Administrator’s Guide

Sun ONE™ Portal Server, Secure Remote Access 6.0

816-6421-10

Contents

About This Guide

This guide explains how to administer the Sun ONE Portal Server, Secure Remote Access.

The Sun ONE™ Portal Server, Secure Remote Access 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.

Secure Remote Access runs on the Solaris™ 8.0 Operating Environment. This guide contains instructions for configuring and administering the Secure Remote Access.

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 Sun ONE Portal Server, Secure Remote Access.

You need root access to the required machines for installing the various components of Sun ONE Portal Server, Secure Remote Access. 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 Sun ONE Portal Server, Secure Remote Access, you need to be familiar with the following:

- Basic Solaris administrative procedures
- LDAP
- Sun ONE Directory Server
- iPlanet Directory Server Access Management Edition
- Sun ONE Web Server
- Sun ONE Portal Server

How This Book is Organized

This book contains the following chapters and appendices:

About This Guide (this chapter)

Chapter 1, “Introduction to Sun ONE Portal Server, Secure Remote Access”

This chapter introduces you to the Secure Remote Access and describes the various components.

Chapter 2, “Administering the Gateway“

This chapter describes the gateway admin console and how to configure the gateway attributes.

Chapter 3, “Configuring the Netlet“

This chapter describes how to administer the Netlet service.

Chapter 4, “Configuring NetFile“

This chapter describes how to administer the NetFile service.

Chapter 5, “Configuring the Rewriter“

This chapter describes the Rewriter and provides sample rules and best practices.

Chapter 6, “Working With Certificates“

This chapter provides information on certificate management, and tells you how you can install self-signed certificates, or certificates from a Certificate Authority.

Chapter 7, “Errors and Troubleshooting“

This chapter lists some common errors that you may run into, and tells you how to troubleshoot such problems.

Chapter , “Configuring the SSL Accelerator“

This chapter describes how you can configure the SSL Accelerator for the Secure Remote Access.

Appendix B, “Country Codes

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

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.

Bold Monospaced Font

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

```
./pssetup
************************************************************************

Sun ONE(TM) Portal Server (6.0 release)

************************************************************************

Installation log at /var/sadm/install/logs/pssetup.13343/install.log

This product will run without a license. However, you must either
purchase a Binary Code License from, or accept the terms of a Binary
Software Evaluation license with, Sun Microsystems, to legally use
this product.

Do you accept? yes/[no] Starting install wizard in graphical mode
```

In this example, **./pssetup** is what you would type from the command line and the rest is what would appear as a result.

Italicized Font

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

Square or Straight Brackets

Square (or straight) brackets [] are used to enclose optional parameters. For example, in this document you will see the usage for the 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

Other documents in the Sun ONE Portal Server, Secure Remote Access 6.0 documentation set are:

- *Sun ONE Portal Server, Secure Remote Access 6.0 Installation Guide*
- *Sun ONE Portal Server, Secure Remote Access 6.0 Attribute Reference Guide*

  (This online help is available from the administration console when you click the Documentation link, and then the SRAP link).

- *Sun ONE Portal Server, Secure Remote Access 6.0 Netlet Online Help*
- *Sun ONE Portal Server, Secure Remote Access 6.0 NetFile Java1 Online Help*
- *Sun ONE Portal Server, Secure Remote Access 6.0 NetFile Java2 Online Help*

Where to Find This Guide Online

The `docs.sun.com` web site enables you to access Sun technical documentation online. You can browse the `docs.sun.com` archive or search for a specific book title or subject. The URL is `docs.sun.com`.

Chapter 1

Introduction to Sun ONE Portal Server, Secure Remote Access

This chapter describes the Sun ONE Portal Server, Secure Remote Access product, the relationship between Sun ONE Portal Server and Secure Remote Access, the components that constitute the Secure Remote Access, and provides information on administering and configuring Secure Remote Access.

This chapter has the following sections:

- Secure Remote Access
- Administering the Sun ONE Portal Server, Secure Remote Access
- Components of the Secure Remote Access
- Configuring the Secure Remote Access
- Configuring URL Access Control
- Managing Single Sign-On
- Customizing the Access List Interface

Secure Remote Access

The Sun ONE™ Portal Server, Secure Remote Access 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.

The Secure Remote Access 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 the Sun ONE Portal Server ensures that users receive secure encrypted access to the content and services that they have permission to access.

The Sun ONE Portal Server, Secure Remote Access is targeted towards enterprises deploying highly secure remote access portals. These portals emphasize security, protection, and privacy of intranet resources. The Secure Remote Access architecture is well suited to these types of portals. The Gateway, NetFile, and Netlet features of the Secure Remote Access enable 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-Secure Remote Access services such as Session, Authentication, and the Desktop reside behind the DMZ in the secured intranet. Communication from the client browser to the gateway is encrypted using HTTPS. Communication from the gateway to the server and intranet resources can be either HTTP or HTTPS.

The Netlet and NetFile applets are downloaded to the client machine, while the support files may reside either on the gateway or on the Sun ONE Portal Server server.

Relation Between Sun ONE Portal Server and Secure Remote Access

Sun ONE Portal Server can function in two modes - open and secure.

Open Mode

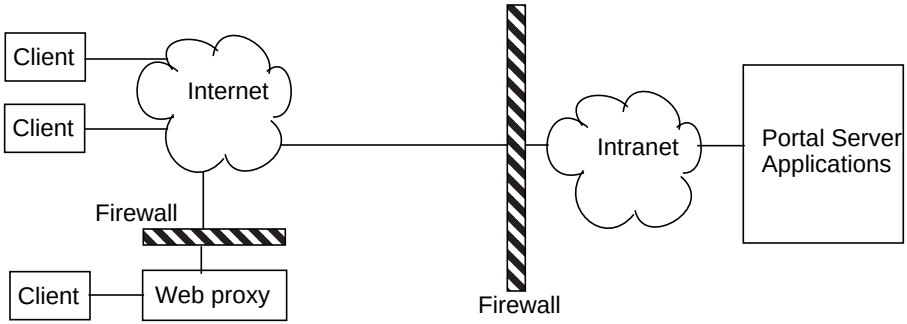
In open mode, the Sun ONE Portal Server is installed without the Secure Remote Access. Although HTTPS communication is possible in this mode, secure remote access is not possible. This means that users cannot access remote file systems and applications.

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 as compared to the secure mode.

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

Figure 1-1 Sun ONE Portal Server in the Open Mode



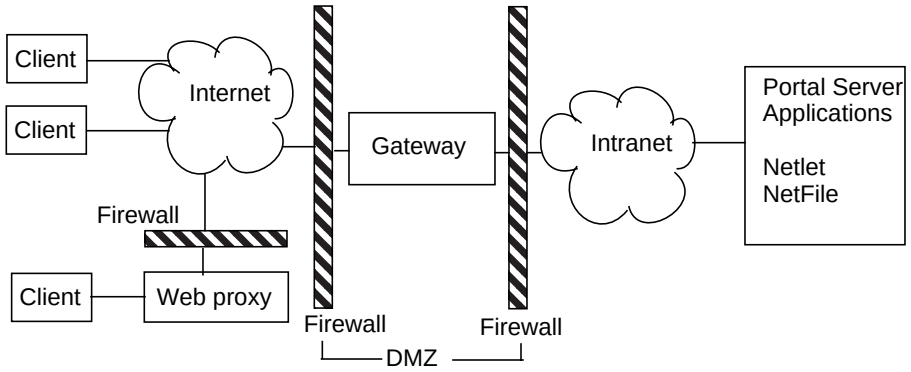
Secure Mode

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

The gateway resides in the demilitarized zone (DMZ). The 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 Sun ONE Portal Server services such as Session, Authentication, and the 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 the Sun ONE Portal Server with the Secure Remote Access. SSL is used to encrypt the connection between the client and the Sun ONE Portal Server gateway over the Internet. SSL can also be used to encrypt the connection between the gateway and the server. The presence of a gateway between the intranet and the internet extends the secure path between the client and the Portal Server.

Figure 1-2 Sun ONE Portal Server in the Secure Mode (with Secure Remote Access)



Additional servers and gateways can be added for site expansion. The components of the Secure Remote Access can be configured in various ways based on the business requirement.

Administering the Sun ONE Portal Server, Secure Remote Access

Secure Remote Access has two interfaces for administration:

- iPlanet Directory Server Access Management Edition Administration console
- Command-Line Utilities

Most administration tasks are performed through the web-based 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.

Components of the Secure Remote Access

Secure Remote Access has four major components:

- Gateway

- Netlet
- NetFile
- Rewriter

Gateway

The Secure Remote Access 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.

See Chapter 2, Administering the Gateway for details.

Netlet

Netlet facilitates the running of popular or company-specific applications on remote desktops in a secure manner. After you implement the 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 3, Configuring the Netlet for details.

NetFile

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

See Chapter 4, Configuring NetFile for details.

Rewriter

The Rewriter enables end users to browse the intranet, and also makes links and other URL references on those pages operate correctly. The rewriter prepends the gateway URL in the location field of the web browser, thereby redirecting content requests through the gateway.

See Chapter 5, Configuring the Rewriter for details.

Configuring the Secure Remote Access

You can configure attributes related to the Secure Remote Access at various levels. See the iPlanet Directory Server Access Management Edition Administrator's Guide for details.

The components of the Secure Remote Access are made available through four services:

- Access List

  This service allows you to allow or restrict access to specific URLs, and also manage the single sign-on feature. See Configuring URL Access Control and Managing Single Sign-On 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 2, Administering 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 4, 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 3, Configuring the Netlet for more information.

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

Restart the gateway to ensure that updated profile attributes (belonging to the gateway or any other service) are used by the gateway. See Restarting the Gateway in Chapter 2, Administering the Gateway.

Configuring URL Access Control

As a Secure Remote Access administrator, you can allow or deny access to the end user through the gateway for specific URLs.

NOTE When you install the Secure Remote Access, 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.

Setting up a URL Deny List

You can specify the list of URLs that end users cannot access through the gateway using this field.

The gateway checks the URL Deny List before checking the URL Allow List.

You can configure this attribute at the organization, role and user levels.

To Set up the URL Deny List

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the arrow next to Access List under SRAP Configuration.

   The Access List page appears.
4. Specify the URL for which you want to deny access through the gateway in the URL Deny List field, and click Add. The format for entering the URL is:

   `http://abc.siroe.com`

   The URL is added to the URL Deny 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.
5. Click Save to record the changes.

Setting up a URL Allow 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 URL Deny List. In the same way, if you want to allow access only to specific URLs, leave the URL Deny List blank, and specify the required URLs in the URL Allow List.

The gateway checks the URL Deny List before checking the URL Allow List.

You can configure this attribute at the organization, role and user levels.

To Set up the URL Allow List

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the arrow next to Access List under SRAP Configuration.

   The Access List page appears.
4. Specify the URL for which you want to allow access through the gateway in the URL Allow List field, and click Add. The format for entering the URL is:

   `http://abc.siroe.com`

   The URL is added to the URL Allow List.

NOTE The URL Allow List has a * by default which means that all URLs can be accessed through the gateway.

5. Click Save to record the changes.

Managing Single Sign-On

The Access List service in the Secure Remote Access 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 admin console should be enabled. See Enabling HTTP Basic Authentication in Chapter 2, Administering the Gateway.

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.

You can configure these attributes at the organization, role and user levels. A user can also configure these attributes using the limited admin console.

To Disable SSO for Hosts

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the arrow next to Access List under SRAP Configuration.

   The Access List page appears.
4. Specify the hosts for which you want to disable SSO in the Hosts for which SSO is disabled field, and click Add.

   Specify the host name in the format `abc.siroe.com`.

   The hostname is added to the list.
5. Click Save to record the changes.

To Enable SSO per Session

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the arrow next to Access List under SRAP Configuration.

   The Access List page appears.
4. Select the Enable SSO per session check box.
5. Click Save to record the changes.

Customizing the Access List Interface

Edit the access list properties file to change the labels on the access list user interface in the iPlanet Directory Server Access Management Edition admin console. Edit the file:

InstallDir/SUNWam/locale/srapGatewayAccess.properties

The following sample shows the lines that can be customized:

```
sunPortalGatewayAccessServiceDescription=Access List
d02=URL Allow List
d05=Policy to Enable/Disable SSO
d04=Enable SSO per Session
d03=Hosts for Which SSO is Disabled
d01= URL Deny List
```

You can change the label text, but not the number associated with the text.

Chapter 2

Administering the Gateway

This chapter describes gateway related concepts, and all the basic configurations required for the smooth running of the gateway. This chapter covers all the attributes in the gateway service.

The following topics are covered:

- Overview of the Gateway
- Creating a Gateway Profile
- Starting and Stopping the Gateway
- Creating Multiple Instances of a Gateway
- Configuring a Proxy to Contact the Portal Server
- Restarting the Gateway
- Configuring the Gateway Attributes
- Authentication Chaining
- Disabling Browser Caching
- Running the Gateway in the chroot Environment
- Customizing the Gateway User Interface
- Understanding the platform.conf File

Overview of the Gateway

The Secure Remote Access 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 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 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. You can:

- 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 iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the arrow next to Gateway under SRAP Configuration.

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

   The Create New Gateway Profile page appears.
5. Specify a name for the new profile in the "Enter the name of new Gateway Profile" field.
6. Select the profile based on which you want to create the new profile, from the "Copy the existing configuration of" drop-down list.

   By default, any new profile that you create is based on the pre-packaged "default" profile. If you have created any 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 and you are returned to the Gateway page, in which the new profile is listed.

   See Configuring the Gateway Attributes to configure individual gateway attributes.
8. Restart the gateway with this profile name if you want the changes to take effect. See “Restarting the Gateway“ for more information.

Starting and Stopping the Gateway

By default, the gateway starts as user noaccess.

To Start the Gateway

After installing the gateway, and creating the required profile, run the following command to start the gateway:

InstallDir`/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.

If you have multiple gateway instances, use:

InstallDir`/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.

Run the following command to check if the gateway is running on the specified port:

`netstat -a | grep` *port number*

NOTE The default gateway port is 443.

To Stop the Gateway

InstallDir`/SUNWps/bin/gateway -n` *new profile name* `stop`

If you have multiple gateway instances, use:

InstallDir`/SUNWps/bin/gateway stop`

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

Creating Multiple Instances of a Gateway

Use the script `gwmultiinstance` to create a new instance of the gateway. You can create a new instance in the following scenarios:

- Creating a New Instance on a Portal Server Node
- Creating a New Instance on a non-Portal Server Node

Creating a New Instance on a Portal Server Node

1. Login as root and navigate to the following directory:

   InstallDir`/SUNWps/bin`

2. Run the multi instance script:

   ```
   ./gwmultiinstance
   ```

Table 2-1 lists the questions that the script asks. The first column lists the question, the second column lists the default value, and the third column has the description.

Table 2-1 Checklist for creating a new gateway instance on a Portal Server node

Parameter	Default Value	Description
New gateway uses Portal Server instance running on this node	y	The script detects an existing instance of the Portal Server and asks this question. Specify y if you want the gateway to run with the Portal Server instance on the same node. Choose n if you want to use a different instance of the Portal Server. In this case, the Creating a New Instance on a non-Portal Server Node checklist applies.
Portal Server instance is the default one created during installation	y	Specify which instance of the Portal Server you want the new gateway instance to work with. If you choose y, the default Portal Server instance that is created during installation is used with the new gateway. If you choose n, you will be asked to specify the name of the required Portal Server instance.

Table 2-1 Checklist for creating a new gateway instance on a Portal Server node

Parameter	Default Value	Description
New Portal Server instance created	y	This question is asked only if you have chosen not to use the default Portal Server instance. Specify whether the Portal Server instance that you want to use with your new gateway instance has already been created. If you choose n, you are asked to create the instance first, and the script aborts.
Name of the new Portal Server instance	*Portal Server instance name*	This question is asked only if you have chosen not to use the default Portal Server instance. Specify the name of the Portal Server instance that you want the new gateway instance to use.
Port on which the new Portal Server instance listens		This question is asked only if you have chosen not to use the default Portal Server instance. Specify the port on which the new Portal Server instance listens.
Deployment URI	`/portal`	This question is asked only if you have chosen not to use the default Portal Server instance. Specify the deployment URI of the new Portal Server instance.
Name of the new gateway instance		Specify the name of the new gateway instance that you want to create.
Protocol to be used by the gateway	`https`	Specify whether you want the gateway to operate in HTTP or HTTPS mode.
Port on which the new gateway instance listens		Specify the port on which the new gateway instance needs to listen. Ensure that this port has not been specified for any other gateway instance.

Table 2-1 Checklist for creating a new gateway instance on a Portal Server node

Parameter	Default Value	Description

Create certificate database for new gateway instance	y	When the gateway is installed, a default certificate database is created as follows:
		`/etc/opt/SUNWps/cert/default`
		The default directory has the following database files:
		`cert7.db, key3.db, secmod.db`
		You can choose to use the same certificate database for various instances of the gateway, or create and assign different certificate databases to different instances.
		You can assign only one certificate to one instance of the gateway. If you want to assign different certificates to different organizations, you need to create multiple instances of the gateway.
		Choose y to create a new certificate database for the new gateway instance.

Create self-signed certificate	y	This question is asked only if you have chosen to create a new certificate database. Choose y to create a self-signed certificate. You are asked a series of questions in order to create this certificate. If you choose n, you can create a self-signed certificate later. See Generating Self-signed Certificates in Chapter 4, Installing SSL Certificates in the *Sun ONE Portal Server, Secure Remote Access 6.0 Installation Guide* for details.
Name of the organization Name of the division Name of the city or locality Name of the state or province Two-letter country code Password for certificate database		These details are asked only if you have chosen y to create a self-signed certificate in the previous question.

Table 2-1 Checklist for creating a new gateway instance on a Portal Server node

Parameter	Default Value	Description
Created a profile for the new gateway instance	y	You are asked if you have already created a profile for the new gateway instance. See To Create a Gateway Profile for details on creating a new gateway profile.
Start the new gateway instance after installation	y	This question is asked only if you choose y for the previous question, that is, you have already created a profile for the new gateway instance. If you have not created a profile, the script reminds you to create one before starting the gateway.

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

InstallDir`/SUNWps/bin/gateway -n` *test* `start`

where `test` is the profile name of the new gateway instance

Creating a New Instance on a non-Portal Server Node

1. Login as root and navigate to the following directory:

   InstallDir`/SUNWps/bin`

2. Run the multi instance script:

   `./gwmultiinstance`

Table 2-2 lists the questions that the script asks. The first column lists the question, the second column lists the default value, and the third column has the description.

Table 2-2 Checklist for creating a new gateway instance on a non- Portal Server node

Parameter	Default Value	Description
Host name of the Directory Server	*hostname*	This is the machine on which the Directory Server is installed. Specify the machine on which Directory Server was installed for the Portal Server.

Table 2-2 Checklist for creating a new gateway instance on a non- Portal Server node

Parameter	Default Value	Description
Sub-domain name for *hostname*		This is the sub-domain to which the Directory Server belongs. Specify the sub-domain of the machine on which the Directory Server was installed for the Portal Server.
Domain name for *hostname*		This is the domain to which the Directory Server machine belongs. Specify the domain of the machine on which the Directory Server was installed for the Portal Server.
Port used to access the Directory Server	389	This is the port which the Portal Server uses to access the Directory Server. Specify the Directory Server port specified during the Portal Server installation.
Root suffix of the directory tree	o=isp	This is the default top level organization. Any new organization that you create is created under this organization.
Organization name		This is the name of the default organization that is created.
Hostname of Portal Server	*Portal Server hostname*	This is the hostname of the Portal Server.
sub-domain for *Portal Server hostname*		This is the sub-domain to which the Portal Server machine belongs.
domain name for *Portal Server hostname*		This is the domain to which the Portal Server machine belongs.
Port used to access Portal Server	80	This is the port used to access the Portal Server.
Protocol used to access Portal Server	http	Specify the protocol that is used to access the Portal Server.
DSAME server deployment URI	/amserver	This is the DSAME deployment URI. Do not change this value.
Portal Server deployment URI	/portal	Specify the deployment URI of the new Portal Server instance.
Name of the new gateway instance		Specify the name of the new gateway instance that you want to create.

Table 2-2 Checklist for creating a new gateway instance on a non- Portal Server node

Parameter	Default Value	Description
Protocol to be used by the gateway	`http`	Specify whether you want the gateway to operate in HTTP or HTTPS mode.
Port on which the new gateway instance listens		Specify the port on which the new gateway instance needs to listen. Ensure that this port has not been specified for any other gateway instance.

Create certificate database for new gateway instance	y	When the gateway is installed, a default certificate database is created as follows:
		`/etc/opt/SUNWps/cert/default`
		The default directory has the following database files:
		`cert7.db, key3.db, secmod.db`
		You can choose to use the same certificate database for various instances of the gateway, or create and assign different certificate databases to different instances.
		You can assign only one certificate to one instance of the gateway. If you want to assign different certificates to different organizations, you need to create multiple instances of the gateway.
		Choose y to create a new certificate database for the new gateway instance.
		If you choose n, the default certificate database is used.

Create self-signed certificate	y	This question is asked only if you have chosen to create a new certificate database. Choose y to create a self-signed certificate. You are asked a series of questions in order to create this certificate. If you choose n, you can create a self-signed certificate later. See Generating Self-signed Certificates in Chapter 4, Installing SSL Certificates in the *Sun ONE Portal Server, Secure Remote Access 6.0 Installation Guide* for details.

Table 2-2 Checklist for creating a new gateway instance on a non- Portal Server node

Parameter	Default Value	Description
Name of the organization Name of the division Name of the city or locality Name of the state or province Two-letter country code Password for certificate database		These details are asked only if you have chosen y to create a self-signed certificate in the previous question.
Created a profile for the new gateway instance	y	You are asked if you have already created a profile for the new gateway instance. See To Create a Gateway Profile for details on creating a new gateway profile.
Start the new gateway instance after installation	y	This question is asked only if you choose y for the previous question, that is, you have already created a profile for the new gateway instance. If you have not created a profile, the script reminds you to create one before starting the gateway.

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

InstallDir`/SUNWps/bin/gateway -n` *test* `start`

where `test` is the profile name of the new gateway instance

Configuring a Proxy to Contact the Portal Server

You can configure the gateway to obtain profile information through a proxy if a direct connection is not available between the gateway and the Portal Server.

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

   `/etc/opt/bin/platform.conf.`*profilename*

2. Add the following entries:

`http.proxyHost=`*proxy hostname*

`http.proxyPort=`*proxy port*

`http.proxySet=true`

3. Restart the gateway to use the specified proxy for Profile Service requests made to the server.

   InstallDir`/SUNWps/bin/gateway -n` *profilename* `start`

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 using:

InstallDir`/SUNWps/bin/gateway -n` *new profilename* `start`

Configuring the watchdog Process to Restart the Gateway

You can schedule a watchdog process to monitor the gateway and restart it if it goes down.

To Configure the watchdog to Restart the Gateway

In a terminal window, connect as root on the gateway machine and do the following:

Start the watchdog process using:

InstallDir/SUNWps/bin/gateway watchdog on

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

NOTE You need to ensure that the gateway is running before enabling the watchdog.

To stop the gateway, ensure that the watchdog process is stopped first.

The watchdog process monitors all running instances of a gateway on a particular machine.

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 * * * * InstallDir/bin/checkgw /var/opt/SUNWps/.gw. 5 > /dev/null
2>&1
```

See the man pages for `crontab` to configure the `crontab` entries.

Configuring the Gateway Attributes

This section lists the attributes that you need to configure for the gateway to function as required.

NOTE Click Documentation at the top right corner of the iPlanet Directory Server Access Management Edition admin console, and click SRAP Help for a quick reference on all the Secure Remote Access attributes.

- Running in HTTP and HTTPS Modes
- Enabling the Rewriter Proxy
- Disabling Netlet
- Enabling Netlet Proxy
- Managing Proxies
- Specifying URLS for Webproxies
- Specifying URLs for which Proxies Should not be Used
- Specifying the Default Domain and Subdomain
- Specifying Proxy Authentication Information
- Configuring Cookies
- Enabling HTTP Basic Authentication
- Configuring Persistent HTTP Connections
- Forward Cookie Configuration
- Specifying URLs that Bypass Authentication
- Specifying the Maximum Connection Queue Length
- Specifying the Gateway Timeout
- Specifying the Maximum Number of Threads
- Specifying the Cached Socket Timeout
- Configuring Personal Digital Certificate (PDC) Authentication
- Allowing 40-bit Browser Connections

- Disabling SSL Version 2.0
- Enabling Cipher Selection
- Specifying the List of Configured Portal Servers
- Specifying the Retry Interval for the Portal Server
- Enabling Logging
- Enabling Netlet Logging

Running in HTTP and HTTPS Modes

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. The benefits of doing this are performance related, since there is an overhead involved in managing SSL sessions and encrypting and decrypting the SSL traffic. Eliminating these steps speeds gateway performance.

To Configure the Gateway to Run in HTTP or HTTPS Mode

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view from the Administration Console.
3. Click the arrow next to Gateway under SRAP Configuration.

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

   The Edit Gateway Profile page appears.
5. Do the following:
   - 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. From a terminal window, restart the gateway using:

   InstallDir/SUNWps/bin/gateway -n *gateway profile name* start

Enabling the Rewriter Proxy

The rewriter proxy needs to be installed only on a Portal Server node.

Using the rewriter proxy enables secure HTTP traffic between the gateway and intranet computers. There are two advantages to using the 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 the 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.

NOTE The rewriter proxy needs to be installed on the Portal Server node.

Ensure that the rewriter proxy and the gateway use the same gateway profile.

The rewriter proxy does not run automatically after installation. You need to enable the rewriter proxy as described below.

To Enable the Rewriter Proxy

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.

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

   The Gateway page appears.

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

   The Edit Gateway Profile page appears.

5. Select the Enable Rewriter Proxy checkbox to enable the rewriter proxy.

6. Specify the desired port for the rewriter proxy in the Rewriter Proxy Port edit box.

7. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.

8. Run *InstallDir*`/SUNWps/bin/certadmin` on the server to create a certificate for the rewriter proxy.

   You need to run this step only if you have not chosen to create a certificate while installing the rewriter proxy.

9. Log in as root to the Portal Server machine and start the rewriter proxy by typing:

   InstallDir`/SUNWps/bin/rwproxyd -n` *gateway profile name* `start`

10. For the changes to take effect, restart the gateway by typing:

    InstallDir`/SUNWps/bin/gateway -n` *gateway profile name* `start`

Disabling 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 the Sun ONE Portal Server.

To Disable Netlet

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the arrow next to Gateway under SRAP Configuration.

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

   The Edit Gateway Profile page appears.
5. Select the Enable Netlet checkbox. This checkbox is selected by default. Removing the selection disables Netlet.
6. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
7. For the changes to take effect, restart the gateway by typing:

   InstallDir`/SUNWps/bin/gateway -n` *gateway profile name* `start`

Enabling Netlet Proxy

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.

See “Configuring the Netlet Proxy“ in Chapter 3, “Configuring the Netlet“ for details on the Netlet Proxy.

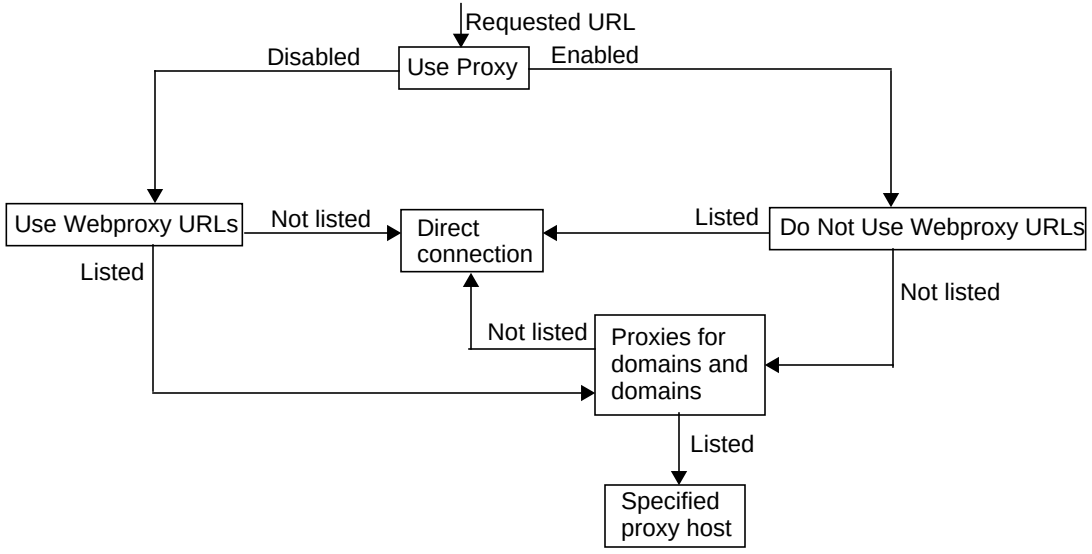
Managing Proxies

You can configure the gateway to contact HTTP resources using web proxies. Different proxies may be used for different domains and subdomains. These entries tell the gateway which web proxy to use to contact specific subdomains in specific domains. The proxy configuration specified in the gateway works as follows:

- Create a list of domains and subdomains along with the required proxies in the Proxies for Domains and Subdomains field in the gateway service.
- With the Use Proxy field 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 Webproxy URLs list.
- With the Use Proxy field 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.

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

Figure 2-1 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 from 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 Sun ONE Portal Server 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 of the 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 2-3. Table 2-3 has four columns. The first column lists the entry number for easy reference in the description. The second column lists the resolved entry from the example list above. The third column lists the corresponding proxy. The fourth column provides the description where appropriate.

Table 2-3 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.

Table 2-3 Mapping of entries in the Proxies for Domains and Subdomains List

Number	Entry in Proxies for Domains and Subdomains List	Proxy	Description
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`, of for `siroe.com`, a direct connection is attempted.
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 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 the rewriter. The 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 2-3, entry 24 is not considered.

See Chapter 5, “Configuring the Rewriter“ for more details on the rewriter and its functionality.

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 Domain Subdomain field of the admin 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`.

To Enable the Usage of Web Proxies

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the arrow next to Gateway under SRAP Configuration.

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

   The Edit Gateway Profile page appears.
5. Select the Use Proxy checkbox to enable the usage of web proxies.
6. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
7. For the changes to take effect, restart the gateway by typing:

   InstallDir`/SUNWps/bin/gateway -n` *gateway profile name* `start`

Specifying 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 “Managing Proxies“ for details on how this value affects the usage of proxies.

To Specify the URLs for Webproxies

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.

2. Select the Service Management view.
3. Click the arrow next to Gateway under SRAP Configuration.

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

   The Edit Gateway Profile page appears.
5. 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.
6. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
7. For the changes to take effect, restart the gateway by typing:

   InstallDir`/SUNWps/bin/gateway -n` *gateway profile name* `start`

Specifying URLs for which Proxies Should not be Used

The gateway tries to connect directly to the URLs listed in the Do Not Use Webproxy for URLs list. A webproxy is not used to connect to these URLs.

To Specify the URLs for which Proxies Should not be Used

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the arrow next to Gateway under SRAP Configuration.

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

   The Edit Gateway Profile page appears.

5. 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.

6. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.

7. For the changes to take effect, restart the gateway by typing:

   InstallDir`/SUNWps/bin/gateway -n` *gateway profile name* `start`

Specifying 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 iPlanet Directory Server Access Management Edition admin console as administrator.

2. Select the Service Management view.

3. Click the right arrow icon next to Gateway under SRAP Configuration.

   The Select Gateway Profile page appears.

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

   The Gateway - *profilename* page appears.

5. Scroll down to the Default Domain Subdomain 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. For the changes to take effect, restart the gateway by typing:

   InstallDir`/SUNWps/bin/gateway -n` *gateway profile name* `start`

Specifying Proxies for Domains and Subdomains

See “Processing of the Proxy Information,” on page 45 for details on how the proxy information is applied to various hosts.

To Specify Proxies for Domains and Subdomains

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the right arrow icon next to Gateway under SRAP Configuration.

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

   The Gateway - *profilename* page appears.
5. Type the required information in the Proxies for Domains and Subdomains edit box 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.
6. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
7. For the changes to take effect, restart the gateway by typing:

   InstallDir`/SUNWps/bin/gateway -n` *gateway profile name* `start`

Specifying Proxy Authentication Information

You need to specify the user name and password required for the gateway to authenticate to the specified proxy server, if the proxy server requires authentication to access some or all the sites.

To Specify the Proxy Authentication Information

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the arrow next to Gateway under SRAP Configuration.

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

   The Edit Gateway Profile page appears.
5. Scroll down to the Proxy Password List field.
6. Type the information for each proxy server in the format `proxyserver|username|password` and click Add.

   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. For the changes to take effect, restart the gateway by typing:

   InstallDir`/SUNWps/bin/gateway -n` *gateway profile name* `start`

Configuring Cookies

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:

- Discard all cookies if the Enable Cookie Management attribute is not selected in the gateway service.

- Pass-through all cookies to the user's browser and back to the appropriate web site(s) when the user makes subsequent visits to the web site(s) if the Enable Cookie Management attribute is selected.

This setting does not apply to the cookies used by the Sun ONE Portal Server to track Portal Server user sessions. It is controlled by the Forward Cookie Configuration.

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).

To Enable Cookie Management

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
1. Select the Service Management view.
2. Click the arrow next to Gateway under SRAP Configuration.

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

   The Edit Gateway Profile page appears.
4. Select the Enable Cookie Management checkbox to enable cookie management.
5. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
6. For the changes to take effect, restart the gateway by typing:

   InstallDir`/SUNWps/bin/gateway -n` *gateway profile name* `start`

Enabling 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). Sun ONE 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 Sun ONE 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).

NOTES 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 admin console. See Chapter 1, “Introduction to Sun ONE Portal Server, Secure Remote Access“ for more information on enabling single sign-on.

To Enable HTTP Basic Authentication

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the arrow next to Gateway under SRAP Configuration.

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

   The Edit Gateway Profile page appears.
5. Select the Enable HTTP Basic Authentication checkbox to enable HTTP basic authentication.
6. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
7. For the changes to take effect, restart the gateway by typing:

   InstallDir`/SUNWps/bin/gateway -n` *gateway profile name* `start`

Configuring 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 iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the arrow next to Gateway under SRAP Configuration.

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

   The Edit Gateway Profile page appears.
5. Select the Enable Persistent HTTP Connections checkbox.
6. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
7. For the changes to take effect, restart the gateway by typing:

   InstallDir`/SUNWps/bin/gateway -n` *gateway profile name* `start`

To Specify the Maximum Number of Requests per Persistent Connection

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the arrow next to Gateway under SRAP Configuration.

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

   The Edit Gateway Profile page appears.

5. Type the required number of requests in the Maximum Number of Requests per Persistent Connection field.
6. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
7. For the changes to take effect, restart the gateway by typing:

   InstallDir`/SUNWps/bin/gateway -n` *gateway profile name* `start`

To Specify the Timeout for the Persistent Socket

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the arrow next to Gateway under SRAP Configuration.

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

   The Edit Gateway Profile page appears.
5. Type the required timeout in seconds in the "Timeout after which Persistent Socket gets Closed" field.
6. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
7. For the changes to take effect, restart the gateway by typing:

   InstallDir`/SUNWps/bin/gateway -n` *gateway profile name* `start`

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 iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.

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

   The Gateway page appears.

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

   The Edit Gateway Profile page appears.

5. Type the required grace timeout in seconds in the Grace Timeout to Account for Turnaround Time field.

6. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.

7. For the changes to take effect, restart the gateway by typing:

   InstallDir`/SUNWps/bin/gateway -n` *gateway profile name* `start`

Forward Cookie Configuration

Sun ONE 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 Forward Cookie URL Lists. 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 iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the arrow next to Gateway under SRAP Configuration.

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

   The Edit Gateway Profile page appears.
5. Type the required URL in the Forward Cookie URLs edit box.
6. Click Add to add this entry to the Forward Cookie URLs list.
7. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
8. For the changes to take effect, restart the gateway by typing:

   InstallDir`/SUNWps/bin/gateway -n` *gateway profile name* `start`

Specifying URLs that Bypass Authentication

You can specify that some URLs do not need any authentication. These are normally directories and folders that contain images.

Specifying Non-authenticated URL Paths

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the arrow next to Gateway under SRAP Configuration.

   The Gateway page appears.

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

   The Edit Gateway Profile page appears.

5. Scroll down to the Non-authenticated URLs field and type the required folder path in the format `folder/subfolder`.

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. For the changes to take effect, restart the gateway by typing:

   InstallDir`/SUNWps/bin/gateway -n` *gateway profile name* `start`

Specifying 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 iPlanet Directory Server Access Management Edition admin console as administrator.

2. Select the Service Management view.

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

   The Gateway page appears.

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

   The Edit Gateway Profile page appears.

5. Scroll down to the Maximum Connection Queue Length field and specify the required number of connections.

6. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.

7. For the changes to take effect, restart the gateway by typing:

   InstallDir/SUNWps/bin/gateway -n *gateway profile name* start

Specifying 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 iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the arrow next to Gateway under SRAP Configuration.

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

   The Edit Gateway Profile page appears.
5. Scroll down to the Gateway Timeout (milliseconds) field and specify the interval required in milliseconds.
6. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
7. For the changes to take effect, restart the gateway by typing:

   InstallDir/SUNWps/bin/gateway -n *gateway profile name* start

Specifying the Maximum Number of Threads

You can specify the maximum number of threads that can be pre-created in the gateway thread pool.

To Specify the Maximum Number of Threads

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.

2. Select the Service Management view.
3. Click the arrow next to Gateway under SRAP Configuration.

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

   The Edit Gateway Profile page appears.
5. Scroll down to the Maximum Thread Pool Size field and specify the required number of threads.
6. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
7. For the changes to take effect, restart the gateway by typing:

   InstallDir`/SUNWps/bin/gateway -n` *gateway profile name* `start`

Specifying 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 iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the arrow next to Gateway under SRAP Configuration.

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

   The Edit Gateway Profile page appears.
5. Scroll down to the Cached Socket Timeout field and specify the interval required in milliseconds.
6. Click Save at the top or bottom of the Edit Gateway Profile page to record the change.
7. For the changes to take effect, restart the gateway by typing:

InstallDir/SUNWps/bin/gateway -n *gateway profile name* start

Configuring 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 Sun ONE 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 login screen appears and no authentication screen appears.

The PDC authentication process involves several steps:

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.

The gateway passes the certificate to the PDC authentication module in the server.

To Configure PDCs and Encoded Devices With the Gateway

Add the following line in the *InstallDir*/SUNWam/lib/AMConfig.properties file on the portal server machine:

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

Configuring PDCs and encoded devices involves the following subtasks:

- Importing the Required Certificates
- Adding the Gateway to the Certificate-enabled Gateway List
- Registering the Required Services
- Modifying the Required Attributes
- Restarting the gateway for the changes to take effect

Importing the Required Certificates

Import the required CA certificates into the certificate database of the gateway that you want PDC-enabled.

See Installing Certificates From a Certificate Authority in Chapter 4, Installing SSL Certificates in the *Sun ONE Portal Server, Secure Remote Access 6.0 Installation Guide*, for details.

Adding the Gateway to the Certificate-enabled Gateway List

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Choose Service Management from the View menu.

   All the services are displayed in the left pane.
3. Click the arrow next to Gateway under SRAP Configuration.

   The Gateway Profiles page is displayed in the right pane.
4. Type the fully qualified name of the gateway for which you want PDC authentication enabled in the Certificate-enabled Gateway Hosts field and click Add.

   Add the gateway in the format host1.sesta.com.

   The gateway is added to the Certificate-enabled Gateway Hosts list.

Registering the Required Services

1. Select User Management under the View menu.
2. Select the required organization.
3. Select Services in the Show menu.

   The Core service, if already registered, displays in the navigation pane. If it is not already registered, it can be done concurrently with the Certificate-based Authentication service.
4. Click Register in the navigation pane.

   A list of available services displays in the data pane.
5. Select the checkbox for Certificate-based Authentication and click Submit.

   The Certificate-based Authentication service appears in the navigation pane confirming that the service has been registered.

Modifying the Required Attributes

1. Select User Management under the View menu.
2. Select the required organization.
3. Select Services in the Show menu.

   The Core service, if already registered, displays in the navigation pane. If it is not already registered, it can be done concurrently with the Certificate-based Authentication service.
4. Select the Certificate-based Authentication checkbox and click the Properties arrow.

   The message "No template available for this service" appears in the data pane.
5. Click Create.

   The Certificate-based Authentication attributes appear in the data pane.
6. Modify the attributes as necessary.
7. Click Save at the top of the page to record the changes.
8. Enable the Dynamic User Profile Creation option under the Core service in DSAME Configuration.
9. Restart DSAME.
10. For the changes to take effect, restart the gateway by typing:

InstallDir/SUNWps/bin/gateway -n *gateway profile name* start

NOTE Dynamic User Profile Creation needs to be enabled in the Core service under DSAME Configuration. This allows the user profile to be created dynamically using the certificate attributes for users logging in using PDC.

Allowing 40-bit Browser 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 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 Browser Connections

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the arrow next to Gateway under SRAP Configuration.

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

   The Edit Gateway Profile page appears.
5. Select the Allow 40-bit Browser 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. For the changes to take effect, restart the gateway by typing:

   InstallDir`/SUNWps/bin/gateway -n` *gateway profile name* `start`

Disabling 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 the Secure Remote Access. This ensures a greater level of security.

To Disable SSL Version 2.0

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the arrow next to Gateway under SRAP Configuration.

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

   The Edit Gateway Profile page appears.
5. Scroll down to the Enable SSL Version 2.0 field and deselect the option.

   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. For the changes to take effect, restart the gateway by typing:

   InstallDir`/SUNWps/bin/gateway -n` *gateway profile name* `start`

Enabling Cipher Selection

The Secure Remote Access 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 iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the arrow next to Gateway under SRAP Configuration.

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

   The Edit Gateway Profile page appears.
5. Scroll down to the Enable SSL Cipher Selection field and select the option.

   This option enables 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.

   This allows you to select the ciphers that you want to be supported at your client sites. Deselecting the "Enable the SSL ciphers individually" option automatically selects all the listed ciphers.
7. For the changes to take effect, restart the gateway by typing:

   InstallDir`/SUNWps/bin/gateway -n` *gateway profile name* `start`

Rewriting all URLs

See Chapter 5, “Configuring the Rewriter“ for details.

Specifying Domain-based Rulesets

See Chapter 5, “Configuring the Rewriter“ for details.

Specifying the MIME Mappings

See Chapter 5, “Configuring the Rewriter“ for details.

Specifying the List of Configured 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 Server List 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 the List of Configured Portal Servers

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the arrow next to Gateway under SRAP Configuration.

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

   The Edit Gateway Profile page appears.
5. Scroll down to the Portal Server List field. Specify the Portal Server in the format `http://portal server name:port number` in the edit field and click Add.

   The specified Portal Server is added to the Portal Server List field.

6. Click Save at the top or bottom of the page to record the changes.
7. For the changes to take effect, restart the gateway by typing:

   InstallDir/SUNWps/bin/gateway -n *gateway profile name* start

Specifying the Retry Interval for the Portal Server

You can set the frequency (in minutes) at which the gateway needs to check if the Portal Server is available.

To Specify the Retry Interval for the Portal Server

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the arrow next to Gateway under SRAP Configuration.

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

   The Edit Gateway Profile page appears.
5. Scroll down to the Server Retry Interval field. Specify the time interval in minutes at which the gateway needs to check whether the Portal Server is available.
6. Click Save at the top or bottom of the page to record the changes.
7. For the changes to take effect, restart the gateway by typing:

   InstallDir/SUNWps/bin/gateway -n *gateway profile name* start

Enabling 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 DSAME Configuration attributes. This log is located on the Portal Server machine.

The log name has 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 DSAME 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 iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the arrow next to Gateway under SRAP Configuration.

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

   The Edit Gateway Profile page appears.
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. For the changes to take effect, restart the gateway by typing:

   InstallDir`/SUNWps/bin/gateway -n` *gateway profile name* `start`

Enabling 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 iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the arrow next to Gateway under SRAP Configuration.

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

   The Edit Gateway Profile page appears.
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. For the changes to take effect, restart the gateway by typing:

   InstallDir/SUNWps/bin/gateway -n *gateway profile name* start

Authentication Chaining

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

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

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

To Enable Authentication Chaining

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select User Management under the View menu.
3. Select the required organization.
4. Select Services in the Show menu.

   The Core service, if already registered, displays under DSAME Configuration in the navigation pane.
5. Click the arrow icon next to Core.

   The Core attributes page is displayed.
6. Select the Authentication Chaining Enabled checkbox under the Organization attributes.
7. Click Save at the top of the page to record the changes.
8. For the changes to take effect, restart the gateway by typing:

InstallDir/SUNWps/bin/gateway -n *gateway profile name* start

To Specify the Authentication Modules

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select User Management under the View menu.
3. Select the required organization.
4. Select Services in the Show menu.

   The Core service, if already registered, displays under DSAME Configuration in the navigation pane.
5. Click the arrow icon next to Core.

   The Core attributes page is displayed.
6. List all the authentication modules required in the Authentication Chaining Modules field under the Organization attributes.

   You can specify any of the authentication modules using a single space to delimit the module names.

NOTE Do not specify Cert as one of the entries in the Authentication Chaining Modules field if you have enabled PDC authentication. If PDC authentication is enabled, it is the first authentication module that will run.

See the *Administration Guide, iPlanet Directory Server Access Management Edition* for more information on authentication modules.

---

7. Click Save at the top of the page to record the changes.
8. For the changes to take effect, restart the gateway by typing:

   InstallDir/SUNWps/bin/gateway -n *gateway profile name* start

Chained Certificates

A chained or stepped up certificate is one that has been upgraded from providing only 40-bit connections to also supporting 128-bit connections.

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.

Creating a Wild Card Certificate

The steps to create a wild card certificate are the same as Generating a Self-Signed SSL Certificate. 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 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.`*profilename*

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 using:

   InstallDir`/SUNWps/bin/gateway -n` *new profile name* `start`

Running the Gateway in the chroot Environment

To provide high security in a chroot environment, the chroot'd 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:

   InstallDir`/SUNWps/bin/chroot`

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

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

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
/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/javadir
```

```
mount -F lofs javadir /safedir/chroot/javadir
```

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:

```
javadir - /safedir/chroot/javadir 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 ./InstallDir/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 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.

To Restart the Gateway in the chroot environment

Follow these steps to run the Secure Remote Access gateway in a chroot environment whenever the gateway machine is rebooted:

1. Stop the gateway running from the '/' directory.

   # *InstallDir*/SUNWps/bin/gateway -n *profilename* stop

2. Start the gateway to run from the chroot directory.

   # chroot /safedir/chroot ./*InstallDir*/SUNWps/bin/gateway -n *profilename* 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 IP address of the system, also change the /safedir/chroot/etc/hosts.

Customizing the Gateway User Interface

This section discuss the various property files that can be edited. You can edit labels on the gateway admin console, error messages, or the order of log information. This is useful if you are trying to customize the product for different locales.

You can customize the following files:

InstallDir/SUNWam/locale/srapGatewayAdminConsole.properties

InstallDir/SUNWps/locale/srapGateway.properties

InstallDir/SUNWps/web-src/WEB-INF/classes/srapgwadminmsg.properties

NOTE You need to store a copy of each of these files in the respective locale directories if you have different locale settings.

srapGatewayAdminConsole.properties File

Edit this file to change the field names that appear on the gateway admin console.

srapgwadminmsg.properties File

Edit this file to:

- Customize the labels that appear on buttons in the gateway admin console
- Customize the status messages and error messages that appear when you are configuring the gateway.

srapGateway.properties File

Edit this file to:

- 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 `InstallDir/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 desktop, you need to copy this file into the respective locale directory, for example `InstallDir/SUNWps/locale_en_US`.

Understanding the platform.conf File

The `platform.conf` file is located at:

`/etc/opt/SUNWps`

The `platform.conf` file contains the details that the gateway needs to start running. 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.

Sample

```
#
# Copyright 11/28/00 Sun Microsystems, Inc. All Rights Reserved.
# "@(#)platform.conf 1.38 00/11/28 Sun Microsystems"
#
gateway.user=noaccess
gateway.jdk.dir=/usr/java_1.3.1_04
gateway.dsame.agent=http://abc.sesta.com:80//portal/RemoteConfigSer
vlet
portal.server.protocol=http
portal.server.host=abc.sesta.com
portal.server.port=80
gateway.protocol=https
gateway.host=olyve.abc.siroe.com
gateway.port=443
gateway.trust_all_server_certs=true
gateway.trust_all_server_cert_domains=false
gateway.virtualhost=olyve.abc.siroe.com 10.12.147.53
gateway.notification.url=http://abc.sesta.com:80/notificationservic
e
gateway.retries=6
gateway.locale=en_US
```

```
gateway.debug=error
gateway.debug.dir=/var/opt/SUNWps/debug
gateway.logdelimiter=&&
gateway.external.ip=10.12.147.53
gateway.certdir=/etc/opt/SUNWps/cert/default
gateway.allow.client.caching=true
gateway.userProfile.cacheSize=1024
gateway.userProfile.cacheSleepTime=60000
gateway.userProfile.cacheCleanupTime=300000
gateway.bindipaddress=10.12.147.53
gateway.sockretries=3
```

Description

Table 2-4 lists and describes all the fields in the `platform.conf` file. The table has three columns. The first column lists the entries in the file, the second column gives the default value, if any, and the third column gives a brief description of the field.

Table 2-4 platform.conf file

Entry	Default Value	Description
`gateway.user`	noaccess	This is the user as whom the gateway runs. The gateway has to 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 iPlanet Directory Server Access Management Edition server that gateway contacts while starting up to get its profile.

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

Table 2-4 platform.conf file

Entry	Default Value	Description
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 IP address in this field.
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 iDS / AME. 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.
gateway.locale		This is the gateway locale

Table 2-4 platform.conf file

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.`*profilename* - Contains the gateway debug messages. `Gateway_to_from_server.`*profilename* - In message mode, this file contains all the requests and response headers between the gateway and internal servers. `Gateway_to_from_browser.`*profilename* - In message mode, this file contains all the requests and response headers between the gateway and the client browser.
`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.
`gateway.external.ip`		In case of a multihomed gateway machine, you need to specify the external IP address here. This IP is used for the Netlet to run FTP.
`gateway.certdir`		This specifies the location of the certificate database.

Table 2-4 platform.conf file

Entry	Default Value	Description
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 client side but there will be a performance drop and 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 of the cache cleanup thread in seconds.
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.
gateway.sockretries	3	Not used currently.

Chapter 3

Configuring the Netlet

This chapter describes how you can use the Netlet to run applications securely between users' remote desktops and the servers running applications on your intranet. Topics covered include:

- Overview of the Netlet
- Defining Netlet Rules
- Configuring Netlet Attributes
- Configuring the Netlet Proxy
- Sample Netlet Rules
- Enabling Netlet Logging
- Customizing the Netlet

Overview of the Netlet

Sun ONE Portal Server 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 the Sun ONE Portal Server 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 the Netlet if:

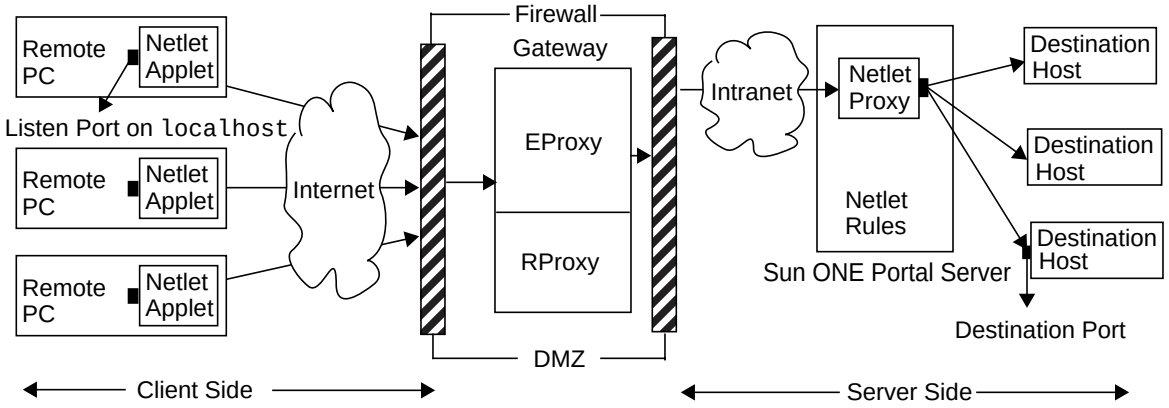
- It is TCP/IP-based.
- It uses fixed ports.

NOTE You cannot use the Netlet with applications that dynamically allocate ports. The exceptions are Microsoft Exchange (Microsoft Exchange 2000 is not supported) and FTP, for which Netlet supports dynamic port capability.

Components of the Netlet

The various components involved in the working of the Netlet are shown in Figure 3-1.

Figure 3-1 Components of the Netlet



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.

If there are static Netlet links on the Portal desktop, Netlet applet is downloaded automatically when the user logs into the portal. If there are only dynamic links, the applet is downloaded when the user clicks on the link.

See “Types of Rules,” on page 95 for details on static and dynamic rules.

Netlet Rules

A Netlet rule maps an application that needs to run on a client machine to the corresponding destination server. This means that the 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 the Netlet. These rules specify various details such as the algorithm 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 the Netlet, these rules help determine how the connection has to be established. See “Defining Netlet Rules,” on page 91 for details.

Netlet Provider

This is the UI component of the Netlet. The provider enables users to configure the required applications from the Sun ONE Portal Server 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 91.

EProxy

All client requests are routed through the EProxy. EProxy handles only Netlet requests and passes any other request to the RProxy. EProxy parses the 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. Netlet packets are decrypted at the gateway and sent to the destination servers. However, the gateway needs to access all the Netlet target hosts through the firewall between the demilitarized zone (DMZ) and the intranet. This requires opening a large number of ports in the firewall.

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, the Netlet packets are decrypted by the proxy and then sent to the destination server. This reduces the number of ports required to be opened in the firewall.

Netlet proxy is optional and you may choose not to install this proxy during the installation.

Destination Port

This is the port on the destination on which the destination application's server listens.

Netlet Usage Scenario

The following sequence of events are involved in using the Netlet:

1. The remote user logs in to the Sun ONE Portal Server 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 91 for details on static and dynamic rules.
3. Netlet listens on the client ports defined in the Netlet rules. See Client Port under Netlet Rule Syntax.
4. Netlet sets up a channel between the remote client and server over the ports specified in the Netlet rule.

Working With Netlet

For the 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 95.
2. Define the global options in the Netlet template in the Service Management view on the iPlanet Directory Server Access Management Edition admin console.
3. Assign the permission to execute Netlet in the Policy Management view on the Administration Console.
4. Determine whether the rules should be organization, role, or user-based and make modifications as required at each level. See the *Sun ONE Portal Server Administrator’s Guide* for details on organization, role and user.

Defining Netlet Rules

Netlet configuration is defined through Netlet rules that are configured in the iPlanet Directory Server Access Management Edition admin console. 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.

Netlet Rule Syntax

Netlet rules consist of the following fields:

- Rule Name
- Encryption Algorithms
- URL
- Download Applet
- Extend Session
- Client Port
- Target Host(s)
- Target Port(s)

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 3-1 lists the fields in the Netlet rule. Table 3-1 has three columns. The first column lists the field name. The second column describes the field, and its function in the Netlet rule. The third column lists possible values for that particular field.

Table 3-1 Fields in a Netlet Rule

Parameter	Description	Value
Rule Name	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 “Defining Access to Netlet Rules,” on page 119 for details.	
Encryption Algorithms	Defines the encryption algorithm, or specifies the list of algorithms that the user can choose from.	The list of algorithms that you select appear in the Netlet provider as a drop-down list. The user can choose the required algorithm. If you select only one from the list, the algorithm is fixed, and the user does not have the option to choose the algorithm. Select "Null" only if you want a significant performance enhancement, and if you are sure that the users are browsing in a safe environment. Default - The Default Encryption Algorithm specified in the Netlet admin console is used.

Table 3-1 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`. `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.	Disabled - Do not download an applet. Enabled - Download the applet from the Sun ONE Portal Server machine using the loopback port. Specify the applet details in the format *clientport:server:serverport* where: • `clientport` indicates the destination port on the client. This port must be different from the default loopback port. Assigning the Default Loopback Port for details. Specify a unique `client port` for each rule. • `server` is the name of the server from which to download the applet. • `serverport` represents the port on the server used to download the applet. If `true`, and if the applet location is not specified, the applet is downloaded from the Sun ONE Portal Server server.

Table 3-1 Fields in a Netlet Rule

Parameter	Description	Value
Extend Session	Indicates that the Sun ONE Portal Server should not time out when the Netlet connection is active.	Enabled - Extend the Portal Server session if Netlet connection is active. Disabled - Do not extend the Portal Server session even if Netlet connection is active.
Client Port	Port on the client where the Netlet listens.	The value of `client port` must be unique. You cannot specify a particular port number in more than one rule. Specify multiple client ports if you are specifying multiple hosts for multiple connections. See “Static Rule With Multiple Host Connections,” on page 101 for the syntax.
Target 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`. You can specify multiple hosts to: • establish connection with each host specified. You need to specify the corresponding client and target ports for each host specified. See “Static Rule With Multiple Host Connections,” on page 101 for the syntax. • try to connect to any available host from the list of hosts specified. See “Static Rule with Multiple Host Selection,” on page 102 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 desktop. You cannot have a combination of a static host and TARGET in a single rule.

Table 3-1 Fields in a Netlet Rule

Parameter	Description	Value
Target Port(s)	The port on the target host	In addition to the host and target, 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 target host. The minus (-) sign between port numbers is the separator between the port numbers for different target 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.

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 a 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. See “Netlet Rule Syntax,” on page 91 for the syntax of the rules.

Rule Name	Encryption Algorithm	URL	Download Applet	Extend Session	Client Port	Target Host(s)	Target Port(s)
ftpstatic	RC4	null	false	true	30021	sesta	21

You can configure multiple target hosts and ports for static rules. See Static Rule With Multiple Host Connections 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. See "Netlet Rule Syntax," on page 91 for the syntax of the rules.

Rule Name	Encryption Algorithm	URL	Download Applet	Extend Session	Client Port	Target Host(s)	Target Port(s)
ftpdynamic	RC4	null	false	true	30021	TARGET	21

Encryption Algorithm

Based on the encryption algorithm, Netlet rules can be further classified as follows:

- **User Configurable Algorithm Rules** - In this rule, you can specify a list of algorithms that users can choose from. These optional algorithms appear as a drop-down list in the Netlet provider. The user can choose the required algorithm from the list. In the following example, the user can choose from `DES` and `RC4` algorithms.

Rule Name	Encryption Algorithm	URL	Download Applet	Extend Session	Client Port	Target Host(s)	Target Port(s)
Telnet	DES RC4	null	false	true	30000	TARGET	23

NOTE Although the Sun ONE Portal Server server may have various algorithms enabled, the user can choose only from the list that is configured as part of the Netlet rule.

See Supported Algorithms for a list of the algorithms supported by the Netlet, and the corresponding keywords.

- **Administrator Configured Algorithm Rules** - In this rule, the algorithm is defined as part of the Netlet rule. The user does not have the option to choose the required algorithm. In the following example, the algorithm is configured to be RC4.

Rule Name	Encryption Algorithm	URL	Download Applet	Extend Session	Client Port	Target Host(s)	Target Port(s)
Telnet	RC4	null	false	true	30000	TARGET	23

See Supported Algorithms for a list of algorithms supported by the Netlet, and the corresponding keywords.

Supported Algorithms

Table 3-2 lists the algorithms supported by the Netlet in the first column, and the keyword used to associate an algorithm in the second column. Use the corresponding keywords to specify the algorithms in the Netlet rules.

NOTE Select "Null" only if you want a significant performance enhancement, and if you are sure that the gateway and Portal Server are running in a secure environment.

Table 3-2 List of Supported Algorithms

Algorithm Name	Keyword
Rivest Cipher #4	RC4
Data Encryption Standard	DES
Triple DES / DESede	TripleDES
AES / Rijndael	Rijndael

Table 3-2 List of Supported Algorithms

Algorithm Name	Keyword
No Encryption / Null Cipher	Null

Backward Compatibility

Earlier versions of the Sun ONE Portal Server did not support algorithms as part of the Netlet rules. For backward compatibility with existing rules without algorithms, a default algorithm is used by the rules. An existing rule without algorithms such as:

Rule Name	Encryption Algorithm	URL	Download Applet	Extend Session	Client Port	Target Host(s)	Target Port(s)
Telnet		telnet://localhost:30000	false	true	30000	TARGET	23

is interpreted as:

Rule Name	Encryption Algorithm	URL	Download Applet	Extend Session	Client Port	Target Host(s)	Target Port(s)
Telnet	Default Algorithm	telnet://localhost:30000	false	true	30000	TARGET	23

This is similar to an Administrator Configured Rule with the Encryption Algorithm field chosen as Default. See “Specifying the Default Encryption Algorithm,” on page 112 for details.

Default Ports for Applications

Table 3-3 identifies the reserved ports for various applications and services. The first column lists the application name, and the second column lists the specific reserved port.

Table 3-3 Default Listen Ports for Certain Applications

Predefined Netlet Rule	Reserved Port
Telnet	30000
GO-Joe	10491
Citrix	1494
pcANYWHERE	4631, 5632
CarbonCopy	1138
LapLink	51547
RapidRemote	45414
ReachOut	43188
RemotelyPossible	799
loopback*	8000
FTP	30021

* loopback is used internally by the system.

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 the 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 Algorithm	URL	Download Applet	Extend Session	Client Port	Target Host(s)	Target Port(s)
myrule	RC4	null	false	true	1111	sesta	23

where:

- `myrule` is the name of the rule.
- `RC4` indicates the algorithm 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.
- Indicates that the Sun ONE Portal Server should not time out when the Netlet connection is active.
- `1111` is the port on the client where the Netlet listens for a connection request from the target host.
- `sesta` is the name of the recipient host in the Telnet connection.
- `23` is the port number on the target host for the connection, in this case the well-known port for Telnet.

Description

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 Algorithm	URL	Download Applet	Extend Session	Client Port	Target Host(s)	Target Port(s)
myrule	RC4	null	false	true	1111	sesta	23
					1234	siroe	23

where:

- `23` is the port number on the target host for the connection – reserved port for Telnet.
- `1111` is the port on the client where the Netlet listens for a connection request from the first target host `sesta`.
- `1234` is the port on the client where the Netlet listens for a connection request from the second target host `siroe`.

The first six fields in this rule are the same as in Basic Static Rule. The difference is that three more fields identify the second target host.

When you add additional targets to a rule, you must add three fields, `client port`, `target host`, and `target port`, for each new target host.

NOTE You can have multiple sets of three fields describing the connection to each target 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.

Description

This rule works the same as the previous rule. The Netlet provider does not display any link, but the Netlet automatically starts and listens on the two ports specified (1234). The user needs to start the client software, in this case a Telnet session that connects to `localhost` on port 1111 or the local host 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 Algorithm	URL	Download Applet	Extend Session	Client Port	Target Host(s)	Target Port(s)
gojoe	RC4	/gojoe.html	8000:gojoeserver:8080	true	10491	siroe+sesta	35+26+491-35+491

where:

- `10491` is the port on the client where the Netlet listens for a connection request from the target 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 target host.
  - The minus (-) sign between port numbers is the separator between the port numbers for different target 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 the Netlet.

Rule Name	Encryption Algorithm	URL	Download Applet	Extend Session	Client Port	Target Host(s)	Target Port(s)
myrule	RC4	telnet://localhost:30000	false	true	30000	TARGET	23

where:

- `myrule` is the name of the rule.
- `RC4` indicates the algorithm to be used.
- `telnet://localhost:30000` is the URL invoked by the rule.
- `false` indicates that no applets are to be downloaded.
- Indicates that the Sun ONE Portal Server should not time out when the Netlet connection is active.
- `30000` is the port on the client where the Netlet will listen for connection requests for this rule.
- `TARGET` indicates that the destination server needs to be configured by the user using the Netlet provider.
- `23` is the port on the target host opened by the Netlet, in this case the well-known port for Telnet.

Description

After this rule is added, the user must complete some steps to get the 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 Sun ONE 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 target 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 target 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 Algorithm	URL	Downlaod Applet	Extend Session	Client Port	Target Host(s)	Target Port(s)
gojoe	RC4	/gojoe.html	8000:gojoe serve:8080	true	3399	TARGET	58

where:

- `gojoe` is the name of the rule.
- `RC4` indicates the algorithm to be used.
- `/gojoe.html` is the path of the HTML page containing the applet, relative to the iPS installation directory *InstallDir*`/SUNWps/public_html` (in a default installation).
- `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.
- Indicates that the Sun ONE Portal Server should not time out when the Netlet connection is active.
- `3399` is the port on the client where the Netlet listens for connection requests of this type.
- `TARGET` indicates that the destination server needs to be configured by the user using the Netlet provider.
- `58` is the port on the destination server opened by the Netlet, in this case the port for GoJoe. Port 58 is the port that the target host listens to for its own traffic. The Netlet passes information to this port from the new applet.

Creating a Netlet Rule

You can create Netlet rules at a global level in the Service Management view of the iPlanet Directory Server Access Management Edition admin 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.

NOTE This chapter lists the procedures to configure various aspects of the Netlet at the organization level.

To Create a Netlet Rule

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Choose the User Management view.
3. Choose the Organization for which you want to create the rule.
4. Click the arrow next to Netlet under SRAP Configuration in the left pane.

   The Netlet page is displayed in the right pane.
5. 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.
6. Type a unique name for the rule in the Rule Name field.
7. Specify the required Encryption Algorithms. Select Default to retain the default encryption algorithm. Select Other to choose from the list of available algorithms.

   See To Specify the Default Algorithm for details on the default algorithm.

NOTE Select "Null" only if you want a significant performance enhancement, and if you are sure that the users are browsing in a safe environment.

8. Type the URL to the application to be invoked in the URL field.

9. Select the Download Applet checkbox if an applet needs to be downloaded. Type the applet details in the format `client port:server host:server port` in the associated edit box.

NOTE Specify a unique `client 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.

10. 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.
11. Type the client port on which Netlet listens in the Client Port field.
12. Type the host that will receive the Netlet connection in the Target Host(s) field.
13. Type the port on the target host in the target Port(s) field.
14. Click Add to List to reflect the last three entries in the Port-Host-Port List field.
15. Click Save.

    The rule is saved and you are returned to the Netlet page. The new rule name appears in the Netlet Rules list.

Modifying an Existing Netlet Rule

You can modify Netlet rules at a global level in the Service Management view of the Administration Console. These rules are inherited by any new organization that you create.

You can also modify existing rules at the organization, role, or user levels.

To Modify a Netlet Rule

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Choose the User Management view.
3. Choose the Organization for which you want to modify the rule.

4. Click the arrow next to Netlet under SRAP Configuration in the left pane.

   The Netlet page is displayed in the right pane.

5. Click Edit... next to the rule that you want to modify under the Netlet Rules field.

   The Edit Netlet Rule page is displayed.

6. Make changes as required and click Save.

   The modified rule is saved and you are returned to the Netlet page.

Deleting a Netlet Rule

You can delete Netlet rules at a global level in the Service Management view of the Administration Console.

To Delete a Netlet Rule

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Choose the User Management view.
3. Choose the Organization for which you want to delete the rule.
4. Click the arrow next to Netlet under SRAP Configuration in the left pane.

   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.

Configuring Netlet Attributes

Other than the Netlet rules, you need to configure the following attributes of Netlet based on your site's requirements. These attributes can be configured at the organization or user levels.

NOTE This chapter describes the configuration of all the attributes at the organization level.

When you create a new user, you need to select the Netlet checkbox in the Create User procedure. This will make the Netlet application available to the new user.

You can carry out the following configurations in the Netlet service:

- Setting the Conflict Resolution Level
- Specifying the Default Encryption Algorithm
- Specifying the Key Size for Algorithms
- Assigning the Default Loopback Port
- Enabling Reauthentication for Connections
- Disabling Warning Popup for Connections
- Enabling the Show Checkbox in Port Warning Dialog
- Setting the Keep Alive Interval
- Setting the Terminate Netlet at Portal Logout Option
- Defining Access to Netlet Rules
- Denying Access to Netlet Rules
- Allowing Access to Hosts
- Denying Access to Hosts

Netlet Attributes at the Service Management Level

The attributes at the Service Management 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 Management level. The new values are reflected only when new organizations are added. Changes in the attribute values at the service management level do not affect existing organizations or users.

Netlet Attributes at the Organization Level

If you configure an attribute at the organization level, the attribute becomes available to all the users under that organization.

Netlet Attributes at the User Level

If you configure an attribute at the user level, the attribute value is valid only for that particular user.

All the attributes that can be configured at the organization level can also be configured at the user level. The values set at the user level override the values set at the organization level. See the *Administration Guide, iPlanet Directory Server Access Management Edition* for more information on organization, role and user level attributes.

In addition, some extra attributes can be configured at the user level. If you do not specify these values in the admin console, the user will be asked for this information when a connection is being established through Netlet for the first time. The user will be asked for this information if:

- The user has Internet Explorer 4.x, 5.x or 6.x with Java plug-in (version 1.3.1._01 or 1.3.1_02), has enabled the "Use Browser Settings" option in the Proxies tab of the Java Plug-in Control Panel, and has specified a PAC 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 1.3.1_02) and has enabled the "Use Browser Settings" option in the Proxies tab of the Java Plug-in Control Panel. Any proxy setting specified by the user is not considered.

In both these cases, Netlet may not be able to determine the browser settings, and hence the user is asked to supply the information.

Browser proxy type

This attribute can take the values DIRECT or MANUAL. If you choose 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 hostnames.

Netlet Password

If you have enabled reauthentication in the admin console, the Netlet Authentication dialog appears each time the user connects to an application through Netlet. The user needs to supply the Netlet password. If reauthentication is not enabled in the admin console, the user will not have the option to change the password.

NOTE By default, the Netlet authentication password is `srap-netlet`.

You can change this authentication password for the user in this field. The user can also change this password using the Edit button on the Netlet channel.

If you have not enabled reauthentication, a port warning dialog appears on the user desktop stating the port through which Netlet is trying to establish connection. The Netlet Authentication dialog does not appear.

NOTE The port warning dialog also may not appear if you have disabled the option in the Netlet administration console.

To Configure Netlet Attributes at the User Level

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 Users from the Show drop-down list for the selected organization.
6. Click the arrow next to the required user in the left pane.

   The *username* page appears in the right pane.
7. Scroll down to the Netlet section and click Edit.

   The Netlet attributes page appears.
8. Make changes to the attribute values as required.

   See the procedure for the respective configuration.
9. Click Save at the top or bottom of the Netlet page to record the change.

Setting the Conflict Resolution Level

You can set the priority level for all the Netlet attributes. If a user inherits multiple attribute templates, say from an organization and a role assignment, and there is a template conflict between the attributes in the two templates, the template with the highest priority is returned. There are seven settings available ranging from Highest to Lowest.

See the *Administration Guide, iPlanet Directory Server Access Management Edition* for more details on conflict resolution.

To Set the Conflict Resolution Level

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.

3. Select Organizations from the Show 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 in the Show drop-down list.
6. Click the arrow next to Netlet under SRAP Configuration.

   The Netlet page is displayed in the right pane.
7. Scroll down to the Conflict Resolution Level field, and select the required level from the drop-down list.
8. Click Save at the top or bottom of the Netlet page to record the change.

Specifying the Default Encryption Algorithm

You need to specify the default algorithm for the Netlet rules. This is useful when using existing rules that did not include the algorithm as a part of the rule. This is a mandatory field. See “Backward Compatibility,” on page 98.

To Specify the Default Algorithm

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 Show drop-down list for the selected organization.
6. Click the arrow next to Netlet in the left pane.

   The Netlet page appears in the right pane.
7. Scroll down to the Default Encryption Algorithm field and select the required algorithm from the drop-down list. See Supported Algorithms for a list of supported algorithms.

NOTE Select "Null" only if you want a significant performance enhancement, and if you are sure that the users are browsing in a safe environment.

8. Click Save at the top or bottom of the Netlet page to record the change.

Specifying the Key Size for Algorithms

You can specify the key size to be associated with each algorithm in the Key Size Specification field. A larger key size ensures greater security, but the performance is affected. The following table lists the recommended key sizes for various algorithms. The table has two columns. The first column lists the algorithm name, and the second column lists the recommended key size.

Algorithm	Recommended Key Size
TripleDES	192
Rjindael	128 or 192 or 256
RC4	128
DES	64

To Specify the Key Size for the Algorithms

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 Show drop-down list for the selected organization.
6. Click the arrow next to Netlet in the left pane.

   The Netlet page appears in the right pane.

7. Scroll down to the Key Size Specification field.
8. Type the required algorithm name and the key size in the format `keyname|keysize` and click Add.

   The keyname-keysize value is updated in the Key Size Specification list box.
9. Click Save at the top or bottom of the Netlet page to record the change.

Assigning the Default Loopback Port

This attribute specifies the port to be used on the client when applets are downloaded through the Netlet. The default value of 8000 is used unless it is overridden in the Netlet rules.

To Assign the Default Loopback Port

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 Show drop-down list for the selected organization.
6. Click the arrow next to Netlet in the left pane.

   The Netlet page appears in the right pane.
7. Scroll down 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.

Enabling 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 Disabling Warning Popup for Connections 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 iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 Show drop-down list for the selected organization.
6. Click the arrow next to Netlet in the left pane.

   The Netlet page appears in the right pane.
7. Scroll down to the Reauthentication for connections field and select the option.
8. Click Save at the top or bottom of the Netlet page to record the change.

Disabling Warning Popup for Connections

This attribute displays a message on the user's desktop warning that someone is trying to connect to Netlet through the listen port. The message appears when the user runs the application over the Netlet, and also when an intruder tries to gain access to the desktop through the listen port.

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 iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 Show drop-down list for the selected organization.
6. Click the arrow next to Netlet in the left pane.

   The Netlet page appears in the right pane.
7. Select the 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.

Enabling the Show Checkbox in Port Warning Dialog

A warning popup is displayed on the user's desktop when Netlet tries to connect to the destination host through a freely available port on the local machine. This warning popup appears on the user's desktop only if the Warning Popup for Connections option is enabled in the admin console.

You can allow the user to suppress this warning popup by enabling the Show 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 iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 Show drop-down list for the selected organization.
6. Click the arrow next to Netlet in the left pane.

   The Netlet page appears in the right pane.

7. Scroll down to the Show checkbox in port warning dialog field and select the option.
8. Click Save at the top or bottom of the Netlet page to record the change.

Setting the Keep Alive Interval

You can set the time interval in minutes for which a Netlet connection is kept alive even if there is no operation.

If you do not specify a value for this attribute, the idle Netlet connection times out with all other Portal Server idle connections per the "Max idle time (minutes)" value specified in the Session Attributes section of the DSAME Configuration.

To Set the Keep Alive Interval

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 Show drop-down list for the selected organization.
6. Click the arrow next to Netlet in the left pane.

   The Netlet page appears in the right pane.
7. Scroll down 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.

Setting 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 Sun ONE 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 Sun ONE Portal Server desktop.

NOTE Disabling this option does not allow the user to make new Netlet connections after logging out of Portal Server. Only existing connections are preserved.

To Set the Terminate Netlet at Portal Logout Option

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 Show drop-down list for the selected organization.
6. Click the arrow next to Netlet in the left pane.

   The Netlet page appears in the right pane.
7. Scroll down 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.

Defining 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 iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 Show drop-down list for the selected organization.
6. Click the arrow next to Netlet in the left pane.

   The Netlet page appears in the right pane.
7. Scroll down 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 iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 Show drop-down list for the selected organization.
6. Click the arrow next to Netlet in the left pane.

   The Netlet page appears in the right pane.
7. Scroll down 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.

Allowing Access to Hosts

You can define access to specific hosts for certain organizations, roles or users. This enables you to restrict 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 iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 Show drop-down list for the selected organization.
6. Click the arrow next to Netlet in the left pane.

   The Netlet page appears in the right pane.
7. Scroll down 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.

Denying 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.

NOTE If you have configured a static rule for a particular host, say `sesta`, and have also included `sesta` in the Denied Hosts list, the host `sesta` will not be denied access.

To Deny Access to Hosts

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 Show drop-down list for the selected organization.
6. Click the arrow next to Netlet in the left pane.

   The Netlet page appears in the right pane.
7. Scroll down 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.

Configuring the Netlet Proxy

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 Sun ONE Portal Server 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 Netlet Proxy Configured" section of Figure 3-2. The Netlet proxy offers improved security benefits through data encryption but may increase the use of system resources.

See the *Sun ONE Portal Server, Secure Remote Access 6.0 Installation Guide* for instructions on installing the Netlet proxy.

You can:

- Choose to install the Netlet proxy on the Portal Server node on or on an independent node.
- Install multiple Netlet proxies and configure them for a single gateway using the admin console. This is useful in load balancing. To Configure the Netlet Proxy for details.
- Configure multiple instances of Netlet proxy on a single machine.
- Point multiple instances of the gateway to a single installation of Netlet proxy.

NOTE If you are using a single Netlet proxy for multiple instances of the gateway, ensure that you specify different Netlet proxy ports in the various gateway profile.

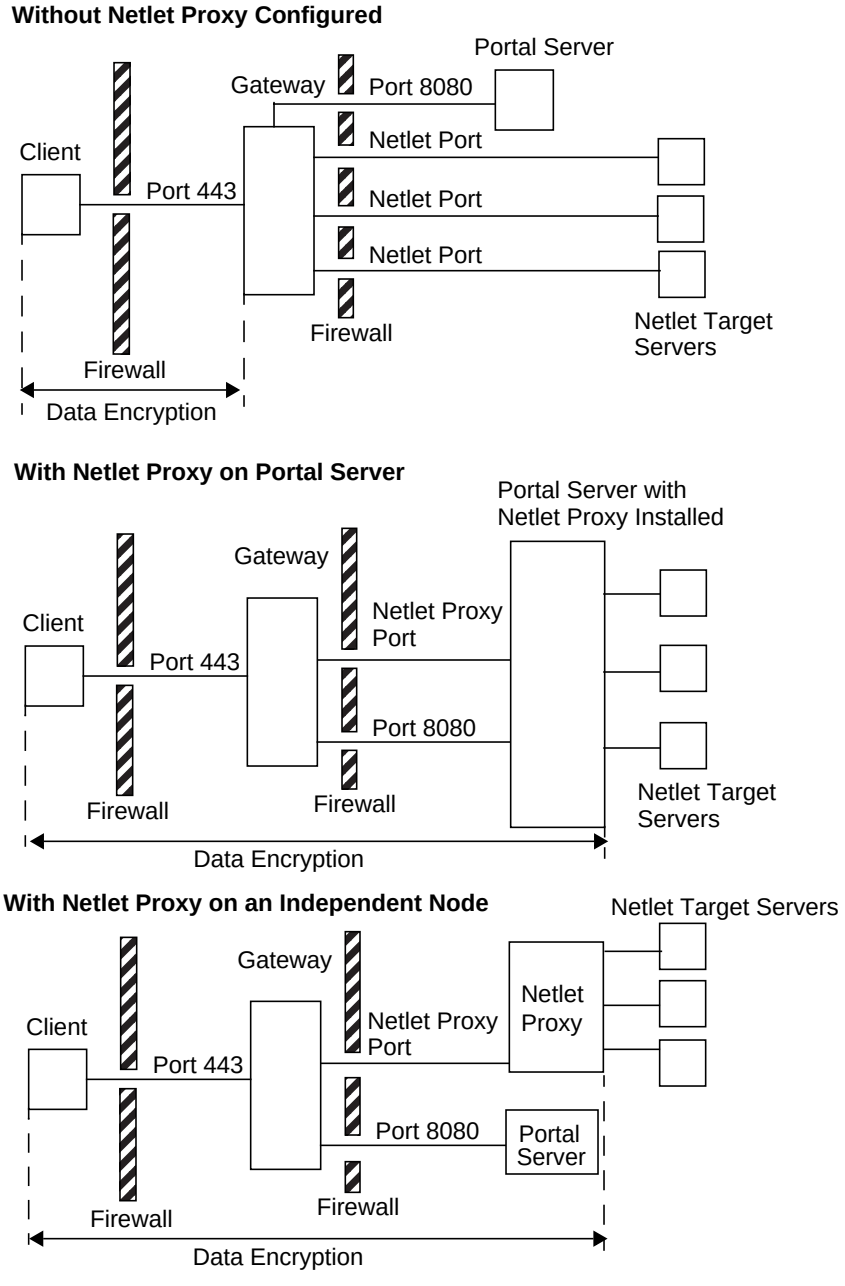
Figure 3-2 shows 3 sample implementations of the gateway and Portal Server with and without the Netlet proxy installed. The components include a client, 2 firewalls, the gateway that resides between the 2 firewalls, the Portal Server, and Netlet target servers.

The first scenario shows the gateway and Portal Server without 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 the Portal Server with the Netlet proxy installed on the 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 the 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 the Netlet proxy installed on an independent node. Installing the Netlet proxy on an independent 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 3-2 Implementation of Netlet proxy



To Configure the Netlet Proxy

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the right arrow icon next to Gateway under SRAP Configuration in the left frame.

   The Gateway page appears on the right pane.
4. Click the required profile.

   The Gateway > Edit Gateway Profile page appears in the right pane.
5. Scroll down and select the Enable Netlet Proxy check box to enable the Netlet proxy.
6. Type the desired Netlet proxy host and port in the Netlet Proxy Hosts edit field, in the format `host name:port`. Click Add.

TIP From the command line, enter:

`netstat -a | grep` *port_number* **`| wc -l`**

To determine if the port desired is available and unused. *port_number* is the required port.

---

7. Click Save at the top or bottom of the page to save the changes.
8. For the changes to take effect, restart the gateway by typing:

   InstallDir`/SUNWps/bin/gateway -n` *gateway profile name* `start`

Restarting the Netlet Proxy

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

You can also restart the Netlet proxy manually.

To Restart the Netlet Proxy

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

- Start the watchdog process using:

  InstallDir/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.

NOTE You need to ensure that Netlet proxy is running before enabling the watchdog.

To stop the Netlet Proxy, ensure that the watchdog is stopped first.

- Start the Netlet proxy manually using:

  InstallDir/SUNWps/bin/netletd -n *profilename* start

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

Configuring Multiple Instances of the Netlet Proxy

Use the nlpmultiinstance script to create a new instance of the Netlet proxy. You can create a new instance in the following scenarios:

- Creating a New Instance on a Portal Server Node
- Creating a New Instance on a non-Portal Server Node

Creating a New Instance on a Portal Server Node

1. Login as root and navigate to the following directory:

   InstallDir/SUNWps/bin

2. Run the multi instance script:

```
./nlpmultiinstance
```

Table 3-4 lists the questions that the script asks. The first column lists the question, the second column lists the default value, and the third column has the description.

Table 3-4 Checklist for creating a new Netlet proxy instance on a Portal Server node

Parameter	Default Value	Description
New Netlet proxy instance uses Portal Server instance running on this node	y	The script detects an existing instance of the Portal Server and asks this question. Specify y if you want the Netlet proxy to run with the Portal Server instance on the same node. Choose n if you want to use a different instance of the Portal Server. In this case, the Creating a New Instance on a non-Portal Server Node checklist applies.
Portal Server instance is the default one created during installation	y	Specify which instance of the Portal Server you want the new Netlet proxy instance to work with. If you choose y, the default Portal Server instance that is created during installation is used with the new Netlet proxy. If you choose n, you will be asked to specify the name of the required Portal Server instance.
New Portal Server instance created	y	This question is asked only if you have chosen not to use the default Portal Server instance. Specify whether the Portal Server instance that you want to use with your new Netlet proxy instance has already been created. If you choose n, you are asked to create the instance first, and the script aborts.
Name of the new Portal Server instance	*Portal Server instance name*	This question is asked only if you have chosen not to use the default Portal Server instance. Specify the name of the Portal Server instance that you want the new Netlet proxy instance to use.
Port on which the new Portal Server instance listens	81	This question is asked only if you have chosen not to use the default Portal Server instance. Specify the port on which the new Portal Server instance listens.

Table 3-4 Checklist for creating a new Netlet proxy instance on a Portal Server node

Parameter	Default Value	Description
Deployment URI	`/portal`	This question is asked only if you have chosen not to use the default Portal Server instance. Specify the deployment URI of the new Portal Server instance.
Name of the new Netlet proxy instance		Specify the name of the new Netlet proxy instance that you want to create.
Port on which the new Netlet proxy instance listens	`10558`	Specify the port on which the new Netlet proxy instance needs to listen. Ensure that this port has not been specified for any other Netlet proxy instance.
Created a corresponding gateway profile for the new Netlet proxy instance	`y`	You are asked if you have created a gateway profile for the new Netlet proxy instance. See To Create a Gateway Profile for details on creating a new gateway profile.

Start the new instance of the Netlet proxy with the required gateway profile name.

InstallDir`/SUNWps/bin/netletd -n` *profilename* `start`

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

Creating a New Instance on a non-Portal Server Node

1. Login as root and navigate to the following directory:

   InstallDir`/SUNWps/bin`

2. Run the multi instance script:

   `./nlpmultiinstance`

Table 3-5 lists the questions that the script asks. The first column lists the question, the second column lists the default value, and the third column has the description.

Table 3-5 Checklist for creating a new Netlet proxy instance on a non- Portal Server node

Parameter	Default Value	Description
New Netlet proxy instance uses Portal Server instance running on this node	n	This question is not asked if the script does not detect an instance of the Portal Server on this node. The script detects an existing instance of the Portal Server and asks this question. Specify y if you want the Netlet proxy to run with the Portal Server instance on the same node. Choose n if you want to use a different instance of the Portal Server.
Host name of the Directory Server	*hostname*	This is the machine on which the Directory Server is installed. Specify the machine on which Directory Server was installed for the Portal Server.
Sub-domain name for *hostname*	*subdomain*	This is the sub-domain to which the Directory Server belongs. Specify the sub-domain of the machine on which the Directory Server was installed for the Portal Server.
Domain name for *hostname*	*domain*	This is the domain to which the Directory Server machine belongs. Specify the domain of the machine on which the Directory Server was installed for the Portal Server.
Port used to access the Directory Server	389	This is the port which the Portal Server uses to access the Directory Server. Specify the Directory Server port specified during the Portal Server installation.
Root suffix of the directory tree	o=isp	This is the default top level organization. Any new organization that you create is created under this organization.
Organization name	*subdomain.domain*	This is the name of the default organization that is created.
Hostname of Portal Server	*Portal Server hostname*	This is the hostname of the Portal Server.
sub-domain for *Portal Server hostname*		This is the sub-domain to which the Portal Server machine belongs.

Table 3-5 Checklist for creating a new Netlet proxy instance on a non- Portal Server node *(Continued)*

Parameter	Default Value	Description
domain name for *Portal Server hostname*		This is the domain to which the Portal Server machine belongs.
Port used to access Portal Server	`80`	This is the port used to access the Portal Server.
Protocol used to access Portal Server	`http`	Specify the protocol that is used to access the Portal Server.
DSAME server deployment URI	`/amserver`	This is the DSAME deployment URI. Do not change this value.
Portal Server deployment URI	`/portal`	Specify the deployment URI of the new Portal Server instance.
Name of the new Netlet proxy instance		Specify the name of the new Netlet proxy instance that you want to create.
Port on which the new Netlet proxy instance listens	`10662`	Specify the port on which the new Netlet proxy instance needs to listen. Ensure that this port has not been specified for any other Netlet proxy instance.
Created a gateway profile for the new Netlet proxy instance	`y`	You are asked if you have already created a profile for the new Netlet proxy instance. See To Create a Gateway Profile for details on creating a new gateway profile.

Start the new instance of the Netlet proxy with the required gateway profile name.

InstallDir`/SUNWps/bin/netletd -n` *profilename* `start`

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

To Configure the Netlet Proxy Watchdog

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

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

Sample Netlet Rules

Table 3-6 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, Client Port, Target Host, Target Port. The last column includes a description of the rule.

NOTE Table 3-6 does not list the Cipher and Extend Session fields of the Netlet rule. Assume these to be "RC4" and "true" for the samples provided.

CAUTION Microsoft Exchange 2000 is not supported.

Table 3-6 Sample Netlet Rules

Rule	URL	Download Applet	Client Port	Target Host	Target Port	Description
IMAP	null	false	10143	imapserver	143	The Netlet `client port` on the client side need not be the same as the `target 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 3-6 Sample Netlet Rules

Rule	URL	Download Applet	Client Port	Target Host	Target Port	Description
Lotus Web Client	null	false	80	lotus-server	80	This rule tells the 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 the 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 the 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 3-6 Sample Netlet Rules

Rule	URL	Download Applet	Client Port	Target Host	Target Port	Description
Microsoft Outlook and Exchange Server This will not work for Windows NT and Windows 2000. Use Outlook web access through the rewriter for Windows NT and 2000.	null	false	135	exchange	135	This rule tells the 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 3-6 Sample Netlet Rules

Rule	URL	Download Applet	Client Port	Target Host	Target 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 client port for your Netlet FTP rule. Dynamic FTP is not supported using a Netlet connection.
Netscape 4.7 Mail Client	null	false	10143 10025	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 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 Netlet. `citrix_start.html` is bundled with Citrix.

Table 3-6 Sample Netlet Rules

Rule	URL	Download Applet	Client Port	Target Host	Target Port	Description
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 admin console. The log files are created in the directory specified in the Log Location attribute as part of the Logging section of the DSAME 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)

To Enable Netlet Logging

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the arrow next to Gateway under SRAP Configuration.

   The Gateway page appears.

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

   The Gateway > Edit Gateway Profile page appears.

5. Select the Enable Netlet logging checkbox to enable Netlet logging.
6. Click Save at the top or bottom of the page to record the changes.

Customizing the Netlet

You can customize the text that appears in message windows, in the Netlet provider, and on the Netlet administration console.

Editing Text on the Netlet Attributes Page

You can edit the text that appears on the Netlet attributes page of the admin console. You need to make the required changes in the following files:

InstallDir`/SUNWam/locale/srapNetlet.properties`

Editing Message Text in the Netlet Provider

You can edit the messages that appear in the Netlet provider on the end user's desktop. You need to make the required changes in the following files:

InstallDir`/SUNWam/locale/srapNetletProvider.properties`

Editing the Error Messages File

You can edit the `srapNetletApplet.properties` file for messages that appear when Netlet has problems with the browser's proxy settings. You need to make the required changes in the following file:

InstallDir`/SUNWam/locale/srapNetletApplet.properties`

Editing the Netlet Messages File

You can edit the `srapNetletServlet.properties` file for messages that appear when Netlet is loading. You need to make the required changes in the following file:

InstallDir`/SUNWam/locale/srapNetletServlet.properties`

Chapter 4

Configuring NetFile

This chapter introduces you to NetFile and explains its configuration and operation in detail.

Topics covered include:

- Overview of NetFile
- Enabling Access to NetFile
- Configuring NetFile Attributes

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 the Secure Remote Access 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 is aimed at increasing the 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

Supported File Access Protocols

NetFile allows you to access remote systems using FTP, SMB (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:
  - Check the host for port 139 on SMB.
  - Check the host for FTP server on port 21. If the FTP response contains the string "NetWare", this is considered as a NETWARE host.
  - Check to see if the host is for NFS and is listening on port 2049.
  - 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.

NOTE The connection fails if the servers are running on non-standard ports.

- NetFile allows users to select the file server / system protocol of their choice.

For each of these file systems, the platforms that are accessed are listed below.

Table 4-1 File Systems and Protocols Supported

File System/Protocol	Platform
NFS	Solaris 2.6 onwards
SMB	Windows 95 / 98 / NT / 2000 / ME / XP
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

NOTE Support for Novell Netware is only through FTP server and not through native access.

Enabling Access to NetFile

When you install the Secure Remote Access, the NetFile service is registered only for the organization that you specified during installation. The NetFile User Role is also created for this organization.

To Enable NetFile for Organizations and Users

1. Assign the NetFile service to the organization that requires NetFile access.
2. Create the NetFile User Role for each of these organizations. Create this role with the following attributes:
   - Type: Services
   - Access Permissions: Organization Help Desk Admin
3. Assign the NetFile service to each user who requires access to NetFile.
4. Assign the NetFile User Role to each user who requires access to NetFile.

   See the *Administration Guide, iPlanet Directory Server Access Management Edition* for more information on creating and assigning roles and services.

Configuring NetFile Attributes

As an administrator, you can configure various attributes at the organization, role, and user levels.

NetFile has two distinct sets of attributes:

Organization - These attributes can be set only at the organization level. These attributes cannot be changed at the role or user levels, and are available to all roles and users under a specific organization. You cannot edit these attributes at the role or user level.

The organization attributes are - Temporary Directory Location, OS Character Set, SMB Client Location, and MIME-types Configuration File Location.

Dynamic - These attributes can be set at the organization, role and user levels. The values set at the user level override the values set at the organization or role levels.

The Dynamic attributes are - Conflict Resolution Level, Window Size, Window Location, Search Directories Limit, Allow Access to Window Hosts, Allow Access to FTP Hosts, Allow Access to NFS Hosts, Allow Access to Netware Hosts, Common Hosts, Allowed Hosts, Denied Hosts, Allow File Deletion, Allow File Rename, Allow Changing User Id, Allow Changing Windows Domains, File Upload Limit(in MB), Default Domain, and Default Windows Domain / Workgroup.

NOTE Conflict Resolution Level is not available at the Service Management level, or at the User level. This is available at the organization and role levels.

NetFile Attributes at the Service Management Level

The attributes at the Service Management 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 Management level. The new values are reflected only when new organizations are added. Changes in the attribute values at the service management level do not affect existing organizations or users.

NetFile Attributes at the Organization Level

If you configure an attribute at the organization level, that attribute is inherited by all roles and users under that organization.

NOTE This chapter describes the configuration of all the attributes at the organization level.

NetFile Attributes at the User Level

Only the dynamic NetFile attributes are available for configuring at the user level. See Configuring NetFile Attributes for details on dynamic attributes.

Specifying the Temporary Files Directory

NetFile needs a temporary directory for various file operations. 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 Sun ONE Portal Server, the disk may quickly run out of space. NetFile will not work if the temporary directory has no space.

To Specify a Temporary Directory

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 in the Show drop-down list.
6. Click the arrow next to NetFile under SRAP Configuration.

   The NetFile page is displayed in the right pane.
7. Type the required temporary directory in the NetFile Temporary Directory Location field.
8. Click Save at the top or bottom of the NetFile page to record the change.

Specifying the OS Character Set

You can specify the character set that needs to be 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 iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 in the Show drop-down list.
6. Click the arrow next to NetFile under SRAP Configuration.

   The NetFile page is displayed in the right pane.
7. Scroll down to the OS Character Set field and type the character set code.
8. Click Save at the top or bottom of the NetFile page to record the change.

Specifying the SMB Client Location

The Samba client is packaged as part of the Sun ONE Portal Server, Secure Remote Access 6.0. You need to install the SMB client and specify the exact location to be able to access Windows hosts.

You need to specify the full path until the `bin` directory that contains the smbclient executable. For example, `/usr/sfw/bin`.

To Specify the Location of the SMB Client

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 in the Show drop-down list.
6. Click the arrow next to NetFile under SRAP Configuration.

   The NetFile page is displayed in the right pane.
7. Scroll down to the SMB Client Location field and type the full path to where the SMB client is located.
8. Click Save at the top or bottom of the NetFile page to record the change.

Specifying 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 Sun ONE Portal Server's web server needs to be used, then the location that needs to be specified is:

InstallDir`/SUNWam/servers/`*instance name of web server machine*`/config`

To Specify the Location of the MIME-types Configuration File

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 in the Show drop-down list.
6. Click the arrow next to NetFile under SRAP Configuration.

   The NetFile page is displayed in the right pane.

7. Scroll down to the MIME-types Configuration File Location field and type the full path to where the MIME-types configuration file is located.
8. Click Save at the top or bottom of the NetFile page to record the change.

Setting the Conflict Resolution Level

You can set the priority level for the dynamic attributes. If a user inherits multiple attribute templates, say from an organization and a role assignment, and there is a template conflict between the attributes in the two templates, the template with the highest priority is inherited. There are seven settings available ranging from Highest to Lowest.

See the *Administration Guide, iPlanet Directory Server Access Management Edition* for more details on conflict resolution.

To Set the Conflict Resolution Level

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 in the Show drop-down list.
6. Click the arrow next to NetFile under SRAP Configuration.

   The NetFile page is displayed in the right pane.
7. Scroll down to the Conflict Resolution Level field, and select the required level from the drop-down list.
8. Click Save at the top or bottom of the NetFile page to record the change.

Specifying 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 admin 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 iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 in the Show drop-down list.
6. Click the arrow next to NetFile under SRAP Configuration.

   The NetFile page is displayed in the right pane.
7. Scroll down to the Window Size field under NetFile - Dynamic 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.
8. Click Save at the top or bottom of the NetFile page to record the change.

Specifying the NetFile Window Location

You can specify the location where the NetFile window appears 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 admin 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 iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 in the Show drop-down list.
6. Click the arrow next to NetFile under SRAP Configuration.

   The NetFile page is displayed in the right pane.
7. Scroll down to the Window Location field under Dynamic 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.
8. Click Save at the top or bottom of the NetFile page to record the change.

Specifying 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 qualified machine 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 iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 in the Show drop-down list.
6. Click the arrow next to NetFile under SRAP Configuration.

   The NetFile page is displayed in the right pane.
7. Scroll down to the Default Domain field, and type the default domain name.
8. Click Save at the top or bottom of the NetFile page to record the change.

Specifying 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 iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 in the Show drop-down list.
6. Click the arrow next to NetFile under SRAP Configuration.

   The NetFile page is displayed in the right pane.
7. Scroll down to the Windows Domain / Workgroup field, and type the default Domain or Workgroup name.
8. Click Save at the top or bottom of the NetFile page to record the change.

Specifying 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. You need to type only positive integers in this field.

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. To continue the search, the user has to 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 iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 in the Show drop-down list.
6. Click the arrow next to NetFile under SRAP Configuration.

   The NetFile page is displayed in the right pane.
7. Scroll down to the Search Directories Limit field under Dynamic and type the required number.

NOTE Ensure that you type an integer value in this field.

8. Click Save at the top or bottom of the NetFile page to record the change.

Specifying 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 iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 in the Show drop-down list.
6. Click the arrow next to NetFile under SRAP Configuration.

   The NetFile page is displayed in the right pane.
7. Scroll down to the required Allow Access to *host type* Hosts option. 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.
8. Click Save at the top or bottom of the page to record the change.

Configuring a Common Host 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:

machine name - You can type either the simple machine name, or the fully qualified name. If the machine name that you have provided matches the machine 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 Host List, `florizon` is listed in the user's NetFile, but no operation can be carried out on `florizon`.

machine type - If the user has already added a machine 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.

You need to specify the type as one of the following:

- FTP
- NFS
- NT
- WIN
- NETWARE

machine 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 considered.

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 log out and logs in again, the edited values are not retained.

To Configure the Common Host List

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 in the Show drop-down list.
6. Click the arrow next to NetFile under SRAP Configuration.

   The NetFile page is displayed in the right pane.
7. Type the required information in the Common Hosts field as shown below:

   `machine_name=`*machinename*

   `machine_type=`*type*

   `machine_encoding=`*encoding*

   `machine_domain=`*domain*

   `machine_password=`*password*

   `machine_user_name=`*username*

   `share_name=`*/share*

   `share_password=`*password*

NOTE Ensure that there are no blank lines in the information set for one host.

Press the Enter or the Return key to type the next line.

You can leave the `machine_domain`, `machine_password`, `machine_user_name`, `share_name` and `share_password` fields blank if no entry is required.

Listed below is a sample information set for a machine abc.

```
machine_name=abc.sesta.com
machine_type=FTP
machine_encoding=ISO-8859-1
```

```
machine_domain=
machine_password=a$$a$$a
machine_user_name=abcdef
share_name=/space
share_password=a$$a$$a
```

NOTE Ensure that there are no spaces, and that all the keyword spellings and case (such as `machine_name` and `machine_encoding`) are correct.

Ensure that the `machine_type` is one of the following:

FTP, NFS, NT, WIN, NETWARE

Specify the `machine_type` as NT for Windows NT, XP and 2000 machines. Specify the `machine_type` as WIN for Windows 95, 98 and ME machines.

You cannot specify any other `machine_type`.

Repeat the `share_name` and `share_password` lines to include multiple shares.

Leave the `share_password` blank if there is no password for a particular share, or if you want the user to supply the password while accessing the share.

8. Repeat this information set for each common host that you want to add.
9. Click Save at the top or bottom of the NetFile page to record the change.

Configuring 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 Configuring the Denied Hosts List 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 iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 in the Show drop-down list.
6. Click the arrow next to NetFile under SRAP Configuration.

   The NetFile page is displayed in the right pane.
7. Scroll down to the Allowed Hosts List field.
8. 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 list box.
9. Click Save at the top or bottom of the page to record the changes.

Configuring the Denied Hosts List

After specifying the list of commonly available hosts under Configuring a Common Host List, 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 Host List

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 in the Show drop-down list.
6. Click the arrow next to NetFile under SRAP Configuration.

   The NetFile page is displayed in the right pane.
7. Scroll down to the Denied Host List field.
8. Type the names of the hosts to which you want to deny access in the edit field and click Add.

   The host name is added to the Denied Host List list box.
9. Click Save at the top or bottom of the page to record the changes.

Setting File Delete Permissions

You can allow or deny permission for a user to delete files from remote machines. This option is enabled by default.

If you disable this option, the Delete button will not be available to the user in the NetFile Java1 application. The Delete button will be disabled in the NetFile Java2 application.

NOTE If you disable this option after the user has started using NetFile, the change takes effect only if the user logs out of NetFile and logs in again.

To Allow File Deletion

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 in the Show drop-down list.
6. Click the arrow next to NetFile under SRAP Configuration.

   The NetFile page is displayed in the right pane.
7. Scroll down to the required Allow File Deletion field under Dynamic and select the option.

   Selecting the option enables all the users in the selected organization to delete files from the remote machine.
8. Click Save at the top or bottom of the NetFile page to record the change.

Setting File Rename Permissions

You can set this option to allow the user to rename files on the remote file system. This option is enabled by default.

If you disable this option, the Rename button will not be available to the user in the NetFile Java1 application. The Rename button is disabled in the NetFile Java2 application.

NOTE If you disable this option after the user has started using NetFile, the change will take effect only if the user logs out of NetFile and logs in again.

To Set File Rename Permission

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 in the Show drop-down list.
6. Click the arrow next to NetFile under SRAP Configuration.

   The NetFile page is displayed in the right pane.
7. Scroll down to the Allow File Rename field and select the option.

   Selecting the option enables all the users in the selected organization to rename files on the remote machine.
8. Click Save at the top or bottom of the NetFile page to record the change.

Allowing User ID Change

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.

This option is enabled by default.

To Allow User Id Change

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 in the Show drop-down list.
6. Click the arrow next to NetFile under SRAP Configuration.

   The NetFile page is displayed in the right pane.
7. Scroll down to the required Allow Changing User ID field under Dynamic and select the option.

   Selecting the option enables all the users in the selected organization to change their user ID if required.
8. Click Save at the top or bottom of the NetFile page to record the change.

Allowing NT Domain Change

This option is applicable to NT domains, and is enabled by default.

If the user specifies an invalid domain name in the User NT Domain name field while adding a system, an error message appears. 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 machine needs to be used, the user needs to remove the domain from the User NT Domain name field.

To Allow Domain Change

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 in the Show drop-down list.

6. Click the arrow next to NetFile under SRAP Configuration.

   The NetFile page is displayed in the right pane.

7. Scroll down to the required Allow Changing Windows Domains field under Dynamic and select the option.

   Selecting the option enables all the users in the selected organization to change their domain if required.

8. Click Save at the top or bottom of the NetFile page to record the change.

Setting 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 iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the User Management view.
3. Select Organizations from the Show 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 in the Show drop-down list.
6. Click the arrow next to NetFile under SRAP Configuration.

   The NetFile page is displayed in the right pane.

7. Scroll down to the File Upload Limit (in MB) field under Dynamic. Type the required size limit in mega bytes.

8. Click Save at the top or bottom of the NetFile page to record the change.

Enabling Debugging for NetFile

The location of the debug information depends on the setting of the `com.iplanet.services.debug.directory` attribute in the `AmConfig.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/srapNetFile`

Then the debug information for NetFile will be available in the `srapNetFile` file in the `/var/opt/SUNWam/debug` directory.

See the *Administration Guide, iPlanet Directory Server Access Management Edition* for more information.

Enabling Logging for NetFile

Specify the log location using the DSAME 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.

Configuring Unix Authentication

You need to configure the the Unix authentication daemon on the Portal Server for accessing NFS systems. This is done as follows:

1. Telnet to the localhost on the configuration port as follows:

   ```
   telnet localhost 8946
   ```

2. Type the Unix Helper Listen Port number.

   Specify the default value of `7946` 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 that `doUnix` has been configured successfully is displayed.

Chapter 5

Configuring the Rewriter

The Rewriter scans the contents of web pages and rewrites all the URLs embedded in the web pages.

This chapter has the following topics:

- Overview of the Rewriter
- Target Audience
- Supported URLs and Exceptions
- Defining Rewriter Rules and Rulesets
- Pre-packaged Rulesets
- Configuring the Rewriter in the Gateway Service
- Using Pattern-matching in Rules
- Rules for HTML Content
- Rules for JavaScript Content
- Rules for XML Content
- Cascading Style Sheets
- Client-side Rewriting
- Sample Ruleset
- Case Study
- Writing Rules for the Rewriter
- Working Samples
- Ruleset DTD

- Enabling Rewriter Debug Information
- Mapping of Rules with SP4

Overview of the Rewriter

In a secure environment, when a user is trying to access intranet pages from home, direct access to intranet pages may not be possible. However, after authentication, the rewriter enables end users to browse the intranet by making links and other URL references on those pages operate correctly. The rewriter scans the content of the webpages that a user wants to view, and identifies the URLs in those pages.

The rewriter has two main functions:

- Expanding relative URLs to absolute URLs
- Prefixing the gateway URL to the existing URL

For the functioning of the rewriter, you need to:

- Define the rules for rewriting various URLs using the Portal Server admin console. A collection of these rules is referred as a ruleset.
- Associate the appropriate ruleset for the various domains in the gateway admin console.

Expanding Relative URLs to Absolute URLs

The rewriter expands relative URLs to absolute URLs. For example, if a user is trying to access the site:

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

The rewriter translates this to:

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

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

In a non-gateway scenario, the URL Scraper provider handles this functionality. See Chapter 7, Administering Rewriter in the *Sun ONE Portal Server Administrator's Guide* for details on the URL Scraper provider.

Prefixing the Gateway URL to the Existing URL

If a user is trying to access intranet web pages through the gateway, the rewriter needs to prefix the gateway URL to the existing URL. For example, a user who is trying to access an html page on `mymachine` types:

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

The 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.

Target Audience

You need to read this guide if you are an administrator who needs to set up the rewriter to rewrite the intranet content as required for your organization.

NOTE Read this guide in conjunction with Chapter 7, Administering Rewriter in the *Sun ONE Portal Server Administrator's Guide*.

Also see Chapter 12, Command-Line Utilities in the *Sun ONE Portal Server Administrator's Guide* for administering rewriter data through the command-line.

You need the following to be able to write the required rules, and get the rewriter to work as expected:

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

Supported URLs and Exceptions

This section lists the types of URLs that are rewritten by the rewriter. It also lists exceptions that the rewriter does not handle.

Supported URLs

All standard URLs as specified in RFC-1738, and with protocol either HTTP or HTTPS are rewritten by the rewriter.

Standard URLs

All URLs with the protocol as either HTTP or HTTPS are recognized. This is 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`

Non-standard URLs

The rewriter supports the rewriting of some basic non-standard URLs.

The information required to convert the non-standard URL to a standard format is taken from the base URL of the page where the URL appears. This information could include:

- protocol
- host name
- port
- path

The back slash is supported only if it is part of a relative URL, not an absolute URL. For example, `http://abc.sesta.com\index.html` is rewritten, but `http:\\abc.sesta.com` is not rewritten.

Exceptions

These URLs are not rewritten.

`http:/abc.com`

Defining Rewriter Rules and Rulesets

The rewriter is designed to modify the URL portions of various elements that appear on a web page. You need to write specific rules for the rewriter to decide what portions of the web pages to rewrite, and how it needs to be rewritten. The types of rules required, and the exact syntax are described in the following sections.

A collection of rules for various categories and subcategories is stored in XML format, and is called a Ruleset.

You need to create a ruleset and administer rules in the Rewriter section of the Portal Server Configuration in the admin console.

Secure Remote Access comes with two pre-packaged rulesets to rewrite each of these elements. These rules are stored in XML format on the Portal Server. The rulesets are:

InstallDir`/SUNWps/export/DefaultGatewayRuleSet.xml`

InstallDir`/SUNWps/export/GenericRuleSet.xml`

See the section Pre-packaged Rulesets for details.

You need to define multiple rules based on the content type in the web pages. For example, the rules required to rewrite HTML content would be different from the rules required to rewrite JavaScript content.

When a page is being parsed by the rewriter, the rules in the ruleset are applied in order to each statement in the page, until a rule matches a particular statement.

Based on the content, rewriter rules fall into the following broad categories:

- Rules for HTML Content
- Rules for JavaScript Content
- Rules for XML Content

NOTE WML is similar to HTML and hence HTML rules are applied for WML content.

No rules are required for CSS content.

Pre-packaged Rulesets

Secure Remote Access comes with two pre-packaged rulesets to rewrite the elements in a web page. These rules are stored in XML format. The rulesets are:

InstallDir/SUNWps/export/DefaultGatewayRuleSet.xml

InstallDir/SUNWps/export/GenericRuleSet.xml

These rulesets are useful in rewriting web pages with commonly used URL naming conventions and referencing techniques.

In addition, these rulesets also contain the rules required for the proper functioning of the gateway, and applications such as NetMail, Netlet and NetFile.

NOTE For customizations, create a new ruleset with the required additional rules, along with the rules in the generic ruleset.

Restoring the Pre-packaged Rulesets

In case you accidentally delete either the default gateway ruleset or the generic ruleset, you can restore it as follows:

```
$ rwadmin store --runasdn "username" --password "password"
InstallDir/SUNWps/export/DefaultGatewayRuleSet.xml
```

```
$ rwadmin store --runasdn "username" --password "password"
InstallDir/SUNWps/export/GenericRuleSet.xml
```

where *username* and *password* are the same as that supplied for `amadmin`.

NOTE The default gateway ruleset or generic ruleset that is packaged with the installation is restored. If you have customized the rulesets, the changes are not restored.

Creating a Ruleset and Defining Rules

See Chapter 7, Administering Sun ONE Portal Server Rewriter in the *Sun ONE Portal Server Administrator's Guide* for details on creating a ruleset.

After creating a new ruleset, you need to define the required rules. Keep the following in mind while writing the rules:

- 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 Assigning Rulesets to Domains for details.
- Restart the gateway using:

  InstallDir`/SUNWps/bin/gateway -n` *gateway profile name* `start`

Configuring the Rewriter in the Gateway Service

The Rewrite all URLs checkbox and the Proxies for Domains and Subdomains list in the gateway service determine the behavior of the rewriter.

The Proxies for Domains and Subdomains list tells the gateway which URLs it may rewrite. Only references to hosts in the specified domains and subdomains are candidates for rewriting. Enabling the Rewrite All URLs option overrides the entries in the Proxies for Domains and Subdomains list.

See Chapter 2, "Administering the Gateway for details on proxy management.

Rewriting all URLs

If you enable the Rewrite All URLs option in the gateway service, the 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 iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the arrow next to Gateway under SRAP Configuration.

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

   The Gateway - *profilename* page appears.
5. Select the Rewrite all URLs checkbox to enable the gateway to rewrite all URLs.
6. Click Save at the top or bottom of the page to record the change.
7. For the changes to take effect, restart the gateway by typing:

   InstallDir`/SUNWps/bin/gateway -n` *gateway profile name* `start`

Assigning Rulesets to Domains

You can specify a particular ruleset to be used by certain domains. Depending on the domain a particular page is fetched from, the corresponding ruleset is used.

Assigning a specific ruleset improves the speed of operation since the specified ruleset contains only the relevant rules. If you assign a common ruleset for all domains, the time taken for the rewriter to run through all the rules in that ruleset will be much higher, than if you have a small subset of the rules for specific pages.

Create the required ruleset in the Rewriter service under Portal Server Configuration in the iPlanet Directory Server Access Management Edition admin console. See the *Sun ONE Portal Server Administrator's Guide* for details.

The following two entries are added by default to the Domain-based Rulesets list:

default domain|`default_gateway_ruleset`

`*|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. See Pre-packaged Rulesets for details.

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 Assign a Ruleset for a Domain

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the arrow next to Gateway under SRAP Configuration.

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

   The Gateway - *profilename* page appears.
5. Type the required domain or host name and the ruleset in the Domain-based rulesets field and click Add. The entry is added to the Domain-based Rulesets list.

   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`.

6. Click Save at the top or bottom of the page to record the change.
7. For the changes to take effect, restart the gateway by typing:

   InstallDir`/SUNWps/bin/gateway -n` *gateway profile name* `start`

Specifying the MIME Mappings

The rewriter has four different parsers to parse the web pages based on the content type - HTML, JAVASCRIPT, XML and WML. Common MIME types are associated with these parsers by default. You can associate new MIME types with these parsers in the MIME mappings field of the gateway service. This extends the rewriter functionality to other MIME types.

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

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 the MIME Mappings

1. Log in to the iPlanet Directory Server Access Management Edition admin console as administrator.
2. Select the Service Management view.
3. Click the arrow next to Gateway under SRAP Configuration.

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

   The Gateway - *profilename* page appears.
5. Scroll down to the MIME mappings 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`
6. Click Add to add the required entry to the list.
7. Click Save at the top or bottom of the page to record the change.
8. For the changes to take effect, restart the gateway by typing:

   InstallDir`/SUNWps/bin/gateway -n` *gateway profile name* `start`

Using Pattern-matching in Rules

You can use `valuePatterns` 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 appears

`name` is the name of the form

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

`valuePatterns` indicates the part of the `field` value that needs to be rewritten. All the content that follows `0|1234|` is rewritten.

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. Since * indicates a match with everything, nothing will follow the `valuePattern`, and hence the 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 A* 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 that appears 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 5-1 lists some sample usages of the * wildcard. The table has three columns. The first column lists the sample statement to be rewritten. The second column lists the sample valuePatterns value. The third column describes the rewriting.

Table 5-1 Sample usage of * wildcard

URL	valuePatterns	Description
`url1, url2, url3, url4`	`valuePatterns = "**, *, **, *"`	In this case, `url1` and `url3` are rewritten since `**` 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. The rest of the statement is discarded since XYZABC matches with the *, and 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 HTML Content

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

- Attribute Rules for HTML Content
- JavaScript Token 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. These tags include:

- src attributes of an "img" tag that point to an image location
- href attributes of an "archive" tag that point to another page or file

The rewriter modifies the values of these attributes by prefixing the gateway URL.

Syntax

```
<Attribute name="attributename" [tag="*" valuePatterns=""]/>
```

where,

`name` specifies the name of the attribute.

`tag` specifies the tag to which the attribute belongs

`valuePatterns` specifies the possible patterns to match with the attribute.

See Using Pattern-matching in Rules for details on `valuePatterns`.

Example

Assume the base URL of the page to be:

```
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/mypage.html>
```

Description

Since the URL to be rewritten is already an absolute URL, only the gateway URL is prefixed to the URL.

JavaScript Token Rules for HTML Content

HTML attributes whose value contains JavaScript that needs to be parsed by the JavaScript parser to determine what needs to be rewritten.

In most cases, the rules provided in the default gateway ruleset are sufficient to rewrite the URLs in JavaScript tokens.

Syntax

`<JSToken>`*token name*`</JSToken>`

where

`token name` is an attribute whose value is JavaScript that needs to be translated.

Example

Assume the base URL of the page to be:

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

Page content

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

Rules

```
<JSToken>onClick</JSToken>
<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 since `paramPatterns` has the value `y`.

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 through may contain forms. Some form elements may take a URL as the value.

Syntax

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

where

`Form source` is the URL of the html page where the form appears

`name` is the name of the form

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

`valuePatterns` indicates the part of the `field` value that needs to be rewritten. All the content that follows `valuePatterns` is rewritten.

See Using Pattern-matching in Rules for details on `valuePatterns`.

Example

Assume the base URL of the page to be:

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

Page Content

Assume the page URI to be `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>
```

Rules

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

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

Output

```
<FORM name=form1  method=POST action="gateway URL://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 form `value` is rewritten as shown in the output. The specified `valuePatterns` is located, and all content following `valuePatterns` is rewritten by prefixing the gateway URL, and the base URL of the page where the form appears.

See Using Pattern-matching in Rules for details on `valuePatterns`.

Applet Rules for HTML Content

A single web page may contain many applets, and each applet may contain many parameters. The rewriter rule for URLs in applets should contain pattern matching information as explained in the syntax:

The rewriter matches the values specified in the rule with the content of the applet and modifies the URLs as required. This replacement is carried out at the server and not when the user is browsing the particular web page.

A wildcard character (*) can also be used as part of the rule. For example, the parameter name could be *, in which case, the rewriter does not compare the parameter name in the applet.

Syntax

```
<Applet source="*/somehtml.jsp" code="classname.class" param="parametername"
[valuePatterns="*"] />
```

where

`source` is the URL of the page that contains the applet

`code` is the name of the applet class

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

`valuePatterns` is the pattern to be matched for rewriting

See Using Pattern-matching in Rules for details on `valuePatterns`.

Example

Assume the base URL of the page to be:

```
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="RewriteURLinApplet.class"
param="Test*"/>
```

Output

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

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

</APPLET>
```

Description

`codebase=appletcode` is rewritten since `<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 appears, and the gateway URL are prefixed to the `value` field.

Rules for JavaScript Content

JavaScript can contains URLs in various locations. The 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 translate the URL.

JavaScript elements that contain URLs are classified as follows:

- Variables in JavaScript
- Function Parameters in JavaScript

Variables in JavaScript

JavaScript variables are again classified into 5 categories:

- URL Variables in JavaScript
- EXPRESSION Variables in JavaScript
- DHTML Variables in JavaScript
- DJS (Dynamic JavaScript) Variables in JavaScript
- System Variables in JavaScript

URL Variables in JavaScript

URL variables have a URL string on the right hand side.

Syntax

```
<Variable type="URL">variablename</Variable>
```

where

`variablename` specifies the name of the variable. The value of the `variablename` is rewritten.

Example

Assume the base URL of the page to be:

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

Page Content

```
<script LANGUAGE="Javascript">
<!--
//URL Variables
var imgsrc="/tmp/tmp.jpg";
var imgsrc="http://srap.sesta.com/tmp/tmp.jpg";
```

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

Rules

```
<Variable type="URL">imgsrc</Variable>
```

Output

```
var imgsrc="gateway URL://abc.siroe.com/tmp/tmp.jpg";
var imgsrc="gateway URL://srap.sesta.com/tmp/tmp.jpg";
```

Description

All variables of type URL and with the name `imgsrc` are rewritten. For the first line of the output, the gateway URL and the base URL of the page on which the variable appears are prefixed. The second line already contains the absolute path, and hence only the gateway URL is prefixed.

EXPRESSION Variables in JavaScript

Expression variables have an expression on the right hand side. The result of this expression is a URL. The 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 since it can handle both scenarios.

Syntax

```
<Variable type="EXPRESSION">y1</Variable>
```

where

`y1` is the JavaScript expression variable.

Example

Assume the base URL of the page to be:

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

Page Content

```
<script LANGUAGE="Javascript">
<!--
//Expression variables
var expvar="../../images/graphics"+".gif";
document.write("<A HREF="+expvar+">EXPRESSION</A><P>")
var expvar="/images/graphics"+".gif";
//-->
</SCRIPT>
```

Rules

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

Output

```
var
expvar=psSRAPRewriter_convert_expression("../../images/graphics"+".
gif");
document.write("<A HREF="+expvar+">EXPRESSION</A><P>")
var
expvar=psSRAPRewriter_convert_expression("/images/graphics"+".gif")
;
```

Description

The function `psSRAPRewriter_convert_expression` is prefixed to the right hand side of the expression variable `expvar`. The function processes the expression and rewrites the content at runtime.

DHTML Variables in JavaScript

These are JavaScript variables that hold HTML content.

Syntax

`<Variable type="DHTML">`*y1*`</Variable>`

where

`y1` is the JavaScript DHTML variable.

Example

Assume the base URL of the page to be:

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

<Attribute name="href"/>

or

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

Output

```
//DHTML Var

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

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

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

//-->
```

Description

The JavaScript parser reads the value of `dhtmlVar` as HTML content. When HTML rules are applied to the page, the second rule (`Attribute name="href"`) is applied and the URL is rewritten.

DJS (Dynamic JavaScript) Variables in JavaScript

These are JavaScript variables that hold JavaScript content.

Syntax

`<Variable type="DJS">`*y1*`</Variable>`

where

`y1` is the JavaScript DHTML variable.

Example

Assume the base URL of the page to be:

```
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 type="DJS">dJSVar</Variable>
<Variable type="URL">dJSimgsrc</Variable>
```

Output

```
//DJS Var - need 2 rules
var dJSVar="var dJSimgsrc='gateway URL://abc.sesta.com/tmp/tmp.jpg';"
var dJSVar="var dJSimgsrc='gateway
URL://abc.sesta.com/dir1/dir2/dir3/jscript/tmp/tmp.jpg';"
var dJSVar="var dJSimgsrc='gateway URL://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 in JavaScript

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`.

Syntax

`<Variable type="SYSTEM">`*variable.name*`</Variable>`

where

`variable.name` is the system variable

Example

Assume the base URL of the page to be:

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

Page Content

```
<script LANGUAGE="Javascript">
<!--
//SYSTEM Var
alert(window.location.pathname);
//-->
</SCRIPT>
```

Rules

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

Output

```
</SCRIPT>
<SCRIPT LANGUAGE="Javascript">
<!--
//SYSTEM Var
```

```
alert(psSRAPRewriter_convert_pathname(window.location.pathname));
//-->
</SCRIPT>
```

Description

The rewriter locates the system variable specified in the rule, and the `psSRAPRewriter_convert_pathname` function is prefixed. This function processes the system variable at runtime, and rewrites the resulting URL accordingly.

Function Parameters in JavaScript

Function parameters are classified into 4 categories:

- URL Parameters in JavaScript
- EXPRESSION Parameters in JavaScript
- DHTML Parameters in JavaScript
- DJS Parameters in JavaScript

URL Parameters in JavaScript

These are string parameters that directly contain the URL.

Syntax

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

where

`type` is the type of the function

`name` is the name of the function that needs to be evaluated

`paramPatterns` specifies the parameters in the function that need to be rewritten

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

Example

Assume the base URL of the page to be:

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

Output

```
<SCRIPT language="JavaScript">
<!--
function test(one,two,three) {
alert(one + "##" + two + "##" +three);
}
test("gateway URL://abc.sesta.com/test.html","gateway
URL://abc.sesta.com/test/rewriter/test1/jscript/test.html","123");
window.open("gateway
URL://abc.sesta.com/index.html","gen",width=500,height=500);
//-->
</SCRIPT>
```

Description

The first rule specifies that the first two parameters in the function `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 in JavaScript

These are variables within a function that result in a URL when they are evaluated.

Syntax

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

where

`jstest1` is the name of the function.

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

Example

Assume the base URL of the page to be:

```
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"/>
```

Output

```
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);
```

Description

The rule specifies that the first parameter of the `jstest1` function needs to be rewritten. In the sample page content, the first parameter is an expression that will be evaluated only at runtime. The 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 in JavaScript

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

Syntax

```
<Function type="DHTML" name="name" paramPatterns="y"/>
```

where

`name` is the name of the function.

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

Example

Assume the base URL of the page to be:

```
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 type="DHTML" name="document.write" paramPatterns="y"/>
<Function type="DHTML" name="document.writeln" paramPatterns="y"/>
<Attribute name="href"/>
```

Output

```
<SCRIPT>
<!--
document.write('<a href="gateway
URL://xyz.siroe.com/index.html">write</a><BR>')
document.writeln('<a href="gateway
URL://xyz.siroe.com/test/rewriter/test1/jscript/JSFUNC/index.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 in JavaScript

Dynamic JavaScript parameters need two rules for the output to be rewritten as required.

Syntax

```
<Function type="DJS" name="name" paramPatterns="y"/>
```

where

`name` is the name of the function.

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

Example

Assume the base URL of the page to be:

```
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 type="DJS" name="NavBarMenuItem" paramPatterns=",y"/>

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

Output

```
<script>
```

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

Description

The first rule specifies that the second parameter of the function `NavBarMenuItem` which contains JavaScript needs 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 in XML
- Attributes in XML

Tag Text in XML

The rewriter translates XML content based on the TAG name.

Syntax

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

where

`attribute` is the name of the tag

`name=src` where `src` indicates the name of the attribute

Example

Assume the base URL of the page to be:

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

Page Content

```
<xml><attribute name="src">test.html</attribute></xml>
```

```
<xml><attribute>abc.html</attribute></xml>
```

Rules

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

Output

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

```
<xml><attribute>abc.html</attribute></xml>
```

Description

The first line in the page content has an attribute with the name `src`, and hence is rewritten based on the rule specified. The second line in the page content does not contain an attribute with the name `src`, and hence no rewriting is done.

Attributes in XML

The rules for XML attributes are similar to the attribute rules for HTML. See "Attribute Rules for HTML Content," on page 175.

The rewriter translates the attribute value based on the attribute and the tag names.

Syntax

```
<Attributes>
   <Attribute name="href" [tag="abc" valuePatterns="123|45|*"]/>
</Attributes>
```

where

`name` is the name of the attribute

`tag` is the name of the tag

`valuePatterns` indicates the portion of the string that needs to be rewritten. All content appearing after the `valuePatterns` is rewritten.

See Using Pattern-matching in Rules for details on `valuePatterns`.

Example

Assume the base URL of the page to be:

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

Page Content

```
<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>
```

Rules

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

Output

```
<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://abc.sesta.com/test/rewriter/test1/xml/string.html"/></xml>
```

Description

In the above example, only the fourth line is rewritten since it meets all the conditions specified in the rule.

See Using Pattern-matching in Rules for details on `valuePatterns`.

Cascading Style Sheets

The Cascading Style Sheets in HTML pages are also translated. There are no rules defined for this translation as the URL appears only in the `url()` function of the CSS.

Client-side Rewriting

The value of variables and function parameters in JavaScript cannot be determined on the server side. This value needs to be determined and rewritten, if required, at runtime on the client side. The rewriter handles such variables by prefixing a wrapper function to the variables.

Two such functions are provided in the rewriter:

`psSRAPRewriter_convert_expression`

This function is appended to EXPRESSION variables and EXPRESSION functions in JavaScript. This function takes the expression as a parameter and evaluates it to the required URL at the client browser.

`psSRAPRewriter_convert_pathname`

This function is used for system variables that are available as part of the JavaScript standard. The rewriter locates the system variable specified in the rule, and the `psSRAPRewriter_convert_pathname` function is prefixed. This function processes the system variable at runtime, and rewrites the resulting URL accordingly.

Sample Ruleset

This section contains a sample rule set. The Case Study is used to illustrate how these rules are interpreted by the 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 type="URL"> _fr.location </Variable>
    <Variable type="URL"> g_szUserBase </Variable>
    <Variable type="URL"> g_szPublicFolderUrl </Variable>
    <Variable type="URL"> g_szExWebDir </Variable>
    <Variable type="URL"> g_szViewClassURL </Variable>
    <Variable type="URL"> g_szVirtualRoot </Variable>
    <Variable type="URL"> g_szBaseURL </Variable>
    <Variable type="URL"> g_szURL </Variable>
    <Function type="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>
```

Case Study

This section includes the source HTML pages for a sample mail client. This case study will 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 in 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 5-2 Mapping Between Sample Ruleset and Case Study

Page Content	Rule Applied	Rewriter Output	Description
`var g_szVirtualRoot="http://abc.siroe.com/mailweb";`	JSRules section of the Sample Ruleset: `<Variable type="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 the rewriter to search for a variable `g_szVirtualRoot` of type URL. If such a variable exists in the web page, the rewriter converts this to an absolute URL, and prefixes the gateway URL.
`src="/destin_files/logo-ie5.gif"`	HTMLRules section of the Sample Ruleset: `<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 the rewriter to search for all attributes with the name `src`, and rewrite the value of that attribute.

Table 5-2 Mapping Between Sample Ruleset and Case Study

Page Content	Rule Applied	Rewriter Output	Description
`href="http://abc.siroe.com/mailclient/destin/Inbox/?Cmd=contents&Page=1"`	HTMLRules section of the Sample Ruleset: `<Attribute name="href"/>`	`href="http://gateway.sesta.com/http://abc.siroe.com/mailclient/destin/Inbox/?Cmd=contents&Page=1"`	href is the name of an attribute, and does not have any tag or valuePattern attached to it. This rule tells the rewriter to search for all attributes with the name `href`, and rewrite the value of that attribute.

Writing Rules for the Rewriter

For the proper functioning of the rewriter, you need to write a comprehensive set of rules to cover all conditions in your intranet pages. 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 of identifying most of the URLs is by searching for "http" and "/".
- Identify the content type of the URL - HTML, JavaScript or XML. See the following sections for details on each content type, further classifications, and the rule syntax for each type of URL:
  - Rules for HTML Content
  - Rules for JavaScript Content
  - Rules for XML Content
- 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 iPlanet Directory Server Access Management Edition admin console.

NOTE 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 "*", it is recommended to have the specific rules first, and then the general rules. Else, the general rule is applied to all statements, even before the specific rule is encountered.

- Combine all these rules into a ruleset for that domain

Working Samples

This section includes simple HTML pages with content that needs to be rewritten. The section also explains the rules required to rewrite the content for each sample HTML page, and the corresponding rewritten HTML page.

All 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 Forms
  - Sample for HTML Attributes
  - Sample for Applets
  - Sample for HTML JavaScript Tokens
- JavaScript Variables
  - Sample for JavaScript URL Variables
  - Sample for JavaScript EXPRESSION Variables

- Sample for JavaScript DHTML Variables
- Sample for JavaScript DJS Variables
- Sample for JavaScript SYSTEM Variables

- JavaScript 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

Sample for Forms

This sample can be accessed from:

portal server URL`/rewriter/HTML/forms/formrule.html`

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.

Add the rule specified in this sample to the `default_gateway_ruleset` in the section "Rules for Rewriting HTML Attributes". Edit the `default_gateway_ruleset` in the Rewriter service of the Portal Server Configuration in the iPlanet Directory Server Access Management Edition admin console.

Restart the gateway using:

InstallDir`/SUNWps/bin/gateway -n` *profilename* `start`

for the changes to take effect.

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://abc.sesta.com/casestudy/html/form.html">
```

/ / This URL is rewritten since `<Attribute name="action"/>` is defined as part of the HTML rules in the default gateway ruleset. Since 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, since 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 for details on valuePatterns.

```
<input type=hidden name=name3 value="../../html/test.html">
```

// This URL is not rewritten since the name does not match the field name specified in the rule.

```
</FORM>
```

**<FORM name=form2 method=POST action="gateway URL://abc.sesta.com/casestudy/html/form.html">
**

// This URL is rewritten since <Attribute name="action"/> is defined as part of the HTML rules in the default ruleset. Since 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 since the form name does not match the name specified in the rule.

```
</FORM>

</BODY>

RW_END

</HTML>
```

Sample for HTML Attributes

This sample can be accessed from:

portal server URL/rewriter/HTML/attrib/attribrule.html

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 since it is already defined in the "Rules for Rewriting HTML Attributes" section.

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 since the `<Attrib name="href"/>` rule is already defined in the default gateway ruleset. Since 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. Else, the gateway URL is not prefixed, since 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. Else, the gateway URL is not prefixed, since a direct connection is assumed.

`<br><br>`

`3 href <a href="gateway URL/portal server URL/rewriter/HTML/images/logo.gif">../images/</a>`

// Since 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 since 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>`

// Since 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>`

// Since 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 since there is no directory called `images` under the `rewriter` directory in the sample structure provided.

`Rewriting ends`

`</html>`

Sample for Applets

The base URL of the page where the applet code is present is:

portal server URL`/rewriter/HTML/applet/rule1.html`

The `RewriteURLinApplet.class` file is present in the following location:

portal server URL/rewriter/HTML/applet/appletcode

Add the rule specified in this sample to the default_gateway_ruleset in the section "Rules for Rewriting HTML Attributes". Edit the default_gateway_ruleset in the Rewriter service of the Portal Server Configuration in the iPlanet Directory Server Access Management Edition admin console.

Restart the gateway using:

InstallDir/SUNWps/bin/gateway -n *profilename* start

for the changes to take effect.

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 since the rule `<Attribute name="codebase"/>` is already present as part of the default gateway ruleset. 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 since the base URL of the page is `rule1.html`, and the param name matches the param `Test*` specified in the rule. Since `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 since 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 since 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>
```

Sample for HTML JavaScript Tokens

This sample can be accessed from:

portal server URL`/rewriter/HTML/jstokens/JStokens.html`

Add the rule specified in this sample to the `default_gateway_ruleset` in the section "Rules for Rewriting JavaScript Source". Edit the `default_gateway_ruleset` in the Rewriter service of the Portal Server Configuration in the iPlanet Directory Server Access Management Edition admin console.

Restart the gateway using:

InstallDir`/SUNWps/bin/gateway -n` *profilename* `start`

for the changes to take effect.

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

```
<JSToken>onClick</JSToken>
```

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

NOTE `<Function type="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. The rewriter detects the JavaScript tokens and passes it to the JavaScript function rules for further processing. The second rule listed in the sample tells the rewriter which parameter to rewrite.

```
</body>

<br>

Rewriting ends

</html>
```

Sample for JavaScript URL Variables

This sample can be accessed from:

portal server URL`/rewriter/JavaScript/variables/url/js_urls.html`

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.

Add the rule specified in this sample to the `default_gateway_ruleset` in the section "Rules for Rewriting JavaScript Source". Edit the `default_gateway_ruleset` in the Rewriter service of the Portal Server Configuration in the iPlanet Directory Server Access Management Edition admin console.

If you added the rule, restart the gateway using:

InstallDir`/SUNWps/bin/gateway -n` *profilename* `start`

for the changes to take effect.

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 type="URL">imgsrc</Variable>
```

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/variables/url/tmp/tmp.jpg";

var imgsrc="gateway URL/portal server
URL/rewriter/JavaScript/variables/tmp/tmp.jpg";

var imgsrc="gateway URL/portal server
URL/rewriter/JavaScript/tmp/tmp.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/variables/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 since the rule `<Attribute name="src"/>` is defined in the default gateway ruleset under the section "Rules for Rewriting HTML Attributes".

```
<br>

Image

</body>

<br>

Rewriting ends

</html>
```

Sample for JavaScript EXPRESSION Variables

This sample can be accessed from:

portal server URL/rewriter/JavaScript/variables/expr/expr.html

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 of the Portal Server Configuration in the iPlanet Directory Server Access Management Edition admin console.

If you added the rule, restart the gateway using:

InstallDir/SUNWps/bin/gateway -n *profilename* start

for the changes to take effect.

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">expvar</Variable>
```

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);
```

/ / The rewriter recognizes the right hand side of this statement to be a JavaScript EXPRESSION variable. The 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. Since 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";
```

/ / The 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. Since 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

This sample can be accessed from:

portal server URL/rewriter/JavaScript/variables/dhtml/dhtml.html

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.

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 of the Portal Server Configuration in the iPlanet Directory Server Access Management Edition admin console.

If you added the rule, restart the gateway using:

InstallDir/SUNWps/bin/gateway -n *profilename* start

for the changes to take effect.

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 type="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. So the HTML rules in the default gateway ruleset 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. So, the relative URL is replaced with the base URL of the page, and the required subdirectories. This is in turn 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. Since 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 since the rule <Attribute name="src"/> is defined in the default gateway ruleset under the section "Rules for Rewriting HTML Attributes".

Image

</body>

</html>

Sample for JavaScript DJS Variables

This sample can be accessed from:

portal server URL/rewriter/JavaScript/variables/djs/djs.html

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.

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 of the Portal Server Configuration in the iPlanet Directory Server Access Management Edition admin console.

Restart the gateway using:

InstallDir/SUNWps/bin/gateway -n *profilename* start

for the changes to take effect.

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 type="DJS">dJSVar</Variable>
<Variable type="URL">dJSimgsrc</Variable>
```

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 hands 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 since the rule `<Attribute name="src"/>` is defined in the default gateway ruleset under the section "Rules for Rewriting HTML Attributes".

```
<br>
Image
</body>
</html>
```

Sample for JavaScript SYSTEM Variables

This sample can be accessed from:

portal server URL`/rewriter/JavaScript/variables/system/system.html`

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 of the Portal Server Configuration in the iPlanet Directory Server Access Management Edition admin console.

Restart the gateway using:

InstallDir`/SUNWps/bin/gateway -n` *profilename* `start`

for the changes to take effect.

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

HTML After Rewriting

```
<html>
<head>
<title>JavaScript SYSTEM Variables Test Page</title>
</head>
<body>
<SCRIPT>
<!--
function psSRAPRewriter_convert_pathname(aPSPath)
{
```

```
    var lPSPath = aPSPath.substr( aPSPath.indexOf( "/",
       aPSPath.lastIndexOf("://") + 3 ) );
    return lPSPath;
}//psSRAPRewriter_convert_pathname()
//-->
</SCRIPT>
<script LANGUAGE="Javascript">
<!--
//SYSTEM Var
alert(psSRAPRewriter_convert_pathname(window.location.pathname));
```

/ / The rewriter identifies `window.location.pathname` as a JavaScript SYSTEM variable. The value of this variable cannot be determined at the server end. So 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

This sample can be accessed from:

portal server URL`/rewriter/JavaScript/functions/url/url.html`

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 of the Portal Server Configuration in the iPlanet Directory Server Access Management Edition admin console.

Restart the gateway using:

InstallDir/SUNWps/bin/gateway -n *profilename* start

for the changes to take effect.

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,height=500);
//-->
</SCRIPT>
</body>
</html>
```

Sample for JavaScript EXPRESSION Functions

This sample can be accessed from:

portal server URL`/rewriter/JavaScript/functions/expr/expr.html`

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 of the Portal Server Configuration in the iPlanet Directory Server Access Management Edition admin console.

Restart the gateway using:

InstallDir`/SUNWps/bin/gateway -n` *profilename* `start`

for the changes to take effect.

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"+jstest2
()));
```

/ / 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

This sample can be accessed from:

portal server URL`/rewriter/JavaScript/functions/dhtml/dhtml.html`

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 of the Portal Server Configuration in the iPlanet Directory Server Access Management Edition admin console.

Restart the gateway using:

InstallDir/SUNWps/bin/gateway -n *profilename* start

for the changes to take effect.

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. The 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. The 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 the 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

This sample can be accessed from:

portal server URL/rewriter/JavaScript/functions/djs/djs.html

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.

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 of the Portal Server Configuration in the iPlanet Directory Server Access Management Edition admin console.

Restart the gateway using:

InstallDir/SUNWps/bin/gateway -n *profilename* start

for the changes to take effect.

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>
```

Rules

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

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

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.sesta.com'"));
```

// `abc.sesta.com` is an entry in the Proxies for Domains and Subdomains list in the gateway service. Hence the rewriter needs to rewrite this URL. But since 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 if the function 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. Since 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 the rewriter does not recognize the second parameter as simple HTML.

```
</script>

</html>
```

Sample for XML Attributes

This sample can be accessed from:

portal server URL`/rewriter/XML/attrib.html`

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". Edit the `default_gateway_ruleset` in the Rewriter service of the Portal Server Configuration in the iPlanet Directory Server Access Management Edition admin console.

Restart the gateway using:

InstallDir`/SUNWps/bin/gateway -n` *profilename* `start`

for the changes to take effect.

HTML 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 since 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 for details on `valuePatterns`.

```
</body>

Rewriting ends

</html>
```

Ruleset DTD

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

<!ENTITY % gtype ’GROUPED’>

<!ENTITY % stype ’SCATTERED’>

<!ENTITY % jURL ’URL’>

<!ENTITY % jEXPRESSION ’EXPRESSION’>

<!ENTITY % jDHTML ’DHTML’>

<!ENTITY % jDJS ’DJS’>

<!ENTITY % jSYSTEM ’SYSTEM’>

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

<!ENTITY % htmlElements ’(Form | Applet | Attribute | JSToken)*’>

<!ENTITY % jsElements ’(Variable | Function)*’>

<!ENTITY % xmlElements ’(Attribute | TagText)*’>

<!ELEMENT RuleSet
(%ruleSetElements;,%ruleSetElements;,%ruleSetElements;)>

<!ATTLIST RuleSet

type (%gtype; | %stype;) "GROUPED"

id ID #REQUIRED

>

<!--

The following constraints are not represented in DTD, but are
handled programatically

1. ID should alway be in lower case.

2. In a rule, all mandatory attributes cannot be "*".

3. Only one instance of the below elements is allowed. They can be in
any order.

1)HTMLRules

2)JSRules

3)XMLRules

-->

<!ELEMENT HTMLRules (%htmlElements;)>
```

```
<!ATTLIST HTMLRules
type (%gtype; | %stype;) "GROUPED"
id CDATA "html_rules"
>
<!ELEMENT Form EMPTY>
<!ATTLIST Form
source CDATA #REQUIRED
name CDATA #REQUIRED
field CDATA #REQUIRED
valuePatterns CDATA ""
>
<!ELEMENT JSToken (#PCDATA)>
<!ELEMENT Applet EMPTY>
<!ATTLIST Applet
source CDATA #REQUIRED
code CDATA #REQUIRED
param CDATA "*"
valuePatterns CDATA ""
>
<!ELEMENT JSRules (%jsElements;)>
type (%gtype; | %stype;) "GROUPED"
id CDATA "js_rules"
>
<!ELEMENT Variable (#PCDATA)>
<!ATTLIST Variable
type (%jURL; | %jEXPRESSION; | %jDHTML; | %jDJS; | %jSYSTEM;) "URL"
>
<!ELEMENT Function EMPTY>
<!ATTLIST Function
type (%jURL; | %jEXPRESSION; | %jDHTML; | %jDJS;) "URL"
name CDATA #REQUIRED
```

```
paramPatterns CDATA #REQUIRED
>
<!ELEMENT XMLRules (%xmlElements;)>
<!ATTLIST XMLRules
type (%gtype; | %stype;) "GROUPED"
id CDATA "xml_rules"
>
<!ELEMENT TagText EMPTY>
<!ATTLIST TagText
tag CDATA #REQUIRED
attributePatterns CDATA ""
>
<!ELEMENT Attribute EMPTY>
<!ATTLIST Attribute
name CDATA #REQUIRED
tag CDATA "*"
valuePatterns CDATA ""
>
```

NOTE You can use * as a part of the rule. But all the mandatory attributes cannot be *. Such rules are ignored, and no error message is displayed.

Enabling Rewriter Debug Information

To enable the rewriter debug:

1. Log in as root to the gateway machine and edit the following file:

   InstallDir/SUNWam/lib/AMConfig.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. The 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.properties file:

   com.iplanet.services.debug.directory=/var/opt/SUNWam/debug

   where /var/opt/SUNWam/debug is the default debug directory.

4. Change the permission of the debug directory as follows:

   chmod -fR 777 *debug directory*

5. Restart the gateway for the changes take effect:

   InstallDir/SUNWps/bin/gateway -n *profilename* start

Debug Files

The following debug files are available:

/var/opt/SUNWam/debug/psSRAPRewriter.*profilename*

This file contains general developer information.

/var/opt/SUNWam/debug/psSRAPRewriter_errors.*profilename*

This file contains logs about serious errors that may cause the rewriter to stop running.

/var/opt/SUNWam/debug/psSRAPRewriter_warning.*profilename*

This file contains logs about warning messages. These are just warnings and may not critically affect the functioning of the rewriter.

`/var/opt/SUNWam/debug/psSRAPRewriter_recordPage.`*profilename*

This file contains the following information about a page that has been rewritten - the page URI, the ruleset that has been applied to the page, the rewritten content, and the original content. Specific warning messages related to parsing also appear in this file.

`/var/opt/SUNWam/debug/psSRAPRewriter_recordURI.`*profilename*

This file contains the following information about the URIs in a page that has been rewritten - page URI, the original URI, absolute URI, and the gateway-prefixed absolute URI.

Mapping of Rules with SP4

The following table lists the mapping of the Sun ONE Portal Server, Secure Remote Access 6.0 rewriter rules with the previous releases of the Sun ONE Portal Server.

Table 5-3 Mapping of Rules with SP4

Rewriter 6.0 DTD Element	Rewriter 3.0 List Box Name
Rules for HTML Content	
Attribute	Rewrite HTML Attributes
JSToken	Rewrite HTML Attributes containing JavaScript
Form	Rewrite Form Input Tag List
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

Table 5-3 Mapping of Rules with SP4 *(Continued)*

Rewriter 6.0 DTD Element	Rewriter 3.0 List Box Name
Function - DJS	Rewrite JavaScript Function Parameters In JavaScript
Rules for XML Content	
Attribute	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 6

Working With Certificates

This chapter explains the authentication mechanisms provided by the Secure Remote Access along with the necessary configuration information.

This chapter covers the following topics:

- Certificate Management
- Certificate Files
- Trust Attributes
- Certificate Authorities (CAs)
- The certadmin Script
- Generating a Self-signed SSL Certificate
- Obtaining and Installing an SSL Certificate From a CA
- Listing Root CA Certificates
- List All Certificates
- Modifying the Trust Attributes of a Certificate

Certificate Management

The Secure Remote Access provides certificate-based authentication for remote users. The Secure Remote Access uses Secure Sockets Layer (SSL) to enable secure communication. The SSL protocol enables secure communication between two machines.

Secure Remote Access 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.

You can either use a certificate that is issued by a Certificate Authority (CA), or generate and use self-signed certificates.

Certificate Files

When Sun ONE Portal Server, Secure Remote Access is installed, a self-signed SSL certificate is created and installed if you have chosen to install a self-signed certificate. If you have chosen not to install a self-signed certificate, only the certificate database is created. Certificate related files are located in `/etc/opt/SUNWps/cert/default`. This directory contains 5 files by default. The files and their descriptions are listed in Table 6-1.

Table 6-1 Certificate Files

Filename	Type	Description
`cert7.db`, `key3.db`, `secmod.db`	Binary	Contain 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 ONE Web Server and are located in *InstallDir*`/netscape/server4/alias`. If necessary, these files can be shared between the Sun ONE Portal Server server and gateway components or the gateway proxy.
`.jsspass`	hidden text file	Contains the password for the encryption module that Sun ONE Portal Server gateway currently uses. The default module is the internal software module.

Table 6-1 Certificate Files

Filename	Type	Description
`.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.

Trust Attributes

The trust attributes of a certificate provide information about:

- Whether the certificate is a regular server certificate (also called user certificate) as opposed to a root certificate
- 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”. For the gateway component, only the first category is useful. 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.

The possible attribute values and the meaning of each value are listed in Table 6-2.

Table 6-2 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)

Table 6-2 Certificate Trust Attributes *(Continued)*

Attribute	Description
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)

Certificate Authorities (CAs)

Most well-known public CAs are already included in the certificate database. The following is the list of all the public CAs included by default, and their trust attributes. See Modifying the Trust Attributes of a Certificate for information on modifying the trust attributes of a public CA. Table 6-3 lists the most common Certificate Authorities with the trust attributes.

Table 6-3 Public Certificate Authorities *(1 of 3)*

Certificate Authority Name	Trust Attributes
ABAecom (sub., Am. Bankers Assn.) Root CA	CG,C,C
American Express CA	C,C,
American Express Global CA	C,C,
Baltimore CyberTrust Code Signing Root	,,C
Baltimore CyberTrust Mobile Commerce Root	CG,C,
Baltimore CyberTrust Root	CG,C,
BelSign Object Publishing CA	,,C
BelSign Secure Server CA	C,,
Deutsche Telekom AG Root CA	C,C,C
Digital Signature Trust Co. Global CA 1	CG,C,C
Digital Signature Trust Co. Global CA 2	CG,C,C
Digital Signature Trust Co. Global CA 3	CG,C,C
Digital Signature Trust Co. Global CA 4	CG,C,C
E-Certify Commerce ID	C,,
E-Certify Internet ID	,C,

Table 6-3 Public Certificate Authorities *(2 of 3)*

Certificate Authority Name	Trust Attributes
Entrust.net Premium 2048 Secure Server CA	C,C,C
Entrust.net Secure Personal CA	C,C,C
Entrust.net Secure Server CA	C,C,C
Equifax Premium CA	C,C,C
Equifax Secure CA	C,C,C
Equifax Secure Global eBusiness CA	C,C,C
Equifax Secure eBusiness CA 1	C,C,C
Equifax Secure eBusiness CA 2	C,C,C
GTE CyberTrust Global Root	CG,C,C
GTE CyberTrust Japan Root CA	CG,C,C
GTE CyberTrust Japan Secure Server CA	CG,C,C
GTE CyberTrust Root 2	CG,C,C
GTE CyberTrust Root 3	CG,C,C
GTE CyberTrust Root 4	CG,C,C
GTE CyberTrust Root 5	CG,C,C
GTE CyberTrust Root CA	CG,C,C
GlobalSign Partners CA	C,C,C
GlobalSign Primary Class 1 CA	C,C,C
GlobalSign Primary Class 2 CA	,C,
GlobalSign Primary Class 3 CA	,C,
GlobalSign Root CA	C,C,C
TC TrustCenter, Germany, Class 0 CA	Cw,C,C
TC TrustCenter, Germany, Class 1 CA	,C,
TC TrustCenter, Germany, Class 2 CA	C,C,C
TC TrustCenter, Germany, Class 3 CA	C,C,C
TC TrustCenter, Germany, Class 4 CA	C,C,C
Thawte Personal Basic CA	,C,C
Thawte Personal Freemail CA	,C,
Thawte Personal Premium CA	,C,C

Table 6-3 Public Certificate Authorities *(3 of 3)*

Certificate Authority Name	Trust Attributes
Thawte Premium Server CA	CG,,C
Thawte Server CA	CG,,C
Thawte Universal CA Root	CG,C,C
ValiCert Class 1 VA	C,C,C
ValiCert Class 2 VA	C,C,C
ValiCert Class 3 VA	C,C,C
ValiCert OCSP Responder	C,C,C
VeriSign Class 4 Primary CA	CG,C,C
Verisign Class 1 Public Primary Certification Authority	,C,
Verisign Class 1 Public Primary Certification Authority - G2	,C,
Verisign Class 1 Public Primary Certification Authority - G3	,C,
Verisign Class 2 Public Primary Certification Authority	,C,C
Verisign Class 2 Public Primary Certification Authority - G2	,C,C
Verisign Class 2 Public Primary Certification Authority - G3	,C,C
Verisign Class 3 Public Primary Certification Authority	CG,C,C
Verisign Class 3 Public Primary Certification Authority - G2	CG,C,C
Verisign Class 3 Public Primary Certification Authority - G3	CG,C,C
Verisign Class 4 Public Primary Certification Authority - G2	CG,C,C
Verisign Class 4 Public Primary Certification Authority - G3	CG,C,C
Verisign/RSA Commercial CA	C,C,
Verisign/RSA Secure Server CA	C,C,

The certadmin Script

When the Sun ONE Portal Server, Secure Remote Access is installed, a self-signed SSL certificate is created and installed.

You can use the `certadmin` script to do additional certificate administration such as:

- Generating a Self-signed SSL Certificate

- Obtaining and Installing an SSL Certificate From a CA
- Installing a Root CA Certificate
- Listing Root CA Certificates
- List All Certificates
- Modifying the Trust Attributes of a Certificate

NOTE `certadmin` does not support multibyte entries. When you invoke any of the options of the `certadmin` tool, and supply a multibyte entry as a value for the questions asked, `certadmin` will not accept the value.

If you generate a certificate signing request (CSR) with multibyte entries using some other utility, `certadmin` will sign the request and handle the certificate.

gwcertutil

The `certadmin` script in *InstallDir*`/SUNWps/bin/` is a script that wraps around the `gwcertutil` command for convenience. The `certadmin` script helps you carry out the conventional tasks related to certificate administration. For any additional functionality, use the `gwcertutil` command directly. For example, use `gwcertutil` to delete a certificate from the certificate database. The command `gwcertutil -H` lists usage.

Generating a Self-signed SSL Certificate

See Generating Self-signed Certificates in Chapter 4, Installing SSL Certificates in the *Sun ONE Portal Server, Secure Remote Access 6.0 Installation Guide* for details.

Obtaining and Installing an SSL Certificate From a CA

During the installation of the gateway component of the Secure Remote Access, 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:

1. Generating a Certificate Signing Request (CSR)
2. Ordering a Certificate from a CA
3. Installing the Certificate from the CA

See Installing Certificates From a Certificate Authority in Chapter 4, Installing SSL Certificates in the *Sun ONE Portal Server, Secure Remote Access 6.0 Installation Guide* for details.

Listing Root CA Certificates

To View the List of Root CAs

1. As root, run the `certadmin` script.

```
# InstallDir/SUNWps/bin/certadmin -n profilename
```

where *profilename* 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) Modify Trust Attributes of Certificate (e.g., for PDC)

6) List Root CA Certificates

7) List All Certificates

8) Quit



choice: [8] 6
```

2. Choose option **6** on the certificate administration menu.

List All Certificates

All certificates and their corresponding trust attributes can be viewed by using the certificate administration script.

To List all the Certificates

1. As root, run the `certadmin` script.

```
# InstallDir/SUNWps/bin/certadmin -n profilename
```

where *profilename* 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) Modify Trust Attributes of Certificate (e.g., for PDC)

6) List Root CA Certificates

7) List All Certificates

8) Quit


choice: [8] 7
```

2. Choose option **7** on the certificate administration menu.

Modifying the Trust Attributes of a Certificate

One case in which the trust attributes of a certificate need 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, for example, the CA certificate should be marked "T" for SSL.

If the gateway component is set up to communicate with an HTTPS site that presents a self-signed certificate, allowing the gateway component to trust any unknown CAs can be a useful approach. However, for a serious deployment, this approach should be used with caution.

To Modify the Trust Attributes for a Certificate

1. As root, run the `certadmin` script.

```
# InstallDir/SUNWps/bin/certadmin -n profilename
```

where *profilename* 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) Modify Trust Attributes of Certificate (e.g., for PDC)

6) List Root CA Certificates

7) List All Certificates
```

```
8) Quit



choice: [8] 5
```

2. Choose option **5** 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.

Appendix A

Configuring the SSL Accelerator

This chapter introduces you to the SSL Accelerator and explains its configuration.

Topics covered include:

- Overview of the SSL Accelerator
- Enabling SSL Hardware Support for the Sun ONE Portal Server, Secure Remote Access
- For More Information

Overview of the SSL Accelerator

Using a hardware accelerator speeds up the execution of cryptographic algorithms, thereby increasing the performance speed.

The Sun Crypto Accelerator 1000 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.

Enabling SSL Hardware Support for the Sun ONE Portal Server, Secure Remote Access

Prerequisites

Ensure that the Sun ONE Portal Server, Secure Remote Access 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 6-4 has two columns. The first column lists the parameter and the second column lists the value.

Table 6-4 SSL Accelerator Installation Checklist

Parameter	Value
Crypto Accelerator	Sun Crypto Accelerator 1000
Secure Remote Access installation base dir	/opt
Secure Remote Access certificate database dir	/etc/opt/SUNWps/cert
Secure Remote Access server certificate nickname	server-cert
Realm	srap
Realm user	crypta

To Configure the SSL Accelerator

NOTE csh is assumed for all shell commands in the following steps.

1. Follow the instructions in the hardware user's guide to install the hardware.
2. Install the following packages from the Sun Crypto Accelerator 1000 install CD.
   - SUNWcrypm

- SUNWcrypu
- SUNWcrysu
- SUNWdcar
- SUNWcrypr
- SUNWcrysl
- SUNWdcamn
- SUNWdcav

3. Install the following patches:

   - 110383-01
   - 108528-05
   - 112438-01

   You can get the patches from the `http://sunsolve.sun.com`

4. Ensure that you have the tools `pk12util` and `modutil`.

   These tools can be found under *InstallDir*`/SUNWps/bin` when you install the Sun ONE Portal Server, Secure Remote Access.

5. Create the `slots` file as follows:

   ```
   vi /etc/opt/SUNWconn/crypto/slots
   ```

6. Include the following single line in the `slots` file:

   ```
   crypta@srap
   ```

7. Create a realm and a user using the following commands:

   ```
   cd InstallDir/SUNWconn/bin
   #./secadm
   secadm> create realm=srap
   System Administrator Login Required
   Login: root
   Password:
   Realm srap created successfully.
   secadm> set realm=srap
   secadm{srap}> su
   ```

```
System Administrator Login Required

Login: root

Password:

secadm{root@srap}# create user=crypta

Initial password:

Confirm password:

User crypta created successfully.

secadm{root@srap}# login user=crypta

Password:
```

See the Sun Crypto Accelerator 1000 User's Guide for details on realms and users.

8. Run the show key command to verify that no keys exist for the user you created.

```
secadm{crypta@srap}> show key

No keys exist for this user.
```

9. Load the Sun Crypto module as follows:

```
cd InstallDir/SUNWps/bin

setenv LD_LIBRARY_PATH InstallDir/SUNWps/lib/solaris/sparc

modutil -dbdir /etc/opt/SUNWps/cert -add "Sun Crypto Module"
-libfile InstallDir/SUNWconn/crypto/lib/libpkcs11.so
```

10. Verify that the Sun Crypto module has been loaded as follows:

```
modutil -list -dbdir /etc/opt/SUNWps/cert
```

11. Export the certificate and the key to the Sun Crypto module as follows:

```
cd InstallDir/SUNWps/bin

setenv LD_LIBRARY_PATH InstallDir/SUNWps/lib/solaris/sparc

pk12util -o servercert.p12 -d /etc/opt/SUNWps/cert -n server-cert

pk12util -i servercert.p12 -d /etc/opt/SUNWps/cert -h
"crypta@srap" -K password -W password
```

12. Run the `show key` command as shown in step 8.

    You should see 2 keys for this user.

13. Change the nickname in the `/etc/opt/SUWNps/cert/.nickname` file.

```
vi /etc/opt/SUWNps/cert/.nickname
```

Replace `server-cert` with `crypta@srap:server-cert`

14. Restart the gateway.

    The gateway is now enabled with the Sun Crypto Hardware Accelerator 1000 support.

For More Information

Sun Crypto Accelerator 1000 User's Guide

http://www.sun.com/products-n-solutions/hardware/docs/pdf/816-2450-10.pdf

Release Notes

http://www.sun.com/products-n-solutions/hardware/docs/pdf/816-2451-10.pdf

More links

http://www.sun.com/products-n-solutions/hardware/docs/Network_Connectivity/Crypto_Boards/

Appendix B

Country Codes

The following table lists the two-letter country codes that you need to specify during certificate administration.

Table B-1 Two-letter Country Codes *(1 of 9)*

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
ba	Bosnia-Herzegovina

Table B-1 Two-letter Country Codes *(2 of 9)*

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
cl	Chile
cm	Cameroon
cn	China
co	Colombia

Table B-1 Two-letter Country Codes *(3 of 9)*

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
fj	Fiji
fk	Falkland Islands
fm	Micronesia
fo	Faroe Islands
fr	France
fx	France (European Territory)
ga	Gabon

Table B-1 Two-letter Country Codes *(4 of 9)*

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 & S. Sandwich Isls.
gt	Guatemala
gu	Guam (USA)
gw	Guinea Bissau
gy	Guyana
hk	Hong Kong
hm	Heard and McDonald Islands
hn	Honduras
hr	Croatia
ht	Haiti
hu	Hungary
id	Indonesia
ie	Ireland
il	Israel
in	India
int	International
io	British Indian Ocean Territory

Table B-1 Two-letter Country Codes *(5 of 9)*

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 & Nevis Anguilla
kp	North Korea
kr	South Korea
kw	Kuwait
ky	Cayman Islands
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

Table B-1 Two-letter Country Codes *(6 of 9)*

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
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

Table B-1 Two-letter Country Codes *(7 of 9)*

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)
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

Table B-1 Two-letter Country Codes *(8 of 9)*

se	Sweden
sg	Singapore
sh	Saint Helena
si	Slovenia
sj	Svalbard and Jan Mayen Islands
sk	Slovak Republic
sl	Sierra Leone
sm	San Marino
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

Table B-1 Two-letter Country Codes *(9 of 9)*

tw	Taiwan
tz	Tanzania
ua	Ukraine
ug	Uganda
uk	United Kingdom
um	USA Minor Outlying Islands
us	United States
uy	Uruguay
uz	Uzbekistan
va	Holy See (Vatican City State)
vc	Saint Vincent & 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

access control Implements the privileges granted by authorization.

address In networking, a unique code that identifies a node to the network. Names like host1.siroe.com are translated to "dotted quad" addresses (1.2.3.4) by the Domain Name Service. (DNS).

administration console The administrator's iPlanet Directory Server Access Management Edition graphical user interface to Sun™ ONE Portal Server 6.0.

API Application Program Interface, a set of calling conventions or instructions defining how programs invoke services in existing software packages.

applet A program written in the Java™ programming language to run within a Web browser. An example would be the Java front end to Sun ONE Portal Server's NetMail and NetFile applications.

attribute Defines the parameters that an iPlanet Directory Server Access Management Edition service provides to an organization. The attributes that make up an iPlanet Directory Server Access Management Edition service are classified as one of the following: Dynamic, Policy, User, Organization, or Global. Using these types to subdivide the attributes in each service allows for a more consistent arrangement of the service schema and easier management of the service parameters.

ASP Access Service Provider. A company that, for a fee, provides access to applications that users can run without owning their own copies. See Internet Service Provider (ISP).

authentication The process of verifying a user's identity.

authentication module An authentication module controls a specific authentication process. For example, Sun ONE Portal Server provides authentication modules for Microsoft Windows NT, UNIX, S/key, and others, as well as opening the authentication API so other authentication modules can be written as needed.

authorization The process of granting specific access privileges to a user. Authorization is based on authentication and enforced by access control.

CA See Certificate Authority.

cache In Web browsers, the archive of recently visited Web pages, graphics, or other files that is stored in memory or on users' disks.

CDP See Certificate Discovery Protocol.

certificate A set of data that identifies a person, machine, or application.

certificate identifier (ID) Generic term used to identify a particular self-generated or issued certificate. It effectively decouples the identification of a key for purposes of key lookup and access control from issues of network topology, routing, and IP addresses.

Certificate Authority (CA) Trusted network entity that digitally signs a certificate containing information that identifies the user; such as the user's name, the issued certificate, and the certificate's expiration date. VeriSign is one of the best known CAs.

channel In the Sun ONE Portal Server Desktop, a channel consists of a provider and configuration. Channels generate content which can consist of markup fragments, a frameset, an HTML page, and so on. Channel content is often aggregated with other channel content to form a portal Desktop.

cipher See encryption algorithm.

component An application or a service in Sun ONE Portal Server. Components have attributes and privileges, much like users.

content filtering Practice of allowing or disallowing traffic based on the content of the data being sent.

content provider A Java class that can write HTML content to a mini-frame in the desktop. Content providers are used to create information in specific areas of a user's desktop.

cookie General mechanism that server-side connections can use to store and retrieve information on the client side of the connection. Cookies are small data files written to a user's hard drive by some Web sites when viewed in a Web browser. These data files contain information that the site can use to track things such as passwords, lists of pages visited, and the date when a certain page was last viewed.

customization The ability to change preferences in the portal such as content received, layout, and color (that is, user-driven). It can also refer to the ability to modify the UI or order of menu events.

data compression Application of an algorithm to reduce the space required to store or the bandwidth required to transmit data.

decryption Process of decrypting information that has been encrypted. See encryption.

demilitarized zone (DMZ) Small protected network between the public Internet and a private intranet, usually demarcated with firewalls on both ends. This area is used to provide limited public access to resources such as Web servers, FTP servers, and other information resources.

Desktop What the user sees on the screen. In the case of Sun ONE Portal Server, it is the HTML presentation of the portal. This usually includes a preferred set of applications and access privileges.

digital signatures Data added to a document to identify the sender using a public-key encryption scheme.

directory server A server that serves out information about people and resources within an organization from a logically centralized repository. See also Lightweight Directory Access Protocol (LDAP), Sun ONE Directory Server, and iPlanet Directory Server Access Management Edition.

DMZ See demilitarized zone.

DNS See Domain Name Service

domain The last part of a fully qualified domain name that identifies the company or organization that owns the domain name (for example, `siroe.com`, `host.siroe.uk`).

Domain Name Service A distributed name and address lookup mechanism used to translate domain names (`siroe.com`) to IP addresses (10.23.134.24). It also allows reverse lookup, to translate IP addresses back into names.

encryption Process of protecting information from unauthorized use by making the information unintelligible. Some encryption methods employ codes, called keys, which are used to encrypt the information. Contrast with *decryption*.

encryption algorithm The method or standard that is used to encrypt the information. Some of the common encryption algorithms are RC4 and RC6.

end user Refers to the person serviced by the customer (for example, a corporate employee).

Extensible Markup Language (XML) XML, a programming language, is essentially a simplified version of SGML that enables Web developers to create customized tags that will organize and deliver content more efficiently. XML is a metalanguage, containing a set of rules for constructing other markup languages. By enabling people to create their own tags, it expands the amount and kinds of information that can be provided about the data held in documents.

File Transfer Protocol (FTP) A file transfer protocol often used on TCP/IP networks to copy files to and from remote computers.

firewall Computer situated between an internal network and the rest of the network, and filters data packets according to user-specified criteria. Firewalls are normally used to protect systems on one side from unauthorized access by users on the other side.

FTP See File Transfer Protocol

fully qualified domain name (FQDN) The complete domain name of a system, including the host name, network name if applicable, and domain; for example `host1.siroe.com`.

gateway A system that provides and controls connections to another network. The gateway in Sun ONE Portal Server 6.0 is part of Secure Remote Access. See *VPN*.

host Name of a device on a TCP/IP network that has an IP address.

HTML Hypertext Markup Language. A file format, based on SGML, for hypertext documents on the Internet.

HTTP Hypertext Transfer Protocol, which describes how Web browsers and Web servers exchange information. See *URL*.

HTTPS Hypertext Transfer Protocol Secure, which describes the use of HTTP over an SSL connection, usually on port 443.

ICMP Internet Control Message Protocol. IP protocol that handles errors and control messages, to enable routers to inform other routers (or hosts) of IP routing problems or make suggestions of better routes. See *ping*.

IMAP Internet Message Access Protocol allows remote access to mailboxes and folders. IMAP clients usually leave some or all messages and folders on the server, unlike POP, in which all messages are downloaded.

Internet Protocol Protocol within TCP/IP suite used to link networks worldwide, developed by the United States Department of Defense and used on the Internet. The prominent feature of this suite is the IP protocol.

IP See Internet Protocol.

iPlanet Compass Server iPlanet's technology to improve user access to network resources typically used with iPlanet Portal Server 3.0. Sun ONE Portal Server 6.0 contains a tightly integrated Search Engine which provides the functionality that iPlanet Compass Server provided with iPlanet Portal Server 3.0.

iPlanet Directory Server Access Management Edition Provides user and service management, authentication, and single-sign-on services, policy management, logging services, debug utility, the admin console, and client support interfaces for Sun ONE Portal Server.

ISP Internet Service Provider. A company providing Internet access. This service often includes a phone number access code, username, and software—all for a provider fee.

issued certificate Certificate that is issued by a Certificate Authority. See self-generated certificate.

ISV Independent Software Vendor. Third-party software developer.

J2ME See Java 2 Platform, Micro Edition.

JATO A library for converting between Java and XML.

Java Object-oriented, platform-independent programming language developed by Sun Microsystems to solve a number of problems in modern programming practice.

Java 2 Platform, Micro Edition (J2ME) Small application environment suitable for mobile devices.

Java Development Kit (JDK) Software tools used to write Java applets or application programs.

JDK See Java Development Kit.

JSP Java Server Page.

JSS See Network Security Services for Java.

key Code for encrypting or decrypting data.

LAN Local area network, a private network at a single location. Multiple LANs can be interconnected to form a WAN.

LDAP Data Interchange Format (LDIF) The format used to represent Directory Server entries in text form.

Lightweight Directory Access Protocol (LDAP) Directory service protocol designed to run over TCP/IP and across multiple platforms. A simplification of the X.500 Directory Access Protocol (DAP) that allows a single point of management for storage, retrieval, and distribution of information, including user profiles, distribution lists, and configuration data across Sun ONE servers. Sun ONE Directory Server uses the LDAP protocol.

load balancer A load balancer controls connections to multiple gateway machines to allow approximately equivalent loads on each of the available systems.

NetFile Java-based file server application that enables users remote access to file systems as well as enabling remote operations on files and directories. This component is available with Sun ONE Portal Server, Secure Remote Access.

Netlet A Java applet used in Sun ONE Portal Server to allow any TCP/IP-based applications to securely connect to servers through an authenticated Sun ONE Portal Server connection. This component is available with Sun ONE Portal Server, Secure Remote Access.

NFS™ Network File System. A file system distributed by Sun Microsystems that enables a set of computers to cooperatively access each others files in a transparent manner.

node A transfer point within a network. Data is passed from node to node in a network until the data reaches its final destination. Used interchangeably with machine.

organization In iPlanet Directory Server Access Management Edition, an object that represents the top level of a hierarchical structure used by an enterprise to manage its departments and resources. Upon installation, iPlanet Directory Server Access Management Edition dynamically creates a top-level organization (`default o=isp`) to manage the iPlanet Directory Server Access Management Edition enterprise configurations. Additional organizations can be created after installation to manage separate enterprises. All created organizations fall beneath the top-level organization. See also suborganization.

passphrase Collection of characters used in a similar manner to, although typically longer than, a password. See password.

password Unique string of characters that a user types as an identification code; a security measure to restrict access to computer systems and sensitive files.

personal digital certificate (PDC) An electronic certificate attached to a message that authenticates a user. A personal digital certificate can be created by correctly entering a user ID and password, or by using an SSL certificate request that in turn uses the security certificate of the server through which the user is connected. 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 mechanism of authentication.

PDC See personal digital certificate.

POP Post Office Protocol. Defines a mechanism with which Internet users can connect to and download their waiting email messages.

PPP See *Point-to-Point Protocol*.

port The location (or socket) to which TCP/IP connections are made. Web servers traditionally use port 80, while FTP uses port 21 and telnet uses port 23. Sun ONE Portal Server uses some special ports, particularly on client systems, to securely communicate through the Sun ONE Portal Server session to servers.

portal A "doorway" or entry point to a set of resources that an enterprise wants to make available to the portal's users. For some consumer portals, the set of resources includes the entire World Wide Web, but for most enterprises, the set of resources includes information, applications, and other resources that are specific to the relationship between the user and the enterprise. The Sun ONE Portal Server Desktop is the application used to generate the portal in Sun ONE Portal Server.

portal node A physical machine that is running Sun ONE Portal Server software or Sun ONE Portal Server Pack software. Also called a "host."

privilege A type of access right that is granted to a user, a set of users, or a resource that is specified by the particular type of authorization implemented.

protocol A formal description of messages to be exchanged and rules to be followed for two or more systems to exchange information.

provider The programmatic aspect of a channel. Adding configuration data to a provider differentiates it into an instance of a channel. A provider is a Java class and is responsible for converting the content in a file, or the output of an application or service into the proper format for a channel. A number of providers are shipped with the iPlanet Portal Server including a bookmark provider, an application provider, and a notes provider. As the Desktop is imaged, each provider is queried in turn for the content of its associated channel. Some providers are capable of generating multiple channels based upon their configuration.

Examples of content providers include the UserInfoProvider and BookmarkProvider.

Examples of container providers include the TabContainerProvider and SingleContainerProvider.

Examples of leaf providers include the JSPProvider, XMLProvider, URLScraperProvider and SimpleWebServicesProvider.

proxy An intermediary program that makes and services requests on behalf of clients. Proxies act as servers and clients in turn and are used to control the content of various network services. See reverse proxy.

preference A user-specified choice about what appears or does not appear on the desktop, and how it appears, or other traits such as timeout settings.

private network A network of computers that is inaccessible unless you have appropriate access privileges. Private networks may be as small as a one-office LAN or as large as a multi-country enterprise network. See also public network.

privilege A type of access right that is granted to a user, a set of users, or a resource that is specified by the particular type of authorization implemented.

profile The attributes and privileges for a Sun ONE Portal Server entity, such as user, role, domain, or component.

profile server A special segment of Sun ONE Portal Server that is devoted to storing profile information.

protocol A formal description of messages to be exchanged and rules to be followed for two or more systems to exchange information.

provider A Java class that can write HTML content to a mini-frame in the desktop. Providers (also called content providers) are used to create information in specific areas of a user's desktop.

proxy An intermediary program that makes and services requests on behalf of clients. Proxies act as servers and clients in turn, and are used to control the content of various network services. See reverse proxy.

public-key certificate A data structure containing a user's public key, as well as information about the time and date during which the certificate is valid.

public-key cryptography Also known as asymmetric key cryptography. In public-key cryptosystems, everyone has two related complementary keys: a publicly revealed key and a *secret* key (also called a private key). Each key unlocks the code that the other key makes. Knowing the public key does not help you deduce the corresponding secret key. The public key can be published and widely disseminated across a communications network. This protocol provides privacy without the need for the secure channels that a conventional cryptosystem requires.

public network Like the Internet, a public network carries traffic from a variety of companies, individuals, and sources and is inherently insecure. Contrast with private network.

reverse proxy A proxy which performs bi-directional URL rewriting and translation between clients and servers. Unlike a proxy, which exists at the client side, a reverse proxy exists at the server side of the network. In Sun ONE Portal Server, the reverse proxy exists on the gateway.

Rewriter The Rewriter provides a Java class library for rewriting URL references in various web languages such as HTML, Javascript, and XML and in HTTP location headers (redirections). The Rewriter defines an iPlanet Directory Server Access Management Edition service for storing rules that define how rewriting is to be done and the data to be rewritten. The Rewriter also includes an admin console module for editing these rules.

role Defines all aspects of a user's experience when running in the Sun ONE Portal Server environment. A role can correspond to a job title (such as manager, engineer, and sales) or can be defined in other ways, such as a full member of a working group or an observer. A role determines what a user sees and can use on the desktop.

Secure Socket Layer (SSL) A form of secure, low-level encryption that is used by other protocols such as HTTP and FTP. The SSL protocol includes provisions for server authentication, encryption of data in transit, and optional client authentication. The version used in Sun ONE Portal Server uses RSA's public and private key encryption, as well as a digital certificate.

self-generated certificate Public key value only used when entities are named using the message digest of their public value, and when these names are securely communicated. See issued certificate.

Server Message Block (SMB) protocol A protocol that provides a method for client applications in a computer to read and write to files on and to request services from server programs in a computer network. The SMB protocol can be used over the Internet on top if its TCP/IP protocol or on top of other network protocols such as Internetwork Packet Exchange and NetBEUI. Sun ONE Portal Server uses SMB for NetFile.

session An Sun ONE Portal Server session is a sequence of interactions between a user and one or more applications, starting with login and ending with logout or timeout.

session key Common cryptographic technique to encrypt each individual conversation between two people with a separate key.

SGML See Standard Generalized Markup Language.

shared-key cryptography Also known as symmetric key cryptography. Cryptography where each party must have the same key to encrypt or decrypt ciphertext.

Simple Mail Transfer Protocol (SMTP) The email protocol most commonly used by the Internet and the protocol supported by the Sun ONE Messaging Server. Defined in RFC 821, with associated message format descriptions in RFC 822.

Simple Network Management Protocol (SNMP) Network management protocol that enables a user to monitor and configure network hosts remotely.

Simple Object Access Protocol (SOAP) A lightweight protocol for exchange of information in a decentralized, distributed environment. SOAP is an XML-based protocol.

single sign-on (SSO) The ability for a user to authenticate once and gain access to multiple services.

SMB protocol See Server Message Block protocol.

SMTP See Simple Mail Transfer Protocol.

SMTP proxy A variant of SMTP that sends messages from one computer to another on a network and is used on the Internet to route email.

SNMP See Simple Network Management Protocol.

SSL See Secure Socket Layer.

SSL Certificate An electronic token that means you or a vendor have given approval to encrypt and decrypt your secure transactions, using PKI. You create a self-signed SSL Certificate when you install Sun ONE Portal Server software. However, you can also obtain an SSL Certificate from a certificate vendor who authorizes secure communications services over the Internet.

SSO See single sign-on.

Standard Generalized Markup Language (SGML) Method of tagging a document to apply to many format elements.

static web content Refers to static HTML files, images, applet JAR files, and anything else that can be served up directly by the web server without using the Java web container. For Sun ONE Portal Server, this gets installed in the web server (same place as dynamic web application).

subdomain The next-to-last part of a fully qualified domain name that identifies the division or department within a company or organization that owns the domain name (for example, support.siroe.com, sales.siroe.com); not always specified.

suborganization In iPlanet Directory Server Access Management Edition, an object created under an organization and used by an enterprise for more granular control of its departments and resources. For example, when setting up your Sun ONE Portal Server, you might create a suborganization called `mycompany` under the top-level object `isp`.

Sun ONE Directory Server Provides the primary configuration and user profile data repository for Sun ONE Portal Server. It is installed by the iPlanet Directory Server Access Management Edition product if it is not already installed on the Sun ONE Portal Server system.

Sun ONE Portal Server Enables remote users to securely access their organization's network and its services over the Internet. Additionally, it creates a secure Internet portal, providing access to content, applications, and data to any targeted audience-employees, business partners, or the general public.

This is also referred to as the "core" part of the complete Sun ONE Portal Server product solution that is shared among all Sun ONE Portal Server packs.

Sun ONE Portal Server Desktop Often referred simply as "Desktop." Provides the primary end-user interface and a mechanism for extensible content aggregation through the Content Provider Interface (PAPI). The Desktop includes a variety of providers that provide a container hierarchy and the basic building blocks for building some types of channels. The Desktop implements a display profile data storage mechanism on top of an iPlanet Directory Server Access Management Edition service for storing content provider and channel data. The Desktop also includes an admin console module for editing the display profile and other Desktop service data.

Sun ONE Portal Server Instant Collaboration Pack Sun ONE's instant messaging product which includes the server, multiplexor and Sun ONE Instant Messenger components. Also known as Sun ONE Instant Messaging Server.

Sun ONE Web Server In Sun ONE Portal Server, it is used as the web container for Sun ONE Portal Server and Sun ONE Portal Server pack web applications. Sun ONE Web Server is included with the iPlanet Directory Server Access Management Edition product.

symmetric key cryptography See shared-key cryptography.

TCP See transmission control protocol.

TCP/IP Transmission Control Protocol / Internet Protocol. Protocol suite originally developed for the Internet. It is also called the Internet protocol suite. Solaris networks run on TCP / IP by default.

target host The host or machine that you are trying to access.

telnet Virtual terminal protocol in the Internet suite of protocols. Enables users of one *host* to log in to a remote host and interact as normal terminal users of that host.

telnet proxy An application which sits between the telnet client and telnet server and acts as an intelligent relay.

transmission control protocol (TCP) Major transport protocol in the Internet suite of protocols providing reliable, connection-oriented, full-duplex streams. Uses IP for delivery. Encrypts only IP packet data, but not the headers. Corresponds to the transport layer, which is the fourth of the seven ISO layers. See TCP / IP.

transparent clustering A condition whereby multiple machines appear as a single machine to the user. In Sun ONE Portal Server, the condition where multiple gateways appear as a single gateway to the user.

tunneling Process of encrypting an entire IP packet, and wrapping it in another (unencrypted) IP packet. The source and destination addresses on the inner and outer packets may be different.

tunnel address Destination address on the outer (unencrypted) IP packet to which tunnel packets are sent. Generally used for encrypted gateways where the IP address of the host serves as the intermediary for any or all hosts on a network whose topology must remain unknown or hidden from the rest of the world.

Uniform Resource Indicator (URI) A standard notation for specifying the path and file name of a resource on a server. The server translates the URI into the native format for its operating system.

URL Uniform Resource Locator. A code that searches for the location of a specific address on the Internet.

user ID Name by which a user is known to the system.

Virtual Private Network A network with the appearance and functionality of a regular network, but which is really like a private network within a public one. The use of encryption in the lower protocol layers provides a secure connection through an otherwise insecure network, typically the Internet. VPNs are generally cheaper than true private networks using private lines, but rely on having the same encryption system at both ends. The encryption may be performed by firewall software or possibly by routers.

VPN gateway The entry point to a VPN. Typically protected by a firewall.

VPN See Virtual Private Network.

Watchdog A process that monitors a gateway and restarts the gateway if its processes fail.

Web page Document on the Web.

web server An application that responds to web requests such as HTTP and FTP.

World Wide Web Network of servers on the Internet that provide information and can include hypertext links to other documents on that server and often other servers as well.

XML See Extensible Markup Language.

XSL See Extensible Style Language.

Index

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

W