gateway uses several rules to determine the elements of a fetched web page that will be rewritten.

Writing Rulesets

You define rulessets in the Portal Server Configuration section under the Service Configuration Tab.

For details on defining a ruleset, see the *Portal Server Administration Guide.* After creating a new ruleset, you need to define the required rules.

This section covers the following topics:

- Public Interface (RuleSet DTD)
- Sample XML DTD
- Procedure to Write Rules

- Ruleset Guidelines
- Defining the RuleSet Root Element
- Using the Recursive Feature
- Rules for HTML Content
- Rules for JavaScript Content
- Rules for XML Content
- Rules for Cascading Style Sheets
- Rules for WML

Public Interface (RuleSet DTD)

Here is the RuleSet DTD:

```
<?xml version="1.0" encoding="UTF-8"?>

<!--

The following constraints are not represented in DTD, but taken care
programatically

    1. In a Rule, All Mandatory attributes cannot be "*".

    2. Only one instance of the below elements is allowed, but in any order.

    1)HTMLRules

    2)JSRules

    3)XMLRules

    3. ID should alway be in lower case.

-->

<!ENTITY % eURL ’URL’>

<!ENTITY % eEXPRESSION ’EXPRESSION’>

<!ENTITY % eDHTML ’DHTML’>

<!ENTITY % eDJS ’DJS’>

<!ENTITY % eSYSTEM ’SYSTEM’>


<!ENTITY % ruleSetElements ’(HTMLRules | JSRules | XMLRules)?’>
```

```
<!ENTITY % htmlElements '(Form | Applet | Attribute)*'>
<!ENTITY % jsElements '(Variable | Function)*'>
<!ENTITY % xmlElements '(Attribute | TagText)*'>

<!ELEMENT RuleSet (%ruleSetElements;,%ruleSetElements;,%ruleSetElements;)>
<!ATTLIST RuleSet
    id ID #REQUIRED
    extends CDATA "none"
>

<!-- Rules for identifying rules in HTML content -->
<!ELEMENT HTMLRules (%htmlElements;)>
<!ELEMENT Form EMPTY>
<!ATTLIST Form
    name CDATA #REQUIRED
    field CDATA #REQUIRED
    valuePatterns CDATA ""
    source CDATA "*"
>

<!ELEMENT Applet EMPTY>
<!ATTLIST Applet
    code CDATA #REQUIRED
    param CDATA "*"
    valuePatterns CDATA ""
    source CDATA "*"
>

<!-- Rules for identifying rules in JS content -->
<!ELEMENT JSRules (%jsElements;)>
```

```
<!ELEMENT Variable EMPTY>
<!ATTLIST Variable
    name CDATA #REQUIRED
    type (%eURL; | %eEXPRESSION; | %eDHTML; | %eDJS; | %eSYSTEM;)
"EXPRESSION"
    source CDATA "*"
>

<!ELEMENT Function EMPTY>
<!ATTLIST Function
    name CDATA #REQUIRED
    paramPatterns CDATA #REQUIRED
    type (%eURL; | %eEXPRESSION; | %eDHTML; | %eDJS;) "EXPRESSION"
    source CDATA "*"
>

<!-- Rules for identifying rules in XML content -->
<!ELEMENT XMLRules (%xmlElements;)>
<!ELEMENT TagText EMPTY>
<!ATTLIST TagText
    tag CDATA #REQUIRED
    attributePatterns CDATA ""
    source CDATA "*"
>

<!ELEMENT Attribute EMPTY>
<!ATTLIST Attribute
    name CDATA #REQUIRED
    tag CDATA "*"
    valuePatterns CDATA ""
    type (%eURL; | %eDHTML; | %eDJS; ) "URL"

    source CDATA "*"

>
```

NOTE You can use * as a part of the rule value. But all the mandatory attribute values cannot be just *. Such rules are ignored, but the message is logged in the RuleSetInfo log file. For information on this log file, see "Debug File Names" on page 134.

Sample XML DTD

This section contains a sample rule set. The "Case Study," on page 140 is used to illustrate how these rules are interpreted by Rewriter.

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!--

Rules for integrating a mail client with the gateway.

-->

<!DOCTYPE RuleSet SYSTEM "jar://rewriter.jar/resources/RuleSet.dtd">

<RuleSet type="GROUPED" id="owa">

<HTMLRules>

    <Attribute name="action" />

    <Attribute name="background" />

    <Attribute name="codebase" />

    <Attribute name="href" />

    <Attribute name="src" />

    <Attribute name="lowsrc" />

    <Attribute name="imagePath" />

    <Attribute name="viewClass" />

    <Attribute name="emptyURL" />

    <Attribute name="draftsURL" />

    <Attribute name="folderURL" />
    <Attribute name="prevMonthImage" />
    <Attribute name="nextMonthImage" />
    <Attribute name="style" />
    <Attribute name="content" tag="meta" />
</HTMLRules>
<JSRules>
<!-- Rules for Rewriting JavaScript variables in URLs -->
    <Variable name="URL"> _fr.location </Variable>
    <Variable name="URL"> g_szUserBase </Variable>
    <Variable name="URL"> g_szPublicFolderUrl </Variable>
    <Variable name="URL"> g_szExWebDir </Variable>
    <Variable name="URL"> g_szViewClassURL </Variable>
    <Variable name="URL"> g_szVirtualRoot </Variable>
    <Variable name="URL"> g_szBaseURL </Variable>
    <Variable name="URL"> g_szURL </Variable>
    <Function name="EXPRESSION" name="NavigateTo" paramPatterns="y"/>
</JSRules>
<XMLRules>
    <Attribute name="xmlns"/>
    <Attribute name="href" tag="a"/>
    <TagText tag="baseroot" />
    <TagText tag="prop2" />
    <TagText tag="prop1" />
    <TagText tag="img" />
    <TagText tag="xsl:attribute"
    attributePatterns="name=src" />
</XMLRules>
</RuleSet>
```

Procedure to Write Rules

Listed below is a general procedure that you can follow to write the rules.

- Identify the directories that contain the HTML pages whose content needs to be rewritten.
- In these directories, identify the pages that need to be rewritten.
- Identify the URLs that need to be rewritten on each page. An easy way identify most of the URLs is to search for "http" and "/".
- Identify the content type of the URL: HTML, JavaScript or XML.
- Write the rule required to rewrite each of these URLs by editing the required ruleset in the Rewriter service under Portal Server Configuration in the Identity Server administration console.
- Combine all these rules into a ruleset for that domain.

Ruleset Guidelines

Keep the following in mind:

- The order of precedence for specific hosts is based on the longest URI match. For example for the following rulesets

  `mail1.central.abc.com|iplanet_mail_ruleset`

  `*.sfbay.abc.com|sfbay_ruleset`

  `*.abc.com|generic_ruleset`

  sfbay_ruleset is used as it has the longest match.

- The rules in the ruleset are applied in order to each statement in the page, until a rule matches a particular statement.

  While writing the rules, keep in mind the order of the rules. Rules are applied to the statements in a page, in the order in which they occur in the ruleset. If you have specific rules, and general rules that contain a "*", define the specific rules first, then the general rules. Otherwise, the general rule is applied to all statements, even before the specific rule is encountered.

- All rules need to be enclosed within the `<RuleSet> </RuleSet>` tags.
- Include all rules that need to rewrite HTML content in the `<HTMLRules> </HTMLRules>` section of the ruleset.

- Include all rules that need to rewrite JavaScript content in the `<JSRules> </JSRules>` section of the ruleset.
- Include all rules that need to rewrite XML content in the `<XMLRules> </XMLRules>` section of the ruleset.
- In your intranet pages, identify the URLs that need to be rewritten, and include the required rules in the appropriate sections (HTML, JSRules, or XMLRules) of the ruleset.
- Assign the ruleset to the required domain. See "Create List of URIs to RuleSet Mappings" on page 270 for details.
- Restart the Gateway to affect any changes:

  gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

Defining the RuleSet Root Element

The ruleset root element has two attributes:

- **`RuleSetName`**. For example, `default_ruleset.` This name is referened in RuleSet to URI mapping.
- **`Extends`**. This attribute refers to the inheritance feature of rulesets. An extends value points to the ruleset from which you would like to derive a ruleset.

  Use the extends value `none` to signify that this new, independent ruleset does not depend on any other ruleset, or specify your *RuleSetName* to signify that your ruleset depends on another ruleset.

Using the Recursive Feature

Rewriter uses the recursive feature to search to the end of the matched string pattern for the same pattern.

For example, when Rewriter parses the following string:

```
<a href="src=abc.jpg,src=bcd.jpg,src=xyz.jpg>
```

the rule

```
<Attribute name="href" valuePatterns="*src=**"/>
```

rewrites only the first occurrence of the pattern and it would look like this:

```
<a href="src=http://jane.sun.com/abc.jpg>
```

but if you use the recursive option as,

```
<Attribute name="href" valuePatterns="REC:*src=**"/>;
```

Rewriter searchs to the end of the matched string pattern for the same pattern, hence the output would be:

```
<a
href="src=http://jane.sun.com/abc.jpg,src=http://jane.sun.com/bcd.jpg,s
rc=http://jane.sun.com/xyz.jpg>
```

Defining Language Based Rules (Defining Rules)

Rules are based on the following languages:

- HTML
- JavaScript
- XML

Rules for HTML Content

HTML content in web pages can be further classified into attributes, forms and applets. Accordingly, the rules for HTML content are classified as:

- Attribute Rules for HTML Content
- Form Rules for HTML Content
- Applet Rules for HTML Content

Attribute Rules for HTML Content

This rule identifies the attributes of a tag whose value needs to be rewritten. The attribute values can be a simple URL, JavaScript, or DHTML content. For example:

- src attributes of an "img" tag point to an image location (simple URL)
- onClick attribute of a href attributes that handles on clicking of the link (DJS)

This section is divided into the following parts:

- Attribute Rule Syntax
- Attribute Rule Example

- DJS Attribute Example

Attribute Rule Syntax

`<Attribute name="`*attributeName*`" [tag="*" valuePatterns="" source=”*” type=”URL|DHTML|DJS”]/>`

where,

`attributeName` is the name of the attribute (mandatory)

`tag` is the tag to which the attribute belongs (optional, default * , meaning any tag)

`valuePatterns` See “Using Pattern-matching in Rules” on page 104.

`source` specifies the URI of the page in which this attribute is defined (optional, default * , meaning in any page)

`type` specifies the type of the value (optional). They can be:

> `URL` - a simple URL (default value).
>
> `DHMTL` - DHTML content. This kind of content is seen in standard HTML content and is used in Microsoft’s HTC format files.
>
> `DJS` - JavaScript content. All HTML event handlers such as onClick and onMouseover have JavaScript inlined with the HTML attribute.

Attribute Rule Example

Assume the base URL of the page is:

`http://mymachine.intranet.com/mypage.html`

Page Content

`<a href="http://mymachine.intranet.com/mypage.html>`

Rules

`<Attribute name="href"/>`

`or`

`<Attribute name="href" tag="a"/>`

Output

`<a href=`*gateway-URL*`/http://mymachine.intranet.com/myhome.html>`

Description

Because the URL to be rewritten is already an absolute URL, only the Gateway URL is prefixed to the URL.

DJS Attribute Example

Assume the base URL of the page is:

```
http://abc.sesta.com/focus.html
```

Page Content

```
<Form>

<input TYPE=TEXT SIZE=20 value=focus
onClick="Check('/focus.html','focus');return;">

</Form>
```

Rules

```
<Attribute name=”onClick” type=”DJS”/>

<Function type="URL" name="Check" paramPatterns="y,"/>
```

Output

```
<Form>

<INPUT TYPE=TEXT SIZE=20 value=focus
onClick="Check('gateway-URL/http://abc.sesta.com/focus.html','focus');return
;">

</Form>
```

Description

Two rules are required to rewrite the specified page content. The first rule identifies the `onClick` JavaScript token. The second rule identifies the parameter of the `check` function that needs to be rewritten. In this case, only the first parameter is rewritten because `paramPatterns` has the value `y` in place of first parameter.

The Gateway URL and the base URL of the page on which the JavaScript tokens appear are prefixed to the required parameter.

Form Rules for HTML Content

The HTML pages that a user browses may contain forms. Some form elements may take a URL as the value.

This section is divided into the following parts:

- Form Rule Syntax
- Form Rule Example

Form Rule Syntax

`<Form name="`*form1*`" field="`*visit*`" [valuePatterns="" source="*"]/>`

where

`name` is the name of the form (mandatory)

`field` is the field in the form whose value needs to be rewritten (mandatory)

`valuePatterns` See "Using Pattern-matching in Rules" on page 104

`source` is the URL of the html page where this form definition is present (optional, default *, meaning in any page)

Form Rule Example

Assume the base URL of the page is:

```
http://test.siroe.com/testcases/html/form.html
```

Page Content

Assume the page URI is `form.html` and is located in the root directory of the server.

```
<form name=form1  method=POST
action="http://test.siroe.com/testcases/html/form.html">

<input type=hidden name=abc1 value="0|1234|/test.html">

</form>
```

To rewrite `/text.html` present in the value of hidden field named `abc1` which is part of `form1`. The following rules are needed.

Rules

```
<Form source="*/form.html" name="form1" field="abc1"
valuePatterns="0|1234|"/>

<Attribute name="action"/>
```

Output

```
<FORM name=”form1” method=”POST”
action="gateway-URL/http://test.siroe.com/testcases/html/form.html">

<input type=hidden name=abc1
value="0|1234|gateway-URL/http://test.siroe.com/test.html">

</FORM>
```

Description

The `action` tag is rewritten using some defined HTML attribute rule.

The input tag attribute value's `value` is rewritten as shown in the output. The specified `valuePatterns` is located, and all content following the matched `valuePatterns` is rewritten by prefixing the Gateway URL, and the base URL of the page. See "Using Pattern-matching in Rules" on page 104.

Applet Rules for HTML Content

A single web page may contain many applets, and each applet may contain many parameters. Rewriter matches the values specified in the rule with the HTML definition of the applet and modifies the URL values present as a part of the applet parameter definition. This replacement is carried out at the server and not when the user is browsing the particular web page. This rule identifies and rewrites the parameters in both the applet and object tags of the HTML content.

This section is divided into the following parts:

- Applet Rule Syntax
- Applet Rule Example

Applet Rule Syntax

`<Applet code="`*ApplicationClassName/ObjectID*`" param="`*parametername*`" [valuePatterns="" source="*"] />`

where

`code` is the name of the applet or object class (mandatory)

`param` is the name of the parameter whose value needs to be rewritten (mandatory)

`valuePatterns` See "Using Pattern-matching in Rules" on page 104.

`source` is the URL of the page that contains the applet definition (optional, default is *, meaning, in any page)

Applet Rule Example

Assume the base URL of the page is:

```
http://abc.siroe.com/casestudy/test/HTML/applet/rule1.html
```

Page Content

```
<applet codebase=”appletcode” code=”RewriteURLinApplet.class”
archive=”/test.jar”>

<param name=Test1 value="/index.html">

</applet>
```

Rules

```
<Applet source="*/rule1.html" code="RewriteURLin*.class" param="Test*"/>
```

Output

```
<APPLET
codebase="gateway-URL/http://abc.siroe.com/casestudy/test/HTML/applet/applet
code" code="RewriteURLinApplet.class" archive="/test.jar">

<param name="Test1" value="gateway-URL/http://abc.siroe.com/index.html">

</APPLET>
```

Description

codebase attribute is rewritten because <Attribute name="codebase"/> is a defined rule in the default_gateway_ruleset.

All parameters whose names begin with Test are rewritten. The base URL of the page on which the applet code displays and the Gateway URL are prefixed to the value attribute of the param tag.

Using Pattern-matching in Rules

You can use the valuePatterns field to achieve pattern-matching and identify the specific parts of a statement that need to be rewritten.

If you have specified valuePatterns as part of a rule, all the content that follows the matched pattern is rewritten.

Consider the sample form rule below.

```
<Form source="*/source.html" name="form1" field="visit" [valuePatterns="0|1234|"]/>
```

where

source is the URL of the html page where the form displays

name is the name of the form

field is the field in the form whose value needs to be rewritten

valuePatterns indicates the portion of the string that needs to be rewritten. All content appearing after valuePatterns is rewritten (optional, default "" means the full value needs to be rewritten).

Specifying Specialized Characters in valuePatterns

You can specify specialized characters by escaping them with a backslash. For example:

```
<Form source="*/source.html" name="form1" field="visit"
[valuePatterns="0|1234|\;original text|changed text"]/>
```

Using Wild Cards in valuePatterns

You can use the * character to achieve pattern matching for rewriting.

You cannot specify just a * in the `valuePatterns` field. Because * indicates a match with everything, nothing will follow the `valuePattern`, and hence Rewriter will have nothing left to rewrite. You can use * in conjunction with another string such as `*abc`. In this case, all content that follows `*abc` is rewritten.

NOTE An asterisk (*) can be used as a wildcard in any of the fields of the rule. But all the fields in the rule cannot contain a *. If all fields contain a *, the rule is ignored. No error message is displayed.

You can use a * or ** along with the separation character (a semicolon or comma) that displays in the original statement to separate multiple fields. One wildcard (*) matches any field that is not to be rewritten, and two wildcards (**) match any field that needs to be rewritten.

Table 3-1 lists some sample usages of the * wildcard.

Table 3-1 Sample Usage of * Wildcard

URL	valuePatterns	Description
`url1, url2, url3, url4`	`valuePatterns = "**, *, **, *"`	In this case, `url1` and `url3` are rewritten because `**` indicates the portion to be rewritten
`XYZABChttp://host1.sesta.com/dir1.html`	`valuePatterns = "*ABC"`	In this case, only the portion `http://host1.sesta.com/dir1.html` is rewritten. Everything after `*ABC` needs to be rewritten.
`"0|dir1|dir2|dir3|dir4|test|url1`	`valuePatterns = "*|*|**|*|**|*|"`	In this case, `dir2`, `dir4` and `url1` are rewritten. The last field that needs to be rewritten does not have to be indicated by using `**`.

Rules for JavaScript Content

JavaScript can contains URLs in various locations. Rewriter cannot directly parse the JavaScript and determine the URL portion. A special set of rules need to be written to help the JavaScript processor to identify and translate the URL.

JavaScript elements with type URL are classified as follows:

- Variables
- Function Arguments

Variables

Generic Syntax

<Variable name="*variableName*"
[type="URL | EXPRESSION | DHTML | DJS | SYSTEM" source="*****"]>

JavaScript variables can be sub-classified into 5 categories depending on the type of value they hold:

- URL Variables
- EXPRESSION Variables
- DHTML(Dynamic HTML) Variables
- DJS (Dynamic JavaScript) Variables
- SYSTEM Variables

URL Variables

The variable value is a simple string which can be treated as a URL.

This section is divided into the following parts:

- URL Variable Syntax
- URL Variable Example

URL Variable Syntax

```
<Variable name="variableName" type="URL" [source="*"]>
```

where

`variableName` is the name of the variable. The value of the `variableName` is rewritten (mandatory).

`type` is the URL variable (mandatory, and the value must to be a URL)

`source` is the URI of the page in which this JavaScript variable is found (optional, default is *, meaning in any page)

URL Variable Example

Assume the base URL is:

```
http://abc.siroe.com/tmp/page.html
```

Page Content

```
<script LANGUAGE="Javascript">

<!--

//URL Variables

var imgsrc1="/tmp/tmp.jpg";

var imgsrc2="http://srap.sesta.com/tmp/tmp.jpg";

var imgsrc3=imgsrc2;

//-->

</SCRIPT>
```

Rules

```
<Variable name=”imgsrc*” type="URL"/>
```

Output

```
<script LANGUAGE="Javascript">

<!--

//URL Variables

var imgsrc="gateway-URL/http://abc.siroe.com/tmp/tmp.jpg";

var imgsrc="gateway-URL/http://srap.sesta.com/tmp/tmp.jpg";

var imgsrc2=imgsrc1;

//-->

</SCRIPT>
```

Description

All variables of type URL and name beginning with `imgsrc` are rewritten. For the first line of the output, the Gateway URL and the base URL of the page on which the variable displays are prefixed. The second line already contains the absolute path, and hence only the Gateway URL is prefixed. Third var `imagsrc2` would not be rewritten as it’s value is not a string but another JavaScript value.

EXPRESSION Variables

Expression variables have an expression on the right hand side. The result of this expression is a URL. Rewriter appends a JavaScript function (`psSRAPRewriter_convert_expression`) to the HTML page as it cannot evaluate such expressions on the server. This function takes the expression as a parameter and evaluates it to the required URL at the client browser.

If you are not sure whether a statement contains a simple URL or an EXPRESSION URL, it is recommended that you use EXPRESSION rules because it can handle both scenarios.

This section is divided into the following parts:

- EXPRESSION Variable Syntax
- EXPRESSION Variable Example

EXPRESSION Variable Syntax

```
<Variable name=”variableName” [type="EXPRESSION" source=”*”]/>
```

where

`variableName` is the name of the JavaScript variable whose value is a expression (mandatory)

`type` is the type of JavaScript variable (optional, default value is EXPRESSION)

`source` is the URI of the pages (optional, default is *, meaning any source)

EXPRESSION Variable Example

Assume the base URL of the page is:

```
http://abc.siroe.com/dir1/dir2/page.html
```

Page Content

```
<script LANGUAGE="Javascript">

<!--

//Expression variables

var expvar= getURIPreFix() + "../../images/graphics"+".gif";

document.write("<A HREF="+expvar+">Link to XYZ content</A><P>")

var expvar="../../images/graphics"+".gif";

//-->

</SCRIPT>
```

Rules

```
<Variable name=”expvar” type="EXPRESSION"/>

or

<Variable name=”expvar”/>
```

Output

```
var expvar=psSRAPRewriter_convert_expression(getURIPreFix() +
"../../images/graphics"+".gif");
```

```
document.write("<a href="+expvar+">>Link to XYZ content</A><P>")
```

var expvar=″*gateway-URL/*http://abc.siroe.com/images/graphics"+".gif";

Description

The function psSRAPRewriter_convert_expression is prefixed to the right side of the expression variable expvar in the first line. This function processes the expression and rewrites the content at runtime. In the third line the value is rewritten as a simple URL.

DHTML(Dynamic HTML) Variables

These are JavaScript variables that contain HTML content.

This section is divided into the following parts:

- DHTML Syntax
- DHTML Example

DHTML Syntax

```
<Variable name=″variableName″ type="DHTML" [source=″*″]/>
```

where

variableName is the name of the JavaScript variable with DHTML content (mandatory)

type is the type of the variable (mandatory, the value must be DHTML)

source is the URL of the page (optional, the default is *, meaning in any page)

DHTML Example

Assume the base URL of the page is:

```
http://abc.sesta.com/graphics/set1/graphics/jsscript/JSVAR/page.html
```

Page Content

```
<script LANGUAGE="Javascript">

<!--

//DHTML Var

var dhtmlVar="<a href=../../images/test.html>"

var dhtmlVar="<a href=/images/test.html>"
var dhtmlVar="<a href=images/test.html>"

//-->

</SCRIPT>
```

Rules

```
<Variable name=”dhtmlVar” type="DHTML"/>

<Attribute name="href"/>

or

<Attribute name="href" tag="a"/>
```

Output

```
<script LANGUAGE="Javascript">

<!--

//DHTML Var

var dhtmlVar="<a
href=gateway-URL/http://abc.sesta.com/graphics/set1/graphics/images/test.htm
l>"

var dhtmlVar="<a href=gateway-URL/http://abc.sesta.com/images/test.html>"

var dhtmlVar="<a
href=gateway-URL/http://abc.sesta.com/graphics/set1/graphics/jscript/JSVAR/im
ages/test.html>"

//-->

</SCRIPT>
```

Description

The JavaScript parser reads the value of `dhtmlVar` as HTML content and sends the content through the HTML parser. The HTML parser applies the HTML rules where the href attribute rules are matched and hence it is rewritten.

DJS (Dynamic JavaScript) Variables

These are JavaScript variables that contain JavaScript content.

This section is divided into the following parts:

- DJS Syntax
- DJS Example

DJS Syntax

```
<Variable name=”variableName” type="DJS" [source=”*”]/>
```

where

`variable` is the JavaScript varible whose value is javascript.

DJS Example

Assume the base URL of the page is:

```
http://abc.sesta.com/dir1/dir2/dir3/jscript/dir4/page.html
```

Page Content

```
//DJS Var

var dJSVar="var dJSimgsrc='/tmp/tmp.jpg';"

var dJSVar="var dJSimgsrc='../tmp/tmp.jpg';"

var dJSVar="var dJSimgsrc='http://abc.sesta.com/tmp/tmp.jpg';"
```

Rules

```
<Variable name="DJS">dJSVar/>

<Variable name="URL">dJSimgsrc/>
```

Output

```
//DJS Var - need 2 rules

var dJSVar="var dJSimgsrc='gateway-URL/http://abc.sesta.com/tmp/tmp.jpg';"

var dJSVar="var
dJSimgsrc='gateway-URL/http://abc.sesta.com/dir1/dir2/dir3/jscript/tmp/tmp.jp
g';"

var dJSVar="var dJSimgsrc='gateway-URL/http://abc.sesta.com/tmp/tmp.jpg';"
```

Description

Two rules are required here. The first rule locates the dynamic JavaScript variable `dJSVar`. The value of this variable is again a JavaScript of type `URL`. The second rule is applied to rewrite the value of this JavaScript variable.

SYSTEM Variables

These are variables that are not declared by the user, but that are available as a part of the JavaScript standard. For example, `window.location.pathname`. There is limited support for these variables.

This section is divided into the following parts:

- SYSTEM Variable Syntax
- SYSTEM Variable Example

SYSTEM Variable Syntax

```
<Variable name=”variableName” type="SYSTEM" [source=”*”]/>
```

where

`variableName` is the JavaScript system variable (mandatory and the values could be ones that match these patterns: document.URL, document.domain, location, doument.location, location.pathname, location.href, location.protocol, location.hostname, location.host and location.port. All these are present in the generic_ruleset. Do not modifiy these system var rules .

`type` specifies system type values (mandatory and value is DJS)

`source` is the URI of this pages (optional, default value is *, meaning in any page)

SYSTEM Variable Example

Assume the base URL of the page is:

```
http://abc.siroe.com/dir1/page.html
```

Page Content

```
<script LANGUAGE="Javascript">

<!--

//SYSTEM Var

alert(window.location.pathname);

//-->

</SCRIPT>
```

Rules

```
<Variable name=”window.location.pathname” type="SYSTEM"/>
```

Output

```
</SCRIPT>

<SCRIPT LANGUAGE="Javascript">

<!--

//SYSTEM Var

alert(psSRAPRewriter_convert_pathname(window.location.pathname));
```

```
//-->
</SCRIPT>
```

Description

Rewriter locates the system variable which matches the rule, then the `psSRAPRewriter_convert_system` function is prefixed. This function processes the system variable at runtime and rewrites the resulting URL accordingly.

Function Arguments

Function parameters whose value needs to be rewritten are classified into 4 categories:

- URL Parameters
- EXPRESSION Parameters
- DHTML Parameters
- DJS Parameters

Generic Syntax

```
<Function name="functionName" paramPatterns="y,y,"
[type="URL|EXPRESSION|DHTML|DJS" source="*"]/>
```

where

`name` is the name of the JavaScript function (mandatory)

`paramPatterns` specifies the parameters that need to be rewritten (mandatory)

`y` the position of `y` indicates the parameter that the needs to be rewritten. For example, in the syntax, the first parameter needs to be rewritten, but the second parameter should not be rewritten.

`type` specifies the kind of value this parameter needs (optional, default is EXPRESSION type)

`source` page source URI (optional, default is *, meaning in any page)

URL Parameters

Function takes this parameter as a string and this string could be treated as URL.

This section is divided into the following parts:

- URL Parameter Syntax
- URL Parameter Example

URL Parameter Syntax

`<Function name="`*functionName*`" paramPatterns="y,," type="URL" [source="*"]/>`

where

`name` is the name of the function with a type parameter of URL (mandatory)

`paramPatterns` specifies the parameters that need to be rewritten (mandatory)

`y` the position of `y` indicates the parameter that needs to be rewritten. For example, in the syntax, the first parameter needs to be rewritten, but the second parameter should not be rewritten.

`type` is the type of the function (mandatory, and the value must be URL)

`source` is the URL of the page which has this function call (optional, default is *, meaning in any URL)

URL Parameter Example

Assume the base URL of the page is:

`http://abc.sesta.com/test/rewriter/test1/jscript/test2/page.html`

Page Content

```
<script language="JavaScript">

<!--

function test(one,two,three){

alert(one + "##" + two + "##" +three);

}

test("/test.html","../test.html","123");

window.open("/index.html","gen",width=500,height=500);

//-->

</SCRIPT>
```

Rules

```
<Function name="URL" name="test" paramPatterns="y,y,"/>

<Function name="URL" name="window.open" paramPatterns="y,,,"/>
```

Output

```
<SCRIPT language="JavaScript">

<!--
```

```
function test(one,two,three) {

alert(one + "##" + two + "##" +three);

}

test("gateway-URL/http://abc.sesta.com/test.html","gateway-URL/http://abc.sesta.c
om/test/rewriter/test1/jscript/test.html","123");

window.open("gateway-URL/http://abc.sesta.com/index.html","gen",width=500,heig
ht=500);

//-->

</SCRIPT>
```

Description

The first rule specifies that the first two parameters in the function with name `test` need to be rewritten. Hence the first two parameters of the test function are rewritten. The second rule specifies that the first parameter of the `window.open` function needs to be written. The URL within the `window.open` function is prefixed with the Gateway URL and the base URL of the page that contains the function parameters.

EXPRESSION Parameters

These parameters take an expression value, which when evaluated, results in a URL.

This section is divided into the following parts:

- EXPRESSION Parameter Syntax
- EXPRESSION Parameter Example

EXPRESSION Parameter Syntax

```
<Function name="functionName" paramPatterns="y" [type="EXPRESSION"
source=”*”]/>
```

where

`name` is the name of the function (mandatory).

`paramPatterns` specifies the parameters that need to be rewritten (mandatory)

`y` the position of `y` indicates the function parameter that needs to be rewritten. In the syntax above, only the first parameter is rewritten.

`type` specifies the value EXPRESSION (optional)

`source` URI of the page where this function is called.

EXPRESSION Parameter Example

Assume the base URL of the page is:

```
http://abc.sesta.com/dir1/dir2/page.html
```

Page Content

```
<script language="JavaScript">
<!--
function jstest2(){
return ".html";
}
function jstest1(one){
return one;
}
var dir="/images/test"
var test1=jstest1(dir+"/test"+jstest2());
document.write("<a HREF="+test1+">TEST</a>");
alert(test1);
//-->
</SCRIPT>
```

Rules

```
<Function type="EXPRESSION" name="jstest1" paramPatterns="y"/>
or
<Function name="jstest1" paramPatterns="y"/>
```

Output

```
<script language="JavaScript">
<!--
function jstest2(){
return ".html";
}
function jstest1(one){
return one;
}

var dir="/images/test"

var
test1=jstest1(psSRAPRewriter_convert_expression(dir+"/test"+jstest2()));

document.write("<a HREF="+test1+">TEST</a>");

alert(test1);

//-->

</SCRIPT>
```

Description

The rule specifies that the first parameter of the `jstest1` function needs to be rewritten by considering this as an EXPRESSION function param. In the sample page content, the first parameter is an expression that will be evaluated only at runtime. Rewriter prefixes this expression with the `psSRAPRewriter_convert_expression` function. The expression is evaluated, and the `psSRAPRewriter_convert_expression` function rewrites the output at runtime.

NOTE In the above example, it is not required to have the variable `test1` as a part of the JavaScript variable rule. The function rule for `jstest1` takes care of the rewriting.

DHTML Parameters

Function parameter whose value is HTML

Native JavaScript methods such as `document.write()` that generate an HTML page dynamically fall under this category.

This section is divided into the following parts:

- DHTML Parameter Syntax
- DHTML Parameter Example

DHTML Parameter Syntax

`<Function name="`*functionName*`" paramPatterns="y" type="DHTML" [source=”*”]/>`

where

`name` is the name of the function.

`paramPatterns` specifies the parameters that need to be rewritten (mandatory) y the position of y indicates the function parameter that needs to be rewritten. In the syntax above, only the first parameter is rewritten.

DHTML Parameter Example

Assume the base URL of the page is:

```
http://xyz.siroe.com/test/rewriter/test1/jscript/JSFUNC/page.html
```

Page Content

```
<script>

<!--

document.write('<a href="/index.html">write</a><BR>')

document.writeln('<a href="index.html">writeln</a><BR>')

document.write("http://abc.sesta.com/index.html<BR>")

document.writeln("http://abc.sesta.com/index.html<BR>")

//-->

</SCRIPT>
```

Rules

```
<Function name="DHTML" name="document.write" paramPatterns="y"/>

<Function name="DHTML" name="document.writeln" paramPatterns="y"/>

<Attribute name="href"/>
```

Output

```
<SCRIPT>

<!--

document.write('<a
href="gateway-URL/http://xyz.siroe.com/index.html">write</a><BR>')

document.writeln('<a
href="gateway-URL/http://xyz.siroe.com/test/rewriter/test1/jscript/JSFUNC/inde
x.html">writeln</a><BR>')

document.write("http://abc.sesta.com/index.html<BR>")

document.writeln("http://abc.sesta.com/index.html<BR>")

//-->

</SCRIPT>
```

Description

The first rule specifies that the first parameter in the function `document.write` needs to be rewritten. The second rule specifies that the first parameter in the function `document.writeln` needs to be rewritten. The third rule is a simple HTML rule that specifies that all attributes with the name `href` need to be rewritten. In the example, the DHTML parameter rules identify the parameters in the functions that need to be rewritten. Then the HTML attribute rule is applied to actually rewrite the identified parameter.

DJS Parameters

Function parameters whose value is JavaScript.

This section is divided into the following sections:

- DJS Parameter Syntax
- DJS Parameter Example

DJS Parameter Syntax

`<Function name="`*functionName*`" paramPatterns="y" type="DJS" [source="*"]/>`

where

`name` is the name of the function where one parameter is DJS (mandatory)

`paramPatterns` specifies which parameter in the above function is DJS (mandatory)

`y` the position of `y` indicates the function parameter that needs to be rewritten. In the syntax above, only the first parameter is rewritten.

`type` is DJS (mandatory)

`source` is the URI of the page (optional, default is *, meaning any URI)

DJS Parameter Example

Assume the base URL of the page is:

`http://abc.sesta.com/page.html`

Page Content

```
<script>

menu.addItem(new NavBarMenuItem("All Available
Information","JavaScript:top.location='http://abc.sesta.com'"));

</script>
```

Rules

```
<Function name="DJS" name="NavBarMenuItem" paramPatterns=",y"/>
```

```
<Variable name="URL">top.location</Variable>
```

Output

```
<script>
```

```
menu.addItem(new NavBarMenuItem("All Available
Information","JavaScript:top.location='gateway-URL/http://abc.sesta.com'"));
```

```
</script>
```

Description

The first rule specifies that the second parameter of the function `NavBarMenuItem` which contains JavaScript needs is to be rewritten. Within the JavaScript, the variable `top.location` also needs to be rewritten. This variable is rewritten using the second rule.

Rules for XML Content

Web pages may contain XML content which in turn can contain URLs. XML content that needs to be rewritten is classified into two categories:

- Tag Text (same as PCDATA or CDATA of the tag)
- Attribute

Tag Text

This rule is for rewriting the PCDATA of CDATA of the tag element.

This section is divided into the following parts:

- Tag Text Syntax
- Tag Text Example

Tag Text Syntax

```
<TagText tag="tagName" [attributePatterns="attribute_patterns_for_
this_tag" source="*"]/>
```

where

`tagName` is the name of the tag

`attributePatterns` is the attributes and their value patterns for this tag (optional, meaning this tag has no attributes at all) `source` is the URI of this xml file (optional, default is *, meaning, any xml page)

Tag Text Example

Assume the base URL of the page is:

```
http://abc.sesta.com/test/rewriter/test1/xml/page.html
```

Page Content

```
<xml>

<Attribute name="src">test.html</attribute>

<attribute>abc.html</attribute>

</xml>
```

Rules

```
<TagText tag="attribute" attributePatterns="name=src"/>
```

Output

```
<xml>

<Attribute
name="src">gateway-URL/http://abc.sesta.com/test/rewriter/test1/xml/test.html<
/attribute>

<attribute>abc.html</attribute>

</xml>
```

Description

The first line in the page content has an Attribute Example. The second line in the page content does not contain an attribute with the attribute called name and value of attribute name to be `src`, and hence no rewriting is done. To rewrite this also we need to have `<TagText tag="attribute"/>`

Attribute

The rules for XML attributes are similar to the attribute rules for HTML. See "Attribute Rules for HTML Content," on page 118. The difference is that attribute rules of XML are cases sensitive while HTML attribute rules are not. This is again due to case sensitivity built into XML and not into HTML.

Rewriter translates the attribute value based on the attribute name.

This section is divided into the following parts:

- Attribute Syntax

- Attribute Example

Attribute Syntax

<Attribute name="*attributeName*" [tag="*" type=”URL” valuePatterns="*" source=”*”]/>

where

`attributeName` is the name of the attribute (mandatory)

`tag` is the name of the tag, where this attribute is present (optional, deafult is * , meaning any tag)

`valuePatterns` See “Using Pattern-matching in Rules” on page 104.

`source` is the URI of this XML page (optional, default is *, meaning in any XML page)

Attribute Example

Assume the base URL of the page is:

```
http://abc.sesta.com/test/rewriter/test1/xml/page.html
```

Page Content

```
<xml>

<baseroot href="/root.html"/>

<img href="image.html"/>

<string href="1234|substring.html"/>

<check href="1234|string.html"/>

</xml>
```

Rules

```
<Attribute name="href"tag="check" valuePatterns="1234|"/>
```

Output

```
<xml>

<baseroot href="/root.html"/>

<img href="image.html"/>

<string href="1234|substring.html"/>
```

```
<check
href="1234|gateway-URL/http://abc.sesta.com/test/rewriter/test1/xml/string.h
tml"/>
```

```
</xml>
```

Description

In the above example, only the fourth line is rewritten because it meets all the conditions specified in the rule. See "Using Pattern-matching in Rules," on page 116.

Rules for Cascading Style Sheets

The Cascading Style Sheets (including CCS2) in HTML pages are translated. There are no rules defined for this translation as the URL presents only in the `url()` functions and import syntaxes of the CSS.

Rules for WML

WML is similar to HTML and hence HTML rules are applied for WML content.Use the generic ruleset for WML content. See "Rules for HTML Content" on page 99.

Using the Recursive Feature

Rewriter uses the recursive feature to search to the end of the matched string pattern for the same pattern.

For example, when Rewriter parses the following string:

```
<a href="src=abc.jpg,src=bcd.jpg,src=xyz.jpg>
```

the rule

```
<Attribute name="href" valuePatterns="*src=**"/>
```

rewrites only the first occurrence of the pattern and it would look like this:

```
<a href="src=http://jane.sun.com/abc.jpg>
```

but if you use the recursive option as,

```
<Attribute name="href" valuePatterns="REC:*src=**"/>;
```

Rewriter searches to the end of the matched string pattern for the same pattern, hence the output would be:

```
<a
href="src=http://jane.sun.com/abc.jpg,src=http://jane.sun.com/bcd.jpg,s
rc=http://jane.sun.com/xyz.jpg>
```

Configuring Rewriter in the Gateway Service

Using the Gateway service, under the Rewriter tab, you can perform the following tasks within two categories, Basic and Advanced:

- Basic Tasks
  - Enable Rewriting of All URLs
  - Create List of URIs to RuleSet Mappings
  - Create List of MIME Types to Parse
  - Specify the Default Domains
- Advanced Tasks
  - Create List of URIs Not to Rewrite
  - Enable MIME Guessing
  - Create List of URI Mappings to Parse
  - Enable Masking
  - Specify the Masking Seed String
  - Create List of URIs Not to Mask
  - Make a Gateway Protocol the Same as the Original URI Protocol

Basic Tasks

Enable Rewriting of All URLs

If you enable the Enable Rewriting of All URIs option in the Gateway service, Rewriter rewrites any URL without checking against the entries in the Proxies for Domains and Subdomains list. Entries in the Proxies for Domains and Subdomains list are ignored.

➤ To Enable the Gateway to Rewrite All URLs

1. Log in to the Sun Java™ System Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway Profile page displays.
4. Click Edit... for the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Click the Rewriter tab.
6. Select the Enable Rewriting of All URIs checkbox to enable the Gateway to rewrite all URLs.
7. Click Save at the top or bottom of the page to record the change.
8. Restart the Gateway from a terminal window:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Create List of URIs to RuleSet Mappings

Rulesets are created in the Rewriter service under Portal Server Configuration in the Identity Server administration console. See the *Portal Server Administration Guide* for details.

After the ruleset is created, associate a domain with the ruleset using the Map URIs to RuleSets field. The following two entries are added by default to the Map URIs to RuleSets field:

- `*://*.Sun.COM/portal/*|default_gateway_ruleset`

  where `sun.com` is the install domain of the portal and /portal is the portal install context
- `*|generic_ruleset`

This means that for all pages from portal directory with the domain `sun.com`, the `default_gateway_ruleset` is applied. For all other pages, the generic ruleset is applied. The `default_gateway_ruleset` and the `generic_ruleset` are pre-packaged rulesets.

NOTE For all the content appearing on the standard Portal Desktop, the ruleset for the `default_gateway_ruleset` is used, irrespective of where the content is fetched from.

For example, assume that the standard Portal Desktop is configured to scrape the content from the URL `yahoo.com`. The Portal Server is in `sesta.com`. The ruleset for `sesta.com` is applied to the fetched content.

NOTE The domain for which you specify a ruleset must be listed in the Proxies for Domains and Subdomains list.

Using Wildcards Within the Syntax

You can map a fully qualified URI or a partial URI by using an asterisk in the ruleset.

For example, you could apply the `java_index_page_ruleset` to an `index.html` page as follows:

```
www.sun.com/java/index.html/java_index_page_ruleset
```

or you could apply all pages in the java directory to the `java_directory_ruleset`, as follows:

```
www.sun.com/java/* /java_directory_ruleset
```

➤ To Map a URI to RuleSet

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway Profile page displays.
4. Click the gateway profile for which you want to set the attribute.

   The Gateway - *gateway-profile-name* page displays.
5. Click the Rewriter tab.

6. Scroll to the Map URIs to RuleSets field.

7. Type the required domain or host name and the ruleset in the Map URIs to RuleSets field and click Add.

   The entry is added to the Map URIs to RuleSets field.

   The format for specifying the domain or host name and the ruleset is as follows:

   ```
   domain name|ruleset name
   ```

   For example:

   ```
   eng.sesta.com|default
   ```

Create List of MIME Types to Parse

Rewriter has four different parsers to parse the web pages based on the content type: HTML, JAVASCRIPT, CSS and XML. Common MIME types are associated with these parsers by default. You can associate new MIME types with these parsers in the Map Parser to MIME Types field of the Gateway service. This extends the Rewriter functionality to other MIME types.

Separate multiple entries with a semicolon or a comma (";" or ",".) For example:

```
HTML=text/html;text/htm;text/x-component;text/wml; text/vnl/wap.wml
```

means any content with these MIMEs are sent to the HTML Rewriter and HTML rules would be applied to rewrite the URLs.

TIP Removing unnecessary parsers from the MIME mappings list can increase the speed of operation. For example, if you are sure that the content from a particular intranet will not have any JavaScript, you can remove the JAVASCRIPT entry from the MIME mappings list.

➤ To Specify MIME Mappings

1. Login to the Identity Server administration console as administrator.

2. Select the Service Configuration tab.

3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway Profile page displays.

4. Click the gateway profile for which you want to set the attribute.

   The Gateway - *gateway-profile-name* page displays.

5. Click the Rewriter tab.
6. Scroll to the Map Parser to MIME Types field, and add the required MIME type in the edit box. Use a semicolon or comma to separate multiple entries.

   Specify the entry in the format `HTML=text/html;text/htm`
7. Click Add to add the required entry to the list.
8. Click Save at the top or bottom of the page to record the change.
9. Restart the Gateway from a terminal window:

   ```
   portal-server-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Create List of URIs Not to Rewrite

➤ To Specify the URIs Not to Rewrite

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway Profile page displays.
4. Click the gateway profile for which you want to set the attribute.

   The Gateway - *gateway-profile-name* page displays.
5. Click the Rewriter tab, Basic subsection.
6. Scroll to the URIs Not to Rewrite field, and add the URI in the edit box.

   Note: Adding #* to this list allows URIs to be rewritten, even when the href rule is part of the ruleset.
7. Click Save at the top or bottom of the page to record the change.
8. Restart the Gateway from a terminal window:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Specify the Default Domains

The default domain and subdomain are useful when URLs contain only the host names without the domain and subdomain. In this case, the Gateway assumes that the host names are in the default domain and subdomain, and proceeds accordingly.

For example, if the host name in the URL is `host1`, and the default domain and subdomain are specified as `red.sesta.com`, the host name is resolved as `host1.red.sesta.com`.

➤ To Specify the Default Domains

1. Login to the identity server administration console as administrator.
2. Click the Service Configuration tab.
3. Click the right arrow next to Gateway under SRA Configuration.

   The Gateway Profile page displays.
4. Click Edit... for the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Scroll to the Default Domains field and type the required default value in the format `subdomain.domain name`.
6. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
7. Restart the Gateway from a terminal window:

   ```
   portal-server-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Advanced Tasks

Enable MIME Guessing

Rewriter depends on the MIME type of the page to choose the parser. Some web servers such as WebLogic and Oracle do not send MIME types. To work around this, you can enable the MIME guessing feature by adding data to the Map Parser to URIs list box.

➤ To Enable MIME Guessing

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway Profile page displays.

4. Click the gateway profile for which you want to set the attribute.

   The Gateway - *gateway-profile-name* page displays.

5. Click the Rewriter tab, Advanced subsection.
6. Select the Enable MIME Guessing checkbox to enable MIME Guessing.
7. Click Save at the top or bottom of the page to record the change.
8. Restart the Gateway from a terminal window:

```
gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
```

Create List of URI Mappings to Parse

If the MIME Guessing checkbox is enabled and the server has not sent a MIME type, use this list box to map the URI to parse.

Multiple URIs are separated by a semicolon.

For example HTML=*.html; *.htm;*Servlet

means that the HTML Rewriter is used to rewrite the content for any page with a html, htm, or Servlet extension.

➤ To Parse URI Mappings

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway Profile page displays.

4. Click the gateway profile for which you want to set the attribute.

   The Gateway - *gateway-profile-name* page displays.

5. Click the Rewriter tab, Advanced subsection.
6. Scroll to the Map Parser to MIME Types field, and add the data to the edit box.
7. Click Save at the top or bottom of the page to record the change.
8. Restart the Gateway from a terminal window:

```
gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
```

Enable Masking

Masking allows Rewriter to rewrite a URI so that the Intranet URL of a page is not seen.

➤ To Enable Masking

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway Profile page displays.
4. Click the gateway profile for which you want to set the attribute.

   The Gateway - *gateway-profile-name* page displays.
5. Click the Rewriter tab, Advanced subsection.
6. Select the Enable Masking checkbox to enable Masking.
7. Click Save at the top or bottom of the page to record the change.
8. Restart the Gateway from a terminal window:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Specify the Masking Seed String

A seed string is used for masking a URI. It is a random string generated by a masking algorithm.

NOTE Book marking of a masked URI may not work if this seed string has been changed or if the Gateway is restarted.

➤ To Specify the Masking Seed String

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway Profile page displays.
4. Click the gateway profile for which you want to set the attribute.

   The Gateway - *gateway-profile-name* page displays.
5. Click the Rewriter tab, Advanced subsection.

6. Scroll to the Masking Seed String field, and add a string to the edit box.
7. Click Save at the top or bottom of the page to record the change.
8. Restart the Gateway from a terminal window:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

Create List of URIs Not to Mask

Some applications (such as an applet) require an Internet URI and cannot be masked. To specify those applications, add the URI to the list box.

For example if you added

```
*/Applet/Param*
```

to the list box, the URL would not be masked if the content URI `http://abc.com/Applet/Param1.html` is matched in the ruleset rule.

➤ To Specify Not to Mask the URI List

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway Profile page displays.
4. Click the gateway profile for which you want to set the attribute.

   The Gateway - *gateway-profile-name* page displays.
5. Click the Rewriter tab, Advanced subsection
6. Scroll to the URIs Not to Mask field, and add the URIs to the edit box.
7. Click Save at the top or bottom of the page to record the change.
8. Restart the Gateway from a terminal window:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

Make a Gateway Protocol the Same as the Original URI Protocol

When a gateway runs in both HTTP and HTTPS mode, you can enable Rewriter to use a consistent protocol to access the referred resources in the HTML content.

For example, if the original URL is `http://intranet.com/Public.html` then the HTTP gateway is added. If the original URL is `https://intranet.com/Public.html` then the HTTPS gateway is added.

NOTE This applies only to static URIs, not to dynamic URIs generated in Javascript.

➤ To Make a Gateway Protocol the Same as the Original URI Protocol

1. Log in to the Identity Server admin console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway Profile page displays.
4. Click the gateway profile for which you want to set the attribute.

   The Gateway - *gateway-profile-name* page displays.
5. Click the Rewriter tab, Advanced subsection.
6. Select the Make Gateway Protocol the Same as the Original URI Protocol checkbox.
7. Click Save at the top or bottom of the page to record the change.
8. Restart the Gateway from a terminal window:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Troubleshooting Using Debug Logs

To troubleshoot a Rewriter problem, you need to enable debug logs.

Debug Messages are classified as follows.

- **error**–Errors that Rewriter cannot recover from
- **warning**–This file contains logs about warning messages. Rewriter is able to recover this type of error, but some misbehavior may or may not result. For example “Not rewriting image content” is logged as a warning message. This is fine as Rewriter is not supposed to rewrite the images.These are just warnings and do not critically affect the functioning of Rewriter. Some messages shown in warnings are informational.

- **message**–This is the highest level of information that Rewriter provides.

Setting the Rewriter Debug Level

➤ To Set the Rewriter Debug Level

1. Log in as root to the Gateway machine and edit the following file:

   gateway-install-root`/SUNWam/config/AMConfig-`*instance-name*`.properties`

2. Set the debug level:

   ```
   com.iplanet.services.debug.level=
   ```

   The debug levels are:

   `error` - Only serious errors are logged in the debug file. Rewriter usually stops functioning when such errors occur.

   `warning` - Warning messages are logged.

   `message` - All debug messages are logged.

   `off` - No debug messages are logged.

3. Specify the directory for the debug files in the following property of the `AMConfig-`*instance-name*`.properties` file:

   ```
   com.iplanet.services.debug.directory=/var/opt/SUNWam/debug
   ```

   where `/var/opt/SUNWam/debug` is the default debug directory.

4. Restart the Gateway from a terminal window:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

Debug File Names

When the debug level is set to message, debug generates a set of files. Table 3-2 lists the Rewriter files and the information contained within them.

Table 3-2 Rewriter Debug Files

Filename	Information
RuleSetInfo	All the rulesets which have been used for rewriting, are logged in this file.

Table 3-2 Rewriter Debug Files

Filename	Information
Original Pages	Contains the page URI, resolveURI (if it is different than the page URI), content MIME, the ruleset that has been applied to the page, parser MIME, and the original content. Specific error/warning/messages related to parsing also appear in this file. In message mode full content is logged, in warning and error mode only exception occurred during rewriting are logged.
Rewritten Pages	Contains the page URI, resolveURI (if it is different than the page URI), content MIME, ruleset that has been applied to the page, parser MIME, and the rewritten content. This is filled when the debug mode is set to message.
Unaffected Pages	Contains a list the pages that were not modified.
URIInfo Pages	This file contains the URLs found and translated. Details of all the pages whose content remain same as original data are logged in this file. Details logged are: Page URI, MIME and Encoding data, rulesetID used for rewriting, and Parser MIME.

In addition to the above files, Rewriter generates a file for debug messages that are not captured in the above files. This filename consists of two parts: the first part is either `pwRewriter` or `psSRARewriter` and the second part is an extension using either `portal` or the *gateway-profile-name*.

The debug files are displayed on the portal or the Gateway. These files are in the directory indicated in the `AMConfig-`*instance-name*`.properties` file.

The Rewriter component generates the following set of files to help in debugging,

*prefix*_RuleSetInfo.*extension*

*prefix*_OrginalPages.*extension*

*prefix*_RewrittenPages.*extension*

*prefix*_UnaffectedPages.*extension*

*prefix*_URIInfo.*extension*

where

prefix is either `psRewriter` for URLScraper usage logs or `psSRAPRewriter` for Gateway usage logs.

extension is either `portal` for URLScraper usage or *`gateway-profile-name`* for Gateway usage.

For example, if the Rewriter on the Gateway is used to convert pages and the default gateway profile is used, debug creates these files:

```
psSRAPRewriter_RuleSetInfo.default

psSRAPRewriter_OriginalPages.default

psSRAPRewriter_RewrittenPages.default

psSRAPRewriter_UnaffectedPages.default

psSRAPRewriter_URIInfo.default

psSRAPRewriter.default
```

Working Samples

This section includes:

- simple HTML pages with content that needs to be rewritten
- the rules required to rewrite the content
- the corresponding rewritten HTML page

These sample pages are available in the *portal-server-URL*/`rewriter` directory. You can browse through the page before the rule is applied, and then view the file with the rewritten output through your Gateway to see how the rule works. In some samples, the rule is already a part of the `default_gateway_ruleset`. In some samples, you may have to include the rule in the `default_gateway_ruleset`. This is mentioned at the appropriate places.

NOTE Some of the statements appear in bold to indicate that they have been rewritten.

The following samples are available:

- HTML
  - Sample for HTML Attributes
  - Sample for HTML Forms
  - Sample for HTML Applets

- JavaScript
  - Variables
    - Sample for JavaScript URL Variables
    - Samples for JavaScript Content
    - Sample for JavaScript DHTML Variables
    - Sample for JavaScript DJS Variables
    - Sample for JavaScript SYSTEM Variables
  - Functions
    - Sample for JavaScript URL Functions
    - Sample for JavaScript EXPRESSION Functions
    - Sample for JavaScript DHTML Functions
    - Sample for JavaScript DJS Functions
- XML
  - Sample for XML Attributes

Samples for HTML Content

Sample for HTML Attributes

➤ To Use the HTML Attributes Sample

1. This sample can be accessed from:

   portal-server-URL / rewriter / HTML / attrib / attribrule.html

2. Ensure that `abc.sesta.com` and `host1.siroe.com` are defined in the Proxies for Domains and Subdomains list in the Gateway service.

   If this is not defined, a direct connection is assumed, and the Gateway URL is not prefixed.

You need not add the rule specified in this sample to the `default_gateway_ruleset` because it is already defined.

HTML Before Rewriting

```
<html>
```

```
Rewriting starts

<head>

<title>TEST PAGE () </title>

</head>

ID-htmlattr.1

<br><br>

1.a href <a href="http://abc.sesta.com/images/logo.gif">http://..</a>

<br><br>

2. href <a href="https://host1.siroe.com">https://..</a>

<br><br>

3. href <a href="../images/logo.gif">../images/</a>

<br><br>

4. href <a href="images/logo.gif">images/..</a> <br><br>

5. href <a href="../../images/logo.gif">../../images/</a> <br><br>

Rewriting ends

</html>
```

Rule

```
<Attribute name="href"/>
```

HTML After Rewriting

```
<html>

Rewriting starts

<head>

<title>TEST PAGE () </title>

</head>

ID-htmlattr.1

<br><br>

1. a href <a
href="gateway-URL/http://abc.sesta.com/images/logo.gif">http://.
.</a> <br>
```

// This URL is rewritten because the `<Attrib name="href"/>` rule is already defined in the `default_gateway_ruleset`. Because the URL is already absolute, only the Gateway URL is prefixed. Ensure that `abc.sesta.com` is defined in the Proxies for Domains and Subdomains list in the Gateway service. Otherwise, the Gateway URL is not prefixed, because a direct connection is assumed.

`2. href <a href="gateway-URL/https://host1.siroe.com">https://..</a>`

// Again, `host1.siroe.com` needs to be defined in the Proxies for Domains and Subdomains list in the Gateway service. Otherwise, the Gateway URL is not prefixed, because a direct connection is assumed.

`<br><br>`

`3. href <a href="gateway-URL/portal-server-URL/rewriter/HTML/images/logo.gif">../images/</a>`

// Because a relative path is specified, the Gateway URL and the portal-server-URL are prefixed along with the required subdirectories. This link will not work because there is no directory called `images` under the `HTML` directory in the sample structure provided.

`<br><br>`

`4 href <a href="gateway-URL/portal-server-URL/rewriter/HTML/attrib/images/logo.gif">images/..</a> <br><br>`

// Because a relative path is specified, the Gateway URL and the Portal Server URL are prefixed along with the required subdirectories.

`5. href <a href="gateway-URL/portal-server-URL/rewriter/images/logo.gif">../../images/</a> <br><br>`

// Because a relative path is specified, the Gateway URL and the Portal Server URL are prefixed along with the required subdirectories. This link will not work because there is no directory called `images` under the `Rewriter` directory in the sample structure provided.

`Rewriting ends`

`</html>`

Sample for HTML Dynamic JavaScript Tokens

➤ **To Use the HTML JavaScript Token Sample:**

1. This sample can be accessed from:

   portal-server-URL / rewriter / HTML / jstokens / JStokens.html

2. Add the rule specified in this sample to the `default_gateway_ruleset` in the section "Rules for Rewriting JavaScript Source".

3. Edit the `default_gateway_ruleset` in the Rewriter service under the Portal Server Configuration in the Identity Server administration console.

4. Restart the Gateway from a terminal window:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

HTML Before Rewriting

```
<html>

<head>

Rewriting starts

<script language="javascript">

function Check(test,ind){

if (ind == 'blur')

{alert("testing onBlur")}

if (ind == 'focus')

{alert("testing onFocus")}

}

</SCRIPT>

</head>

<body>

<form>

<input TYPE=TEXT SIZE=20 value=blur
onAbort="Check('/indexblur.html','blur');return;">

<input TYPE=TEXT SIZE=20 value=blur
onBlur="Check('/indexblur.html','blur');return;">

<input TYPE=TEXT SIZE=20 value=focus
onFocus="Check('/focus.html','focus');return;">
```

```
<input TYPE=TEXT SIZE=20 value=focus
onChange="Check('/focus.html','focus');return;">

<input TYPE=TEXT SIZE=20 value=focus
onClick="Check('/focus.html','blur');return;">

<br><br>

</form>

</body>

Rewriting ends

</html>
```

Rule

```
<Attribute name=”onClick” type=”DJS”/>

<Function type="URL" name="Check" paramPatterns="y"/>
```

NOTE `<Function name="URL" name="Check" paramPatterns="y"/>` is a JavaScript function rule and is explained in detail in the JavaScript function sample.

HTML After Rewriting

```
<html>

<head>

Rewriting starts

<script language="javascript">

function Check(test,ind){

if (ind == 'blur')

{alert("testing onBlur")}

if (ind == 'focus')

{alert("testing onFocus")}

}

</SCRIPT>

</head>

<body>

<form>
```

```
<input TYPE=TEXT SIZE=20 value=blur onAbort="Check('gateway
URL/portal-server-URL/indexblur.html','blur');return;">

<input TYPE=TEXT SIZE=20 value=blur onBlur="Check('gateway
URL/portal-server-URL/indexblur.html','blur');return;">

<input TYPE=TEXT SIZE=20 value=focus onFocus="Check('gateway
URL/portal-server-URL/focus.html','focus');return;">

<input TYPE=TEXT SIZE=20 value=focus onChange="Check('gateway
URL/portal-server-URL/focus.html','focus');return;">

<input TYPE=TEXT SIZE=20 value=focus onClick="Check('gateway
URL/portal-server-URL/focus.html','blur');return;">
```

// All the statements are rewritten in this sample. The Gateway and Portal Server URLs are prefixed in each case. This is because rules for `onAbort`, `onBlur`, `onFocus`, `onChange`, and `onClick` are defined in the `default_gateway_ruleset` file. Rewriter detects the JavaScript tokens and passes it to the JavaScript function rules for further processing. The second rule listed in the sample tells Rewriter which parameter to rewrite.

```
</body>

<br>

Rewriting ends

</html>
```

Sample for HTML Forms

➤ To Use the Form Sample

1. Access the sample from:

   portal-server-URL/rewriter/HTML/forms/formrule.html

2. Ensure that `abc.sesta.com` is defined in the Proxies for Domains and Subdomains list in the Gateway service.

   If this is not defined, a direct connection is assumed, and the Gateway URL is not prefixed.

3. Add the rule specified in this sample to the `default_gateway_ruleset` in the section "Rules for Rewriting HTML Attributes".

4. Edit the `default_gateway_ruleset` in the Rewriter service under the Portal Server Configuration in the Identity Server administration console.

5. Restart the Gateway from a terminal window:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

HTML Page Before Rewriting

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">

<html>

<head>

</head>

<body>

RW_START

<p>

<form name="form1" method="Post"
action="http://abc.sesta.com/casestudy/html/form.html">

<input type="hidden" name="name1" value="0|1234|/test.html">

<input type="hidden" name="name3" value="../../html/test.html">

<form name="form2" method="Post"
action="http://abc.sesta.com/testcases/html/form.html"><br>

<input type="hidden" name="name1"
value="0|1234|../../html/test.html"></form>

RW_END </p>

</body>

</html>
```

Rule

```
<Form source="*" name="form1" field="name1" valuePatterns="0|1234|"/>
```

HTML Page After Rewriting

```
<HTML>

<HEAD>

RW_START

</HEAD>

<BODY>

<P>
```

```
<FORM name=form1  method=POST
action="gateway-URL/http://abc.sesta.com/casestudy/html/form.htm
l">
```

// This URL is rewritten because `<Attribute name="action"/>` is defined as part of the HTML rules in the `default_gateway_ruleset`. Because the URL is already absolute, only the Gateway URL needs to be prefixed. Ensure that `abc.sesta.com` is defined in the Proxies for Domains and Subdomains list in the Gateway service. Else, the Gateway URL is not prefixed because a direct connection is assumed.

```
<input type=hidden name=name1 value="0|1234|gateway
URL/portal-server-URL/test.html">
```

// Here the form name is `form1`, and the field name is `name1`. This matches the form name and field name specified in the rule. The rule states the `valuePatterns` as `0|1234|` which matches the `value` in this statement. Hence the URL occurring after the `valuePattern` is rewritten. The Portal Server URL and the Gateway URL are prefixed. See “Using Pattern-matching in Rules,” on page 116 for details on `valuePatterns`.

```
<input type=hidden name=name3 value="../../html/test.html">
```

// This URL is not rewritten because the `name` does not match the `field` name specified in the rule.

```
</FORM>
```

```
<FORM name=form2 method=POST
action="gateway-URL/http://abc.sesta.com/casestudy/html/form.htm
l"><BR>
```

// This URL is rewritten because `<Attribute name="action"/>` is defined as part of the HTML rules in the default ruleset. Because the URL is already absolute, only the Gateway URL needs to be prefixed.

```
<input type=hidden name=name1 value="0|1234|../../html/test.html">
```

// This URL is not rewritten because the form name does not match the name specified in the rule.

```
</FORM>

</BODY>

RW_END

</HTML>
```

Sample for HTML Applets

➤ To Use the Sample for Applets

1. Obtain the applet class file. The `RewriteURLinApplet.class` file is present in the following location:

   portal-server-URL / rewriter / HTML / applet / appletcode

   The base URL of the page where the applet code is present is:

   portal-server-URL / rewriter / HTML / applet / rule1.html

2. Add the rule specified in this sample to the `default_gateway_ruleset` in the section "Rules for Rewriting HTML Attributes".

3. Edit the `default_gateway_ruleset` in the Rewriter service under the Portal Server Configuration in the Identity Server administration console.

4. Restart the Gateway:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

HTML Before Rewriting

```
<html>

Rewriting starts

<br>

<applet codebase=appletcode code=RewriteURLinApplet.class archive=/test>

<param name=Test1 value="/index.html">

<param name=Test2 value="../index.html">

<param name=Test3 value="../../index.html">

</applet>

Rewriting ends

</html>
```

Rule

```
<Applet source="*/rule1.html" code="RewriteURLinApplet.class" param="Test*"
/>
```

HTML After Rewriting

```
<HTML>

Rewriting starts
```

```
<BR>
```

`<APPLET codebase=gateway-URL/portal-server-URL/rewriter/HTML/applet/appletcode=RewriteURLinApplet.class archive=/test>`

// This URL is rewritten because the rule `<Attribute name="codebase"/>` is already present as part of the `default_gateway_ruleset` file. the Gateway and the Portal Server URLs are prefixed along with the path up to the `appletcode` directory.

`<param name=Test1 value="gateway-URL/portal-server-URL/index.html">`

// This URL is rewritten because the base URL of the page is `rule1.html`, and the param name matches the param `Test*` specified in the rule. Because `index.html` is specified to be at the root level, the Gateway and Portal Server URLs are prefixed directly.

`<param name=Test2 value="gateway-URL/portal-server-URL/rewriter/HTML/index.html">`

// This URL is rewritten because the base URL of the page is `rule1.html`, and the param name matches the param `Test*` specified in the rule. The path is prefixed as required.

`<param name=Test3 value="gateway-URL/portal-server-URL/rewriter/index.html">`

// This URL is rewritten because the base URL of the page is `rule1.html`, and the param name matches the param `Test*` specified in the rule. The path is prefixed as required.

```
</APPLET>
```

```
Rewriting ends
```

```
</HTML>
```

Samples for JavaScript Content

Sample for JavaScript URL Variables

➤ To Use the JavaScript URL Variables Sample

1. This sample can be accessed from:

   portal-server-URL/rewriter/JavaScript/variables/url/js_urls.html

2. Ensure that `abc.sesta.com` is defined in the Proxies for Domains and Subdomains list in the Gateway service.

   If this is not defined, a direct connection is assumed, and the Gateway URL is not prefixed.

3. Add the rule specified in this sample to the `default_gateway_ruleset` in the section "Rules for Rewriting JavaScript Source".

4. Edit the `default_gateway_ruleset` in the Rewriter service under Portal Server Configuration in the Identity Server administration console.

5. If you added the rule, restart the Gateway:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

HTML Page Before Rewriting

```
<html>

Rewriting starts

<head>

<title>JavaScript Variable test page</title>

</head>

<body>

<script LANGUAGE="Javascript">

<!--

//URL Variables

var imgsrc="/tmp/tmp.jpg";

var imgsrc="./tmp/tmp.jpg";

var imgsrc="../tmp/tmp.jpg";

var imgsrc="../../tmp/tmp.jpg";

var imgsrc="http://abc.sesta.com/tmp/tmp.jpg";

var imgsrc="../../../tmp/tmp.jpg";

var imgsrc="tmp/tmp.jpg";

//-->

</SCRIPT>

<br>
```

```
Testing JavaScript variables!

<br>

<img src="images/logo.gif">

<br>

Image

</body>

<br>

Rewriting ends

</html>
```

Rule

```
<Variable name=”imgsrc” type="URL"/>
```

HTML Page After Rewriting

```
<html>

Rewriting starts

<head>

<title>JavaScript Variable test page</title>

</head>

<body>

<script LANGUAGE="Javascript">

<!--

//URL Variables

var imgsrc="gateway-URL/portal-server-URL/tmp/tmp.jpg";

var
imgsrc="gateway-URL/portal-server-URL/rewriter/JavaScript/variab
les/url/tmp/tmp.jpg";

var
imgsrc="gateway-URL/portal-server-URL/rewriter/JavaScript/variab
les/tmp/tmp.jpg";

var
imgsrc="gateway-URL/portal-server-URL/rewriter/JavaScript/tmp/tm
p.jpg";

var imgsrc="gateway-URL/http://abc.sesta.com/tmp/tmp.jpg";
var imgsrc="gateway-URL/portal-server-URL/rewriter/tmp/tmp.jpg";
```

```
var
imgsrc="gateway-URL/portal-server-URL/rewriter/JavaScript/variab
les/url/tmp/tmp.jpg";
```

// All the above URLs are JavaScript variables of type URL and name `imgsrc` as specified in the rule. Hence they are prefixed with the Gateway and the Portal Server URLs. The path following the Portal Server URL is prefixed as required.

```
//-->
```

```
</SCRIPT>
```

```
<br>
```

```
Testing JavaScript variables!
```

```
<br>
```

```
<img src="gateway
URL/portal-server-URL/rewriter/JavaScript/variables/url/images/logo.gif">
```

// This line is rewritten because the rule `<Attribute name="src"/>` is defined in the `default_gateway_ruleset`

```
<br>
```

```
Image
```

```
</body>
```

```
<br>
```

```
Rewriting ends
```

```
</html>
```

Sample for JavaScript EXPRESSION Variables

➤ To Use the JavaScript Expression Variables Sample

1. This sample can be accessed from:

   portal-server-URL/rewriter/JavaScript/variables/expr/expr.html

2. Add the rule specified in this sample (if it does not already exist) to the `default_gateway_ruleset` in the section "Rules for Rewriting JavaScript Source".

3. Edit the `default_gateway_ruleset` in the Rewriter service under Portal Server Configuration in the Identity Server administration console.

4. If you added the rule, restart the Gateway:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

HTML Page Before Rewriting

```
<html>

<head>

<title>JavaScript EXPRESSION Variables Test Page</title>

</head>

<body>

<script LANGUAGE="Javascript">

<!--

//Expression variables

var expvar1="images";

var expvar2="/logo.gif";

var expvar = expvar1 + expvar2;

document.write("<A HREF="+expvar+">EXPRESSION</A><P>")

var expvar="/images/logo"+".gif";

document.write("<A HREF="+expvar+">EXPRESSION</A><P>")

//-->

</SCRIPT>

Testing JavaScript EXPRESSION variables

</body>

</html>
```

Rule

```
<Variable type=”EXPRESSION” name="expvar"/>
```

HTML Page After Rewriting

```
<html>

<head>

<title>JavaScript EXPRESSION Variables Test Page</title>

</head>
```

```
<body>

<SCRIPT>

// Rewriter appends the wrapper function
psSRAPRewriter_convert_expression here

</SCRIPT>

<script LANGUAGE="Javascript">

<!--

//Expression variables

var expvar1="images";

var expvar2="/logo.gif";

var expvar =psSRAPRewriter_convert_expression( expvar1 +
expvar2);
```

// Rewriter recognizes the right hand side of this statement to be a JavaScript EXPRESSION variable. Rewriter is not able to resolve the value of this expression at the server end. Hence, the `psSRAPRewriter_convert_expression` function is prefixed to the expression. The expression is evaluated at the client end, and rewritten as required.

```
document.write("<A HREF="+expvar+">EXPRESSION</A><P>")
```

// The rewritten value of `expvar` from the previous statement is used to arrive at the value of this expression. Because the result is a valid URL (a graphic exists at this location in the sample), the link will work.

```
var expvar="gateway URL/portal-server-URL/images/logo"+".gif";
```

// Rewriter recognizes the right hand side of `expvar` to be a string expression. This can be resolved at the server side, and hence is rewritten directly.

```
document.write("<A HREF="+expvar+">EXPRESSION</A><P>")
```

// The rewritten value of `expvar` from the previous statement is used to arrive at the value of this expression. Because the result is a not a valid URL (a graphic does not exist at the resultant location), the link will not work.

```
//-->

</SCRIPT>

Testing JavaScript EXPRESSION variables

</body>

</html>
```

Sample for JavaScript DHTML Variables

➤ To Use the JavaScript DHTML Variables Sample

1. This sample can be accessed from:

   portal-server-URL/rewriter/JavaScript/variables/dhtml/dhtml.html

2. Ensure that `abc.sesta.com` is defined in the Proxies for Domains and Subdomains list in the Gateway service. If this is not defined, a direct connection is assumed, and the Gateway URL is not prefixed.

3. Add the rule specified in this sample (if it does not already exist) to the `default_gateway_ruleset` in the section "Rules for Rewriting JavaScript Source". Edit the `default_gateway_ruleset` in the Rewriter service under Portal Server Configuration in the Identity Server administration console.

4. If you added the rule, restart the Gateway:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

HTML Page Before Rewriting

```
<html>

<head>

<title>JavaScript DHTML Variable Test Page</title>

</head>

<body>

<script LANGUAGE="Javascript">

<!--

//DHTML Var

var dhtmlVar="<a href=../../images/test.html>"

var dhtmlVar="<a href=/../images/test.html>"

var dhtmlVar="<a href=/images/test.html>"

var dhtmlVar="<a href=images/test.html>"

var dhtmlVar="<a href=http://abc.sesta.com/images/test.html>"

var dhtmlVar="<img src=http://abc.sesta.com/images/test.html>"

//-->

</SCRIPT>

<br><br>
```

```
Testing DHTML Variables

<br><br>

<img src="images/logo.gif">IMAGE

</body>

</html>
```

Rule

```
<Variable name="DHTML">dhtmlVar</Variable>
```

HTML Page After Rewriting

```
<html>

<head>

<title>JavaScript DHTML Variable Test Page</title>

</head>

<body>

<script LANGUAGE="Javascript">

<!--

//DHTML Var
```

`var dhtmlVar="<a href=gateway-URL/portal-server-URL/rewriter/JavaScript/images/test.html>"`

// The JavaScript DHTML rule identifies the right hand side of the `dhtmlVar` as dynamic HTML content. Hence, the HTML rules in the `default_gateway_ruleset` file are applied. The dynamic HTML contains a `href` attribute. The `default_gateway_ruleset` defines the rule `<Attribute name="href"/>`. Hence the value of the `href` attribute is rewritten. But the URL is not absolute; therefore, the relative URL is replaced with the base URL of the page, and the required subdirectories. This in turn is prefixed with the Gateway URL to derive the final rewritten output.

`var dhtmlVar="<a href=gateway-URL/portal-server-URL/../images/test.html>"`

// Although the base URL of the page is appended, and the Gateway URL is prefixed, the resultant URL will not work. This is because the initial URL `/../images/test.html` is inaccurate.

`var dhtmlVar="<a href=gateway-URL/portal-server-URL/images/test.html>"`

// Here again, the JavaScript DHTML rule identifies the right hand side to be dynamic HTML content, and passes it to the HTML rules. The HTML rule `<Attribute name="href"/>` from the `default_gateway_ruleset` is applied, and the statement is rewritten as shown. The Gateway URL and Portal Server URL are prefixed.

```
var dhtmlVar="<a href=gateway URL/portal-server-URL/rewriter/JavaScript/variables/dhtml/images/test.html>"

var dhtmlVar="<a href=gateway URL/http://abc.sesta.com/images/test.html>"
```

```
var dhtmlVar="<img src=gateway-URL/http://abc.sesta.com/images/test.html>"
```

// The JavaScript DHTML rule identifies the dynamic HTML content on the right hand side, and passes the statement to the HTML rules. The `<Attribute name="src"/>` rule in the `default_gateway_ruleset` is applied. Because the URL is absolute, only the Gateway URL needs to be prefixed. Ensure that `abc.sesta.com` is defined in the Proxies for Domains and Subdomains list for this URL to be rewritten.

```
//-->

</SCRIPT>

<br><br>

Testing DHTML Variables

<br><br>
```

```
<img src="gateway-URL/portal-server-URL/rewriter/JavaScript/variables/dhtml/images/logo.gif">
```

// This line is rewritten because the rule `<Attribute name="src"/>` is defined in the `default_gateway_ruleset`.

```
<br><br>

Image

</body>

</html>
```

Sample for JavaScript DJS Variables

➤ To Use the JavaScript DJS Variables Sample

1. This sample can be accessed from:

   portal-server-URL / rewriter / JavaScript / variables / djs / djs.html

2. Ensure that `abc.sesta.com` is defined in the Proxies for Domains and Subdomains list in the Gateway service. If this is not defined, a direct connection is assumed, and the Gateway URL is not prefixed.

3. Add the two rules specified in this sample (if it does not already exist) to the `default_gateway_ruleset` in the section "Rules for Rewriting JavaScript Source". Edit the `default_gateway_ruleset` in the Rewriter service under Portal Server Configuration in the Identity Server administration console.

4. Restart the Gateway:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

HTML Page Before Rewriting

```
<html>

<head>

<title>Dynamic JavaScript Variable Test Page</title>

</head>

<body>

<script LANGUAGE="Javascript">

<!--

var dJSVar="var dJSimgsrc='/tmp/tmp/jpg';"

var dJSVar="var dJSimgsrc='../../../tmp/tmp/jpg';"

var dJSVar="var dJSimgsrc='http://abc.sesta.com/tmp/tmp/jpg';"

//-->

</SCRIPT>

<br>

Testing Dynamic JavaScript Variables

<br>

<img src="images/logo.gif">

<br>
```

```
Image

</body>

</html>
```

Rule

```
<Variable name=”dJSVar” type="DJS"/>

<Variable name="dJSimgsrc“ type=URL"/>
```

HTML Page After Rewriting

```
<html>

<head>

<title>Dynamic JavaScript Variable Test Page</title>

</head>

<body>

<script LANGUAGE="Javascript">

<!--

var dJSVar="var
dJSimgsrc='gateway-URL/portal-server-URL/tmp/tmp/jpg';"

var dJSVar="var
dJSimgsrc='gateway-URL/portal-server-URL/rewriter/tmp/tmp/jpg';"

var dJSVar="var
dJSimgsrc='gateway-URL/http://abc.sesta.com/tmp/tmp/jpg';"
```

// All the above statements are rewritten with the Gateway and Portal Server URLs. The required path is prefixed as appropriate. The first rule identifies the right hand side of `dJSVar` as a dynamic JavaScript variable. This is then passed to the second rule which identifies the right hand side of `dJSimgsrc` as a JavaScript variable of type URL. This is rewritten accordingly.

```
//-->

</SCRIPT>

<br>

Testing Dynamic JavaScript Variables

<br>
```

```
<img
src="gateway-URL/portal-server-URL/rewriter/JavaScript/variables
/djs/images/logo.gif">
```

// This line is rewritten because the rule `<Attribute name="src"/>` is defined in the `default_gateway_ruleset`.

```
<br>

Image

</body>

</html>
```

Sample for JavaScript SYSTEM Variables

➤ To Use the JavaScript System Variables Sample

1. This sample can be accessed from:

   portal-server-URL/rewriter/JavaScript/variables/system/system.html

2. Add the rule specified in this sample (if it does not already exist) to the `default_gateway_ruleset` in the section "Rules for Rewriting JavaScript Source".

3. Edit the `default_gateway_ruleset` in the Rewriter service under Portal Server Configuration in the Identity Server administration console.

4. Restart the Gateway:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

HTML Page Before Rewriting

```
<html>

<head>

<title>JavaScript SYSTEM Variables Test Page</title>

</head>

<body>

<script LANGUAGE="Javascript">

<!--

//SYSTEM Var

alert(window.location.pathname);
```

```
//document.write("<A HREF="+window.location.pathname+">SYSTEM</A><P>")

//-->

</SCRIPT>

Testing JavaScript SYSTEM Variables

<br>

This page displays the path where the current page is located when it is
loaded.

</body>

</html>
```

Rule

```
<Variable name=”window.location.pathname” type="SYSTEM"/>
```

HTML After Rewriting

```
<html>

<head>

<title>JavaScript SYSTEM Variables Test Page</title>

</head>

<body>

<SCRIPT>

convertsystem function definition...

</SCRIPT>

<script LANGUAGE="Javascript">

<!--

//SYSTEM Var
```

`alert(psSRAPRewriter_convert_system(window.location, window.location.pathname,”window.location”));`

// Rewriter identifies `window.location.pathname` as a JavaScript SYSTEM variable. The value of this variable cannot be determined at the server end. So the Rewriter prefixes the variable with the `psSRAPRewriter_convert_pathname` function. This wrapper function determines the value of the variable at the client end and rewrites as required.

```
//-->
```

```
</SCRIPT>

Testing JavaScript SYSTEM Variables

<br>

This page displays the path where the current page is located when it is
loaded.

</body>

</html>
```

Sample for JavaScript URL Functions

➤ To Use the JavaScript URL Functions Sample

1. This sample can be accessed from:

   portal-server-URL/rewriter/JavaScript/functions/url/url.html

2. Add the rule specified in this sample (if it does not already exist) to the `default_gateway_ruleset` in the section "Rules for Rewriting JavaScript Source". Edit the `default_gateway_ruleset` in the Rewriter service under the Portal Server Configuration in the Identity Server administration console.

3. Restart the Gateway:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

HTML Page Before Rewriting

```
<html>

<body>

JavaScript URL Function Test Page

<br>

<script language="JavaScript">

<!--

function test(one,two,three)

{

alert(one + "##" + two + "##" +three);

}

test("/test.html","../test.html","123");

window.open("/index.html","gen",width=500,height=500);
```

```
//-->

</SCRIPT>

</body>

</html>
```

Rule

```
<Function type="URL" name="test" paramPatterns="y,y"/>

<Function type="URL" name="window.open" paramPatterns="y"/>
```

HTML Page After Rewriting

```
<html>

<body>

JavaScript URL Function Test Page

<br>

<script language="JavaScript">

<!--

function test(one,two,three)

{

alert(one + "##" + two + "##" +three);

}

test("/test.html","../test.html","123");

window.open("gateway-URL/portal-server-URL/index.html","gen",width=500,hei
ght=500);

//-->

</SCRIPT>

</body>

</html>
```

Sample for JavaScript EXPRESSION Functions

➤ To Use the JavaScript Expressions Function Sample

1. This sample can be accessed from:

   portal-server-URL/rewriter/JavaScript/functions/expr/expr.html

2. Add the rule specified in this sample (if it does not already exist) to the `default_gateway_ruleset` in the section "Rules for Rewriting JavaScript Source".

3. Edit the `default_gateway_ruleset` in the Rewriter service under the Portal Server Configuration in the Identity Server administration console.

4. Restart the Gateway:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

HTML Page Before Rewriting

```
<html>

<body>

JavaScript EXPRESSION Function Test Page

<br><br><br>

<script language="JavaScript">

<!--

function jstest2()

{

return ".html";

}

function jstest1(one)

{

return one;

}

var dir="/images/test"

var test1=jstest1(dir+"/test"+jstest2());

document.write("<a HREF="+test1+">Test</a>");

alert(test1);

//-->

</SCRIPT>

</body>

</html>
```

Rule

```
<Function type="EXPRESSION" name="jstest1" paramPatterns="y"/>
```

HTML Page After Rewriting

```
<html>

<body>

JavaScript EXPRESSION Function Test Page

<br><br><br>

<script>

<!--

// various functions including psSRAPRewriter_convert_expression appear
here.

//-->

</SCRIPT>

<script language="JavaScript">

<!--

function jstest2()

{

return ".html";

}

function jstest1(one)

{

return one;

}

var dir="/images/test"

var
test1=jstest1(psSRAPRewriter_convert_expression(dir+"/test"+jste
st2()));
```

// The rule states that the first parameter in the function `jstest1` which is of type EXPRESSION needs to be rewritten. The value of this expression is `/test/images/test.html`. This is prefixed with the Portal Server and the Gateway URLs.

```
document.write("<a HREF="+test1+">Test</a>");
```

```
alert(test1);

//-->

</SCRIPT>

</body>

</html>
```

Sample for JavaScript DHTML Functions

➤ To Use the JavaScript DHTML Functions Sample

1. This sample can be accessed from:

   portal-server-URL/rewriter/JavaScript/functions/dhtml/dhtml.html

2. Add the rule specified in this sample (if it does not already exist) to the `default_gateway_ruleset` in the section "Rules for Rewriting JavaScript Source".

3. Edit the `default_gateway_ruleset` in the Rewriter service under Portal Server Configuration in the Identity Server administration console.

4. Restart the Gateway:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

HTML Page Before Rewriting

```
<html>

<head>

Testing JavaScript DHTML Functions

<br>

<br>

<script>

<!--

document.write('<a href="/index.html">write</a><BR>')

document.writeln('<a href="index.html">writeln</a><BR>')

document.write("http://abc.sesta.com/index.html<BR>")

document.writeln("http://abc.sesta.com/index.html<BR>")

//-->
```

```
</SCRIPT>

</head>

<body BGCOLOR=white>

<br><br>

Testing document.write and document.writeln

</body>

</html>
```

Rule

```
<Function type="DHTML" name=" document.write" paramPatterns="y"/>

<Function type="DHTML" name=" document.writeln" paramPatterns="y"/>
```

HTML Page After Rewriting

```
<html>

<head>

Testing JavaScript DHTML Functions

<br>

<br>

<script>

<!--
```

`document.write('<a href="gateway-URL/portal-server-URL/index.html">write</a><BR>')`

// The first rule specifies that the first parameter of the DHTML JavaScript function `document.write` needs to be rewritten. Rewriter identifies the first parameter to be a simple HTML statement. The HTML rules section in the `default_gateway_ruleset` has the rule `<Attribute name="href" />` which indicates that the statement needs to be rewritten.

`document.writeln('<a href="gateway-URL/portal-server-URL/rewriter/JavaScript/functions/dhtml/index.html">writeln</a><BR>')`

// The second rule specifies that the first parameter of the DHTML JavaScript function `document.writeln` needs to be rewritten. Rewriter identifies the first parameter to be a simple HTML statement. The HTML rules section in the `default_gateway_ruleset` has the rule `<Attribute name="href" />` which indicates that the statement needs to be rewritten.

```
document.write("http://abc.sesta.com/index.html<BR>")
```

```
document.writeln("http://abc.sesta.com/index.html<BR>")
```

// The above statements are not rewritten although the DHTML rule identifies the functions `document.write` and `document.writeln`. This is because the first parameter in this case is not simple HTML. It could be any string, and Rewriter does not know how to rewrite this.

```
//-->

</SCRIPT>

</head>

<body BGCOLOR=white>

<br><br>

Testing document.write and document.writeln

</body>

</html>
```

Sample for JavaScript DJS Functions

➤ To Use the JavaScript DJS Functions Sample

1. This sample can be accessed from:

   portal-server-URL/rewriter/JavaScript/functions/djs/djs.html

2. Ensure that `abc.sesta.com` is defined in the Proxies for Domains and Subdomains list in the Gateway service.

   If this is not defined, a direct connection is assumed, and the Gateway URL is not prefixed.

3. Add the rule specified in this sample (if it does not already exist) to the `default_gateway_ruleset` in the section "Rules for Rewriting JavaScript Source". Edit the `default_gateway_ruleset` in the Rewriter service under Portal Server Configuration in the Identity Server administration console.

4. Restart the Gateway:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

HTML Page Before Rewriting

```
<html>

Test for JavaScript DJS Functions
```

```
<br>

<script>

menu.addItem(new NavBarMenuItem("All Available

Information","JavaScript:top.location='http://abc.sesta.com'"));

//menu.addItem(new NavBarMenuItem("All Available
Information","http://abc.sesta.com"));

</script>

</html>
```

Rule

```
<Function type="DJS" name="NavBarMenuItem" paramPatterns=",y"/>

<Variable type="URL" name=”top.location”/>
```

HTML Page After Rewriting

```
<html>

Testing JavaScript DJS Functions

<br>

<script>

menu.addItem(new NavBarMenuItem("All Available
Information","javaScript:top.location='gateway-URL/http://abc.se
sta.com'"));
```

// `abc.sesta.com` is an entry in the Proxies for Domains and Subdomains list in the Gateway service. Hence Rewriter needs to rewrite this URL. But because it is an absolute URL, the Portal Server URL need not be prefixed. The DJS rule states that the second parameter of the DJS function `NavBarMenuItem` needs to be rewritten. But the second parameter is again a JavaScript variable. A second rule is required to rewrite the value of this variable. The second rule specifies that the value of the JavaScript variable `top.location` needs to be rewritten. Because all these conditions are met, the URL is rewritten.

```
//menu.addItem(new NavBarMenuItem("All Available
Information","http://abc.sesta.com"));
```

// Although the DJS rule specifies that the second parameter of the function `NavBarMenuItem` needs to be rewritten, it does not happen in this statement. This is because Rewriter does not recognize the second parameter as simple HTML.

```
</script>

</html>
```

Sample for XML Attributes

➤ To Use the XML Attributes Sample

1. This sample can be accessed from:

   portal-server-URL / rewriter / XML / attrib.html

2. Add the rule specified in this sample (if it does not already exist) to the `default_gateway_ruleset` in the section "Rules for Rewriting XML Source".

3. Edit the `default_gateway_ruleset` in the Rewriter service under the Portal Server Configuration in the Identity Server administration console.

4. Restart the Gateway:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

XML Before Rewriting

```
<html>

RW_START

<body>

<xml>

<baseroot href="/root.html"/>

</xml>

<xml>

<img href="image.html"/>

</xml>

<xml>

<string href="1234|substring.html"/>

</xml>

<xml>

<check href="1234|string.html"/>

</xml>

</body>

RW_END

</html>
```

Rule

```
<Attribute name="href" tag="check" valuePatterns="1234|"/>
```

HTML After Rewriting

```
<html>

Rewriting starts

<br>

<br>

<body>

<xml><baseroot href="/root.html"/></xml>

<xml><img href="image.html"/></xml>

<xml><string href="1234|substring.html"/></xml>
```

`<xml><check href="1234|gateway-URL/portal-server-URL/rewriter/XML/string.html"/></xml>`

// This statement is rewritten because it matches the conditions specified in the rule. The `Attribute name` is `href`, `tag` is `check` and the `valuePatterns` is `1234`. The string following `valuePatterns` is rewritten. See "Using Pattern-matching in Rules," on page 116 for details on `valuePatterns`.

```
</body>

Rewriting ends

</html>
```

Case Study

This section includes the source HTML pages for a sample mail client. This case study does not cover all possible scenarios and rules. This is just a sample ruleset to help you put together the rules for your intranet pages.

Assumptions

The following assumptions are made for this case study:

- The base URL of the mail client is assumed to be `abc.siroe.com`
- the Gateway URL is assumed to be `gateway.sesta.com`

- Relevant entries exist in the Proxies for Domains and Subdomains list in the Gateway service

Sample page 1

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<!-- saved from
url=(0053)http://abc.siroe.com/mailclient/destin/?Cmd=navbar -->
<HTML XMLNS:WM><HEAD>
<META http-equiv=Content-Type content="text/html; CHARSET=utf-8">
<META http-equiv=Pragma content=no-cache>
<META http-equiv=Expires content=0><!--Copyright (c) 2000 Microsoft
Corporation.  All rights reserved.--><!--CURRENT FILE== "IE5" "WIN32"
navbar -->
<STYLE>WM\:DROPMENU {
BEHAVIOR: url(http://abc.siroe.com/mailweb/controls/dropmenu.htc)
}
</STYLE>
<LINK href="destin_files/navbar.css" type=text/css rel=stylesheet>
<SCRIPT language=javascript>
var g_szUserBase= "http://abc.siroe.com/mailclient/destin"+"/";
var g_szFolder= ".";
var g_szVirtualRoot= "http://abc.siroe.com/mailweb";
var g_szImagePath= g_szVirtualRoot + "/img/";
</SCRIPT>
<SCRIPT src="/destin_files/navbar.js"></SCRIPT>
<META content="MSHTML 6.00.2600.0" name=GENERATOR></HEAD>
<BODY oncontextmenu=return(event.ctrlKey); onselectstart=return(false);
id=outbar_mainbody style="BACKGROUND-COLOR: appworkspace" leftMargin=0
topMargin=0 scroll=no>
<TABLE class=nbTableMain id=nbTableMain style="HEIGHT: 100%" cellSpacing=0
cols=1 cellPadding=0 rows="2">
<TBODY>
```

```
<TR>
<TD class=treeBrand>
<DIV class=treeOFLOW><IMG
style="PADDING-RIGHT: 0px; PADDING-LEFT: 0px; PADDING-BOTTOM: 0px;
PADDING-TOP: 0px"
src="/destin_files/logo-ie5.gif" border=0></DIV></TD></TR>
<TR height="100%">
<TD>
<TABLE class=nbTable cellSpacing=0 cols=1 cellPadding=0 rows="4">
<TBODY>
<TR>
<TD class=nbFlybar id=show_navbar onkeydown=flybar_keydown()
onclick=ToggleTab(this.id) tabIndex=0 noWrap>
<DIV class=treeOFLOW>Shortcuts</DIV></TD></TR>
<TR style="HEIGHT: 100%">
<TD id=idOutbarpane style="TEXT-ALIGN: center" vAlign=top><A
id=inbox
href="http://abc.siroe.com/mailclient/destin/Inbox/?Cmd=contents
&amp;Page=1"
target=viewer alt="Go to inbox"><IMG class=nbImage alt="Go to inbox"
src="destin_files/navbar-inbox.gif"></A>
<DIV class=nbLabel>Inbox</DIV><BR><A id=calendar
href="http://abc.siroe.com/mailclient/destin/Calendar/?Cmd=contents"
target=viewer alt="Go to calendar"><IMG class=nbImage
alt="Go to calendar" src="destin_files/navbar-calendar.gif"></A>
<DIV class=nbLabel>Calendar</DIV><BR><A id=contacts

href="http://abc.siroe.com/mailclient/destin/Contacts/?Cmd=contents"
target=viewer alt="Go to contacts"><IMG class=nbImage
alt="Go to contacts" src="destin_files/navbar-contacts.gif"></A>
<DIV class=nbLabel>Contacts</DIV><BR><A id=options
```

```
href="http://abc.siroe.com/mailclient/destin/?Cmd=options"
target=viewer alt="Go to options"><IMG class=nbImage
alt="Go to options" src="destin_files/navbar-options.gif"></A>
<DIV class=nbLabel>Options</DIV></TD></TR>
<TR style="HEIGHT: 1.5em">
<TD class=nbFlybar id=show_folders onkeydown=flybar_keydown()
onclick=ToggleTab(this.id) tabIndex=0 noWrap>
<DIV class=treeOFLOW>Folders</DIV></TD></TR>
<TR>
<TD class=nbTreeProgress id=treeProgress style="DISPLAY: none"
vAlign=top noWrap><SPAN id=idLoading
style="OVERFLOW: hidden">Loading...</SPAN>
</TD></TR></TBODY></TABLE></TD></TR></TBODY></TABLE>
</BODY></HTML>
```

Description

Table 3-3 shows the mapping between the sample ruleset and the case study.

Table 3-3 Mapping Between Sample Ruleset and Case Study

Page Content	Rule Applied	Rewriter Output	Description
`var g_szVirtualRoot="http://abc.siroe.com/mailweb";`	<Variable name="URL"> g_szVirtualRoot </Variable>	`var g_szVirtualRoot= "http://gateway.sesta.com/http://abc.siroe.com/mailweb";`	`g_szVirtualRoot` is a variable whose value is a simple URL. This rule tells Rewriter to search for a variable `g_szVirtualRoot` of type URL. If such a variable exists in the web page, Rewriter converts this to an absolute URL, and prefixes the Gateway URL.

Table 3-3 Mapping Between Sample Ruleset and Case Study

Page Content	Rule Applied	Rewriter Output	Description
`src="/destin_files/logo-ie5.gif"`	<Attribute name="src" />	`src="http://gateway.sesta.com/http://abc.siroe.com/destin_files/logo-ie5.gif`	src is the name of an attribute, and does not have any tag or valuePattern attached to it. This rule tells Rewriter to search for all attributes with the name `src`, and rewrite the value of that attribute.
`href="http://abc.siroe.com/mailclient/destin/Inbox/?Cmd=contents&amp;Page=1"`	`<Attribute name="href"/>`	`href="http://gateway.sesta.com/http://abc.siroe.com/mailclient/destin/Inbox/?Cmd=contents&amp;Page=1"`	href is the name of an attribute, and does not have any tag or valuePattern attached to it. This rule tells Rewriter to search for all attributes with the name `href`, and rewrite the value of that attribute.

NOTE The order of priority for applying the ruleset is `hostname-subdomain-domain`.

For example, assume that you have the following entries in the Domain-based rulesets list:

`sesta.com|ruleset1`

`eng.sesta.com|ruleset2`

`host1.eng.sesta.com|ruleset3`

`ruleset3` is applied for all pages on `host1`.

`ruleset2` is applied for all pages in the `eng` subdomain, except for pages retrieved from `host1`.

`ruleset1` is applied for all pages in the `sesta.com` domain, except for pages retrieved from the `eng` subdomain, and from `host1`.

5. Click Save at the top or bottom of the page to record the change.
6. Restart the Gateway from a terminal window:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Ruleset for Outlook Web Access

SRA software supports MS Exchange 2000 SP3 installation and MS Exchange 2003 of Outlook Web Access (OWA) on the Sun Java System Web Server (formerly Sun™ ONE Web Server) and the IBM application server.

➤ To Configure the OWA Ruleset

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway Profile page displays.
4. Click the Gateway profile for which you want to set the attribute.

   The Gateway - *gateway-profile-name* page displays.
5. In the Map URIs to RuleSets field, enter the server name where Exchange 2000 is installed followed by the Exchange 2000 Service Pack 4 OWA ruleset.

   For example:

   ```
   exchange.domain.com|exchange_2000sp3_owa_ruleset.
   ```

Mapping of 6.x RuleSet with 3.0

The following table lists the mapping of the SRA Rewriter rules with the previous releases of the Portal Server product.

Table 3-4 Mapping of Rules with SP3

Rewriter 6.0 DTD Element	Rewriter 3.0 List Box Name
Rules for HTML Content	
Attribute - URL	Rewrite HTML Attributes
Attribute - DJS	Rewrite HTML Attributes containing JavaScript
Form	Rewrite Form Input Tag List

Table 3-4 Mapping of Rules with SP3

Rewriter 6.0 DTD Element	Rewriter 3.0 List Box Name
Applet	Rewrite Applet/Object Parameter Values List
Rules for JavaScript Content	
Variable - URL	Rewrite JavaScript Variables in URL
Variable - EXPRESSION	Rewrite JavaScript Variables Function
Variable - DHTML	Rewrite JavaScript Variables in HTML
Variable - DJS	Rewrite JavaScript Variables in JavaScript
Variable - SYSTEM	Rewrite JavaScript System Variables
Function - URL	Rewrite JavaScript Function Parameters
Function - EXPRESSION	Rewrite JavaScript Function Parameters Function
Function - DHTML	Rewrite JavaScript Function Parameters in HTML
Function - DJS	Rewrite JavaScript Function Parameters In JavaScript
Rules for XML Content	
Attribute - URL	Rewrite Attribute value of XML Document
TagText	Rewrite Text data of XMl Document
Rules for CSS Content	
Rules are not required. By default, all URLs are translated	
Rules for WML Content	
No rules defined. WML is treated at HTML and HTML rules are applied.	
Rules for WMLScript Content	
No support for WML Script	

Chapter 4

NetFile

This chapter describes NetFile and explains its operation. To configure NetFile, see Chapter 10, “Configuring NetFile” on page 283.

This chapter covers the following topics:

- Overview of NetFile
- Supported File Access Protocols
- Enabling Access to NetFile
- Enabling Logging for NetFile
- Configure UNIX Authentication

Overview of NetFile

NetFile is a file manager application that enables the user to access and operate on remote file systems and directories.

The NetFile component of SRA is available as Java1 and Java2 applets. Users who do not have the Java2 Plugin for their browsers can use the Java1 applet. The Java2 applet has a better interface and increased ease of accessibility.

NetFile provides the following key features:

- Facility to add or remove shares or folders
- File upload and download
- Search for files and folders
- File compression using GZIP and ZIP
- Mail facility within the NetFile environment

- Save the current NetFile session information
- Drag and Drop of files

To configure NetFile, see Chapter 10, “Configuring NetFile”.

Supported File Access Protocols

NetFile allows you to access remote systems using FTP, JCIFS (Windows), and NFS protocols. It includes the following file access protocol features:

- If the user specifies AUTODETECT to add a system, NetFile uses the following sequence to automatically detect which protocol to use:
    - Checks the host for FTP server on port 21. If the FTP response contains the string "NetWare", this is considered a NETWARE host.
    - Checks the host for NFS server on port 2049.
    - Checks the host for Windows on port 139.
    - If all of the above fail, a message saying unable to determine the host type is displayed.

  The first file system type that is detected is used to connect to the requested host. The host detection order can be changed in the Identity Server administration console.

NOTE The connection fails if the servers are running on non-standard ports.

- NetFile allows users to select the file server and protocol of their choice.

  For each of these protocols, the platforms that are supported are listed below.

Table 4-1 File Systems and Supported Protocols

File System/Protocol	Platform
NFS	Solaris 2.6 and higher
JCIFS	Windows 95/98/NT/2000/ME/XP

Table 4-1 File Systems and Supported Protocols

File System/Protocol	Platform
FTP	Novell FTP 5.1 Server on Novell Netware MS FTP Server 4.0 on Win NT 4.0 MS FTP Server 5.0 on Win NT 2000 Solaris FTP Server WU_FTP 2.6.1 ProFTPD 1.2.8 vsFTPd 1.2.0

NOTE Support for Novell Netware is only through FTP server and not through native access.

NOTE To upload files to a ProFTPD server using NetFile, "AllowStoreRestart" needs to be set to "on" in the `proftpd.conf` file on the host running ProFTPD server.

Enabling Access to NetFile

When you install SRA, the NetFile service is registered only for the organization that you specified during installation.

➤ To Enable NetFile for Organizations and Users

1. Register the NetFile service to the organization that requires NetFile access.
2. Create the NetFile policy based on the NetFile service and assign the NetFile policy for organization and role which require access to NetFile.
3. Assign the NetFile service to each user who requires access to NetFile.

   See the *Identity Server Administration Guide* for more information on creating and assigning policies and services.

Enabling Logging for NetFile

Specify the log location using the Identity Server Logging service to enable logging for NetFile. The name of the log file is `srapNetFile`. By default it is located in the `/var/opt/SUNWam/logs` directory.

Configure UNIX Authentication

➤ To Enable Unix Authentication

1. Log in to the Identity Server administration console as administrator.
2. Select the Identity Management tab from the administration console.
3. Select Services from the View drop down menu in the left view pane.

   If UNIX shows up in the right view pane, it needs to be registered.
4. Register the service by selecting the checkbox next to UNIX and click Register.
5. Click the arrow next to UNIX in the left view pane and click Create.

   The service template is created.
6. Click Save.
7. Log out of the administration console.
8. Restart the Identity Server as root or the user Identity Server it is configured to run as:

   ```
   /etc/init.d/amserver startall
   ```
9. Verify that the doUnix process is running:

   ```
   ps -ef | grep doUnix
   ```

➤ To Configure Unix Authentication

1. Telnet to the local host on the configuration port as follows:

   ```
   telnet localhost 58946
   ```
2. Type the Unix Helper Listen Port number.

   Specify the default value of `57946` for the Listen Port.
3. Type the Unix Helper Session Timeout value in seconds.

4. Type the Unix Helper Max Sessions value.

   A message saying “doUnix configured successfully” is displayed.

Chapter 5

Netlet

This chapter describes how to use Netlet to run applications securely between users’ remote desktops and the servers running applications on your intranet. To configure Netlet, see Chapter 11, “Configuring Netlet” on page 301.

This chapter covers the following topics:

- Overview of Netlet
- Downloading an Applet From a Remote Host
- Defining Netlet Rules
- Sample Netlet Rules
- Enabling Netlet Logging
- Running Netlet in a Sun Ray Environment

Overview of Netlet

Sun Java™ System Portal Server software users may want to run popular or company-specific applications on their remote desktops in a secure manner. You can provide secure access to these applications by setting up Netlet on your platform.

Netlet enables users to securely run common TCP/IP services over insecure networks such as the Internet. You can run TCP/IP applications (such as Telnet and SMTP), HTTP applications, and any fixed port applications.

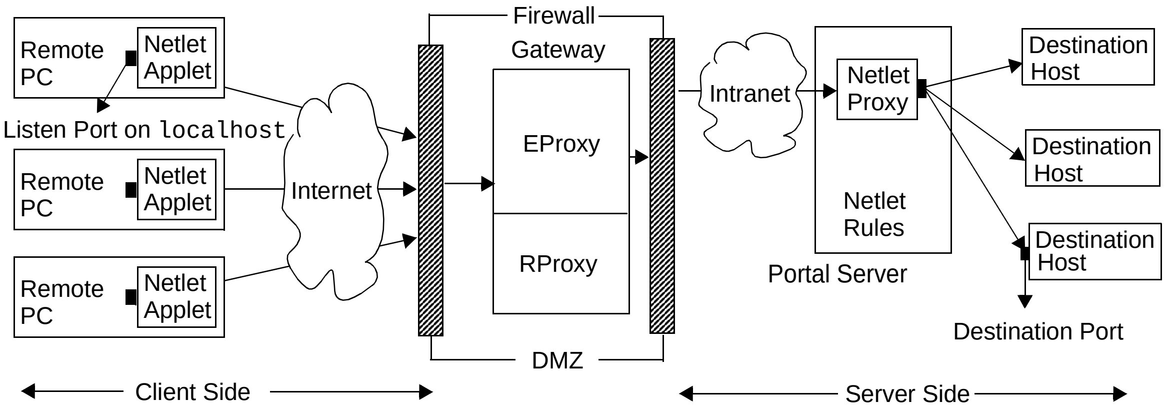
You can run an application over Netlet if it is TCP/IP-based or it uses fixed ports.

NOTE Dynamic ports are supported only when FTP is used. To use Microsoft Exchange, use OWA (Outlook Web Access).

Netlet Components

The various components used by Netlet are shown in Figure 5-1.

Figure 5-1 Netlet Components



Listen Port on localhost

This is the port on the client machine on which the Netlet applet listens. The client machine is the localhost.

Netlet Applet

The Netlet applet is responsible for setting up an encrypted TCP/IP tunnel between the remote client machine and intranet applications such as Telnet, Graphon or Citrix. The applet encrypts the packets and sends them to the Gateway, and decrypts the response packets from the Gateway and sends them to the local application.

For static rules the Netlet applet is downloaded automatically when the user logs into the portal. For dynamic rules, the applet is downloaded when the user clicks on the link corresponding to the dynamic rule. See “Types of Rules” on page 188 for details on static and dynamic rules.

To run Netlet in a Sun Ray Environment, see “Running Netlet in a Sun Ray Environment” on page 201.

Netlet Rules

A Netlet rule maps an application that needs to run on a client machine to the corresponding destination host. This means that Netlet operates only on packets sent to ports defined in the Netlet rule. This ensures greater security.

As an administrator, you need to configure certain rules for the functioning of Netlet. These rules specify various details such as the cipher to be used, URL to invoke, the applets to be downloaded, the destination port and the destination host. When a user on a client machine makes a request through Netlet, these rules help determine how the connection has to be established. See "Defining Netlet Rules" on page 185 for details.

Netlet Provider

This is the UI component of Netlet. The provider allows users to configure the required applications from the Portal Server, Secure Remote Access desktop. A link is created in the provider, and the user clicks on this to run the required application. Users can also specify the destination host for a dynamic rule in the desktop Netlet provider. See "Defining Netlet Rules" on page 185.

EProxy

All client requests are routed through the EProxy. EProxy handles only Netlet requests and passes any other requests to the RProxy. EProxy parses Netlet requests and passes them to the Netlet proxy (if it is enabled) or directly to the destination host.

Netlet Proxy (Optional)

The Gateway ensures a secure tunnel between the remote client machine and the Gateway. The Netlet proxy is optional and you may choose not to install this proxy during the installation. For information on the Netlet proxy, see "Using a Netlet Proxy" on page 65.

Destination Port

This is the port on which the destination application's host listens.

Netlet Usage Scenario

The following sequence of events are involved in using Netlet:

1. The remote user logs into the Portal Server, Secure Remote Access desktop.

2. If a static Netlet rule has been defined for a user, role or organization, the Netlet applet is automatically downloaded to the remote client.

   If a dynamic rule has been defined for a user, role, or organization, the user needs to configure the required application in the Netlet provider. The Netlet applet is downloaded when the user clicks on the application link in the Netlet provider. See "Defining Netlet Rules" on page 185 for details on static and dynamic rules.

3. Netlet listens on the local ports defined in the Netlet rules.

4. Netlet sets up a channel between the remote client and host over the ports specified in the Netlet rule.

Working With Netlet

For Netlet to work as required for various users across different organizations, you need to do the following:

1. Determine whether you need to create static or dynamic rules based on the user requirements. See "Types of Rules" on page 188.

2. Define the global options in the Netlet template from the Service Configuration tab on the Identity Server administration console. See Chapter 11, "Configuring Netlet" on page 301.

3. Determine whether the rules should be organization, role, or user-based and make modifications as required at each level. See the *Portal Server Administration Guide* for details on organization, role and user.

NOTE Do not localize the value for the frameset parameter in the `srapNetletServlet.properties` file.

Downloading an Applet From a Remote Host

Sometimes a page is returned by a URL that contains an embedded applet that needs to be fetched from a remote machine. However Java security does not allow an applet to communicate with a host that it is not downloaded from. To allow the applet to communicate with the Gateway through the local network port, you need to check the Download Applet field on the Identity Server administration console and specify the following syntax:

local-port:server-host:server-port

where

local-port is the local port where Netlet listens for traffic originating from the applet

server-host is where the applet is to be downloaded from

server-port is the port used to download the applet

Defining Netlet Rules

Netlet configuration is defined through Netlet rules that are configured in the Identity Server administration console under the SRA Configuration section. Netlet rules can be configured for organizations, roles, or users. If the Netlet rule is for a role or user, select the desired role or user after selecting the organization.

CAUTION Netlet rules do not support multibyte entries. Do not specify multibyte characters for any of the editable fields in Netlet rules.

Netlet rules cannot contain any port number higher than 64000.

Table 5-1 lists the fields in a Netlet rule.

Table 5-1 Fields in a Netlet Rule

Parameter	Description	Value
RuleName	Designates a name for this Netlet rule. You need to specify a unique name for each rule. This is useful while defining user access to specific rules. See "Define Access to Netlet Rules" on page 310 for details.	
Encryption Ciphers	Defines the encryption cipher, or specifies the list of ciphers that the user can choose from.	The ciphers that you select appear in the Netlet provider as a list. The user can choose the required ciphers from the selected list. Default - The Default VM Native Cipher and the Default Java Plugin Cipher specified in the Netlet administration console are used.

Table 5-1 Fields in a Netlet Rule

Parameter	Description	Value
URL	Specifies the URL that the browser opens when the user clicks the associated link in the Netlet provider. The browser opens the window for the application and connects to `localhost` at the local port number specified later in the rule. You need to specify a relative URL.	URL to the application invoked by the Netlet rule. For example, `telnet://localhost:30000`. Specify a URL if the application uses an applet to invoke the application. `null` – Value that you set if the application is not started by a URL or controlled by the desktop. This is normally true for non-web-based applications.
Download Applet	Indicates whether it is necessary to download an applet for this rule.	False - Do not download an applet. True - Download the applet from the Portal Server machine using the loopback port. Specify the applet details in the format *local-port:server-host:server-port* where: • *local-port* indicates the destination port on the client. This port must be different from the default loopback port. See Chapter 11, “Configuring Netlet” for details. Specify a unique `local port` for each rule. • *server-host* is the name of the server from which to download the applet. • *server-port* represents the port on the server used to download the applet. If an applet is to be downloaded, and if the server is not specified, the applet is downloaded from the Portal Server host.
Extend Session	This controls the idle time-out of a Portal Server session when Netlet is active.	Enabled - This is required to keep the portal session alive when only Netlet is active and rest of the portal application is idle. Disabled - The portal session idle times out at session idle time-out even though the Netlet application is active but rest of the portal application is idle.

Table 5-1 Fields in a Netlet Rule

Parameter	Description	Value
Local Port	Port on the client where Netlet listens.	The value of *local-port* must be unique. You cannot specify a particular port number in more than one rule. Specify multiple local ports if you are specifying multiple hosts for multiple connections. See "Static Rule With Multiple Host Connections" on page 193 for the syntax. For an FTP rule the local port value has to be 30021
Destination Host(s)	Recipient of the Netlet connection.	*host* - Name of the host to receive the Netlet connection. This is used in a static rule. Use either the simple host name such as `siroe`, or a fully-qualified DNS-style host name such as `siroe.mycompany.com`. Specify multiple hosts for the following reasons: • to establish connection with each host specified. You need to specify the corresponding client and destination ports for each host specified. See "Static Rule With Multiple Host Connections" on page 193 for the syntax. • to try to connect to any available host from the list of hosts specified. See "Static Rule with Multiple Host Selection" on page 194 for the syntax. `TARGET` - Rules that specify `TARGET` in the syntax are dynamic rules. `TARGET` indicates that end-users can specify the required destination host or hosts in the Netlet provider of the desktop. You cannot have a combination of a static host and TARGET in a single rule.

Table 5-1 Fields in a Netlet Rule

Parameter	Description	Value
Destination Port(s)	The port on the destination host	In addition to the host and destination host, you must specify a destination port. You can specify multiple destination ports in case of multiple destination hosts. Specify multiple ports in the format `port1+port2+port3-port4+port5`. The plus (+) sign between ports numbers indicates the alternative ports for a single destination host. The minus (-) sign between port numbers is the separator between the port numbers for different destination hosts. Here, Netlet tries to connect to the first destination host specified using `port1`, `port2` and `port3` in order. If this fails, Netlet tries to connect to the second host using `port4` and `port5` in that order. You can configure multiple ports only for static rules.

For the Gateway to get the session notification from Portal Server, add the following:

`com.iplanet.am.jassproxy.trustAllServerCerts=true`

to the following property file

`/etc/opt/SUNWam/config/AMConfig.properties` on the Portal Server

2. Restart the Identity Server.

Types of Rules

There are two types of Netlet rules based on how the destination host is specified in the rule.

Static Rule

A static rule specifies a destination host as part of the rule. If you create a static rule, the user does not have the option to specify the required destination host. In the following example, sesta is the destination host.

Rule Name	Encryption Cipher	URL	Download Applet	Extend Session	Local Port	Destination Host(s)	Destination Port(s)
ftpstatic	SSL_RSA_ WITH_RC4 _128_MD5	null	false	true	30021	sesta	21

You can configure multiple destination hosts and ports for static rules. See "Static Rule With Multiple Host Connections" on page 193 for an example.

Dynamic Rule

In a dynamic rule, the destination host is not specified as a part of the rule. The user can specify the required destination host in the Netlet provider. In the following example, TARGET is the placeholder for the destination host.

Rule Name	Encryption Cipher	URL	Download Applet	Extend Session	Local Port	Destination Host(s)	Destination Port(s)
ftpdynamic	SSL_RSA_ WITH_RC4 _128_MD5	null	false	true	30021	TARGET	21

Encryption Ciphers

Based on the encryption cipher, Netlet rules can be further classified as follows:

- **User Configurable Cipher Rules -** In this rule, you can specify a list of ciphers that users can choose from. These optional ciphers appear as a list in the Netlet provider. The user can choose the required cipher from the list. In the following example, the user can choose from multiple ciphers.

Rule Name	Encryption Cipher	URL	Download Applet	Extend Session	Local Port	Destination Host(s)	Destination Port(s)
Telnet	SSL_RSA_WITH _RC4_128_SHA	null	false	true	30000	TARGET	23

Rule Name	Encryption Cipher	URL	Download Applet	Extend Session	Local Port	Destination Host(s)	Destination Port(s)
	SSL_RSA_WITH _RC4_128_MD5						

NOTE Although the Portal Server host may have various ciphers enabled, the user can choose only from the list that is configured as part of the Netlet rule.

See "Supported Ciphers" on page 190 for a list of the ciphers supported by Netlet.

- **Administrator Configured Cipher Rules -** In this rule, the cipher is defined as part of the Netlet rule. The user does not have the option to choose the required cipher. In the following example, the cipher is configured to be SSL_RSA_WITH_RC4_128_MD5.

Rule Name	Encryption Cipher	URL	Download Applet	Extend Session	Local Port	Destination Host(s)	Destination Port(s)
Telnet	SSL_RSA_WITH_RC4_128_MD5	null	false	true	30000	TARGET	23

See "Supported Ciphers" on page 190 for a list of ciphers supported by Netlet.

Supported Ciphers

Table 5-2 lists the ciphers supported by Netlet.

Table 5-2 List of Supported Ciphers

Ciphers
Native VM Ciphers
KSSL_SSL3_RSA_WITH_3DES_EDE_CBC_SHA
KSSL_SSL3_RSA_WITH_RC4_128_MD5
KSSL_SSL3_RSA_WITH_RC4_128_SHA

Table 5-2 List of Supported Ciphers

Ciphers
KSSL_SSL3_RSA_EXPORT_WITH_RC4_40_MD5
KSSL_SSL3_RSA_WITH_DES_CBC_SHA
Java Plugin Ciphers
SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5
SSL_RSA_WITH_DES_CBC_SHA
SSL_RSA_WITH_NULL_MD5

Backward Compatibility

Earlier versions of Portal Server did not support ciphers as part of the Netlet rules. For backward compatibility with existing rules without ciphers, a default cipher is used by the rules. An existing rule without ciphers such as:

Rule Name	Encryption Cipher	URL	Download Applet	Extend Session	Local Port	Destination Host(s)	Destination Port(s)
Telnet		telnet://localhost:30000	false	true	30000	TARGET	23

is interpreted as:

Rule Name	Encryption Cipher	URL	Download Applet	Extend Session	Local Port	Destination Host(s)	Destination Port(s)
Telnet	Default ciphers	telnet://localhost:30000	false	true	30000	TARGET	23

This is similar to an Administrator Configured Rule with the Encryption cipher field chosen as Default. See "Specify the Default Encryption Cipher" on page 305 for details.

NOTE Netlet rules cannot contain any port number higher than 64000.

Netlet Rule Examples

This section contains some examples of Netlet rules to illustrate how Netlet syntax works.

- Basic Static Rule
- Static Rule With Multiple Host Connections
- Dynamic Rule to Invoke a URL
- Dynamic Rule to Download an Applet

Basic Static Rule

This rule supports a Telnet connection from the client to the machine sesta.

Rule Name	Encryption Cipher	URL	Download Applet	Extend Session	Local Port	Destination Host(s)	Destination Port(s)
myrule	SSL_RSA_ WITH_RC4 _128_MD5	null	false	true	1111	sesta	23

where

myrule is the name of the rule.

SSL_RSA_WITH_RC4_128_MD5 indicates the cipher to be used.

null indicates that this application is not invoked by a URL or run through the desktop.

false indicates that the client does not download an applet to run this application.

true indicates that Portal Server should not time out when the Netlet connection is active.

1111 is the port on the client where Netlet listens for a connection request from the destination host.

sesta is the name of the recipient host in the Telnet connection.

23 is the port number on the destination host for the connection, in this case the well-known port for Telnet.

The desktop Netlet provider does not display a link, but Netlet automatically starts and listens on the port specified (1111). Instruct the user to start the client software - in this case a Telnet session that connects to localhost on port 1111.

For example, to start the Telnet session, the client needs to type the following on the UNIX command line in a terminal:

```
telnet localhost 1111
```

Static Rule With Multiple Host Connections

This rule supports a Telnet connection from the client to two machines, sesta and siroe.

Rule Name	Encryption Cipher	URL	Download Applet	Extend Session	Local Port	Destination Host(s)	Destination Port(s)
myrule	SSL_RSA_WITH_RC4_128_MD5	null	false	true	1111	sesta	23
					1234	siroe	23

where

23 is the port number on the destination host for the connection – reserved port for Telnet.

1111 is the port on the client where Netlet listens for a connection request from the first destination host sesta.

1234 is the port on the client where Netlet listens for a connection request from the second destination host siroe.

The first six fields in this rule are the same as in "Basic Static Rule" on page 192. The difference is that three more fields identify the second destination host.

When you add additional targets to a rule, you must add three fields, `local port`, `destination host`, and `destination port`, for each new destination host.

NOTE You can have multiple sets of three fields describing the connection to each destination host. Listen port numbers which are less than 2048 must not be used if the remote client is UNIX-based because low numbered ports are restricted and you must be root to start a listener.

This rule works the same as the previous rule. The Netlet provider does not display any link, but Netlet automatically starts and listens on the two ports specified (1111 and 1234). The user needs to start the client software, in this case a Telnet session that connects to `localhost` on port 1111 or the `localhost` on port 1234 to connect to host example2.

Static Rule with Multiple Host Selection

Use this rule to specify multiple alternative hosts. If connection to the first host in the rule fails, Netlet tries to connect to the second host specified and so on.

Rule Name	Encryption Cipher	URL	Download Applet	Extend Session	Local Port	Destination Host(s)	Destination Port(s)
gojoe	SSL_RSA_WITH_RC4_128_MD5	/gojoe.html	8000:gojoeserver:8080	true	10491	siroe+sesta	35+26+491-35+491

where

`10491` is the port on the client where Netlet listens for a connection request from the destination host.

Netlet tries to establish connection with `siroe` on port `35`, port `26` and port `491` in the same order, depending on which one is available.

If connections to `siroe` are not possible, Netlet tries to connect to `sesta` on port `35` and `491` in the same order.

The plus (+) sign between hosts indicates alternative hosts.

The plus (+) sign between ports numbers indicates the alternative ports for a single destination host.

The minus (-) sign between port numbers is the separator between the port numbers for different destination hosts.

Dynamic Rule to Invoke a URL

This rule enables a user to configure the destination host required, enabling the user to telnet to various hosts over Netlet.

Rule Name	Encryption Cipher	URL	Download Applet	Extend Session	Local Port	Destination Host(s)	Destination Port(s)
myrule	SSL_RSA_WITH_RC4_128_MD5	telnet://localhost:30000	false	true	30000	TARGET	23

where

`myrule` is the name of the rule.

SSL_RSA_WITH_RC4_128_MD5 indicates the cipher to be used.

`telnet://localhost:30000` is the URL invoked by the rule.

`false` indicates that no applets are to be downloaded.

`Extend Session(true)` indicates that the Portal Server should not time out when the Netlet connection is active.

`30000` is the port on the client where Netlet listens for connection requests for this rule.

`TARGET` indicates that the destination host needs to be configured by the user using the Netlet provider.

`23` is the port on the destination host opened by Netlet, in this case the well-known port for Telnet.

➤ To Run Netlet After a Rule is Added

After this rule is added, the user must complete some steps to get Netlet running as expected. The user needs to do the following on the client side:

1. Click Edit in the Netlet provider section of the standard Portal Server desktop.

   The new Netlet rule is listed under Rule Name in the Add New Target section.

2. Choose the rule name and type the name of the destination host.
3. Save the changes.

   The user returns to the desktop with the new link visible in the Netlet provider section.
4. Click the new link.

   A new browser is launched that goes to the URL given in the Netlet rule.

NOTE You can add more than one destination host for the same rule by repeating these steps.

Dynamic Rule to Download an Applet

This rule defines a GO-Joe connection from the client to hosts that are dynamically allocated. The rule downloads a GO-Joe applet from the server on which the applet is located, to the client.

Rule Name	Encryption Cipher	URL	Downlaod Applet	Extend Session	Local Port	Destination Host(s)	Destination Port(s)
gojoe	SSL_RSA_WITH_RC4_128_MD5	/gojoe.html	8000:gojoeserve:8080	true	3399	TARGET	58

where

`gojoe` is the name of the rule.

SSL_RSA_WITH_RC4_128_MD5 indicates the cipher to be used.

`/gojoe.html` for example is the path of the HTML page containing the applet, the path should be relative to the documentation root of the web container on which portal is deployed.

`8000:server:8080` indicates that port 8000 is the destination port on the client to receive the applet, `gojoeserve` is the name of the server providing the applet, and `8080` is the port on the server from which the applet is downloaded.

`Extended Session (true)` indicates that the Portal Server should not time out when the Netlet connection is active.

3399 is the port on the client where Netlet listens for connection requests of this type.

TARGET indicates that the destination host needs to be configured by the user using the Netlet provider.

58 is the port on the destination host opened by Netlet, in this case the port for GoJoe. Port 58 is the port that the destination host listens to for its own traffic. Netlet passes information to this port from the new applet.

Sample Netlet Rules

Table 5-3 lists sample Netlet rules for some common applications.

The table has 7 columns corresponding to the following fields in a Netlet rule: Rule Name, URL, Download Applet, Local Port, Destination Host, Destination Port. The last column includes a description of the rule.

NOTE Table 5-3 does not list the Cipher and Extend Session fields of the Netlet rule. Assume these to be "SSL_RSA_WITH_RC4_128_MD5" and "true" for the samples provided.

Table 5-3 Sample Netlet Rules

Rule	URL	Download Applet	LOCAL Port	Destination Host	Destination Port	Description
IMAP	null	false	10143	imapserver	143	The Netlet `local port` on the client side need not be the same as the `destination port` on the server side. If you use anything other than the standard IMAP and SMTP ports, make sure that the client is configured to connect on a port that is different from the standard port. Solaris client users will have trouble connecting to port numbers lower than 1024 unless they are running as root.
SMTP	null	false	10025	smtpserver	25	

Table 5-3 Sample Netlet Rules

Rule	URL	Download Applet	LOCAL Port	Destination Host	Destination Port	Description
Lotus Web Client	null	false	80	lotus-server	80	This rule tells Netlet to listen for the client on port 80, and connect to the server lotus-server on port 80. A requirement of the Lotus Web Client is that the client listen port must match the server port.
Lotus Notes Non-web Client	null	false	1352	lotus-domino	1352	With this rule, the Lotus Notes client can connect to a Lotus Domino server through Netlet. Ensure that when the client tries to connect to the server it must not point to `localhost` as the server name. It must point to the actual server name of the Lotus Domino server. The server name must be the same as the system name for the server. The client must resolve that name to `127.0.0.1` when using Netlet. There are two ways to accomplish this: • Set the server name to point to `127.0.0.1` in the client host table. • Export a DNS entry of the name of the server that points to `127.0.0.1`. The server name must be the same server name that was used to configure the Domino server during setup.

Table 5-3 Sample Netlet Rules

Rule	URL	Download Applet	LOCAL Port	Destination Host	Destination Port	Description
Microsoft Outlook and Exchange Server This will not work for Windows NT, 2000 and XP. Use Outlook Web Access through the Rewriter for Windows NT, 2000, and XP.	null	false	135	exchange	135	This rule tells Netlet to listen at port 135 on the client and connect to the server `exchange` on port 135. The Outlook client uses this port to make an initial attempt to contact the Exchange server and determine what subsequent ports to use to talk to the server. On the client machine: • The user has to change the hostname of the Exchange server that is configured in the Outlook client to `localhost`. The location of this option varies with the version of Outlook. • The user must map the hostname (single and fully qualified) of the Exchange server to the IP address `127.0.0.1` using the hosts file. • On Windows 95 or 98, the file is in `\Windows\Hosts` • On Windows NT4, the file is in `\WinNT\System32\drivers\etc\Hosts`. The entry looks like this: `127.0.0.1 exchange exchange.company.com` The Exchange server sends back its own name to the Outlook client. This mapping ensures that the Outlook client uses the Netlet client to connect back to the server.

Table 5-3 Sample Netlet Rules

Rule	URL	Download Applet	LOCAL Port	Destination Host	Destination Port	Description
FTP	null	false	30021	*your-ftp_server.your-domain*	21	You can provide FTP service to a single FTP Server, with controlled end-user accounts. This will ensure secure remote FTP transfers from an end-user system to a single location. Without a username, an FTP URL is interpreted as an anonymous FTP connection. You *must* define port 30021 as the local port for your Netlet FTP rule. Dynamic FTP is not supported using a Netlet connection.
Netscape 4.7 Mail Client	null	false	30143, 30025.	TARGET TARGET	10143 10025	In the Netscape client, the user needs to specify: `localhost:30143` for IMAP or incoming mails `localhost:30025` for SMTP or outgoing mails
Graphon	third_party/xsession_start.html	true	10491	TARGET	491	This is the rule used to access Graphon through the Netlet. `xsession_start.html` is bundled with Graphon.
Citrix	third_party/citrix_start.html	true	1494	TARGET	1494	This is the rule used to access Citrix through the Netlet. `citrix_start.html` is bundled with Citrix.
Remote Control	third_party/pca_start.html	true	5631 5632	TARGET TARGET	5631 5632	This is the rule used to access Remote Control through Netlet. `pca_start.html` is bundled with Remote Control.

Enabling Netlet Logging

You can enable logging of Netlet related activities in the Gateway service. See "Enable Netlet Logging" on page 280. The log files are created in the directory specified in the Log Location attribute as part of the Logging section of the Identity Server Configuration attributes.

The log file name has the following convention:

`srapNetlet`*_gateway-hostname_gateway-profile-name*

The Netlet log captures the following information:

- Start time
- Source address
- Source port
- Server address
- Server port(s)
- Stop time
- Status (start or stop)

Running Netlet in a Sun Ray Environment

If you want to run an application which requires the applet to be downloaded to the client machine on a Sun Ray environment, you need to change the HTML file. Here is a sample file showing you the necessary modifications that need to be done.

New HTML File

```
<!-- @(#)citrix_start.html 2.1     98/08/17 Copyright (c) 1998 i-Planet, Inc., All rights
reserved.  -->

<html>

<script language="JavaScript">

var KEY_VALUES;  // KEY_VALUES['key'] = 'value';

function retrieveKeyValues() {

      KEY_VALUES = new Object();

      var queryString  = '' + this.location;

      queryString = unescape(queryString);

      queryString = queryString.substring((queryString.indexOf('?')) + 1);

      if (queryString.length < 1) {
          return false; }
      var keypairs = new Object();
      var numKP = 0;
      while (queryString.indexOf('&') > -1) {
        keypairs[numKP] = queryString.substring(0,queryString.indexOf('&'));
        queryString = queryString.substring((queryString.indexOf('&')) + 1);
        numKP++;
      }
      // Store what's left in the query string as the final keypairs[] data.
      keypairs[numKP++] = queryString;
      var keyName;
      var keyValue;
      for (var i=0; i < numKP; ++i) {
        keyName = keypairs[i].substring(0,keypairs[i].indexOf('='));
        keyValue = keypairs[i].substring((keypairs[i].indexOf('=')) + 1);
        while (keyValue.indexOf('+') > -1) {
          keyValue = keyValue.substring(0,keyValue.indexOf('+')) + ' ' +
keyValue.substring(keyValue.indexOf('+') + 1);
        }
        keyValue = unescape(keyValue);
          // Unescape non-alphanumerics
        KEY_VALUES[keyName] = keyValue;
      }
}
function getClientPort(serverPort) {
    var keyName = "clientPort['" + serverPort +"']";
    return KEY_VALUES[keyName];
}
function generateContent() {
    retrieveKeyValues();
    var newContent =
        "<html>\n"
          + "<head></head>\n"
          + "<body>\n"
          + "<applet code=\"com.citrix.JICA.class\" archive=\"JICAEngN.jar\" width=800
height=600>\n"
          + "<param name=\"cabbase\" value=\"JICAEngM.cab\">\n"
          + "<param name=\"address\" value=\"localhost\">\n"
          + "<param name=ICAPortNumber value="
          + getClientPort('1494')
          + ">\n"
          + "</applet>\n"
          + "</body>\n"
          + "</html>\n";
    document.write(newContent);
}
</script>
<body onLoad="generateContent();">
</body>
</html>
```

Deprecated HTML File:

```
<html>
<body>
<applet code="com.citrix.JICA.class" archive="JICAEngN.jar" width=800 height=600>
<param name="cabbase" value="JICAEngM.cab">
<param name="address" value="localhost">
<param name=ICAPortNumber value=1494>
</applet>
</body></html>
```

Chapter 6

Netlet With PDC

This chapter describes how to configure the client browser's Java Plugin so that Netlet can be used with PDC.

NOTE Only Virtual Machines (VMs) with JSSE support Netlet with PDC.

Configuring Netlet for PDC

➤ To Configure Netlet for PDC

1. Export the client certificate from the browser in one of the following formats:

    - PKCS
    - JKS

    After exporting the client certificate, the Java Plugin should have the following JVM parameters that enable the VM to use the certificate:

    javax.net.ssl.keyStoreType

    javax.net.ssl.keyStorePassword

    javax.netl.ssl.keyStore

2. Go to Control Panel and Launch Java Plugin

3. Choose Advanced Tab, Java Runtime Environment

4. Specify the Java Runtime Parameters. For example:

   Djavax.net.ssl.keyStoreType=pkcs

   Djavax.net.ssl.keyStorePassword=testing123

   Djavax.netl.ssl.keyStore="C:\dir\test.cert"

5. Click Apply.

6. Close the Java plugin and restart the associated browsers.

Chapter 7

Certificates

This chapter describes certificate management and explains how to install self-signed certificates and certificates from a Certificate Authority.

This chapter covers the following topics:

- Overview of SSL Certificates
- Certificate Files
- Certificate Trust Attributes
- CA Trust Attributes
- The certadmin Script
- Generating Self-Signed Certificates
- Installing SSL Certificates From the Certificate Authority
- Adding a Root CA Certificate
- Modifying the Trust Attributes of a Certificate
- Listing Root CA Certificates
- Listing All Certificates
- Deleting a Certificate
- Printing a Certificate

Overview of SSL Certificates

The Portal Server Secure Remote Access software provides certificate-based authentication for remote users. SRA uses Secure Sockets Layer (SSL) to enable secure communication. The SSL protocol enables secure communication between two machines.

A SSL certificate provides encryption and decryption capabilities using a public and private key pair.

There are two types of certificates:

- Self-signed certificates (also called root CA certificate)
- Certificates issued by Certificate Authority (CA)

By default, a self-signed certificate is generated and installed when you install the Gateway.

You can generate, obtain, or replace a certificate anytime after installation.

SRA also supports client authentication with Personal Digital Certificates (PDCs). PDCs are a mechanism to authenticate a user through SSL client authentication. With SSL client authentication, the SSL handshake ends at the Gateway. The Gateway extracts the user's PDC and passes it to the authenticated server. This server uses the PDC to authenticate the user. To configure PDCs along with Authentication Chaining, see "Using Authentication Chaining" on page 76.

SRA provides a tool named `certadmin` that you can use to manage the SSL certificates. See "The certadmin Script" on page 214.

Certificate Files

Certificate related files are located in `/etc/opt/SUNWps/cert/default/gateway-profile-name`. This directory contains 5 files by default.

Table 7-1 lists these files and their descriptions.

Table 7-1 Certificate Files

Filename	Type	Description
`cert8.db`, `key3.db`, `secmod.db`	Binary	Contains the data for certificates, keys, and cryptographic modules. Can be manipulated using the `certadmin` script. Have the same format as the database files used by the Sun Java™ System Web Server and are located in *portal-server-install-root*`/SUNWwbsvr/alias`. If necessary, these files can be shared between the Portal Server host and gateway components or the Gateway.
`.jsspass`	hidden text file	Contains the encrypted password for the SRA key database.
`.nickname`	hidden text file	Stores the names of the token and certificate that the Gateway needs to use in the format *token-name:certificate-name*. If you are using the default token (the token on the default internal software encryption module), omit the token name. In most cases, the `.nickname` file stores only the certificate name. As an administrator, you can modify the certificate name in this file. The certificate that you specify will now be used by the Gateway.

Certificate Trust Attributes

The trust attributes of a certificate indicate the following information:

- Whether the certificate (in the case of client or server certificate) was issued by a Trusted CA.
- Whether the certificate (in the case of a root certificate) can be trusted as the issuer of a server or client certificate.

There are three available trust categories for each certificate, expressed in this order: “SSL, email, object signing”. Only the first category is useful got the Gateway. In each category position, zero or more trust attribute codes are used.

The attribute codes for the categories are separated by commas, and the entire set of attributes is enclosed by quotation marks. For example, the self-signed certificate generated and installed during the Gateway installation is marked "u,u,u" which means it is a server certificate (user certificate) as opposed to a root CA certificate.

Table 7-2 lists the possible attribute values and the meaning of each value..

Table 7-2 Certificate Trust Attributes

Attribute	Description
p	Valid peer
P	Trusted peer (implies p)
c	Valid CA
T	Trusted CA to issue client certificates (implies c)
C	Trusted CA to issue server certificates (SSL only) (implies c)
u	Certificate can be used for authentication or signing
w	Send warning (use with other attributes to include a warning when the certificate is used in that context)

CA Trust Attributes

Most well-known public CAs are included in the certificate database. See "Modifying the Trust Attributes of a Certificate" on page 225 for information on modifying the trust attributes of a public CA.

Table 7-3 lists the most common Certificate Authorities with the trust attributes.

Table 7-3 Public Certificate Authorities

Certificate Authority Name	Trust Attribute
Verisign/RSA Secure Server CA	CPp,CPp,CPp
VeriSign Class 4 Primary CA	CPp,CPp,CPp
GTE CyberTrust Root CA	CPp,CPp,CPp
GTE CyberTrust Global Root	CPp,CPp,CPp
GTE CyberTrust Root 5	CPp,CPp,CPp
GTE CyberTrust Japan Root CA	CPp,CPp,CPp
GTE CyberTrust Japan Secure Server CA	CPp,CPp,CPp

Table 7-3 Public Certificate Authorities

Thawte Personal Basic CA	CPp,CPp,CPp
Thawte Personal Premium CA	CPp,CPp,CPp
Thawte Personal Freemail CA	CPp,CPp,CPp
Thawte Server CA	CPp,CPp,CPp
Thawte Premium Server CA	CPp,CPp,CPp
American Express CA	CPp,CPp,CPp
American Express Global CA	CPp,CPp,CPp
Equifax Premium CA	CPp,CPp,CPp
Equifax Secure CA	CPp,CPp,CPp
BelSign Object Publishing CA	CPp,CPp,CPp
BelSign Secure Server CA	CPp,CPp,CPp
TC TrustCenter, Germany, Class 0 CA	CPp,CPp,CPp
TC TrustCenter, Germany, Class 1 CA	CPp,CPp,CPp
TC TrustCenter, Germany, Class 2 CA	CPp,CPp,CPp
TC TrustCenter, Germany, Class 3 CA	CPp,CPp,CPp
TC TrustCenter, Germany, Class 4 CA	CPp,CPp,CPp
ABAecom (sub., Am. Bankers Assn.) Root CA	CPp,CPp,CPp
Digital Signature Trust Co. Global CA 1	CPp,CPp,CPp
Digital Signature Trust Co. Global CA 3	CPp,CPp,CPp
Digital Signature Trust Co. Global CA 2	CPp,CPp,CPp
Digital Signature Trust Co. Global CA 4	CPp,CPp,CPp
Deutsche Telekom AG Root CA	CPp,CPp,CPp
Verisign Class 1 Public Primary Certification Authority	CPp,CPp,CPp
Verisign Class 2 Public Primary Certification Authority	CPp,CPp,CPp
Verisign Class 3 Public Primary Certification Authority	CPp,CPp,CPp

Table 7-3 Public Certificate Authorities

Verisign Class 1 Public Primary Certification Authority - G2	CPp,CPp,CPp
Verisign Class 2 Public Primary Certification Authority - G2	CPp,CPp,CPp
Verisign Class 3 Public Primary Certification Authority - G2	CPp,CPp,CPp
Verisign Class 4 Public Primary Certification Authority - G2	CPp,CPp,CPp
GlobalSign Root CA	CPp,CPp,CPp
GlobalSign Partners CA	CPp,CPp,CPp
GlobalSign Primary Class 1 CA	CPp,CPp,CPp
GlobalSign Primary Class 2 CA	CPp,CPp,CPp
GlobalSign Primary Class 3 CA	CPp,CPp,CPp
ValiCert Class 1 VA	CPp,CPp,CPp
ValiCert Class 2 VA	CPp,CPp,CPp
ValiCert Class 3 VA	CPp,CPp,CPp
Thawte Universal CA Root	CPp,CPp,CPp
Verisign Class 1 Public Primary Certification Authority - G3	CPp,CPp,CPp
Verisign Class 2 Public Primary Certification Authority - G3	CPp,CPp,CPp
Verisign Class 3 Public Primary Certification Authority - G3	CPp,CPp,CPp
Verisign Class 4 Public Primary Certification Authority - G3	CPp,CPp,CPp
Entrust.net Secure Server CA	CPp,CPp,CPp
Entrust.net Secure Personal CA	CPp,CPp,CPp
Entrust.net Premium 2048 Secure Server CA	CPp,CPp,CPp
ValiCert OCSP Responder	CPp,CPp,CPp
Baltimore CyberTrust Code Signing Root	CPp,CPp,CPp
Baltimore CyberTrust Root	CPp,CPp,CPp
Baltimore CyberTrust Mobile Commerce Root	CPp,CPp,CPp
Equifax Secure Global eBusiness CA	CPp,CPp,CPp

Table 7-3 Public Certificate Authorities

Equifax Secure eBusiness CA 1	CPp,CPp,CPp
Equifax Secure eBusiness CA 2	CPp,CPp,CPp
Visa International Global Root 1	CPp,CPp,CPp
Visa International Global Root 2	CPp,CPp,CPp
Visa International Global Root 3	CPp,CPp,CPp
Visa International Global Root 4	CPp,CPp,CPp
Visa International Global Root 5	CPp,CPp,CPp
beTRUSTed Root CA	CPp,CPp,CPp
Xcert Root CA	CPp,CPp,CPp
Xcert Root CA 1024	CPp,CPp,CPp
Xcert Root CA v1	CPp,CPp,CPp
Xcert Root CA v1 1024	CPp,CPp,CPp
Xcert EZ	CPp,CPp,CPp
CertEngine CA	CPp,CPp,CPp
BankEngine CA	CPp,CPp,CPp
FortEngine CA	CPp,CPp,CPp
MailEngine CA	CPp,CPp,CPp
TraderEngine CA	CPp,CPp,CPp
USPS Root	CPp,CPp,CPp
USPS Production 1	CPp,CPp,CPp
AddTrust Non-Validated Services Root	CPp,CPp,CPp
AddTrust External Root	CPp,CPp,CPp
AddTrust Public Services Root	CPp,CPp,CPp
AddTrust Qualified Certificates Root	CPp,CPp,CPp
Verisign Class 1 Public Primary OCSP Responder	CPp,CPp,CPp

Table 7-3 Public Certificate Authorities

Verisign Class 2 Public Primary OCSP Responder	CPp,CPp,CPp
Verisign Class 3 Public Primary OCSP Responder	CPp,CPp,CPp
Verisign Secure Server OCSP Responder	CPp,CPp,CPp
Verisign Time Stamping Authority CA	CPp,CPp,CPp
Thawte Time Stamping CA	CPp,CPp,CPp
E-Certify CA	CPp,CPp,CPp
E-Certify RA	CPp,CPp,CPp
Entrust.net Global Secure Server CA	CPp,CPp,CPp
Entrust.net Global Secure Personal CA	CPp,CPp,CPp

The certadmin Script

You can use the `certadmin` script to do the following certificate administration tasks:

- Generating Self-Signed Certificates
- Generating a Certificate Signing Request (CSR)
- Adding a Root CA Certificate
- Installing a Certificate from a CA
- Deleting a Certificate
- Modifying the Trust Attributes of a Certificate
- Listing Root CA Certificates
- Listing All Certificates
- Printing a Certificate

Generating Self-Signed Certificates

You need to generate certificates for SSL communication between each server and Gateway.

➤ To Generate a Self-Signed Certificate After Installation

1. As root, run the `certadmin` script on the Gateway machine for which you want to generate a certificate:

   portal-server-install-root`/SUNWps/bin/certadmin -n` *gateway-profile-name*

   The certificate administration menu is displayed.

```
1) Generate Self-Signed Certificate

2) Generate Certificate Signing Request (CSR)

3) Add Root CA Certificate

4) Install Certificate From Certificate Authority (CA)

5) Delete Certificate

6) Modify Trust Attributes of Certificate (e.g., for PDC)

7) List Root CA Certificates

8) List All Certificates

9) Print Certificate Content

10) Quit

choice: [10] 1
```

2. Choose option **1** on the certificate administration menu.

   The certificate administration script asks you if you want to keep the existing database files.

3. Enter organization-specific information, token name, and the certificate name.

NOTE For a wild card certificate, specify a * in the fully-qualified DNS name of the host. For example, if the fully-qualified DNS name of the host is `abc.sesta.com`, specify it as `*.sesta.com`. The certificate that is generated is now valid for all host names in the `sesta.com` domain.

```
What is the fully-qualified DNS name of this host? [host_name.domain_name]

What is the name of your organization (ex: Company)? []

What is the name of your organizational unit (ex: division)? []

What is the name of your City or Locality? []

What is the name (no abbreviation please) of your State or Province? []

What is the two-letter country code for this unit? []

Token name is needed only if you are not using the default internal
(software) cryptographic module, for example, if you want to use a crypto
card (Token names could be listed using: modutil -dbdir
/etc/opt/SUNWps/cert/gateway-profile-name -list); Otherwise, just hit Return
below.

Please enter the token name. []

Enter the name you like for this certificate?

Enter the validity period for the certificate (months) [6]
A self-signed certificate is generated and the prompt returns.
```

The token name (default being empty) and certificate name are stored in the `.nickname` file under `/etc/opt/SUNWps/cert/`*gateway-profile-name*.

4. Restart the Gateway for the certificate to take effect:

gateway-install-root`/SUNWps/bin/gateway -n` *new gateway-profile-name* `start`

Generating a Certificate Signing Request (CSR)

Before you can order a certificate from a CA, you need to generate a certificate signing request which will contain the information that is required by the CA.

➤ To Generate a CSR

1. As root, run the `certadmin` script:

   portal-server-install-root`/SUNWps/bin/certadmin -n` *gateway-profile-name*

   The certificate administration menu is displayed.

```
1) Generate Self-Signed Certificate

2) Generate Certificate Signing Request (CSR)

3) Add Root CA Certificate

4) Install Certificate From Certificate Authority (CA)

5) Delete Certificate

6) Modify Trust Attributes of Certificate (e.g., for PDC)

7) List Root CA Certificates

8) List All Certificates

9) Print Certificate Content

10) Quit

choice: [10] 2
```

2. Choose option **2** on the certificate administration menu.

   The script prompts you for organization-specific information, token name, and web master’s email and phone number.

   Ensure that you specify the fully-qualified DNS name of the host.

```
What is the fully-qualified DNS name of this host? [snape.sesta.com]

What is the name of your organization (ex: Company)? []

What is the name of your organizational unit (ex: division)? []

What is the name of your City or Locality? []

What is the name (no abbreviation please) of your State or Province? []

What is the two-letter country code for this unit? []

Token name is needed only if you are not using the default internal
(software) cryptographic module, for example, if you want to use a crypto
card (Token names could be listed using: modutil -dbdir /etc/opt/SUNWps/cert
-list); Otherwise, just hit Return below.

Please enter the token name []

Now input some contact information for the webmaster of the machine that the
certificate is to be generated for.

What is the email address of the admin/webmaster for this server [] ?

What is the phone number of the admin/webmaster for this server [] ?
```

3. Type all the required information.

NOTE Do not leave the web master’s email and phone number blank. The information is necessary for obtaining a valid CSR.

A CSR is generated and stored in the file *portal-server-install-root*/`SUNWps/bin/csr.hostname.datetimestamp`. The CSR is also printed on the screen. You can directly copy and paste the CSR when you order a certificate from a CA.

Adding a Root CA Certificate

If a client site presents a certificate signed by a CA that is unknown to the Gateway certificate database, the SSL handshake will fail.

To prevent this, you need to add a root CA certificate to the certificate database. This ensures that the CA becomes known to the Gateway.

Browse to the CA's website and obtain the root certificate for that CA. When you use the `certadmin` script, specify the filename and path of the root CA certificate.

➤ To Add a Root CA Certificate

1. As root, run the `certadmin` script.

   portal-server-install-root`/SUNWps/bin/certadmin -n` *gateway-profile-name*

   The certificate administration menu is displayed.

```
1) Generate Self-Signed Certificate

2) Generate Certificate Signing Request (CSR)

3) Add Root CA Certificate

4) Install Certificate From Certificate Authority (CA)

5) Delete Certificate

6) Modify Trust Attributes of Certificate (e.g., for PDC)

7) List Root CA Certificates

8) List All Certificates

9) Print Certificate Content

10) Quit

choice: [10] 3
```

2. Choose option **3** on the certificate administration menu.
3. Enter the name of the file that contains the root certificate and enter the name of the certificate.

   The root CA certificate is added to the certificate database.

Installing SSL Certificates From the Certificate Authority

During the installation of the Gateway, a self-signed certificate is created and installed by default. At any point after installation, you can install SSL certificates signed by vendors who provide official certificate authority (CA) services, or by your corporate CA.

The three steps involved in this task are:

- Generating a Certificate Signing Request (CSR)
- Ordering a Certificate from a CA
- Installing a Certificate from a CA

Ordering a Certificate from a CA

After generating a certificate signing request (CSR), you need to order the certificate from the CA using a CSR.

➤ **To Order a Certificate From a CA**

1. Go to the Certificate Authority’s web site and order your certificate.
2. Provide the CSR as requested by the CA. Provide other information if requested by the CA.

   You will receive your certificate from the CA. Save it in a file. Include the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines with the certificate in the file.

   The following example omits the actual certificate data.

```
-----BEGIN CERTIFICATE-----

The certificate contents...

----END CERTIFICATE-----
```

Installing a Certificate from a CA

Using the `certadmin` script, install the certificate obtained from the CA in your local database files in `/etc/opt/SUNWps/cert/`*gateway-profile-name*.

➤ To Install a Certificate From a CA

1. As root, run the `certadmin` script.

   ```
   portal-server-install-root/SUNWps/bin/certadmin -n gateway-profile-name
   ```

   The certificate administration menu is displayed.

```
1) Generate Self-Signed Certificate

2) Generate Certificate Signing Request (CSR)

3) Add Root CA Certificate

4) Install Certificate From Certificate Authority (CA)

5) Delete Certificate

6) Modify Trust Attributes of Certificate (e.g., for PDC)

7) List Root CA Certificates

8) List All Certificates
```

```
9) Print Certificate Content

10)Quit

choice: [10] 4
```

2. Choose option **4** on the certificate administration menu.

   The script asks you to enter the certificate file name, certificate name, and the token name.

```
What is the name (including path) of file that contains the certificate?
Please enter the token name you used when creating CSR for this certificate.
[]
```

3. Supply all the required information.

   The certificate is installed in `/etc/opt/SUNWps/cert/`*gateway-profile-name*, and the screen prompt returns.

4. Restart the Gateway for the certificate to take effect:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

Deleting a Certificate

You can delete a certificate by using the certificate administration script.

➤ To Delete a Certificate

1. As root, run the `certadmin` script.

```
portal-server-install-root/SUNWps/bin/certadmin -n gateway-profile-name
```

where *gateway-profile-name* is the name of the Gateway instance.

The certificate administration menu is displayed.

```
1) Generate Self-Signed Certificate

2) Generate Certificate Signing Request (CSR)

3) Add Root CA Certificate

4) Install Certificate From Certificate Authority (CA)

5) Delete Certificate

6) Modify Trust Attributes of Certificate (e.g., for PDC)

7) List Root CA Certificates

8) List All Certificates

9) Print Certificate Content

10)Quit

choice: [10] 5
```

2. Choose option **5** on the certificate administration menu.
3. Enter the name of the certificate to be deleted.

Modifying the Trust Attributes of a Certificate

One case in which the trust attributes of a certificate needs to be modified is if client authentication is used with the Gateway. An example of client authentication is PDC (Personal Digital Certificate). The CA that issues the PDCs must be trusted by the Gateway, and the CA certificate must be marked "T" for SSL.

If the Gateway is set up to communicate with an HTTPS site, the CA of the HTTPS site server certificate must be trusted by the Gateway, and the CA certificate must be marked "C" for SSL.

➤ To Modify the Trust Attributes for a Certificate

1. As root, run the `certadmin` script.

```
gateway-install-root/SUNWps/bin/certadmin -n gateway-profile-name
```

where *gateway-profile-name* is the name of the Gateway instance.

The certificate administration menu is displayed.

```
1) Generate Self-Signed Certificate

2) Generate Certificate Signing Request (CSR)

3) Add Root CA Certificate

4) Install Certificate From Certificate Authority (CA)

5) Delete Certificate

6) Modify Trust Attributes of Certificate (e.g., for PDC)

7) List Root CA Certificates

8) List All Certificates
```

```
9) Print Certificate Content

10)Quit

choice: [10] 6
```

2. Choose option **6** on the certificate administration menu.

3. Enter the name of the certificate. For example, Thawte Personal Freemail C.

```
Please enter the name of the certificate?
Thawte Personal Freemail CA
```

4. Enter the trust attribute for the certificate.

```
Please enter the trust attribute you want the certificate to have [CT,CT,CT]
```

The certificate trust attribute will be changed.

Listing Root CA Certificates

You can view all root CA certificates by using the certificate administration script.

➤ To View the List of Root CAs

1. As root, run the `certadmin` script.

```
portal-server-install-root/SUNWps/bin/certadmin -n gateway-profile-name
```

where *gateway-profile-name* is the name of the Gateway instance.

The certificate administration menu is displayed.

```
1) Generate Self-Signed Certificate

2) Generate Certificate Signing Request (CSR)

3) Add Root CA Certificate

4) Install Certificate From Certificate Authority (CA)

5) Delete Certificate

6) Modify Trust Attributes of Certificate (e.g., for PDC)

7) List Root CA Certificates

8) List All Certificates

9) Print Certificate Content

10)Quit

choice: [10] 7
```

2. Choose option **7** on the certificate administration menu.

   All root CA certificates are displayed.

Listing All Certificates

You can view all certificates and their corresponding trust attributes by using the certificate administration script.

➤ To List All the Certificates

1. As root, run the `certadmin` script.

```
portal-server-install-root/SUNWps/bin/certadmin -n gateway-profile-name
```

where *gateway-profile-name* is the name of the Gateway instance.

The certificate administration menu is displayed.

```
1) Generate Self-Signed Certificate

2) Generate Certificate Signing Request (CSR)

3) Add Root CA Certificate

4) Install Certificate From Certificate Authority (CA)

5) Delete Certificate

6) Modify Trust Attributes of Certificate (e.g., for PDC)

7) List Root CA Certificates

8) List All Certificates

9) Print Certificate Content

10)Quit

choice: [10] 8
```

2. Choose option **8** on the certificate administration menu.

   All CA certificates are displayed.

Printing a Certificate

You can print a certificate by using the certificate administration script.

➤ To Print a Certificates

1. As root, run the `certadmin` script.

```
portal-server-install-root/SUNWps/bin/certadmin -n gateway-profile-name
```

where *gateway-profile-name* is the name of the Gateway instance.

The certificate administration menu is displayed.

```
1) Generate Self-Signed Certificate

2) Generate Certificate Signing Request (CSR)

3) Add Root CA Certificate

4) Install Certificate From Certificate Authority (CA)

5) Delete Certificate

6) Modify Trust Attributes of Certificate (e.g., for PDC)

7) List Root CA Certificates

8) List All Certificates
```

```
9) Print Certificate Content

10)Quit

choice: [10] 9
```

2. Choose option **9** on the certificate administration menu.
3. Enter the name of the certificate.

Chapter 8

Configuring URL Access Control

This chapter describes how to allow or deny access to the end-user from the Sun Java™ System Identity Server administration console.

NOTE Click Documentation at the top right corner of the Identity Server administration console, and click SRA Help for a quick reference on all the Sun Java System Portal Server Secure Remote Access (SRA) attributes.

➤ To Configure URL Access Control

1. Log in to the Identity Server administration console as administrator.

2. Select the Service Configuration tab from the administration console.

3. Click the arrow next to Access List under SRA Configuration.

   The Access List page displays.

From here you can perform the following tasks:

- Set up a Denied URLs List
- Set up a Allowed URLs List
- Manage Single Sign-On

NOTE When you install SRA, the Access List service is not available to all users by default. This service is enabled only to the `amadmin` user that is created by default during installation. Other users will not be able to access the desktop through the Gateway without this service. Log in as `amadmin`, and assign this service to all the users.

Set up a Denied URLs List

You can specify the list of URLs that end-users cannot access through the Gateway using this field.

The Gateway checks the Denied URLs list before checking the Allowed URLs list.

➤ To Set up the Denied URL List

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Access List under SRA Configuration.

   The Access List page displays.
4. Specify the URL for which you want to deny access through the Gateway in the Denied URL field. The format for entering the URL is:

   `http://abc.siroe.com`
5. Click Add.

   The URL is added to the Denied URL List.

   You can also use regular expressions such as `http://*.siroe.com`. In this case, users are denied access to all hosts in the `siroe.com` domain.
6. Click Save to record the changes.

Set up a Allowed URLs List

You can specify all the URLs that can be accessed by the end-user through the Gateway. By default, this list has a wild card entry (*), which means that all URLs can be accessed. If you want to allow access to all URLs, and restrict access only to specific URLs, add the restricted URLs to the Denied URL list. In the same way, if you want to allow access only to specific URLs, leave the Denied URLs field blank, and specify the required URLs in the Allowed URLs field.

The Gateway checks the Denied URLs before checking the Allowed URLs.

➤ To Set up the Allowed URLs List

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.

3. Click the arrow next to Access List under SRA Configuration.

   The Access List page displays.

4. Specify the URL for which you want to allow access through the Gateway in the Allowed URLs field. The format for entering the URL is:

   `http://abc.siroe.com`

5. Click Add.

   The URL is added to the Allow URLs.

NOTE The Allowed URLs field has a * by default which means that all URLs can be accessed through the Gateway.

6. Click Save to record the changes.

Manage Single Sign-On

The Access List service in SRA software allows you to control the single sign-on feature for various hosts. But for the single sign-on feature to be available, the Enable HTTP Basic Authentication option in the Gateway service must be enabled. See “Enable HTTP and HTTPS Connections” on page 237.

With the Access List service, you can disable single sign-on for certain hosts. This means that an end user needs to authenticate each time to connect to the hosts that require HTTP basic authentication, unless you enable single sign-on per session.

If you have disabled single sign-on for a certain host, the user can reconnect to that host within a single Portal Server session. For example, assume that you have disabled single sign-on to `abc.sesta.com`. The first time the user connects to this site, authentication is required. The user may browse other pages and return to this page later, and if the page is in the same Portal Server session, authentication is not required.

A user can also configure these attributes using the limited administration console.

➤ To Disable Single Sign On for Hosts

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.

3. Click the arrow next to Access List under SRA Configuration.

   The Access List page displays.

4. Specify the hosts for which you want to disable SSO in the SSO Disabled Hosts field.

   Specify the host name in the format `abc.siroe.com`.

5. Click Add.

   The hostname is added to the list.

6. Click Save to record the changes.

➤ To Enable Single Sign On per Session

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Access List under SRA Configuration.

   The Access List page displays.

4. Select the Enable Single Sign On per Session checkbox to enable a single-sign on session.
5. Click Save to record the changes.

➤ To Specify Authentication Levels

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Access List under SRA Configuration.

   The Access List page displays.

4. Scroll to the Allowed Authentication Levels field.
5. Enter the allowed authentications. Use an asterisk to allow all levels.
6. Click Save to record the changes.

Chapter 9

Configuring the Gateway

This chapter describes how to configure the Gateway attributes from the Sun Java™ System Identity Server administration console.

NOTE Click Help at the top right corner of the Identity Server administration console, and click SRA Help for a quick reference on all the Sun Java System Portal Server Secure Remote Access (SRA) attributes.

To set up a gateway, see "Creating a Gateway Profile" on page 38.

After you have created the gateway profile, you need to configure the Gateway attributes.

➤ To Configure the Gateway Attributes

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab from the administration console.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.
4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.

   From here, click the appropriate tab:

   - The Core Tab
   - The Proxies Tab
   - The Security Tab

- The Rewriter Tab
- The Logging Tab

The tabs and the attributes that can be configured under each tab are listed below.

The Core Tab

Using the Core tab, in the Gateway service, you can perform the following tasks:

- Enable HTTP and HTTPS Connections
- Enable and Create a List of Rewriter Proxies
- Enable Netlet
- Enable and Create a List of Netlet Proxies
- Enable Proxylet
- Enable Cookie Management
- Enable HTTP Basic Authentication
- Enable Persistent HTTP Connections
- Specify the Maximum Number of Requests per Persistent Connection
- Specify Timeout for Persistent Socket Connections
- Specify Grace Timeout to Account for Turnaround Time
- Create Forward User Session Cookie to the URL List
- Specify the Maximum Connection Queue Length
- Specify the Gateway Timeout
- Specify the Maximum Thread Pool Size
- Specify the Cached Socket Timeout
- Create List of Portal Servers
- Specify Server Retry Interval
- Enable Storage of External Server Cookies
- Obtaining of a Session from a URL
- Enable Marking Cookies as Secure

Enable HTTP and HTTPS Connections

The Gateway runs in HTTPS mode after installation if you have chosen to run the Gateway in the HTTPS mode during installation. In the HTTPS mode, the Gateway accepts SSL connections from browsers and rejects non-SSL connections.

However, you can also configure the Gateway to run in HTTP mode. This speeds Gateway performance as the overhead involved in managing SSL sessions and encrypting and decrypting the SSL traffic are not involved.

➤ To Configure the Gateway to Run in HTTP or HTTPS Mode

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab from the administration console.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.
4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Do the following under the Core tab.
   - Select the Enable HTTP Connections, Enable HTTPS Connections, or both checkboxes as required.
   - Specify the required HTTPS port in the HTTPS Port field.
   - Specify the required HTTP port in the HTTP Port field.
6. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
7. Restart the Gateway from a terminal window:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Enable and Create a List of Rewriter Proxies

The Rewriter proxy enables secure HTTP traffic between the Gateway and intranet computers. If you do not specify a Rewriter proxy, the Gateway component makes a direct connection to intranet computers when a user tries to access one of those intranet computers.

The Rewriter proxy does not run automatically after installation. You need to enable the Rewriter proxy as described below.

➤ To Enable Rewriter Proxies and Create a List of Rewriter Proxies

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.
4. Click Edit... next to the gateway profile for which you want to set the attribute.

NOTE	Ensure that the Rewriter proxy and the Gateway use the same gateway profile.

   The Edit Gateway Profile page displays.

5. Click the Core tab.
6. Select the Enable the Rewriter Proxies checkbox to enable the Rewriter proxy.
7. Type the desired host and port in the Rewriter Proxies edit box, in the format `hostname:port`.
8. Click Add.
9. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
10. Run *portal-server-install-root*`/SUNWps/bin/certadmin` on the server to create a certificate for the Rewriter proxy.

    You need to do this step only if you have not chosen to create a certificate while installing the Rewriter proxy.
11. Log in as root to the machine where the Rewriter proxy is installed and start the Rewriter proxy:

    rewriter-proxy-install-root`/SUNWps/bin/rwproxyd -n` *gateway-profile-name* `start`
12. Log in as root to the machine where the Gateway is installed and restart the Gateway:

    gateway-install-root/`SUNWps/bin/gateway -n` *gateway-profile-name* `start`

Enable Netlet

Netlet enables users to securely run common TCP/IP services over insecure networks such as the Internet. You can run TCP/IP applications (such as Telnet and SMTP), HTTP applications, and any fixed port applications.

If Netlet is enabled, the Gateway needs to determine whether the incoming traffic is Netlet traffic or Portal Server traffic. Disabling Netlet reduces this overhead since the Gateway assumes that all incoming traffic is either HTTP or HTTPS traffic. Disable Netlet only if you are sure you do not want to use any application with Portal Server.

➤ To Enable Netlet

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.
4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Click the Core tab.
6. Select the Enable Netlet checkbox. This checkbox is selected by default. Removing the selection disables Netlet.
7. Select the Enable the Netlet Proxy checkbox to enable the Netlet proxy.
8. Type the desired host and port in the Netlet Proxy List edit box, in the format `hostname:port`.
9. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
10. Restart the Gateway from a terminal window:

    ```
    gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
    ```

Enable and Create a List of Netlet Proxies

The Netlet proxy enhances the security of Netlet traffic between the Gateway and the intranet by extending the secure tunnel from the client, through the Gateway to the Netlet proxy that resides in the intranet.

If the Netlet proxy is enabled, the Netlet packets are decrypted by the Netlet proxy and then sent to the destination server. This reduces the number of ports required to be opened in the firewall.

➤ To Enable Netlet Proxies and Create a List of Netlet Proxies

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the right arrow next to Gateway under SRA Configuration in the left frame.

   The Gateway page displays on the right pane.
4. Click Edit next to the required profile.

   Edit Gateway Profile page displays in the right pane.
5. Select the Enable Netlet Proxy checkbox to enable the Netlet proxy.
6. Type the desired Netlet proxy host and port in the Netlet Proxy Hosts field, in the format `host hostname:port`.

TIP To determine if the port desired is available and unused, from the command line, enter:

```
netstat -a | grep port-number | wc -l
```

port-number is the required port.

7. Click Add.
8. Click Save at the top or bottom of the page to save the changes.
9. Restart the Gateway from a terminal window:

```
gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
```

Enable Proxylet

➤ To Enable Proxylet

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.

3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Click the Core tab.
6. Click the arrow next to Gateway under SRA Configuration.
7. Select the Enable Proxylet checkbox.
8. Click the Proxies tab.Scroll down to the Proxies for Domains and Subdomains field and enter the domains for URLs that are to be directed to the Gateway.
9. Click Save.

Enable Cookie Management

Many web sites use cookies to track and manage user sessions. When the Gateway routes requests to web sites that set cookies in the HTTP header, the Gateway either discards or passes-through those cookies in the following manner:

- Cookies are not rewritten if Enable Cookie Management attribute is not selected in the Gateway service. So, the cookies from the browser might not reach the intranet hosts and vice-versa.
- Gateway rewrites cookies if the Enable Cookie Management attribute is selected. Gateway ensures that the cookies from the browser reach the intended intranet hosts and vice-versa.

This setting does not apply to the cookies used by Portal Server to track Portal Server user sessions. It is controlled by the configuration of the User Session to which User Session Cookie is Forwarded URL option. See “Create Forward User Session Cookie to the URL List” on page 246.

This setting applies to all web sites that the user is permitted to access (that is, you cannot choose to discard cookies from some sites and retain cookies from others).

NOTE Do not remove URLs from the Cookie Domain list, even in a Gateway without cookies. See the *Identity Server Administration Guide* for information on the Cookie Domain list.

➤ To Enable Cookie Management

1. Log in to the Identity Server administration console as administrator.

1. Select the Service Configuration tab.
2. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.
3. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
4. Click the Core tab.
5. Select the Enable Cookie Management checkbox to enable cookie management.
6. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
7. Restart the Gateway from a terminal window:

```
gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
```

Enable HTTP Basic Authentication

HTTP basic authentication can be set in the Gateway service.

Web sites may be protected with HTTP Basic Authentication, requiring visitors to enter a username and password before viewing the site (the HTTP response code is 401 and WWW-authenticate: BASIC). Portal Server can save the username and password so that users need not re-enter their credentials when they revisit BASIC-protected web sites. These credentials are stored in the user profile on the directory server.

This setting does not determine whether or not a user may visit BASIC-protected sites, but only whether the credentials the user enters will be saved in the user's profile.

This setting applies to all web sites that the user is permitted to access (that is, HTTP basic authentication caching cannot be enabled for some sites and disabled for others).

NOTE Browsing to URLs served by Microsoft's Internet Information Server (IIS) protected by Windows NT challenge/response (HTTP response code 401, WWW-Authenticate: NTLM) instead of BASIC authentication is not supported.

You can also enable single sign-on using the Access List service in the administration console. See "Manage Single Sign-On" on page 233 for more information on enabling single sign-on.

➤ To Enable HTTP Basic Authentication

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.
4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Click the Core tab.
6. Select the Enable HTTP Basic Authentication checkbox to enable HTTP basic authentication.
7. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
8. Restart the Gateway from a terminal window:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

Enable Persistent HTTP Connections

You can enable HTTP persistent connections at the Gateway to prevent sockets being opened for every object (such as images and style sheets) in the web pages.

➤ To Enable Persistent HTTP Connections

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.
4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Click the Core tab.

6. Select the Enable Persistent HTTP Connections checkbox to enable HTTP connections.
7. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
8. Restart the Gateway from a terminal window:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

Specify the Maximum Number of Requests per Persistent Connection

➤ To Specify the Maximum Number of Requests per Persistent Connection

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.
4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Click the Core tab.
6. Scroll to the Maximum Number of Requests per Persistent Connection field and type the required number of requests.
7. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
8. Restart the Gateway from a terminal window:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

Specify Timeout for Persistent Socket Connections

➤ To Specify the Timeout for a Persistent Socket Connection

1. Log in to the Identity Server administration console as administrator.

2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.
4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Click the Core tab.
6. Scroll to Socket Timeout for Persistent Connections field and type the required timeout in seconds.
7. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
8. Restart the Gateway from a terminal window:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Specify Grace Timeout to Account for Turnaround Time

Grace timeout turnaround time is the sum of:

- time taken for the request to reach the gateway after the browser has sent it.
- time between gateway sending the response and the browser actually receiving it.

This is dependent on factors such as network conditions and the client’s connection speed.

➤ To Specify Timeout to Account for Turnaround Time

This is the round trip time for the network traffic between the client (browser) and the Gateway.

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.

4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.

5. Click the Core tab.

6. Scroll to the Grace Timeout to Account for Turnaround Time field and type the required grace timeout in seconds.

7. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.

8. Restart the Gateway from a terminal window:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Create Forward User Session Cookie to the URL List

Portal server utilizes a cookie to track user sessions. This cookie is forwarded to the server when the Gateway makes HTTP requests to the server (for example, when the desktop servlet is called to generate the user's desktop page). Applications on the server use the cookie to validate and identify the user.

The Portal Server's cookie is not forwarded to HTTP requests made to machines other than the server, unless URLs on those machines are specified in the User Session to which User Session Cookie is Forwarded list. Adding URLs to this list therefore enables servlets and CGIs to receive the Portal Server's cookie and use the APIs to identify the user.

URLs are matched using an implicit trailing wildcard. For example, the default entry in the list:

```
http://server:8080
```

causes the cookie to be forwarded to all URLs starting with `http://server:8080`.

Adding:

```
http://newmachine.eng.siroe.com/subdir
```

causes the cookie to be forwarded to all URLs starting with that exact string.

For this example, the cookie is not forwarded to any URLs starting with "`http://newmachine.eng/subdir`", since this string does not start with the exact string in the forward list. To have cookies forwarded to URLs starting with this variation of the machine's name, an additional entry has to be added to the forward list.

Similarly, the cookie is not forwarded to URLs starting with "`https://newmachine.eng.siroe.com/subdir`" unless an appropriate entry is added to the list.

➤ To Add a Forward Cookie URL

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.
4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Click the Core tab.
6. Scroll to the User Session to which User Session Cookie is Forwarded edit box and type the required URL.
7. Click Add to add this entry to the User Session to which User Session Cookie is Forwarded list.
8. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
9. Restart the Gateway from a terminal window:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

Specify the Maximum Connection Queue Length

You can specify the maximum concurrent connections that the Gateway needs to accept. Any connection attempts beyond this number are not accepted by the Gateway.

➤ To Specify the Maximum Connection Queue Length

1. Log in to the Identity Server administration console as administrator.

2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.
4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Click the Core tab.
6. Scroll to the Maximum Connection Queue Length field and specify the required number of connections.
7. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
8. Restart the Gateway from a terminal window:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Specify the Gateway Timeout

You can specify the time interval in milliseconds after which the Gateway times out its connection with the browser.

➤ To Specify the Gateway Timeout

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.
4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Click the Core tab.
6. Scroll to the Gateway Timeout (milliseconds) field and specify the interval required in milliseconds.
7. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
8. Restart the Gateway from a terminal window:

```
gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
```

Specify the Maximum Thread Pool Size

You can specify the maximum number of threads that can be pre-created in the Gateway thread pool.

➤ To Specify the Maximum Thread Pool Size

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.
4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Click the Core tab.
6. Scroll to the Maximum Thread Pool Size field and specify the required number of threads.
7. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
8. Restart the Gateway from a terminal window:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Specify the Cached Socket Timeout

You can specify the time interval in milliseconds after which the Gateway times out its connection with the Portal Server.

➤ **To Specify the Cached Socket Timeout**

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.

4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.

5. Click the Core tab.

6. Scroll to the Cached Socket Timeout field and specify the interval required in milliseconds.

7. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.

8. Restart the Gateway from a terminal window:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Create List of Portal Servers

You can configure multiple Portal Servers for the Gateway to service requests. While installing the Gateway, you would have specified the Portal Server that the Gateway needs to work with. This Portal Server is listed in the Portal Servers field by default. You can add more Portal Servers to the list in the format `http://portal server name:port number`. The Gateway tries to contact each of the Portal Servers listed in a round robin manner to service the requests.

➤ To Specify Portal Servers

1. Log in to the Identity Server administration console as administrator.

2. Select the Service Configuration tab.

3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.

4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.

5. Click the Core tab.

6. Scroll to the Portal Server field and specify the Portal Servers.

   Specify the Portal Server in the format `http://portal server name:port number` in the edit field and click Add.

7. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.

8. Restart the Gateway from a terminal window:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

Specify Server Retry Interval

This attribute specifies the time interval between requests to try to start the Portal Server, Rewriter proxy or Netlet proxy if it becomes unavailable (such as a crash or it was brought down).

➤ To Specify Portal Server Retry Interval

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.
4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Click the Core tab.
6. Scroll to the Portal Server Retry Interval field and specify the number of seconds.
7. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
8. Restart the Gateway from a terminal window:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

Enable Storage of External Server Cookies

When the Store External Server Cookies option is enabled, the Gateway stores and manages cookies for any third party application or server that is accessed through the Gateway. Even if the application or server cannot service cookieless devices or depends on cookies for state management (for legacy reasons), it transparently masks the application or server from knowing that it is servicing a cookieless device. For information on cookieless devices and client detection, refer to the *Identity Server Customization and API Guide.*

➤ To Store External Server Cookies

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.
4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Click the Core tab.
6. Select the Store External Server Cookies checkbox to enable storage of external server cookies.
7. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
8. Restart the Gateway from a terminal window:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Obtaining of a Session from a URL

When the Obtain Session from URL option is selected, session information is encoded as part of the URL, whether cookies are supported or not. This means that the Gateway uses the session information found in the URL for validation rather than using the session cookie that is sent from the client's browser.

➤ To Obtain a Session from a URL

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.
4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Click the Core tab.
6. Select the Obtain Session from URL checkbox to obtain a session from a URL.

7. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.

8. Restart the Gateway from a terminal window:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Enable Marking Cookies as Secure

When a cookie is marked as secure, the browser treats the cookie with additional security. The implementation of security depends on the browser. The Enable Cookie Management attribute must be enabled for this to work.

➤ To Mark Cookies as Secure

1. Log in to the Identity Server administration console as administrator.

2. Select the Service Configuration tab.

3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.

4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.

5. Click the Core tab.

6. Select the Mark Cookies as secure checkbox to mark cookies as secure.

   Ensure that the Enable Cookie Management attribute is enabled.

7. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.

8. Restart the Gateway from a terminal window:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

The Proxies Tab

Using the Proxies tab, in the Gateway service, you can perform the following tasks:

- Enable Usage of Web Proxies
- Create List of URLS for Webproxies

- Create List of URLs for Proxies Not to be Used
- Create List of Proxies for Domains and Subdomains
- Create List of Proxy Passwords
- Enable Automatic Proxy Configuration Support
- Specify Automatic Proxy Configuration File Location
- Enable Netlet Tunneling via Web Proxy

Enable Usage of Web Proxies

➤ **To Enable Usage of Web Proxies**

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.
4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Click the Proxies tab.
6. Select the Use Proxy checkbox to enable the usage of web proxies.
7. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
8. Restart the Gateway from a terminal window:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Create List of URLS for Webproxies

You can specify that the Gateway needs to contact certain URLs only through the webproxies listed in the Proxies for Domains and Subdomains list, even if the Use Proxy option is disabled. You need to specify these URLs in the Use Webproxy URLs field. See "Specifying a Proxy to Contact the Identity Server" on page 56 for details on how this value affects the usage of proxies.

➤ To Specify URLs for Webproxies

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.
4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Click the Proxies tab.
6. Type the required URL in the Use Webproxy URLs edit box in the format `http://host name.subdomain.com`. Click Add.

   The URL is added to the Use Webproxy URLs list.
7. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
8. Restart the Gateway from a terminal window:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

Create List of URLs for Proxies Not to be Used

The Gateway tries to connect directly to the URLs listed in the Do Not Use Webproxy URLs list. A webproxy is not used to connect to these URLs.

➤ To Specify URLs Not To Be Used

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.
4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Click the Proxies tab.

6. Type the required URL in the Do Not Use Webproxy URLs edit box and click Add.

   The URL is added to the Do Not Use Webproxy URLs list.

7. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.

8. Restart the Gateway from a terminal window:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Create List of Proxies for Domains and Subdomains

➤ To Specify Proxies for Domains and Subdomains

See "Specifying a Proxy to Contact the Identity Server" on page 56 for details on how the proxy information is applied to various hosts.

1. Log in to the Identity Server administration console as administrator.

2. Select the Service Configuration tab.

3. Click the right arrow next to Gateway under SRA Configuration.

   The Gateway Profile page displays.

4. Click Edit. for the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.

5. Click the Proxies tab.

6. Scroll to the Proxies for Domains and Subdomains edit box and type the required information in the and click Add. The entry is added to the Proxies for Domains and Subdomains list box.

   The format for entering the proxy information is as follows:

   ```
   domainname proxy1:port1|subdomain1 proxy2:port2|subdomain2
   proxy3:port3|* proxy4:port4
   ```

   * indicates that the proxy defined after the * needs to be used for all domains and subdomains other than those specifically mentioned.

   If you do not specify the port for the proxy, port 8080 is used by default.

7. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.

8. Restart the Gateway from a terminal window:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

Create List of Proxy Passwords

You need to specify the user name and password required for the Gateway to authenticate to a specified proxy server, if the proxy server requires authentication to access some or all the sites.

➤ To Specify Proxy Passwords

1. Log in to the Identity Server administration console as administrator.

2. Select the Service Configuration tab.

3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.

4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.

5. Click the Proxies tab.

6. Scroll to the Proxy Password List field and type the information for each proxy server and click Add

   The format for entering the proxy information is as follows:

   ```
   proxyserver|username|password
   ```

   The `proxyserver` corresponds to the proxy server defined in the Proxies for Domains and Subdomains list.

7. Repeat step 6 for all the proxies that require authentication.

8. Click Save at the top or bottom of the page to record the changes.

9. Restart the Gateway from a terminal window:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

Enable Automatic Proxy Configuration Support

If you select the option Enable Automatic Proxy Configuration, the information provided in the Proxies for Domains and Subdomains field is ignored. The Gateway will use only the Proxy Automatic Configuration (PAC) file for intranet configuration. See "Using Automatic Proxy Configuration" on page 62 for information on PAC files.

➤ To Enable Automatic Proxy Configuration Support

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.
4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Click the Proxies tab.
6. Select the Enable Automatic Proxy Configuration Support checkbox to enable PAC support.
7. Click Save at the top or bottom of the page to record the changes.
8. Restart the Gateway from a terminal window:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Specify Automatic Proxy Configuration File Location

➤ To Specify Automatic Proxy Configuration File Location

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.

4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.

5. Click the Proxies tab.
6. Scroll to the Automatic Proxy Configuration File location field and type the name and location of the PAC file.
7. Click Save at the top or bottom of the page to record the changes.
8. Restart the Gateway from a terminal window:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

Enable Netlet Tunneling via Web Proxy

➤ To Enable the Tunnel Netlet via Web Proxy

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.

4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.

5. Click the Proxies tab.
6. Select the Enable Netlet Tunneling via Web Proxy checkbox to enable tunneling.
7. Click Save at the top or bottom of the page to record the changes.
8. Restart the Gateway from a terminal window:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

The Security Tab

Using the Security tab, in the Gateway service, you can perform the following tasks:

- Create List of Non-authenticated URLs

- Create List of Certificate-Enabled Gateway Hosts
- Allow 40-bit Encryption Connections
- Enable SSL Version 2.0
- Enable SSL Cipher Selection
- Enable SSL Version 3.0
- Enable Null Ciphers
- Create List of Trusted SSL Domains
- Configure Personal Digital Certificate (PDC) Authentication
- Enable Marking Cookies as Secure
- Enable HTTP and HTTPS Connections

Create List of Non-authenticated URLs

You can specify that some URLs do not need any authentication. These are normally directories and folders that contain images.

➤ To Specify Non-authenticated URL Paths

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.
4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Scroll to the Non-authenticated URLs field and type the required folder path in the format `folder/subfolder`.

   URLs that are not fully-qualified (for example, /images) are treated as portal URLs.

   To add a non-portal URL, fully qualify the URL.
6. Click Add to add this entry to the Non-authenticated URLs list.
7. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.

8. Restart the Gateway from a terminal window:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

Create List of Certificate-Enabled Gateway Hosts

➤ To Add the Gateway to the Certificate-Enabled Gateway Hosts List

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.

   All the services are displayed in the left pane.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway Profiles page is displayed in the right pane.
4. Click Edit... for the profile where you want to enable certificate based authentication.
5. Click the Security tab.
6. Add the Gateway name to the Certificate-enabled Gateway Hosts.

   Add the Gateway in the format `host1.sesta.com`.
7. Click Add.

Allow 40-bit Encryption Connections

Select this option if you want to allow 40-bit (weak) Secure Sockets Layer (SSL) connections. If you do not select this option, only 128-bit connections are supported.

If you disable this option, the user needs to ensure that the browser is configured to support the required connection type.

NOTE The user needs to do the following in the case of Netscape Navigator 4.7x:

- Select Security Info under Tools in the Communicator menu.
- Click the Navigator link in the left pane.
- Click Configure SSL v2 or Configure SSL v3 under Advanced Security (SSL) Configuration.
- Enable the required ciphers.

➤ To Allow 40-bit Encryption Connections

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.
4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Select the Allow 40-bit Encryption checkbox to enable 40-bit browser connections.
6. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
7. Restart the Gateway from a terminal window:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Enable SSL Version 2.0

You can enable or disable SSL version 2.0. Disabling SSL 2.0 means that browsers that support only the older SSL 2.0 will not be able to authenticate to SRA. This ensures a greater level of security.

➤ To Enable SSL Version 2.0

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.

3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.

4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.

5. Select the Enable SSL Version 2.0 checkbox to enable version 2.0.

   This option is enabled by default.

6. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.

7. Restart the Gateway from a terminal window:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Enable SSL Cipher Selection

SRA supports a number of standard ciphers. You have the option of supporting all the pre-packaged ciphers, or selecting the required ciphers individually. You can select specific SSL ciphers for each Gateway instance. If any of the selected ciphers is present at the client site, the SSL handshake occurs successfully.

➤ To Enable Individual Cipher Selection

1. Log in to the Identity Server administration console as administrator.

2. Select the Service Configuration tab.

3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.

4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.

5. Scroll to the Enable SSL Cipher Selection field and select the option.

   This option allows you to select the required ciphers from the list of SSL2, SSL3 and TLS ciphers.

6. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.

7. Restart the Gateway from a terminal window:

```
gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
```

Enable SSL Version 3.0

You can enable or disable SSL version 3.0. Disabling SSL 3.0 means that browsers that support only the SSL 3.0 will not be able to authenticate to SRA software. This ensures a greater level of security.

➤ To Enable SSL Version 3.0

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.
4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Select the Enable SSL Version 3.0 checkbox to enable version 3.0.
6. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
7. Restart the Gateway from a terminal window:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Enable Null Ciphers

➤ To Enable Null Ciphers

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.
4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Select the Enable Null Ciphers checkbox to enable null ciphers.

6. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
7. Restart the Gateway from a terminal window:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Create List of Trusted SSL Domains

➤ To Create List of Trusted SSL Domains

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.
4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Scroll to the Trusted SSL Domains List, enter the domain names and click Add.
6. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
7. Restart the Gateway from a terminal window:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Configure Personal Digital Certificate (PDC) Authentication

PDCs are issued by a Certification Authority (CA) and signed with the CA's private key. The CA validates the identity of a requesting body before issuing a certificate. Thus the presence of a PDC is a very powerful authentication mechanism.

PDCs contain the owner's public key, the owner's name, an expiration date, the name of the Certification Authority that issued the Digital Certificate, a serial number, and maybe some other information.

Users can use PDCs and encoded devices such as Smart Cards and Java Cards for authentication in the Portal Server. The encoded devices carry an electronic equivalent of a PDC stored on the card. If a user logs in using one of these mechanisms, no Log in screen displays and no authentication screen displays.

The PDC authentication process involves several steps:

1. From a browser, the user types a connection request, say `https://my.sesta.com`.

   The response to this request depends on whether the Gateway to `my.sesta.com` has been configured to accept certificates.

NOTE When a Gateway is configured to accept certificates, it will accept only logins with certificates, not any other kind of login.

   The Gateway checks that the certificate has been issued by a known Certificate Authority, has not expired, and has not been tampered with. If the certificate is valid, the Gateway lets the user proceed to the next step in the authentication process.

2. The Gateway passes the certificate to the PDC authentication module in the server.

➤ To Configure PDCs and Encoded Devices

The following steps are involved in configuring PDCs and encoded devices:

1. Add the following line in the *portal-server-install-root*`/SUNWam/config/AMConfig-`*instance-name*`.properties` file on the Portal Server machine:

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

   (Add anywhere in the file)

2. Import the Required Certificates into the certificate database of the Gateway that you want PDC-enabled.

   See the Chapter 7, “Certificates” for more information.

3. Register the certificate:

   a. Log in to the Identity Server administration console as administrator.

   b. Select the Identity Management tab.

c. Select your Organization.

d. Click Services from the View drop-down menu.

e. Click the arrow next to Core.

f. Select Cert and LDAP in the Organization Authentication Modules list box LDAP.

g. Choose Dynamically Created from the User Profile drop-down menu.

h. Click Save.

4. Create Trusted Remote Host list.

   a. Click the Service Configuration tab.

   b. Click the arrow next to Certificate under Authentication Configuration.

   c. Scroll to the list box named Trusted Remote Host.

   d. Highlight 'none' and click Remove.

   e. Type 'any' in the text box

   f. Click Add.

   g. Click Save.

5. Create the new instance.

   a. Click the Identity Management tab.

   b. Select Services from the View drop-down menu.

   c. Click the arrow next to the Authentication Configuration.

   d. The Service Instance List displays.

   e. Click New.

   f. The New Service Instance page displays.

   g. Enter the service instance name as gatewaypdc.

   h. Note: You must use this name.

   i. Click Submit.

   j. The gatewaypdc Service Instance List displays.

   k. Click gatewaypdc to edit the service.

   l. The gatewaypdc show properties page displays.

m. Click Edit link next to Authentication Configuration.

n. A popup window appears.

o. Click Add.

The Authentication for Configuration *YourOrganization* page displays

p. Click Add.

q. The Add Authentication Module page displays.

r. Choose Cert from the Module Name field and REQUIRED from the Enforcement Criteria field.

s. Click OK.

t. Click OK again and close the popup window.

6. Associate the certificate with the gateway host.

a. Select Service Configuration tab.

b. Click the arrow next to Gateway.

Gateway Profiles are displayed in the right pane.

c. Select your gateway profile.

d. Click on security Tab.

e. Add the Gateway name to the Certificate-enabled Gateway hosts list box.

f. Click Save.

g. Restart the server.

h. Restart the Gateway from a terminal window:

gateway-install-root/SUNWps/bin/gateway -n *gateway-profile-name* start

7. Install the client certificate issued from CA into the browser from where one has to access PDC enabled gateway.

8. Access your gateway profile and organization:

https://*gateway:instance-port/YourOrganization*

You should be logged in without any prompt for Username and Password with the name of the certificate.

The Rewriter Tab

Using the Rewriter tab, in the Gateway service, you can perform the following tasks:

- Enable Rewriting of All URLs
- Create List of URIs to RuleSet Mappings
- Create List of MIME Types to Parse
- Specify the Default Domain and Subdomain
- Create List of URIs Not to Rewrite
- Enable MIME Guessing
- Create List of URI Mappings to Parse
- Enable Masking
- Specify the Masking Seed String
- Create List of URIs Not to Mask
- Make a Gateway Protocol the Same as the Original URI Protocol

Enable Rewriting of All URLs

If you enable the Enable Rewriting of All URIs option in the Gateway service, Rewriter rewrites any URL without checking against the entries in the Proxies for Domains and Subdomains list. Entries in the Proxies for Domains and Subdomains list are ignored.

➤ To Enable the Gateway to Rewrite All URLs

1. Log in to the Sun Java™ System Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway Profile page displays.
4. Click Edit... for the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Click the Rewriter tab, Basic subsection.

6. Select the Enable Rewriting of All URIs checkbox to enable the Gateway to rewrite all URLs.

7. Click Save at the top or bottom of the page to record the change.

8. Restart the Gateway from a terminal window:

```
gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
```

Create List of URIs to RuleSet Mappings

Rulesets are created in the Rewriter service under Portal Server Configuration in the Identity Server administration console. See the *Portal Server Administration Guide* for details.

After the ruleset is created, you associate a domain with the ruleset using the Map URIs to RuleSets field. The following two entries are added by default to the Map URIs to RuleSets field:

- *://*.Sun.COM/portal/*|default_gateway_ruleset

  where sun.com is the install domain of the portal and /portal is the portal install context

- *|generic_ruleset

This means that for all pages from the default domain, the default Gateway ruleset is applied. For all other pages, the generic ruleset is applied. The default Gateway ruleset and the generic ruleset are pre-packaged rulesets.

NOTE For all the content appearing on the desktop, the ruleset for the default domain is used, irrespective of where the content is fetched from.

For example, assume that the desktop is configured to scrape the content from the URL `yahoo.com`. The Portal Server is in `sesta.com`. The ruleset for `sesta.com` is applied to the fetched content.

NOTE The domain for which you specify a ruleset must be listed in the Proxies for Domains and Subdomains list.

➤ To Map a URI to RuleSet

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway Profile page displays.
4. Click the gateway profile for which you want to set the attribute.

   The Gateway - *gateway-profile-name* page displays.
5. Click the Rewriter tab, Basic subsection.
6. Scroll to the Map URIs to RuleSets field.
7. Type the required domain or host name and the ruleset in the Map URIs to RuleSets field and click Add.

   The entry is added to the Map URIs to RuleSets field.

   The format for specifying the domain or host name and the ruleset is as follows:

   `domain name|ruleset name`

   For example:

   `eng.sesta.com|default`

NOTE The order of priority for applying the ruleset is `hostname-subdomain-domain`.

For example, assume that you have the following entries in the Domain-based rulesets list:

`sesta.com|ruleset1`

`eng.sesta.com|ruleset2`

`host1.eng.sesta.com|ruleset3`

`ruleset3` is applied for all pages on `host1`.

`ruleset2` is applied for all pages in the `eng` subdomain, except for pages retrieved from `host1`.

`ruleset1` is applied for all pages in the `sesta.com` domain, except for pages retrieved from the `eng` subdomain, and from `host1`.

---

8. Click Save at the top or bottom of the page to record the change.

9. Restart the Gateway from a terminal window:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Ruleset for Outlook Web Access

SRA software supports MS Exchange 2000 SP3 installation and MS Exchange 2003 of Outlook Web Access (OWA).

➤ **To Configure the OWA RuleSet**

1. Log in to the Identity Server administration console as administrator.

2. Select the Service Configuration tab.

3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway Profile page displays.

4. Click the gateway profile for which you want to set the attribute.

   The Gateway - *gateway-profile-name* page displays.

5. In the Map URIs to RuleSets field, enter the server name where Exchange 2000 is installed followed by the exchange 2000 Service Pack 4 OWA ruleset.

   For example:

   ```
   exchange.domain.com|exchange_2000sp3_owa_ruleset.
   ```

Create List of MIME Types to Parse

Rewriter has four different parsers to parse the web pages based on the content type - HTML, JAVASCRIPT, CSS and XML. Common MIME types are associated with these parsers by default. You can associate new MIME types with these parsers in the Map Parser to MIME Types field of the Gateway service. This extends Rewriter functionality to other MIME types.

Separate multiple entries with a semicolon or a comma (";" or ",".)

For example:

HTML=text/html;text/htm;text/x-component;text/wml; text/vnl/wap.wml

means any content with these MIMEs are sent to the HTML Rewriter and HTML Rules would be applied to rewrite the URLs.

TIP Removing unnecessary parsers from the MIME mappings list can increase the speed of operation. For example, if you are sure that the content from a certain intranet will not have any JavaScript, you can remove the JAVASCRIPT entry from the MIME mappings list.

➤ To Specify MIME Mappings

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway Profile page displays.
4. Click the gateway profile for which you want to set the attribute.

   The Gateway - *gateway-profile-name* page displays.
5. Click the Rewriter tab, Basic subsection.
6. Scroll to the Map Parser to MIME Types field, and add the required MIME type in the edit box. Use a semicolon or comma to separate multiple entries.

   Specify the entry in the format `HTML=text/html;text/htm`
7. Click Add to add the required entry to the list.
8. Click Save at the top or bottom of the page to record the change.
9. Restart the Gateway from a terminal window:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

Specify the Default Domain and Subdomain

The default domain and subdomain are useful when URLs contain only the host names without the domain and subdomain. In this case, the Gateway assumes that the host names are in the default domain and subdomain, and proceeds accordingly.

For example, if the host name in the URL is `host1`, and the default domain and subdomain are specified as `red.sesta.com`, the host name is resolved as `host1.red.sesta.com`.

➤ To Specify the Default Domain and Subdomain

1. Log in to the Identity Server administration console as administrator.
2. Click the Service Configuration tab.
3. Click the right arrow next to Gateway under SRA Configuration.

   The Gateway Profile page displays.
4. Click Edit... for the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Click the Rewriter tab, Basic subsection.
6. Scroll to the Default Domains field and type the required default value in the format `subdomain.domain name`.
7. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
8. Restart the Gateway from a terminal window:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Create List of URIs Not to Rewrite

➤ To Specify the Default Domain and Subdomain

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway Profile page displays.
4. Click the gateway profile for which you want to set the attribute.

   The Gateway - *gateway-profile-name* page displays.
5. Click the Rewriter tab, Advanced subsection.
6. Scroll to the URIs Not to Rewrite field, and add the URI in the edit box.

   Note: Adding #* to this list allows URIs to be rewritten, even when the href rule is part of the ruleset.
7. Click Save at the top or bottom of the page to record the change.

8. Restart the Gateway from a terminal window:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

Enable MIME Guessing

Rewriter depends on the MIME type of the page to choose the parser. Some web servers such as WebLogic and Oracle do not send MIME types. To work around this, you can enable the MIME guessing feature by adding data to the Map Parser to URIs list box.

➤ To Enable MIME Guessing

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway Profile page displays.
4. Click the gateway profile for which you want to set the attribute.

   The Gateway - *gateway-profile-name* page displays.
5. Click the Rewriter tab, Advanced subsection.
6. Select the Enable MIME Guessing checkbox to enable MIME Guessing.
7. Click Save at the top or bottom of the page to record the change.
8. Restart the Gateway from a terminal window:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

Create List of URI Mappings to Parse

If the MIME Guessing checkbox is enabled and the server has not sent a MIME type, use this list box to map the parser to the URI.

Multiple URIs are separated by a semicolon.

For example HTML=*.html; *.htm;*Servlet

means that the HTML Rewriter is used to rewrite the content for any page with a html, htm, or Servlet extension.

➤ To Parse URI Mappings

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway Profile page displays.
4. Click the gateway profile for which you want to set the attribute.

   The Gateway - *gateway-profile-name* page displays.
5. Click the Rewriter tab, Advanced subsection.
6. Scroll to the Map Parser to MIME-Types field, and add the data to the edit box.
7. Click Save at the top or bottom of the page to record the change.
8. Restart the Gateway from a terminal window:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Enable Masking

Masking allows Rewriter to rewrite a URI so that the intranet URL of a page is not seen.

➤ To Enable Masking

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway Profile page displays.
4. Click the gateway profile for which you want to set the attribute.

   The Gateway - *gateway-profile-name* page displays.
5. Click the Rewriter tab, Advanced subsection.
6. Select the Enable Masking checkbox to enable masking.
7. Click Save at the top or bottom of the page to record the change.
8. Restart the Gateway from a terminal window:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Specify the Masking Seed String

A seed string is used for masking a URI. It is a random string generated by a masking algorithm.

NOTE Book marking of an masked URI may not work if this seed string has been changed or if the Gateway is restarted.

➤ To Specify the Masking Seed String

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway Profile page displays.
4. Click the gateway profile for which you want to set the attribute.

   The Gateway - *gateway-profile-name* page displays.
5. Click the Rewriter tab, Advanced subsection.
6. Scroll to the Masking Seed String field, and add a string to the edit box.
7. Click Save at the top or bottom of the page to record the change.
8. Restart the Gateway from a terminal window:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Create List of URIs Not to Mask

Some applications (such as an applet) require an Internet URI and cannot be masked. To specify those applications, add the URI to the list box.

For example if you added

```
*/Applet/Param*
```

to the list box, the URL would not be masked if the content URI `http://abc.com/Applet/Param1.html` is matched in the ruleset rule.

➤ To Specify Not to Mask URIs

1. Log in to the Identity Server administration console as administrator.

2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway Profile page displays.
4. Click the gateway profile for which you want to set the attribute.

   The Gateway - *gateway-profile-name* page displays.
5. Click the Rewriter tab., Advanced subsection
6. Scroll to the Not to Mask the URI list field, and add the URIs to the edit box.
7. Click Save at the top or bottom of the page to record the change.
8. Restart the Gateway from a terminal window:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Make a Gateway Protocol the Same as the Original URI Protocol

When a Gateway runs in both HTTP and HTTPS mode, you can enable Rewriter to use a consistent protocol to access the referred resources in the HTML content.

For example, if the original URL is `http://intranet.com/Public.html` then the http Gateway is added. If the original URL is `https://intranet.com/Public.html` then the https Gateway is added.

NOTE This applies only to static URIs, not to dynamic URIs generated in Javascript.

➤ To Make a Gateway Protocol the Same as the Original URI Protocol

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway Profile page displays.
4. Click the gateway profile for which you want to set the attribute.

   The Gateway - *gateway-profile-name* page displays.
5. Click the Rewriter tab, Advanced subsection.

6. Select the Make Gateway Protocol the Same as the Original URI Protocol checkbox.
7. Click Save at the top or bottom of the page to record the change.
8. Restart the Gateway from a terminal window:

   gateway-install-root`/SUNWps/bin/gateway -n` *gateway-profile-name* `start`

The Logging Tab

Using the Logging tab, in the Gateway service, you can perform the following tasks:

- Enable Logging
- Enable Netlet Logging

Enable Logging

You can specify the Gateway log file to capture either minimum information or detailed information about each session. The log information is saved in the directory specified in the Log Location attribute as part of the Logging section of the Identity Server Configuration attributes. This log is located on the Portal Server machine.

The log name uses the following convention:

`srapGateway`*_gatewayhostname_gateway-profile-name*

The log information can be saved as a file or as a database as specified in the Identity Server Configuration. The fields in the log are comma-separated ASCII values, and can be exported to other data analysis tools.

➤ To Enable Gateway Logging

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.

4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.

5. Select the Enable Logging checkbox to enable Gateway logging.

6. Select the Enable per Session Logging checkbox to capture minimum log information such as Client Address, Request Type, and Destination Host.

NOTE Log information is captured only if the Enable Logging field has already been enabled.

7. Select the Enable Detailed per Session Logging for the Gateway to capture detailed log information such as Client, Request Type, Destination Host, Type of Request, Client Requested URL, Client Post Data size, SessionID, Response Result code, and Complete Response size.

NOTE Detailed log information is captured only if the Enable per Session Logging checkbox has already been enabled.

8. Click Save at the top or bottom of the page to record the changes.

9. Restart the Gateway from a terminal window:

```
gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
```

Enable Netlet Logging

You can enable logging for Netlet related activities by selecting this option. The Netlet log will contain the following details about the Netlet sessions:

- Start time
- Source address
- Source port
- Server address
- Server port(s)
- Stop time
- Status (start or stop)

➤ To Enable Netlet Logging

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

   The Gateway page displays.
4. Click Edit... next to the gateway profile for which you want to set the attribute.

   The Edit Gateway Profile page displays.
5. Select the Enable Netlet Logging checkbox to enable Netlet logging.
6. Click Save at the bottom of the page to record the changes.
7. Restart the Gateway from a terminal window:

   ```
   gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
   ```

Chapter 10

Configuring NetFile

This chapter describes how to configure NetFile from the Sun Java™ System Identity Server administration console.

NOTE Click Help at the top right corner of the Identity Server administration console, and click SRA Help for a quick reference on all the SRA attributes.

➤ To Configure NetFile Attributes

1. Log in to the Identity Server administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View list box.
6. Click the arrow next to NetFile under SRA Configuration.

   From here, click the appropriate tab.

   - The Hosts Tab
   - The Permissions Tab
   - The View Tab
   - The Operations Tab
   - The General Tab

The tabs and the attributes that can be configured under each are listed below.

The Hosts Tab

Using the Hosts Tab, in the NetFile service, you can perform the following tasks:

- Specify the OS Character Set
- Specify Host Detection Order
- Configure a Common Hosts List
- Specify the Default Domain
- Specify the Windows Domain/Workgroup
- Specify the Default WINS/DNS Server
- Specify Access to Different Types of Hosts
- Configure the Allowed Hosts List
- Configure the Denied Hosts List

Specify the OS Character Set

You can specify the character set used as the default encoding for communicating with hosts. The default value is `UTF-8`.

CAUTION If the character set is not specified correctly, the behavior of the machine and error messages that appear cannot be predicted.

➤ To Specify the OS Character Set

1. Log in to the Identity Server administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View list box.
6. Click the arrow next to NetFile under SRA Configuration.

   The NetFile page displays.
7. Click the Hosts tab, subsection Config.

8. Scroll to the OS Character Set field and select the character set code.

9. Click Save at the top or bottom of the NetFile page to record the change.

Specify Host Detection Order

➤ **To Specify the Host Detection Order**

1. Log in to the Identity Server administration console as administrator.

2. Select the Identity Management tab.

3. Select Organizations from the View drop-down list.

4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.

5. Select Services from the View list box.

6. Click the arrow next to NetFile under SRA Configuration.

   The NetFile page displays.

7. Click the Hosts tab, subsection Config.

8. Scroll to the Hosts Detection Order field and select a host type.

9. Use the Move Up and Move Down buttons to change the host detection order.

10. Click Save at the top or bottom of the NetFile page to record the change.

Configure a Common Hosts List

You can configure a list of hosts to be available through NetFile to all remote NetFile users. You need to specify the following information for each host that you add:

Host Name—You can type either the simple host name, or the fully qualified name. If the host name that you have provided matches the host name configured by the user, the two sets of information are merged and the user-specified values override the values that you specified.

For example, suppose you have configured 4 common hosts - sesta, siroe, florizon, and abc. A user configures 3 hosts out of which 2 are sesta and siroe. User-specified values override administrator-specified values in such conflict situations. florizon and abc are also listed in the user's NetFile, and the user can carry out various operations on those hosts. In case you have listed florizon in the Denied Hosts List, florizon is listed in the user's NetFile, but no operation can be carried out on florizon.

Host Type—If the user has already added a host that is listed in the Common Hosts list, the user setting takes precedence. If there is a conflict in the type, the shares added by the administrator are not added for that user. If the user and the administrator add the same share, the share is added, but the password set by the user takes precedence.

Encoding—If there is a conflict between the value specified here and the user setting, the user setting takes precedence. If you have specified a blank or invalid setting, the character set of the client OS (user's machine) is used.

NOTE The user can edit any of these values in the NetFile client application. But the edited values are valid only for the current session. If the user logs out and logs in again, the edited values are not retained.

➤ To Configure the Common Hosts List

1. Log in to the Identity Server administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View list box.
6. Click the arrow next to NetFile under SRA Configuration.

   The NetFile page displays.
7. Click the Hosts tab, subsection Config.

   The NetFile > AddNetFile Host page is displayed.
8. To add a common host:

   a. Enter the required information in the following fields:

- Host Name
- Host Type
- Encoding
- Windows Domain / Workgroup
- User Name
- Password

b. For each share you want to add, enter the required information in the following fields and click Add to List:

- Share List
- Share Name
- Share Password

c. Click OK.

d. Repeat this information set for each common host that you want to add or delete.

9. To delete a common host from the Common Hosts list:

a. Click Delete and select the Host Name in the Share List. Then click Remove.

b. Click Save at the top or bottom of the NetFile page to record the change.

Specify the Default Domain

You can specify the default domain that NetFile needs to use to contact allowed hosts.

This default domain value is applicable only if the user does not specify a fully qualified host name while adding a host using NetFile.

CAUTION Ensure that the Default Domain field is not blank, and that it contains a valid domain name.

➤ To Specify the Default Domain

1. Log in to the Identity Server administration console as administrator.

2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View list box.
6. Click the arrow next to NetFile under SRA Configuration.

   The NetFile page displays.
7. Click the Hosts tab, subsection Config.
8. Scroll to the Default Domain field and type the default domain name.
9. Click Save at the top or bottom of the NetFile page to record the change.

Specify the Windows Domain/Workgroup

This is the default Windows domain or workgroup which the users choose to access a Windows host.

A user can override this value by specifying a different value while adding a machine.

➤ To Specify the Default Windows Domain or Workgroup

1. Log in to the Identity Server administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View list box.
6. Click the arrow next to NetFile under SRA Configuration.

   The NetFile page displays.
7. Click the Hosts tab, subsection Config.
8. Scroll to the Default Windows Domain/Workgroup field and type the default domain or workgroup name.
9. Click Save at the top or bottom of the NetFile page to record the change.

Specify the Default WINS/DNS Server

This is the WINS/DNS server NetFile uses to access windows hosts.

➤ **To Specify the Default WINS/DNS Server**

1. Log in to the Identity Server administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View list box.
6. Click the arrow next to NetFile under SRA Configuration.

   The NetFile page displays.
7. Click the Hosts tab, subsection Config.
8. Scroll to the Default WINS/DNS Server field and type the default Windows or DNS server name.
9. Click Save at the top or bottom of the NetFile page to record the change.

Specify Access to Different Types of Hosts

You can specify whether users can access specific hosts such as Windows, FTP, NFS or Netware hosts. You can set the option to allow or deny access to each type of host. All these options are enabled by default.

➤ **To Specify Access to Different Types of Hosts**

1. Log in to the Identity Server administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View list box.
6. Click the arrow next to NetFile under SRA Configuration.

   The NetFile page displays.

7. Click the Hosts tab, subsection Access.
8. Click the host type to which access is enabled.You can choose to enable:
   - Allow Access to Windows Hosts
   - Allow Access to FTP Hosts
   - Allow Access to NFS Hosts
   - Allow Access to Netware Hosts

   Selecting the option enables users to access that particular type of host. Clearing the checkbox prevents users from accessing that type of host.
9. Click Save at the top or bottom of the page to record the change.

Configure the Allowed Hosts List

By default, users are allowed to access all the hosts through NetFile because of the * entry in this list. If you want to change that, remove the * entry and specify only those hosts to which users need to have access through NetFile, in this list. Alternatively, you can keep the * entry here, and specify the hosts to which you want to deny access in the Denied Hosts list. In that case, all the hosts except the ones specified in the Denied Hosts list are allowed access.

See "Configure the Denied Hosts List" on page 291 for details.

NOTE If both the Allowed Hosts and Denied Hosts lists are blank, access is not allowed to any host.

➤ To Create the Allowed Hosts List

1. Log in to the Identity Server administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Organizations from the View drop-down list.
6. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.

7. Select Organizations from the View drop-down list.
8. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
9. Select Services from the View list box.
10. Click the arrow next to NetFile under SRA Configuration.

    The NetFile page displays.
11. Click the Hosts tab, subsection Access.
12. Scroll to the Allowed Hosts field. Type the names of the hosts to which you want to allow access in the edit field and click Add.

    The host name is added to the Allowed Hosts list box.
13. Click Save at the top or bottom of the page to record the changes.

Configure the Denied Hosts List

After specifying the list of commonly available hosts under "Configure a Common Hosts List" on page 285, you can also specify a list of hosts to which users are denied access through NetFile.

NOTE If you deny access to a host, and a user has already added this host in the NetFile window, the denied host will continue to be displayed in the NetFile window of the user. But the user will not be able to carry out any operations on the host.

In NetFile Java2, denied hosts, if displayed in the application, are marked with a red cross to indicate that they are inaccessible.

NOTE If both the Allowed Hosts and Denied Hosts lists are blank, access is not allowed to any host.

➤ To Create a Denied Hosts List

1. Log in to the Identity Server administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.

4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Organizations from the View drop-down list.
6. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
7. Select Services from the View list box.
8. Click the arrow next to NetFile under SRA Configuration.

   The NetFile page displays.
9. Click the Hosts tab, subsection Access.
10. Scroll to the Denied Hosts field. Type the names of the hosts to which you want to deny access in the edit field.
11. Click Add.

    The host name is added to the Denied Hosts list box.
12. Click Save at the top or bottom of the page to record the changes.

The Permissions Tab

Using the Permissions tab, in the NetFile service, you can allow or deny permission for users to perform the following tasks from remote hosts:

- Rename files
- Delete files and folders
- Upload files
- Download files and folders
- Search for a file
- Mail files
- Compress files
- Change User Id

This option lets you specify whether a user can use different IDs to connect to hosts using NetFile. In a large organization, users may have multiple user IDs. You may want to restrict users to use a single user ID. In that case, you can disable the Allow Changing User ID option. This prevents all the users in the specific organization from changing their user ID, and limits them to using a single ID (the desktop login ID) to connect to hosts using NetFile. In another situation, a user may have different login IDs on different machines, in which case, you may want to allow the user to change the ID as required.

- Change Windows Domains

  This option is applicable to NT domains.

  If the user specifies an invalid domain name in the User NT Domain name field while adding a system, an error message displays. If the user edits the host information later, and specifies an invalid domain name, an error message does not appear.

  If the user specifies a domain name, the username and password for that domain also needs to be specified. If the username and password for the host needs to be used, the user needs to remove the domain from the User NT Domain name field.

The permission options are enabled by default.

➤ To Enable/Disable Permissions

1. Log in to the Identity Server administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View list box.
6. Click the arrow next to NetFile under SRA Configuration.

   The NetFile page displays.
7. Click the Permissions tab.
8. Scroll to the required Allow field and click the checkbox to allow permission.
9. Click Save at the top or bottom of the NetFile page to record the change.

NOTE If you disable these options after the user has started using NetFile, the change takes effect only if the user logs out of NetFile and logs in again.

The View Tab

Using the View tab, in the NetFile service, you can perform the following tasks:

- Specify the NetFile Window Size
- Specify the NetFile Window Location

Specify the NetFile Window Size

You can specify the size of the NetFile window in pixels on the user's desktop. The default value is `700|400` in pixels. If you enter an invalid value, NetFile uses the default value.

NOTE The user can also edit this value in the limited administration console that is available to the user. The value that you specify is replaced with the new values if the user resizes the NetFile window on the desktop.

➤ To Specify the Size of the NetFile Window

1. Log in to the Identity Server administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View list box.
6. Click the arrow next to NetFile under SRA Configuration.

   The NetFile page displays.
7. Click the View tab.

8. Scroll to the Window Size field and type the required window size in pixels.

   Type the value in the format `700|400` without any spaces. The coordinates are in the form `x|y`. No other character should be used as a separator.

9. Click Save at the top or bottom of the NetFile page to record the change.

Specify the NetFile Window Location

You can specify the location where the NetFile window displays on the user's desktop. The default value is `100|50` in pixels. If you enter an invalid value, NetFile uses the default value.

NOTE The user can also edit this value in the limited administration console that is available to the user. The value that you specify is replaced with the new values if the user relocates the NetFile window on the desktop.

➤ **To Specify the Location of the NetFile Window**

1. Log in to the Identity Server administration console as administrator.

2. Select the Identity Management tab.

3. Select Organizations from the View drop-down list.

4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.

5. Select Services from the View list box.

6. Click the arrow next to NetFile under SRA Configuration.

   The NetFile page displays.

7. Click the View tab.

8. Scroll to the Window Location field and type the required window location coordinates.

   Type the value in the format `100|50` without any spaces. The coordinates are in the form `x|y`. No other character should be used as a separator.

9. Click Save at the top or bottom of the NetFile page to record the change.

The Operations Tab

Using the Operations tab, in the NetFile service, you can perform the following tasks:

- Specify the Temporary Files Directory
- Set the File Upload Size Limit
- Specify the Search Directories Limit
- Specify Compression

Specify the Temporary Files Directory

NetFile needs a temporary directory for some file operations such as mailing files. The default temporary directory is `/tmp`. The temporary files are deleted after the required operation has been carried out.

The specified temporary directory is created if it does not exist on the server.

Ensure that the ID with which the web server is running (such as `nobody` or `noaccess`) has `rwx` permissions for the specified directory. Also ensure that the ID has `rx` permissions for the entire path to the required temporary directory.

TIP You may want to create a separate temporary directory for NetFile. If you specify a temporary directory that is common to all modules of the Portal Server, the disk may quickly run out of space. A few operations in NetFile, such as mailing files, will not work if the temporary directory has no space.

➤ **To Specify a Temporary Directory**

1. Log in to the Sun Java™ System Identity Server administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Select Services from the View list box.
5. Click the arrow next to NetFile under SRA Configuration.

   The NetFile page displays.

6. Click the Operations tab, Traffic subsection.
7. Scroll to the Temporary Directory Location field and type the required temporary directory location.
8. Click Save at the top or bottom of the NetFile page to record the change.

Set the File Upload Size Limit

You can specify the maximum size of the files that can be uploaded in this field. If the size of the file being uploaded exceeds the limit specified here, an error message is displayed and the file is not uploaded. The default value is 5 MB. If you enter an invalid value, NetFile resets the value to the default.

You can specify different file upload size limits for different users.

NOTE Specify the maximum file size for upload in megabytes. Ensure that you type an integer value.

➤ **To Set the File Upload Size Limit**

1. Log in to the Identity Server administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View list box.
6. Click the arrow next to NetFile under SRA Configuration.

   The NetFile page displays.
7. Click the Operations tab, Traffic subsection.
8. Scroll to the File Upload Limit (in MB) field. Type the required size limit in mega bytes.
9. Click Save at the top or bottom of the NetFile page to record the change.

Specify the Search Directories Limit

You can configure the maximum number of directories that will be searched in a single search operation. This limit helps reduce network clogging and increases the speed of access if a number of users are logged in simultaneously. The default value is `100`. If you type an invalid value, NetFile resets the value to the default.

Suppose a user has a directory called A. Assume that A has 100 subdirectories. If you specify the maximum directories to be searched as 100, the search operation will go through directory A and stop. The search will not proceed through the other directories in the user's machine since the limit of 100 was reached with directory A. The search results accumulated until the search limit is reached are displayed to the user along with an error message stating that the search exceeded its limit. To continue the search, the user must manually restart the search at the next directory.

The search operation is carried out in a depth-first manner. This means that the search operation is carried out in all the subdirectories of the directory that the user selected, before moving on to the next directory.

➤ **To Specify the Search Directories Limit**

1. Log in to the Identity Server administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View list box.
6. Click the arrow next to NetFile under SRA Configuration.

   The NetFile page displays.
7. Click the Operations tab, Search subsection.
8. Scroll to the Search Directories Limit field-and type the required number.

NOTE	Ensure that you type an integer value in this field.

9. Click Save at the top or bottom of the NetFile page to record the change.

Specify Compression

These compression attributes apply only to NetFile Java2.

➤ **To Specify the Default Compression Type**

1. Log in to the Identity Server administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View list box.
6. Click the arrow next to NetFile under SRA Configuration.

   The NetFile page displays.
7. Click the Operations tab, Compression subsection.
8. Scroll to the Default Compression Type field.

   Choose Zip or GZip
9. Click Save at the top or bottom of the NetFile page to record the change.

The General Tab

Using the General tab, in the NetFile service, you can specify the MIME-types configuration file location.

Specify the MIME-types Configuration File Location

This information is required to determine the response content type to send to the client browser. The browser needs this information to determine the application that a file needs to be associated with during a NetFile open or download operation. This is configured during installation.

If the MIME-types file of the Portal Server's web server needs to be used, specify the location:

portal-server-install-root/`SUNWam/servers/`*instance-name-of-web-server-machine*/`config`

NOTE MIME-types Configuration File Location attribute can be set only at the organization level.

➤ To Specify the Location of the MIME-types Configuration File

1. Log in to the Identity Server administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View list box.
6. Click the arrow next to NetFile under SRA Configuration.

   The NetFile page displays.
7. Click the General tab.
8. Scroll to the MIME-types Configuration File Location field and type the full path to where the MIME-types configuration file is located.
9. Click Save at the top or bottom of the NetFile page to record the change.

Enable Debugging for NetFile

The location of the debug information depends on the setting of the `com.iplanet.services.debug.directory` attribute in the `AMConfig-`*instance-name*`.properties` file on the Portal Server node.

For example, if the value of the `com.iplanet.services.debug.directory` attribute is:

```
/var/opt/SUNWam/debug/
```

Then the debug information for NetFile will be available in the `srapNetFile` file in the `/var/opt/SUNWam/debug` directory.

See the *Identity Server Administration Guide* for more information.

Chapter 11

Configuring Netlet

This chapter describes how to configure Netlet attributes from the Sun Java™ System Identity Server administration console.

NOTE Click Help at the top right corner of the Identity Server administration console, and click SRA Help for a quick reference on all the SRA attributes.

All the attributes that can be configured at the organization level can also be configured at the user level. See the *Identity Server Administration Guide* for more information on organization, role and user level attributes.

To configure Netlet attributes, follow these steps to configure attributes at the organization level:

1. Log in to the Sun Java™ System Identity Server administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View drop-down list.
6. Click the arrow next to Netlet under SRA Configuration.

   From here, you can perform the following tasks:

   - Add a Netlet Rule
   - Assign Netlet Service to a User
   - Add a Netlet Rule

- Modify an Existing Netlet Rule
- Delete a Netlet Rule

Other than configuring user profiles and creating Netlet rules, you need to configure the following attributes based on your site's requirements. These attributes can be configured at the organization or user levels.

- Specify the Default Encryption Cipher
- Assign the Default Loopback Port
- Enable Reauthentication for Connections
- Enable Warning Popup Dialog Box for Connections
- Enable the Display Checkbox in Port Warning Dialog
- Set the Keep Alive Interval
- Set the Terminate Netlet at Portal Logout Option
- Define Access to Netlet Rules
- Denying Access to Netlet Rules
- Allow Access to HostsDeny Access to Hosts

Assign Netlet Service to a User

1. Log in to the Identity Server administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name.

   The selected organization name is reflected as the location in the top left corner of the admin console.
5. Select Users from the View drop-down list for the selected organization.
6. Click the arrow next to the required user in the left pane.
7. Select Services from the View drop-down list for this user, if the Netlet service is not already available for this user
8. Click Add.

9. Select Netlet from the Available Services list.

10. Click Save

11. The Netlet attributes can be modified by selecting Netlet service from the View drop-down list for this user.

Add a Netlet Rule

You can add or create Netlet rules at a global level in the Identity Management tab of the Identity Server administration console. These rules are inherited by any new organization that you create.

You can also create new rules or modify existing rules at the organization, role, or user levels.

➤ To Add a Netlet Rule

1. Log in to the Identity Server administration console as administrator.

2. Choose the Identity Management tab.

3. Choose the Organization for which you want to create the rule.

4. Select Services from the View drop-down list.

5. Click the arrow next to Netlet under SRA Configuration.

   The Netlet page is displayed in the right pane.

6. Click Add in the Netlet Rules field.

   The Add Netlet Rule page is displayed. All the fields of the rule are populated with sample values that you can change as required.

7. Type a unique name for the rule in the Rule Name field.

8. Specify the required ciphers. Select Default to retain the default encryption cipher. Select Other to choose from the list of available ciphers.

   See "To Specify the Default Cipher" on page 306 for details on the default cipher.

9. Type the URL to the application to be invoked in the URL field.

10. Select the Download Applet checkbox if an applet needs to be downloaded. Type the applet details in the format *local-port:server-host:server-port* in the associated edit box.

NOTE Specify a unique `local port for` each rule.

You need to specify the applet details only if the applet needs to be downloaded from a host other than the Portal Server host. The edit box is disabled if you do not select the checkbox. For more information see "Downloading an Applet From a Remote Host" on page 184.

11. Select the Extend Session checkbox to ensure that the Portal Server session time is extended while the Netlet session corresponding to this rule is running.
12. Type the local port on which Netlet listens in the Local Port field.

    For an FTP rule, the local port value must be 30021.
13. Type an entry in the Target Host(s) field.

    For a static rule, enter the host name of the target machine for the Netlet connection.

    For a dynamic rule, enter "TARGET".
14. Type the port on the target host in the Target Port(s) field.
15. Click Add to List to reflect the last three entries in the Local Port to Destination Port fields.
16. Click Save.

    The rule is saved and you are returned to the Netlet page. The new rule name displays in the Netlet Rules list.

Modify an Existing Netlet Rule

You can modify existing rules at the organization, role, or user levels from the Identity Management tab in the administration console. These rules are inherited by any new organization that you create.

➤ To Modify a Netlet Rule

1. Log in to the Identity Server administration console as administrator.
2. Choose the Identity Management tab.
3. Choose the Organization for which you want to modify the rule.
4. Select Services from the View drop-down list.

5. Click the arrow next to Netlet under SRA Configuration.

   The Netlet page is displayed in the right pane.

6. Click name of the rule that you want to modify.

   The Edit Netlet Rule page is displayed.

7. Make changes as required and click Save.

   The modified rule is saved and you are returned to the Netlet page.

Delete a Netlet Rule

You can delete Netlet rules at a global level in the Identity Management tab of the administration console.

➤ To Delete a Netlet Rule

1. Log in to the Identity Server administration console as administrator.

2. Choose the Identity Management tab.

3. Choose the Organization for which you want to delete the rule.

4. Click the arrow next to Netlet under SRA Configuration.

   The Netlet page is displayed in the right pane.

5. Select the checkbox next to the rule that you want to delete from the Netlet Rules list.

6. Click Delete.

   The selected rule is removed from the Netlet Rules list.

NOTE This section describes the configuration of all the attributes at the organization level.

Specify the Default Encryption Cipher

You need to specify the default cipher for the Netlet rules. This is useful when using existing rules that did not include the cipher as a part of the rule. This is a mandatory field. See “Backward Compatibility” on page 191.

➤ To Specify the Default Cipher

1. Log in to the Identity Server administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View drop-down list.
6. Click the arrow next to Netlet under SRA Configuration.

   The Netlet page displays in the right pane.
7. Scroll to the Default Native VM Cipher or Default Java Plugin Cipher field and select the required cipher from the drop-down list. See "Supported Ciphers" on page 190 for a list of supported ciphers.
8. Click Save at the top or bottom of the Netlet page to record the change.

Assign the Default Loopback Port

This attribute specifies the port to be used on the local machine when applets are downloaded through Netlet. The default value of 58000 is used unless it is overridden in the Netlet rules.

➤ To Assign the Default Loopback Port

1. Log in to the Identity Server administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View drop-down list.
6. Click the arrow next to Netlet under SRA Configuration.

   The Netlet page displays in the right pane.
7. Scroll to the Default Loopback Port field and type the desired port number.
8. Click Save at the top or bottom of the Netlet page to record the change.

Enable Reauthentication for Connections

Enable this option if you want the user to enter the Netlet password each time a Netlet connection needs to be established. If you enable this option, the warning popup for connections is not displayed on the user's desktop. See "Enable Warning Popup Dialog Box for Connections" on page 307 for details.

Enabling this option allows the user to change the reauthentication password using the Netlet channel edit option. The initial password is `srap-Netlet` by default.

➤ To Enable Reauthentication for Connections

1. Log in to the Identity Server administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View drop-down list.
6. Click the arrow next to Netlet under SRA Configuration.

   The Netlet page displays in the right pane.
7. Scroll to the Reauthenticate for Connections field and select the option.
8. Click Save at the top or bottom of the Netlet page to record the change.

Enable Warning Popup Dialog Box for Connections

This attribute displays a warning popup dialog box on the user's desktop when someone is trying to connect to Netlet through the listen port and the user is running an application using Netlet. If you do not want the popup to appear on the user's desktop, deselect this attribute.

➤ To Enable the Warning Popup for Connections

1. Log in to the Identity Server administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.

4. Click the required organization name. The selected organization name is reflected as the "location" in the top left corner of the administration console.

5. Select Services from the View drop-down list.

6. Click the arrow next to Netlet under SRA Configuration.

   The Netlet page displays in the right pane.

7. Select the Display Warning Popup for Connections checkbox to enable the warning popup.

8. Click Save at the top or bottom of the Netlet page to record the change.

Enable the Display Checkbox in Port Warning Dialog

This attribute displays a checkbox in the warning popup on the users desktop when Netlet tries to connect to the destination host through a freely available port on the local machine, if its enabled in the administration console. This checkbox gives the user the option to enable or disable the popup, by checking or unchecking it accordingly on the desktop.

You can allow the user to suppress this warning popup by disabling the Display Checkbox in Port Warning Dialog option in the administration console.

➤ **To Allow the User to Suppress the Port Warning Dialog**

1. Log in to the Identity Server administration console as administrator.

2. Select the Identity Management tab.

3. Select Organizations from the View drop-down list.

4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.

5. Select Services from the View drop-down list.

6. Click the arrow next to Netlet under SRA Configuration.

   The Netlet page displays in the right pane.

7. Scroll to the Display Checkbox in Port Warning Dialog field and uncheck the box.

8. Click Save at the top or bottom of the Netlet page to record the change.

Set the Keep Alive Interval

If the client is connecting to the Gateway through a web proxy, then idle Netlet connections are disconnecteed due to proxy timeout. To prevent this, give a value less than the proxy timeout for this parameter.

➤ To Set the Keep Alive Interval

1. Log in to the Identity Server administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View drop-down list.
6. Click the arrow next to Netlet under SRA Configuration.

   The Netlet page displays in the right pane.
7. Scroll to the Keep Alive Interval (in minutes) field, and type the required time interval.
8. Click Save at the top or bottom of the Netlet page to record the change.

Set the Terminate Netlet at Portal Logout Option

Enable this option if you want to ensure that all connections are terminated when a user logs out of the Portal Server. This ensures greater security. This option is enabled by default.

Disable this option to ensure that live Netlet connections are operational even after the user has logged out of the Portal Server desktop.

NOTE Disabling this option does not allow the user to make new Netlet connections after logging out of the Portal Server. Only existing connections are preserved.

➤ To Set the Terminate Netlet at Portal Logout Option

1. Log in to the Identity Server administration console as administrator.

2. Select the Identity Management tab.

3. Select Organizations from the View drop-down list.

4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.

5. Select Services from the View drop-down list.

6. Click the arrow next to Netlet under SRA Configuration.

   The Netlet page displays in the right pane.

7. Scroll to the Terminate Netlet at Portal Logout field and select or deselect the option as required.

8. Click Save at the top or bottom of the Netlet page to record the change.

   See also Running Netlet in a Sun Ray Environment.

Define Access to Netlet Rules

You can define access to specific Netlet rules for certain organizations, roles or users.

➤ To Define Access to Netlet Rules

1. Log in to the Identity Server administration console as administrator.

2. Select the Identity Management tab.

3. Select Organizations from the View drop-down list.

4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.

5. Select Services from the View drop-down list.

6. Click the arrow next to Netlet under SRA Configuration.

   The Netlet page displays in the right pane.

7. Scroll to the Access to Netlet Rules field.

8. Type the name of the rule that you want to make available for the selected organization in the Access to Netlet Rules field.

   An asterisk (*) in this field indicates that all the defined Netlet rules are available for the selected organization.

9. Click Add.

   The specified rule is added to the Access to Netlet Rules list.

10. Repeat steps 7, 8 and 9 for each Netlet rule that you want to make available.
11. Click Save at the top or bottom of the Netlet page to record the change.

Denying Access to Netlet Rules

You can deny access to specific Netlet rules for certain organizations, roles or users.

➤ To Deny Access to Netlet Rules

1. Log in to the Identity Server administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View drop-down list.
6. Click the arrow next to Netlet under SRA Configuration.

   The Netlet page displays in the right pane.

7. Scroll to the Deny Netlet Rules field.
8. Type the name of the rule to which you want to deny access for the selected organization in the Deny Netlet Rules field.

   An asterisk (*) in this field indicates that all the defined Netlet rules are denied access for the selected organization.

9. Click Add.

   The specified rule is added to the Deny Netlet Rules list.

10. Repeat steps 7, 8 and 9 for each Netlet rule for which you want to deny access.
11. Click Save at the top or bottom of the Netlet page to record the change.

Allow Access to Hosts

You can define access to specific hosts for certain organizations, roles or users. This enables you to allow access to certain hosts. For example, you can set up the Allow list with five hosts to which the user can telnet.

➤ To Allow Access to Hosts

1. Log in to the Identity Server administration console as administrator.

2. Select the Identity Management tab.

3. Select Organizations from the View drop-down list.

4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.

5. Select Services from the View drop-down list.

6. Click the arrow next to Netlet under SRA Configuration.

   The Netlet page displays in the right pane.

7. Scroll to the Allowed Hosts field.

8. Type the name of the host for which you want to allow access in the Allow Hosts field.

   An asterisk (*) in this field indicates that all the hosts in the specified domain are accessible. For example, if you specify `*.sesta.com`, all the Netlet targets within the `sesta.com` domain can be executed by the user. You can also specify a wild card IP address such as `xxx.xxx.xxx.*`.

9. Click Add.

   The specified host is added to the Allowed Hosts list.

10. Repeat steps 7 and 8 for each host that you want to make available.

11. Click Save at the top or bottom of the Netlet page to record the change.

Deny Access to Hosts

You can deny access to specific hosts within an organization. Specify the host for which you want to deny access in the Denied Hosts list.

➤ To Deny Access to Hosts

1. Log in to the Identity Server administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View drop-down list.
6. Click the arrow next to Netlet under SRA Configuration.

   The Netlet page displays in the right pane.
7. Scroll to the Denied Hosts field.
8. Type the name of the host for which you want to deny access in the Denied Hosts field.

   An asterisk (*) in this field indicates that the user is denied access to all the hosts within the selected organization. For example, to deny access to all the hosts in the organization `sesta`, type `*.sesta.com` in the Denied Hosts field.

   To deny access to a specific host, specify the fully qualified name. For example, to deny access to a host `abc`, type `abc.sesta.com`.
9. Click Add.

   The specified domain is added to the Access to Domains list.
10. Repeat steps 7 and 8 for each domain that you want to make available.
11. Click Save at the top or bottom of the Netlet page to record the change.

Proxy Configuration

The following attributes can be configured at the user level:

- Browser proxy type
- Browser proxy host
- Browser proxy port
- Browser proxy override list

If you do not specify these values in the administration console and Netlet is unable to determine the browser proxy setting, the user is asked for this information when a connection is being established through Netlet for the first time. This information is stored and used for future connections by the user.

Netlet fails to determine the browser proxy setting in the following scenarios:

- The user has Internet Explorer 4.x, 5.x or 6.x with Java plug-in (version less then 1.4.0), has enabled the "Use Browser Settings" option in the Proxies tab of the Java Plug-in Control Panel, and has specified an add-on product or INS file in the "Use automatic configuration script" field in the Local Area Network Settings dialog of Internet Explorer.
- The user has Netscape 6.2 with Java Plug-in (version 1.3.1_01 or greater) and has enabled the "Use Browser Settings" option in the Proxies tab of the Java Plug-in Control Panel.

In both these cases, Netlet may not be able to determine the browser settings, and hence the user is asked to supply the following information:

- Browser proxy type

  This attribute can take the values DIRECT or MANUAL. If the user chooses DIRECT from the drop-down list, Netlet connects directly to the gateway host.
- Browser proxy host

  Specify the required proxy host through which Netlet needs to connect.
- Browser proxy port

  Specify the port on the proxy host through which Netlet needs to connect.
- Browser proxy override list (Comma separated)

  Specify the hosts for which you do not want Netlet to connect through the proxy. This list can contain multiple comma-separated host names.

Enable Debug Logging

The location of the debug information depends on the setting of the `com.iplanet.services.debug.directory` attribute in the `AMConfig-`*instance-name*`.properties` file on the Portal Server node.

For example, if the value of the `com.iplanet.services.debug.directory` attribute is:

```
/var/opt/SUNWam/debug/
```

Then the debug information for Netlet will be available in the `srapNetlet` file in the `/var/opt/SUNWam/debug` directory.

See the *Identity Server Administration Guide* for more information.

Chapter 12

Configuring Proxylet

This chapter describes how to configure Proxylet from the Sun Java™ System Identity Server administration console.

NOTE	Click Help at the top right corner of the Identity Server administration console, and click SRA Help for a quick reference on all the SRA attributes.

Configuring Proxylet

Proxylet can be configured to launch automatically when the user logs in by checking the Download Proxylet Applet Automatically checkbox in the Proxylet channet edit page. If the Download Proxylet Automatically checkbox is not checked, the user can get Proxylet on-demand by clicking the “Launch the Proxylet” link in the Proxylet channel of the standard Portal Desktop.

➤ To Configure Proxylet Attributes

1. Log in to the Identity Server administration console as administrator.
2. Select the Service Configuration tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Click the arrow next to Proxylet under SRA Configuration.
6. Click the Download Proxylet Applet Automatically checkbox, if that is desired.
7. Enter the Default Proxylet Applet Bind IP address where the Proxylet will run.

8. Enter the required port number where Proxylet will listen in the Default Proxylet Applet Port field.

9. Click Save.

NOTE If the user is logged in to Portal Server and invoked Proxylet, then installed a Java Plugin, the user must restart the Netscape browser.

Chapter 13

Configuring SSL Accelerators

This chapter describes how to configure various accelerators for Sun Java™ System Portal Server Secure Remote Access.

This chapter covers the following topics:

- Sun Crypto Accelerator 1000
- Sun Crypto Accelerator 4000
- External SSL Device and Proxy Accelerators

Overview

External accelerators are dedicated hardware co-processors that off-load the SSL functions from a server's CPU, thereby freeing the CPU to perform other tasks and increasing the processing speed for SSL transactions.

Sun Crypto Accelerator 1000

The Sun™ Crypto Accelerator 1000 (Sun CA1000) board is a short PCI board that functions as a cryptographic co-processor to accelerate public key and symmetric cryptography. This product has no external interfaces. The board communicates with the host through the internal PCI bus interface. The purpose of this board is to accelerate a variety of computationally intensive cryptographic algorithms for security protocols in eCommerce applications.

Many critical cryptographic functions, such as RSA [7] and Triple-DES (3DES) [8], can be off-loaded from an application to the Sun CA1000 and performed in parallel. This frees the CPU to perform other tasks, increasing the processing speed for SSL transactions.

Enable Crypto Accelerator 1000

Ensure that Portal Server Secure Remote Access has been installed, and a gateway server certificate (self-signed or issued by any CA) has been installed. See the Certificates chapter for details.

Table 13-1 is a checklist to help you keep track of the required information before installing the SSL Accelerator.lists the Crypto Accelerator 1000 parameters and values.

Table 13-1 Crypto Accelerator 1000 Installation Checklist

Parameter	Value
SRA installation base directory	/opt
SRA certificate database path	/etc/opt/SUNWps/cert/default
SRA server certificate nickname	server-cert
Realm	sra-keystore
Realm user	crypta

Configure Crypto Accelerator 1000

➤ To Configure Crypto Accelerator 1000

1. Follow the instructions in the user's guide to install the hardware. See:

   `http://www.sun.com/products-n-solutions/hardware/docs/pdf/816-2450-11.pdf`

2. Install the following packages from the CD.

   `SUNWcrypm, SUNWcrypu, SUNWcrysu, SUNWdcar, SUNWcrypr, SUNWcrysl, SUNWdcamn,  SUNWdcav`

3. Install the following patches. (You can get them from the `http://sunsolve.sun.com`)

   110383-01, 108528-05, 112438-01

4. Make sure you have the tools `pk12util` and `modutil`.

   These tools are installed under `/usr/sfw/bin`. If the tools are not available in the `/usf/sfw/bin` directory, you need to manually add the SUNWtlsu package from the Sun Java System distribution media:

   ```
   Solaris_[sparc/x86]/Product/shared_components/
   ```

5. Create the slots file:

   ```
   vi /etc/opt/SUNWconn/crypto/slots
   ```

   and put "crypta@sra" as the first and only line in the file.

6. Create and set a realm.

   a. Login as root.

   b. Type these commands:

      ```
      cd /opt/SUNWconn/bin/secadm
      secadm> create realm=sra
      Realm sra created successfully.
      ```

7. Create a user:

   a. Type and respond to these commands:

      ```
      secadm> set realm=sra
      secadm{srap}> su
      secadm{root@sra}>create user=crypta
      Initial password:
      Confirm password:
      User crypta created successfully.
      ```

8. Login as the user you created.

   ```
   secadm{root@sra}> login user=crypta
   Password:
   secadm{crypta@sra}> show key
   No keys exist for this user.
   ```

9. Load the Sun Crypto module.

   The environment variable `LD_LIBRARY_PATH` must point to `/usr/lib/mps/secv1/`

   Type:

   ```
   modutil -dbdir /etc/opt/SUNWps/cert/default -add "Sun Crypto Module"
   -libfile  /opt/SUNWconn/crypto/lib/libpkcs11.so
   ```

   Use the following command to verify that this module is loaded:

   ```
   modutil -list -dbdir /etc/opt/SUNWps/cert /default
   ```

10. Export the gateway certificate and the key to the "Sun Crypto Module".

    The environment variable `LD_LIBRARY_PATH` must point to `/usr/lib/mps/secv1/`

    Type:

    ```
    pk12util -o servercert.p12 -d /etc/opt/SUNWps/cert/default -n
    server-cert
    ```

    ```
    pk12util -i servercert.p12 -d /etc/opt/SUNWps/cert/default -h
    "crypta@sra"
    ```

    Now run the show key command:

    ```
    secadm{crypta@sra}> show key
    ```

    You should see two keys for this user.

11. Change the nickname in the /etc/opt/SUNWps/cert/default/.nickname file.

    ```
    vi /etc/opt/SUNWps/cert/default/.nickname
    ```

    replace the `server-cert` with `crypta@sra:server-cert`

12. Enable ciphers for acceleration.

    See“Enable SSL Cipher Selection” on page 263

    SUN CA1000 accelerates RSA functions but supports acceleration only for DES and 3DES ciphers.

13. Modify the `/etc/opt/SUNWps/platform.conf.`*gateway-profile-name* to enable the accelerator:

    ```
    gateway.enable.accelerator=true
    ```

14. From a terminal window, restart the gateway:

    ```
    portal-server-install-root/SUNWps/bin/gateway -n gateway-profile-name start
    ```

NOTE Gateway binds to a plain ServerSocket (non SSL) on the port mentioned as https port in the gateway profile.

No SSL encryption or decryption is done on the incoming client traffic. This is done by the accelerator.

PDC is not be functional in this mode.

Sun Crypto Accelerator 4000

The Sun™ Crypto Accelerator 4000 board is a Gigabit Ethernet-based network interface card that supports cryptographic hardware acceleration for IPsec and SSL (both symmetric and asymmetric) on Sun servers.

In addition to operating as a standard Gigabit Ethernet network interface card for unencrypted network traffic, the board contains cryptographic hardware to support a higher throughput for encrypted IPsec traffic.

The Crypto Accelerator 4000 board accelerates cryptographic algorithms in both hardware and software. It also supports bulk encryption for ciphers DES and 3DES.

Enable Crypto Accelerator 4000

Ensure that SRA has been installed and a gateway server certificate (self-signed or issued by any CA) has been installed. The following checklist helps you keep track of the required information before installing the SSL Accelerator.

Table 13-1 lists the Crypto Accelerator 4000 parameters and values..

Table 13-2 Crypto Accelerator 4000 Installation Checklist

Parameter	Value
Secure Remote Access installation base directory	/opt
SRA instance	default
SRA certificate database path	/etc/opt/SUNWps/cert/default
SRA server certificate nickname	server-cert

Table 13-2 Crypto Accelerator 4000 Installation Checklist

Parameter	Value
CA4000 keystore	srap
CA4000 keystore user	crypta

Configure Crypto Accelerator 4000

➤ To Configure Crypto Accelerator 4000

1. Follow the instructions in the user's guide to install the hardware and the software packages. See:

   http://www.sun.com/products-n-solutions/hardware/docs/pdf/816-2450-11.pdf

2. Install the following patch. (You can get them from the http://sunsolve.sun.com): 114795

3. Make sure that you have the tools `certutil`, `pk12util` and `modutil`.

   These tools are installed under `/usr/sfw/bin`

   If the tools are not available in the `/usf/sfw/`bin directory, you need

   to manually add the SUNWtlsu package from the Sun Java System distribution media:

   `Solaris_[sparc/x86]/Product/shared_components/`

4. Initialize the board.

   Run the `/opt/SUNWconn/bin/vcadm` tool to initialize the crypto board and set the following values.

   Initial Security Officer Name: `sec_officer`

   Keystore name: `sra-keystore`

   Run in FIPS 140-2 Mode: `No`

5. Create a user.

   vcaadm{vca0@localhost, sec_officer}> `create user`

   New user name: `crypta`

   Enter new user password:

   Confirm password:

   User crypta created successfully.

6. Map token to the key store.

   ```
   vi /opt/SUNWconn/cryptov2/tokens
   ```

   and append `sra-keystore` to the file.

7. Enable bulk encryption.

   ```
   touch /opt/SUNWconn/cryptov2/sslreg
   ```

8. Load the Sun Crypto module.

   The environment variable `LD_LIBRARY_PATH` must point to `/usr/lib/mps/secv1/`

   Type:

   ```
   modutil -dbdir /etc/opt/SUNWps/cert/default -add "Sun Crypto Module"
   -libfile /opt/SUNWconn/cryptov2/lib/libvpkcs11.so
   ```

   You can verify that this module is loaded using the following command:

   ```
   modutil -list -dbdir /etc/opt/SUNWps/cert/default
   ```

9. Export the gateway certificate and the key to the "`Sun Crypto Module`".

   The environment variable `LD_LIBRARY_PATH` must point to `/usr/lib/mps/secv1/`

   ```
   pk12util -o servercert.p12 -d /etc/opt/SUNWps/cert/default -n
   server-cert
   ```

   ```
   pk12util -i servercert.p12 -d /etc/opt/SUNWps/cert/default -h
   "sra-keystore"
   ```

   You can verify that the key has been exported using the following command:

   ```
   certutil -K -h "sra-keystore" -d /etc/opt/SUNWps/cert/default
   ```

10. Change the nickname in the `/etc/opt/SUNWps/cert/default/.nickname` file:

    ```
    vi /etc/opt/SUNWps/cert/default/.nickname
    ```

    replace the `server-cert` with `sra-keystore:server-cert`

11. Enable the ciphers for acceleration.

    See "Enable SSL Cipher Selection" on page 263

12. From a terminal window, restart the gateway:

    ```
    portal-server-install-root/SUNWps/bin/gateway -n gateway-profile-name start
    ```

    The gateway will prompt you to enter the keystore password.

    Enter Password or Pin for "sra-keystore":crypta:crytpa-password

NOTE Gateway binds to a plain ServerSocket (non SSL) on the port mentioned as https port in the gateway profile.

No SSL encryption or decryption is done on the incoming client traffic. This is done by the accelerator.

PDC is not be functional in this mode.

External SSL Device and Proxy Accelerators

An external SSL device can run in front of Sun Java System Portal Server Secure Remote Access (SRA) in open mode. It provides the SSL link between the client and SRA.

Enable an External SSL Device Accelerator

Ensure that SRA has been installed and a gateway is running in secure mode (HTTPS mode):

Gateway >> Enable HTTPS Connections

Gateway>> HTTP Port: 880

Table 13-3 lists the external SSL device and proxy accelerator parameters and values.

Table 13-3 External SSL Device and Proxy Accelerators Checklist

Parameter	Value
SRA instance	default
Gateway Mode	https

Table 13-3 External SSL Device and Proxy Accelerators Checklist

Parameter	Value
Gateway Port	880
External Device/Proxy Port	443

Configure an External SSL Device Accelerator

➤ To Configure External SSL Device Accelerators

1. Follow the instructions in the user guide to install the hardware and software packages.

2. Install the required patches, if any.

3. Enable SSL Device / Proxy support by entering values in the `platform.conf` file:

   `vi /etc/opt/SUNWps/platform.conf.default`

   `gateway.enable.accelerator=true`

   If the external device / proxy host name is different from the gateway host name:

   `gateway.enable.customurl=true`

   `gateway.httpsurl=`*external-device.domain.subdomain/proxy-URL*

4. Gateway notification can be configured in two ways:

   - When the Identity Server can contact the gateway machine at port 880 (Session notifications will be in http), enter values in the `platform.conf` file.

     `vi /etc/opt/SUNWps/platform.conf.default`

     `gateway.protocol=http`

     `gateway.port=880`

   - When the Identity Server can contact the external device / proxy at port 443 (Session notifications will be in HTTPS), enter values in the `platform.conf` file.

     `vi /etc/opt/SUNWps/platform.conf.default`

     `gateway.host=External Device/Proxy Host Name`

     `gateway.protocol=https`

```
gateway.port=443
```

5. Make sure that the SSL device / proxy is up and running and configured to tunnel the traffic to the gateway port.

6. From a terminal window, restart the gateway:

   gateway-install-root/`SUNWps/bin/gateway -n` *gateway-profile-name* `start`

Appendix A

Log Files

The following log files are in the default `/var/opt/SUNWps/debug` directory and contain debug and other types of information.:

Table A-1 Informational and Debug Files

Filename	Contents
The following log files are controlled by the debug parameter in the `AMConfig-`*instance-name*`.properties file in the` default directory `/etc/opt/SUNWam/config/` file:	
amconsole	Netfile, Netlet and Gateway Admin files
srapNetFile	NetFile information file
srapNetlet	Netlet information file
The following log files are controlled by the debug parameter `gateway.debug` in the `platform.conf`.*gateway-profile-name* file in the default directory `/etc/opt/SUNWps:`	
srapGateway.*gateway-profile-name*	Gateway information
Gateway_to_from_server.*gateway-profile-name*	
Gateway_to_from_browser.*gateway-profile-name*	
srapNetletProxy.*gateway-profile-name*	
srapRewriterProxy.*gateway-profile-name*	
rwproxy.log.*rewriter-proxy-instance-name*	Start and stop time of Rewriter Proxy
nlproxy.log.*netlet-proxy-instance-name*	Start and stop time of Netlet Proxy
gateway.log.*gateway.instance.name*	Start and stop time of the Gateway
The following Rewriter files are controlled by the debug parameter in the `AMConfig-`*instance-name*`.properties file in the` default directory `/var/opt/SUNWam/config/` file. See "Troubleshooting Using Debug Logs" on page 133 for more information.	

Table A-1 Informational and Debug Files

Filename	Contents
RuleSetInfo	All the rulesets which have been used for rewriting, are logged in this file.
Original Pages	Contains the page URI, resolveURI (if it is different than the page URI), content MIME, the ruleset that has been applied to the page, parser MIME, and the original content. Specific error/warning/messages related to parsing also appear in this file. In message mode full content is logged, in warning and error mode only exception occurred during rewriting are logged.
Rewritten Pages	Contains the page URI, resolveURI (if it is different than the page URI), content MIME, ruleset that has been applied to the page, parser MIME, and the rewritten content. This is filled when the debug mode is set to message.
Unaffected Pages	Contains a list the pages that were not modified.
URIInfo Pages	This file contains the URLS found and translated. Details of all the pages whose content remain same as original data is logged in this file. Details logged are: Page URI, MIME and Encoding data, rulesetID used for rewriting, and Parser MIME.

Appendix B

Configuration Attributes

This appendix describes attributes that you can configure for Portal Server Secure Remote Access through the Identity Server administration console from the Service Configuration for each Secure Remote Access component:

- Access List Service
- Gateway Service
- NetFile Service
- Netlet Service
- Proxylet Service

Access List Service

Table B-1 lists the Access List service attributes.

Table B-1 Access List Service Attributes

Attribute	Default Value	Description
Denied URLs		List of URLs that end-users cannot access through Gateway.
Allowed URLs	*	List of URLs that end-users can access through Gateway.
Single Sign On Disabled Hosts		Disables single sign-on for a list of hosts.
Enable Single Sign On per Session		Enables single sign-on for a session.
Allowed Authorization Levels	*	Indicates how much to trust an authentication.Use an asterisk to allow all authentication levels. For information on authentication levels, see the *Identity Server Administration Guide*.

Gateway Service

When you click the Gateway service, the right pane displays a button to create a new profile and a list of any gateway profiles that have been created.

If you click New, the next pane asks you to enter the new gateway profile name. You have the option to use the default template or a previously created gateway profile as the template.

If you click one of the listed gateway profile names, a list of tabs are presented. They are:

- Core
- Proxies
- Security
- Rewriter
- Logging

Core

Table B-2 lists the Gateway service core attributes.

Table B-2 Gateway Service Core Attributes

Attribute	Default Value	Description
Enable HTTPS Connections		Enables HTTPS connections.
HTTPS Port	443	Specifies the HTTPS port.
Enable HTTP Connections	*	Enables HTTP connections.
HTTP Port	80	Specifies the HTTP port.
Enable Rewriter Proxy	*	Enables secure HTTP traffic between Gateway and the intranet. Rewriter proxy and Gateway use the same gateway profile.
Rewriter Proxy List		List of Rewriter proxies. For multiple instances of Rewriter proxies enter the details for each in the form *host-name:port*
Enable Netlet	Checked	Enables security for TCP/IP (such as Telnet and SMTP), HTTP applications, and fixed port applications.
Enable Proxylet	Checked	Enables the download of Proxylet on a client machine.

Table B-2 Gateway Service Core Attributes

Attribute	Default Value	Description
Enable Netlet Proxy		Enhances security for Netlet traffic between Gateway and the intranet by extending the secure tunnel from the client, through Gateway to Netlet proxy residing on the intranet. Disable if you do not want to use applications with Portal Server.
Netlet Proxy Hosts		Lists Netlet proxy hosts, in the format: host hostname:port
Enable Cookie Management		Tracks and manages user sessions for all web sites that the user is permitted to access. (Does not apply to the cookies used by Portal Server to track Portal Server user sessions).
Enable HTTP Basic Authentication	Checked	Saves the username and password so that users need not re-enter their credentials when they revisit BASIC-protected web sites.
Enable Persistent HTTP Connections	Checked	Enables HTTP persistent connections at Gateway to prevent sockets being opened for every object (such as images and style sheets) in the web pages.
Maximum Number of Requests per Persistent Connection	10	Specifies the number of requests per persistent connection.
Timeout for Persistent Socket Connections	50	Specifies the amount of time that needs to lapse before sockets are closed.
Grace Timeout to Account for Turnaround Time	20	Specifies the grace amount of time for the request to reach Gateway after the browser has sent i and the time between gateway sending the response and the browser actually receiving it.
URLs to which User Session Cookie is Forwarded		Enables servlets and CGIs to receive Portal Server's cookie and use the APIs to identify the user.
Maximum Connection Queue Length	50	Specifies the maximum concurrent connections that Gateway can accept.
Gateway Timeout (milliseconds)	120000	Specifies the time interval in milliseconds before Gateway times out its connection with the browser.
Maximum Thread Pool Size	200	Specifies the maximum number of threads that can be pre-created in the Gateway thread pool.
Cached Socket Timeout	200000	Specifies the time interval in milliseconds before Gateway times out its connection with Portal Server.

Table B-2 Gateway Service Core Attributes

Attribute	Default Value	Description
Portal Servers		Specifies Portal Servers in the format `http://`*portal server name:port -number*`.` Gateway tries to contact each of the Portal Servers listed in a round robin manner to service the requests.
Server Retry Interval (minutes)	2	Specifies the time interval between requests to try to start Portal Server, Rewriter proxy or Netlet proxy after it becomes un-available (such as a crash or it was brought down).
Store External Server Cookies		Allows Gateway to store and manage cookies for any third party application or server that is accessed through Gateway.
Obtain Session Information from URL		Encodes session information as part of the URL, whether cookies are supported or not. Gateway uses this session information found in the URL for validation rather than using the session cookie that is sent from the client's browser.
Mark Cookies as secure		Marks cookies as secure. The Enable Cookie Management option must be enabled.

Proxies

Table B-3 lists the Gateway service proxies attributes.

Table B-3 Gateway Service Proxies Attributes

Attribute	Default Value	Description
Use Proxy		Enables usage of web proxies.
Use Webproxy URLs		Lists the URLs that Gateway needs to contact only through the webproxies listed in the Proxies for Domains and Subdomains list, even if the Use Proxy option is disabled.
Do Not Use Webproxy URLs		Lists URLs that Gateway can connect directly to.
Proxies for Domains and Subdomains	iportal.com sun.com	Specifies which proxy to use to contact specific subdomains in specific domains.
Proxy Password List		Specifies the user name and password required for Gateway to authenticate to a specified proxy server, if the proxy server requires authentication to access some or all the sites.

Table B-3 Gateway Service Proxies Attributes

Attribute	Default Value	Description
Enable Automatic Proxy Configuration Support		Specifies that the information provided in the Proxies for Domains and Subdomains field is to be ignored.
Automatic Proxy Configuration File location		Specifies the location of files to be used for PAC support.
Enable Netlet Tunneling via Web Proxy		Extends the secure tunnel from the client, through Gateway to the web proxy that resides in the intranet.

Security

Table B-4 lists the Gateway service security attributes.

Table B-4 Gateway Service Security Attributes

Attribute	Default Value	Description
Non-authenticated URLs	/portal/desktop/images /amserver/login_images /portal/desktop/css /amserver/jss /amconsole/console/css /portal/searchadmin/console/js /amconsole/console/js /amserver/css	Specifies URLs that do not need any authentication, such as directories that contain images.
Certificate-enabled Gateway hosts		Lists the certificate-enabled Gateway hosts.
Allow 40-bit Encryption		Allows 40-bit (weak) Secure Sockets Layer (SSL) connections. If you do not select this option, only 128-bit connections are supported.
Enable SSL Version 2.0	checked	Enables SSL version 2.0. Disabling SSL 2.0 means that browsers that support only the older SSL 2.0 will not be able to authenticate to SRA.This ensures a greater level of security.
Enable SSL Cipher Selection		Enables SSL cipher selection. You have the option of to support all the pre-packaged ciphers, or you can select the required ciphers individually. You can select specific SSL ciphers for each Gateway instance.

Table B-4 Gateway Service Security Attributes

Attribute	Default Value	Description
SSL2 Ciphers		Lists the SSL version 2 ciphers you can choose.
SSL3 Ciphers		Lists the SSL version 3 ciphers you can choose.
TLS Ciphers		Lists the TLS ciphers.
Enable SSL Version 3.0	checked	Enables SSL version 3.0. Disabling SSL 3.0 means that browsers that support only the SSL 3.0 will not be able to authenticate to SRA. This ensures a greater level of security.
Enable Null Ciphers		Enables null ciphers.
Trusted SSL Domains		Lists the trusted SSL domains.

Rewriter

The Rewriter tab has two subsections:

- Basic
- Advanced

Basic

Table B-5 lists the Gateway service Rewriter basic attributes.

Table B-5 Gateway Service Rewriter Attributes - Basic

Attribute	Default Value	Description
Enable Rewriting of All URIs		Specifies that any URL is rewritten without checking against the entries in the Proxies for Domains and Subdomains list.

Table B-5 Gateway Service Rewriter Attributes - Basic

Attribute	Default Value	Description
Map URIs to RuleSets	*://*.iportal.com*/portal/*|default_gateway_ruleset */portal/NetFileOpenFileServlet*|null_ruleset *|generic_ruleset REPLACE_WITH_IPLANET_MAIL_SERVER_NAME|iplanet_mail_ruleset REPLACE_WITH_EXCHANGE_SERVER_NAMEexchange_2000sp3_owa_ruleset *://*.iportal.com*/amconsole/*|default_gateway_ruleset REPLACE_WITH_INOTES_SERVER_NAME|inotes_ruleset http*://*/portal/NetFileController*|null_ruleset	Associates a domain with the ruleset using the Map URIs to RuleSets list. Rulesets are created under Portal Server Configuration in the Identity Server administration console.

Map Parser to MIME Types	JAVASCRIPT=application/x-java
	XML=text/xml
	HTML=text/html;text/htm;text/x-component;text/wml;text/vnd.wap.wml
	CSS=text/css
		Associates new MIME types with HTML, JAVASCRIPT, CSS or XML. Separate multiple entries with a semicolon or a comma.

URIs Not to Rewrite		Lists the URIs not to rewrite. Note: Adding #* to this list allows URIs to be rewritten, even when the href rule is part of the ruleset.
Default Domains		Resolves a host name to a default domain and subdomain. This is specified during installation

Advanced

Table B-6 lists the Gateway service Rewriter advanced attributes.

Table B-6 Gateway Service Rewriter Attributes - Advanced

Attribute	Default Value	Description
Enable MIME Guessing		Enables MIME guessing when MIME is not sent. You must add data to the Map Parser to URIs list box.
Map Parser to URI Mappings		Maps a parser to the URI. Multiple URIs are separated by a semicolon. For example HTML=*.html; *.htm;*Servlet means that Rewriter is used to rewrite the content for any page with a html, htm, or Servlet extension.
Enable Masking		Allows Rewriter to rewrite a URI so that the Intranet URL of a page is not seen.
Seed String for Masking		Specifies a seed string used for masking a URI. It is a random string generated by an masking algorithm.
URIs not to Mask		Specifies Internet URIs not to be mask. This is used when applications (such as an applet) require an Internet URI. For example if you added */Applet/Param* to the list box, the URL would not be masked if the content URI `http://abc.com/Applet/Param1.html` is matched in the ruleset rule.
Make Gateway protocol Same as Original URI Protocol		Enables Rewriter to use a consistent protocol to access the referred resources in the HTML content. This applies only to static URIs, not to dynamic URIs generated in Javascript.

Logging

Table B-7 lists the Gateway service logging attributes.

Table B-7 Gateway Service Logging Attributes

Attribute	Default Value	Description
Enable Logging		Enables logging.

Table B-7 Gateway Service Logging Attributes

Attribute	Default Value	Description
Enable per Session Logging		Enables capture of minimum log information such as Client Address, Request Type, and Destination Host.
Enable Detailed per Session Logging		Enables capture of detailed log information such as Client, Request Type, Destination Host, Type of Request, Client Requested URL, Client Post Data size, SessionID, Response Result code, and Complete Response size. Note: Enable per Session Logging must be enabled.
Enable Netlet Logging		Specifies if logging is enabled. If so the following information is captured: Start time, Source, Address, Source port, Server address, Server port(s), Stop time, Status (start or stop)

NetFile Service

When you click the NetFile Service, the right pane displays tabs. They are:

- Hosts
- Permissions
- View
- Operations
- General

Hosts

The Hosts tab has two subsections:

- Config
- Access

Config

Table B-8 lists the NetFile hosts configuration attributes.

Table B-8 NetFile Service Hosts Configuration Attributes

Attribute	Default Value	Description
OS Character Set	Unicode(UTF-8)	Specifies the character set used as the default encoding for communicating with hosts.
Host Detection Order	WIN, NETWARE, FTP, NFS	Specifies the host detection order.
Common Hosts		Specifies hosts to be available through NetFile to all remote NetFile users.
Default Domain		Specifies the default domain that NetFile needs to use to contact allowed hosts.
Default Windows Domain/Workgroup		Specifies the default Windows domain or workgroup which the users choose to access a Windows host.
Default WINS/DNS Server		Specifies the WINS/DNS server that NetFile uses to access windows hosts.

Access

Table B-9 lists the NetFile service hosts access attributes.

Table B-9 NetFile Service Hosts Access Attributes

Attribute	Default Value	Description
Allow Access to Windows Hosts	Checked	Allows access to windows hosts.
Allow Access to FTP Hosts	Checked	Allows access to FTP hosts.
Allow Access to NFS Hosts	Checked	Allows access to NFS hosts.
Allow Access to Netware Hosts	Checked	Allows access to Netware hosts.
Allowed Hosts	*	Specifies hosts that users can access through NetFile.
Denied Hosts		Specifies hosts that users cannot access through NetFile.

Permissions

If you disable these options after the user has started using NetFile, the change takes effect only if the user logs out of NetFile and logs in again.

Table B-10 lists the NetFile service permission attributes.

Table B-10 NetFile Service Permissions Attributes

Attribute	Default Value	Description
Allow File Rename	Checked	Allows users to rename files.
Allow File/Folder Deletion	Checked	Allows users to delete files and folders.
Allow File Upload	Checked	Allows users to upload files.
Allow File/Folder Download	Checked	Allows users to download files and folders.
Allow File Search	Checked	Allows users to search.
Allow File Mail	Checked	Allows file mailing.
Allow File Compression	Checked	Allows file compression.
Allow Changing User Id	Checked	Allows user to use a different ID.
Allow Changing Windows Domains	Checked	Allows users to change windows domains.

View

Table B-11 lists the NetFile Service view attributes.

Table B-11 NetFle Service View Attributes

Attribute	Default Value	Description
Window Size	700|400	Specifies the size of the NetFile window in pixels on the user's desktop. If you enter an invalid value, NetFile uses the default value.
Window Location	100|50	Specifies the location where the NetFile window displays on the user's desktop. If you enter an invalid value, NetFile uses the default value.

Operations

The Operations tab has the following subsections:

- Traffic
- Search
- Compression

Traffic

Table B-12 lists the NetFile service operations traffic attributes.

Table B-12 NetFile Service Operations - Traffic Attributes

Attribute	Default Value	Description
Temporary Directory Location	/tmp	Specifies a temporary directory for various NetFile file operations. Ensure that the ID with which the web server is running (such as nobody or noaccess) has rwx permissions for the specified directory. Also ensure that the ID has rx permissions for the entire path to the required temporary directory. You may want to create a separate temporary directory for NetFile. If you specify a temporary directory that is common to all modules of the Portal Server, the disk may quickly run out of space. NetFile will not work if the temporary directory has no space.
File Upload Limit (MB)	5	Specifies the maximum size of the files that can be uploaded. If you enter an invalid value, NetFile resets the value to the default. Ensure that you type an integer value. You can specify different file upload size limits for different users.

Search

Table B-13 lists the NetFile service operations search attributes.

Table B-13 NetFile Service Operations - Search Attributes

Attribute	Default Value	Description
Search Directories Limit	100	Specifies the maximum number of directories that will be searched in a single search operation.

Compression

Table B-14 lists the NetFile service operations compression attributes.

Table B-14 NetFile Service Operations - Compression Attributes

Attribute	Default Value	Description
Default Compression Type	Zip	Specifies either Zip or Gzip compression type.
Default Compression Level	6	Specifies the compression level, a number between 1 and 9.

General

Table B-15 lists the Netfile service general attributes.

Table B-15 NetFile Service - General Attribute

Attribute	Default Value	Description
MIME-types Configuration File Location	/opt/S1PS62/SUNWps/samples/config/netfile	Specifies the response content type to send to the client browser.

Netlet Service

Table B-16 lists the Netlet service attributes.

Table B-16 Netlet Service Attributes

Attribute	Default Value	Description
Netlet Rules		Choose to add or delete a rule.
If you add a rule, the following nine attributes are necessary:		
--Rule Name		Specifies a unique name for the rule.
--Encryption Ciphers		Specifies the required ciphers.
--URL		Specifies the URL to the application to be invoked.
--Download Applet		Specifies if an applet needs to be downloaded. If an applet is used, the syntax in the associated edit box is: *local-port:server-host:server-port*
--Extend Session		Ensures that the Portal Server session time is extended while the Netlet session corresponding to this rule is running.

Table B-16 Netlet Service Attributes

Attribute	Default Value	Description
--Map Local Port to Destination Server Port		Specifies local port, target host and target ports. After entering those values (in the next three rows of this table), click add to make them appear in the list.
--Local Port		Specifies the local port on which Netlet listens. For an FTP rule, the local port value must be 30021.
--Destination Hosts		Static rules contain the host name of the destination machine for the Netlet connection. Dynamic rules contain the word "TARGET".
-- Destination Ports		Specifies the port on the destination host.
Default Native VM Cipher		Specifies the default cipher for the Netlet rules. This is useful when using existing rules that did not include the cipher as a part of the rule.
Default Java Plugin Cipher		Specifies the default cipher for the Netlet rules. This is useful when using existing rules that did not include the cipher as a part of the rule.
Default Loopback Port	58000	Specifies the port to be used on the client when applets are downloaded through Netlet. The default value can be overridden in the Netlet rules.
Reauthenticate for Connections		Ensures that users enter the Netlet password each time a Netlet connection needs to be established.
Display Warning Popup for Connections	Checked	Displays a message when the user runs the application over Netlet, and also when an intruder tries to gain access to the desktop through the listen port.
Display Checkbox in Port Warning Dialog	Checked	Provides the user with the option to supress the Warning Dialog Popup when Netlet tries to connect to the destination host on the user's standard Portal Desktop.
Keep Alive Interval (minutes)	0	If the client is connecting to the Gateway through a web proxy, then idle Netlet connections are disconnecteed due to proxy timeout. To prevent this, give a value less than the proxy timeout for this parameter.
Terminate Netlet at Portal Logout	Checked	Ensures that all connections are terminated when a user logs out of the Portal Server.
Access to Netlet Rules	*	Define access to specific Netlet rules for certain organizations, roles or users.

Table B-16 Netlet Service Attributes

Attribute	Default Value	Description
Deny Netlet Rules		Denies access to specific Netlet rules for certain organizations, roles or users.
Allowed Hosts	*	Defines access to specific hosts for certain organizations, roles or users.
Denied Hosts		Denies access to specific hosts within an organization.

Proxylet Service

Table B-17 lists the Proxylet service attributes.

Table B-17 Proxylet Service Attributes

Attribute	Default Values	Description
Download Proxylet Applet Automatically	127.0.0.1	When the checkbox is checked, Proxylet is downloaded to the client machine when the user logs on.
Default Proxylet Applet Bind IP	127.0.0.1	The IP address where the Proxylet Applet resides.
Default Proxylet Applet Port	58080	This is the port where Proxylet listens.

Appendix C

Country Codes

The following table lists the two-letter country codes that you need to specify during certificate administration.

Table C-1 Two-letter Country Codes *(1 of 10)*

ad	Andorra, Principality of
ae	United Arab Emirates
af	Afghanistan, Islamic State of
ag	Antigua and Barbuda
ai	Anguilla
al	Albania
am	Armenia
an	Netherlands Antilles
ao	Angola
aq	Antarctica
ar	Argentina
arpa	Old style Arpanet
as	American Samoa
at	Austria
au	Australia
aw	Aruba
az	Azerbaidjan

Table C-1 Two-letter Country Codes *(2 of 10)*

ba	Bosnia-Herzegovina
bb	Barbados
bd	Bangladesh
be	Belgium
bf	Burkina Faso
bg	Bulgaria
bh	Bahrain
bi	Burundi
bj	Benin
bm	Bermuda
bn	Brunei Darussalam
bo	Bolivia
br	Brazil
bs	Bahamas
bt	Bhutan
bv	Bouvet Island
bw	Botswana
by	Belarus
bz	Belize
ca	Canada
cc	Cocos (Keeling) Islands
cf	Central African Republic
cd	Congo, The Democratic Republic of the
cg	Congo
ch	Switzerland
ci	Ivory Coast (Cote D'Ivoire)
ck	Cook Islands

Table C-1 Two-letter Country Codes *(3 of 10)*

cl	Chile
cm	Cameroon
cn	China
co	Colombia
com	Commercial
cr	Costa Rica
cs	Former Czechoslovakia
cu	Cuba
cv	Cape Verde
cx	Christmas Island
cy	Cyprus
cz	Czech Republic
de	Germany
dj	Djibouti
dk	Denmark
dm	Dominica
do	Dominican Republic
dz	Algeria
ec	Ecuador
edu	Educational
ee	Estonia
eg	Egypt
eh	Western Sahara
er	Eritrea
es	Spain
et	Ethiopia
fi	Finland

Table C-1 Two-letter Country Codes *(4 of 10)*

fj	Fiji
fk	Falkland Islands
fm	Micronesia
fo	Faroe Islands
fr	France
fx	France (European Territory)
ga	Gabon
gb	Great Britain
gd	Grenada
ge	Georgia
gf	French Guyana
gh	Ghana
gi	Gibraltar
gl	Greenland
gm	Gambia
gn	Guinea
gov	USA Government
gp	Guadeloupe (French)
gq	Equatorial Guinea
gr	Greece
gs	S. Georgia and S. Sandwich Isls.
gt	Guatemala
gu	Guam (USA)
gw	Guinea Bissau
gy	Guyana
hk	Hong Kong
hm	Heard and McDonald Islands

Table C-1 Two-letter Country Codes *(5 of 10)*

hn	Honduras
hr	Croatia
ht	Haiti
hu	Hungary
id	Indonesia
ie	Ireland
il	Israel
in	India
int	International
io	British Indian Ocean Territory
iq	Iraq
ir	Iran
is	Iceland
it	Italy
jm	Jamaica
jo	Jordan
jp	Japan
ke	Kenya
kg	Kyrgyz Republic (Kyrgyzstan)
kh	Cambodia, Kingdom of
ki	Kiribati
km	Comoros
kn	Saint Kitts and Nevis Anguilla
kp	North Korea
kr	South Korea
kw	Kuwait
ky	Cayman Islands

Table C-1 Two-letter Country Codes *(6 of 10)*

kz	Kazakhstan
la	Laos
lb	Lebanon
lc	Saint Lucia
li	Liechtenstein
lk	Sri Lanka
lr	Liberia
ls	Lesotho
lt	Lithuania
lu	Luxembourg
lv	Latvia
ly	Libya
ma	Morocco
mc	Monaco
md	Moldavia
mg	Madagascar
mh	Marshall Islands
mil	USA Military
mk	Macedonia
ml	Mali
mm	Myanmar
mn	Mongolia
mo	Macau
mp	Northern Mariana Islands
mq	Martinique (French)
mr	Mauritania
ms	Montserrat

Table C-1 Two-letter Country Codes *(7 of 10)*

mt	Malta
mu	Mauritius
mv	Maldives
mw	Malawi
mx	Mexico
my	Malaysia
mz	Mozambique
na	Namibia
nato	NATO (this was purged in 1996 - see hq.nato.int)
nc	New Caledonia (French)
ne	Niger
net	Network
nf	Norfolk Island
ng	Nigeria
ni	Nicaragua
nl	Netherlands
no	Norway
np	Nepal
nr	Nauru
nt	Neutral Zone
nu	Niue
nz	New Zealand
om	Oman
org	Non-Profit Making Organisations (sic)
pa	Panama
pe	Peru
pf	Polynesia (French)

Table C-1 Two-letter Country Codes *(8 of 10)*

pg	Papua New Guinea
ph	Philippines
pk	Pakistan
pl	Poland
pm	Saint Pierre and Miquelon
pn	Pitcairn Island
pr	Puerto Rico
pt	Portugal
pw	Palau
py	Paraguay
qa	Qatar
re	Reunion (French)
ro	Romania
ru	Russian Federation
rw	Rwanda
sa	Saudi Arabia
sb	Solomon Islands
sc	Seychelles
sd	Sudan
se	Sweden
sg	Singapore
sh	Saint Helena
si	Slovenia
sj	Svalbard and Jan Mayen Islands
sk	Slovak Republic
sl	Sierra Leone
sm	San Marino

Table C-1 Two-letter Country Codes *(9 of 10)*

sn	Senegal
so	Somalia
sr	Suriname
st	Saint Tome (Sao Tome) and Principe
su	Former USSR
sv	El Salvador
sy	Syria
sz	Swaziland
tc	Turks and Caicos Islands
td	Chad
tf	French Southern Territories
tg	Togo
th	Thailand
tj	Tadjikistan
tk	Tokelau
tm	Turkmenistan
tn	Tunisia
to	Tonga
tp	East Timor
tr	Turkey
tt	Trinidad and Tobago
tv	Tuvalu
tw	Taiwan
tz	Tanzania
ua	Ukraine
ug	Uganda
uk	United Kingdom

Table C-1 Two-letter Country Codes *(10 of 10)*

um	USA Minor Outlying Islands
us	United States
uy	Uruguay
uz	Uzbekistan
va	Holy See (Vatican City State)
vc	Saint Vincent and Grenadines
ve	Venezuela
vg	Virgin Islands (British)
vi	Virgin Islands (USA)
vn	Vietnam
vu	Vanuatu
wf	Wallis and Futuna Islands
ws	Samoa
ye	Yemen
yt	Mayotte
yu	Yugoslavia
za	South Africa
zm	Zambia
zr	Zaire
zw	Zimbabwe

Glossary

Refer to the Java Enterprise System Glossary (http://docs.sun.com/doc/816-6873) for a complete list of terms that are used in this documentation set.

Index