



Sun Java™ System

Portal Server Secure Remote Access 6 Administration Guide

2005Q4

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

Part No: 819-4158-10

Copyright © 2005 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.sun.com/patents> and one or more additional patents or pending patent applications in the U.S. and in other countries.

THIS PRODUCT CONTAINS CONFIDENTIAL INFORMATION AND TRADE SECRETS OF SUN MICROSYSTEMS, INC. USE, DISCLOSURE OR REPRODUCTION IS PROHIBITED WITHOUT THE PRIOR EXPRESS WRITTEN PERMISSION OF SUN MICROSYSTEMS, INC.

U.S. Government Rights - Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

This distribution may include materials developed by third parties.

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

Sun, Sun Microsystems, the Sun logo, Java, Solaris, JDK, Java Naming and Directory Interface, JavaMail, JavaHelp, J2SE, iPlanet, the Duke logo, the Java Coffee Cup logo, the Solaris logo, the SunTone Certified logo and the Sun ONE logo are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon architecture developed by Sun Microsystems, Inc.

Legato and the Legato logo are registered trademarks, and Legato NetWorker, are trademarks or registered trademarks of Legato Systems, Inc. The Netscape Communications Corp logo is a trademark or registered trademark of Netscape Communications Corporation.

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

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

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

Copyright © 2005 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, Etats-Unis. Tous droits réservés.

Sun Microsystems, Inc. détient les droits de propriété intellectuelle relatifs à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et ce sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plus des brevets américains listés à l'adresse <http://www.sun.com/patents> et un ou les brevets supplémentaires ou les applications de brevet en attente aux Etats - Unis et dans les autres pays.

CE PRODUIT CONTIENT DES INFORMATIONS CONFIDENTIELLES ET DES SECRETS COMMERCIAUX DE SUN MICROSYSTEMS, INC. SON UTILISATION, SA DIVULGATION ET SA REPRODUCTION SONT INTERDITES SANS L'AUTORISATION EXPRESSE, ECRITE ET PREALABLE DE SUN MICROSYSTEMS, INC.

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

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, Java, Solaris, JDK, Java Naming and Directory Interface, JavaMail, JavaHelp, J2SE, iPlanet, le logo Duke, le logo Java Coffee Cup, le logo Solaris, le logo SunTone Certified et le logo Sun[tm] ONE sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

Legato, le logo Legato, et Legato NetWorker sont des marques de fabrique ou des marques déposées de Legato Systems, Inc. Le logo Netscape Communications Corp est une marque de fabrique ou une marque déposée de Netscape Communications Corporation.

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

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

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

Contents

List of Figures	11
List of Tables	13
List of Procedures	15
Preface	21
Who Should Read This Book	21
How This Book is Organized	22
Conventions Used in This Book	24
Typographic Conventions	24
Default Paths and File Names	25
Using Linux	25
Limitations Using Linux	25
Comparison of Solaris and Linux Path Names	26
Related Information	26
Books in This Documentation Set	26
Other Portal Server Documentation	27
Other Server Documentation	27
Accessing Sun Resources Online	27
Contacting Sun Technical Support	28
Related Third-Party Web Site References	28
Sun Welcomes Your Comments	28
Chapter 1 Introduction to Portal Server Secure Remote Access	29
Overview of SRA Software	29
Open Mode	30
Secure Mode	31

SRA Services	33
Gateway	33
Rewriter	33
NetFile	33
Netlet	34
Proxylet	34
Administering the SRA Product	34
Configuring SRA Attributes	34
Setting Conflict Resolution	36
Supported Applications	36
Chapter 2 The Gateway	39
Overview of the Gateway	40
Creating a Gateway Profile	40
Understanding the platform.conf File	42
Creating Instances of a Gateway	48
Creating Multi-homed Gateway Instances	51
Creating Gateway Instances Using the Same LDAP	51
Running the Gateway in the chroot Environment	52
Restarting Gateway in the chroot Environment	55
Starting and Stopping the Gateway	56
Restarting the Gateway	57
Specifying a Virtual Host	58
Specifying a Proxy to Contact Access Manager	58
Using Web Proxies	59
Using Automatic Proxy Configuration	65
Specifying PAC File Location	68
Adding Services in Separate Sessions	68
Using a Netlet Proxy	68
Creating Instances of a Netlet Proxy	72
Enabling a Netlet Proxy	73
Restarting a Netlet Proxy	73
Using a Rewriter Proxy	74
Creating Instances of a Rewriter Proxy	74
Enabling a Rewriter Proxy	76
Restarting a Rewriter Proxy	76
Using a Reverse Proxy with the Gateway	77
Obtaining Client Information	77
Using Authentication Chaining	80
Using Wild Card Certificates	81
Disabling Browser Caching	81
Customizing the Gateway Service User Interface	82
Sharing LDAP Directories	83

Using Federation Management	84
Federation Management Scenario	84
Configuring Federation Management Resources	85
Chapter 3 Proxylet and Rewriter	91
Overview of Proxylet	92
Advantages of Using Proxylet	93
Configuring Proxylet	93
HTTPS Support	93
Overview of Rewriter	94
Character Set Encoding	94
Rewriter Usage Scenarios	94
URLScraper	95
The Gateway	95
Writing Rulesets	96
Public Interface (RuleSet DTD)	96
Sample XML DTD	99
Procedure to Write Rules	101
Ruleset Guidelines	101
Defining the RuleSet Root Element	102
Using the Recursive Feature	103
Defining Language Based Rules (Defining Rules)	103
Rules for HTML Content	103
Rules for JavaScript Content	110
Rules for XML Content	125
Rules for Cascading Style Sheets	128
Rules for WML	128
Using the Recursive Feature	128
Configuring Rewriter in the Gateway Service	128
Basic Tasks	129
Advanced Tasks	134
Troubleshooting Using Debug Logs	138
Setting the Rewriter Debug Level	138
Debug File Names	139
Working Samples	141
Samples for HTML Content	142
Samples for JavaScript Content	151
Sample for XML Attributes	171
Case Study	173
Mapping of 6.x RuleSet with 3.0	178

Chapter 4 NetFile	181
Overview of NetFile	181
Supported File Access Protocols	182
Setting NetFile Locale	184
Opening Files from a Local Host	184
Enabling Debugging for NetFile	184
Enabling Logging for NetFile	185
Chapter 5 Netlet	187
Overview of Netlet	187
Netlet Components	188
Netlet Usage Scenario	190
Working With Netlet	190
Downloading an Applet From a Remote Host	191
Defining Netlet Rules	191
Types of Rules	195
Netlet Rule Examples	198
Sample Netlet Rules	203
Enabling Netlet Logging	208
Enable Debug Logging	208
Running Netlet in a Sun Ray Environment	209
New HTML File	209
Deprecated HTML File:	211
Chapter 6 Netlet With PDC	213
Configuring Netlet for PDC	213
Chapter 7 Certificates	215
Overview of SSL Certificates	216
Certificate Files	216
Certificate Trust Attributes	217
CA Trust Attributes	218
The certadmin Script	222
Generating Self-Signed Certificates	222
Generating a Certificate Signing Request (CSR)	224
Adding a Root CA Certificate	227
Installing SSL Certificates From the Certificate Authority	228
Ordering a Certificate from a CA	228
Installing a Certificate from a CA	229
Deleting a Certificate	230
Modifying the Trust Attributes of a Certificate	232
Listing Root CA Certificates	233

Listing All Certificates	235
Printing a Certificate	236
Chapter 8 Configuring URL Access Control	239
Set up a Denied URLs List	240
Set up a Allowed URLs List	240
Manage Single Sign-On	241
Chapter 9 Configuring the Gateway	243
The Core Tab	244
Enable HTTP and HTTPS Connections	245
Enable and Create a List of Rewriter Proxies	246
Enable Netlet	247
Enable and Create a List of Netlet Proxies	248
Enable Proxylet	249
Enable Cookie Management	249
Enable HTTP Basic Authentication	250
Enable Persistent HTTP Connections	252
Specify the Maximum Number of Requests per Persistent Connection	252
Specify Timeout for Persistent Socket Connections	253
Specify Grace Timeout to Account for Turnaround Time	253
Create List of URLs for Cookie Forwarding	254
Specify the Maximum Connection Queue Length	256
Specify the Gateway Timeout	256
Specify the Maximum Thread Pool Size	257
Specify the Cached Socket Timeout	257
Create List of Portal Servers	258
Specify Server Retry Interval	259
Enable Storage of External Server Cookies	260
Obtain a Session from a URL	260
Set Minimum Gateway Authentication Level	261
Enable Marking Cookies as Secure	262
The Proxies Tab	262
Enable Usage of Web Proxies	263
Create List of URLs for Webproxies	263
Create List of URLs for Proxies Not to be Used	264
Create List of Proxies for Domains and Subdomains	265
Create List of Proxy Passwords	265
Enable Automatic Proxy Configuration Support	266
Specify Automatic Proxy Configuration File Location	267
Enable Netlet Tunneling Through Web Proxy	268
The Security Tab	268

Create List of Non-authenticated URLs	269
Create List of Certificate-Enabled Gateway Hosts	269
Allow 40-bit Encryption Connections	270
Enable SSL Version 2.0	271
Enable SSL Cipher Selection	272
Enable SSL Version 3.0	272
Enable Null Ciphers	273
Create List of Trusted SSL Domains	273
Configure Personal Digital Certificate (PDC) Authentication	274
The Rewriter Tab	278
Enable Rewriting of All URIs	278
Create List of URIs to RuleSet Mappings	279
Create List of MIME Types to Parse	281
Create List of URIs Not to Rewrite	282
Specify the Default Domains	283
Enable MIME Guessing	284
Create List of URI Mappings to Parse	284
Enable Masking	285
Specify the Masking Seed String	286
Create List of URIs Not to Mask	286
Make a Gateway Protocol the Same as the Original URI Protocol	287
The Logging Tab	288
Enable Logging	288
Change the Log User Password	289
Enable Netlet Logging	290
Chapter 10 Configuring NetFile	291
The Hosts Tab	292
Specify the OS Character Set	292
Specify Host Detection Order	293
Configure a Common Hosts List	294
Specify the Default Domain	295
Specify the Windows Domain/Workgroup	296
Specify the Default WINS/DNS Server	297
Specify Access to Different Types of Hosts	297
Configure the Allowed Hosts List	298
Configure the Denied Hosts List	299
The Permissions Tab	300
The View Tab	302
Specify the NetFile Window Size	302
Specify the NetFile Window Location	303
The Operations Tab	304
Specify the Temporary Files Directory	304

Set the File Upload Size Limit	305
Specify the Search Directories Limit	306
Specify Compression	307
The General Tab	307
Specify the MIME-types Configuration File Location	307
Chapter 11 Configuring Netlet	309
Assign Netlet Service to a User	310
Add a Netlet Rule	311
Modify an Existing Netlet Rule	312
Delete a Netlet Rule	313
Specify the Default Encryption Cipher	313
Assign the Default Loopback Port	314
Enable Reauthentication for Connections	315
Display Warning Popup for Connections	315
Enable the Display Checkbox in Port Warning Dialog	316
Set the Keep Alive Interval	317
Set the Terminate Netlet at Portal Logout Option	317
Define Access to Netlet Rules	318
Deny Access to Netlet Rules	319
Allow Access to Hosts	320
Deny Access to Hosts	320
Launch Netlet	321
Proxy Configuration	322
Chapter 12 Configuring Proxylet	325
Configure Proxylet	325
Chapter 13 Configuring SSL Accelerators	327
Overview	327
Sun Crypto Accelerator 1000	327
Enable Crypto Accelerator 1000	328
Configure Crypto Accelerator 1000	328
Sun Crypto Accelerator 4000	331
Enable Crypto Accelerator 4000	331
Configure Crypto Accelerator 4000	332
External SSL Device and Proxy Accelerators	334
Enable an External SSL Device Accelerator	334
Configure an External SSL Device Accelerator	335

Appendix A Log Files	337
Appendix B Configuration Attributes	339
Access List Service	339
Gateway Service	340
Core	340
Proxies	343
Security	343
Rewriter	345
Logging	348
NetFile Service	348
Hosts	348
Permissions	350
View	350
Operations	350
General	352
Netlet Service	352
Proxylet Service	354
Appendix C Country Codes	355
Glossary	365

List of Figures

Figure 1-1	The Portal Server in Open Mode	31
Figure 1-2	Portal Server in Secure Mode (with SRA software)	32
Figure 2-1	Web Proxy Management	60
Figure 2-2	Implementation of Netlet Proxy	71
Figure 5-1	Netlet Components	188

List of Tables

Table 1	How This Book is Organized	22
Table 2	Typographic Conventions	24
Table 3	Default Paths and File Names	25
Table 4	Comparison of Solaris and Linux Path Names	26
Table A-1	Informational and Debug Files	337
Table B-1	Access List Service Attributes	339
Table B-2	Gateway Service Core Attributes	340
Table B-3	Gateway Service Proxies Attributes	343
Table B-4	Gateway Service Rewriter Attributes - Basic	345
Table B-5	Gateway Service Rewriter Attributes - Advanced	347
Table B-6	Gateway Service Logging Attributes	348
Table B-7	NetFile Service Hosts Configuration Attributes	349
Table B-8	NetFile Service Hosts Access Attributes	349
Table B-9	NetFile Service Permissions Attributes	350
Table B-10	NetFile Service View Attributes	350
Table B-11	NetFile Service Operations - Traffic Attributes	351
Table B-12	NetFile Service Operations - Search Attributes	351
Table B-13	NetFile Service Operations - Compression Attributes	352
Table B-14	NetFile Service - General Attribute	352
Table B-15	Netlet Service Attributes	352
Table B-16	Proxylet Service Attributes	354
Table C-1	Two-letter Country Codes	355

List of Procedures

To Set the Conflict Resolution Level	36
To Create a Gateway Profile	41
To Install chroot	52
To Restart Gateway in the chroot Environment	55
To Start the Gateway	56
To Stop the Gateway	57
To Restart the Gateway with a Different Profile	57
To Restart the Gateway	57
To Configure the Gateway Watchdog	58
To Specify a Virtual Host	58
To Specify a Proxy	58
To Restart a Netlet Proxy	73
To Configure a Netlet Proxy Watchdog	74
To Restart a Rewriter Proxy	76
To Configure a Rewriter Proxy Watchdog	76
To Enable a Reverse Proxy	77
To Add Authentication Modules to an Existing PDC Instance	80
To Disable Browser Caching	82
To Enable the Gateway to Rewrite All URLs	129
To Map a URI to RuleSet	131
To Specify MIME Mappings	132
To Specify the URIs Not to Rewrite	133
To Specify the Default Domains	133
To Enable MIME Guessing	134
To Parse URI Mappings	135
To Enable Masking	135
To Specify the Masking Seed String	136

To Specify Not to Mask the URI List	137
To Make a Gateway Protocol the Same as the Original URI Protocol	137
To Set the Rewriter Debug Level	138
To Use the HTML Attributes Sample	142
To Use the HTML JavaScript Token Sample:	144
To Use the Form Sample	147
To Use the Sample for Applets	149
To Use the JavaScript URL Variables Sample	151
To Use the JavaScript Expression Variables Sample	154
To Use the JavaScript DHTML Variables Sample	156
To Use the JavaScript DJS Variables Sample	159
To Use the JavaScript System Variables Sample	161
To Use the JavaScript URL Functions Sample	163
To Use the JavaScript Expressions Function Sample	165
To Use the JavaScript DHTML Functions Sample	167
To Use the JavaScript DJS Functions Sample	169
To Use the XML Attributes Sample	171
To Configure the OWA Ruleset	177
To Allow a Local File to be Opened	184
To Run Netlet After a Rule is Added	202
To Configure Netlet for PDC	213
To Generate a Self-Signed Certificate After Installation	222
To Generate a CSR	225
To Add a Root CA Certificate	227
To Order a Certificate From a CA	228
To Install a Certificate From a CA	229
To Delete a Certificate	230
To Modify the Trust Attributes for a Certificate	232
To View the List of Root CAs	233
To List All the Certificates	235
To Print a Certificates	236
To Configure URL Access Control	239
To Set up the Denied URL List	240
To Set up the Allowed URLs List	240
To Disable Single Sign On for Hosts	241
To Enable Single Sign On per Session	242
To Specify Authentication Levels	242

To Configure the Gateway Attributes	243
To Configure the Gateway to Run in HTTP or HTTPS Mode	245
To Enable Rewriter Proxies and Create a List of Rewriter Proxies	246
To Enable Netlet	247
To Enable Netlet Proxies and Create a List of Netlet Proxies	248
To Enable Proxylet	249
To Enable Cookie Management	250
To Enable HTTP Basic Authentication	251
To Enable Persistent HTTP Connections	252
To Specify the Maximum Number of Requests per Persistent Connection	252
To Specify the Timeout for a Persistent Socket Connection	253
To Specify Timeout to Account for Turnaround Time	254
To Add a Forward Cookie URL	255
To Specify the Maximum Connection Queue Length	256
To Specify the Gateway Timeout	256
To Specify the Maximum Thread Pool Size	257
To Specify the Cached Socket Timeout	258
To Specify Portal Servers	258
To Specify Portal Server Retry Interval	259
To Store External Server Cookies	260
To Obtain a Session from a URL	260
To Set Minimum Gateway Authentication Level	261
To Mark Cookies as Secure	262
To Enable Usage of Web Proxies	263
To Specify URLs for Webproxies	263
To Specify URLs Not To Be Used	264
To Specify Proxies for Domains and Subdomains	265
To Specify Proxy Passwords	266
To Enable Automatic Proxy Configuration Support	266
To Specify Automatic Proxy Configuration File Location	267
To Enable the Tunnel Netlet Through Web Proxy	268
To Specify Non-authenticated URL Paths	269
To Add the Gateway to the Certificate-Enabled Gateway Hosts List	269
To Allow 40-bit Encryption Connections	270
To Enable SSL Version 2.0	271
To Enable Individual Cipher Selection	272
To Enable SSL Version 3.0	272

To Enable Null Ciphers	273
To Create List of Trusted SSL Domains	273
To Configure PDCs and Encoded Devices	275
To Enable the Gateway to Rewrite All URIs	278
To Map a URI to RuleSet	280
To Configure the OWA RuleSet	281
To Specify MIME Mappings	282
To Specify the URIs Not to Rewrite	282
To Specify Default Domains	283
To Enable MIME Guessing	284
To Parse URI Mappings	284
To Enable Masking	285
To Specify the Masking Seed String	286
To Specify Not to Mask URIs	286
To Make a Gateway Protocol the Same as the Original URI Protocol	287
To Enable Gateway Logging	288
To Change the Log User Password	289
To Enable Netlet Logging	290
To Set the NetFile Locale	291
To Configure NetFile Attributes	291
To Specify the OS Character Set	293
To Specify the Host Detection Order	293
To Configure the Common Hosts List	294
To Specify the Default Domain	296
To Specify the Default Windows Domain or Workgroup	296
To Specify the Default WINS/DNS Server	297
To Specify Access to Different Types of Hosts	298
To Create the Allowed Hosts List	299
To Create a Denied Hosts List	300
To Enable/Disable Permissions	301
To Specify the Size of the NetFile Window	302
To Specify the Location of the NetFile Window	303
To Specify a Temporary Directory	304
To Set the File Upload Size Limit	305
To Specify the Search Directories Limit	306
To Specify the Default Compression Type	307
To Specify the Location of the MIME-types Configuration File	308

To Add a Netlet Rule	311
To Modify a Netlet Rule	312
To Delete a Netlet Rule	313
To Specify the Default Cipher	314
To Assign the Default Loopback Port	314
To Enable Reauthentication for Connections	315
To Enable the Warning Popup for Connections	315
To Allow the User to Suppress the Port Warning Dialog	316
To Set the Keep Alive Interval	317
To Set the Terminate Netlet at Portal Logout Option	317
To Define Access to Netlet Rules	318
To Deny Access to Netlet Rules	319
To Allow Access to Hosts	320
To Deny Access to Hosts	321
To Select Netlet Launch Mode	321
To Configure Proxylet Attributes	325
To Configure Crypto Accelerator 1000	328
To Configure Crypto Accelerator 4000	332
To Enable an External SSL Device Accelerator	334
To Configure External SSL Device Accelerators	335

Preface

This guide explains how to administer the Sun Java™ System Portal Server Secure Remote Access.

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

SRA runs on the Solaris™ 8.0 Operating System and higher and the Linux platform. This guide contains instructions for configuring and administering SRA.

This Preface includes the following sections:

- Who Should Read This Book
- How This Book is Organized
- Conventions Used in This Book
- Default Paths and File Names
- Accessing Sun Resources Online
- Contacting Sun Technical Support
- Related Third-Party Web Site References
- Sun Welcomes Your Comments

Who Should Read This Book

This Administration Guide is intended for user that configure and administer SRA.

This Administration Guide assumes that you are a network or system administrator experienced in managing UNIX® systems and TCP/IP networks. You do not need root access to the required machines for installing the various components of SRA. You do need the required administrative privileges to carry out other operations such as configuring users and services.

Portal Server Secure Remote Access administrators should understand the following technology:

- Basic Solaris™ Operating System administrative procedures
- Lightweight Directory Access Protocol (LDAP)
- Sun Java System Directory Server
- Sun Java System Web Server
- Sun Java System Portal Server

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

- Understanding of Hypertext Markup Language (HTML) and HTML tags
- A fair knowledge of JavaScript
- Basic knowledge of Extensible Markup Language (XML)

How This Book is Organized

The following table summarizes the content of this book.

Table 1 How This Book is Organized

Chapter	Description
Chapter 1, “Introduction to Portal Server Secure Remote Access” on page 29	This chapter describes the SRA software and the relationship between the Portal Server and SRA software components. It also provides information on administering and configuring SRA software.
Chapter 2, “The Gateway” on page 39	This chapter describes Gateway related concepts and information required for the smooth running of the Gateway.
Chapter 3, “Proxylet and Rewriter” on page 91	This chapter describes Proxylet and Rewriter. For Rewriter, it provides sample rules and best practices.

Table 1 How This Book is Organized

Chapter	Description
Chapter 4, “NetFile” on page 181	Describes NetFile and explains its operation.
Chapter 5, “Netlet” on page 187	Describes how to use Netlet to run applications securely between users’ remote standard Portal Desktops and the servers running applications on your intranet.
Chapter 6, “Netlet With PDC” on page 213	Describes how to configure the client browser’s Java Plugin so that Netlet can be used with PDC.
Chapter 7, “Certificates” on page 215	Describes certificate management and explains how to install self-signed certificates or certificates from a Certificate Authority.
Chapter 8, “Configuring URL Access Control” on page 239	Describes how to allow or deny access to the end-user through the Gateway for specific URLs.
Chapter 9, “Configuring the Gateway” on page 243	Describes how to configure the Gateway attributes from the Access Manager administration console.
Chapter 10, “Configuring NetFile” on page 291	Describes how to configure NetFile from the Access Manager administration console.
Chapter 11, “Configuring Netlet” on page 309	Describes how to configure Netlet attributes from the Access Manager administration console.
Chapter 12, “Configuring Proxylet” on page 325	Describes how to configure Proxylet from the Access Manager administration console.
Chapter 13, “Configuring SSL Accelerators” on page 327	Describes how to configure various accelerators for Portal Server Secure Remote Access.
Appendix A, “Log Files”	This appendix lists all the Portal Server Secure Remote Accesslog files and their descriptions.
Appendix B, “Configuration Attributes”	Lists the attributes you set for Portal Server Secure Remote Access on the Access Manager administration console.

Table 1 How This Book is Organized

Chapter	Description
Appendix C, “Country Codes”	Lists the two-letter country codes that you need to specify during certificate administration.
Glossary	Contains the link to the global glossary for the Sun Java System.

Conventions Used in This Book

The tables in this section describe the conventions used in this book.

Typographic Conventions

The following table describes the typographic changes used in this book.

Table 2 Typographic Conventions

Typeface	Meaning	Examples
AaBbCc123 (Monospace)	API and language elements, HTML tags, web site URLs, command names, file names, directory path names, onscreen computer output, sample code.	<p>Edit your <code>.login</code> file.</p> <p>Use <code>ls -a</code> to list all files.</p> <p>% You have mail.</p>
AaBbCc123 (Monospace bold)	What you type, when contrasted with onscreen computer output.	<p>% su</p> <p>Password:</p>
<i>AaBbCc123</i> (Italic)	<p>Book titles, new terms, words to be emphasized.</p> <p>A placeholder in a command or path name to be replaced with a real name or value.</p>	<p>Read Chapter 6 in the <i>User’s Guide</i>.</p> <p>These are called <i>class</i> options.</p> <p>Do <i>not</i> save the file.</p> <p>The file is located in the <i>install-dir/bin</i> directory.</p>

Default Paths and File Names

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

Table 3 Default Paths and File Names

Path Name	Description
<code>/etc/opt/SUNWps/platform.conf.default</code>	location for all the <code>platform.conf.*</code> files
<code>gateway-install-root/SUNWps/bin/gateway</code>	location of gateway-instance names
<code>/etc/opt/SUNWam/config/</code>	location of <code>AMConfig-instance-name.properties</code>
<code>portal-server-install-root/SUNWps/locale</code>	location of <code>srapGateway.properties</code>
<code>/var/opt/SUNWps/debug</code>	location of gateway debug log files
<code>/var/opt/SUNWam/debug</code>	default debug directory for service logs when debug is turned on from the Access Manager administration console.
<code>/var/opt/SUNWam/logs/srapNetFile</code>	location of log files
<code>/etc/opt/SUNWps/cert/default/</code>	location of certificate related files
<code>/opt/S1PS62/SUNWps/samples/config/netfile</code>	MIME-types configuration file location

Using Linux

Sun Java™ System Portal Server supports RedHat 2.1 and 3.0 Linux platform, however, please note the differences between the Solaris and Linux platforms:

Limitations Using Linux

IBM and BEA web containers are not supported.

The `mkchroot` command is not available on Linux.

Configuration files, deployment, and Application Programming Interfaces are the same for Solaris and Linux.

Comparison of Solaris and Linux Path Names

Table 4 Comparison of Solaris and Linux Path Names

Solaris Path Name	Linux Path Name
/opt/SUNWps (default)	/opt/sun/portal (default)
/etc/opt/SUNWps (config)	/etc/opt/sun/portal (config)
/var/opt/SUNWps (data)	/var/opt/sun/portal (data)

Related Information

The <http://docs.sun.com>SM web site enables you to access Sun technical documentation online. You can browse the archive or search for a specific book title or subject.

Books in This Documentation Set

Portal Server Secure Remote Access comes with supplementary information for administrators as well as documentation for developers. Use the following URL to see all the Portal Server Secure Remote Access documentation:

<http://docs.sun.com/db/coll/1293.1>.

The following table summarizes the books included in the Portal Server Secure Remote Access core documentation set.

Book Title	Description
<i>Portal Server Deployment Planning Guide</i>	Describes how to plan for and deploy Portal Server software.
<i>Portal Server Administration Guide</i>	Describes how to administer Portal Server using the Access Manager administration console and the command line.
<i>Portal Server Secure Remote Access Administration Guide</i>	Describes how to administer Portal Server Secure Remote Access.

Book Title	Description
<i>Portal Server Release Notes</i>	Available after the product is released. Contains last-minute information, including a description of what is new in this current release, known problems and limitations, installation notes, and how to report issues with the software or the documentation.
<i>Portal Server Technical Reference Guide</i>	Provides detailed information on the Portal Server technical concepts (such as Display Profile, Rewriter), command line utilities, tag libraries (in the software), and files (such as templates and JSPs). This guide serves as a single source for such essential background information.

Other Portal Server Documentation

Other Portal Server books include:

- *Portal Server Administratio Guide*
- *Portal Server Desktop Customization Guide*
- *Portal Server Developer's Guide*
- *Portal Server Mobile Access Developer's Guide*
- *Portal Server Mobile Access Developer's Reference*
- *Portal Server Mobile Access Deployment Planning Guide*
- *Portal Server Mobile Access Tag Library Reference*

Other Server Documentation

For other server documentation, go to the following:

- Directory Server documentation
- Web Server documentation
- Application Server documentation
- Web Proxy Server documentation

Accessing Sun Resources Online

For product downloads, professional services, patches and support, and additional developer information, go to the following:

- **Download Center**
<http://www.sun.com/software/download/>
- **Professional Services**
<http://www.sun.com/service/sunps/sunone/index.html>
- **Sun Enterprise Services, Solaris Operating System Patches, and Support**
<http://sunsolve.sun.com/>
- **Developer Information**
<http://developers.sun.com/prodtech/index.html>

Contacting Sun Technical Support

If you have technical questions about this product that are not answered in the product documentation, go to <http://www.sun.com/service/contacting>.

Related Third-Party Web Site References

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

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions.

To share your comments, go to <http://docs.sun.com> and click Send Comments. In the online form, provide the document title and part number. The part number is a seven-digit or nine-digit number that can be found on the title page of the book or at the top of the document. For example, the title of this book is *Portal Server Secure Remote Access 2005Q4 Administration Guide*, and the part number is 819-4158-10.

Sun Welcomes Your Comments

Introduction to Portal Server Secure Remote Access

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

This chapter covers the following topics:

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

Overview of SRA Software

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

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

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

The Portal Server can function in two modes:

- Open Mode
- Secure Mode

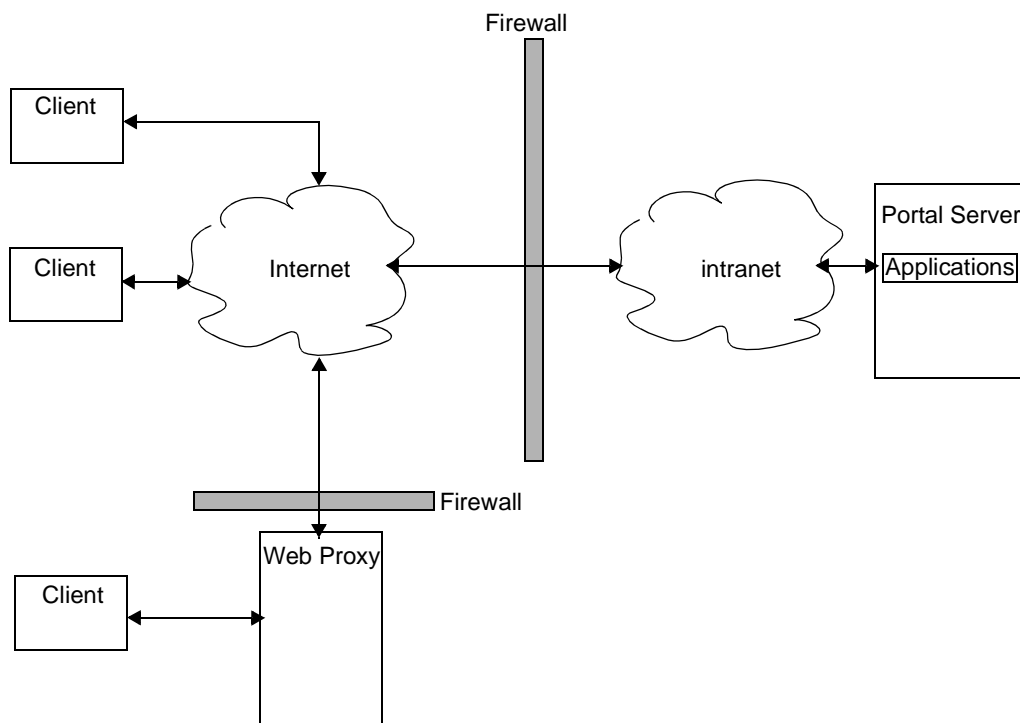
Open Mode

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

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

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

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

Figure 1-1 The Portal Server in Open Mode

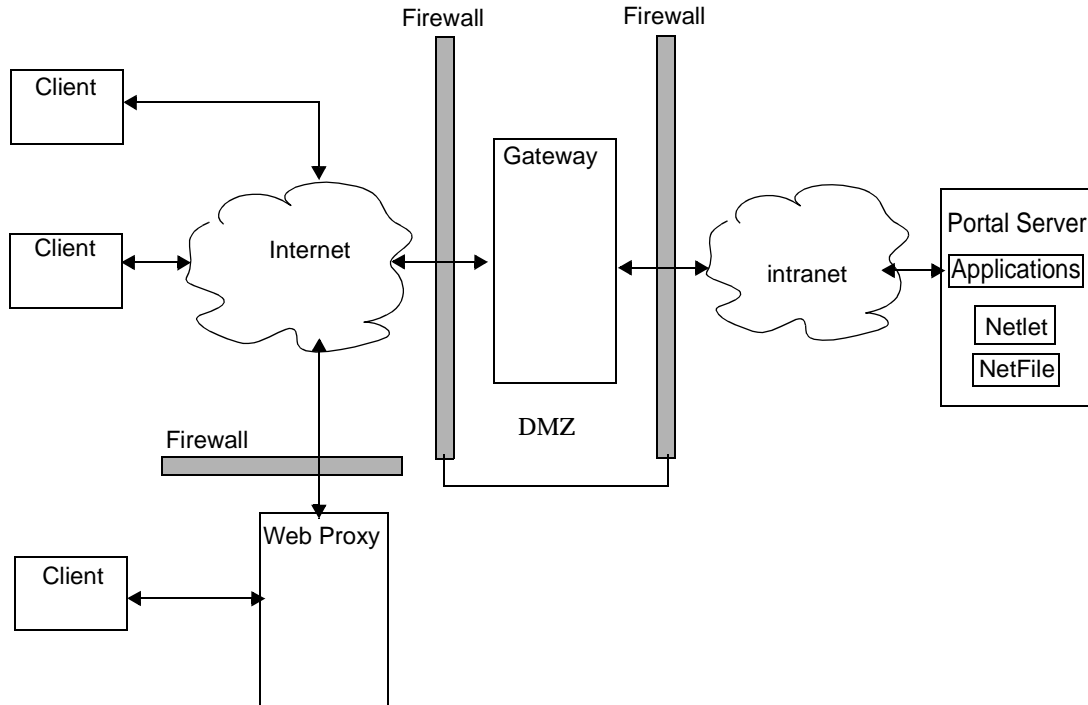
Secure Mode

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

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 Portal Server services such as Session, Authentication, and the standard Portal Desktop reside behind the DMZ in the secured intranet. Communication from the client browser to the Gateway is encrypted using HTTP over Secure Sockets Layer (SSL). Communication from the Gateway to the server and intranet resources can be either HTTP or HTTPS.

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

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



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

SRA Services

SRA software has five major components:

- Gateway
- Rewriter
- NetFile
- Netlet
- Proxylet

Gateway

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

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

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

Rewriter

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

NetFile

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

Netlet

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

Proxylet

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

Administering the SRA Product

SRA software has two interfaces for administration:

- The Access Manager administration console
- The command-line

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

Configuring SRA Attributes

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

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

- Conflict Resolution Level cannot be set at the user level and is not available from the Service Configuration tab. See “Setting Conflict Resolution” on page 36.
- MIME types Configuration File Location attribute can be set only at the organization level. See “Specify the MIME-types Configuration File Location” on page 307.

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

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

You configure SRA attributes on the Access Manager administration console under SRA Configuration using the following services:

- Access List

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

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

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

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

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

CAUTION The Gateway does not receive notifications for attribute changes that are made while Gateway is running. Restart Gateway to ensure that updated profile attributes (belonging to the Gateway or any other service) are used by Gateway. See “Using Authentication Chaining” on page 80.

Setting Conflict Resolution

► **To Set the Conflict Resolution Level**

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

Supported Applications

SRA software supports the following applications:

- MS Exchange 2000 SP3 and MS Exchange 2003 of Outlook Web Access (OWA).
- OWA ruleset named `exchange_2003_owa_ruleset`.
- iNotes - Notes 5.0.11
- Sun Java System Calendar Server Release 5.1.1 and later
- Sun Java System Messenger Express 6 2005Q4 - Sun Java System Messaging Server 5.2 and later

- Sun Java System Communications Express 6 2005Q1 and later

Supported Applications

The Gateway

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

This chapter covers the following topics:

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

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

Overview of the Gateway

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

Each Gateway requires that you do the following:

- Create a gateway profile. See “Creating a Gateway Profile” on page 40
- Create an instance of the Gateway. See “Creating Instances of a Gateway” on page 48
- Configure the Gateway. See Chapter 9, “Configuring the Gateway” on page 243.

Creating a Gateway Profile

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

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

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

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

See “Understanding the platform.conf File” on page 42 for more information on the contents of the `platform.conf` file.

You can:

- Create multiple profiles, define attributes for each profile, and assign these profiles to different Gateways as required.

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

CAUTION Do not assign the same profile to different instances of the Gateway running on the same machine. This causes a conflict because the port numbers would 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 causes a conflict.

► **To Create a Gateway Profile**

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

The Gateway page is displayed in the right pane.

4. Click New.

The Create New Gateway Profile page is displayed.

5. Enter the name of new gateway profile.
6. Select the profile to use for creating the new profile from the drop-down list.

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

The existing profile that is copied for the new one, copies the same port. Change the port for the new profile so that it does not conflict with the existing one.

7. Click Create.

The new profile is created and you are returned to the Gateway page, where the new profile is listed.

8. Run the `gwmultiinstance` script to create an instance of the Gateway. Refer to “Starting and Stopping the Gateway” on page 56.

9. Restart the Gateway with this gateway profile name if you want the changes to take effect:

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

See “Starting and Stopping the Gateway” on page 56. To configure the Gateway, see Chapter 9, “Configuring the Gateway”

Understanding the platform.conf File

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

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

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

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

Here is a sample:

```
#
# Copyright 11/28/00 Sun Microsystems, Inc. All Rights Reserved.
# "(#)platform.conf1.38 00/11/28 Sun Microsystems"
#
gateway.user=noaccess
gateway.jdk.dir=/usr/java_1.3.1_06
gateway.dsame.agent=http://pserv2.iportal.com:8080/sunportal/RemoteConfigServlet
portal.server.protocol=http
portal.server.host=pserv2.iportal.com
portal.server.port=8080
gateway.protocol=https
gateway.host=siroe.india.sun.com
gateway.port=333
gateway.trust_all_server_certs=true
```

```
gateway.trust_all_server_cert_domains=false
gateway.virtualhost=siroel.india.sun.com 10.13.147.81
gateway.virtualhost.defaultOrg=o=root,dc=test,dc=com
gateway.notification.url=/notification
gateway.retries=6
gateway.debug=error
gateway.debug.dir=/var/opt/SUNWps/debug
gateway.logdelimiter=&&
gateway.external.ip=10.12.147.71
gateway.certdir=/etc/opt/SUNWps/cert/portal
gateway.allow.client.caching=true
gateway.userProfile.cacheSize=1024
gateway.userProfile.cacheSleepTime=60000
gateway.userProfile.cacheCleanupTime=300000
gateway.bindipaddress=10.12.147.71
gateway.sockretries=3
gateway.enable.accelerator=false
gateway.enable.customurl=false
gateway.httpurl=http://siroe.india.sun.com
gateway.httpsurl=https://siroe.india.sun.com
gateway.favicon=https://siroe.india.sun.com
gateway.logging.password=ALKJDF123SFLKJJSDFU
portal.server.instance=
gateway.cdm.cacheSleepTime=60000
gateway.cdm.cacheCleanUpTime=300000
netletproxy.port=10555
rewriterproxy.port=10556
```

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

Table 2-1 The `platform.conf` File Properties

Entry	Default Value	Description
<code>gateway.user</code>	<code>noaccess</code>	The Gateway runs as this user. The Gateway must be started as root and after initialization, it loses its root privileges to become this user.
<code>gateway.jdk.dir</code>		This is the location of the JDK directory that the Gateway uses.
<code>gateway.dsame.agent</code>		This is the URL of the Access Manager that the Gateway contacts while starting up to get its profile.
<code>portal.server.protocol</code> <code>portal.server.host</code> <code>portal.server.port</code>		This is the protocol, host and port that the default Portal Server installation is using.
<code>gateway.protocol</code> <code>gateway.host</code> <code>gateway.port</code>		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.
<code>gateway.trust_all_server_certs</code>	<code>true</code>	This indicates whether the Gateway has to trust all server certificates, or only those that are in the Gateway certificate database.
<code>gateway.trust_all_server_cert_domains</code>	<code>false</code>	When an SSL communication is 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.
<code>gateway.virtualhost</code>		If the Gateway machines has multiple hostnames configured, you can specify a different name and identity provider address in this field.

Table 2-1 The platform.conf File Properties

Entry	Default Value	Description
gateway.virtualhost.de faultOrg=org		<p>This specifies the default Org to which the user logs into.</p> <p>For example suppose the virtual host field entries are the following:</p> <pre>gateway.virtualhost=test.com employee.test.com Managers.test.com</pre> <p>with the default org entries as:</p> <pre>test.com.defaultOrg = o=root,dc=test,dc=com employee.test.com.defaultOrg = o=employee,dc=test,dc=com Manager.test.com.defaultOrg = o=Manager,dc=test,dc=com</pre> <p>The user can use https://manager.test.com to log into the manager's org instead of https://test.com/o=Manager,dc=test,dc=com</p> <p>Note: virtualhost and defaultOrg are case sensitive in the platform.conf file, but not when using it in the URL.</p>
gateway.notification.url		<p>A combination of the Gateway host, protocol and port is used to construct the notification URL. This is used to receive session notification from the Access Manager.</p> <p>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 gets a blank page instead of the login page.</p>
gateway.retries		<p>This is the number of times that the Gateway tries to contact the Portal Server while starting up.</p>

Table 2-1 The platform.conf File Properties

Entry	Default Value	Description
gateway.debug	error	<p>This sets the debug level of the Gateway. The debug log file is located at <i>debug-directory/files</i>. The debug file location is specified in the <i>gateway.debug.dir</i> entry.</p> <p>The debug levels are:</p> <p>error - Only serious errors are logged in the debug file. The Gateway usually stops functioning when such errors occur.</p> <p>warning - Warning messages are logged.</p> <p>message - All debug messages are logged.</p> <p>on - All debug messages are displayed on the console.</p> <p>The debug files are:</p> <p><i>srpGateway.gateway-profile-name</i> - Contains the Gateway debug messages.</p> <p><i>Gateway_to_from_server.gateway-profile-name</i> - In message mode, this file contains all the requests and response headers between the Gateway and internal servers.</p> <p>To generate this file, change the write permission on <i>/var/opt/SUNWps/debug</i> directory.</p> <p><i>Gateway_to_from_browser.gateway-profile-name</i> - In message mode, this file contains all the requests and response headers between the Gateway and the client browser.</p> <p>To generate this file, change the write permission on <i>/var/opt/SUNWps/debug</i> directory.</p>
gateway.debug.dir		<p>This is the directory where all the debug files are generated.</p> <p>This directory should have sufficient permissions for the user mentioned in <i>gateway.user</i> to write to files.</p>
gateway.logdelimiter		Not used currently.
gateway.external.ip		In case of a multi-homed Gateway machine (one with multiple IP addresses), you need to specify the external IP address here. This IP is used for Netlet to run FTP.
gateway.certdir		This specifies the location of the certificate database.

Table 2-1 The platform.conf File Properties

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, nothing is cached and security is higher but performance drops with the higher network load.
gateway.userProfile.cacheSize		This is the number of user profile entries that get cached at the Gateway. If the number of entries exceeds this value, frequent retries occur to cleanup the cache.
gateway.userProfile.cacheSleepTime		Sets the sleep time, in seconds, for the cache cleanup.
gateway.userProfile.cacheCleanupTime		The maximum time in seconds after which a profile entry can get removed.
gateway.bindipaddress		On a multihomed machine, this is the IP address to which the Gateway binds its serversocket. To configure the Gateway to listen to all interfaces, replace the ip address so that the gateway.bindipaddress=0.0.0.0
gateway.sockretries	3	Not used currently.
gateway.enable.accelerator	false	If set to true external accelerator support is allowed. If set to true, the Gateway does not use Rewriter.
gateway.enable.customurl	false	If set to true the administrator is allowed to specify a custom URL for the Gateway to rewrite pages to.
gateway.httpurl		The HTTP reverse proxy URL for a custom URL for the Gateway to rewrite pages to. When Proxylet is enabled use this entry.
gateway.httpsurl		The HTTPS reverse proxy URL for a custom URL for the Gateway to rewrite pages to. Do not use this entry if Proxylet is enabled.
gateway.favicon		The URL to which the Gateway redirects requests for the favicon.icon file. This is used for the "favorite icon" in Internet Explore and Netscape 7.0 and higher. If left empty, the Gateway sends a 404 not found message back to browser.

Table 2-1 The platform.conf File Properties

Entry	Default Value	Description
gateway.logging.password		The LDAP password of the user "amService-srapGateway" that gateway uses for creating its application session. This can be either encrypted or in plain text.
http.proxyHost		This proxy host is used to contact the Portal Server.
http.proxyPort		This is the port for the host used to contact Portal Server.
http.proxySet		This property is set to true if a proxy host is required. If the property is set to false, http.proxyHost and http.proxyPort are ignored.
portal.server.instance		The value of this property is the corresponding /etc/opt/SUNWam/config/AMConfig- <i>instance-name</i> .properties file. If the value is default, then it points to AMConfig.properties.
gateway.cdm.cacheSleepTime	60000	The time out value for cache Client Detection Module responses sent to the Gateway from the Access Manager.
gateway.cdm.cacheCleanupTime	300000	The time out value for cache Client Detection Module responses sent to the Gateway from the Access Manager.
netletproxy.port	10555	The Netlet Proxy daemon listens for requests on this port.
rewriterproxy.port	10555	The Rewriter Proxy daemon listens for requests on this port.
gateway.ignoreServerList	false	If set to true, the Access Manager server URL is constructed using the values specified in the AMConfig.properties file. Set this property to true when the Access Manager server is behind a load balancer.

Creating Instances of a Gateway

Use the `gwmultiinstance` script to create or remove an instance of the Gateway. Run this script after the gateway profile has been created.

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

gateway-install-root/SUNWps/bin/

2. Run the multi-instance script:

```
./gwmultiinstance
```

Choose one of the following installation options:

- 1) Create a new gateway instance
- 2) Remove a gateway instance
- 3) Remove all gateway instances
- 4) Exit

If you chose 1, answer the following questions:

What is the name of the new gateway instance?

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

What port will the new gateway instance listen on?

What is the fully qualified hostname of the portal server?

What port should be used to access the portal server?

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

What is the portal server deploy URI?

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

What is the Access Manager URI? [/amserver]

What is the Access Manager password encryption key?

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

What is the name of your organization?

What is the name of your division?

What is the name of your city or locality?

What is the name of your state or province?

What is the two-letter country code?

What is the password for the Certificate Database? Again?

What is the password for the logging user? Again?

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

Start the gateway after installation? [y]/n

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

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

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

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

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

Creating Multi-homed Gateway Instances

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

```
gatewaybindipaddress = 0.0.0.0
```

Creating Gateway Instances Using the Same LDAP

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

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

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

```
am.encrypted.pwd= string_key_specified_in gateway-install
```

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

```
com.ipplanet.am.service.secret= string_key_specified_in  
gateway-install
```

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

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

```
<DirPassword>string_key_specified_in_gateway-install</DirPassword>
```

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

```
<DirPassword>string_key_specified_in_gateway-install </DirPassword>
```

4. Restart `ams` server services.

Running the Gateway in the chroot Environment

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

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

► To Install chroot

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

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

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

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

2. Run the `mkchroot` script from:

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

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

In the event of an error during the execution of the `mkchroot` script, see “Execution Failure of the `mkchroot` Script” on page 55.

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/javal.2...done
Creating loopback mount for/safedir/chroot/proc...done
Creating loopback mount for/safedir/chroot/dev/random...done
Do you need /dev/fd (if you do not know what it means, press return)[n]:
Updating /etc/vfstab...done
Creating a /safedir/chroot/etc/mnttab file, based on these loopback mounts.
Copying SRAP related data ...
Using /safedir/chroot as root.
Creating filesystem structure.....done
mkchroot successfully done.
```

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

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

For Solaris 9, do the following:

```
mkdir -p /safedir/chroot/usr/lib/32
mount -F lofs /usr/lib/32 /safedir/chroot/usr/lib/32
mkdir -p /safedir/chroot/usr/lib/64
mount -F lofs /usr/lib/64 /safedir/chroot/usr/lib/64
```

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

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

For Solaris 9:

```
/usr/lib/32 - /safedir/chroot/usr/lib/32 lofs - no -
/usr/lib/64 - /safedir/chroot/usr/lib/64 lofs - no -
```

For Linux:

```
# mount red.iplanet.com:/misc/export /misc/local
```

where

`red.iplanet.com` is the hostname of the NFS fileserver

`/misc/export` is the file system that `red.iplanet.com` is exporting

`/misc/local` is the location to mount the file system on the local machine.

Note: The mount point directory on local machine (`/misc/local` in the above example) must exist.

After the mount command runs (and if the client has proper permissions from the `red.iplanet.com` NFS server) the client user can execute the command `ls /misc/local` to display a listing of the files in `/misc/export` on `red.iplanet.com`

4. Type the command below to restart the Gateway:


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

Execution Failure of the mkchroot Script

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

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

If the following error message is encountered:

```
Not a Clean Exit
```

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

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

```
umount /safedir/chroot/proc
```

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

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

Restarting Gateway in the chroot Environment

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

► To Restart Gateway in the chroot Environment

1. Stop Gateway running from the `'/'` directory.

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

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

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

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

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

Starting and Stopping the Gateway

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

► To Start the Gateway

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

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

`default` is the default gateway profile that is created during installation. You can create your own profiles later, and restart the Gateway with the new profile. See “Creating a Gateway Profile” on page 40.

If you have multiple Gateway instances, use:

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

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

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

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

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

```
netstat -an | grep port-number
```

The default Gateway port is 443.

► **To Stop the Gateway**

1. Use the following command to stop the Gateway:

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

If you have multiple Gateway instances, use:

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

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

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

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

Restarting the Gateway

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

- 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.
- The Gateway crashes due errors such as OutOfMemory errors.
- The Gateway hangs and does not respond to requests.

► **To Restart the Gateway with a Different Profile**

Restart the Gateway:

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

► **To Restart the Gateway**

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

- Start the watchdog process:

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

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

➤ **To Configure the Gateway Watchdog**

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

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

See the crontab man page to configure the crontab entries.

Specifying a Virtual Host

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

➤ **To Specify a Virtual Host**

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

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

2. Add the following entries:

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

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

3. Restart the Gateway:

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

If these values are not specified, the Gateway defaults to normal behavior.

Specifying a Proxy to Contact Access Manager

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

➤ **To Specify a Proxy**

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

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

2. Add the following entries:

```
http.proxyHost=proxy-host
```

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

```
http.proxySet=true
```

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

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

Using Web Proxies

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

Web Proxy Configuration

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

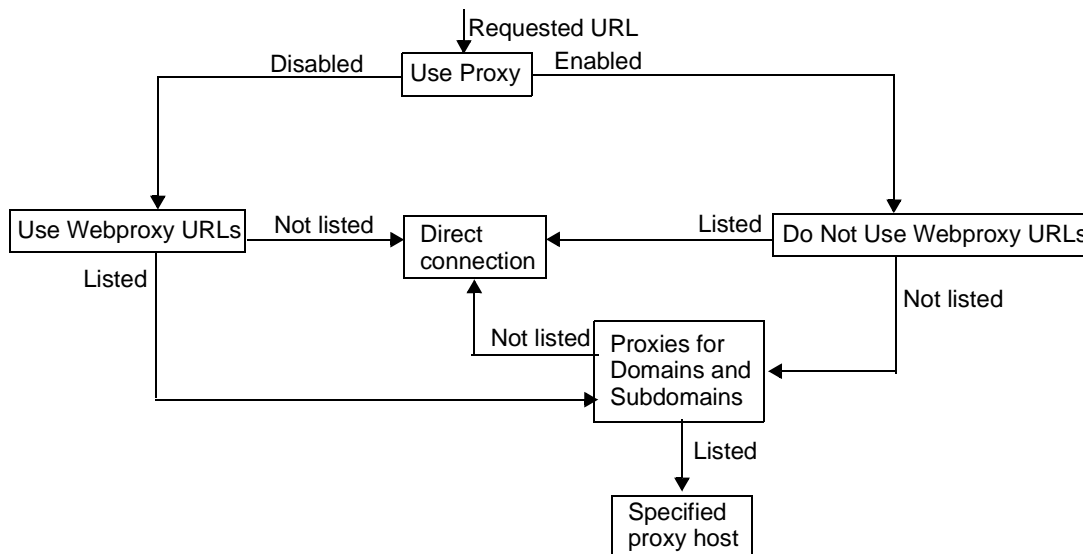
- Creates a list of domains and subdomains along with the required proxies in the Proxies for Domains and Subdomains field in the Gateway service.
For information on configuring proxies for domains and subdomains, see “Create List of Proxies for Domains and Subdomains” on page 265.
- With the Use Proxy option enabled:
 - The proxies specified in the Proxies for Domains and Subdomains field are used for the specified hosts.
 - To enable direct connections for certain URLs within the domains and subdomains specified in the Proxies for Domains and Subdomains list, specify these URLs in the Do Not Use Web Proxy URLs field.
- With the Use Proxy option disabled:
 - To ensure that proxies are used for certain URLs within the domains and subdomains specified in the Proxies for Domains and Subdomains field, specify these URLs in the Use Webproxy URLs list.

Although the Use Proxy option is disabled, a proxy is used to connect to the URLs listed under Use Webproxy URLs. The proxies for these URLs are obtained from the Proxies for Domains and Subdomains list.

To configure the Use Proxy option, see “Enable Usage of Web Proxies” on page 263.

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

Figure 2-1 Web Proxy Management



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

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

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

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

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

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

Syntax

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

Example

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

* is a wild card that matches everything

where,

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

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

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

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

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

Processing the Web Proxy Information

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

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

- Else, the list is searched for *.com. If an entry is found, the corresponding proxy is used.
- Else the list is searched for com. If an entry is found, the corresponding proxy is used.
- Else the list is searched for *. If an entry is found, the corresponding proxy is used.
- Else, a direct connection is attempted.

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

```
com p1 | host1 p2 | host2 | * p3
sesta.com p4 | host5 p5 | * p6
florizon.com | host6
abc.sesta.com p8 | host7 p7 | host8 p8 | * p9
host6.florizon.com p10
host9.sesta.com p11
siroe.com | host12 p12 | host13 p13 | host14 | * p14
siroe.com | host15 p15 | host16 | * p16
* p17
```

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

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

Number	Entry in Proxies for Domains and Subdomains List	Proxy	Description
1	com	p1	As specified in the list.
2	host1.com	p2	As specified in the list.
3	host2.com	p1	The proxy for the domain is used as no proxy is specified against host2.
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.

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

Number	Entry in Proxies for Domains and Subdomains List	Proxy	Description
10	abc.sesta.com	p8	As specified in the list.
11	host7.abc.sesta.com	p7	As specified in the list.
12	host8.abc.sesta.com	p8	As specified in the list.
13	*.abc.sesta.com	p9	As specified in the list. For all hosts other than <code>host7</code> and <code>host8</code> under the <code>abc.sesta.com</code> domain, <code>p9</code> 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 <code>p10</code> should be used. In a case with 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	A direct connection is attempted because no proxy is specified for <code>siroe.com</code> .
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	A direct connection is attempted because no proxy is specified for <code>host14</code> .
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	A direct connection is attempted because no proxy is specified for <code>host16</code> or <code>siroe.com</code> .
23	*.siroe.com	p16	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, <code>p17</code> is used as the proxy.

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

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

you can specify it as:

```
sesta.com p1
```

```
red.sesta.com p2
```

```
*.sesta.com p3
```

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

Rewriting Based on the Proxies for Domains and Subdomains List

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

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

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

Default Domain and Subdomain

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

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

```
red.sesta.com
```

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

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

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

Using Automatic Proxy Configuration

To ignore the information in the Proxies for Domains and Subdomains list, enable the Automatic Proxy Configuration feature. To configure this, see “Enable Automatic Proxy Configuration Support” on page 266.

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

- Portal Server, Gateway, Netlet, and Proxylet use Rhino software to parse the PAC file. You can install the `SUNWrhino` package from the Java™ Enterprise System Accessory CD.

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

- The `js.jar` must be present in the `$JRE_HOME/lib/ext` directory on the Gateway machine, otherwise the Gateway cannot parse the PAC file.
- Gateway fetches the PAC file at bootup from the location specified in the gateway profile Automatic Proxy Configuration File location field. To configure the location, see “Specify Automatic Proxy Configuration File Location” on page 267.
- Gateway uses the `URLConnection` API to reach this location. If the proxy needs to be configured to reach the Gateway, the proxy needs to be configured in the following way:

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

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

- b. Add the following entries:

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

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

```
http.proxySet=true
```

- c. Restart the Gateway to use the specified proxy:

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

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

If you want the Gateway to use a direct connection to the host, return "DIRECT". See "Example with Either DIRECT or NULL Return" on page 66.

- Gateway only uses the first proxy returned when multiple proxies are specified. It does not try to failover or loadbalance among the various proxies specified for a host.
- Gateway ignores SOCKS proxies and attempts a direct connection and assumes that the host is part of the intranet.
- To specify a proxy to be used to reach any host not part of the intranet, use the proxy type "STARPROXY". This is an extension of the PAC file format and is similar to the entry * proxyHost:port in Proxies for Domains and Subdomains section of the gateway profile. See "Example with STARPROXY Return" on page 67

Sample PAC File Usage

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

Example with Either DIRECT or NULL Return

Using these proxies for domains and subdomains:

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

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

the corresponding PAC file is:

```
// Start of the PAC File
function FindProxyForURL(url, host) {
    if (dnsDomainIs(host, ".intranet1.com")) {
        return "DIRECT";
    }
}
```

```

        if (dnsDomainIs(host, ".intranet2.com")) {
            return "PROXY proxy.intranet1.com:8080";
        }
        return "NULL";
    }
//End of the PAC File

```

Example with STARPROXY Return

Using these proxies for domains and subdomains:

```

intranet1.com
intranet2.com.proxy.intranet1.com:8080
internetproxy.intranet1.com:80

```

the corresponding PAC file is:

```

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

```

In this case, if the request is for a host in .intranet2.com domain, the Gateway contacts proxy.intranet1.com:8080. If proxy.intranet1.com:8080 is down, the request fails. The Gateway does not failover and contacts proxy1.intranet1.com:8080.

Specifying PAC File Location

The format for specifying the location of the PAC file depends upon its location as follows:

- If the pacfile resides on a webserver, enter the PAC URL as:

```
http://hostname/pacfile-name.pac
```

- If the pacfile is a local file (for example, c:\pacfile\sample.pac), for java 1.4.1_x, enter the PAC URL as:

```
file://c:/pacfile/sample.pac
```

- If the pacfile is a local file (for example, c:\pacfile\sample.pac), for java 1.4.2_x, enter the PAC URL as:

```
file:///c:/pacfile/sample.pac
```

Adding Services in Separate Sessions

When you add Portal Server services in separate sessions, ensure that:

- All Portal Servers are listed under Gateway > Core in the administration console. For more information see “Create List of Portal Servers” on page 258
- All Portal Server URLs are listed in the Non-authenticated URLs under Gateway > Security. For more information see “Create List of Non-authenticated URLs” on page 269

Using a Netlet Proxy

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

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

The Netlet proxy is useful for the following reasons:

- To add an additional layer of security.
- To minimize the use of extra IP addresses and ports from the Gateway through an internal firewall in a significantly sized deployment environment.
- To restrict the number of open ports between the Gateway and the Portal Server to 1. This port number can be configured during installation.
- To extend the secure channel between the client and the Gateway, up to the Portal Server as shown in the "With a Netlet Proxy Configured" section of Figure 2-2. The Netlet proxy offers improved security benefits through data encryption but may increase the use of system resources. See the *Sun Java Enterprise System Installation Guide* for information on installing the Netlet proxy.

You can:

- Choose to install the Netlet proxy on the Portal Server node or on a separate node.
- Install multiple Netlet proxies and configure them for a single Gateway using the administration console. This is useful in load balancing. "Enable and Create a List of Netlet Proxies" on page 248 for details.
- Configure multiple instances of the Netlet proxy on a single machine.
- Point multiple instances of the Gateway to a single installation of the Netlet proxy.
- Tunnel Netlet through a web proxy. To configure this, see "Enable Netlet Tunneling Through Web Proxy" on page 268.

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

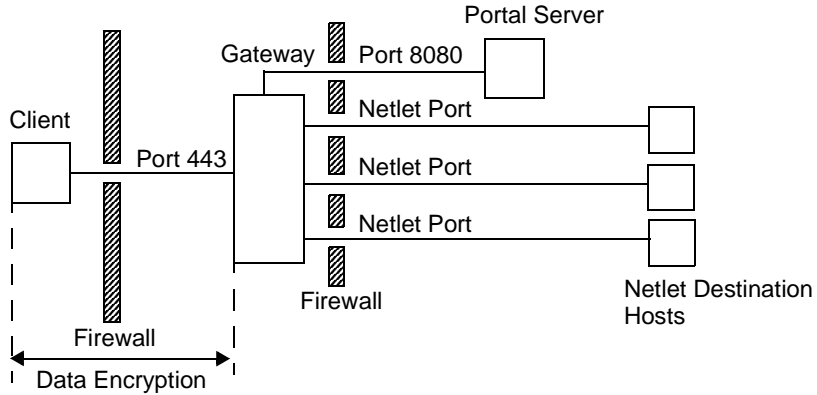
The first scenario shows the Gateway and Portal Server without a Netlet proxy installed. Here the data encryption extends only from the client to the Gateway. A port is opened in the second firewall for each Netlet connection request.

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

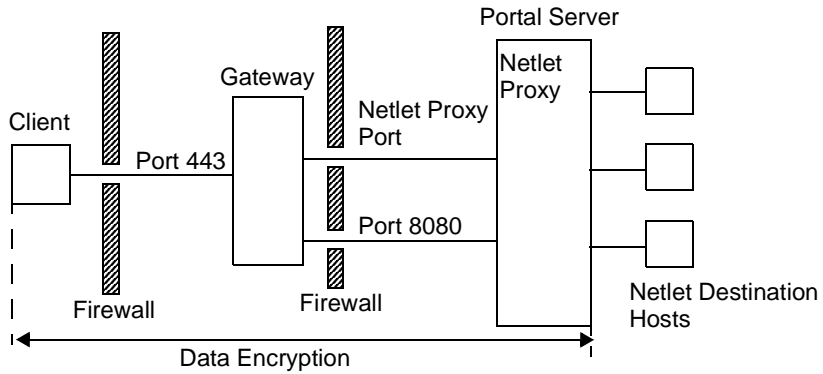
The third scenario shows the Gateway and the Portal Server with a Netlet proxy installed on a separate node. Installing a Netlet proxy on a separate node reduces the load on the Portal Server node. Here again, only two ports need to be opened in the second firewall. One port services requests to the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

Figure 2-2 Implementation of Netlet Proxy

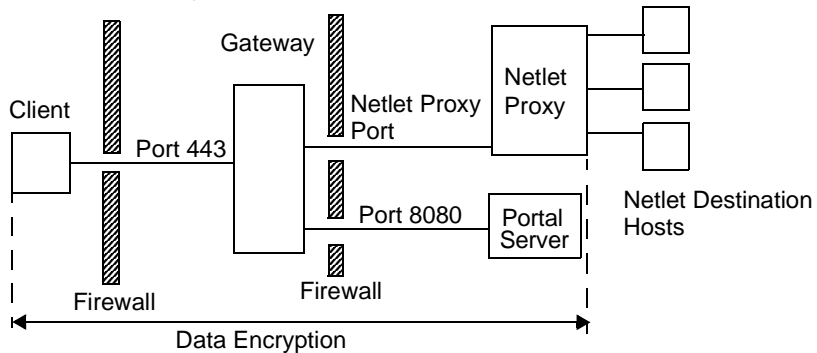
Without a Netlet Proxy Configured



With a Netlet Proxy on the Portal Server



With a Netlet Proxy on a Separate Node



Creating Instances of a Netlet Proxy

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

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

```
netlet-install-dir/SUNWps/bin
```

2. Run the multi-instance script:

```
./nlpmultiinstance
```

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

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

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

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

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

Enabling a Netlet Proxy

You enable a Netlet proxy through the Gateway service under SRA Configuration in the Access Manager administration console. See “Enable and Create a List of Netlet Proxies” on page 248.

Restarting a Netlet Proxy

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

You can also restart a Netlet proxy manually.

► To Restart a Netlet Proxy

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

- Start the watchdog process:

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

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

- Start a Netlet proxy manually:

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

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

► To Configure a Netlet Proxy Watchdog

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

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

Using a Rewriter Proxy

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

The two advantages to using a Rewriter proxy are as follows:

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

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

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

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

Creating Instances of a Rewriter Proxy

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

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

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

2. Run the multi instance script:

```
./rwpmultiinstance
```

3. Answer the questions asked by the script:

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

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

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

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

Enabling a Rewriter Proxy

Enable a Rewriter proxy through the Gateway service under SRA Configuration in the Access Manager administration console. See “Enable and Create a List of Rewriter Proxies” on page 246.

Restarting a Rewriter Proxy

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

You can also restart a Rewriter proxy manually.

► To Restart a Rewriter Proxy

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

- Start the watchdog process:

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

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

- Start manually:

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

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

► To Configure a Rewriter Proxy Watchdog

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

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

Using a Reverse Proxy with the Gateway

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

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

► To Enable a Reverse Proxy

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

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

2. Add the following entries:

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

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

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

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

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

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

3. Restart the Gateway:

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

If these values are not specified, the Gateway defaults to normal behavior.

Obtaining Client Information

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

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

Table 2-3 Information in HTTP Headers

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

Table 2-3 Information in HTTP Headers

Header.	Syntax	Description
PS-GW-Rewriting-URL	X-PS-GW-URL: http(s)://gatewayURL(: port)/[SessionInfo]	<p>Indicates the URL that the Gateway rewrites all the pages to.</p> <ol style="list-style-type: none"> 1. When the browser supports cookies, the value of this header is the same as the PS-GW-URL header. 2. When the browser does not support cookies: <ul style="list-style-type: none"> • and if the destination host is in the "User Session to which User Session Cookie is Forwarded" field, the value is the actual URL to which the Gateway rewrites the page to (which includes the encoded SessionID info). • or if the destination host is not in the "User Session to which User Session Cookie is Forwarded" field, then the SessionInfo string is "\$SessionID" <p>Note: As part of the response, if the user's Access Manager sessionId changes (like response from authentication page) then the pages are rewritten with that value (and not the value that was previously indicated in the header).</p> <p>For example:</p> <ul style="list-style-type: none"> • If the browser supports cookies: <pre>PS-GW-Rewriting-URL: https://siroe.india.sun.com :10443/</pre> • If the browser does not support cookies and the endserver is in "User Session to which User Session Cookie is Forwarded" field. <pre>PS-GW-Rewriting-URL: https://siroe.india.sun.com :10443/SessIDValCustomEn codedValue/</pre> • If the browser does not support cookies and endserver is not in "User Session to which User Session Cookie is Forwarded" field. <pre>PS-GW-Rewriting-URL: https://siroe.india.sun.com :10443/\$SessionID</pre>

Table 2-3 Information in HTTP Headers

Header.	Syntax	Description
PS-GW-CLientIP	X-PS-GW-CLientIP: <i>IP</i>	This is the IP that the Gateway obtained from <code>recievedSocket.getInetAddress().getHostAddress()</code> This gives the client's IP if directly connected to the Gateway.

Using Authentication Chaining

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

The procedure described here is only for enabling authentication chaining along with a Personal Digital Certificate (PDC) authentication at the Gateway. For information on authentication chaining without PDC authentication at the Gateway, refer to the *Access Manager Administration Guide*.

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

NOTE When enabled, PDC is always the first authentication module to be presented to the user.

► To Add Authentication Modules to an Existing PDC Instance

1. Log in to the Access Manager administration console as administrator.
2. Choose the required organization.
3. Select Services from the View drop-down menu.
The services are displayed in the left pane.
4. Click the arrow next to Authentication Configuration.
The Service Instance List is displayed.
5. Click gatewaypc.
The Gatewaypc properties page is displayed.

6. Click Edit in front of Authentication Configuration.
Add Module is displayed.
7. Select Module Name and set Flag to Required. Option can be blank.
8. Click OK.
9. Click Save after adding one or more modules.
10. Click Save in the gatewaypdc properties page.
11. For the changes to take effect, restart the Gateway:

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

Using Wild Card Certificates

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

This enables 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.

Disabling Browser Caching

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

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

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

► **To Disable Browser Caching**

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

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

2. Edit the following line:

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

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

3. Restart the Gateway:

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

Customizing the Gateway Service User Interface

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

srpGateway.properties File

You can edit this file for the following purposes:

- Customize the error messages that may appear when the Gateway is running.
 - `HTML-CharSets=ISO-8859-1` specifies the character set that was used to create this file.
 - The number in braces (for example, `{0}`) indicates that the value 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 to be displayed since the number and the message are associated.
- Customize the log information.

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

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

srapgwadminmsg.properties File

You can edit this file for the following reasons:

- Customize the labels that appear on buttons for the Gateway service on the administration console.
- Customize the status messages and error messages that appear when you are configuring the Gateway.

Sharing LDAP Directories

When two instances of Portal Server and Access Manager servers share the same LDAP directories, please use this workaround for all subsequent Portal Server, Access Manager, and Gateways:

1. Modify the following areas in `AMConfig.properties` to be in sync with the first installed instance of Portal Server and Access Manager servers:

#The key that will be used to encrypt and decrypt passwords.

```
am.encryption.pwd=t/vnY9Uqjfl2NbFywKuAaaHibwlDFNLO <== REPLACE
THIS STRING WITH THE ONE FROM FIRST PORTAL INSTALL
```

/* The following key is the shared secret for application auth module */

```
com.iplanet.am.service.secret=AQICxIPLNc0WWQRVLYZN0PnKgyvq3gTU8JA9
<== REPLACE THIS STRING WITH THE ONE FROM FIRST PORTAL
INSTALL
```

2. In `/etc/opt/SUNWam/config/ums` modify the following areas in `serverconfig.xml` to be insync with the first installed instance of Portal Server and Access Manager server:

```
<DirDN>
```

```
cn=puser,ou=DSAME Users,dc=sun,dc=net
```

```
</DirDN>
```

```
<DirPassword>
```

```
AQICxIPLNc0WWQT22gQnGgnCp9rUf+FuaqpY <== REPLACE THIS STRING
WITH THE ONE FROM FIRST PORTAL INSTALL
```

```
</DirPassword>
```

```
<DirDN>
```

```
cn=dsameuser,ou=DSAME Users,dc=sun,dc=net
</DirDN>
<DirPassword>
    AQICxIPLNc0WWQT22gQnGgnCp9rUf+FuaqpY <== REPLACE THIS STRING
    WITH THE ONE FROM FIRST PORTAL INSTALL
</DirPassword>
```

3. Restart amserver services.

Using Federation Management

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

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

Refer to the *Access Manager Federation Management Guide* for detailed information on Federation Management.

Federation Management Scenario

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

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

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

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

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

Configuring Federation Management Resources

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

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

Configuration 1

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

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

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab from the administration console.

3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Core tab.
6. Select the Enable Cookie Management checkbox to enable cookie management.
7. Click the Security tab.
8. Scroll to the Portal Servers field and enter Portal Server names so that you can use relative URLs like /amserver or /portal/dt listed in the Non-authenticated URLs list. For example:

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

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

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

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

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

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

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

9. Scroll to the Portal Servers field and enter the Portal Server name. For example /amserver.
10. Click Save.
11. Click the Security tab.
12. Scroll to the Non-authenticated URLs list and add the Federation resources.
For example:

`/amserver/config/federation`

`/amserver/IntersiteTransferService`

`/amserver/AssertionConsumerservice`

`/amserver/fed_images`

`/amserver/preLogin`

`/portal/dt`

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

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

Configuration 2

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

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

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab from the administration console.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Core tab.
6. Select the Enable Cookie Management checkbox to enable cookie management.

7. Scroll to the Portal Servers field and enter service provider portal server names so that you can use relative URLs like /amserver or /portal/dt listed in the Non-authenticated URLs list.

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

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

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

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

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

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

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

8. Click Save.
9. Click the Security tab.
10. Scroll to the Non-authenticated URLs list and add the Federation resources. For example:

`/amserver/config/federation`

`/amserver/IntersiteTransferService`

`/amserver/AssertionConsumerservice`

`/amserver/fed_images`

`/amserver/preLogin`

`/portal/dt`

11. Click Add.
12. Click Save.
13. If web proxies are needed to reach the URLs listed in the Non-authenticated URLs list, click the Proxies tab.
14. Scroll to the Proxies for Domains and Subdomains field and enter the necessary web proxies.
15. Click Add.
16. Click Save.

17. From a terminal window, restart the Gateway:

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

Configuration 3

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

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

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

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab from the administration console.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Core tab.
6. Select the Enable Cookie Management checkbox to enable cookie management.

7. Scroll to the Portal Servers field and enter identity provider portal server so that you can use relative URLs like /amserver or /portal/dt listed in the Non-authenticated URLs list.

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

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

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

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

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

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

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

8. Click Save.
9. Click the Security tab.
10. Scroll to the Non-authenticated URLs list and add the Federation resources. For example:

`/amserver/config/federation`

`/amserver/IntersiteTransferService`

`/amserver/AssertionConsumerservice`

`/amserver/fed_images`

`/amserver/preLogin`

`/portal/dt`

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

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

Proxylet and Rewriter

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

The following topics are covered for Proxylet:

- Overview of Proxylet

The following topics are covered for Rewriter:

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

Overview of Proxylet

Proxylet is a Java applet that sets itself as a proxy server on the client machine. Proxylet reads and modifies the proxy settings in the Proxy Auto Config (PAC) file on the client machine so that the proxy settings point to the local proxy server or Proxylet.

Proxylet inherits the transport mode from the Gateway. If the Gateway is configured to run on SSL, Proxylet establishes a secure channel between the client machine and the Gateway or destination server. For encryption, Proxylet uses the JSSE API if the client JVM is 1.4 or higher or if the required jar files reside on the client machine. Otherwise it uses the KSSL API. Decryption occurs on the client machine.

The domain and subdomain for URLs that are to be directed to the Gateway are specified in the gateway profile. If a URL is not part of a domain that the gateway handles, the request is directed to the Internet.

Proxylet supports client-side authentication if a Personal Digital Certificate (PDC) is enabled at the Gateway. To check if PDC is enabled, see “Obtaining Client Information” on page 77.

Proxylet is enabled from the Access Manager administration console where the client IP address or proxy hostname and port are specified. If Proxylet is enabled, it checks the client machine for the following:

- Correct browser permissions
- JVM version 2 (for all browsers)
- The browser is Netscape 7.0/7.1, Mozilla 1.4/1.5, Internet Explorer 5.5 or greater
- The machine or device can run a server application

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

When Proxylet is used, it retrieves the proxy settings from the Proxy Auto Configuration (PAC) file.

Advantages of Using Proxylet

Unlike Rewriter, Proxylet requires little or no postinstallation changes. Integration with third party software such as Microsoft Exchange Server is easy. Also the performance of the Gateway increases as Proxylet does not touch web content. Because Proxylet does not modify content or change the data, users can download any type of content, such as tar and gzip files.

Configuring Proxylet

For information on enabling and configuring, Proxylet, see Chapter 12, “Configuring Proxylet” on page 325.

NOTE If the user does not have the appropriate Java Virtual Machine (JVM) to run Proxylet, the browser connects to the sun.com site to download the Java Runtime Environment. If the user's browser settings do not contain the correct value or if the user is using Direct proxy settings without access to the Internet, then Proxylet cannot be downloaded.

HTTPS Support

Proxylet supports HTTPS with the following results:

- Decryption is done at the client server.
- You can access destination servers running in SSL mode.
- The client certificate is presents directly to the destination server.
- Basic authentication single-sign (SSO) is not supported at the Gateway. (The Gateway cannot insert SSO information in http headers.)
- URL-based access control is not supported, only host-based access control.
- External accelerators and external Reverse proxies in front of the Gateway are not currently supported.
- This support is not for Proxylet when Portal Server uses HTTPS.

Overview of Rewriter

The Rewriter component of SRA enables end users to browse the intranet by modifying Uniform Resource Identifier (URI) references on web pages so that they point to the Gateway. A URI defines a way to encapsulate a name in any registered name space, and labels it with the name space. The most common kinds of URIs are Uniform Resource Locators (URLs). Rewriter supports only HTTP or HTTPS and this support exists regardless of the capitalization of the protocol. Rewriter only supports backslashes when they are part of a relative URL.

For example,

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

These URLs would not be rewritten:

`http:\\abc.sesta.com`

`http:/abc.com`

Character Set Encoding

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

Sun Microsystems provides a third-party product to detect the character sets. To enable this product, install the `SUNWjchdt` package from the Java™ Enterprise System Accessory CD. If the product is installed, Rewriter will detect it and use it if necessary.

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

Rewriter Usage Scenarios

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

- URLScaper

- The Gateway

URLScrapper

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

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

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

Rewriter translates this to:

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

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

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

The Gateway

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

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

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

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

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

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

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

Writing Rulesets

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

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

This section covers the following topics:

- Public Interface (RuleSet DTD)
- Sample XML DTD
- Procedure to Write Rules
- Ruleset Guidelines
- Defining the RuleSet Root Element
- Using the Recursive Feature
- Rules for HTML Content
- Rules for JavaScript Content
- Rules for XML Content
- Rules for Cascading Style Sheets
- Rules for WML

Public Interface (RuleSet DTD)

Here is the RuleSet DTD:

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

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

1. In a Rule, All Mandatory attributes cannot be "*".
 2. Only one instance of the below elements is allowed, but in any order.
- 1)HTMLRules
 - 2)JSRules

3)XMLRules

3. ID should always be in lower case.

```
-->
<!ENTITY % eURL 'URL'>
<!ENTITY % eEXPRESSION 'EXPRESSION'>
<!ENTITY % eDHTML 'DHTML'>
<!ENTITY % eDJS 'DJS'>
<!ENTITY % eSYSTEM 'SYSTEM'>

<!ENTITY % ruleSetElements '(HTMLRules | JSRules | XMLRules)?'>
<!ENTITY % htmlElements '(Form | Applet | Attribute)*'>
<!ENTITY % jsElements '(Variable | Function)*'>
<!ENTITY % xmlElements '(Attribute | TagText)*'>

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

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

```

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

<!-- Rules for identifying rules in JS content -->
<!ELEMENT JSRules (%jsElements;)>
<!ELEMENT Variable EMPTY>
<!ATTLIST Variable
    name CDATA #REQUIRED
    type (%eURL; | %eEXPRESSION; | %eDHTML; | %eDJS; | %eSYSTEM;)
"EXPRESSION"
    source CDATA "*"
>

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

<!-- Rules for identifying rules in XML content -->
<!ELEMENT XMLRules (%xmlElements;)>
<!ELEMENT TagText EMPTY>
<!ATTLIST TagText

```

```

tag CDATA #REQUIRED
attributePatterns CDATA ""
source CDATA "*"
>

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

```

NOTE You can use * as a part of the rule value. But all the mandatory attribute values cannot be just *. Such rules are ignored, but the message is logged in the RuleSetInfo log file. For information on this log file, see “Debug File Names” on page 139.

Sample XML DTD

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

```

<?xml version="1.0" encoding="ISO-8859-1"?>
<!--
Rules for integrating a mail client with the gateway.
-->
<!DOCTYPE RuleSet SYSTEM "jar://rewriter.jar/resources/RuleSet.dtd">
<RuleSet type="GROUPED" id="owa">
<HTMLRules>
  <Attribute name="action" />

```

```

<Attribute name="background" />
<Attribute name="codebase" />
<Attribute name="href" />
<Attribute name="src" />
<Attribute name="lowsrc" />
<Attribute name="imagePath" />
<Attribute name="viewClass" />
<Attribute name="emptyURL" />
<Attribute name="draftsURL" />
<Attribute name="folderURL" />
<Attribute name="prevMonthImage" />
<Attribute name="nextMonthImage" />
<Attribute name="style" />
<Attribute name="content" tag="meta" />
</HTMLRules>
<JSRules>
<!-- Rules for Rewriting JavaScript variables in URLs -->
  <Variable name="URL"> _fr.location </Variable>
  <Variable name="URL"> g_szUserBase </Variable>
  <Variable name="URL"> g_szPublicFolderUrl </Variable>
  <Variable name="URL"> g_szExWebDir </Variable>
  <Variable name="URL"> g_szViewClassURL </Variable>
  <Variable name="URL"> g_szVirtualRoot </Variable>
  <Variable name="URL"> g_szBaseURL </Variable>
  <Variable name="URL"> g_szURL </Variable>
  <Function name="EXPRESSION" name="NavigateTo" paramPatterns="y"/>
</JSRules>
<XMLRules>
  <Attribute name="xmlns"/>
  <Attribute name="href" tag="a"/>

```

```

<TagText tag="baseroot" />
<TagText tag="prop2" />
<TagText tag="prop1" />
<TagText tag="img" />
<TagText tag="xsl:attribute"
attributePatterns="name=src" />
</XMLRules>
</RuleSet>

```

Procedure to Write Rules

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

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

Ruleset Guidelines

Keep the following in mind:

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

```

mail1.central.abc.com|iplanet_mail_ruleset
*.sfbay.abc.com|sfbay_ruleset
*.abc.com|generic_ruleset

```

`sfbay_ruleset` is used as it has the longest match.

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

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

- All rules need to be enclosed within the `<RuleSet>` `</RuleSet>` tags.
- Include all rules that need to rewrite HTML content in the `<HTMLRules>` `</HTMLRules>` section of the ruleset.
- Include all rules that need to rewrite JavaScript content in the `<JSRules>` `</JSRules>` section of the ruleset.
- Include all rules that need to rewrite XML content in the `<XMLRules>` `</XMLRules>` section of the ruleset.
- In your intranet pages, identify the URLs that need to be rewritten, and include the required rules in the appropriate sections (HTML, JSRules, or XMLRules) of the ruleset.
- Assign the ruleset to the required domain. See "Create List of URIs to RuleSet Mappings" on page 279 for details.
- Restart the Gateway to affect any changes:

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

Defining the RuleSet Root Element

The ruleset root element has two attributes:

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

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

Using the Recursive Feature

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

For example, when Rewriter parses the following string:

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

the rule

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

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

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

but if you use the recursive option as,

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

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

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

Defining Language Based Rules (Defining Rules)

Rules are based on the following languages:

- HTML
- JavaScript
- XML

Rules for HTML Content

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

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

- Applet Rules for HTML Content

Attribute Rules for HTML Content

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

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

This section is divided into the following parts:

- Attribute Rule Syntax
- Attribute Rule Example
- DJS Attribute Example

Attribute Rule Syntax

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

where,

attributeName is the name of the attribute (mandatory)

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

valuePatterns See "Using Pattern Matching in Rules" on page 108.

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

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

URL - a simple URL (default value).

DHTML - DHTML content. This kind of content is seen in standard HTML content and is used in Microsoft's HTC format files.

DJS - JavaScript content. All HTML event handlers such as onClick and onMouseover have JavaScript inlined with the HTML attribute.

Attribute Rule Example

Assume the base URL of the page is:

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

Page Content

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

Rules

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

or

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

Output

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

Description

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

DJS Attribute Example

Assume the base URL of the page is:

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

Page Content

```
<Form>
```

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

```
</Form>
```

Rules

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

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

Output

```
<Form>
```

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

```
</Form>
```

Description

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

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

Form Rules for HTML Content

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

This section is divided into the following parts:

- Form Rule Syntax
- Form Rule Example

Form Rule Syntax

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

where

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

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

`valuePatterns` See “Using Pattern Matching in Rules” on page 108

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

Form Rule Example

Assume the base URL of the page is:

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

Page Content

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

```
<form name=form1 method=POST
action="http://test.siroe.com/testcases/html/form.html">
<input type=hidden name=abc1 value="0|1234|/test.html">
</form>
```

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

Rules

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

Output

```
<FORM name="form1" method="POST"
action="gateway-URL/http://test.siroe.com/testcases/html/form.html">
<input type=hidden name=abc1
value="0|1234|gateway-URL/http://test.siroe.com/test.html">
</FORM>
```

Description

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

The `input` tag attribute value's `value` is rewritten as shown in the output. The specified `valuePatterns` is located, and all content following the matched `valuePatterns` is rewritten by prefixing the Gateway URL, and the base URL of the page. See "Using Pattern Matching in Rules" on page 108.

Applet Rules for HTML Content

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

This section is divided into the following parts:

- Applet Rule Syntax
- Applet Rule Example

Applet Rule Syntax

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

where

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

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

valuePatterns See “Using Pattern Matching in Rules” on page 108.

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

Applet Rule Example

Assume the base URL of the page is:

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

Page Content

```
<applet codebase="appletcode" code="RewriteURLinApplet.class"
archive="/test.jar">
<param name=Test1 value="/index.html">
</applet>
```

Rules

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

Output

```
<APPLET
codebase="gateway-URL/http://abc.siroe.com/casestudy/test/HTML/applet/applet
code" code="RewriteURLinApplet.class" archive="/test.jar">
<param name="Test1" value="gateway-URLhttp://abc.siroe.com/index.html">
</APPLET>
```

Description

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

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

Using Pattern Matching in Rules

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

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

Consider the sample form rule below.

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

where

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

`name` is the name of the form

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

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

Specifying Specialized Characters in valuePatterns

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

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

Using Wild Cards in valuePatterns

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

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

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

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

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

Table 3-1 Sample Usage of * Wildcard

URL	valuePatterns	Description
url1, url2, url3, url4	valuePatterns = "**, *, **, *"	In this case, url1 and url3 are rewritten because ** indicates the portion to be rewritten

Table 3-1 Sample Usage of * Wildcard

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

Rules for JavaScript Content

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

JavaScript elements with type URL are classified as follows:

- Variables
- Function Arguments

Variables

Generic Syntax

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

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

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

URL Variables

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

This section is divided into the following parts:

- URL Variable Syntax
- URL Variable Example

URL Variable Syntax

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

where

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

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

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

URL Variable Example

Assume the base URL is:

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

Page Content

```
<script LANGUAGE="Javascript">
<!--
//URL Variables
var imgsrc1="/tmp/tmp.jpg";
var imgsrc2="http://srap.sesta.com/tmp/tmp.jpg";
var imgsrc3=imgsrc2;
//-->
</SCRIPT>
```

Rules

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

Output

```
<script LANGUAGE="Javascript">
```

```

<!--
//URL Variables
var imgsrc="gateway-URL/http://abc.siroe.com/tmp/tmp.jpg";
var imgsrc="gateway-URL/http://sraps.sesta.com/tmp/tmp.jpg";
var imgsrc2=imgsrc1;
//-->
</SCRIPT>

```

Description

All variables of type URL and name beginning with `imgsrc` are rewritten. For the first line of the output, the Gateway URL and the base URL of the page on which the variable displays are prefixed. The second line already contains the absolute path, and hence only the Gateway URL is prefixed. Third `imgsrc2` would not be rewritten as its value is not a string but another JavaScript value.

EXPRESSION Variables

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

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

This section is divided into the following parts:

- EXPRESSION Variable Syntax
- EXPRESSION Variable Example

EXPRESSION Variable Syntax

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

where

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

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

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

EXPRESSION Variable Example

Assume the base URL of the page is:

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

Page Content

```

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

```

Rules

```

<Variable name="expvar" type="EXPRESSION"/>
or
<Variable name="expvar"/>

```

Output

```

var expvar=psSRAPrewriter_convert_expression(getURIPreFix() +
"../images/graphics"+".gif");
document.write("<a href="+expvar+">>Link to XYZ content</A><P>")
var expvar="gateway-URL/http://abc.siroe.com/images/graphics"+".gif";

```

Description

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

DHTML(Dynamic HTML) Variables

These are JavaScript variables that contain HTML content.

This section is divided into the following parts:

- DHTML Syntax

- **DHTML Example**

DHTML Syntax

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

where

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

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

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

DHTML Example

Assume the base URL of the page is:

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

Page Content

```
<script LANGUAGE="Javascript">
<!--
//DHTML Var
var dhtmlVar="<a href=../../images/test.html>"
var dhtmlVar="<a href=/images/test.html>"
var dhtmlVar="<a href=images/test.html>"
//-->
</SCRIPT>
```

Rules

```
<Variable name="dhtmlVar" type="DHTML"/>
<Attribute name="href"/>
or
<Attribute name="href" tag="a"/>
```

Output

```
<script LANGUAGE="Javascript">
<!--
//DHTML Var
```

```

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

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

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

//-->
</SCRIPT>

```

Description

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

DJS (Dynamic JavaScript) Variables

These are JavaScript variables that contain JavaScript content.

This section is divided into the following parts:

- DJS Syntax
- DJS Example

DJS Syntax

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

where

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

DJS Example

Assume the base URL of the page is:

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

Page Content

```

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

```

Rules

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

Output

```
//DJS Var - need 2 rules
var dJSVar="var dJSimgsrc='gateway-URL/http://abc.sesta.com/tmp/tmp.jpg';"
var dJSVar="var
dJSimgsrc='gateway-URL/http://abc.sesta.com/dir1/dir2/dir3/jscript/tmp/tmp.jp
g';"
var dJSVar="var dJSimgsrc='gateway-URL/http://abc.sesta.com/tmp/tmp.jpg';"
```

Description

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

SYSTEM Variables

These variables are not declared by the user and have limited support. They are available as a part of the JavaScript standard. For example, `window.location.pathname`.

This section is divided into the following parts:

- `SYSTEM` Variable Syntax
- `SYSTEM` Variable Example

SYSTEM Variable Syntax

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

where

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

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

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

SYSTEM Variable Example

Assume the base URL of the page is:

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

Page Content

```
<script LANGUAGE="Javascript">
<!--
//SYSTEM Var
alert(window.location.pathname);
//-->
</SCRIPT>
```

Rules

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

Output

```
</SCRIPT>
<SCRIPT LANGUAGE="Javascript">
<!--
//SYSTEM Var
alert(psSRAPRewriter_convert_pathname(window.location.pathname));
//-->
</SCRIPT>
```

Description

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

Function Arguments

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

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

Generic Syntax

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

where

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

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

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

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

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

URL Parameters

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

This section is divided into the following parts:

- URL Parameter Syntax
- URL Parameter Example

URL Parameter Syntax

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

where

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

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

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

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

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

URL Parameter Example

Assume the base URL of the page is:


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

Page Content

```
<script language="JavaScript">
<!--
function test(one,two,three){
alert(one + "##" + two + "##" +three);
}
test("/test.html","../test.html","123");
window.open("/index.html","gen",width=500,height=500);
//-->
</SCRIPT>
```

Rules

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

Output

```
<SCRIPT language="JavaScript">
<!--
function test(one,two,three) {
alert(one + "##" + two + "##" +three);
}
test("gateway-URLhttp://abc.sesta.com/test.html","gateway-URLhttp://abc.sesta.com/test/rewriter/test1/jscript/test.html","123");
window.open("gateway-URLhttp://abc.sesta.com/index.html","gen",width=500,height=500);
//-->
</SCRIPT>
```

Description

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

EXPRESSION Parameters

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

This section is divided into the following parts:

- **EXPRESSION Parameter Syntax**
- **EXPRESSION Parameter Example**

EXPRESSION Parameter Syntax

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

where

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

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

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

`type` specifies the value `EXPRESSION` (optional)

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

EXPRESSION Parameter Example

Assume the base URL of the page is:

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

Page Content

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

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

Rules

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

Output

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

Description

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

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

DHTML Parameters

Function parameter whose value is HTML

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

This section is divided into the following parts:

- DHTML Parameter Syntax
- DHTML Parameter Example

DHTML Parameter Syntax

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

where

`name` is the name of the function.

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

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

DHTML Parameter Example

Assume the base URL of the page is:

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

Page Content

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

```

document.writeln('<a href="index.html">writeln</a><BR>')
document.write("http://abc.sesta.com/index.html<BR>")
document.writeln("http://abc.sesta.com/index.html<BR>")
//-->
</SCRIPT>

```

Rules

```

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

```

Output

```

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

```

Description

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

DJS Parameters

Function parameters whose value is JavaScript.

This section is divided into the following sections:

- DJS Parameter Syntax
- DJS Parameter Example

DJS Parameter Syntax

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

where

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

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

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

`type` is DJS (mandatory)

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

DJS Parameter Example

Assume the base URL of the page is:

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

Page Content

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

Rules

```
<Function name="DJS" name="NavBarMenuItem" paramPatterns="y"/>
<Variable name="URL">top.location</Variable>
```

Output

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

Description

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

Rules for XML Content

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

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

Tag Text

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

This section is divided into the following parts:

- Tag Text Syntax
- Tag Text Example

Tag Text Syntax

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

where

`tagName` is the name of the tag

`attributePatterns` is the attributes and their value patterns for this tag (optional, meaning this tag has no attributes at all)

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

Tag Text Example

Assume the base URL of the page is:

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

Page Content

```
<xml>
```

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

```
<attribute>abc.html</attribute>
```

```
</xml>
```

Rules

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

Output

```
<xml>
```

```
<Attribute
```

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

```
<attribute>abc.html</attribute>
```

```
</xml>
```

Description

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

Attribute

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

Rewriter translates the attribute value based on the attribute name.

This section is divided into the following parts:

- Attribute Syntax
- Attribute Example

Attribute Syntax

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

where

attributeName is the name of the attribute (mandatory)

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

valuePatterns See “Using Pattern Matching in Rules” on page 108.

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

Attribute Example

Assume the base URL of the page is:

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

Page Content

```
<xml>
<baseroot href="/root.html"/>
<img href="image.html"/>
<string href="1234|substring.html"/>
<check href="1234|string.html"/>
</xml>
```

Rules

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

Output

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

Description

In the above example, only the fourth line is rewritten because it meets all the conditions specified in the rule. See “Using Pattern Matching in Rules” on page 108.

Rules for Cascading Style Sheets

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

Rules for WML

WML is similar to HTML and hence HTML rules are applied for WML content. Use the generic ruleset for WML content. See “Rules for HTML Content” on page 103.

Using the Recursive Feature

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

For example, when Rewriter parses the following string:

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

the rule

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

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

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

but if you use the recursive option as,

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

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

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

Configuring Rewriter in the Gateway Service

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

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

Basic Tasks

Enable Rewriting of All URIs

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

► **To Enable the Gateway to Rewrite All URLs**

1. Log in to the Sun Java System Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.

5. Click the Rewriter tab.
6. Select the Enable Rewriting of All URIs checkbox to enable the Gateway to rewrite all URLs.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Create List of URIs to RuleSet Mappings

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

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

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

where `sun.com` is the install domain of the portal and `/portal` is the portal install context

- `*|generic_ruleset`

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

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

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

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

Using Wildcards Within the Syntax

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

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

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

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

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

► **To Map a URI to RuleSet**

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

The Gateway page is displayed.

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

The Edit Gateway Profile page is displayed.

5. Click the Rewriter tab.
6. Scroll to the Map URIs to RuleSets field.
7. Type the required domain or host name and the ruleset in the Map URIs to RuleSets field and click Add.

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

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

```
domain name|ruleset name
```

For example:

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

Create List of MIME Types to Parse

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

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

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

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

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

► To Specify MIME Mappings

1. Login to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.

The Gateway page is displayed.

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

The Edit Gateway Profile page is displayed.

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

Specify the entry in the format `HTML=text/html;text/htm`

7. Click Add to add the required entry to the list.
8. Click Save to record the change.
9. Restart the Gateway from a terminal window:

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

Create List of URIs Not to Rewrite

This rule means if a URL such as `http://host.domain.com` appears on a page, it does not get rewritten. But the page will be rewritten if it contains any other URLs. If you do not want the page whose URI is `http://host.domain.com`, add a ruleset mapping: `http://host.domain.com" |null_ruleset`

► To Specify the URIs Not to Rewrite

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

The Gateway page is displayed.

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

The Edit Gateway Profile page is displayed.

5. Click the Rewriter tab, Basic subsection.
6. Scroll to the URIs Not to Rewrite field, and add the URI in the edit box.

Note: Adding `#*` to this list allows URIs to be rewritten, even when the href rule is part of the ruleset.

7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Specify the Default Domains

The default domain and subdomain are useful when URLs contain only the host names without the domain and subdomain. In this case, the Gateway assumes that the host names are in the default domain and subdomain, and proceeds accordingly.

For example, if the host name in the URL is `host1`, and the default domain and subdomain are specified as `red.sesta.com`, the host name is resolved as `host1.red.sesta.com`.

► To Specify the Default Domains

1. Login to the Access Manager administration console as administrator.
2. Click the Service Configuration tab.

3. Click the right arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Rewriter tab.
6. Scroll to the Default Domains field and type the required default value in the format `subdomain.domain name`.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Advanced Tasks

Enable MIME Guessing

Rewriter depends on the MIME type of the page to choose the parser. Some web servers such as WebLogic and Oracle do not send MIME types. To work around this, you can enable the MIME guessing feature by adding data to the Map Parser to URIs list box.

► To Enable MIME Guessing

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Click the gateway profile for which you want to set the attribute.
The Edit Gateway Profile is displayed.
5. Click the Rewriter tab, Advanced subsection.
6. Select the Enable MIME Guessing checkbox to enable MIME Guessing.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:


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

Create List of URI Mappings to Parse

If the MIME Guessing checkbox is enabled and the server has not sent a MIME type, use this list box to map the URI to parse.

Multiple URIs are separated by a semicolon.

For example `HTML=*.html;*.htm;*.Servlet`

means that the HTML Rewriter is used to rewrite the content for any page with a `html`, `htm`, or `Servlet` extension.

► To Parse URI Mappings

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Click the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Rewriter tab, Advanced subsection.
6. Scroll to the Map Parser to MIME Types field, and add the data to the edit box.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Enable Masking

Masking enables Rewriter to rewrite a URI so that the Intranet URL of a page is not seen.

► To Enable Masking

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

The Gateway page is displayed.

4. Click the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Rewriter tab, Advanced subsection.
6. Select the Enable Masking checkbox to enable Masking.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Specify the Masking Seed String

A seed string is used for masking a URI. A seed string is a random string generated by a masking algorithm.

NOTE Book marking of a masked URI may not work if this seed string has been changed or if the Gateway is restarted.

► To Specify the Masking Seed String

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Click the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Rewriter tab, Advanced subsection.
6. Scroll to the Masking Seed String field, and add a string to the edit box.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Create List of URIs Not to Mask

Some applications (such as an applet) require an Internet URI and cannot be masked. To specify those applications, add the URI to the list box.

For example if you added

```
*/Applet/Param*
```

to the list box, the URL would not be masked if the content URI `http://abc.com/Applet/Param1.html` is matched in the ruleset rule.

► **To Specify Not to Mask the URI List**

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

The Gateway page is displayed.

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

The Edit Gateway Profile is displayed.

5. Click the Rewriter tab, Advanced subsection
6. Scroll to the URIs Not to Mask field, and add the URIs to the edit box.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Make a Gateway Protocol the Same as the Original URI Protocol

When a gateway runs in both HTTP and HTTPS mode, you can enable Rewriter to use a consistent protocol to access the referred resources in the HTML content.

For example, if the original URL is `http://intranet.com/Public.html` then the HTTP gateway is added. If the original URL is `https://intranet.com/Public.html` then the HTTPS gateway is added.

NOTE This applies only to static URIs, not to dynamic URIs generated in Javascript.

► **To Make a Gateway Protocol the Same as the Original URI Protocol**

1. Log in to the Access Manager admin console as administrator.
2. Select the Service Configuration tab.

3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Click the gateway profile for which you want to set the attribute.
The Edit Gateway Profile is displayed.
5. Click the Rewriter tab, Advanced subsection.
6. Select the Make Gateway Protocol the Same as the Original URI Protocol checkbox.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Troubleshooting Using Debug Logs

To troubleshoot a Rewriter problem, you need to enable debug logs.

Debug Messages are classified as follows.

- **Error** – errors that Rewriter cannot recover from
- **Warning** – warnings that do not critically affect the functioning of Rewriter. Rewriter is able to recover this type of error, but some misbehavior may or may not result. Some messages shown in warnings are informational. For example “Not rewriting image content” is logged as a warning message. This is fine as Rewriter is not supposed to rewrite the images.
- **Message** – the highest level of information that Rewriter provides.

Setting the Rewriter Debug Level

► To Set the Rewriter Debug Level

1. Log in as root to the Gateway machine and edit the following file:

```
gateway-install-root/SUNWam/config/AMConfig-instance-name.properties
```

2. Set the debug level:

```
com.iplanet.services.debug.level=
```

The debug levels are:

error - Only serious errors are logged in the debug file. Rewriter usually stops functioning when such errors occur.

warning - Warning messages are logged.

message - All debug messages are logged.

off - No debug messages are logged.

3. Specify the directory for the debug files in the following property of the AMConfig-*instance-name*.properties file:

```
com.iplanet.services.debug.directory=/var/opt/SUNWam/debug
```

where /var/opt/SUNWam/debug is the default debug directory.

4. Restart the Gateway from a terminal window:

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

Debug File Names

When the debug level is set to message, debug generates a set of files. Table 3-2 lists the Rewriter files and the information contained within them.

Table 3-2 Rewriter Debug Files

File Name	Information
RuleSetInfo	Contains all the rulesets which have been used for rewriting, are logged in this file.
Original Pages	Contains the page URI, resolveURI (if different than the page URI), content MIME, the ruleset that has been applied to the page, parser MIME, and the original content. Specific error/warning/messages related to parsing also appear in this file. In message mode full content is logged. In warning and error mode only exceptions that occurred during rewriting are logged.
Rewritten Pages	Contains the page URI, resolveURI (if different than the page URI), content MIME, ruleset that has been applied to the page, parser MIME, and the rewritten content. This is filled when the debug mode is set to message.
Unaffected Pages	Contains a list the pages that were not modified.

Table 3-2 Rewriter Debug Files

File Name	Information
URIInfo Pages	<p>Contains the URLs found and translated. Details of all the pages whose content remain same as original data are logged in this file.</p> <p>Details logged are: Page URI, MIME and Encoding data, rulesetID used for rewriting, and Parser MIME.</p>

In addition to the above files, Rewriter generates a file for debug messages that are not captured in the above files. This file name consists of two parts: the first part is either `pwRewriter` or `psSRAPRewriter` and the second part is an extension using either `portal` or the `gateway-profile-name`.

The debug files are displayed on the portal or the Gateway. These files are in the directory indicated in the `AMConfig-instance-name.properties` file.

The Rewriter component generates the following set of files to help in debugging,

prefix_RuleSetInfo.extension

prefix_OriginalPages.extension

prefix_RewrittenPages.extension

prefix_UnaffectedPages.extension

prefix_URIInfo.extension

where

prefix is either `psRewriter` for URLScrapper usage logs or `psSRAPRewriter` for Gateway usage logs.

extension is either `portal` for URLScrapper usage or `gateway-profile-name` for Gateway usage.

For example, if the Rewriter on the Gateway is used to convert pages and the default gateway profile is used, debug creates these files:

```
psSRAPRewriter_RuleSetInfo.default
psSRAPRewriter_OriginalPages.default
psSRAPRewriter_RewrittenPages.default
psSRAPRewriter_UnaffectedPages.default
psSRAPRewriter_URIInfo.default
psSRAPRewriter.default
```

Working Samples

This section includes:

- Simple HTML pages with content that needs to be rewritten
- Rules required to rewrite the content
- Corresponding rewritten HTML page

These sample pages are available in the *portal-server-URL/rewriter* directory. You can browse through the page before the rule is applied, and then view the file with the rewritten output through your Gateway to see how the rule works. In some samples, the rule is already a part of the `default_gateway_ruleset`. In some samples, you may have to include the rule in the `default_gateway_ruleset`. This is mentioned at the appropriate places.

NOTE Some of the statements appear in bold to indicate that they have been rewritten.

The following samples are available:

- HTML
 - Sample for HTML Attributes
 - Sample for HTML Forms
 - Sample for HTML Applets
- JavaScript
 - Variables
 - Sample for JavaScript URL Variables
 - Samples for JavaScript Content
 - Sample for JavaScript DHTML Variables
 - Sample for JavaScript DJS Variables
 - Sample for JavaScript SYSTEM Variables
 - Functions
 - Sample for JavaScript URL Functions
 - Sample for JavaScript EXPRESSION Functions

- Sample for JavaScript DHTML Functions
- Sample for JavaScript DJS Functions
- XML
 - Sample for XML Attributes

Samples for HTML Content

Sample for HTML Attributes

► To Use the HTML Attributes Sample

1. This sample can be accessed from:

portal-server-URL/rewriter/HTML/attrib/attribute.html

2. Ensure that `abc.sesta.com` and `host1.siroe.com` are defined in the Proxies for Domains and Subdomains list in the Gateway service.

If this is not defined, a direct connection is assumed, and the Gateway URL is not prefixed.

You need not add the rule specified in this sample to the `default_gateway_ruleset` because the rule is already defined.

HTML Before Rewriting

```
<html>
```

```
Rewriting starts
```

```
<head>
```

```
<title>TEST PAGE () </title>
```

```
</head>
```

```
ID-htmlattr.1
```

```
<br><br>
```

```
1. a href <a href="http://abc.sesta.com/images/logo.gif">http://..</a>
```

```
<br><br>
```

```
2. href <a href="https://host1.siroe.com">https://..</a>
```

```
<br><br>
```

```
3. href <a href=" ../images/logo.gif">../images/</a>
```



```

<br><br>
4. href <a href="images/logo.gif">images/..</a> <br><br>
5. href <a href="../../images/logo.gif">../../images/</a> <br><br>
Rewriting ends
</html>

```

Rule

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

HTML After Rewriting

```

<html>
Rewriting starts
<head>
<title>TEST PAGE () </title>
</head>
ID-htmlattr.1
<br><br>
1. a href <a
href="gateway-URL/http://abc.sesta.com/images/logo.gif">http://.
..</a> <br>
// This URL is rewritten because the <Attrib name="href"/> rule is already
defined in the default_gateway_ruleset. Because the URL is already absolute, only
the Gateway URL is prefixed. Ensure that abc.sesta.com is defined in the Proxies
for Domains and Subdomains list in the Gateway service. Otherwise, the Gateway
URL is not prefixed, because a direct connection is assumed.
2. href <a
href="gateway-URL/https://host1.siroe.com">https://..</a>
// Again, host1.siroe.com needs to be defined in the Proxies for Domains and
Subdomains list in the Gateway service. Otherwise, the Gateway URL is not
prefixed, because a direct connection is assumed.
<br><br>
3. href <a
href="gateway-URL/portal-server-URL/rewriter/HTML/images/logo.gi
f">../images/</a>

```

// Because a relative path is specified, the Gateway URL and the portal-server-URL are prefixed along with the required subdirectories. This link will not work because a directory called `images` under the `HTML` directory is not specified in the sample structure provided.

```
<br><br>
```

```
4 href <a
href="gateway-URL/portal-server-URL/rewriter/HTML/attrib/images/
logo.gif">images/..</a> <br><br>
```

// Because a relative path is specified, the Gateway URL and the Portal Server URL are prefixed along with the required subdirectories.

```
5. href <a
href="gateway-URL/portal-server-URL/rewriter/images/logo.gif">..
../images/</a> <br><br>
```

// Because a relative path is specified, the Gateway URL and the Portal Server URL are prefixed along with the required subdirectories. This link will not work because a directory called `images` under the `Rewriter` directory is not specified in the sample structure provided

```
Rewriting ends
```

```
</html>
```

Sample for HTML Dynamic JavaScript Tokens

► To Use the HTML JavaScript Token Sample:

1. This sample can be accessed from:
2. Add the rule specified in this sample to the `default_gateway_ruleset` in the section "Rules for Rewriting JavaScript Source".
3. Edit the `default_gateway_ruleset` in the Rewriter service under the Portal Server Configuration in the Access Manager administration console.
4. Restart the Gateway from a terminal window:

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

HTML Before Rewriting

```
<html>
```

```
<head>
```

```
Rewriting starts
```

```

<script language="javascript">
function Check(test,ind){
if (ind == 'blur')
{alert("testing onBlur")}
if (ind == 'focus')
{alert("testing onFocus")}
}
</SCRIPT>
</head>
<body>
<form>
<input TYPE=TEXT SIZE=20 value=blur
onAbort="Check('/indexblur.html','blur');return;">
<input TYPE=TEXT SIZE=20 value=blur
onBlur="Check('/indexblur.html','blur');return;">
<input TYPE=TEXT SIZE=20 value=focus
onFocus="Check('/focus.html','focus');return;">
<input TYPE=TEXT SIZE=20 value=focus
onChange="Check('/focus.html','focus');return;">
<input TYPE=TEXT SIZE=20 value=focus
onClick="Check('/focus.html','blur');return;">
<br><br>
</form>
</body>
Rewriting ends
</html>

```

Rule

```

<Attribute name="onClick" type="DJS"/>
<Function type="URL" name="Check" paramPatterns="y"/>

```

NOTE <Function name="URL" name="Check" paramPatterns="y"/> is a JavaScript function rule and is explained in detail in the JavaScript function sample.

HTML After Rewriting

```

<html>

<head>

Rewriting starts

<script language="javascript">

function Check(test,ind){
if (ind == 'blur')
{alert("testing onBlur")}
if (ind == 'focus')
{alert("testing onFocus")}
}
</SCRIPT>

</head>

<body>

<form>

<input TYPE=TEXT SIZE=20 value=blur onAbort="Check('gateway
URL/portal-server-URL/indexblur.html','blur');return;">

<input TYPE=TEXT SIZE=20 value=blur onBlur="Check('gateway
URL/portal-server-URL/indexblur.html','blur');return;">

<input TYPE=TEXT SIZE=20 value=focus onFocus="Check('gateway
URL/portal-server-URL/focus.html','focus');return;">

<input TYPE=TEXT SIZE=20 value=focus onChange="Check('gateway
URL/portal-server-URL/focus.html','focus');return;">

<input TYPE=TEXT SIZE=20 value=focus onClick="Check('gateway
URL/portal-server-URL/focus.html','blur');return;">

// All the statements are rewritten in this sample. The Gateway and Portal Server
URLs are prefixed in each case. This is because rules for onBlur, onFocus,
onChange, and onClick are defined in the default_gateway_ruleset file. Rewriter
detects the JavaScript tokens and passes it to the JavaScript function rules for
further processing. The second rule listed in the sample tells Rewriter which
parameter to rewrite.

</body>

<br>

```

Rewriting ends

</html>

Sample for HTML Forms

► To Use the Form Sample

1. Access the sample from:

portal-server-URL/rewriter/HTML/forms/formrule.html

2. Ensure that `abc.sesta.com` is defined in the Proxies for Domains and Subdomains list in the Gateway service.

If this is not defined, a direct connection is assumed, and the Gateway URL is not prefixed.

3. Add the rule specified in this sample to the `default_gateway_ruleset` in the section "Rules for Rewriting HTML Attributes".
4. Edit the `default_gateway_ruleset` in the Rewriter service under the Portal Server Configuration in the Access Manager administration console.
5. Restart the Gateway from a terminal window:

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

HTML Page Before Rewriting

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
</head>
<body>
RW_START
<p>
<form name="form1" method="Post"
action="http://abc.sesta.com/casestudy/html/form.html">
<input type="hidden" name="name1" value="0|1234|/test.html">
<input type="hidden" name="name3" value="../../html/test.html">
<form name="form2" method="Post"
action="http://abc.sesta.com/testcases/html/form.html"><br>
```

```
<input type="hidden" name="name1"
value="0|1234|../../html/test.html"></form>
```

```
RW_END </p>
```

```
</body>
```

```
</html>
```

Rule

```
<Form source="*" name="form1" field="name1" valuePatterns="0|1234|"/>
```

HTML Page After Rewriting

```
<HTML>
```

```
<HEAD>
```

```
RW_START
```

```
</HEAD>
```

```
<BODY>
```

```
<P>
```

```
<FORM name=form1 method=POST
```

```
action="gateway-URL/http://abc.sesta.com/casestudy/html/form.htm
1">
```

// This URL is rewritten because `<Attribute name="action"/>` is defined as part of the HTML rules in the `default_gateway_ruleset`. Because the URL is already absolute, only the Gateway URL needs to be prefixed. Ensure that `abc.sesta.com` is defined in the Proxies for Domains and Subdomains list in the Gateway service. Else, the Gateway URL is not prefixed because a direct connection is assumed.

```
<input type=hidden name=name1 value="0|1234|gateway
URL/portal-server-URL/test.html">
```

// Here the form name is `form1`, and the field name is `name1`. This matches the form name and field name specified in the rule. The rule states the `valuePatterns` as `0|1234|` which matches the `value` in this statement. Hence the URL occurring after the `valuePattern` is rewritten. The Portal Server URL and the Gateway URL are prefixed. See “Using Pattern Matching in Rules” on page 108 for details on `valuePatterns`.

```
<input type=hidden name=name3 value="../../html/test.html">
```

// This URL is not rewritten because the `name` does not match the `field name` specified in the rule.

```
</FORM>
```

```
<FORM name=form2 method=POST
action="gateway-URL/http://abc.sesta.com/casestudy/html/form.htm
1"><BR>
```

// This URL is rewritten because `<Attribute name="action"/>` is defined as part of the HTML rules in the default ruleset. Because the URL is already absolute, only the Gateway URL needs to be prefixed.

```
<input type=hidden name=name1 value="0|1234|../../html/test.html">
```

// This URL is not rewritten because the form name does not match the name specified in the rule.

```
</FORM>
```

```
</BODY>
```

```
RW_END
```

```
</HTML>
```

Sample for HTML Applets

► To Use the Sample for Applets

1. Obtain the applet class file. The `RewriteURLinApplet.class` file is present in the following location:

```
portal-server-URL/rewriter/HTML/applet/appletcode
```

The base URL of the page where the applet code is present is:

```
portal-server-URL/rewriter/HTML/applet/rule1.html
```

2. Add the rule specified in this sample to the `default_gateway_ruleset` in the section "Rules for Rewriting HTML Attributes".
3. Edit the `default_gateway_ruleset` in the Rewriter service under the Portal Server Configuration in the Access Manager administration console.
4. Restart the Gateway:

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

HTML Before Rewriting

```
<html>
```

```
Rewriting starts
```

```
<br>
```

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

```

<param name=Test1 value="/index.html">
<param name=Test2 value="../index.html">
<param name=Test3 value="../../index.html">
</applet>
Rewriting ends
</html>

```

Rule

```

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

```

HTML After Rewriting

```

<HTML>

```

Rewriting starts

```

<BR>

```

```

<APPLET

```

```

codebase=gateway-URL/portal-server-URL/rewriter/HTML/applet/appl
etcode=RewriteURLinApplet.class archive=/test>

```

// This URL is rewritten because the rule `<Attribute name="codebase"/>` is already present as part of the `default_gateway_ruleset` file. the Gateway and the Portal Server URLs are prefixed along with the path up to the `appletcode` directory.

```

<param name=Test1
value="gateway-URL/portal-server-URL/index.html">

```

// This URL is rewritten because the base URL of the page is `rule1.html`, and the param name matches the param `Test*` specified in the rule. Because `index.html` is specified to be at the root level, the Gateway and Portal Server URLs are prefixed directly.

```

<param name=Test2
value="gateway-URL/portal-server-URL/rewriter/HTML/index.html">

```

// This URL is rewritten because the base URL of the page is `rule1.html`, and the param name matches the param `Test*` specified in the rule. The path is prefixed as required.

```

<param name=Test3
value="gateway-URL/portal-server-URL/rewriter/index.html">

```


// This URL is rewritten because the base URL of the page is `rule1.html`, and the param name matches the param `Test*` specified in the rule. The path is prefixed as required.

```
</APPLET>
```

```
Rewriting ends
```

```
</HTML>
```

Samples for JavaScript Content

Sample for JavaScript URL Variables

► To Use the JavaScript URL Variables Sample

1. This sample can be accessed from:

```
portal-server-URL/rewriter/JavaScript/variables/url/js_urls.html
```

2. Ensure that `abc.sesta.com` is defined in the Proxies for Domains and Subdomains list in the Gateway service.

If this is not defined, a direct connection is assumed, and the Gateway URL is not prefixed.

3. Add the rule specified in this sample to the `default_gateway_ruleset` in the section "Rules for Rewriting JavaScript Source".
4. Edit the `default_gateway_ruleset` in the Rewriter service under Portal Server Configuration in the Access Manager administration console.
5. If you added the rule, restart the Gateway:

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

HTML Page Before Rewriting

```
<html>
```

```
Rewriting starts
```

```
<head>
```

```
<title>JavaScript Variable test page</title>
```

```
</head>
```

```
<body>
```

```

<script LANGUAGE="Javascript">
<!--
//URL Variables
var imgsrc="/tmp/tmp.jpg";
var imgsrc="./tmp/tmp.jpg";
var imgsrc="../tmp/tmp.jpg";
var imgsrc="../../tmp/tmp.jpg";
var imgsrc="http://abc.sesta.com/tmp/tmp.jpg";
var imgsrc="../../../tmp/tmp.jpg";
var imgsrc="tmp/tmp.jpg";
//-->
</SCRIPT>
<br>
Testing JavaScript variables!
<br>

<br>
Image
</body>
<br>
Rewriting ends
</html>

```

Rule

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

HTML Page After Rewriting

```

<html>
Rewriting starts
<head>
<title>JavaScript Variable test page</title>
</head>

```

```

<body>
<script LANGUAGE="Javascript">
<!--
//URL Variables
var imgsrc="gateway-URL/portal-server-URL/tmp/tmp.jpg";

var
imgsrc="gateway-URL/portal-server-URL/rewriter/JavaScript/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>



// This line is rewritten because the rule <Attribute name="src"/> is defined in the
default_gateway_ruleset

<br>

Image

</body>

```

```
<br>
Rewriting ends
</html>
```

Sample for JavaScript EXPRESSION Variables

► To Use the JavaScript Expression Variables Sample

1. This sample can be accessed from:

portal-server-URL/rewriter/JavaScript/variables/expr/expr.html

2. Add the rule specified in this sample (if it does not already exist) to the `default_gateway_ruleset` in the section "Rules for Rewriting JavaScript Source".
3. Edit the `default_gateway_ruleset` in the Rewriter service under Portal Server Configuration in the Access Manager administration console.
4. If you added the rule, restart the Gateway:

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

HTML Page Before Rewriting

```
<html>
<head>
<title>JavaScript EXPRESSION Variables Test Page</title>
</head>
<body>
<script LANGUAGE="Javascript">
<!--
//Expression variables
var expvar1="images";
var expvar2="/logo.gif";
var expvar = expvar1 + expvar2;
document.write(" <A HREF="+expvar+">EXPRESSION</A><P>")
var expvar="/images/logo"+".gif";
document.write(" <A HREF="+expvar+">EXPRESSION</A><P>")
```

```
//-->
</SCRIPT>
Testing JavaScript EXPRESSION variables
</body>
</html>
```

Rule

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

HTML Page After Rewriting

```
<html>
<head>
<title>JavaScript EXPRESSION Variables Test Page</title>
</head>
<body>
<SCRIPT>
// Rewriter appends the wrapper function
psSRAPRewriter_convert_expression here
</SCRIPT>
<script LANGUAGE="Javascript">
<!--
//Expression variables
var expvar1="images";
var expvar2="/logo.gif";
var expvar =psSRAPRewriter_convert_expression( expvar1 +
expvar2);
// Rewriter recognizes the right hand side of this statement to be a JavaScript
EXPRESSION variable. Rewriter is not able to resolve the value of this expression
at the server end. Hence, the psSRAPRewriter_convert_expression function is
prefixed to the expression. The expression is evaluated at the client end, and
rewritten as required.
document.write("<A HREF="+expvar+">EXPRESSION</A><P>")
```

// The rewritten value of `expvar` from the previous statement is used to arrive at the value of this expression. Because the result is a valid URL (a graphic exists at this location in the sample), the link will work.

```
var expvar="gateway URL/portal-server-URL/images/logo"+" .gif";
```

// Rewriter recognizes the right hand side of `expvar` to be a string expression. This can be resolved at the server side, and hence is rewritten directly.

```
document.write("<A HREF="+expvar+">EXPRESSION</A><P>")
```

// The rewritten value of `expvar` from the previous statement is used to arrive at the value of this expression. Because the result is not a valid URL (a graphic does not exist at the resultant location), the link will not work.

```
//-->
```

```
</SCRIPT>
```

```
Testing JavaScript EXPRESSION variables
```

```
</body>
```

```
</html>
```

Sample for JavaScript DHTML Variables

► To Use the JavaScript DHTML Variables Sample

1. This sample can be accessed from:

```
portal-server-URL/rewriter/JavaScript/variables/dhtml/dhtml.html
```

2. Ensure that `abc.sesta.com` is defined in the Proxies for Domains and Subdomains list in the Gateway service. If this is not defined, a direct connection is assumed, and the Gateway URL is not prefixed.
3. Add the rule specified in this sample (if it does not already exist) to the `default_gateway_ruleset` in the section "Rules for Rewriting JavaScript Source". Edit the `default_gateway_ruleset` in the Rewriter service under Portal Server Configuration in the Access Manager administration console.
4. If you added the rule, restart the Gateway:

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

HTML Page Before Rewriting

```
<html>
```

```
<head>
```

```

<title>JavaScript DHTML Variable Test Page</title>
</head>
<body>
<script LANGUAGE="Javascript">
<!--
//DHTML Var
var dhtmlVar="<a href=../../images/test.html>"
var dhtmlVar="<a href=../images/test.html>"
var dhtmlVar="<a href=/images/test.html>"
var dhtmlVar="<a href=images/test.html>"
var dhtmlVar="<a href=http://abc.sesta.com/images/test.html>"
var dhtmlVar="<img src=http://abc.sesta.com/images/test.html>"
//-->
</SCRIPT>
<br><br>
Testing DHTML Variables
<br><br>
IMAGE
</body>
</html>

```

Rule

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

HTML Page After Rewriting

```

<html>
<head>
<title>JavaScript DHTML Variable Test Page</title>
</head>
<body>
<script LANGUAGE="Javascript">
<!--

```

```
//DHTML Var
var dhtmlVar="

```



```

<br><br>
Testing DHTML Variables
<br><br>

// This line is rewritten because the rule <Attribute name="src"/> is defined in the
default_gateway_ruleset.
<br><br>
Image
</body>
</html>

```

Sample for JavaScript DJS Variables

► To Use the JavaScript DJS Variables Sample

1. This sample can be accessed from:

```
portal-server-URL/rewriter/JavaScript/variables/djs/djs.html
```

2. Ensure that `abc.sesta.com` is defined in the Proxies for Domains and Subdomains list in the Gateway service. If this is not defined, a direct connection is assumed, and the Gateway URL is not prefixed.
3. Add the two rules specified in this sample (if it does not already exist) to the `default_gateway_ruleset` in the section "Rules for Rewriting JavaScript Source". Edit the `default_gateway_ruleset` in the Rewriter service under Portal Server Configuration in the Access Manager administration console.
4. Restart the Gateway:

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

HTML Page Before Rewriting

```

<html>
<head>
<title>Dynamic JavaScript Variable Test Page</title>
</head>
<body>

```

```

<script LANGUAGE="Javascript">
<!--
var dJSVar="var dJSimgsrc='/tmp/tmp/jpg' ;"
var dJSVar="var dJSimgsrc='../.../tmp/tmp/jpg' ;"
var dJSVar="var dJSimgsrc='http://abc.sesta.com/tmp/tmp/jpg' ;"
//-->
</SCRIPT>
<br>
Testing Dynamic JavaScript Variables
<br>

<br>
Image
</body>
</html>

```

Rule

```

<Variable name="dJSVar" type="DJS" />
<Variable name="dJSimgsrc" type="URL" />

```

HTML Page After Rewriting

```

<html>
<head>
<title>Dynamic JavaScript Variable Test Page</title>
</head>
<body>
<script LANGUAGE="Javascript">
<!--
var dJSVar="var
dJSimgsrc='gateway-URL/portal-server-URL/tmp/tmp/jpg' ;"
var dJSVar="var
dJSimgsrc='gateway-URL/portal-server-URL/rewriter/tmp/tmp/jpg' ;"

```

```

var dJSVar="var
dJSimgsrc='gateway-URL/http://abc.sesta.com/tmp/tmp/jpg';"
// All the above statements are rewritten with the Gateway and Portal Server
URLs. The required path is prefixed as appropriate. The first rule identifies the
right hand side of dJSVar as a dynamic JavaScript variable. This is then passed to
the second rule which identifies the right hand side of dJSimgsrc as a JavaScript
variable of type URL. This is rewritten accordingly.

//-->
</SCRIPT>

<br>

Testing Dynamic JavaScript Variables

<br>



// This line is rewritten because the rule <Attribute name="src"/> is defined in the
default_gateway_ruleset.

<br>

Image

</body>

</html>

```

Sample for JavaScript SYSTEM Variables

► To Use the JavaScript System Variables Sample

1. This sample can be accessed from:

portal-server-URL/rewriter/JavaScript/variables/system/system.html

2. Add the rule specified in this sample (if it does not already exist) to the `default_gateway_ruleset` in the section "Rules for Rewriting JavaScript Source".
3. Edit the `default_gateway_ruleset` in the Rewriter service under Portal Server Configuration in the Access Manager administration console.
4. Restart the Gateway:

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

HTML Page Before Rewriting

```

<html>
<head>
<title>JavaScript SYSTEM Variables Test Page</title>
</head>
<body>
<script LANGUAGE="Javascript">
<!--
//SYSTEM Var
alert(window.location.pathname);
//document.write("<A HREF="+window.location.pathname+">SYSTEM</A><P>")
//-->
</SCRIPT>
Testing JavaScript SYSTEM Variables
<br>
This page displays the path where the current page is located when loaded.
</body>
</html>

```

Rule

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

HTML After Rewriting

```

<html>
<head>
<title>JavaScript SYSTEM Variables Test Page</title>
</head>
<body>
<SCRIPT>
convertsystem function definition...
</SCRIPT>
<script LANGUAGE="Javascript">

```

```

<!--
//SYSTEM Var

alert(psSRAPRewriter_convert_system(window.location,
window.location.pathname,"window.location"));

// Rewriter identifies window.location.pathname as a JavaScript SYSTEM variable.
The value of this variable cannot be determined at the server end. So the Rewriter
prefixes the variable with the psSRAPRewriter_convert_pathname function. This
wrapper function determines the value of the variable at the client end and
rewrites as required.

//-->
</SCRIPT>

Testing JavaScript SYSTEM Variables

<br>

This page displays the path where the current page is located when loaded.

</body>
</html>

```

Sample for JavaScript URL Functions

► To Use the JavaScript URL Functions Sample

1. This sample can be accessed from:

portal-server-URL/rewriter/JavaScript/functions/url/url.html

2. Add the rule specified in this sample (if it does not already exist) to the `default_gateway_ruleset` in the section "Rules for Rewriting JavaScript Source". Edit the `default_gateway_ruleset` in the Rewriter service under the Portal Server Configuration in the Access Manager administration console.

3. Restart the Gateway:

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

HTML Page Before Rewriting

```

<html>

<body>

JavaScript URL Function Test Page

<br>

```

```

<script language="JavaScript">
<!--
function test(one,two,three)
{
alert(one + "##" + two + "##" +three);
}
test("/test.html","../test.html","123");
window.open("/index.html","gen",width=500,height=500);
//-->
</SCRIPT>
</body>
</html>

```

Rule

```

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

```

HTML Page After Rewriting

```

<html>
<body>
JavaScript URL Function Test Page
<br>
<script language="JavaScript">
<!--
function test(one,two,three)
{
alert(one + "##" + two + "##" +three);
}
test("/test.html","../test.html","123");
window.open("gateway-URL/portal-server-URL/index.html","gen",width=500,height=500);
//-->

```

```

</SCRIPT>
</body>
</html>

```

Sample for JavaScript EXPRESSION Functions

► To Use the JavaScript Expressions Function Sample

1. This sample can be accessed from:

portal-server-URL/rewriter/JavaScript/functions/expr/expr.html

2. Add the rule specified in this sample (if it does not already exist) to the `default_gateway_ruleset` in the section "Rules for Rewriting JavaScript Source".
3. Edit the `default_gateway_ruleset` in the Rewriter service under the Portal Server Configuration in the Access Manager administration console.
4. Restart the Gateway:

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

HTML Page Before Rewriting

```

<html>
<body>
JavaScript EXPRESSION Function Test Page
<br><br><br>
<script language="JavaScript">
<!--
function jstest2()
{
return ".html";
}
function jstest1(one)
{
return one;
}

```

```

var dir="/images/test"
var test1=jstest1(dir+"/test"+jstest2());
document.write("<a HREF="+test1+">Test</a>");
alert(test1);
//-->
</SCRIPT>
</body>
</html>

```

Rule

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

HTML Page After Rewriting

```

<html>
<body>
JavaScript EXPRESSION Function Test Page
<br><br><br>
<script>
<!--
// various functions including pSSRAPRewriter_convert_expression appear
here.
//-->
</SCRIPT>
<script language="JavaScript">
<!--
function jstest2()
{
return ".html";
}
function jstest1(one)
{
return one;

```



```

}
var dir="/images/test"

var
test1=jstest1(psSRAPRewriter_convert_expression(dir+"/test"+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

► To Use the JavaScript DHTML Functions Sample

1. This sample can be accessed from:

portal-server-URL/rewriter/JavaScript/functions/dhtml/dhtml.html

2. Add the rule specified in this sample (if it does not already exist) to the `default_gateway_ruleset` in the section "Rules for Rewriting JavaScript Source".
3. Edit the `default_gateway_ruleset` in the Rewriter service under Portal Server Configuration in the Access Manager administration console.
4. Restart the Gateway:

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

HTML Page Before Rewriting

```

<html>
<head>
Testing JavaScript DHTML Functions
<br>

```

```

<br>
<script>
<!--
document.write('<a href="/index.html">write</a><BR>')
document.writeln('<a href="index.html">writeln</a><BR>')
document.write("http://abc.sesta.com/index.html<BR>")
document.writeln("http://abc.sesta.com/index.html<BR>")
//-->
</SCRIPT>
</head>
<body BGCOLOR=white>
<br><br>
Testing document.write and document.writeln
</body>
</html>

```

Rule

```

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

```

HTML Page After Rewriting

```

<html>
<head>
Testing JavaScript DHTML Functions
<br>
<br>
<script>
<!--
document.write('<a
href="gateway-URL/portal-server-URL/index.html">write</a><BR>')

```

// The first rule specifies that the first parameter of the DHTML JavaScript function `document.write` needs to be rewritten. Rewriter identifies the first parameter to be a simple HTML statement. The HTML rules section in the `default_gateway_ruleset` has the rule `<Attribute name="href" />` which indicates that the statement needs to be rewritten.

```
document.writeln('<a
href="gateway-URL/portal-server-URL/rewriter/JavaScript/function
s/dhtml/index.html">writeln</a><BR>')
```

// The second rule specifies that the first parameter of the DHTML JavaScript function `document.writeln` needs to be rewritten. Rewriter identifies the first parameter to be a simple HTML statement. The HTML rules section in the `default_gateway_ruleset` has the rule `<Attribute name="href" />` which indicates that the statement needs to be rewritten.

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

// The above statements are not rewritten although the DHTML rule identifies the functions `document.write` and `document.writeln`. This is because the first parameter in this case is not simple HTML. It could be any string, and Rewriter does not know how to rewrite this.

```
//-->
</SCRIPT>
</head>
<body BGCOLOR=white>
<br><br>
Testing document.write and document.writeln
</body>
</html>
```

Sample for JavaScript DJS Functions

► To Use the JavaScript DJS Functions Sample

1. This sample can be accessed from:

portal-server-URL/rewriter/JavaScript/functions/djs/djs.html

2. Ensure that `abc.sesta.com` is defined in the Proxies for Domains and Subdomains list in the Gateway service.

If this is not defined, a direct connection is assumed, and the Gateway URL is not prefixed.

3. Add the rule specified in this sample (if it does not already exist) to the `default_gateway_ruleset` in the section "Rules for Rewriting JavaScript Source". Edit the `default_gateway_ruleset` in the Rewriter service under Portal Server Configuration in the Access Manager administration console.

4. Restart the Gateway:

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

HTML Page Before Rewriting

```
<html>
Test for JavaScript DJS Functions
<br>
<script>
menu.addItem(new NavBarMenuItem("All Available
Information", "JavaScript:top.location='http://abc.sesta.com'"));
//menu.addItem(new NavBarMenuItem("All Available
Information", "http://abc.sesta.com"));
</script>
</html>
```

Rule

```
<Function type="DJS" name="NavBarMenuItem" paramPatterns=",y"/>
<Variable type="URL" name="top.location"/>
```

HTML Page After Rewriting

```
<html>
Testing JavaScript DJS Functions
<br>
<script>
menu.addItem(new NavBarMenuItem("All Available
Information", "javaScript:top.location='gateway-URL/http://abc.se
sta.com'"));

```

// `abc.sesta.com` is an entry in the Proxies for Domains and Subdomains list in the Gateway service. Hence Rewriter needs to rewrite this URL. But because an absolute URL, the Portal Server URL need not be prefixed. The DJS rule states that the second parameter of the DJS function `NavBarMenuItem` needs to be rewritten. But the second parameter is again a JavaScript variable. A second rule is required to rewrite the value of this variable. The second rule specifies that the value of the JavaScript variable `top.location` needs to be rewritten. Because all these conditions are met, the URL is rewritten.

```
//menu.addItem(new NavBarMenuItem( "All Available
Information", "http://abc.sesta.com" ) );
```

// Although the DJS rule specifies that the second parameter of the function `NavBarMenuItem` needs to be rewritten, it does not happen in this statement. This is because Rewriter does not recognize the second parameter as simple HTML.

```
</script>
```

```
</html>
```

Sample for XML Attributes

► To Use the XML Attributes Sample

1. This sample can be accessed from:

portal-server-URL/rewriter/XML/attrib.html

2. Add the rule specified in this sample (if it does not already exist) to the `default_gateway_ruleset` in the section "Rules for Rewriting XML Source".
3. Edit the `default_gateway_ruleset` in the Rewriter service under the Portal Server Configuration in the Access Manager administration console.
4. Restart the Gateway:

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

XML Before Rewriting

```
<html>
```

```
RW_START
```

```
<body>
```

```
<xml>
```

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

```

</xml>
<xml>
<img href="image.html"/>
</xml>
<xml>
<string href="1234|substring.html"/>
</xml>
<xml>
<check href="1234|string.html"/>
</xml>
</body>
RW_END
</html>

```

Rule

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

HTML After Rewriting

```

<html>
Rewriting starts
<br>
<br>
<body>
<xml><baseroot href="/root.html"/></xml>
<xml><img href="image.html"/></xml>
<xml><string href="1234|substring.html"/></xml>
<del>xml</del><b>check
href="1234|gateway-URL/portal-server-URL/rewriter/XML/string.htm
l"/></del></xml>

```

// This statement is rewritten because it matches the conditions specified in the rule. The `Attribute` name is `href`, tag is `check` and the `valuePatterns` is `1234`. The string following `valuePatterns` is rewritten. See “Using Pattern Matching in Rules” on page 108 for details on `valuePatterns`.

```

</body>
Rewriting ends
</html>

```

Case Study

This section includes the source HTML pages for a sample mail client. This case study does not cover all possible scenarios and rules. This is just a sample ruleset to help you put together the rules for your intranet pages.

Assumptions

The following assumptions are made for this case study:

- The base URL of the mail client is assumed to be `abc.siroe.com`
- The Gateway URL is assumed to be `gateway.sesta.com`
- Relevant entries exist in the Proxies for Domains and Subdomains list in the Gateway service

Sample page 1

```

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<!-- saved from
url=(0053)http://abc.siroe.com/mailclient/destin/?Cmd=navbar -->
<HTML XMLNS:WM><HEAD>
<META http-equiv=Content-Type content="text/html; CHARSET=utf-8">
<META http-equiv=Pragma content=no-cache>
<META http-equiv=Expires content=0><!--Copyright (c) 2000 Microsoft
Corporation. All rights reserved.--><!--CURRENT FILE== "IE5" "WIN32"
navbar -->
<STYLE>WM\:DROPMENU {
BEHAVIOR: url(http://abc.siroe.com/mailweb/controls/dropmenu.htc)
}
</STYLE>
<LINK href="destin_files/navbar.css" type=text/css rel=stylesheet>
<SCRIPT language=javascript>

```

```

var g_szUserBase= "http://abc.siroe.com/mailclient/destin"+""/";
var g_szFolder= ".";
var g_szVirtualRoot= "http://abc.siroe.com/mailweb";
var g_szImagePath= g_szVirtualRoot + "/img/";
</SCRIPT>
<SCRIPT src="/destin_files/navbar.js"></SCRIPT>
<META content="MSHTML 6.00.2600.0" name=GENERATOR></HEAD>
<BODY oncontextmenu=return(event.ctrlKey); onselectstart=return(false);
id=outbar_mainbody style="BACKGROUND-COLOR: appworkspace" leftMargin=0
topMargin=0 scroll=no>
<TABLE class=nbTableMain id=nbTableMain style="HEIGHT: 100%" cellSpacing=0
cols=1 cellPadding=0 rows="2">
<TBODY>
<TR>
<TD class=treeBrand>
<DIV class=treeOFLOW><IMG
style="PADDING-RIGHT: 0px; PADDING-LEFT: 0px; PADDING-BOTTOM: 0px;
PADDING-TOP: 0px"
src="/destin_files/logo-ie5.gif" border=0></DIV></TD></TR>
<TR height="100%">
<TD>
<TABLE class=nbTable cellSpacing=0 cols=1 cellPadding=0 rows="4">
<TBODY>
<TR>
<TD class=nbFlybar id=show_navbar onkeydown=flybar_keydown()
onclick=ToggleTab(this.id) tabIndex=0 noWrap>
<DIV class=treeOFLOW>Shortcuts</DIV></TD></TR>
<TR style="HEIGHT: 100%">
<TD id=idOutbarpane style="TEXT-ALIGN: center" vAlign=top><A
id=inbox

```



```

href="http://abc.siroe.com/mailclient/destin/Inbox/?Cmd=contents
&Page=1"
target=viewer alt="Go to inbox"><IMG class=nbImage alt="Go to inbox"
src="destin_files/navbar-inbox.gif"></A>
<DIV class=nbLabel>Inbox</DIV><BR><A id=calendar
href="http://abc.siroe.com/mailclient/destin/Calendar/?Cmd=contents"
target=viewer alt="Go to calendar"><IMG class=nbImage
alt="Go to calendar" src="destin_files/navbar-calendar.gif"></A>
<DIV class=nbLabel>Calendar</DIV><BR><A id=contacts
href="http://abc.siroe.com/mailclient/destin/Contacts/?Cmd=contents"
target=viewer alt="Go to contacts"><IMG class=nbImage
alt="Go to contacts" src="destin_files/navbar-contacts.gif"></A>
<DIV class=nbLabel>Contacts</DIV><BR><A id=options
href="http://abc.siroe.com/mailclient/destin/?Cmd=options"
target=viewer alt="Go to options"><IMG class=nbImage
alt="Go to options" src="destin_files/navbar-options.gif"></A>
<DIV class=nbLabel>Options</DIV></TD></TR>
<TR style="HEIGHT: 1.5em">
<TD class=nbFlybar id=show_folders onkeydown=flybar_keydown()
onclick=ToggleTab(this.id) tabIndex=0 noWrap>
<DIV class=treeOFLOW>Folders</DIV></TD></TR>
<TR>
<TD class=nbTreeProgress id=treeProgress style="DISPLAY: none"
vAlign=top noWrap><SPAN id=idLoading
style="OVERFLOW: hidden">Loading...</SPAN>
</TD></TR></TBODY></TABLE></TD></TR></TBODY></TABLE>
</BODY></HTML>

```

Description

Table 3-3 shows the mapping between the sample ruleset and the case study.

Table 3-3 Mapping Between Sample Ruleset and Case Study

Page Content	Rule Applied	Rewriter Output	Description
<pre>var g_szVirtualRoot= "http://abc.siroe.com/mailweb";</pre>	<pre><Variable name="URL"> g_szVirtualRoot </Variable></pre>	<pre>var g_szVirtualRoot= "http://gateway.sesta.com/http://abc.siroe.com/mailweb";</pre>	<p><code>g_szVirtualRoot</code> is a variable whose value is a simple URL.</p> <p>This rule tells Rewriter to search for a variable <code>g_szVirtualRoot</code> of type URL. If such a variable exists in the web page, Rewriter converts this to an absolute URL, and prefixes the Gateway URL.</p>
<pre>src="/destin_files/logo-ie5.gif"</pre>	<pre><Attribute name="src" /></pre>	<pre>src="http://gateway.sesta.com/http://abc.siroe.com/destin_files/logo-ie5.gif"</pre>	<p><code>src</code> is the name of an attribute, and does not have any tag or valuePattern attached to it.</p> <p>This rule tells Rewriter to search for all attributes with the name <code>src</code>, and rewrite the value of that attribute.</p>
<pre>href="http://abc.siroe.com/mailclient/destin/Inbox/?Cmd=contents&Page=1"</pre>	<pre><Attribute name="href" /></pre>	<pre>href="http://gateway.sesta.com/http://abc.siroe.com/mailclient/destin/Inbox/?Cmd=contents&Page=1"</pre>	<p><code>href</code> is the name of an attribute, and does not have any tag or valuePattern attached to it.</p> <p>This rule tells Rewriter to search for all attributes with the name <code>href</code>, and rewrite the value of that attribute.</p>

NOTE The order of priority for applying the ruleset is
hostname-subdomain-domain.

For example, assume that you have the following entries in the Domain-based rulesets list:

sesta.com|ruleset1

eng.sesta.com|ruleset2

host1.eng.sesta.com|ruleset3

ruleset3 is applied for all pages on host1.

ruleset2 is applied for all pages in the eng subdomain, except for pages retrieved from host1.

ruleset1 is applied for all pages in the sesta.com domain, except for pages retrieved from the eng subdomain, and from host1.

5. Click Save to record the change.
6. Restart the Gateway from a terminal window:

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

Ruleset for Outlook Web Access

SRA software supports MS Exchange 2000 SP3 installation and MS Exchange 2003 of Outlook Web Access (OWA) on the Sun Java System Web Server and the IBM application server.

► **To Configure the OWA Ruleset**

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

The Gateway page is displayed.

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

The Edit Gateway Profile page is displayed.

5. In the Map URIs to RuleSets field, enter the server name where Exchange 2000 is installed followed by the Exchange 2000 Service Pack 4 OWA ruleset.

For example:

`exchange.domain.com|exchange_2000sp3_owa_ruleset.`

Using Public Folders

On the Exchange side Public Folders are configured to use NTLM Authorization. It needs to be changed to use HTTP Basic Authorization.

To do this, go to the Exchange server and select the Control Panel-->Administrative Tools, then open Internet Information Services.

Under Default Web Site there is a tab for Public Folders called Public. Right Click and select properties. Click on Directory Security Tab. Select "Edit.." on the Anonymous Access and Authentication control panel. Unselect everything else and select only Basic Authentication.

Mapping of 6.x RuleSet with 3.0

The following table lists the mapping of the SRA Rewriter rules with the previous releases of the Portal Server product.

Table 3-4 Mapping of Rules with SP3

Rewriter 6.0 DTD Element	Rewriter 3.0 List Box Name
Rules for HTML Content	
Attribute - URL	Rewrite HTML Attributes
Attribute - DJS	Rewrite HTML Attributes containing JavaScript
Form	Rewrite Form Input Tag List
Applet	Rewrite Applet/Object Parameter Values List
Rules for JavaScript Content	
Variable - URL	Rewrite JavaScript Variables in URL
Variable - EXPRESSION	Rewrite JavaScript Variables Function
Variable - DHTML	Rewrite JavaScript Variables in HTML
Variable - DJS	Rewrite JavaScript Variables in JavaScript
Variable - SYSTEM	Rewrite JavaScript System Variables
Function - URL	Rewrite JavaScript Function Parameters
Function - EXPRESSION	Rewrite JavaScript Function Parameters Function
Function - DHTML	Rewrite JavaScript Function Parameters in HTML
Function - DJS	Rewrite JavaScript Function Parameters In JavaScript
Rules for XML Content	

Table 3-4 Mapping of Rules with SP3

Rewriter 6.0 DTD Element	Rewriter 3.0 List Box Name
Attribute - URL	Rewrite Attribute value of XML Document
TagText	Rewrite Text data of XMI 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	

NetFile

This chapter describes NetFile and explains its operation. To configure NetFile, see Chapter 10, “Configuring NetFile” on page 291.

This chapter covers the following topics:

- Overview of NetFile
- Supported File Access Protocols
- Setting NetFile Locale
- Opening Files from a Local Host
- Enabling Debugging for NetFile
- Enabling Logging for NetFile

Overview of NetFile

NetFile is a file manager application that enables the user to access and operate on remote file systems and directories.

The NetFile component of SRA is available as Java1 and Java2 applets. Users who do not have the Java2 Plugin for their browsers can use the Java1 applet. The Java2 applet has a better interface and increased ease of accessibility.

NetFile provides the following key features:

- Facility to add or remove shares or folders
- File upload and download
- Search for files and folders
- File compression using GZIP and ZIP

- Mail facility within the NetFile environment
- Save the current NetFile session information
- Drag and Drop of files

To configure NetFile, see Chapter 10, “Configuring NetFile”.

Supported File Access Protocols

NetFile allows you to access remote systems using FTP, NFS, and jCIFS (Microsoft Windows) protocols. It includes the following file access protocol features:

- If the user specifies AUTODETECT to add a system, NetFile uses the following sequence to automatically detect which protocol to use:
 - Checks the host for FTP server on port 21. If the FTP response contains the string "NetWare", this is considered a NETWARE host.
 - Checks the host for NFS server on port 2049.
 - Checks the host for Microsoft Windows on port 139.
 - If all of the above fail, a message saying unable to determine the host type is displayed.

The first file system type that is detected is used to connect to the requested host. The host detection order can be changed in the Access Manager administration console.

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

- NetFile enables users to select the file server and protocol of their choice.

For each of these protocols, the platforms that are supported are listed below.

Table 4-1 File Systems and Supported Protocols

File System/Protocol	Platform
FTP	Novell FTP 5.1 Server on Novell Netware MS FTP Server 4.0 on Win NT 4.0 MS FTP Server 5.0 on Win NT 2000 Solaris FTP Server WU_FTP 2.6.1 ProFTPD 1.2.8 vsFTPd 1.2.0
NFS	Solaris 2.6 and higher
jCIFS	Windows 95/98/NT/2000/ME/XP

NOTE To upload files to a ProFTPD server using NetFile, "AllowStoreRestart" needs to be set to "on" in the `proftpd.conf` file on the host running ProFTPD server.

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

NOTE To access Microsoft Windows (SMB/CIFS) file systems jCIFS must be installed on the Portal Server. jCIFS is an Open Source client library that implements the CIFS/SMB networking protocol.

1. Create the NetFile policy based on the NetFile service and assign the NetFile policy for organization and role which require access to NetFile.
2. Assign the NetFile service to each user who requires access to NetFile.

See the *Access Manager Administration Guide* for more information on creating and assigning policies and services.

Setting NetFile Locale

The language used by NetFile is by default English or the web container. However, you can change a user preferred language. From the Access Manager, for each user you can either customize the preferred locale or force it to be inherited. For instructions to do this, see Chapter 10, “Configuring NetFile” on page 291.

Opening Files from a Local Host

When using HTTP protocol, some browsers restrict applets from opening local documents.

► To Allow a Local File to be Opened

1. Change directory to the browser installation directory.
2. Change directory to the appropriate profile directory.
3. Modify the user.prefs file to add the following value:

```
user_pref("security.checkloaduri", false);
```

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-instance-name.properties` file on the Portal Server node.

For example, if the value of the `com.iplanet.services.debug.directory` attribute is:

```
/var/opt/SUNWam/debug/
```

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

See the *Access Manager Administration Guide* for more information.

Enabling Logging for NetFile

Specify the log location using the Access Manager Logging service to enable logging for NetFile. The name of the log file is `srapNetFile` and by default is located in the `/var/opt/SUNWam/logs` directory.

Enabling Logging for NetFile

Netlet

This chapter describes how to use Netlet to run applications securely between users' remote desktops and the servers running applications on your intranet. To configure Netlet, see Chapter 11, "Configuring Netlet" on page 309.

This chapter covers the following topics:

- Overview of Netlet
- Downloading an Applet From a Remote Host
- Defining Netlet Rules
- Sample Netlet Rules
- Enabling Netlet Logging
- Enable Debug Logging
- Running Netlet in a Sun Ray Environment

Overview of Netlet

Sun Java™ System Portal Server software users may want to run popular or company-specific applications on their remote desktops in a secure manner. You can provide secure access to these applications by setting up Netlet on your platform.

Netlet enables users to securely run common TCP/IP services over insecure networks such as the Internet. You can run TCP/IP applications (such as Telnet and SMTP), HTTP applications, and any fixed port applications.

If an application is TCP/IP-based or it uses fixed ports, you can run the application over Netlet. .

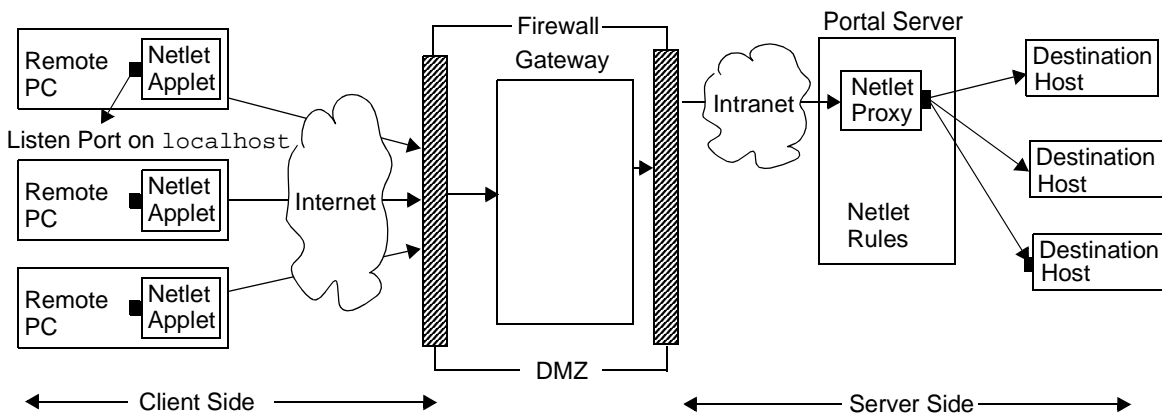
NOTE Dynamic ports are supported only when FTP is used. To use Microsoft Exchange, use OWA (Outlook Web Access).

Please advise your users that when using Netlet applets, browser pop-up blockers must be disabled.

Netlet Components

The various components used by Netlet are shown in Figure 5-1.

Figure 5-1 Netlet Components



Listen Port on localhost

This is the port on the client machine on which the Netlet applet listens. The client machine is the localhost.

Netlet Applet

The Netlet applet is responsible for setting up an encrypted TCP/IP tunnel between the remote client machine and intranet applications such as Telnet, Graphon or Citrix. The applet encrypts the packets and sends them to the Gateway, and decrypts the response packets from the Gateway and sends them to the local application.

For static rules the Netlet applet is downloaded automatically when the user logs into the portal. For dynamic rules, the applet is downloaded when the user clicks on the link corresponding to the dynamic rule. See “Types of Rules” on page 195 for details on static and dynamic rules.

To run Netlet in a Sun Ray Environment, see “Running Netlet in a Sun Ray Environment” on page 209.

Netlet Rules

A Netlet rule maps an application that needs to run on a client machine to the corresponding destination host. This means that Netlet operates only on packets sent to ports defined in the Netlet rule. This ensures greater security.

As an administrator, you need to configure certain rules for the functioning of Netlet. These rules specify various details such as the cipher to be used, URL to invoke, the applets to be downloaded, the destination port and the destination host. When a user on a client machine makes a request through Netlet, these rules help determine how the connection must be established. See “Defining Netlet Rules” on page 191 for details.

Netlet Provider

This is the UI component of Netlet. The provider allows users to configure the required applications from the 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 191.

Netlet Proxy (Optional)

The Gateway ensures a secure tunnel between the remote client machine and the Gateway. The Netlet proxy is optional and you may choose not to install this proxy during the installation. For information on the Netlet proxy, see “Using a Netlet Proxy” on page 68.

Netlet Usage Scenario

The following sequence of events are involved in using Netlet:

1. The remote user logs into the 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 191 for details on static and dynamic rules.

3. Netlet listens on the local ports defined in the Netlet rules.
4. Netlet sets up a channel between the remote client and host over the ports specified in the Netlet rule.

Working With Netlet

For Netlet to work as required for various users across different organizations, you need to do the following:

1. Determine whether you need to create static or dynamic rules based on the user requirements. See “Types of Rules” on page 195.
2. Define the global options in the Netlet template from the Service Configuration tab on the Access Manager administration console. See Chapter 11, “Configuring Netlet” on page 309.
3. Determine whether the rules should be organization, role, or user based and make modifications as required at each level. See the *Portal Server Administration Guide* for details on organization, role and user.

NOTE Do not localize the value for the frameset parameter in the `srapNetletServlet.properties` file.

Downloading an Applet From a Remote Host

Sometimes a page is returned by a URL that contains an embedded applet that needs to be fetched from a remote machine. However Java™ security does not allow an applet to communicate with a host that it is not downloaded from. To allow the applet to communicate with the Gateway through the local network port, you need to check the Download Applet field on the Access Manager administration console and specify the following syntax:

local-port:server-host:server-port

where

local-port is the local port where Netlet listens for traffic originating from the applet

server-host is where the applet is to be downloaded from

server-port is the port used to download the applet

Defining Netlet Rules

Netlet configuration is defined by Netlet rules that are configured in the Access Manager administration console under the SRA Configuration section. Netlet rules can be configured for organizations, roles, or users. If the Netlet rule is for a role or user, select the desired role or user after selecting the organization.

CAUTION Netlet rules do not support multibyte entries. Do not specify multibyte characters for any of the editable fields in Netlet rules.

Netlet rules cannot contain any port number higher than 64000.

Table 5-1 lists the fields in a Netlet rule.

Table 5-1 Fields in a Netlet Rule

Parameter	Description	Value
RuleName	Designates a name for this Netlet rule. You need to specify a unique name for each rule. This is useful while defining user access to specific rules. See "Define Access to Netlet Rules" on page 318 for details.	
Encryption Ciphers	Defines the encryption cipher, or specifies the list of ciphers that the user can choose from.	The ciphers that you select appear in the Netlet provider as a list. The user can choose the required ciphers from the selected list. Default - The Default VM Native Cipher and the Default Java Plugin Cipher specified in the Netlet administration console are used.
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, <code>telnet://localhost:30000</code> . Specify a URL if the application uses an applet to invoke the application. <code>null</code> – 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.

Table 5-1 Fields in a Netlet Rule

Parameter	Description	Value
Download Applet	Indicates whether it is necessary to download an applet for this rule.	<p>False - Do not download an applet.</p> <p>True - Download the applet from the Portal Server machine using the loopback port.</p> <p>Specify the applet details in the format <i>local-port:server-host:server-port</i> where:</p> <ul style="list-style-type: none"> <i>local-port</i> indicates the destination port on the client. This port must be different from the default loopback port. See Chapter 11, "Configuring Netlet" for details. Specify a unique <code>local port</code> for each rule. <i>server-host</i> is the name of the server from which to download the applet. <i>server-port</i> represents the port on the server used to download the applet. <p>If an applet is to be downloaded, and if the server is not specified, the applet is downloaded from the Portal Server host.</p>
Extend Session	This controls the idle time-out of a Portal Server session when Netlet is active.	<p>True - This is required to keep the portal session alive when only Netlet is active and the rest of the portal application is idle.</p> <p>False - The portal session idle times out at session idle time-out even though the Netlet application is active and the rest of the portal application is idle.</p>
Local Port	Port on the client where Netlet listens.	<p>The value of <i>local-port</i> must be unique. You cannot specify a particular port number in more than one rule.</p> <p>Specify multiple local ports if you are specifying multiple hosts for multiple connections. See "Static Rule With Multiple Host Connections" on page 199 for the syntax.</p> <p>For an FTP rule the local port value must be 30021.</p>

Table 5-1 Fields in a Netlet Rule

Parameter	Description	Value
Destination Host(s)	Recipient of the Netlet connection.	<p><i>host</i> - Name of the host to receive the Netlet connection. This is used in a static rule. Use either the simple host name such as <i>sir0e</i>, or a fully-qualified DNS-style host name such as <i>sir0e.mycompany.com</i>. Specify multiple hosts for the following reasons:</p> <ul style="list-style-type: none"> to establish connection with each host specified. You need to specify the corresponding client and destination ports for each host specified. See “Static Rule With Multiple Host Connections” on page 199 for the syntax. to try to connect to any available host from the list of hosts specified. See “Static Rule with Multiple Host Selection” on page 200 for the syntax. <p>TARGET - Rules that specify TARGET in the syntax are dynamic rules. TARGET indicates that end-users can specify the required destination host or hosts in the Netlet provider of the desktop.</p> <p>You cannot have a combination of a static host and TARGET in a single rule.</p>
Destination Port(s)	The port on the destination host	<p>In addition to the host and destination host, you must specify a destination port.</p> <p>You can specify multiple destination ports in case of multiple destination hosts. Specify multiple ports in the format <code>port1+port2+port3-port4+port5</code>.</p> <p>The plus (+) sign between ports numbers indicates the alternative ports for a single destination host.</p> <p>The minus (-) sign between port numbers is the separator between the port numbers for different destination hosts.</p> <p>Here, Netlet tries to connect to the first destination host specified using <code>port1</code>, <code>port2</code> and <code>port3</code> in order. If this fails, Netlet tries to connect to the second host using <code>port4</code> and <code>port5</code> in that order.</p> <p>You can configure multiple ports only for static rules.</p>

For the Gateway to get the session notification from Portal Server, add the following:

```
com.ipplanet.am.jassproxy.trustAllServerCerts=true
```

to the following property file

`/etc/opt/SUNWam/config/AMConfig.instance-name.properties` on the Portal Server

2. Restart the Access Manager.

Types of Rules

Two types of Netlet rules are based on how the destination host is specified in the rule.

Static Rule

A static rule specifies a destination host as part of the rule. If you create a static rule, the user does not have the option to specify the required destination host. In the following example, `sesta` is the destination host.

Rule Name	Encryption Cipher	URL	Download Applet	Extend Session	Local Port	Destination Host(s)	Destination Port(s)
ftpstatic	SSL_RSA_WITH_RC4_128_MD5	null	false	true	30021	sesta	21

You can configure multiple destination hosts and ports for static rules. See “Static Rule With Multiple Host Connections” on page 199 for an example.

Dynamic Rule

In a dynamic rule, the destination host is not specified as a part of the rule. The user can specify the required destination host in the Netlet provider. In the following example, `TARGET` is the placeholder for the destination host.

Rule Name	Encryption Cipher	URL	Download Applet	Extend Session	Local Port	Destination Host	Destination Port(s)
ftpdynamic	SSL_RSA_WITH_RC4_128_MD5	null	false	true	30021	TARGET	21

Encryption Ciphers

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

- **User Configurable Cipher Rules** - In this rule, you can specify a list of ciphers that users can choose from. These optional ciphers appear as a list in the Netlet provider. The user can choose the required cipher from the list. In the following example, the user can choose from multiple ciphers.

Rule Name	Encryption Cipher	URL	Download Applet	Extend Session	Local Port	Destination Host(s)	Destination Port(s)
Telnet	SSL_RSA_WITH_RC4_128_SHA SSL_RSA_WITH_RC4_128_MD5	null	false	true	30000	TARGET	23

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

See “Supported Ciphers” on page 196 for a list of the ciphers supported by Netlet.

- **Administrator Configured Cipher Rules** - In this rule, the cipher is defined as part of the Netlet rule. The user does not have the option to choose the required cipher. In the following example, the cipher is configured to be SSL_RSA_WITH_RC4_128_MD5.

Rule Name	Encryption Cipher	URL	Download Applet	Extend Session	Local Port	Destination Host(s)	Destination Port(s)
Telnet	SSL_RSA_WITH_RC4_128_MD5	null	false	true	30000	TARGET	23

See “Supported Ciphers” on page 196 for a list of ciphers supported by Netlet.

Supported Ciphers

Table 5-2 lists the ciphers supported by Netlet.

Table 5-2 List of Supported Ciphers**Ciphers****Native VM Ciphers**

KSSL_SSL3_RSA_WITH_3DES_EDE_CBC_SHA
 KSSL_SSL3_RSA_WITH_RC4_128_MD5
 KSSL_SSL3_RSA_WITH_RC4_128_SHA
 KSSL_SSL3_RSA_EXPORT_WITH_RC4_40_MD5
 KSSL_SSL3_RSA_WITH_DES_CBC_SHA

Java Plugin Ciphers

SSL_RSA_WITH_3DES_EDE_CBC_SHA
 SSL_RSA_WITH_RC4_128_MD5
 SSL_RSA_WITH_RC4_128_SHA
 SSL_RSA_EXPORT_WITH_RC4_40_MD5
 SSL_RSA_WITH_DES_CBC_SHA
 SSL_RSA_WITH_NULL_MD5

Backward Compatibility

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

Rule Name	Encryption Cipher	URL	Download Applet	Extend Session	Local Port	Destination Host(s)	Destination Port(s)
Telnet		telnet://localhost:3000	false	true	30000	TARGET	23

is interpreted as:

Rule Name	Encryption Cipher	URL	Download Applet	Extend Session	Local Port	Destination Host(s)	Destination Port(s)
Telnet	Default ciphers	telnet://localhost:30000	false	true	30000	TARGET	23

This is similar to an Administrator Configured Rule with the Encryption cipher field chosen as Default. See “Specify the Default Encryption Cipher” on page 313 for details.

NOTE Netlet rules cannot contain any port number higher than 64000.

Netlet Rule Examples

This section contains some examples of Netlet rules to illustrate how Netlet syntax works.

- Basic Static Rule
- Static Rule With Multiple Host Connections
- Dynamic Rule to Invoke a URL
- Dynamic Rule to Download an Applet

Basic Static Rule

This rule supports a Telnet connection from the client to the machine `sesta`.

Rule Name	Encryption Cipher	URL	Download Applet	Extend Session	Local Port	Destination Host(s)	Destination Port(s)
myrule	SSL_RSA_WITH_RC4_128_MD5	null	false	true	1111	sesta	23

where

`myrule` is the name of the rule.

`SSL_RSA_WITH_RC4_128_MD5` indicates the cipher to be used.

`null` indicates that this application is not invoked by a URL or run through the desktop.

`false` indicates that the client does not download an applet to run this application.

`true` indicates that Portal Server should not time out when the Netlet connection is active.

`1111` is the port on the client where Netlet listens for a connection request from the destination host.

`sesta` is the name of the recipient host in the Telnet connection.

`23` is the port number on the destination host for the connection, in this case the well-known port for Telnet.

The desktop Netlet provider does not display a link, but Netlet automatically starts and listens on the port specified (`1111`). Instruct the user to start the client software - in this case a Telnet session that connects to `localhost` on port `1111`.

For example, to start the Telnet session, the client needs to type the following on the UNIX command line in a terminal:

```
telnet localhost 1111
```

Static Rule With Multiple Host Connections

This rule supports a Telnet connection from the client to two machines, `sesta` and `siroe`.

Rule Name	Encryption Cipher	URL	Download Applet	Extend Session	Local Port	Destination Host(s)	Destination Port(s)
myrule	SSL_RSA_WITH_RC4_128_MD5	null	false	true	1111	sesta	23
					1234	siroe	23

where

23 is the port number on the destination host for the connection – reserved port for Telnet.

1111 is the port on the client where Netlet listens for a connection request from the first destination host `sesta`.

1234 is the port on the client where Netlet listens for a connection request from the second destination host `siroe`.

The first six fields in this rule are the same as in “Basic Static Rule” on page 198. The difference is that three more fields identify the second destination host.

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

NOTE You can have multiple sets of three fields describing the connection to each destination host. Listen port numbers which are less than 2048 must not be used if the remote client is UNIX-based because low numbered ports are restricted and you must be root to start a listener.

This rule works the same as the previous rule. The Netlet provider does not display any link, but Netlet automatically starts and listens on the two ports specified (1111 and 1234). The user needs to start the client software, in this case a Telnet session that connects to `localhost` on port 1111 or the `localhost` on port 1234 to connect to the host in the second example.

Static Rule with Multiple Host Selection

Use this rule to specify multiple alternative hosts. If connection to the first host in the rule fails, Netlet tries to connect to the second host specified and so on.

Rule Name	Encryption Cipher	URL	Download Applet	Extend Session	Local Port	Destination Host(s)	Destination Port(s)
gojoe	SSL_RSA_WITH_RC4_128_MD5	/gojoe.html	8000:gojoeserver:8080	true	10491	siroe+sesta	35+26+491-35+491

where

10491 is the port on the client where Netlet listens for a connection request from the destination host.

Netlet tries to establish connection with `sir0e` on port 35, port 26 and port 491 in the same order, depending on which one is available.

If connections to `sir0e` are not possible, Netlet tries to connect to `sesta` on port 35 and 491 in the same order.

The plus (+) sign between hosts indicates alternative hosts.

The plus (+) sign between ports numbers indicates the alternative ports for a single destination host.

The minus (-) sign between port numbers is the separator between the port numbers for different destination hosts.

Dynamic Rule to Invoke a URL

This rule enables a user to configure the destination host required, enabling the user to telnet to various hosts over Netlet.

Rule Name	Encryption Cipher	URL	Download Applet	Extend Session	Local Port	Destination Host(s)	Destination Port(s)
myrule	SSL_RSA_WITH_RC4_128_MD5	telnet://localhost:30000	false	true	30000	TARGET	23

where

`myrule` is the name of the rule.

`SSL_RSA_WITH_RC4_128_MD5` indicates the cipher to be used.

`telnet://localhost:30000` is the URL invoked by the rule.

`false` indicates that no applets are to be downloaded.

`Extend Session(true)` indicates that the Portal Server should not time out when the Netlet connection is active.

`30000` is the port on the client where Netlet listens for connection requests for this rule.

TARGET indicates that the destination host needs to be configured by the user using the Netlet provider.

23 is the port on the destination host opened by Netlet, in this case the well-known port for Telnet.

► **To Run Netlet After a Rule is Added**

After this rule is added, the user must complete some steps to get Netlet running as expected. The user needs to do the following on the client side:

1. Click Edit in the Netlet provider section of the standard Portal Server desktop.
The new Netlet rule is listed under Rule Name in the Add New Target section.
2. Choose the rule name and type the name of the destination host.
3. Save the changes.

The user returns to the desktop with the new link visible in the Netlet provider section.

4. Click the new link.

A new browser is launched that goes to the URL given in the Netlet rule.

NOTE You can add more than one destination host for the same rule by repeating these steps. Only the last link selected is active.

Dynamic Rule to Download an Applet

This rule defines a connection from the client to hosts that are dynamically allocated. The rule downloads a GO-Joe applet from the server on which the applet is located, to the client.

Rule Name	Encryption Cipher	URL	Downlaod Applet	Extend Session	Local Port	Destination Host(s)	Destina tion Port(s)
gojoe	SSL_RSA_WITH_RC4_128_MD5	/gojoe.html	8000:gojoe server:8080	true	3399	TARGET	58

where

`gojoe` is the name of the rule.

`SSL_RSA_WITH_RC4_128_MD5` indicates the cipher to be used.

`/gojoe.html` for example is the path of the HTML page containing the applet, the path should be relative to the documentation root of the web container on which portal is deployed.

`8000:server:8080` indicates that port 8000 is the destination port on the client to receive the applet, `gojoeserve` is the name of the server providing the applet, and 8080 is the port on the server from which the applet is downloaded.

`Extended Session (true)` indicates that the Portal Server should not time out when the Netlet connection is active.

3399 is the port on the client where Netlet listens for connection requests of this type.

`TARGET` indicates that the destination host needs to be configured by the user using the Netlet provider.

58 is the port on the destination host opened by Netlet, in this case the port for GoJoe. Port 58 is the port that the destination host listens to for its own traffic. Netlet passes information to this port from the new applet.

Sample Netlet Rules

Table 5-3 lists sample Netlet rules for some common applications.

The table has 7 columns corresponding to the following fields in a Netlet rule: Rule Name, URL, Download Applet, Local Port, Destination Host, Destination Port. The last column includes a description of the rule.

NOTE Table 5-3 does not list the Cipher and Extend Session fields of the Netlet rule. Assume these to be "SSL_RSA_WITH_RC4_128_MD5" and "true" for the samples provided.

Table 5-3 Sample Netlet Rules

Rule	URL	Download Applet	LOCAL Port	Destination Host	Destination Port	Description
IMAP	null	false	10143	imapserver	143	The Netlet local port on the client side need not be the same as the destination port on the server side. If you use anything other than the standard IMAP and SMTP ports, make sure that the client is configured to connect on a port that is different from the standard port. Solaris client users cannot connect to port numbers lower than 1024 unless they are running as root.
SMTP	null	false	10025	smtpserver	25	
Lotus Web Client	null	false	80	lotus-server	80	This rule tells Netlet to listen for the client on port 80, and connect to the server lotus-server on port 80. A requirement of the Lotus Web Client is that the client listen port must match the server port.

Table 5-3 Sample Netlet Rules

Rule	URL	Download Applet	LOCAL Port	Destination Host	Destination Port	Description
Lotus Notes Non-web Client	null	false	1352	lotus-dominio	1352	<p>With this rule, the Lotus Notes client can connect to a Lotus Domino server through Netlet. Ensure that when the client tries to connect to the server it must not point to localhost as the server name. It must point to the actual server name of the Lotus Domino server. The server name must be the same as the system name for the server. The client must resolve that name to 127.0.0.1 when using Netlet. Two ways to accomplish this are:</p> <ul style="list-style-type: none"> • 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. <p>The server name must be the same server name that was used to configure the Domino server during setup.</p>

Table 5-3 Sample Netlet Rules

Rule	URL	Download Applet	LOCAL Port	Destination Host	Destination Port	Description
Microsoft Outlook and Exchange Server This will not work for Windows NT, 2000 and XP. Use Outlook Web Access through the Rewriter for Windows NT, 2000, and XP.	null	false	135	exchange	135	<p>This rule tells Netlet to listen at port 135 on the client and connect to the server exchange on port 135. The Outlook client uses this port to make an initial attempt to contact the Exchange server and determine what subsequent ports to use to talk to the server.</p> <p>On the client machine:</p> <ul style="list-style-type: none"> • The user must 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. <p>The entry looks like this:</p> <pre>127.0.0.1 exchange</pre>

Table 5-3 Sample Netlet Rules

Rule	URL	Download Applet	LOCAL Port	Destination Host	Destination Port	Description
FTP	null	false	30021	<i>your-ftp_</i> <i>server.your-d</i> <i>omain</i>	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 <i>must</i> define port 30021 as the local port for your Netlet FTP rule. Dynamic FTP is not supported using a Netlet connection.
Netscape 4.7 Mail Client	null	false	30143, 30025.	TARGET TARGET	10143 10025	In the Netscape client, the user needs to specify: localhost:30143 for IMAP or incoming mails localhost:30025 for SMTP or outgoing mails
Graphon	third_	true	10491	TARGET	491	This is the rule used to access Graphon through the Netlet. <i>xsession_start.html</i> is bundled with Graphon.
Citrix	third_	true	1494	TARGET	1494	This is the rule used to access Citrix through the Netlet. <i>citrix_start.html</i> is bundled with Citrix.

Table 5-3 Sample Netlet Rules

Rule	URL	Download Applet	LOCAL Port	Destination Host	Destination 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. <code>pca_start.html</code> is bundled with Remote Control.

Enabling Netlet Logging

You can enable logging of Netlet related activities in the Gateway service. See “Enable Netlet Logging” on page 290. The log files are created in the directory specified in the Log Location attribute as part of the Logging section of the Access Manager Configuration attributes.

The log file name has the following convention:

```
srappNetlet_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)

Enable Debug Logging

The location of the debug information depends on the setting of the `com.ipplanet.services.debug.directory` attribute in the `AMConfig-instance-name.properties` file on the Portal Server node.

For example, if the value of the `com.ipplanet.services.debug.directory` attribute is:

```
/var/opt/SUNWam/debug/
```

Then the debug information for Netlet is available in the `srappNetlet` file in the `/var/opt/SUNWam/debug` directory.

See the *Access Manager Administration Guide* for more information.

Running Netlet in a Sun Ray Environment

If you want to run an application which requires the applet to be downloaded to the client machine on a Sun Ray environment, you need to change the HTML file. Here is a sample file showing you the necessary modifications that need to be done.

New HTML File

```
<!-- @(#)citrix_start.html 2.1      98/08/17 Copyright (c) 1998 i-Planet, Inc., All rights
reserved. -->

<html>

<script language="JavaScript">
var KEY_VALUES; // KEY_VALUES['key'] = 'value';
function retrieveKeyValues() {
    KEY_VALUES = new Object();
    var queryString = '' + this.location;
    queryString = unescape(queryString);
    queryString = queryString.substring((queryString.indexOf('?') + 1);
    if (queryString.length < 1) {
        return false; }
    var keypairs = new Object();
    var numKP = 0;
    while (queryString.indexOf('&') > -1) {
        keypairs[numKP] = queryString.substring(0,queryString.indexOf('&'));
        queryString = queryString.substring((queryString.indexOf('&')) + 1);
        numKP++;
    }
}
```

```

    }
    // Store what's left in the query string as the final keypairs[] data.
    keypairs[numKP++] = queryString;
    var keyName;
    var keyValue;
    for (var i=0; i < numKP; ++i) {
        keyName = keypairs[i].substring(0,keypairs[i].indexOf('='));
        keyValue = keypairs[i].substring((keypairs[i].indexOf('=') + 1);
        while (keyValue.indexOf('+') > -1) {
            keyValue = keyValue.substring(0,keyValue.indexOf('+')) + ' ' +
keyValue.substring(keyValue.indexOf('+') + 1);
        }
        keyValue = unescape(keyValue);
        // Unescape non-alphanumerics
        KEY_VALUES[keyName] = keyValue;
    }
}

function getClientPort(serverPort) {
    var keyName = "clientPort['" + serverPort + "']";
    return KEY_VALUES[keyName];
}

function generateContent() {
    retrieveKeyValues();
    var newContent =
        "<html>\n"
        + "<head></head>\n"
        + "<body>\n"
        + "<applet code=\"com.citrix.JICA.class\" archive=\"JICAEngN.jar\" width=800
height=600>\n"
        + "<param name=\"cabbase\" value=\"JICAEngM.cab\">\n"

```

```

+ "<param name=\"address\" value=\"localhost\">\n"
+ "<param name=ICAPortNumber value="
+ getClientPort('1494')
+ ">\n"
+ "</applet>\n"
+ "</body>\n"
+ "</html>\n";
    document.write(newContent);
}
</script>
<body onLoad="generateContent();">
</body>
</html>

```

Deprecated HTML File:

```

<html>
<body>
<applet code="com.citrix.JICA.class" archive="JICAEngN.jar" width=800 height=600>
<param name="cabbage" value="JICAEngM.cab">
<param name="address" value="localhost">
<param name=ICAPortNumber value=1494>
</applet>
</body></html>

```


Netlet With PDC

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

NOTE Only Virtual Machines (VMs) with JSSE support Netlet with PDC.

Configuring Netlet for PDC

► **To Configure Netlet for PDC**

1. Export the client certificate from the browser in one of the following formats:
 - PKCS
 - JKS

After exporting the client certificate, the Java Plugin should have the following JVM parameters that enable the VM to use the certificate:

```
javax.net.ssl.keyStoreType  
javax.net.ssl.keyStorePassword  
javax.net1.ssl.keyStore
```

2. Go to Control Panel and Launch Java Plugin.
3. Choose Advanced Tab, Java Runtime Environment.

4. Specify the Java Runtime Parameters. For example:

```
Djavax.net.ssl.keyStoreType=pkcs
```

```
Djavax.net.ssl.keyStorePassword=testing123
```

```
Djavax.net1.ssl.keyStore="C:\dir\test.cert"
```

5. Click Apply.

6. Close the Java plugin and restart the associated browsers.

Certificates

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

This chapter covers the following topics:

- Overview of SSL Certificates
- Certificate Files
- Certificate Trust Attributes
- CA Trust Attributes
- The certadmin Script
- Generating Self-Signed Certificates
- Installing SSL Certificates From the Certificate Authority
- Adding a Root CA Certificate
- Modifying the Trust Attributes of a Certificate
- Listing Root CA Certificates
- Listing All Certificates
- Deleting a Certificate
- Printing a Certificate

Overview of SSL Certificates

The Sun Java™ System Portal Server Secure Remote Access software provides certificate-based authentication for remote users. SRA uses Secure Sockets Layer (SSL) to enable secure communication. The SSL protocol enables secure communication between two machines.

A SSL certificate provides encryption and decryption capabilities using a public and private key pair.

The two types of certificates are:

- Self-signed certificates (also called root CA certificate)
- Certificates issued by Certificate Authority (CA)

By default, a self-signed certificate is generated and installed when you install the Gateway.

You can generate, obtain, or replace a certificate anytime after installation.

SRA also supports client authentication with Personal Digital Certificates (PDCs). PDCs are a mechanism to authenticate a user through SSL client authentication. With SSL client authentication, the SSL handshake ends at the Gateway. The Gateway extracts the user's PDC and passes it to the authenticated server. This server uses the PDC to authenticate the user. To configure PDCs along with Authentication Chaining, see "Using Authentication Chaining" on page 80.

SRA provides a tool named `certadmin` that you can use to manage the SSL certificates. See "The `certadmin` Script" on page 222.

NOTE Certificate pop up windows are common in SSL applications. Advise users to accept the warning and proceed.

Certificate Files

Certificate related files are located in `/etc/opt/SUNWps/cert/gateway-profile-name`. This directory contains 5 files by default.

Table 7-1 lists these files and their descriptions.

Table 7-1 Certificate Files

File Name	Type	Description
cert8.db, key3.db, secmod.db	Binary	Contains the data for certificates, keys, and cryptographic modules. Can be manipulated using the <code>certadmin</code> script. Have the same format as the database files used by the Sun Java System Web Server and are located in <code>portal-server-install-root/SUNWwbsvr/alias</code> . If necessary, these files can be shared between the Portal Server host and gateway components or the Gateway.
.jsspass	hidden text file	Contains the encrypted password for the SRA key database.
.nickname	hidden text file	Stores the names of the token and certificate that the Gateway needs to use in the format <code>token-name:certificate-name</code> . If you are using the default token (the token on the default internal software encryption module), omit the token name. In most cases, the <code>.nickname</code> file stores only the certificate name. As an administrator, you can modify the certificate name in this file. The certificate that you specify is now used by the Gateway.

Certificate Trust Attributes

The trust attributes of a certificate indicate the following information:

- Whether the certificate (in the case of client or server certificate) was issued by a Trusted CA.
- Whether the certificate (in the case of a root certificate) can be trusted as the issuer of a server or client certificate.

The three available trust categories for each certificate are expressed in this order: “SSL, email, object signing”. Only the first category is useful got the Gateway. In each category position, zero or more trust attribute codes are used.

The attribute codes for the categories are separated by commas, and the entire set of attributes is enclosed by quotation marks. For example, the self-signed certificate generated and installed during the Gateway installation is marked "u,u,u" which means the certificate is a server certificate (user certificate) and not a root CA certificate.

Table 7-2 lists the possible attribute values and the meaning of each value.

Table 7-2 Certificate Trust Attributes

Attribute	Description
p	Valid peer
P	Trusted peer (implies p)
c	Valid CA
T	Trusted CA to issue client certificates (implies c)
C	Trusted CA to issue server certificates (SSL only) (implies c)
u	Certificate can be used for authentication or signing
w	Send warning (use with other attributes to include a warning when the certificate is used in that context)

CA Trust Attributes

Most well-known public CAs are included in the certificate database. See “Modifying the Trust Attributes of a Certificate” on page 232 for information on modifying the trust attributes of a public CA.

Table 7-3 lists the most common Certificate Authorities with the trust attributes.

Table 7-3 Public Certificate Authorities

Certificate Authority Name	Trust Attribute
Verisign/RSA Secure Server CA	CPp,CPp,CPp
VeriSign Class 4 Primary CA	CPp,CPp,CPp
GTE CyberTrust Root CA	CPp,CPp,CPp
GTE CyberTrust Global Root	CPp,CPp,CPp
GTE CyberTrust Root 5	CPp,CPp,CPp
GTE CyberTrust Japan Root CA	CPp,CPp,CPp
GTE CyberTrust Japan Secure Server CA	CPp,CPp,CPp
Thawte Personal Basic CA	CPp,CPp,CPp
Thawte Personal Premium CA	CPp,CPp,CPp
Thawte Personal Freemail CA	CPp,CPp,CPp

Table 7-3 Public Certificate Authorities

Thawte Server CA	CPp,CPp,CPp
Thawte Premium Server CA	CPp,CPp,CPp
American Express CA	CPp,CPp,CPp
American Express Global CA	CPp,CPp,CPp
Equifax Premium CA	CPp,CPp,CPp
Equifax Secure CA	CPp,CPp,CPp
BelSign Object Publishing CA	CPp,CPp,CPp
BelSign Secure Server CA	CPp,CPp,CPp
TC TrustCenter, Germany, Class 0 CA	CPp,CPp,CPp
TC TrustCenter, Germany, Class 1 CA	CPp,CPp,CPp
TC TrustCenter, Germany, Class 2 CA	CPp,CPp,CPp
TC TrustCenter, Germany, Class 3 CA	CPp,CPp,CPp
TC TrustCenter, Germany, Class 4 CA	CPp,CPp,CPp
ABAecom (sub., Am. Bankers Assn.) Root CA	CPp,CPp,CPp
Digital Signature Trust Co. Global CA 1	CPp,CPp,CPp
Digital Signature Trust Co. Global CA 3	CPp,CPp,CPp
Digital Signature Trust Co. Global CA 2	CPp,CPp,CPp
Digital Signature Trust Co. Global CA 4	CPp,CPp,CPp
Deutsche Telekom AG Root CA	CPp,CPp,CPp
Verisign Class 1 Public Primary Certification Authority	CPp,CPp,CPp
Verisign Class 2 Public Primary Certification Authority	CPp,CPp,CPp
Verisign Class 3 Public Primary Certification Authority	CPp,CPp,CPp
Verisign Class 1 Public Primary Certification Authority - G2	CPp,CPp,CPp
Verisign Class 2 Public Primary Certification Authority - G2	CPp,CPp,CPp
Verisign Class 3 Public Primary Certification Authority - G2	CPp,CPp,CPp

Table 7-3 Public Certificate Authorities

Verisign Class 4 Public Primary Certification Authority - G2	CPp,CPp,CPp
GlobalSign Root CA	CPp,CPp,CPp
GlobalSign Partners CA	CPp,CPp,CPp
GlobalSign Primary Class 1 CA	CPp,CPp,CPp
GlobalSign Primary Class 2 CA	CPp,CPp,CPp
GlobalSign Primary Class 3 CA	CPp,CPp,CPp
ValiCert Class 1 VA	CPp,CPp,CPp
ValiCert Class 2 VA	CPp,CPp,CPp
ValiCert Class 3 VA	CPp,CPp,CPp
Thawte Universal CA Root	CPp,CPp,CPp
Verisign Class 1 Public Primary Certification Authority - G3	CPp,CPp,CPp
Verisign Class 2 Public Primary Certification Authority - G3	CPp,CPp,CPp
Verisign Class 3 Public Primary Certification Authority - G3	CPp,CPp,CPp
Verisign Class 4 Public Primary Certification Authority - G3	CPp,CPp,CPp
Entrust.net Secure Server CA	CPp,CPp,CPp
Entrust.net Secure Personal CA	CPp,CPp,CPp
Entrust.net Premium 2048 Secure Server CA	CPp,CPp,CPp
ValiCert OCSP Responder	CPp,CPp,CPp
Baltimore CyberTrust Code Signing Root	CPp,CPp,CPp
Baltimore CyberTrust Root	CPp,CPp,CPp
Baltimore CyberTrust Mobile Commerce Root	CPp,CPp,CPp
Equifax Secure Global eBusiness CA	CPp,CPp,CPp
Equifax Secure eBusiness CA 1	CPp,CPp,CPp
Equifax Secure eBusiness CA 2	CPp,CPp,CPp
Visa International Global Root 1	CPp,CPp,CPp

Table 7-3 Public Certificate Authorities

Visa International Global Root 2	CPp,CPp,CPp
Visa International Global Root 3	CPp,CPp,CPp
Visa International Global Root 4	CPp,CPp,CPp
Visa International Global Root 5	CPp,CPp,CPp
beTRUSTed Root CA	CPp,CPp,CPp
Xcert Root CA	CPp,CPp,CPp
Xcert Root CA 1024	CPp,CPp,CPp
Xcert Root CA v1	CPp,CPp,CPp
Xcert Root CA v1 1024	CPp,CPp,CPp
Xcert EZ	CPp,CPp,CPp
CertEngine CA	CPp,CPp,CPp
BankEngine CA	CPp,CPp,CPp
FortEngine CA	CPp,CPp,CPp
MailEngine CA	CPp,CPp,CPp
TraderEngine CA	CPp,CPp,CPp
USPS Root	CPp,CPp,CPp
USPS Production 1	CPp,CPp,CPp
AddTrust Non-Validated Services Root	CPp,CPp,CPp
AddTrust External Root	CPp,CPp,CPp
AddTrust Public Services Root	CPp,CPp,CPp
AddTrust Qualified Certificates Root	CPp,CPp,CPp
Verisign Class 1 Public Primary OCSP Responder	CPp,CPp,CPp
Verisign Class 2 Public Primary OCSP Responder	CPp,CPp,CPp
Verisign Class 3 Public Primary OCSP Responder	CPp,CPp,CPp
Verisign Secure Server OCSP Responder	CPp,CPp,CPp
Verisign Time Stamping Authority CA	CPp,CPp,CPp
Thawte Time Stamping CA	CPp,CPp,CPp
E-Certify CA	CPp,CPp,CPp

Table 7-3 Public Certificate Authorities

E-Certify RA	CPp,CPp,CPp
Entrust.net Global Secure Server CA	CPp,CPp,CPp
Entrust.net Global Secure Personal CA	CPp,CPp,CPp

The certadmin Script

You can use the `certadmin` script to do the following certificate administration tasks:

- Generating Self-Signed Certificates
- Generating a Certificate Signing Request (CSR)
- Adding a Root CA Certificate
- Installing a Certificate from a CA
- Deleting a Certificate
- Modifying the Trust Attributes of a Certificate
- Listing Root CA Certificates
- Listing All Certificates
- Printing a Certificate

Generating Self-Signed Certificates

You need to generate certificates for SSL communication between each server and Gateway.

► To Generate a Self-Signed Certificate After Installation

1. As root, run the `certadmin` script on the Gateway machine for which you want to generate a certificate:

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

The certificate administration menu is displayed.


```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate From Certificate Authority (CA)
5) Delete Certificate
6) Modify Trust Attributes of Certificate (e.g., for PDC)
7) List Root CA Certificates
8) List All Certificates
9) Print Certificate Content
10) Quit
choice: [10] 1
```

2. Choose option 1 on the certificate administration menu.

The certificate administration script asks you if you want to keep the existing database files.

3. Enter organization-specific information, token name, and the certificate name.

NOTE For a wild card certificate, specify a * in the fully-qualified DNS name of the host. For example, if the fully-qualified DNS name of the host is `abc.sesta.com`, specify it as `*.sesta.com`. The certificate that is generated is now valid for all host names in the `sesta.com` domain.

```
What is the fully-qualified DNS name of this host? [host_name.domain_name]

What is the name of your organization (ex: Company)? []

What is the name of your organizational unit (ex: division)? []

What is the name of your City or Locality? []

What is the name (no abbreviation please) of your State or Province? []

What is the two-letter country code for this unit? []

Token name is needed only if you are not using the default internal
(software) cryptographic module, for example, if you want to use a crypto
card (Token names could be listed using: modutil -dbdir
/etc/opt/SUNWps/cert/gateway-profile-name -list); Otherwise, just hit Return
below.

Please enter the token name. []

Enter the name you like for this certificate?

Enter the validity period for the certificate (months) [6]
A self-signed certificate is generated and the prompt returns.
```

The token name (default being empty) and certificate name are stored in the `.nickname` file under `/etc/opt/SUNWps/cert/gateway-profile-name`.

4. Restart the Gateway for the certificate to take effect:

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

Generating a Certificate Signing Request (CSR)

Before you can order a certificate from a CA, you need to generate a certificate signing request which contains the information that is required by the CA.

► **To Generate a CSR**

1. As root, run the `certadmin` script:

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

The certificate administration menu is displayed.

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate From Certificate Authority (CA)
5) Delete Certificate
6) Modify Trust Attributes of Certificate (e.g., for PDC)
7) List Root CA Certificates
8) List All Certificates
9) Print Certificate Content
10) Quit

choice: [10] 2
```

2. Choose option **2** on the certificate administration menu.

The script prompts you for organization-specific information, token name, and web master's email and phone number.

Ensure that you specify the fully-qualified DNS name of the host.

```
What is the fully-qualified DNS name of this host? [snape.sesta.com]

What is the name of your organization (ex: Company)? []

What is the name of your organizational unit (ex: division)? []

What is the name of your City or Locality? []

What is the name (no abbreviation please) of your State or Province? []

What is the two-letter country code for this unit? []

Token name is needed only if you are not using the default internal
(software) cryptographic module, for example, if you want to use a crypto
card (Token names could be listed using: modutil -dbdir /etc/opt/SUNWps/cert
-list); Otherwise, just hit Return below.

Please enter the token name []

Now input some contact information for the webmaster of the machine that the
certificate is to be generated for.

What is the email address of the admin/webmaster for this server [] ?

What is the phone number of the admin/webmaster for this server [] ?
```

3. Type all the required information.

NOTE Do not leave the web master's email and phone number blank. The information is necessary for obtaining a valid CSR.

A CSR is generated and stored in the file `portal-server-install-root/SUNWps/bin/csr.hostname.datetimestamp`. The CSR is also printed on the screen. You can directly copy and paste the CSR when you order a certificate from a CA.

Adding a Root CA Certificate

If a client site presents a certificate signed by a CA that is unknown to the Gateway certificate database, the SSL handshake fails.

To prevent this, you need to add a root CA certificate to the certificate database. This ensures that the CA becomes known to the Gateway.

Browse to the CA's website and obtain the root certificate for that CA. When you use the `certadmin` script, specify the file name and path of the root CA certificate.

► To Add a Root CA Certificate

1. As root, run the `certadmin` script.

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

The certificate administration menu is displayed.

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate From Certificate Authority (CA)
5) Delete Certificate
6) Modify Trust Attributes of Certificate (e.g., for PDC)
7) List Root CA Certificates
8) List All Certificates
9) Print Certificate Content
10) Quit

choice: [10] 3
```

2. Choose option 3 on the certificate administration menu.
3. Enter the name of the file that contains the root certificate and enter the name of the certificate.

The root CA certificate is added to the certificate database.

Installing SSL Certificates From the Certificate Authority

During the installation of the Gateway, a self-signed certificate is created and installed by default. At any point after installation, you can install SSL certificates signed by vendors who provide official certificate authority (CA) services, or by your corporate CA.

The three steps involved in this task are:

- Generating a Certificate Signing Request (CSR)
- Ordering a Certificate from a CA
- Installing a Certificate from a CA

Ordering a Certificate from a CA

After generating a certificate signing request (CSR), you need to order the certificate from the CA using a CSR.

► **To Order a Certificate From a CA**

1. Go to the Certificate Authority's web site and order your certificate.
2. Provide the CSR as requested by the CA. Provide other information if requested by the CA.

You will receive your certificate from the CA. Save it in a file. Include the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines with the certificate in the file.

The following example omits the actual certificate data.

```

-----BEGIN CERTIFICATE-----

The certificate contents...

-----END CERTIFICATE-----

```

Installing a Certificate from a CA

Using the `certadmin` script, install the certificate obtained from the CA in your local database files in `/etc/opt/SUNWps/cert/gateway-profile-name`.

► To Install a Certificate From a CA

1. As root, run the `certadmin` script.

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

The certificate administration menu is displayed.

```

1) Generate Self-Signed Certificate

2) Generate Certificate Signing Request (CSR)

3) Add Root CA Certificate

4) Install Certificate From Certificate Authority (CA)

5) Delete Certificate

6) Modify Trust Attributes of Certificate (e.g., for PDC)

7) List Root CA Certificates

8) List All Certificates

```

```
9) Print Certificate Content
```

```
10)Quit
```

```
choice: [10] 4
```

2. Choose option 4 on the certificate administration menu.

The script asks you to enter the certificate file name, certificate name, and the token name.

```
What is the name (including path) of file that contains the certificate?  
Please enter the token name you used when creating CSR for this certificate.  
[]
```

3. Supply all the required information.

The certificate is installed in `/etc/opt/SUNWps/cert/gateway-profile-name`, and the screen prompt returns.

4. Restart the Gateway for the certificate to take effect:

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

Deleting a Certificate

You can delete a certificate by using the certificate administration script.

► To Delete a Certificate

1. As root, run the `certadmin` script.


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

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

The certificate administration menu is displayed.

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate From Certificate Authority (CA)
5) Delete Certificate
6) Modify Trust Attributes of Certificate (e.g., for PDC)
7) List Root CA Certificates
8) List All Certificates
9) Print Certificate Content
10)Quit
choice: [10] 5
```

2. Choose option 5 on the certificate administration menu.
3. Enter the name of the certificate to be deleted.

Modifying the Trust Attributes of a Certificate

One case in which the trust attributes of a certificate needs to be modified is if client authentication is used with the Gateway. An example of client authentication is PDC (Personal Digital Certificate). The CA that issues the PDCs must be trusted by the Gateway, and the CA certificate must be marked "T" for SSL.

If the Gateway is set up to communicate with an HTTPS site, the CA of the HTTPS site server certificate must be trusted by the Gateway, and the CA certificate must be marked "C" for SSL.

► To Modify the Trust Attributes for a Certificate

1. As root, run the certadmin script.

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

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

The certificate administration menu is displayed.

- 1) Generate Self-Signed Certificate
- 2) Generate Certificate Signing Request (CSR)
- 3) Add Root CA Certificate
- 4) Install Certificate From Certificate Authority (CA)
- 5) Delete Certificate
- 6) Modify Trust Attributes of Certificate (e.g., for PDC)
- 7) List Root CA Certificates
- 8) List All Certificates

```
9) Print Certificate Content
```

```
10)Quit
```

```
choice: [10] 6
```

2. Choose option **6** on the certificate administration menu.
3. Enter the name of the certificate. For example, Thawte Personal Freemail C.

```
Please enter the name of the certificate?
Thawte Personal Freemail CA
```

4. Enter the trust attribute for the certificate.

```
Please enter the trust attribute you want the certificate to have [CT,CT,CT]
```

The certificate trust attribute will be changed.

Listing Root CA Certificates

You can view all root CA certificates by using the certificate administration script.

► To View the List of Root CAs

1. As root, run the `certadmin` script.

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

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

The certificate administration menu is displayed.

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate From Certificate Authority (CA)
5) Delete Certificate
6) Modify Trust Attributes of Certificate (e.g., for PDC)
7) List Root CA Certificates
8) List All Certificates
9) Print Certificate Content
10)Quit
choice: [10] 7
```

2. Choose option 7 on the certificate administration menu.

All root CA certificates are displayed.

Listing All Certificates

You can view all certificates and their corresponding trust attributes by using the certificate administration script.

► **To List All the Certificates**

1. As root, run the `certadmin` script.

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

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

The certificate administration menu is displayed.

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate From Certificate Authority (CA)
5) Delete Certificate
6) Modify Trust Attributes of Certificate (e.g., for PDC)
7) List Root CA Certificates
8) List All Certificates
9) Print Certificate Content
10)Quit
choice: [10] 8
```

2. Choose option 8 on the certificate administration menu.

All CA certificates are displayed.

Printing a Certificate

You can print a certificate by using the certificate administration script.

► To Print a Certificates

1. As root, run the `certadmin` script.

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

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

The certificate administration menu is displayed.

```
1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request (CSR)
3) Add Root CA Certificate
4) Install Certificate From Certificate Authority (CA)
5) Delete Certificate
6) Modify Trust Attributes of Certificate (e.g., for PDC)
7) List Root CA Certificates
8) List All Certificates
```

```
9) Print Certificate Content
```

```
10)Quit
```

```
choice: [10] 9
```

2. Choose option 9 on the certificate administration menu.
3. Enter the name of the certificate.

Configuring URL Access Control

This chapter describes how to allow or deny access to the end user from the Sun Java™ System Access Manager administration console.

NOTE Click Documentation at the top right corner of the Access Manager administration console, and click SRA Help for a quick reference on all the Sun Java System Portal Server Secure Remote Access (SRA) attributes.

► **To Configure URL Access Control**

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab from the administration console.
3. Click the arrow next to Access List under SRA Configuration.

The Access List page is displayed.

From here you can perform the following tasks:

- Set up a Denied URLs List
- Set up a Allowed URLs List
- Manage Single Sign-On

NOTE When you install SRA, the Access List service is not available to all users by default. This service is enabled only to the `amadmin` user that is created by default during installation. Other users cannot access the desktop through the Gateway without this service. Log in as `amadmin`, and assign this service to all the users.

Set up a Denied URLs List

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

The Gateway checks the Denied URLs list before checking the Allowed URLs list.

► To Set up the Denied URL List

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Access List under SRA Configuration.

The Access List page is displayed.

4. Specify the URL for which you want to deny access through the Gateway in the Denied URL field. The format for entering the URL is:

```
http://abc.siroe.com
```

5. Click Add.

The URL is added to the Denied URL List.

You can also use regular expressions such as `http://*.siroe.com`. In this case, users are denied access to all hosts in the `siroe.com` domain.

6. Click Save to record the changes.

Set up a Allowed URLs List

You can specify all the URLs that can be accessed by the end user through the Gateway. By default, this list has a wild card entry (*), which means that all URLs can be accessed. If you want to allow access to all URLs, and restrict access only to specific URLs, add the restricted URLs to the Denied URL list. In the same way, if you want to allow access only to specific URLs, leave the Denied URLs field blank, and specify the required URLs in the Allowed URLs field.

The Gateway checks the Denied URLs before checking the Allowed URLs.

► To Set up the Allowed URLs List

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.

3. Click the arrow next to Access List under SRA Configuration.

The Access List page is displayed.

4. Specify the URL for which you want to allow access through the Gateway in the Allowed URLs field. The format for entering the URL is:

`http://abc.siroe.com`

5. Click Add.

The URL is added to the Allow URLs.

NOTE The Allowed URLs field has a * by default which means that all URLs can be accessed through the Gateway.

6. Click Save to record the changes.

Manage Single Sign-On

The Access List service in SRA software allows you to control the single sign-on feature for various hosts. For the single sign-on feature to be available, the Enable HTTP Basic Authentication option in the Gateway service must be enabled. See “Enable HTTP and HTTPS Connections” on page 245.

With the Access List service, you can disable single sign-on for certain hosts. This means that an end user needs to authenticate each time to connect to the hosts that require HTTP basic authentication, unless you enable single sign-on per session.

If you have disabled single sign-on for a certain host, the user can reconnect to that host within a single Portal Server session. For example, assume that you have disabled single sign-on to `abc.sesta.com`. The first time the user connects to this site, authentication is required. The user may browse other pages and return to this page later, and if the page is in the same Portal Server session, authentication is not required.

A user can also configure these attributes using the limited administration console.

► To Disable Single Sign On for Hosts

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.

3. Click the arrow next to Access List under SRA Configuration.
The Access List page is displayed.
4. Specify the hosts for which you want to disable SSO in the SSO Disabled Hosts field.
Specify the host name in the format `abc.siroe.com`.
5. Click Add.
The hostname is added to the list.
6. Click Save to record the changes.

➤ **To Enable Single Sign On per Session**

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Access List under SRA Configuration.
The Access List page is displayed.
4. Select the Enable Single Sign On per Session checkbox to enable a single-sign on session.
5. Click Save to record the changes.

➤ **To Specify Authentication Levels**

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Access List under SRA Configuration.
The Access List page is displayed.
4. Scroll to the Allowed Authentication Levels field.
5. Enter the allowed authentication levels. Use an asterisk to allow all levels.
6. Click Save to record the changes.

Configuring the Gateway

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

NOTE Click Help at the top right corner of the Access Manager administration console, and click SRA Help for a quick reference on all the Sun Java System Portal Server Secure Remote Access (SRA) attributes.

To create an instance of a gateway, see “Creating Instances of a Gateway” on page 48.

To create a gateway profile, see “Creating a Gateway Profile” on page 40

After you have created the gateway profile, you need to configure the Gateway attributes.

➤ **To Configure the Gateway Attributes**

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

The Gateway page is displayed.

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

The Edit Gateway Profile page is displayed.

From here, click the appropriate tab:

- The Core Tab

- The Proxies Tab
- The Security Tab
- The Rewriter Tab
- The Logging Tab

The tabs and the attributes that can be configured under each tab are listed below.

The Core Tab

Using the Core tab, in the Gateway service, you can perform the following tasks:

- Enable HTTP and HTTPS Connections
- Enable and Create a List of Rewriter Proxies
- Enable Netlet
- Enable and Create a List of Netlet Proxies
- Enable Proxylet
- Enable Cookie Management
- Enable HTTP Basic Authentication
- Enable Persistent HTTP Connections
- Specify the Maximum Number of Requests per Persistent Connection
- Specify Timeout for Persistent Socket Connections
- Specify Grace Timeout to Account for Turnaround Time
- Create List of URLs for Cookie Forwarding
- Specify the Maximum Connection Queue Length
- Specify the Gateway Timeout
- Specify the Maximum Thread Pool Size
- Specify the Cached Socket Timeout
- Create List of Portal Servers
- Specify Server Retry Interval
- Enable Storage of External Server Cookies

- Obtain a Session from a URL
- Set Minimum Gateway Authentication Level
- Enable Marking Cookies as Secure

Enable HTTP and HTTPS Connections

The Gateway runs in HTTPS mode after installation if you have chosen to run the Gateway in the HTTPS mode during installation. In the HTTPS mode, the Gateway accepts SSL connections from browsers and rejects non-SSL connections.

However, you can also configure the Gateway to run in HTTP mode. This speeds Gateway performance as the overhead involved in managing SSL sessions and encrypting and decrypting the SSL traffic are not involved.

► To Configure the Gateway to Run in HTTP or HTTPS Mode

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

The Gateway page is displayed.

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

The Edit Gateway Profile page is displayed.

5. Do the following under the Core tab.
 - Select the Enable HTTP Connections, Enable HTTPS Connections, or both checkboxes as required.
 - Specify the required HTTPS port in the HTTPS Port field.
 - Specify the required HTTP port in the HTTP Port field.
6. Click Save to record the change.
7. Restart the Gateway from a terminal window:

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

Enable and Create a List of Rewriter Proxies

The Rewriter proxy enables secure HTTP traffic between the Gateway and intranet computers. If you do not specify a Rewriter proxy, the Gateway component makes a direct connection to intranet computers when a user tries to access one of those intranet computers.

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

► **To Enable Rewriter Proxies and Create a List of Rewriter Proxies**

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.

NOTE Ensure that the Rewriter proxy and the Gateway use the same gateway profile.

The Edit Gateway Profile page is displayed.

5. Click the Core tab.
6. Select the Enable the Rewriter Proxies checkbox to enable the Rewriter proxy.
7. Type the desired host and port in the Rewriter Proxies edit box, in the format `hostname:port`.

TIP To determine if the port desired is available and unused, from the command line, enter:

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

port-number is the required port.

8. Click Add.

9. Click Save to record the change.
10. Run `portal-server-install-root/SUNWps/bin/certadmin` on the server to create a certificate for the Rewriter proxy.
 You need to do this step only if you have not chosen to create a certificate while installing the Rewriter proxy.
11. Log in as root to the machine where the Rewriter proxy is installed and start the Rewriter proxy:

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

12. Log in as root to the machine where the Gateway is installed and restart the Gateway:

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

Enable Netlet

Netlet enables users to securely run common TCP/IP services over insecure networks such as the Internet. You can run TCP/IP applications (such as Telnet and SMTP), HTTP applications, and any fixed port applications.

If Netlet is enabled, the Gateway needs to determine whether the incoming traffic is Netlet traffic or Portal Server traffic. Disabling Netlet reduces this overhead since the Gateway assumes that all incoming traffic is either HTTP or HTTPS traffic. Disable Netlet only if you are sure you do not want to use any application with Portal Server.

► To Enable Netlet

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
 The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.
 The Edit Gateway Profile page is displayed.
5. Click the Core tab.
6. Select the Enable Netlet checkbox. This checkbox is selected by default. Removing the selection disables Netlet.

7. Select the Enable the Netlet Proxy checkbox to enable the Netlet proxy.
8. Type the desired host and port in the Netlet Proxy List edit box, in the format `hostname:port`.
9. Click Save to record the change.
10. Restart the Gateway from a terminal window:

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

Enable and Create a List of Netlet Proxies

The Netlet proxy enhances the security of Netlet traffic between the Gateway and the intranet by extending the secure tunnel from the client, through the Gateway to the Netlet proxy that resides in the intranet.

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

► To Enable Netlet Proxies and Create a List of Netlet Proxies

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the right arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Select the Enable Netlet Proxy checkbox to enable the Netlet proxy.
6. Type the desired Netlet proxy host and port in the Netlet Proxy Hosts field, in the format `hostname:port`.

TIP To determine if the port desired is available and unused, from the command line, enter:

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

port-number is the required port.

7. Click Add.
8. Click Save to save the changes.
9. Restart the Gateway from a terminal window:

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

Enable Proxylet

► To Enable Proxylet

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the right arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Core tab.
6. Select the Enable Proxylet checkbox.
7. Click the Proxies tab. Scroll down to the Proxies for Domains and Subdomains field and enter the domains for URLs that are to be directed to the Gateway.
8. Click Save.

Enable Cookie Management

Many web sites use cookies to track and manage user sessions. When the Gateway routes requests to web sites that set cookies in the HTTP header, the Gateway either discards or passes-through those cookies in the following manner:

- Cookies are not rewritten if Enable Cookie Management attribute is not selected in the Gateway service. So, the cookies from the browser might not reach the intranet hosts and vice-versa.
- Gateway rewrites cookies if the Enable Cookie Management attribute is selected. Gateway ensures that the cookies from the browser reach the intended intranet hosts and vice-versa.

This setting does not apply to the cookies used by Portal Server to track Portal Server user sessions. The setting is controlled by the configuration of the URLs to which User Session Cookie is Forwarded URL option. See “Create List of URLs for Cookie Forwarding” on page 254.

This setting applies to all web sites that the user is permitted to access (that is, you cannot choose to discard cookies from some sites and retain cookies from others).

NOTE Do not remove URLs from the Cookie Domain list, even in a Gateway without cookies. See the *Access Manager Administration Guide* for information on the Cookie Domain list.

➤ **To Enable Cookie Management**

1. Log in to the Access Manager administration console as administrator.
1. Select the Service Configuration tab.
2. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
3. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
4. Click the Core tab.
5. Select the Enable Cookie Management checkbox to enable cookie management.
6. Click Save to record the change.
7. Restart the Gateway from a terminal window:

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

Enable HTTP Basic Authentication

HTTP basic authentication can be set in the Gateway service.

Web sites may be protected with HTTP Basic Authentication, requiring visitors to enter a username and password before viewing the site (the HTTP response code is 401 and WWW-authenticate: BASIC). Portal Server can save the username and password so that users need not re-enter their credentials when they revisit BASIC-protected web sites. These credentials are stored in the user profile on the directory server.

This setting does not determine whether or not a user may visit BASIC-protected sites, but only whether the credentials the user enters are saved in the user's profile.

This setting applies to all web sites that the user is permitted to access (that is, HTTP basic authentication caching cannot be enabled for some sites and disabled for others).

NOTE Browsing to URLs served by Microsoft's Internet Information Server (IIS) protected by Windows NT challenge/response (HTTP response code 401, WWW-Authenticate: NTLM) instead of BASIC authentication is not supported.

You can also enable single sign-on using the Access List service in the administration console. See "Manage Single Sign-On" on page 241 for more information on enabling single sign-on.

► **To Enable HTTP Basic Authentication**

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Core tab.
6. Select the Enable HTTP Basic Authentication checkbox to enable HTTP basic authentication.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Enable Persistent HTTP Connections

You can enable HTTP persistent connections at the Gateway to prevent sockets being opened for every object (such as images and style sheets) in the web pages.

► To Enable Persistent HTTP Connections

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

The Gateway page is displayed.

4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Core tab.
6. Select the Enable Persistent HTTP Connections checkbox to enable HTTP connections.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Specify the Maximum Number of Requests per Persistent Connection

► To Specify the Maximum Number of Requests per Persistent Connection

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

The Gateway page is displayed.

4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Core tab.

6. Scroll to the Maximum Number of Requests per Persistent Connection field and type the required number of requests.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Specify Timeout for Persistent Socket Connections

► To Specify the Timeout for a Persistent Socket Connection

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Core tab.
6. Scroll to Timeout for Persistent Socket Connections field and type the required timeout in seconds.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Specify Grace Timeout to Account for Turnaround Time

Grace timeout turnaround time is the sum of:

- Time taken for the request to reach the gateway after the browser has sent it
- Time between gateway sending the response and the browser actually receiving it

This is dependent on factors such as network conditions and the client's connection speed.

► **To Specify Timeout to Account for Turnaround Time**

This is the round trip time for the network traffic between the client (browser) and the Gateway.

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

The Gateway page is displayed.

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

The Edit Gateway Profile page is displayed.

5. Click the Core tab.
6. Scroll to the Grace Timeout to Account for Turnaround Time field and type the required grace timeout in seconds.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Create List of URLs for Cookie Forwarding

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 URLs to which User Session Cookie is Forwarded list. Adding URLs to this list therefore enables servlets and CGIs to receive the Portal Server's cookie and use the APIs to identify the user.

URLs are matched using an implicit trailing wildcard. For example, the default entry in the list:

```
http://server:8080
```


causes the cookie to be forwarded to all URLs starting with `http://server:8080`.

Adding:

```
http://newmachine.eng.siroe.com/subdir
```

causes the cookie to be forwarded to all URLs starting with that exact string.

For this example, the cookie is not forwarded to any URLs starting with `"http://newmachine.eng/subdir"`, since this string does not start with the exact string in the forward list. To have cookies forwarded to URLs starting with this variation of the machine's name, an additional entry has to be added to the forward list.

Similarly, the cookie is not forwarded to URLs starting with `"https://newmachine.eng.siroe.com/subdir"` unless an appropriate entry is added to the list.

► To Add a Forward Cookie URL

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Core tab.
6. Scroll to the URLs to which User Session Cookie is Forwarded edit box and type the required URL.
7. Click Add to add this entry to the URLs to which User Session Cookie is Forwarded list.
8. Click Save to record the change.
9. Restart the Gateway from a terminal window:

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

Specify the Maximum Connection Queue Length

You can specify the maximum concurrent connections that the Gateway needs to accept. Any connection attempts beyond this number are not accepted by the Gateway.

► To Specify the Maximum Connection Queue Length

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

The Gateway page is displayed.

4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Core tab.
6. Scroll to the Maximum Connection Queue Length field and specify the required number of connections.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Specify the Gateway Timeout

You can specify the time interval in seconds after which the Gateway times out its connection with the browser.

► To Specify the Gateway Timeout

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

The Gateway page is displayed.

4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.

5. Click the Core tab.
6. Scroll to the Gateway Timeout field and specify the interval required in seconds.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Specify the Maximum Thread Pool Size

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

► To Specify the Maximum Thread Pool Size

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Core tab.
6. Scroll to the Maximum Thread Pool Size field and specify the required number of threads.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Specify the Cached Socket Timeout

You can specify the time interval in seconds after which the Gateway times out its connection with the Portal Server.

► **To Specify the Cached Socket Timeout**

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Core tab.
6. Scroll to the Cached Socket Timeout field and specify the interval required in seconds.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Create List of Portal Servers

You can configure multiple Portal Servers for the Gateway to service requests. While installing the Gateway, you would have specified the Portal Server that the Gateway needs to work with. This Portal Server is listed in the Portal Servers field by default. You can add more Portal Servers to the list in the format `http://portal-server-name:port number`. The Gateway tries to contact each of the Portal Servers listed in a round robin manner to service the requests.

► **To Specify Portal Servers**

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Core tab.

6. Scroll to the Portal Server fields and specify the Portal Servers.

Specify the Portal Server in the format

`http://portal-server-name:port-number` in the edit field and click Add.

7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Specify Server Retry Interval

This attribute specifies the time interval between requests to try to start the Portal Server, Rewriter proxy or Netlet proxy if it becomes unavailable (such as a crash or it was brought down).

► To Specify Portal Server Retry Interval

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

The Gateway page is displayed.

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

The Edit Gateway Profile page is displayed.

5. Click the Core tab.
6. Scroll to the Portal Server Retry Interval field and specify the number of seconds.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Enable Storage of External Server Cookies

When the Store External Server Cookies option is enabled, the Gateway stores and manages cookies for any third party application or server that is accessed through the Gateway. Even if the application or server cannot service cookieless devices or depends on cookies for state management (for legacy reasons), the Gateway transparently masks the application or server from knowing that the Gateway is servicing a cookieless device. For information on cookieless devices and client detection, refer to the *Access Manager Customization and API Guide*.

► To Store External Server Cookies

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Core tab.
6. Select the Store External Server Cookies checkbox to enable storage of external server cookies.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Obtain a Session from a URL

When the Obtain Session from a URL option is selected, session information is encoded as part of the URL, whether cookies are supported or not. This means that the Gateway uses the session information found in the URL for validation rather than using the session cookie that is sent from the client's browser.

► To Obtain a Session from a URL

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.

3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Core tab.
6. Select the Obtain Session from URL checkbox to obtain a session from a URL.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Set Minimum Gateway Authentication Level

You can set the Authentication Level specifically for the Gateway here. For global authentication, see “To Specify Authentication Levels” on page 242.

► To Set Minimum Gateway Authentication Level

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Core tab.
6. Scroll to Minimum Gateway Authentication Level.
7. Enter the authentication level. Use an asterisk to allow all levels.
8. Click Save to record the change.
9. Restart the Gateway from a terminal window:

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

Enable Marking Cookies as Secure

When a cookie is marked as secure, the browser treats the cookie with additional security. The implementation of security depends on the browser. The Enable Cookie Management attribute must be enabled for this to work.

► To Mark Cookies as Secure

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Core tab.
6. Select the Mark Cookies as secure checkbox to mark cookies as secure.
Ensure that the Enable Cookie Management attribute is enabled.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

The Proxies Tab

Using the Proxies tab, in the Gateway service, you can perform the following tasks:

- Enable Usage of Web Proxies
- Create List of URLs for Webproxies
- Create List of URLs for Proxies Not to be Used
- Create List of Proxies for Domains and Subdomains
- Create List of Proxy Passwords
- Enable Automatic Proxy Configuration Support
- Specify Automatic Proxy Configuration File Location

- Enable Netlet Tunneling Through Web Proxy

Enable Usage of Web Proxies

► To Enable Usage of Web Proxies

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Proxies tab.
6. Select the Use Proxy checkbox to enable the usage of web proxies.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Create List of URLs for Webproxies

You can specify that the Gateway needs to contact certain URLs only through the webproxies listed in the Proxies for Domains and Subdomains list, even if the Use Proxy option is disabled. You need to specify these URLs in the Use Webproxy URLs field. See “Specifying a Proxy to Contact Access Manager” on page 58 for details on how this value affects the usage of proxies.

► To Specify URLs for Webproxies

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.

4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Proxies tab.
6. Type the required URL in the Use Webproxy URLs edit box in the format `http://host name.subdomain.com`. Click Add.
The URL is added to the Use Webproxy URLs list.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Create List of URLs for Proxies Not to be Used

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

► To Specify URLs Not To Be Used

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Proxies tab.
6. Type the required URL in the Do Not Use Webproxy URLs edit box and click Add.
The URL is added to the Do Not Use Webproxy URLs list.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Create List of Proxies for Domains and Subdomains

► To Specify Proxies for Domains and Subdomains

See “Specifying a Proxy to Contact Access Manager” on page 58 for details on how the proxy information is applied to various hosts.

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

The Gateway page is displayed.

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

The Edit Gateway Profile page is displayed.

5. Click the Proxies tab.

6. Scroll to the Proxies for Domains and Subdomains edit box and type the required information. Click Add.

The entry is added to the Proxies for Domains and Subdomains list box.

The format for entering the proxy information is as follows:

```
domainname proxy1:port1|subdomain1 proxy2:port2|subdomain2
proxy3:port3|* proxy4:port4
```

* indicates that the proxy defined after the * needs to be used for all domains and subdomains other than those specifically mentioned.

If you do not specify the port for the proxy, port 8080 is used by default.

7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Create List of Proxy Passwords

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

➤ **To Specify Proxy Passwords**

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

The Gateway page is displayed.

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

The Edit Gateway Profile page is displayed.

5. Click the Proxies tab.
6. Scroll to the Proxy Password List field and type the information for each proxy server and click Add.

The format for entering the proxy information is as follows:

```
proxyserver|username|password
```

The `proxyserver` corresponds to the proxy server defined in the Proxies for Domains and Subdomains list.

7. Repeat step 6 for all the proxies that require authentication.
8. Click Save to record the changes.
9. Restart the Gateway from a terminal window:

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

Enable Automatic Proxy Configuration Support

If you select the option Enable Automatic Proxy Configuration, the information provided in the Proxies for Domains and Subdomains field is ignored. The Gateway uses the Proxy Automatic Configuration (PAC) file only for intranet configuration. See “Using Automatic Proxy Configuration” on page 65 for information on PAC files.

➤ **To Enable Automatic Proxy Configuration Support**

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

The Gateway page is displayed.

4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Proxies tab.
6. Select the Enable Automatic Proxy Configuration Support checkbox to enable PAC support.
7. Click Save to record the changes.
8. Restart the Gateway from a terminal window:

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

Specify Automatic Proxy Configuration File Location

► To Specify Automatic Proxy Configuration File Location

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Proxies tab.
6. Scroll to the Automatic Proxy Configuration File location field and type the name and location of the PAC file.
7. Click Save to record the changes.
8. Restart the Gateway from a terminal window:

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

Enable Netlet Tunneling Through Web Proxy

► To Enable the Tunnel Netlet Through Web Proxy

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Proxies tab.
6. Select the Enable Netlet Tunneling via Web Proxy checkbox to enable tunneling.
7. Click Save to record the changes.
8. Restart the Gateway from a terminal window:

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

The Security Tab

Using the Security tab, in the Gateway service, you can perform the following tasks:

- Create List of Non-authenticated URLs
- Create List of Certificate-Enabled Gateway Hosts
- Allow 40-bit Encryption Connections
- Enable SSL Version 2.0
- Enable SSL Cipher Selection
- Enable SSL Version 3.0
- Enable Null Ciphers
- Create List of Trusted SSL Domains
- Configure Personal Digital Certificate (PDC) Authentication

- Enable Marking Cookies as Secure
- Enable HTTP and HTTPS Connections

Create List of Non-authenticated URLs

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

► To Specify Non-authenticated URL Paths

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

The Gateway page is displayed.

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

The Edit Gateway Profile page is displayed.

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

URLs that are not fully-qualified (for example, `/images`) are treated as portal URLs.

To add a non-portal URL, fully qualify the URL.

7. Click Add to add this entry to the Non-authenticated URLs list.
8. Click Save to record the change.
9. Restart the Gateway from a terminal window:

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

Create List of Certificate-Enabled Gateway Hosts

► To Add the Gateway to the Certificate-Enabled Gateway Hosts List

1. Log in to the Access Manager administration console as administrator.

2. Select the Service Configuration tab.
All the services are displayed in the left pane.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed in the right pane.
4. Select the gateway profile where you want to enable certificate based authentication.
5. Click the Security tab.
6. Add the Gateway name to the Certificate-enabled Gateway hosts.
Add the Gateway in the format `host1.sesta.com`.
7. Click Add.

Allow 40-bit Encryption Connections

Select this option if you want to allow 40-bit (weak) Secure Sockets Layer (SSL) connections. If you do not select this option, only 128-bit connections are supported.

If you disable this option, the user needs to ensure that the browser is configured to support the required connection type.

NOTE The user needs to do the following in the case of Netscape Navigator 4.7x:

- Select Security Info under Tools in the Communicator menu.
 - Click the Navigator link in the left pane.
 - Click Configure SSL v2 or Configure SSL v3 under Advanced Security (SSL) Configuration.
 - Enable the required ciphers.
-

► To Allow 40-bit Encryption Connections

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.

3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Security tab.
6. Select the Allow 40-bit Encryption checkbox to enable 40-bit browser connections.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Enable SSL Version 2.0

You can enable or disable SSL version 2.0. Disabling SSL 2.0 means that browsers that support only the older SSL 2.0 cannot authenticate to SRA. This ensures a greater level of security.

► To Enable SSL Version 2.0

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Security tab.
6. Select the Enable SSL Version 2.0 checkbox to enable version 2.0.
This option is enabled by default.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Enable SSL Cipher Selection

SRA supports a number of standard ciphers. You have the option of supporting all the pre-packaged ciphers, or selecting the required ciphers individually. You can select specific SSL ciphers for each Gateway instance. If any of the selected ciphers is present at the client site, the SSL handshake occurs successfully.

► To Enable Individual Cipher Selection

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

The Gateway page is displayed.

4. Select the gateway profile for which you want to set the attribute.
5. Click the Security tab.
6. Scroll to the Enable SSL Cipher Selection checkbox and select the option.

This option enables you to select the required ciphers from the list of SSL2, SSL3 and TLS ciphers.

7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Enable SSL Version 3.0

You can enable or disable SSL version 3.0. Disabling SSL 3.0 means that browsers that support only the SSL 3.0 cannot authenticate to SRA software. This ensures a greater level of security.

► To Enable SSL Version 3.0

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

The Gateway page is displayed.

4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Security tab.
6. Select the Enable SSL Version 3.0 checkbox to enable version 3.0.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Enable Null Ciphers

► To Enable Null Ciphers

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Security tab.
6. Select the Enable Null Ciphers checkbox to enable null ciphers.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Create List of Trusted SSL Domains

► To Create List of Trusted SSL Domains

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.

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

The Gateway page is displayed.

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

The Edit Gateway Profile page is displayed.

5. Click the Security tab.

6. Click the Security tab.

7. Scroll to the Trusted SSL Domains field, enter the domain names and click Add.

The format for the Trusted SSL Domains items should be one of the following:

- *fully-qualified-host-name* (For example, `siroe.india.sun.com`)
- **pattern* (For example, `*.india.sun.com`)
- *pattern** (For example, `siroe.india.*`)

This tells the Gateway to always accept certificates from hosts that match the specified pattern.

8. Click Save to record the change.

9. Restart the Gateway from a terminal window:

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

Configure Personal Digital Certificate (PDC) Authentication

PDCs are issued by a Certification Authority (CA) and signed with the CA's private key. The CA validates the identity of a requesting body before issuing a certificate. Thus the presence of a PDC is a powerful authentication mechanism.

PDCs contain the owner's public key, the owner's name, an expiration date, the name of the Certification Authority that issued the Digital Certificate, a serial number, and maybe some other information.

Users can use PDCs and encoded devices such as Smart Cards and Java Cards for authentication in the Portal Server. The encoded devices carry an electronic equivalent of a PDC stored on the card. If a user logs in using one of these mechanisms, no Log in screen displays and no authentication screen is displayed.

The PDC authentication process involves several steps:

1. From a browser, the user types a connection request, say `https://my.sesta.com`.

The response to this request depends on whether the Gateway to `my.sesta.com` has been configured to accept certificates.

NOTE When a Gateway is configured to accept certificates, it accepts only logins with certificates, not any other kind of login.

The Gateway checks that the certificate has been issued by a known Certificate Authority, has not expired, and has not been tampered with. If the certificate is valid, the Gateway lets the user proceed to the next step in the authentication process.

2. The Gateway passes the certificate to the PDC authentication module in the server.

► To Configure PDCs and Encoded Devices

The following steps are involved in configuring PDCs and encoded devices:

1. Add the following line in the `portal-server-install-root/SUNWam/config/AMConfig-instance-name.properties` file on the Portal Server machine:

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

(Add anywhere in the file)

2. Import the Required Certificates into the certificate database of the Gateway that you want PDC-enabled.

See the Chapter 7, “Certificates” for more information.

3. Register the certificate:
 - a. Log in to the Access Manager administration console as administrator.
 - b. Select the Identity Management tab.
 - c. Select your Organization.
 - d. Click Services from the View drop-down menu.
 - e. Click the arrow next to Core.

- f. Select Cert and LDAP in the Organization Authentication Modules list box LDAP.
 - g. Choose Dynamic from the User Profile drop-down menu.
 - h. Click Save.
4. Create Trusted Remote Host list.
 - a. Click the Service Configuration tab.
 - b. Click the arrow next to Certificate under Authentication Configuration.
 - c. Scroll to the Trusted Remote Hosts list box.
 - d. Highlight 'none' and click Remove.
 - e. Type 'any' in the text box
 - f. Click Add.
 - g. Click Save.
5. Create the new instance.
 - a. Click the Identity Management tab.
 - b. Select Services from the View drop-down menu.
 - c. Click the arrow next to the Authentication Configuration.
The Service Instance List is displayed.
 - d. Click New.
The New Service Instance page is displayed.
 - e. Enter the service instance name as gatewaypc.
Note: You must use this name.
 - f. Click Submit.
The gatewaypc Service Instance List is displayed.
 - g. Click gatewaypc to edit the service.
The gatewaypc show properties page is displayed.
 - h. Click Edit link next to Authentication Configuration in the right pane.
A popup window appears.

- i. Click Add.
The Authentication for Configuration *YourOrganization* page is displayed.
 - j. Click Add.
The Add Authentication Module page is displayed.
 - k. Choose Cert from the Module Name field and REQUIRED from the Enforcement Criteria field.
 - l. Click OK.
 - m. Click OK again and close the popup window.
6. Associate the certificate with the gateway host.
 - a. Select Service Configuration tab.
 - b. Click the arrow next to Gateway.
Gateway profiles are displayed in the right pane.
 - c. Select your gateway profile.
 - d. Click on security Tab.
 - e. Add the Gateway name to the Certificate-enabled Gateway hosts list box.
 - f. Click Save.
 - g. Restart the server.
 - h. Restart the Gateway from a terminal window:
gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start
 7. Install the client certificate issued from CA into the browser from where one has to access the PDC enabled gateway.
 8. Access your gateway profile and organization:
https://gateway:instance-port/YourOrganization
You should be logged in without any prompt for Username and Password with the name of the certificate.

The Rewriter Tab

Using the Rewriter tab, in the Gateway service, you can perform the following tasks:

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

Enable Rewriting of All URIs

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

► To Enable the Gateway to Rewrite All URIs

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Rewriter tab, Basic subsection.

6. Select the Enable Rewriting of All URIs checkbox to enable the Gateway to rewrite all URLs.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Create List of URIs to RuleSet Mappings

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

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

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

where `sun.com` is the install domain of the portal and `/portal` is the portal install context

- `*|generic_ruleset`

This means that for all pages from the default domain, the default Gateway ruleset is applied. For all other pages, the generic ruleset is applied. The default Gateway ruleset and the generic ruleset are pre-packaged rulesets.

NOTE For all the content appearing on the desktop, the ruleset for the default domain is used, irrespective of where the content is fetched from.

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

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

► **To Map a URI to RuleSet**

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

The Gateway page is displayed.

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

The Gateway - *gateway-profile-name* page is displayed.

5. Click the Rewriter tab, Basic subsection.
6. Scroll to the Map URIs to RuleSets field.

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

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

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

```
domain-name|ruleset-name
```

For example:

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

NOTE The order of priority for applying the ruleset is
hostname-subdomain-domain.

For example, assume that you have the following entries in the Domain-based rulesets list:

```
sesta.com|ruleset1
```

```
eng.sesta.com|ruleset2
```

```
host1.eng.sesta.com|ruleset3
```

ruleset3 is applied for all pages on host1.

ruleset2 is applied for all pages in the eng subdomain, except for pages retrieved from host1.

ruleset1 is applied for all pages in the sesta.com domain, except for pages retrieved from the eng subdomain, and from host1.

8. Click Save to record the change.
9. Restart the Gateway from a terminal window:

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

Ruleset for Outlook Web Access

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

► To Configure the OWA RuleSet

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

The Gateway page is displayed.

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

The Gateway - *gateway-profile-name* page is displayed.

5. In the Map URIs to RuleSets field, enter the server name where Exchange 2000 is installed followed by the exchange 2000 Service Pack 4 OWA ruleset.

For example:

```
exchange.domain.com|exchange_2000sp3_owa_ruleset.
```

Create List of MIME Types to Parse

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

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

For example:

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

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

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

► **To Specify MIME Mappings**

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

The Gateway page is displayed.

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

The Gateway - *gateway-profile-name* page is displayed.

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

Specify the entry in the format `HTML=text/html;text/htm`

7. Click Add to add the required entry to the list.
8. Click Save to record the change.
9. Restart the Gateway from a terminal window:

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

Create List of URIs Not to Rewrite

► **To Specify the URIs Not to Rewrite**

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

The Gateway page is displayed.

4. Click the gateway profile for which you want to set the attribute.
The Gateway - *gateway-profile-name* page is displayed.
5. Click the Rewriter tab, Basic subsection.
6. Scroll to the URIs Not to Rewrite field, and add the URI in the edit box.
Note: Adding *#** to this list allows URIs to be rewritten, even when the href rule is part of the ruleset.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Specify the Default Domains

The default domains 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 list, 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 Default Domains

1. Log in to the Access Manager administration console as administrator.
2. Click the Service Configuration tab.
3. Click the right arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Rewriter tab, Basic subsection.
6. Scroll to the Default Domains field and type the required default value in the format `subdomain.domain name`.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Enable MIME Guessing

Rewriter depends on the MIME type of the page to choose the parser. Some web servers such as WebLogic and Oracle do not send MIME types. To work around this, you can enable the MIME guessing feature by adding data to the Map Parser to URIs list box.

► To Enable MIME Guessing

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Click the gateway profile for which you want to set the attribute.
The Gateway - *gateway-profile-name* page is displayed.
5. Click the Rewriter tab, Advanced subsection.
6. Select the Enable MIME Guessing checkbox to enable MIME Guessing.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Create List of URI Mappings to Parse

If the MIME Guessing checkbox is enabled and the server has not sent a MIME type, use this list box to map the parser to the URI.

Multiple URIs are separated by a semicolon.

For example `HTML=*.html;*.htm;*Servlet`

means that the HTML Rewriter is used to rewrite the content for any page with a `html`, `htm`, or `Servlet` extension.

► To Parse URI Mappings

1. Log in to the Access Manager administration console as administrator.

2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Click the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Rewriter tab, Advanced subsection.
6. Scroll to the Parser to URI Mappings field, and add the data to the edit box.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Enable Masking

Masking allows Rewriter to rewrite a URI so that the intranet URL of a page is not seen.

► To Enable Masking

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Click the gateway profile for which you want to set the attribute.
The Gateway - *gateway-profile-name* page is displayed.
5. Click the Rewriter tab, Advanced subsection.
6. Select the Enable Masking checkbox to enable masking.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Specify the Masking Seed String

A seed string is used for masking a URI. A masking algorithm generates the string.

NOTE Book marking of an masked URI may not work if this seed string has been changed or if the Gateway is restarted.

► To Specify the Masking Seed String

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Click the gateway profile for which you want to set the attribute.
The Gateway - *gateway-profile-name* page is displayed.
5. Click the Rewriter tab, Advanced subsection.
6. Scroll to the Seed String for Masking field, and add a string to the edit box.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Create List of URIs Not to Mask

Some applications (such as an applet) require an Internet URI and cannot be masked. To specify those applications, add the URI to the list box.

For example if you added

```
*/Applet/Param*
```

to the list box, the URL would not be masked if the content URI `http://abc.com/Applet/Param1.html` is matched in the ruleset rule.

► To Specify Not to Mask URIs

1. Log in to the Access Manager administration console as administrator.

2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Click the gateway profile for which you want to set the attribute.
The Gateway - *gateway-profile-name* page is displayed.
5. Click the Rewriter tab, Advanced subsection
6. Scroll to the URIs Not to Mask list field, and add the URIs to the edit box.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

Make a Gateway Protocol the Same as the Original URI Protocol

When a Gateway runs in both HTTP and HTTPS mode, you can enable Rewriter to use a consistent protocol to access the referred resources in the HTML content.

For example, if the original URL is `http://intranet.com/Public.html` then the http Gateway is added. If the original URL is `https://intranet.com/Public.html` then the https Gateway is added.

NOTE This applies only to static URIs, not to dynamic URIs generated in Javascript.

► To Make a Gateway Protocol the Same as the Original URI Protocol

1. Log in to the Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Click the gateway profile for which you want to set the attribute.
The Gateway - *gateway-profile-name* page is displayed.
5. Click the Rewriter tab, Advanced subsection.

6. Select the Make Gateway protocol Same as Original URI Protocol checkbox.
7. Click Save to record the change.
8. Restart the Gateway from a terminal window:

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

The Logging Tab

Using the Logging tab, in the Gateway service, you can perform the following tasks:

- Enable Logging
- Enable Netlet Logging

Enable Logging

You can specify the Gateway log file to capture either minimum information or detailed information about each session. The log information is saved in the directory specified in the Log Location attribute as part of the Logging section of the Access Manager Configuration attributes. This log is located on the Portal Server machine.

The log name uses the following convention:

```
srapGateway_gatewayhostname_gateway-profile-name
```

The log information can be saved as a file or as a database as specified in the Access Manager 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 Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.

5. Click the Logging tab.
6. Select the Enable Logging checkbox to enable Gateway logging.

NOTE Log information is captured only if the Enable Logging field has already been enabled.

7. Select the Enable per Session Logging checkbox to capture minimum log information such as Client Address, Request Type, and Destination Host.
8. 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.

9. Click Save to record the changes.
10. Restart the Gateway from a terminal window:

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

Change the Log User Password

Use this procedure if you want to change the password frequently for security purposes or if you forget the log user password. This procedure will change the `gateway.logging.password` in the `platform.conf.profile` file.

► To Change the Log User Password

1. At the system prompt, enter:

```
psadmin change-loguser-password
```

2. Change the password in the directory server:

```
default org -> Agents and change the password for the amService-srapgateway
```

Enable Netlet Logging

You can enable logging for Netlet related activities by selecting this option. The Netlet log contains 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 Access Manager administration console as administrator.
2. Select the Service Configuration tab.
3. Click the arrow next to Gateway under SRA Configuration.
The Gateway page is displayed.
4. Select the gateway profile for which you want to set the attribute.
The Edit Gateway Profile page is displayed.
5. Click the Logging tab.
6. Select the Enable Netlet Logging checkbox to enable Netlet logging.
7. Click Save at the bottom of the page to record the changes.
8. Restart the Gateway from a terminal window:

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

Configuring NetFile

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

NOTE Click Help at the top right corner of the Access Manager administration console, and click SRA Help for a quick reference on all the SRA attributes.

► **To Set the NetFile Locale**

1. Log in to the Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Users from the View drop-down list.
4. Click the arrow next to the user name.
The User information page is displayed.
5. Scroll to the Preferred Locale field and select the desired locale.
6. In the field next to Preferred Locale, select Customize or Inherit.
7. Click Save to record the change.

► **To Configure NetFile Attributes**

1. Log in to the Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.

5. Select Services from the View list box.
6. Click the arrow next to NetFile under SRA Configuration.

From here, click the appropriate tab.

- The Hosts Tab
- The Permissions Tab
- The View Tab
- The Operations Tab
- The General Tab

The tabs and the attributes that can be configured under each are listed below.

The Hosts Tab

Using the Hosts Tab, in the NetFile service, you can perform the following tasks:

- Specify the OS Character Set
- Specify Host Detection Order
- Configure a Common Hosts List
- Specify the Default Domain
- Specify the Windows Domain/Workgroup
- Specify the Default WINS/DNS Server
- Specify Access to Different Types of Hosts
- Configure the Allowed Hosts List
- Configure the Denied Hosts List

Specify the OS Character Set

You can specify the character set used as the default encoding for communicating with hosts. The default value is `UTF-8`.

CAUTION If the character set is not specified correctly, the behavior of the machine and error messages that appear cannot be predicted.

► **To Specify the OS Character Set**

1. Log in to the Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View list box.
6. Click the arrow next to NetFile under SRA Configuration.
The NetFile page is displayed.
7. Click the Hosts tab, subsection Config.
8. Scroll to the OS Character Set field and select the character set code.
9. Click Save to record the change.

Specify Host Detection Order

► **To Specify the Host Detection Order**

1. Log in to the Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View list box.
6. Click the arrow next to NetFile under SRA Configuration.
The NetFile page is displayed.
7. Click the Hosts tab, subsection Config.
8. Scroll to the Hosts Detection Order field and select a host type.
9. Use the Move Up and Move Down buttons to change the host detection order.
10. Click Save to record the change.

Configure a Common Hosts List

You can configure a list of hosts to be available through NetFile to all remote NetFile users. You need to specify the following information for each host that you add:

Host Name—You can type either the host name or the fully qualified name. If the host name that you have provided matches the host name configured by the user, the two sets of information are merged and the user-specified values override the values that you specified.

For example, suppose you have configured 4 common hosts - *sesta*, *siroe*, *florizon*, and *abc*. A user configures 3 hosts out of which 2 are *sesta* and *siroe*. User-specified values override administrator-specified values in such conflict situations. *florizon* and *abc* are also listed in the user's NetFile, and the user can carry out various operations on those hosts. In case you have listed *florizon* in the Denied Hosts List, *florizon* is listed in the user's NetFile, but no operation can be carried out on *florizon*.

Host Type—If the user has already added a host that is listed in the Common Hosts list, the user setting takes precedence. If a conflict in the type exists, the shares added by the administrator are not added for that user. If the user and the administrator add the same share, the share is added, but the password set by the user takes precedence.

Encoding—If a conflict exists between the value specified here and the user setting, the user setting takes precedence. If you have specified a blank or invalid setting, the character set of the client OS (user's machine) is used.

NOTE The user can edit any of these values in the NetFile client application. But the edited values are valid only for the current session. If the user logs out and logs in again, the edited values are not retained.

► To Configure the Common Hosts List

1. Log in to the Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View list box.

6. Click the arrow next to NetFile under SRA Configuration.
The NetFile page is displayed.
7. Click the Hosts tab, subsection Config.
The NetFile page is displayed.
8. To add a common host:
 - a. Click New... under the Common Hosts field.
 - b. Enter the required information in the following fields:
 - Host Name
 - Host Type
 - Encoding
 - Microsoft Windows Domain/Workgroup
 - User Name
 - Password
 - c. For each share you want to add, enter the required information in the following fields and click Add to List:
 - Share List
 - Share Name
 - Share Password
 - d. Click OK.
 - e. Repeat this information set for each common host that you want to add or delete.
9. To delete a common host from the Common Hosts list:
 - a. Click Delete and select the Host Name in the Share List. Then click Remove.
 - b. Click Save to record the change.

Specify the Default Domain

You can specify the default domain that NetFile needs to use to contact allowed hosts.

This default domain value is applicable only if the user does not specify a fully qualified host name while adding a host using NetFile.

CAUTION Ensure that the Default Domain field is not blank, and that it contains a valid domain name.

► **To Specify the Default Domain**

1. Log in to the Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View list box.
6. Click the arrow next to NetFile under SRA Configuration.
The NetFile page is displayed.
7. Click the Hosts tab, subsection Config.
8. Scroll to the Default Domain field and type the default domain name.
9. Click Save to record the change.

Specify the Windows Domain/Workgroup

This is the default Microsoft Windows domain or workgroup which the users choose to access a Microsoft 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 Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.

5. Select Services from the View list box.
6. Click the arrow next to NetFile under SRA Configuration.
The NetFile page is displayed.
7. Click the Hosts tab, subsection Config.
8. Scroll to the Default Windows Domain/Workgroup field and type the default domain or workgroup name.
9. Click Save to record the change.

Specify the Default WINS/DNS Server

This is the WINS/DNS server NetFile uses to access Microsoft Windows' hosts.

► To Specify the Default WINS/DNS Server

1. Log in to the Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View list box.
6. Click the arrow next to NetFile under SRA Configuration.
The NetFile page is displayed.
7. Click the Hosts tab, subsection Config.
8. Scroll to the Default WINS/DNS Server field and type the default Microsoft Windows or DNS server name.
9. Click Save to record the change.

Specify Access to Different Types of Hosts

You can specify whether users can access specific hosts such as Microsoft 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 Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View list box.
6. Click the arrow next to NetFile under SRA Configuration.
The NetFile page is displayed.
7. Click the Hosts tab, subsection Access.
8. Click the host type to which access is enabled. You can choose to enable:
 - Allow Access to Microsoft Windows Hosts
 - Allow Access to FTP Hosts
 - Allow Access to NFS Hosts
 - Allow Access to Netware HostsSelecting the option enables users to access that particular type of host. Clearing the checkbox prevents users from accessing that type of host.
9. Click Save to record the change.

Configure the Allowed Hosts List

By default, users are allowed to access all the hosts through NetFile because of the * entry in this list. If you want to change that, remove the * entry and specify only those hosts to which users need to have access through NetFile, in this list. Alternatively, you can keep the * entry here, and specify the hosts to which you want to deny access in the Denied Hosts list. In that case, all the hosts except the ones specified in the Denied Hosts list are allowed access.

See “Configure the Denied Hosts List” on page 299 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 Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View list box.
6. Click the arrow next to NetFile under SRA Configuration.
The NetFile page is displayed.
7. Click the Hosts tab, subsection Access.
8. Scroll to the Allowed Hosts field. Type the names of the hosts to which you want to allow access in the edit field and click Add.
The host name is added to the Allowed Hosts list box.
9. Click Save to record the changes.

Configure the Denied Hosts List

After specifying the list of commonly available hosts under “Configure a Common Hosts List” on page 294, 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 continues to be displayed in the NetFile window of the user. But the user is not be able to carry out any operations on the host.

In NetFile Java2, denied hosts, if displayed in the application, are marked with a red cross to indicate that they are inaccessible.

NOTE If both the Allowed Hosts and Denied Hosts lists are blank, access is not allowed to any host.

► **To Create a Denied Hosts List**

1. Log in to the Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View list box.
6. Click the arrow next to NetFile under SRA Configuration.
The NetFile page is displayed.
7. Click the Hosts tab, subsection Access.
8. Scroll to the Denied Hosts field. Type the names of the hosts to which you want to deny access in the edit field.
9. Click Add.
The host name is added to the Denied Hosts list box.
10. Click Save to record the changes.

The Permissions Tab

Using the Permissions tab, in the NetFile service, you can allow or deny permission for users to perform the following tasks from remote hosts:

- Rename files
- Delete files and folders
- Upload files
- Download files and folders
- Search for a file
- Mail files
- Compress files
- Change User Id

This option lets you specify whether a user can use different IDs to connect to hosts using NetFile. In a large organization, users may have multiple user IDs. You may want to restrict users to use a single user ID. In that case, you can disable the Allow Changing User ID option. This prevents all the users in the specific organization from changing their user ID, and limits them to using a single ID (the desktop login ID) to connect to hosts using NetFile. In another situation, a user may have different login IDs on different machines, in which case, you may want to allow the user to change the ID as required.

- **Change Microsoft Windows Domains**

This option is applicable to NT domains.

If the user specifies an invalid domain name in the User NT Domain name field while adding a system, an error message is displayed. If the user edits the host information later, and specifies an invalid domain name, an error message does not appear.

If the user specifies a domain name, the username and password for that domain also needs to be specified. If the username and password for the host needs to be used, the user needs to remove the domain from the User NT Domain name field.

The permission options are enabled by default.

► **To Enable/Disable Permissions**

1. Log in to the Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View list box.
6. Click the arrow next to NetFile under SRA Configuration.

The NetFile page is displayed.

7. Click the Permissions tab.
8. Scroll to the required Allow field and click the checkbox to allow permission.
9. Click Save to record the change.

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

The View Tab

Using the View tab, in the NetFile service, you can perform the following tasks:

- Specify the NetFile Window Size
- Specify the NetFile Window Location

Specify the NetFile Window Size

You can specify the size of the NetFile window in pixels on the user's desktop. The default value is 700 | 400 in pixels. If you enter an invalid value, NetFile uses the default value.

NOTE The user can also edit this value in the limited administration console that is available to the user. The value that you specify is replaced with the new values if the user resizes the NetFile window on the desktop.

► To Specify the Size of the NetFile Window

1. Log in to the Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View list box.
6. Click the arrow next to NetFile under SRA Configuration.
The NetFile page is displayed.
7. Click the View tab.

8. Scroll to the Window Size field and type the required window size in pixels.
Type the value in the format 700|400 without any spaces. The coordinates are in the form x|y. No other character should be used as a separator.
9. Click Save to record the change.

Specify the NetFile Window Location

You can specify the location where the NetFile window displays on the user's desktop. The default value is 100|50 in pixels. If you enter an invalid value, NetFile uses the default value.

NOTE The user can also edit this value in the limited administration console that is available to the user. The value that you specify is replaced with the new values if the user relocates the NetFile window on the desktop.

► To Specify the Location of the NetFile Window

1. Log in to the Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View list box.
6. Click the arrow next to NetFile under SRA Configuration.
The NetFile page is displayed.
7. Click the View tab.
8. Scroll to the Window Location field and type the required window location coordinates.
Type the value in the format 100|50 without any spaces. The coordinates are in the form x|y. No other character should be used as a separator.
9. Click Save to record the change.

The Operations Tab

Using the Operations tab, in the NetFile service, you can perform the following tasks:

- Specify the Temporary Files Directory
- Set the File Upload Size Limit
- Specify the Search Directories Limit
- Specify Compression

Specify the Temporary Files Directory

NetFile needs a temporary directory for some file operations such as mailing files. The default temporary directory is `/tmp`. The temporary files are deleted after the required operation has been carried out.

The specified temporary directory is created if it does not exist on the server.

Ensure that the ID with which the web server is running (such as `nobody` or `noaccess`) has `rwX` permissions for the specified directory. Also ensure that the ID has `rx` permissions for the entire path to the required temporary directory.

TIP You may want to create a separate temporary directory for NetFile. If you specify a temporary directory that is common to all modules of the Portal Server, the disk may quickly run out of space. A few operations in NetFile, such as mailing files, do not work if the temporary directory has no space.

► To Specify a Temporary Directory

1. Log in to the Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Select Services from the View list box.
5. Click the arrow next to NetFile under SRA Configuration.

The NetFile page is displayed.

6. Click the Operations tab, Traffic subsection.

7. Scroll to the Temporary Directory Location field and type the required temporary directory location.
8. Click Save to record the change.

Set the File Upload Size Limit

You can specify the maximum size of the files that can be uploaded in this field. If the size of the file being uploaded exceeds the limit specified here, an error message is displayed and the file is not uploaded. The default value is 5 MB. If you enter an invalid value, NetFile resets the value to the default.

You can specify different file upload size limits for different users.

NOTE Specify the maximum file size for upload in megabytes. Ensure that you type an integer value.

► To Set the File Upload Size Limit

1. Log in to the Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View list box.
6. Click the arrow next to NetFile under SRA Configuration.
The NetFile page is displayed.
7. Click the Operations tab, Traffic subsection.
8. Scroll to the File Upload Limit field. Type the required size limit in mega bytes.
9. Click Save to record the change.

Specify the Search Directories Limit

You can configure the maximum number of directories that can be searched in a single search operation. This limit helps reduce network clogging and increases the speed of access if a number of users are logged in simultaneously. The default value is 100. If you type an invalid value, NetFile resets the value to the default.

Suppose a user has a directory called A. Assume that A has 100 subdirectories. If you specify the maximum directories to be searched as 100, the search operation goes through directory A and stops. The search does not proceed through the other directories in the user's machine since the limit of 100 was reached with directory A. The search results accumulated until the search limit is reached are displayed to the user along with an error message stating that the search exceeded its limit. To continue the search, the user must manually restart the search at the next directory.

The search operation is carried out in a depth-first manner. This means that the search operation is carried out in all the subdirectories of the directory that the user selected, before moving on to the next directory.

► To Specify the Search Directories Limit

1. Log in to the Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View list box.
6. Click the arrow next to NetFile under SRA Configuration.
The NetFile page is displayed.
7. Click the Operations tab, Search subsection.
8. Scroll to the Search Directories Limit field and type the required number.

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

9. Click Save to record the change.

Specify Compression

These compression attributes apply only to NetFile Java2.

► **To Specify the Default Compression Type**

1. Log in to the Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View list box.
6. Click the arrow next to NetFile under SRA Configuration.

The NetFile page is displayed.

7. Click the Operations tab, Compression subsection.
8. Scroll to the Default Compression Type field.
Choose Zip or GZip
9. Click Save to record the change.

The General Tab

Using the General tab, in the NetFile service, you can specify the MIME-types configuration file location.

Specify the MIME-types Configuration File Location

This information is required to determine the response content type to send to the client browser. The browser needs this information to determine the application that a file needs to be associated with during a NetFile open or download operation. This is configured during installation.

If the MIME-types file of the Portal Server's web server needs to be used, specify the location:

portal-server-install-root/SUNWam/servers/instance-name-of-web-server-machine/config

NOTE MIME-types Configuration File Location attribute can be set only at the organization level.

► **To Specify the Location of the MIME-types Configuration File**

1. Log in to the Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View list box.
6. Click the arrow next to NetFile under SRA Configuration.
The NetFile page is displayed.
7. Click the General tab.
8. Scroll to the MIME-types Configuration File Location field and type the full path to where the MIME-types configuration file is located.
9. Click Save to record the change.

Configuring Netlet

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

NOTE Click Help at the top right corner of the Access Manager administration console, and click SRA Help for a quick reference on all the SRA attributes.

All the attributes that can be configured at the organization level can also be configured at the user level. See the *Access Manager Administration Guide* for more information on organization, role and user level attributes.

To configure Netlet attributes, follow these steps to configure attributes at the organization level:

1. Log in to the Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View drop-down list.
6. Click the arrow next to Netlet under SRA Configuration.

From here, you can perform the following tasks:

- Add a Netlet Rule
- Assign Netlet Service to a User
- Add a Netlet Rule

- Modify an Existing Netlet Rule
- Delete a Netlet Rule

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

- Specify the Default Encryption Cipher
- Assign the Default Loopback Port
- Enable Reauthentication for Connections
- Display Warning Popup for Connections
- Enable the Display Checkbox in Port Warning Dialog
- Set the Keep Alive Interval
- Set the Terminate Netlet at Portal Logout Option
- Define Access to Netlet Rules
- Deny Access to Netlet Rules
- Allow Access to HostsDeny Access to Hosts

Assign Netlet Service to a User

1. Log in to the Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name.

The selected organization name is reflected as the location in the top left corner of the admin console.

5. Select Users from the View drop-down list for the selected organization.
6. Click the arrow next to the required user in the left pane.
7. Select Services from the View drop-down list for this user, if the Netlet service is not already available for this user
8. Click Add.

9. Select Netlet from the Available Services list.
10. Click Save
11. The Netlet attributes can be modified by selecting Netlet service from the View drop-down list for this user.

Add a Netlet Rule

You can add or create Netlet rules at a global level in the Identity Management tab of the Access Manager administration console. These rules are inherited by any new organization that you create.

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

► To Add a Netlet Rule

1. Log in to the Access Manager administration console as administrator.
2. Choose the Identity Management tab.
3. Choose the Organization for which you want to create the rule.
4. Select Services from the View drop-down list.
5. Click the arrow next to Netlet under SRA Configuration.

The Netlet page is displayed in the right pane.

6. Click Add in the Netlet Rules field.

The Add Netlet Rule page is displayed. All the fields of the rule are populated with sample values that you can change as required.

7. Type a unique name for the rule in the Rule Name field.
8. Specify the required ciphers. Select Default to retain the default encryption cipher. Select Other to choose from the list of available ciphers.

See “To Specify the Default Cipher” on page 314 for details on the default cipher.

9. Type the URL to the application to be invoked in the URL field.
10. Select the Download Applet checkbox if an applet needs to be downloaded. Type the applet details in the format *local-port:server-host:server-port* in the associated edit box.

NOTE Specify a unique local port for each rule.

You need to specify the applet details only if the applet needs to be downloaded from a host other than the Portal Server host. The edit box is disabled if you do not select the checkbox. For more information see “Downloading an Applet From a Remote Host” on page 191.

11. Select the Extend Session checkbox to ensure that the Portal Server session time is extended while the Netlet session corresponding to this rule is running.
12. Type the local port on which Netlet listens in the Local Port field.
For an FTP rule, the local port value must be 30021.
13. Type an entry in the Destination Host(s) field.
For a static rule, enter the host name of the target machine for the Netlet connection.
For a dynamic rule, enter "TARGET".
14. Type the port on the target host in the Target Port(s) field.
15. Click Add to List to reflect the last three entries in the Map Local Port to Destination Server Port fields.
16. Click OK.

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

Modify an Existing Netlet Rule

You can modify existing rules at the organization, role, or user levels from the Identity Management tab in the administration console. These rules are inherited by any new organization that you create.

► To Modify a Netlet Rule

1. Log in to the Access Manager administration console as administrator.
2. Choose the Identity Management tab.
3. Choose the Organization for which you want to modify the rule.
4. Select Services from the View drop-down list.

5. Click the arrow next to Netlet under SRA Configuration.
The Netlet page is displayed in the right pane.
6. Select the checkbox next to the rule that you want to modify.
The Edit Netlet Rule page is displayed.
7. Make changes as required and click Save.
The modified rule is saved and you are returned to the Netlet page.

Delete a Netlet Rule

You can delete Netlet rules at a global level in the Identity Management tab of the administration console.

► To Delete a Netlet Rule

1. Log in to the Access Manager administration console as administrator.
2. Choose the Identity Management tab.
3. Choose the Organization for which you want to delete the rule.
4. Click the arrow next to Netlet under SRA Configuration.
The Netlet page is displayed in the right pane.
5. Select the checkbox next to the rule that you want to delete from the Netlet Rules list.
6. Click Delete.
The selected rule is removed from the Netlet Rules list.

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

Specify the Default Encryption Cipher

You need to specify the default cipher for the Netlet rules. This is useful when using existing rules that did not include the cipher as a part of the rule. This is a mandatory field. See “Backward Compatibility” on page 197.

► **To Specify the Default Cipher**

1. Log in to the Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View drop-down list.
6. Click the arrow next to Netlet under SRA Configuration.

The Netlet page is displayed in the right pane.

7. Scroll to the Default Native VM Cipher or Default Java Plugin Cipher field and select the required cipher from the drop-down list. See “Supported Ciphers” on page 196 for a list of supported ciphers.
8. Click Save to record the change.

Assign the Default Loopback Port

This attribute specifies the port to be used on the local machine when applets are downloaded through Netlet. The default value of 58000 is used unless the value is overridden in the Netlet rules.

► **To Assign the Default Loopback Port**

1. Log in to the Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View drop-down list.
6. Click the arrow next to Netlet under SRA Configuration.

The Netlet page is displayed in the right pane.

7. Scroll to the Default Loopback Port field and type the desired port number.
8. Click Save to record the change.

Enable Reauthentication for Connections

Enable this option if you want the user to enter the Netlet password each time a Netlet connection needs to be established. If you enable this option, the warning popup for connections is not displayed on the user's desktop. See "Display Warning Popup for Connections" on page 315 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 Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View drop-down list.
6. Click the arrow next to Netlet under SRA Configuration.
The Netlet page is displayed in the right pane.
7. Scroll to the Reauthenticate for Connections field and select the option.
8. Click Save to record the change.

Display Warning Popup for Connections

This attribute displays a warning popup dialog box on the user's desktop when someone is trying to connect to Netlet through the listen port and the user is running an application using Netlet. If you do not want the popup to appear on the user's desktop, deselect this attribute.

► To Enable the Warning Popup for Connections

1. Log in to the Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the "location" in the top left corner of the administration console.

5. Select Services from the View drop-down list.
6. Click the arrow next to Netlet under SRA Configuration.
The Netlet page is displayed in the right pane.
7. Select the Display Warning Popup for Connections checkbox to enable the warning popup.
8. Click Save to record the change.

Enable the Display Checkbox in Port Warning Dialog

This attribute displays a checkbox in the warning popup on the users desktop when Netlet tries to connect to the destination host through a freely available port on the local machine, if its enabled in the administration console. This checkbox gives the user the option to enable or disable the popup, by checking or unchecking it accordingly on the desktop.

You can allow the user to suppress this warning popup by disabling the Display Checkbox in Port Warning Dialog option in the administration console.

► To Allow the User to Suppress the Port Warning Dialog

1. Log in to the Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View drop-down list.
6. Click the arrow next to Netlet under SRA Configuration.
The Netlet page is displayed in the right pane.
7. Scroll to the Display Checkbox in Port Warning Dialog field and uncheck the box.
8. Click Save to record the change.

Set the Keep Alive Interval

If the client is connecting to the Gateway through a web proxy, then idle Netlet connections are disconnected due to proxy time out. To prevent this, give a value less than the proxy time-out for this parameter.

► To Set the Keep Alive Interval

1. Log in to the Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View drop-down list.
6. Click the arrow next to Netlet under SRA Configuration.
The Netlet page is displayed in the right pane.
7. Scroll to the Keep Alive Interval (in minutes) field, and type the required time interval.
8. Click Save to record the change.

Set the Terminate Netlet at Portal Logout Option

Enable this option if you want to ensure that all connections are terminated when a user logs out of the Portal Server. This ensures greater security. This option is enabled by default.

Disable this option to ensure that live Netlet connections are operational even after the user has logged out of the Portal Server desktop.

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

► To Set the Terminate Netlet at Portal Logout Option

1. Log in to the Access Manager administration console as administrator.

2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View drop-down list.
6. Click the arrow next to Netlet under SRA Configuration.
The Netlet page is displayed in the right pane.
7. Scroll to the Terminate Netlet at Portal Logout field and select or deselect the checkbox as required.
8. Click Save to record the change.
See also “Running Netlet in a Sun Ray Environment” on page 209.

Define Access to Netlet Rules

You can define access to specific Netlet rules for certain organizations, roles or users.

► To Define Access to Netlet Rules

1. Log in to the Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View drop-down list.
6. Click the arrow next to Netlet under SRA Configuration.
The Netlet page is displayed in the right pane.
7. Scroll to the Access to Netlet Rules field.
8. Type the name of the rule that you want to make available for the selected organization in the Access to Netlet Rules field.
An asterisk (*) in this field indicates that all the defined Netlet rules are available for the selected organization.

9. Click Add.

The specified rule is added to the Access to Netlet Rules list.

10. Repeat steps 7, 8 and 9 for each Netlet rule that you want to make available.
11. Click Save to record the change.

Deny 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 Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View drop-down list.
6. Click the arrow next to Netlet under SRA Configuration.

The Netlet page is displayed in the right pane.

7. Scroll to the Deny Netlet Rules field.
8. Type the name of the rule to which you want to deny access for the selected organization in the Deny Netlet Rules field.

An asterisk (*) in this field indicates that all the defined Netlet rules are denied access for the selected organization.

9. Click Add.

The specified rule is added to the Deny Netlet Rules list.

10. Repeat steps 7, 8 and 9 for each Netlet rule for which you want to deny access.
11. Click Save to record the change.

Allow Access to Hosts

You can define access to specific hosts for certain organizations, roles or users. This enables you to allow access to certain hosts. For example, you can set up the Allow list with five hosts to which the user can telnet.

► To Allow Access to Hosts

1. Log in to the Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View drop-down list.
6. Click the arrow next to Netlet under SRA Configuration.

The Netlet page is displayed in the right pane.

7. Scroll to the Allowed Hosts field.
8. Type the name of the host for which you want to allow access in the Allow Hosts field.

An asterisk (*) in this field indicates that all the hosts in the specified domain are accessible. For example, if you specify *.sesta.com, all the Netlet targets within the sesta.com domain can be executed by the user. You can also specify a wild card IP address such as xxx.xxx.xxx.*.

9. Click Add.

The specified host is added to the Allowed Hosts list.

10. Repeat steps 7 and 8 for each host that you want to make available.
11. Click Save to record the change.

Deny Access to Hosts

You can deny access to specific hosts within an organization. Specify the host for which you want to deny access in the Denied Hosts list.

► **To Deny Access to Hosts**

1. Log in to the Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View drop-down list.
6. Click the arrow next to Netlet under SRA Configuration.

The Netlet page is displayed in the right pane.

7. Scroll to the Denied Hosts field.
8. Type the name of the host for which you want to deny access in the Denied Hosts field.

An asterisk (*) in this field indicates that the user is denied access to all the hosts within the selected organization. For example, to deny access to all the hosts in the organization `sesta`, type `*.sesta.com` in the Denied Hosts field.

To deny access to a specific host, specify the fully qualified name. For example, to deny access to a host `abc`, type `abc.sesta.com`.

9. Click Add.
The specified domain is added to the Access to Domains list.
10. Repeat steps 7 and 8 for each domain that you want to make available.
11. Click Save to record the change.

Launch Netlet

► **To Select Netlet Launch Mode**

1. Log in to the Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.

5. Select Services from the View drop-down list.
6. Click the arrow next to Netlet under SRA Configuration.

The Netlet page is displayed in the right pane.

7. Select the Launch Mode from the pull down window.

Choosing Java Web Start, when the user clicks Netlet icon on the desktop, the browser is launched and Netlet runs. Once Java Web Start is deployed, Netlet does not need to be downloaded again.

8. Click Save to record the change.

Proxy Configuration

The following attributes can be configured at the user level:

- Browser proxy type
- Browser proxy host
- Browser proxy port
- Browser proxy override list

If you do not specify these values in the administration console and Netlet is unable to determine the browser proxy setting, the user is asked for this information when a connection is being established through Netlet for the first time. This information is stored and used for future connections by the user.

Netlet fails to determine the browser proxy setting in the following scenarios:

- The user has Internet Explorer 4.x, 5.x or 6.x with Java plug-in (version less than 1.4.0), has enabled the "Use Browser Settings" option in the Proxies tab of the Java Plug-in Control Panel, and has specified an add-on product or INS file in the "Use automatic configuration script" field in the Local Area Network Settings dialog of Internet Explorer.
- The user has Netscape 6.2 with Java Plug-in (version 1.3.1_01 or greater) and has enabled the "Use Browser Settings" option in the Proxies tab of the Java Plug-in Control Panel.

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

- Browser proxy type

This attribute can take the values `DIRECT` or `MANUAL`. If the user chooses `DIRECT` from the drop-down list, Netlet connects directly to the gateway host.

- **Browser proxy host**
Specify the required proxy host through which Netlet needs to connect.
- **Browser proxy port**
Specify the port on the proxy host through which Netlet needs to connect.
- **Browser proxy override list (Comma separated)**
Specify the hosts for which you do not want Netlet to connect through the proxy. This list can contain multiple comma-separated host names.

Configuring Proxylet

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

NOTE Click Help at the top right corner of the Access Manager administration console, and click SRA Help for a quick reference on all the SRA attributes.

Configure Proxylet

Proxylet can be configured to launch automatically when the user logs in by checking the Download Proxylet Applet Automatically checkbox in the Proxylet channel edit page. If the Download Proxylet Automatically checkbox is not checked, the user can get Proxylet on-demand by clicking the “Launch the Proxylet” link in the Proxylet channel of the standard Portal Desktop.

► To Configure Proxylet Attributes

1. Log in to the Access Manager administration console as administrator.
2. Select the Identity Management tab.
3. Select Organizations from the View drop-down list.
4. Click the required organization name. The selected organization name is reflected as the location in the top left corner of the administration console.
5. Select Services from the View drop-down list.
6. Click the arrow next to Proxylet under SRA Configuration.
7. Click the Download Proxylet Applet Automatically checkbox, if that is desired.
8. Enter the Default Proxylet Applet Bind IP address where Proxylet will run.

9. Enter the required port number where Proxylet will listen in the Default Proxylet Applet Port field. This can also be configured at the client level edit window.
10. Click Save.

NOTE If the user is logged in to Portal Server and invoked Proxylet, then installed a Java Plugin, the user must restart the Netscape browser.

NOTE If Proxylet is enabled, use the `gateway.httpurl` in the `platform.conf` file, not the `gateway.httpsurl` entry.

Configuring SSL Accelerators

This chapter describes how to configure various accelerators for Sun Java™ System Portal Server Secure Remote Access.

This chapter covers the following topics:

- Sun Crypto Accelerator 1000
- Sun Crypto Accelerator 4000
- External SSL Device and Proxy Accelerators

Overview

External accelerators are dedicated hardware co-processors that off-load the SSL functions from a server's CPU, thereby freeing the CPU to perform other tasks and increasing the processing speed for SSL transactions.

Sun Crypto Accelerator 1000

The Sun™ Crypto Accelerator 1000 (Sun CA1000) board is a short PCI board that functions as a cryptographic co-processor to accelerate public key and symmetric cryptography. This product has no external interfaces. The board communicates with the host through the internal PCI bus interface. The purpose of this board is to accelerate a variety of computationally intensive cryptographic algorithms for security protocols in eCommerce applications.

Many critical cryptographic functions, such as RSA [7] and Triple-DES (3DES) [8], can be off-loaded from an application to the Sun CA1000 and performed in parallel. This frees the CPU to perform other tasks, increasing the processing speed for SSL transactions.

Enable Crypto Accelerator 1000

Ensure that Portal Server Secure Remote Access has been installed, and a gateway server certificate (self-signed or issued by any CA) has been installed. See the Chapter 7, “Certificates” on page 215 for details.

Table 13-1 is a checklist to help you keep track of the required information before installing the SSL Accelerator. lists the Crypto Accelerator 1000 parameters and values.

Table 13-1 Crypto Accelerator 1000 Installation Checklist

Parameter	Value
SRA installation base directory	/opt
SRA certificate database path	/etc/opt/SUNWps/cert/default
SRA server certificate nickname	server-cert
Realm	sra-keystore
Realm user	crypta

Configure Crypto Accelerator 1000

► To Configure Crypto Accelerator 1000

1. Follow the instructions in the user's guide to install the hardware. See:

<http://www.sun.com/products-n-solutions/hardware/docs/pdf/816-2450-11.pdf>

2. Install the following packages from the CD.

SUNWcrypm, SUNWcrypu, SUNWcrysus, SUNWdcar, SUNWcrypr, SUNWcrys1, SUNWdcamn, SUNWdcav

3. Install the following patches. (You can get them from the <http://sunsolve.sun.com>)

110383-01, 108528-05, 112438-01

4. Make sure you have the tools `pk12util` and `modutil`.

These tools are installed under `/usr/sfw/bin`. If the tools are not available in the `/usr/sfw/bin` directory, you need to manually add the SUNWtisu package from the Sun Java System distribution media:

```
Solaris_[sparc/x86]/Product/shared_components/
```

5. Create the slots file:

```
vi /etc/opt/SUNWconn/crypto/slots
```

and put "crypta@sra" as the first and only line in the file.

6. Create and set a realm.

- a. Login as root.

- b. Type these commands:

```
cd /opt/SUNWconn/bin/secadm
```

```
secadm> create realm=sra
```

Realm sra created successfully.

7. Create a user:

- a. Type and respond to these commands:

```
secadm> set realm=sra
```

```
secadm{srap}> su
```

```
secadm{root@sra}>create user=crypta
```

Initial password:

Confirm password:

User crypta created successfully.

8. Login as the user you created.

```
secadm{root@sra}> login user=crypta
```

Password:

```
secadm{crypta@sra}> show key
```

No keys exist for this user.

9. Load the Sun Crypto module.

The environment variable `LD_LIBRARY_PATH` must point to `/usr/lib/mps/secv1/`

Type:

```
modutil -dbdir /etc/opt/SUNWps/cert/default -add "Sun Crypto Module"
-libfile /opt/SUNWcom/crypto/lib/libpkcs11.so
```

Use the following command to verify that this module is loaded:

```
modutil -list -dbdir /etc/opt/SUNWps/cert /default
```

10. Export the gateway certificate and the key to the "Sun Crypto Module".

The environment variable `LD_LIBRARY_PATH` must point to `/usr/lib/mps/secv1/`

Type:

```
pk12util -o servercert.p12 -d /etc/opt/SUNWps/cert/default -n
server-cert
```

```
pk12util -i servercert.p12 -d /etc/opt/SUNWps/cert/default -h
"crypta@sra"
```

Now run the show key command:

```
secadm{crypta@sra}> show key
```

You should see two keys for this user.

11. Change the nickname in the `/etc/opt/SUNWps/cert/default/.nickname` file.

```
vi /etc/opt/SUNWps/cert/default/.nickname
```

replace the `server-cert` with `crypta@sra:server-cert`

12. Enable ciphers for acceleration.

SUN CA1000 accelerates RSA functions but supports acceleration only for DES and 3DES ciphers.

13. Modify the `/etc/opt/SUNWps/platform.conf` *gateway-profile-name* to enable the accelerator:

```
gateway.enable.accelerator=true
```

14. From a terminal window, restart the gateway:

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

NOTE	<p>Gateway binds to a plain ServerSocket (non SSL) on the port mentioned as https port in the gateway profile.</p> <p>No SSL encryption or decryption is done on the incoming client traffic. This is done by the accelerator.</p> <p>PDC is not be functional in this mode.</p>
-------------	--

Sun Crypto Accelerator 4000

The Sun™ Crypto Accelerator 4000 board is a Gigabit Ethernet-based network interface card that supports cryptographic hardware acceleration for IPsec and SSL (both symmetric and asymmetric) on Sun servers.

In addition to operating as a standard Gigabit Ethernet network interface card for unencrypted network traffic, the board contains cryptographic hardware to support a higher throughput for encrypted IPsec traffic.

The Crypto Accelerator 4000 board accelerates cryptographic algorithms in both hardware and software. It also supports bulk encryption for ciphers DES and 3DES.

Enable Crypto Accelerator 4000

Ensure that SRA has been installed and a gateway server certificate (self-signed or issued by any CA) has been installed. The following checklist helps you keep track of the required information before installing the SSL Accelerator.

Table 13-1 lists the Crypto Accelerator 4000 parameters and values.

Table 13-2 Crypto Accelerator 4000 Installation Checklist

Parameter	Value
Portal Server Secure Remote Access installation base directory	/opt
SRA instance	default
SRA certificate database path	/etc/opt/SUNWps/cert/default

Table 13-2 Crypto Accelerator 4000 Installation Checklist

Parameter	Value
SRA server certificate nickname	server-cert
CA4000 keystore	srap
CA4000 keystore user	crypta

Configure Crypto Accelerator 4000

► To Configure Crypto Accelerator 4000

1. Follow the instructions in the user's guide to install the hardware and the software packages. See:

<http://www.sun.com/products-n-solutions/hardware/docs/pdf/816-2450-11.pdf>

2. Install the following patch. (You can get them from the <http://sunsolve.sun.com>): 114795
3. Make sure that you have the tools `certutil`, `pk12util` and `modutil`.

These tools are installed under `/usr/sfw/bin`

If the tools are not available in the `/usr/sfw/bin` directory, you need to manually add the `SUNWtisu` package from the Sun Java System distribution media:

`Solaris_[sparc/x86]/Product/shared_components/`

4. Initialize the board.

Run the `/opt/SUNWconn/bin/vcadm` tool to initialize the crypto board and set the following values.

Initial Security Officer Name: `sec_officer`

Keystore name: `sra-keystore`

Run in FIPS 140-2 Mode: `No`

5. Create a user.

```
vcaadm{vca0@localhost, sec_officer}> create user
```

```
New user name: crypta
```

```
Enter new user password:
```

```
Confirm password:
```

```
User crypta created successfully.
```

6. Map token to the key store.

```
vi /opt/SUNWconn/cryptov2/tokens
```

and append sra-keystore to the file.

7. Enable bulk encryption.

```
touch /opt/SUNWconn/cryptov2/sslreg
```

8. Load the Sun Crypto module.

The environment variable `LD_LIBRARY_PATH` must point to `/usr/lib/mps/secv1/`

Type:

```
modutil -dbdir /etc/opt/SUNWps/cert/default -add "Sun Crypto Module"
-libfile /opt/SUNWconn/cryptov2/lib/libvpkcs11.so
```

You can verify that this module is loaded using the following command:

```
modutil -list -dbdir /etc/opt/SUNWps/cert/default
```

9. Export the gateway certificate and the key to the "Sun Crypto Module".

The environment variable `LD_LIBRARY_PATH` must point to `/usr/lib/mps/secv1/`

```
pk12util -o servercert.p12 -d /etc/opt/SUNWps/cert/default -n
server-cert
```

```
pk12util -i servercert.p12 -d /etc/opt/SUNWps/cert/default -h
"sra-keystore"
```

You can verify that the key has been exported using the following command:

```
certutil -K -h "sra-keystore" -d /etc/opt/SUNWps/cert/default
```

10. Change the nickname in the `/etc/opt/SUNWps/cert/default/.nickname` file:

```
vi /etc/opt/SUNWps/cert/default/.nickname
```

replace the `server-cert` with `sra-keystore:server-cert`

11. Enable the ciphers for acceleration.

See “Enable SSL Cipher Selection” on page 272

12. From a terminal window, restart the gateway:

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

The Gateway prompts you to enter the keystore password.

Enter Password or Pin for "sra-keystore": crypta: cryptpa-password

NOTE Gateway binds to a plain ServerSocket (non SSL) on the port mentioned as https port in the gateway profile.

No SSL encryption or decryption is done on the incoming client traffic. This is done by the accelerator.

PDC is not be functional in this mode.

External SSL Device and Proxy Accelerators

An external SSL device can run in front of Secure Remote Access (SRA) in open mode. It provides the SSL link between the client and SRA.

Enable an External SSL Device Accelerator

► **To Enable an External SSL Device Accelerator**

1. Ensure that SRA has been installed and a gateway is running in open mode (HTTP mode).
2. Enable an HTTP Connection. Refer to “Enable HTTP Basic Authentication” on page 250.

Table 13-3 lists the external SSL device and proxy accelerator parameters and values.

Table 13-3 External SSL Device and Proxy Accelerators Checklist

Parameter	Value
SRA instance	default
Gateway Mode	http

Table 13-3 External SSL Device and Proxy Accelerators Checklist

Parameter	Value
Gateway Port	880
External Device/Proxy Port	443

Configure an External SSL Device Accelerator

► To Configure External SSL Device Accelerators

1. Follow the instructions in the user guide to install the hardware and software packages.
2. Install the required patches, if any.
3. Configure a gateway instance to use HTTP.
4. Enter the following values in the `platform.conf` file:

```
gateway.enable.customurl=true
gateway.enable.accelerator=true
gateway.httpurl=https://external-device-URL:port-number
```

5. Gateway notification can be configured in two ways:
 - When the Access Manager can contact the gateway machine at port 880 (Session notifications are in HTTP), enter values in the `platform.conf` file.

```
vi /etc/opt/SUNWps/platform.conf.default
gateway.protocol=http
gateway.port=880
```

- When the Access Manager can contact the external device/proxy at port 443 (Session notifications are in HTTPS), enter values in the `platform.conf` file.

```
vi /etc/opt/SUNWps/platform.conf.default
gateway.host=External Device/Proxy Host Name
gateway.protocol=https
gateway.port=443
```

6. Make sure that the SSL device/proxy is up and running and configured to tunnel the traffic to the gateway port.

7. From a terminal window, restart the gateway:

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

Log Files

The following log files are in the default `/var/opt/SUNWps/debug` directory and contain debug and other types of information.:

Table A-1 Informational and Debug Files

File Name	Contents
<p>The following log files are controlled by the debug parameter in the <code>AMConfig-<i>instance-name</i>.properties</code> file in the default directory <code>/etc/opt/SUNWam/debug/</code> file. For Linux path names, see “Comparison of Solaris and Linux Path Names” on page 26</p>	
<code>amconsole</code>	Netfile, Netlet and Gateway Admin files
<code>srapNetFile</code>	NetFile information file
<code>srapNetlet</code>	Netlet information file
<code>srapProxylet</code>	Proxylet information file
<p>The following log files are controlled by the debug parameter <code>gateway.debug</code> in the <code>platform.conf.gateway-profile-name</code> file in the default directory <code>/etc/opt/SUNWps/</code>. For Linux path names, see “Comparison of Solaris and Linux Path Names” on page 26</p>	
<code>srapGateway.gateway-profile-name</code>	Gateway information
<code>Gateway_to_from_server.gateway-profile-name</code>	
<code>Gateway_to_from_browser.gateway-profile-name</code>	
<code>srapNetletProxy.gateway-profile-name</code>	
<code>srapRewriterProxy.gateway-profile-name</code>	

Table A-1 Informational and Debug Files

File Name	Contents
<code>rwproxy.log.rewriter-proxy-instance-name</code>	Start and stop time of Rewriter Proxy
<code>nlproxy.log.netlet-proxy-instance-name</code>	Start and stop time of Netlet Proxy
<code>gateway.log.gateway.instance.name</code>	Start and stop time of the Gateway
<p>The following Rewriter files are controlled by the debug parameter in the <code>AMConfig-instance-name.properties</code> file in the default directory <code>/var/opt/SUNWam/config/</code> file. See "Troubleshooting Using Debug Logs" on page 138 for more information.</p>	
RuleSetInfo	All the rulesets which have been used for rewriting, are logged in this file.
Original Pages	Contains the page URI, resolved URI (if the resolved URI is different than the page URI), content MIME, the ruleset that has been applied to the page, parser MIME, and the original content. Specific error/warning/messages related to parsing also appear in this file. In message mode full content is logged, in warning and error mode only exception occurred during rewriting are logged.
Rewritten Pages	Contains the page URI, resolved URI (if the resolved URI is different than the page URI), content MIME, ruleset that has been applied to the page, parser MIME, and the rewritten content. This is filled when the debug mode is set to message.
Unaffected Pages	Contains a list the pages that were not modified.
URIInfo Pages	This file contains the URLs found and translated. Details of all the pages whose content remain same as original data is logged in this file. Details logged are: Page URI, MIME and Encoding data, rulesetID used for rewriting, and Parser MIME.

Configuration Attributes

This appendix describes attributes that you can configure for Sun Java™ System Portal Server Secure Remote Access through the Access Manager administration console from the Service Configuration for each Portal Server Secure Remote Access component:

- Access List Service
- Gateway Service
- NetFile Service
- Netlet Service
- Proxylet Service

Access List Service

Table B-1 lists the Access List service attributes.

Table B-1 Access List Service Attributes

Attribute	Default Value	Description
Denied URLs		List of URLs that end-users cannot access through Gateway.
Allowed URLs	*	List of URLs that end-users can access through Gateway.
Single Sign On Disabled Hosts		Disables single sign-on for a list of hosts.
Enable Single Sign On per Session		Enables single sign-on for a session.

Table B-1 Access List Service Attributes

Attribute	Default Value	Description
Allowed Authorization Levels	*	Indicates how much to trust an authentication. Use an asterisk to allow all authentication levels. For information on authentication levels, see the <i>Access Manager Administration Guide</i> .

Gateway Service

When you click the Gateway service, the right pane displays a button to create a new profile and a list of any gateway profiles that have been created.

If you click New, the next pane asks you to enter the new gateway profile name. You have the option to use the default template or a previously created gateway profile as the template.

If you click one of the listed gateway profile names, a list of tabs are presented. They are:

- Core
- Proxies
- Security
- Rewriter
- Logging

Core

Table B-2 lists the Gateway service core attributes.

Table B-2 Gateway Service Core Attributes

Attribute	Default Value	Description
Enable HTTPS Connections		Enables HTTPS connections.
HTTPS Port	443	Specifies the HTTPS port.
Enable HTTP Connections	*	Enables HTTP connections.
HTTP Port	80	Specifies the HTTP port.

Table B-2 Gateway Service Core Attributes

Attribute	Default Value	Description
Enable Rewriter Proxy	*	Enables secure HTTP traffic between Gateway and the intranet. Rewriter proxy and Gateway use the same gateway profile.
Rewriter Proxy List		List of Rewriter proxies. For multiple instances of Rewriter proxies enter the details for each in the form <i>host-name:port</i>
Enable Netlet	Checked	Enables security for TCP/IP (such as Telnet and SMTP), HTTP applications, and fixed port applications.
Enable Proxylet	Checked	Enables the download of Proxylet on a client machine.
Enable Netlet Proxy		Enhances security for Netlet traffic between Gateway and the intranet by extending the secure tunnel from the client, through Gateway to Netlet proxy residing on the intranet. Disable if you do not want to use applications with Portal Server.
Netlet Proxy Hosts		Lists Netlet proxy hosts, in the format: <i>hostname:port</i>
Enable Cookie Management		Tracks and manages user sessions for all web sites that the user is permitted to access. (Does not apply to the cookies used by Portal Server to track Portal Server user sessions).
Enable Persistent HTTP Connections	Checked	Enables HTTP persistent connections at Gateway to prevent sockets being opened for every object (such as images and style sheets) in the web pages.
Maximum Number of Requests per Persistent Connection	10	Specifies the number of requests per persistent connection.
Timeout for Persistent Socket Connections	50	Specifies the amount of time that needs to lapse before sockets are closed.
Grace Timeout to Account for Turnaround Time	20	Specifies the grace amount of time for the request to reach Gateway after the browser has sent it and the time between gateway sending the response and the browser actually receiving it.

Table B-2 Gateway Service Core Attributes

Attribute	Default Value	Description
URLs to which User Session Cookie is Forwarded		Enables servlets and CGIs to receive Portal Server's cookie and use the APIs to identify the user.
Maximum Connection Queue Length	50	Specifies the maximum concurrent connections that Gateway can accept.
Gateway Timeout (seconds)	120	Specifies the time interval in seconds before Gateway times out its connection with the browser.
Maximum Thread Pool Size	200	Specifies the maximum number of threads that can be pre-created in the Gateway thread pool.
Cached Socket Timeout	200	Specifies the time interval in seconds before Gateway times out its connection with Portal Server.
Portal Servers		Specifies Portal Servers in the format <code>http://portal server name:port -number</code> . Gateway tries to contact each of the Portal Servers listed in a round robin manner to service the requests.
Server Retry Interval (seconds)	120	Specifies the time interval between requests to try to start Portal Server, Rewriter proxy or Netlet proxy after it becomes un-available (such as a crash or it was brought down).
Store External Server Cookies		Allows Gateway to store and manage cookies for any third party application or server that is accessed through Gateway.
Obtain Session Information from URL		Encodes session information as part of the URL, whether cookies are supported or not. Gateway uses this session information found in the URL for validation rather than using the session cookie that is sent from the client's browser.

Proxies

Table B-3 lists the Gateway service proxies attributes.

Table B-3 Gateway Service Proxies Attributes

Attribute	Default Value	Description
Use Proxy		Enables usage of web proxies.
Use Webproxy URLs		Lists the URLs that Gateway needs to contact only through the webproxies listed in the Proxies for Domains and Subdomains list, even if the Use Proxy option is disabled.
Do Not Use Webproxy URLs		Lists URLs that Gateway can connect directly to.
Proxies for Domains and Subdomains	iportal.com sun.com	Specifies which proxy to use to contact specific subdomains in specific domains.
Proxy Password List		Specifies the server name, user name and password required for Gateway to authenticate to a specified proxy server, if the proxy server requires authentication to access some or all the sites.
Enable Automatic Proxy Configuration Support		Specifies that the information provided in the Proxies for Domains and Subdomains field is to be ignored.
Automatic Proxy Configuration File location		Specifies the location of files to be used for PAC support.
Enable Netlet Tunneling via Web Proxy		Extends the secure tunnel from the client, through Gateway to the web proxy that resides in the intranet.

Security

Table 13-4 lists the Gateway service security attributes.

Table 13-4 Gateway Service Security Attributes

Attribute	Default Value	Description
Enable HTTP Basic Authentication	Checked	Saves the username and password so that users need not re-enter their credentials when they revisit BASIC-protected web sites.

Table 13-4 Gateway Service Security Attributes

Attribute	Default Value	Description
Non-authenticated URLs	/portal/desktop/images /amserver/login_images /portal/desktop/css /amserver/jss /amconsole/console/css /portal/searchadmin/console/js /amconsole/console/js /amserver/css	Specifies URLs that do not need any authentication, such as directories that contain images.
Certificate-enabled Gateway hosts		Lists the certificate-enabled Gateway hosts.
Allow 40-bit Encryption		Allows 40-bit (weak) Secure Sockets Layer (SSL) connections. If you do not select this option, only 128-bit connections are supported.
Enable SSL Version 2.0	checked	Enables SSL version 2.0. Disabling SSL 2.0 means that browsers that support only the older SSL 2.0 cannot authenticate to SRA. This ensures a greater level of security.
Enable SSL Cipher Selection		Enables SSL cipher selection. You have the option of to support all the pre-packaged ciphers, or you can select the required ciphers individually. You can select specific SSL ciphers for each Gateway instance.
SSL2 Ciphers		Lists the SSL version 2 ciphers you can choose.
SSL3 Ciphers		Lists the SSL version 3 ciphers you can choose.
TLS Ciphers		Lists the TLS ciphers.
Enable SSL Version 3.0	checked	Enables SSL version 3.0. Disabling SSL 3.0 means that browsers that support only the SSL 3.0 cannot authenticate to SRA. This ensures a greater level of security.
Enable Null Ciphers		Enables null ciphers.

Table 13-4 Gateway Service Security Attributes

Attribute	Default Value	Description
Trusted SSL Domains		Lists the trusted SSL domains.
Mark Cookies as secure		Marks cookies as secure. The Enable Cookie Management option must be enabled.

Rewriter

The Rewriter tab has two subsections:

- Basic
- Advanced

Basic

Table B-4 lists the Gateway service Rewriter basic attributes.

Table B-4 Gateway Service Rewriter Attributes - Basic

Attribute	Default Value	Description
Enable Rewriting of All URIs		Specifies that any URI is rewritten without checking against the entries in the Proxies for Domains and Subdomains list.

Table B-4 Gateway Service Rewriter Attributes - Basic

Attribute	Default Value	Description
Map URIs to RuleSets	<pre> *//* .iportal.com*/portal /* default_gateway_rule set */portal/NetFileOpenFileServlet* null_ruleset * generic_ruleset REPLACE_WITH_IPLANET_MAIL_SERVER_NAME iplanet_mail_ruleset REPLACE_WITH_EXCHANGE_SERVER_NAMEexchange_2000sp3_owa_ruleset *//* .iportal.com*/amconsole/* default_gateway_ruleset REPLACE_WITH_INOTES_SERVER_NAME inotes_ruleset http*://*/portal/NetFileController* null_ruleset </pre>	Associates a domain with the ruleset using the Map URIs to RuleSets list. Rulesets are created under Portal Server Configuration in the Access Manager administration console.
Map Parser to MIME Types	<pre> JAVASCRIPT=application/x-java XML=text/xml HTML=text/html;text/html;text/x-component;text/wml;text/vnd.wap.wml CSS=text/css </pre>	Associates new MIME types with HTML, JAVASCRIPT, CSS or XML. Separate multiple entries with a semicolon or a comma.
URIs Not to Rewrite		Lists the URIs not to rewrite. Note: Adding #* to this list allows URIs to be rewritten, even when the href rule is part of the ruleset.
Default Domains		Resolves a host name to a default domain and subdomain. This is specified during installation

Advanced

Table B-5 lists the Gateway service Rewriter advanced attributes.

Table B-5 Gateway Service Rewriter Attributes - Advanced

Attribute	Default Value	Description
Enable MIME Guessing		Enables MIME guessing when MIME is not sent. You must add data to the Map Parser to URIs list box.
Map Parser to URI Mappings		<p>Maps a parser to the URI. Multiple URIs are separated by a semicolon.</p> <p>For example HTML=*.html; *.htm;*Servlet means that Rewriter is used to rewrite the content for any page with a html, htm, or Servlet extension.</p>
Enable Masking		Allows Rewriter to rewrite a URI so that the Intranet URL of a page is not seen.
Seed String for Masking		Specifies a seed string used for masking a URI. A masking algorithm generates this random string.
URIs not to Mask		<p>Specifies Internet URIs not to be mask. This is used when applications (such as an applet) require an Internet URI.</p> <p>For example if you added</p> <p><code>*/Applet/Param*</code></p> <p>to the list box, the URL would not be masked if the content URI</p> <p><code>http://abc.com/Applet/Param1.html</code> is matched in the ruleset rule.</p>
Make Gateway protocol Same as Original URI Protocol		<p>Enables Rewriter to use a consistent protocol to access the referred resources in the HTML content.</p> <p>This applies only to static URIs, not to dynamic URIs generated in Javascript.</p>

Logging

Table B-6 lists the Gateway service logging attributes.

Table B-6 Gateway Service Logging Attributes

Attribute	Default Value	Description
Enable Logging		Enables logging.
Enable per Session Logging		Enables capture of minimum log information such as Client Address, Request Type, and Destination Host.
Enable Detailed per Session Logging		Enables capture of detailed log information such as Client, Request Type, Destination Host, Type of Request, Client Requested URL, Client Post Data size, SessionID, Response Result code, and Complete Response size. Note: Enable per Session Logging must be enabled.
Enable Netlet Logging		Specifies if logging is enabled. If so the following information is captured: Start time, Source, Address, Source port, Server address, Server port(s), Stop time, Status (start or stop)

NetFile Service

When you click the NetFile Service, the right pane displays tabs. They are:

- Hosts
- Permissions
- View
- Operations
- General

Hosts

The Hosts tab has two subsections:

- Config

- Access

Config

Table B-7 lists the NetFile hosts configuration attributes.

Table B-7 NetFile Service Hosts Configuration Attributes

Attribute	Default Value	Description
OS Character Set	Unicode(UTF-8)	Specifies the character set used as the default encoding for communicating with hosts.
Host Detection Order	WIN, NETWARE, FTP, NFS	Specifies the host detection order.
Common Hosts		Specifies hosts to be available through NetFile to all remote NetFile users.
Default Domain		Specifies the default domain that NetFile needs to use to contact allowed hosts.
Default Microsoft Windows Domain/Workgroup		Specifies the default Microsoft Windows domain or workgroup which the users choose to access a Windows host.
Default WINS/DNS Server		Specifies the WINS/DNS server that NetFile uses to access windows hosts.

Access

Table B-8 lists the NetFile service hosts access attributes.

Table B-8 NetFile Service Hosts Access Attributes

Attribute	Default Value	Description
Allow Access to Windows Hosts	Checked	Allows access to Microsoft Windows hosts.
Allow Access to FTP Hosts	Checked	Allows access to FTP hosts.
Allow Access to NFS Hosts	Checked	Allows access to NFS hosts.
Allow Access to Netware Hosts	Checked	Allows access to Netware hosts.
Allowed Hosts	*	Specifies hosts that users can access through NetFile.
Denied Hosts		Specifies hosts that users cannot access through NetFile.

Permissions

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

Table B-9 lists the NetFile service permission attributes.

Table B-9 NetFile Service Permissions Attributes

Attribute	Default Value	Description
Allow File Rename	Checked	Allows users to rename files.
Allow File/Folder Deletion	Checked	Allows users to delete files and folders.
Allow File Upload	Checked	Allows users to upload files.
Allow File/Folder Download	Checked	Allows users to download files and folders.
Allow File Search	Checked	Allows users to search.
Allow File Mail	Checked	Allows file mailing.
Allow File Compression	Checked	Allows file compression.
Allow Changing User Id	Checked	Allows user to use a different ID.
Allow Changing Windows Domains	Checked	Allows users to change Microsoft Windows domains.

View

Table B-10 lists the NetFile Service view attributes.

Table B-10 NetFile Service View Attributes

Attribute	Default Value	Description
Window Size	700 400	Specifies the size of the NetFile window in pixels on the user's desktop. If you enter an invalid value, NetFile uses the default value.
Window Location	100 50	Specifies the location where the NetFile window displays on the user's desktop. If you enter an invalid value, NetFile uses the default value.

Operations

The Operations tab has the following subsections:

- Traffic
- Search
- Compression

Traffic

Table B-11 lists the NetFile service operations traffic attributes.

Table B-11 NetFile Service Operations - Traffic Attributes

Attribute	Default Value	Description
Temporary Directory Location	/tmp	<p>Specifies a temporary directory for various NetFile file operations.</p> <p>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.</p> <p>You may want to create a separate temporary directory for NetFile. If you specify a temporary directory that is common to all modules of the Portal Server, the disk may quickly run out of space. NetFile does not work if the temporary directory has no space.</p>
File Upload Limit (MB)	5	<p>Specifies the maximum size of the files that can be uploaded. If you enter an invalid value, NetFile resets the value to the default. Ensure that you type an integer value.</p> <p>You can specify different file upload size limits for different users.</p>

Search

Table B-12 lists the NetFile service operations search attributes.

Table B-12 NetFile Service Operations - Search Attributes

Attribute	Default Value	Description
Search Directories Limit	100	Specifies the maximum number of directories that can be searched in a single search operation.

Compression

Table B-13 lists the NetFile service operations compression attributes.

Table B-13 NetFile Service Operations - Compression Attributes

Attribute	Default Value	Description
Default Compression Type	Zip	Specifies either Zip or Gzip compression type.
Default Compression Level	6	Specifies the compression level, a number between 1 and 9.

General

Table B-14 lists the Netfile service general attributes.

Table B-14 NetFile Service - General Attribute

Attribute	Default Value	Description
MIME-types Configuration File Location	/opt/S1PS62/SUNWps/samples/config/netfile	Specifies the response content type to send to the client browser.

Netlet Service

Table B-15 lists the Netlet service attributes.

Table B-15 Netlet Service Attributes

Attribute	Default Value	Description
Netlet Rules		Choose to add or delete a rule.
If you add a rule, the following nine attributes are necessary:		
--Rule Name		Specifies a unique name for the rule.
--Encryption Ciphers		Specifies the required ciphers.
--URL		Specifies the URL to the application to be invoked.
--Download Applet		Specifies if an applet needs to be downloaded. If an applet is used, the syntax in the associated edit box is: <i>local-port:server-host:server-port</i>

Table B-15 Netlet Service Attributes

Attribute	Default Value	Description
--Extend Session		Ensures that the Portal Server session time is extended while the Netlet session corresponding to this rule is running.
--Map Local Port to Destination Server Port		Specifies local port, target host and target ports. After entering those values (in the next three rows of this table), click add to make them appear in the list.
--Local Port		Specifies the local port on which Netlet listens. For an FTP rule, the local port value must be 30021.
--Destination Hosts		Static rules contain the host name of the destination machine for the Netlet connection. Dynamic rules contain the word "TARGET".
-- Destination Ports		Specifies the port on the destination host.
Default Native VM Cipher		Specifies the default cipher for the Netlet rules. This is useful when using existing rules that did not include the cipher as a part of the rule.
Default Java™ Plugin Cipher		Specifies the default cipher for the Netlet rules. This is useful when using existing rules that did not include the cipher as a part of the rule.
Default Loopback Port	58000	Specifies the port to be used on the client when applets are downloaded through Netlet. The default value can be overridden in the Netlet rules.
Reauthenticate for Connections		Ensures that users enter the Netlet password each time a Netlet connection needs to be established.
Display Warning Popup for Connections	Checked	Displays a message when the user runs the application over Netlet, and also when an intruder tries to gain access to the desktop through the listen port.
Display Checkbox in Port Warning Dialog	Checked	Provides the user with the option to suppress the Warning Dialog Popup when Netlet tries to connect to the destination host on the user's standard Portal Desktop.

Table B-15 Netlet Service Attributes

Attribute	Default Value	Description
Keep Alive Interval (minutes)	0	If the client is connecting to the Gateway through a web proxy, then idle Netlet connections are disconnected due to proxy timeout. To prevent this, give a value less than the proxy timeout for this parameter.
Terminate Netlet at Portal Logout	Checked	Ensures that all connections are terminated when a user logs out of the Portal Server.
Access to Netlet Rules	*	Define access to specific Netlet rules for certain organizations, roles or users.
Deny Netlet Rules		Denies access to specific Netlet rules for certain organizations, roles or users.
Allowed Hosts	*	Defines access to specific hosts for certain organizations, roles or users.
Denied Hosts		Denies access to specific hosts within an organization.

Proxylet Service

Table B-16 lists the Proxylet service attributes.

Table B-16 Proxylet Service Attributes

Attribute	Default Values	Description
Download Proxylet Applet Automatically		When the checkbox is checked, Proxylet is downloaded to the client machine when the user logs on.
Default Proxylet Applet Bind IP	127.0.0.1	The IP address where the Proxylet Applet resides.
Default Proxylet Applet Port	58080	This is the port where Proxylet listens.

Country Codes

The following table lists the two-letter country codes that you need to specify during certificate administration.

Table C-1 Two-letter Country Codes (*1 of 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	Azerbaijan
ba	Bosnia-Herzegovina
bb	Barbados
bd	Bangladesh

Table C-1 Two-letter Country Codes (2 of 9)

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
com	Commercial
cr	Costa Rica
cs	Former Czechoslovakia

Table C-1 Two-letter Country Codes *(3 of 9)*

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
gb	Great Britain
gd	Grenada
ge	Georgia
gf	French Guyana

Table C-1 Two-letter Country Codes (4 of 9)

gh	Ghana
gi	Gibraltar
gl	Greenland
gm	Gambia
gn	Guinea
gov	USA Government
gp	Guadeloupe (French)
gq	Equatorial Guinea
gr	Greece
gs	S. Georgia and S. Sandwich Isls.
gt	Guatemala
gu	Guam (USA)
gw	Guinea Bissau
gy	Guyana
hk	Hong Kong
hm	Heard and McDonald Islands
hn	Honduras
hr	Croatia
ht	Haiti
hu	Hungary
id	Indonesia
ie	Ireland
il	Israel
in	India
int	International
io	British Indian Ocean Territory
iq	Iraq
ir	Iran
is	Iceland
it	Italy
jm	Jamaica

Table C-1 Two-letter Country Codes *(5 of 9)*

jo	Jordan
jp	Japan
ke	Kenya
kg	Kyrgyz Republic (Kyrgyzstan)
kh	Cambodia, Kingdom of
ki	Kiribati
km	Comoros
kn	Saint Kitts and Nevis Anguilla
kp	North Korea
kr	South Korea
kw	Kuwait
ky	Cayman Islands
kz	Kazakhstan
la	Laos
lb	Lebanon
lc	Saint Lucia
li	Liechtenstein
lk	Sri Lanka
lr	Liberia
ls	Lesotho
lt	Lithuania
lu	Luxembourg
lv	Latvia
ly	Libya
ma	Morocco
mc	Monaco
md	Moldavia
mg	Madagascar
mh	Marshall Islands
mil	USA Military
mk	Macedonia

Table C-1 Two-letter Country Codes (6 of 9)

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
no	Norway
np	Nepal
nr	Nauru
nt	Neutral Zone
nu	Niue
nz	New Zealand
om	Oman

Table C-1 Two-letter Country Codes (7 of 9)

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
se	Sweden
sg	Singapore
sh	Saint Helena
si	Slovenia
sj	Svalbard and Jan Mayen Islands
sk	Slovak Republic
sl	Sierra Leone
sm	San Marino

Table C-1 Two-letter Country Codes *(8 of 9)*

sn	Senegal
so	Somalia
sr	Suriname
st	Saint Tome (Sao Tome) and Principe
su	Former USSR
sv	El Salvador
sy	Syria
sz	Swaziland
tc	Turks and Caicos Islands
td	Chad
tf	French Southern Territories
tg	Togo
th	Thailand
tj	Tadjikistan
tk	Tokelau
tm	Turkmenistan
tn	Tunisia
to	Tonga
tp	East Timor
tr	Turkey
tt	Trinidad and Tobago
tv	Tuvalu
tw	Taiwan
tz	Tanzania
ua	Ukraine
ug	Uganda
uk	United Kingdom
um	USA Minor Outlying Islands
us	United States
uy	Uruguay
uz	Uzbekistan

Table C-1 Two-letter Country Codes *(9 of 9)*

va	Holy See (Vatican City State)
vc	Saint Vincent and Grenadines
ve	Venezuela
vg	Virgin Islands (British)
vi	Virgin Islands (USA)
vn	Vietnam
vu	Vanuatu
wf	Wallis and Futuna Islands
ws	Samoa
ye	Yemen
yt	Mayotte
yu	Yugoslavia
za	South Africa
zm	Zambia
zr	Zaire
zw	Zimbabwe

Glossary

Refer to the Java™ Enterprise System Glossary (<http://docs.sun.com/doc/816-6873>) for a complete list of terms that are used in this documentation set.

Index

A

- accelerators
 - external SSL Device 334
 - proxy 334
 - Sun Crypto 1000 327
 - Sun Crypto 4000 331
- access
 - allowing to hosts 320
 - denying to hosts 320
- Access List
 - allowed URLs 240
 - denied URLs 240
 - single sign-on 241
- administration console 34
- administrator configured cipher 196
- allowed URLs 240
- allowing
 - 40-bit browser connections 270
- AMConfig properties file 51
- AMConfig property file
 - default 48
- applet 189
 - downloading 202
- applications
 - running 187
 - supported 36
- assigning
 - default loopback port 314
 - Netlet service to a user 310
- attributes
 - configuring 34

- SRA 339

- authentication
 - chaining 80
 - PDC 80, 216
- authorization levels 242
- Autodetect
 - in Netfile 182
- Automatic Proxy Configuration
 - file location 267

B

- browser caching
 - disabling 81

C

- cached socket timeout 257
- Calendar 36
- cascading style sheets
 - in Rewriter 128
- case study
 - Rewriter 173
- certadmin script 222
- certificates
 - certadmin script 222
 - certificate signing request 224
 - deleting 230

- files 216
 - installing from CA 228
 - listing all 235
 - listing root CA certificates 233
 - modifying trust attributes 232
 - ordering 228
 - printing 236
 - public certificates 218
 - Root CA certificates 227
 - self-signed 222
 - SSL 216
 - trust attributes 217, 218
 - wild card 81
 - character set encoding 94
 - checkbox
 - enabling in port warning dialog box 316
 - chroot 52
 - ciphers
 - administrator configured 196
 - default encryption 313
 - null 273
 - selecting 272
 - supported 196
 - user configurable 196
 - Citrix
 - html file 209
 - common host list
 - configuring 294
 - Communication Express 37
 - components
 - Netlet 188
 - compression
 - for NetFile 307
 - configuring
 - allowed hosts list 298
 - common host list 294
 - denied hosts list 299
 - denied URLs 240
 - Gateway 243
 - Netlet 309
 - Outlook Web Access 177
 - persistent HTTP connections 252
 - Personal Digital Certificates 274
 - Proxylet 325
 - Rewriter 128
 - Secure Remote Access 34
 - conflict resolution 36
 - connections
 - enable warning popup dialog box 315
 - persistent 252
 - cookies
 - enabling 249
 - marking as secure 262
 - storage of external 260
 - country codes
 - two letter values 355
 - creating
 - gateway profile 40
 - hostproxy 58
 - list of certificate-enabled gateway hosts 269
 - list of mappings to parse 284
 - list of non-authenticated URLs 269
 - list of parser to URI mappings 135
 - list of portal servers 258
 - list of trusted SSL domains 273
 - list of URIs not to mask 286
 - list of URIs not to rewrite 130, 282
 - list of URIs to ruleset mappings 279
 - Rewriter Proxy 74
 - customizing
 - Gateway user interface 82
- ## D
- debug logs
 - Rewriter 138
 - debugging
 - location of information 208
 - NetFile 184
 - default
 - domain 64
 - gateway profile 40
 - Windows domain 296, 297
 - Windows workgroup 296
 - default domain
 - rewriting 64
 - specifying 283, 295
 - default encryption ciphers 313
 - deleting

- Netlet rules 313
- demilitarized zone 30
- denying
 - URLs 240
- disabling
 - browser caching 81
 - Netlet Proxy 248
 - single sign-on 241
 - SSL Version 2.0 271
- DMZ 30
- DNS 205
- dynamic rule
 - downloading applet 202
 - invoking 201
 - Netlet 195

E

- enabling
 - 40-bit browser connections 270
 - authentication chaining 80
 - cipher selection 272
 - connections 245
 - cookies 249
 - debugging 184
 - display checkbox in port warning dialog 316
 - HTTP basic authentication 250
 - HTTP connections 252
 - logging 288
 - marking cookies as secure 262
 - masking 135, 285
 - MIME guessing 134, 284
 - NetFile access 183
 - Netlet logging 208, 290
 - Netlet Proxy 73, 248
 - null ciphers 273
 - PDC authentication 274
 - Proxylet 249
 - reauthentication for connections 315
 - Reverse Proxy 77
 - Rewriter Proxy 76, 246
 - rewriting of all URLs 129
 - single sign-on 241
 - SSL Version 2.0 271

- SSL version 3.0 272
- storage of external server cookies 260
- use of web proxies 263
- warning popup dialog box 315
- web proxies 263

F

- federation management 84
- file upload limit 305
- FTP
 - support in NetFile 182

G

- Gateway
 - certificate-enabled 269
 - chroot mode 52
 - configuring 243
 - enabling connections 245
 - gateway profile 40
 - HTTP mode 245
 - HTTPS mode 245
 - introduction 39
 - logging 288
 - multi-homed 51
 - obtaining of a session from URL 260
 - restarting 57
 - specifying thread pool 257
 - starting 56
 - stopping 57
 - timeout 256
 - using PAC file 65
- Gateway service 33
- generating
 - self-signed certificates 222
- grace timeout 253

H

headers

- HTTP 77

host detection order

- configuring 293
- used in NetFile 182

hostproxy

- creating 58

hosts

- allowing access 320
- configuring allowed host list 298, 299
- denying access 320
- specifying access 297

HTML

- rules in Rewriter 103

HTML meta tags 94

HTTP

- basic authentication 250
- contacting resources 59
- headers 77
- resources using web proxies 59

I

iNotes 36

J

Java™ Enterprise System Accessory CD

- jchdt package 94
- SUNWrhino package 65

JavaScript

- rules in Rewriter 110

Jcharset

- using PAC file 65

jCIFS

- for Windows access 183
- support in NetFile 182

K

keep alive interval

- setting 317

L

log files

- filenames 337

logging

- enabling debugging 208
- Gateway 288
- NetFile 185
- Netlet 208
- Rewriter 138

loopback port

- assigning 314

M

masking

- enabling 135, 285
- seed string 286

maximum number of requests 252

Messenger Express 36

Microsoft Exchange Server 206

MIME

- guessing 134, 284
- types to parse 281

MIME types

- creating list 281

MIME-types

- specifying 307

mode

- HTTP 245
- HTTPS 245
- open 30
- secure 31

modifying

- Netlet rules 312

multi-homed gateway 51

- multiple instances
 - Gateway 51
 - Rewriter proxies 74

N

- Net rules
 - samples 203
- NetFile 181
 - access to hosts 297
 - allowing access to hosts 298
 - common host list 294
 - compression 307
 - configuring 291
 - debugging 184
 - denying access to hosts 299
 - enabling access 183
 - host detection order 182
 - introduction 181
 - logging 185
 - supported protocols 182
 - temporary files directory 304
 - upload size limit 305
 - using Novell Netware 183
 - using ProFTPD server 183
 - window location 303
 - window size 302
- NetFile service 33
- Netlet 189
 - access to hosts 320
 - adding a rule 311
 - applet 189
 - components 188
 - configuring 309
 - configuring for PDC 213
 - denying access to hosts 320
 - download applet checkbox 311
 - downloading applet from a remote host 191
 - enabling 247
 - enabling reauthentication for connections 315
 - in a Sun Ray environment 209
 - introduction 187
 - keep alive interval 317
 - listen port 188
 - logging 208, 290
 - port number 198
 - provider 189
 - rules 189, 191
 - terminating at logout 317
 - tunneling via web proxy 268
 - usage scenario 190
 - using PAC file 65
- Netlet Proxy 189
 - advantages 68
 - creating 72
 - enabling 73
 - restarting 73
 - using 68
- Netlet rule samples
 - FTP 207
 - IMAP 204
 - Lotus Notes non-web client 205
 - Lotus web client 204
 - Microsoft Outlook and Exchange Server 206
 - Netscape 4.7 mail client 207
 - SMTP 204
- Netlet rules 312
 - deleting 313
 - denying access 319
 - dynamic 195
 - modifying 312
 - specifying access 318
 - static rule 195
- Netlet service 34
 - assigning to a user 310
- NFS
 - support in NetFile 182
- nlpmultiinstance script 72
- notifications 36
- Novell Netware
 - protocol for NetFile 183

O

- open mode 30
- OS character set 292
- Outlook Web Access 206

- configuring 177
- ruleset 177, 281

P

PAC

- configuration 65

PAC file

- location 267
- using Rhino software 65

- parser to URI mapping 135

passwords

- proxy 265

PDC

- authentication 216
- authentication chaining 80
- configuring 213, 274

- platform.conf 42

- properties 44

port

- loopback 314
- Netlet 188

- port number

- Netlet 198

Portal Server

- instances 83

portal servers

- creating list 258

- processing order

- proxies 61

ProFTPD

- using NetFile 183

properties

- platform.conf 44

protocols

- NetFile 182
- supported in NetFile 182

- Proxies for Domains and Subdomains 61

proxy

- accelerators 334
- authentication 265
- Netlet 189, 248
- passwords 265

- Reverse 77

- Rewriter 246

- specifying 263

- specifying a hostproxy 58

- Web 59

- Proxy Auto Configuration 65

Proxylet

- advantages 93

- configuring 325

- enabling 249

- using PAC file 65

- Proxylet service 34

R

reauthentication

- connections 315

restarting

- Gateway 57

- Netlet Proxy 73

- Rewriter Proxy 76

- Reverse Proxy 77

- enabling 77

Rewriter

- and Proxies for Domains and Subdomains list 64

- case study 173

- configuring 128

- consistent protocol 287

- creating list of parser to URI mappings 135

- creating list of URIs not to rewrite 130

- creating list of URIs to ruleset mappings 279

- enabling masking 135

- enabling rewriting of all URLs 278

- HTML rules 103

- JavaScript rules 110

- mapping 6.x ruleset with 3.0 178

- pattern-matching in rules 108

- rewriting all URLs 129

- RuleSet DTD 96

- samples 141

- URLScraper 95

- using debug logs 138

- using wildcards 131

- working samples 141

- writing rules 101
- XML rules 125
- Rewriter Proxy
 - advantages 74
 - creating 74
 - enabling 76
 - restarting 76
- Rewriter service 33
- Rhino software
 - to parse PAC files 65
- rules
 - adding 311
 - cascading style sheets 128
 - HTML in Rewriter 103
 - JavaScript in Rewriter 110
 - Netlet 191
 - Rewriter 101
 - WML 128
- ruleset
 - generic 130
 - OWA 281
- ruleset mapping
 - creating list of URIs 279
- running
 - applications 187
 - HTTP mode 245
 - HTTPS mode 245
- rwpmultiinstance 74

S

- samples
 - Rewriter 141
- search
 - directory limit 306
- secure mode 31
- Secure Sockets Layer 32
- selecting
 - ciphers 272
- self-signed certificates 222
- server retry interval 259
- services
 - SRA 33

- single sign-on 241
- SMB
 - for windows access 183
- SMTP 247
- socket
 - connection timeout 253
- Solaris
 - patches 28
 - support 28
- specifying 242
 - access to hosts 297
 - authorization levels 242
 - cached socket timeout 257
 - conflict resolution 36
 - default domain 283, 295
 - default WINS/DNS 297
 - direct connection 264
 - Gateway thread pool size 257
 - Gateway timeout 256
 - keep alive interval 317
 - loopback port 314
 - maximum connection queue length 256
 - MIME-types file 307
 - NetFile window location 303
 - NetFile window size 302
 - OS character set 292
 - proxies 263
 - proxy authentication 265
 - search directories limit 306
 - temporary directory 304
 - Windows domain 296

SRA

- contacting SRA Core 58
- list of all attributes 339
- services 33
- software 29
- SSL 216
- SSL version 3.0 272
- SSO 241
- starting
 - Gateway 56
- static rule 195
- stopping
 - Gateway 57
- SUNWjchdt package 94

- support
 - Solaris 28
- supported ciphers 196
- suppressing
 - port warnings 316

T

- TCP/IP 188, 247
- Telnet 247
- temporary files directory 304
- terminating
 - Netlet 317
- timeout
 - cached sockets 257
 - Gateway 256
 - grace 253
 - socket connection 253
- troubleshooting 138
- trust attributes 217
- trusted SSL domains 273

U

- UNIX
 - command line 34
- upload size limit
 - for NetFile 305
- URLs
 - allowed 240
 - creating list for web proxy 263
 - denied 240
 - enabling rewriting 278
 - invoked by dynamic Netlet rules 201
 - non-authenticated 269
 - not to rewrite 282
 - obtaining session 260
- URLScraper 95
- user-configurable cipher 196

W

- warning popup dialog box 315
- watchdog
 - Netlet Proxy 73
 - Rewriter Proxy 76
- Web Proxy 59
- web proxy
 - enabling 263
 - Netlet tunneling 268
- wild card certificates 81
- wildcard
 - in Rewriter 131
 - in Web Proxy 61
- window location
 - for NetFile 303
- window size
 - for NetFile 302
- Windows
 - domain 296, 297
 - jCIFS needed 183
- Windows domain
 - specifying 296
- WINS/DNS server
 - specifying 297
- WML
 - rules in Rewriter 128

X

- XML rules
 - in Rewriter 125