



Sun Java™ System

# Portal Server Secure Remote Access 6 管理指南

---

2004Q2

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

文件号码: 817-7146

版权所有 © 2004 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. 保留所有权利。

对于本文档中介绍的产品，Sun Microsystems, Inc. 对其所涉及的技术拥有相关知识产权。需特别指出的是（但不局限于此），这些知识产权可能包括在 <http://www.sun.com/patents> 中列出的一项或多项美国专利，以及在美国和其他国家/地区申请的一项或多项其他专利和待批专利。

本产品含有 Sun Microsystems, Inc. 的机密信息和商业秘密。未经 Sun Microsystems, Inc. 事先明确书面许可，禁止使用、公开或复制。

美国政府权利商业软件。政府用户对软件的使用须遵循 Sun Microsystems, Inc. 标准许可协议和 FAR 及其附录中的适用条款的规定。

本发行本中可能包含第三方编写的资料。

本产品的某些部分可能是从 Berkeley BSD 系统衍生出来的，并获得了加利福尼亚大学的许可。UNIX 是 X/Open Company, Ltd. 在美国和其他国家 / 地区独家许可的注册商标。

Sun、Sun Microsystems、Sun 徽标、Java、Solaris、JDK、Java Naming and Directory Interface、JavaMail、JavaHelp、J2SE、iPlanet、Duke 徽标、Java Coffee Cup 徽标、Solaris 徽标、SunTone Certified 徽标以及 Sun ONE 徽标是 Sun Microsystems, Inc. 在美国及其他国家的商标或注册商标。

所有 SPARC 商标的使用均已获得许可，它们是 SPARC International, Inc. 在美国及其他国家 / 地区的商标或注册商标。带有 SPARC 商标的产品均基于由 Sun Microsystems, Inc. 开发的体系结构。

Legato 和 Legato 徽标是注册商标，Legato NetWorker 是 Legato Systems, Inc. 的商标或注册商标，Netscape Communications Corp 徽标是 Netscape Communications Corporation 的商标或注册商标。

OPEN LOOK 和 Sun(TM) Graphical User Interface 是 Sun Microsystems, Inc. 为其用户和许可持有者开发的。Sun 感谢 Xerox 在研究可视或图形用户界面的概念方面为计算机行业所做的开创性贡献。Sun 已从 Xerox 获得了对 Xerox 图形用户界面的非独占性许可证，该许可证还适用于实现 OPEN LOOK GUI 和其他方面遵守 Sun 书面许可协议的 Sun 许可证持有者。

本服务手册所涉及产品及所包含信息受“美国出口控制”法律制约，并可能受其他国家进出口法律的限制。严禁核武器、导弹、生化武器或海上核能最终用户或最终用户以直接或间接方式使用这些产品。严禁向美国禁运法令的目标国家或美国禁止出口清单上所列实体（包括，但不限于被施禁的个人及专门指定的国民清单）出口或再出口这些产品。

本文档按“原样”提供，对所有明示或默示的条件、陈述和担保，包括对适销性、特殊用途的适用性或非侵权性的默示保证，均不承担任何责任，除非此免责声明的适用范围在法律上无效。

# 目录

<b>图目录</b> .....	<b>11</b>
<b>表目录</b> .....	<b>13</b>
<b>过程目录</b> .....	<b>15</b>
<b>关于本指南</b> .....	<b>21</b>
哪些人应阅读本指南 .....	21
您需要了解哪些内容 .....	22
本书的组织结构 .....	22
本指南所使用的文档约定 .....	24
等宽字体 .....	24
斜体字体 .....	24
方括号 .....	24
命令行提示符 .....	25
在何处查找相关信息 .....	25
相关第三方站点引用 .....	26
在哪里可找到本在线指南 .....	26
<b>第 1 章 Portal Server Secure Remote Access 简介</b> .....	<b>27</b>
SRA 软件概述 .....	27
开放模式 .....	28
安全模式 .....	29
SRA 服务 .....	31
网关 .....	32
重写器 .....	32
NetFile .....	32
Netlet .....	32

Proxylet .....	33
管理 SRA 产品 .....	33
配置 SRA 属性 .....	33
设置冲突解决 .....	35
支持的应用程序 .....	35
<b>第 2 章 网关 .....</b>	<b>37</b>
网关概述 .....	38
创建网关配置文件 .....	38
了解 platform.conf 文件 .....	40
运行 chroot 环境中的网关 .....	46
在 chroot 环境重新启动网关 .....	48
创建网关的多个实例 .....	49
创建多宿主网关实例 .....	51
使用同一 LDAP 创建网关实例 .....	51
启动和停止网关 .....	52
重新启动网关 .....	53
指定虚拟主机 .....	54
指定联系 Identity Server 的代理 .....	55
使用网络代理 .....	55
使用自动代理配置 .....	61
使用 Netlet 代理 .....	64
创建 Netlet 代理的实例 .....	67
启用 Netlet 代理 .....	68
重新启动 Netlet 代理 .....	68
使用重写器代理 .....	69
创建重写器代理的实例 .....	69
启用重写器代理 .....	71
重新启动重写器代理 .....	71
与网关一起使用反向代理 .....	72
获取客户机信息 .....	72
使用验证链 .....	75
使用通配符证书 .....	76
禁用浏览器高速缓存 .....	76
自定义网关服务用户界面 .....	77
使用联合管理 .....	78
联合管理方案 .....	78
配置联合管理资源 .....	79
<b>第 3 章 Proxylet 和重写器 .....</b>	<b>85</b>
Proxylet 概述 .....	86
使用 Proxylet 的优点 .....	86

配置 Proxylet .....	87
重写器概述 .....	87
字符集编码 .....	88
重写器使用方案 .....	88
URLScaper .....	88
网关 .....	89
编写规则集 .....	89
公共接口（规则集 DTD） .....	90
XML DTD 示例 .....	93
规则编写步骤 .....	95
规则集指导原则 .....	95
定义规则集根元素 .....	96
使用递归功能 .....	96
定义基于语言的规则（定义规则） .....	97
HTML 内容规则 .....	97
JavaScript 内容规则 .....	103
XML 内容规则 .....	118
层叠样式表规则 .....	121
WML 规则 .....	121
使用递归功能 .....	121
在网关服务中配置重写器 .....	122
基本任务 .....	122
高级任务 .....	127
使用调试日志排除故障 .....	131
设置重写器调试级别 .....	132
调试文件名称 .....	132
工作示例 .....	134
HTML 内容示例 .....	135
JavaScript 内容示例 .....	144
XML 属性示例 .....	165
实例研究 .....	166
6.x 与 3.0 的规则集映射 .....	171
<b>第 4 章 NetFile .....</b>	<b>173</b>
NetFile 概述 .....	173
支持的文件访问协议 .....	174
启用对 NetFile 的访问 .....	175
启用 NetFile 的日志 .....	176
配置 UNIX 验证 .....	176
<b>第 5 章 Netlet .....</b>	<b>179</b>
Netlet 概述 .....	179

Netlet 组件 .....	180
Netlet 使用方案 .....	181
使用 Netlet .....	182
从远程主机下载 Applet .....	182
定义 Netlet 规则 .....	183
规则类型 .....	186
Netlet 规则示例 .....	190
Netlet 规则示例 .....	195
启用 Netlet 日志 .....	198
在 Sun Ray 环境中运行 Netlet .....	199
新 HTML 文件 .....	199
弃用的 HTML 文件: .....	201
<b>第 6 章 具有 PDC 的 Netlet .....</b>	<b>203</b>
为 PDC 配置 Netlet .....	203
<b>第 7 章 证书 .....</b>	<b>205</b>
SSL 证书概述 .....	206
证书文件 .....	206
证书委托属性 .....	207
CA 委托属性 .....	208
certadmin 脚本 .....	212
生成自签名证书 .....	213
生成证书签名请求 (CSR) .....	215
添加根 CA 证书 .....	218
安装来自证书授权机构的 SSL 证书 .....	219
从 CA 订购证书 .....	219
安装来自 CA 的证书 .....	220
删除证书 .....	221
修改证书的委托属性 .....	223
列出根 CA 证书 .....	224
列出所有证书 .....	226
打印证书 .....	227
<b>第 8 章 配置 URL 访问控制 .....</b>	<b>229</b>
设置拒绝的 URL 列表 .....	230
设置允许的 URL 列表 .....	230
管理单点登录 .....	231
<b>第 9 章 配置网关 .....</b>	<b>233</b>
核心选项卡 .....	234
启用 HTTP 和 HTTPS 连接 .....	235

启用和创建重写器代理列表	235
启用 Netlet	237
启用和创建 Netlet 代理列表	237
启用 Proxylet	238
启用 Cookie 管理	239
启用 HTTP 基本验证	240
启用持久性 HTTP 连接	241
指定每个持久性连接的最大请求数量	242
指定持久套接字连接超时	242
指定周转时间的宽限期超时	243
创建将用户会话 Cookie 转发到 URL 列表	244
指定最大连接队列长度	245
指定网关超时	246
指定线程池容量最大值	247
指定高速缓存套接字超时	247
创建 Portal Server 列表	248
指定服务器重试间隔	249
启用存储外部服务器 Cookie	249
从 URL 获取会话	250
启用将 Cookie 标记为安全	251
代理选项卡	251
启用“使用网络代理”	252
创建网络代理的 URL 列表	252
创建不使用代理的 URL 列表	253
创建域和子域代理列表	254
创建代理口令列表	255
启用自动代理配置支持	256
指定自动代理配置文件位置	256
通过网络代理启用 Netlet 隧穿	257
安全选项卡	257
创建非验证 URL 列表	258
创建已启用证书的网关主机列表	259
允许 40 位加密连接	259
启用 SSL 2.0 版本	260
启用 SSL 密码选择	261
启用 SSL 3.0 版本	261
启用空密码	262
创建信任的 SSL 域列表	263
配置个人数字证书 (PDC) 验证	263
重写器选项卡	267
启用全部 URL 重写	267
创建 URI 到规则集映射列表	268
创建要分析的 MIME 类型列表	270

指定默认域和子域 .....	271
创建禁止重写的 URI 列表 .....	272
启用 MIME 推测 .....	273
创建要分析的 URI 映射列表 .....	273
启用屏蔽 .....	274
指定屏蔽种子字符串 .....	275
创建禁止屏蔽的 URI 列表 .....	275
使网关协议与原始 URI 协议相同 .....	276
记录选项卡 .....	277
启用记录 .....	277
启用 Netlet 日志 .....	278
<b>第 10 章 配置 NetFile .....</b>	<b>281</b>
主机选项卡 .....	282
指定 OS 字符集 .....	282
指定主机侦测顺序 .....	283
配置公共主机列表 .....	284
指定默认域 .....	286
指定 Windows 域 / 工作组 .....	287
指定默认 WINS/DNS 服务器 .....	288
指定对不同类型主机的访问 .....	288
配置允许的主机列表 .....	289
配置拒绝的主机列表 .....	290
权限选项卡 .....	292
查看选项卡 .....	293
指定 NetFile 窗口大小 .....	294
指定 NetFile 窗口位置 .....	295
操作选项卡 .....	296
指定临时文件目录 .....	296
设置文件上传大小限制 .....	297
指定搜索目录限制 .....	298
指定压缩 .....	299
常规选项卡 .....	300
指定 MIME 类型配置文件位置 .....	300
启用 NetFile 的调试功能 .....	301
<b>第 11 章 配置 Netlet .....</b>	<b>303</b>
为用户分配 Netlet 服务 .....	304
添加 Netlet 规则 .....	305
修改现有 Netlet 规则 .....	306
删除 Netlet 规则 .....	307
指定默认加密密码 .....	307

分配默认回环端口 .....	308
启用连接时重新验证 .....	309
启用连接时弹出警告对话框 .....	309
启用在端口警告对话框中显示复选框 .....	310
设置保活间隔 .....	311
设置门户注销时终止 Netlet 选项 .....	311
定义 Netlet 访问规则 .....	312
拒绝 Netlet 访问规则 .....	313
允许访问主机 .....	314
拒绝访问主机 .....	314
代理配置 .....	315
启用调试日志 .....	316
<b>第 12 章 配置 Proxylet .....</b>	<b>319</b>
配置 Proxylet .....	319
<b>第 13 章 配置 SSL 加速器 .....</b>	<b>321</b>
概述 .....	321
Sun Crypto Accelerator 1000 .....	321
启用 Crypto Accelerator 1000 .....	322
配置 Crypto Accelerator 1000 .....	322
Sun Crypto Accelerator 4000 .....	325
启用 Crypto Accelerator 4000 .....	325
配置 Crypto Accelerator 4000 .....	326
外部 SSL 设备和代理加速器 .....	328
启用外部 SSL 设备加速器 .....	328
配置外部 SSL 设备加速器 .....	329
<b>附录 A 日志文件 .....</b>	<b>331</b>
<b>附录 B 配置属性 .....</b>	<b>333</b>
访问列表服务 .....	333
网关服务 .....	334
核心 .....	334
代理 .....	336
安全 .....	337
重写器 .....	338
日志 .....	340
NetFile 服务 .....	341
主机 .....	341
权限 .....	342
视图 .....	343

操作 .....	343
常规 .....	345
Netlet 服务 .....	345
Proxylet 服务 .....	347
<b>附录 C 国家代码 .....</b>	<b>349</b>
<b>术语表 .....</b>	<b>359</b>

# 图目录

图 1-1	开放模式下的 Portal Server .....	29
图 1-2	安全模式下的 Portal Server（具有 SRA 软件） .....	31
图 2-1	网络代理管理 .....	57
图 2-2	Netlet 代理的实现 .....	67
图 5-1	Netlet 组件 .....	182



# 表目录

表 2-1	platform.conf 文件属性 .....	41
表 2-2	域和子域代理列表中条目的映射 .....	59
表 2-3	HTTP 报头中的信息 .....	73
表 3-1	* 通配符用法示例 .....	103
表 3-2	重写器调试文件 .....	132
表 3-3	示例规则集与实例研究间的映射 .....	169
表 3-4	与 SP3 的规则映射 .....	171
表 4-1	文件系统和支持的协议 .....	174
表 5-3	Netlet 规则示例 .....	195
表 7-1	证书文件 .....	207
表 7-2	证书委托属性 .....	208
表 7-3	公共证书授权机构 .....	208
表 13-1	Crypto Accelerator 1000 安装清单 .....	322



# 过程目录

设置冲突解决级别 .....	35
创建网关配置文件 .....	39
安装 chroot .....	46
在 chroot 环境中重新启动网关 .....	48
启动网关 .....	52
停止网关 .....	53
用不同的配置文件重新启动网关 .....	53
重新启动网关 .....	53
配置网关监视器 .....	54
指定虚拟主机 .....	54
指定代理 .....	55
重新启动 Netlet 代理 .....	68
配置 Netlet 代理监视器 .....	69
重新启动重写器代理 .....	71
配置重写器代理监视器 .....	71
启用反向代理 .....	72
向现有 PDC 实例添加验证模块 .....	75
禁用浏览器高速缓存 .....	76
允许网关重写所有 URL .....	123
将 URI 映射至规则集 .....	124
指定 MIME 映射 .....	125
指定禁止重写的 URI .....	126
指定默认域 .....	127
启用 MIME 推测 .....	127
分析 URI 映射 .....	128
启用屏蔽 .....	129
指定屏蔽种子字符串 .....	129

指定禁止屏蔽 URI 列表	130
使网关协议与原始 URI 协议相同	131
设置重写器调试级别	132
使用 HTML 属性示例	135
使用 HTML JavaScript 标志示例:	138
使用表单示例	140
使用 Applet 示例	143
使用 JavaScript URL 变量示例	144
使用 JavaScript 表达式变量示例	147
使用 JavaScript DHTML 变量示例	150
使用 JavaScript DJS 变量示例	153
使用 JavaScript 系统变量示例	155
使用 JavaScript URL 函数示例	157
使用 JavaScript 表达式函数示例	158
使用 JavaScript DHTML 函数示例	161
使用 JavaScript DJS 函数示例	163
使用 XML 属性示例	165
配置 OWA 规则集	171
为组织与用户启用 NetFile	175
启用 Unix 验证	176
配置 Unix 验证	176
在添加规则之后运行 Netlet	193
为 PDC 配置 Netlet	203
在安装后生成自签名证书	213
生成 CSR	216
添加根 CA 证书	218
从 CA 订购证书	219
安装来自 CA 的证书	220
删除证书	221
修改证书的委托属性	223
查看根 CA 的列表	224
列出所有证书	226
打印证书	227
配置 URL 访问控制	229
设置拒绝的 URL 列表	230
设置允许的 URL 列表	230
禁用主机的单点登录	231

启用每一会话的单个登录 .....	232
指定验证级别 .....	232
配置网关属性 .....	233
将网关配置为在 HTTP 或 HTTPS 模式运行 .....	235
启用“重写器代理”和创建“重写器代理”列表 .....	236
启用 Netlet .....	237
启用“Netlet 代理”和创建“Netlet 代理”列表 .....	238
启用 Proxylet .....	238
启用 Cookie 管理 .....	239
启用 HTTP 基本验证 .....	241
启用持久性 HTTP 连接 .....	241
指定每个持久性连接的最大请求数量 .....	242
指定持久套接字连接超时 .....	242
指定周转时间的超时 .....	243
添加转发 Cookie URL .....	245
指定最大连接队列长度 .....	245
指定网关超时 .....	246
指定线程池容量最大值 .....	247
指定高速缓存套接字超时 .....	247
指定 Portal Server .....	248
指定 Portal Server 重试间隔 .....	249
存储外部服务器 Cookie .....	250
从 URL 获取会话 .....	250
将 Cookie 标记为安全 .....	251
启用“使用网络代理” .....	252
指定 Webproxy 的 URL .....	253
指定不使用代理的 URL .....	253
指定域和子域的代理 .....	254
指定代理口令 .....	255
启用自动代理配置支持 .....	256
指定自动代理配置文件位置 .....	256
通过网络代理启用隧道 Netlet .....	257
指定非验证 URL 路径 .....	258
将网关添加到“已启用证书的网关主机”列表 .....	259
允许 40 位加密连接 .....	260
启用 SSL 2.0 版本 .....	260
启用“单个密码选择” .....	261

启用 SSL 3.0 版本 .....	261
启用空密码 .....	262
创建信任的 SSL 域列表 .....	263
配置 PDC 和编码设备 .....	264
允许网关重写所有 URL .....	267
将 URI 映射至规则集 .....	269
配置 OWA 规则集 .....	270
指定 MIME 映射 .....	271
指定默认的域和子域 .....	272
指定默认的域和子域 .....	272
启用 MIME 推测 .....	273
分析 URI 映射 .....	274
启用屏蔽 .....	274
指定屏蔽种子字符串 .....	275
指定禁止屏蔽 URI .....	275
使网关协议与原始 URI 协议相同 .....	276
启用网关日志 .....	277
启用 Netlet 日志 .....	279
配置 NetFile 属性 .....	281
指定 OS 字符集 .....	282
指定主机侦测顺序 .....	283
配置公共主机列表 .....	285
指定默认域 .....	286
指定默认 Windows 域或工作组 .....	287
指定默认 WINS/DNS 服务器 .....	288
指定对不同类型主机的访问 .....	289
创建允许的主机列表 .....	290
创建拒绝的主机列表 .....	291
启用 / 禁用权限 .....	293
指定 NetFile 窗口的大小 .....	294
指定 NetFile 窗口的位置 .....	295
指定临时目录 .....	296
设置文件上传大小限制 .....	297
指定搜索目录限制 .....	298
指定默认压缩类型 .....	299
指定 MIME 类型配置文件的位置 .....	300
添加 Netlet 规则 .....	305

修改 Netlet 规则 .....	306
删除 Netlet 规则 .....	307
指定默认密码 .....	308
分配默认回环端口 .....	308
启用连接时重新验证 .....	309
启用连接时弹出警告 .....	309
允许用户禁止端口警告对话框 .....	310
设置保活间隔 .....	311
设置门户注销时终止 Netlet 选项 .....	311
定义 Netlet 访问规则 .....	312
拒绝 Netlet 访问规则 .....	313
允许访问主机 .....	314
拒绝访问主机 .....	315
配置 Proxylet 属性 .....	319
配置 Crypto Accelerator 1000 .....	322
配置 Crypto Accelerator 4000 .....	326
配置外部 SSL 设备加速器 .....	329



# 关于本指南

本指南介绍如何管理 Sun Java™ System Portal Server Secure Remote Access（之前的 Sun ONE™ Portal Server, Secure Remote Access）

Sun Java System Portal Server Secure Remote Access (SRA) 使远程用户可通过 Internet 安全地访问其组织的网络及网络服务。此外，可为贵组织提供一个安全的 Internet 门户，从而使所有目标观众 - 雇员、商业合作伙伴以及普通公众能够访问其内容、应用程序和数据。

SRA 在 Solaris™ 8.0 及 9.0 操作系统中运行。本指南包含配置及管理 SRA 的说明。

本“前言”包括以下部分：

- [哪些人应阅读本指南](#)
- [您需要了解哪些内容](#)
- [本书的组织结构](#)
- [本指南所使用的文档约定](#)
- [在何处查找相关信息](#)
- [在哪里可找到本在线指南](#)

## 哪些人应阅读本指南

本指南假定您是网络或系统管理员，有管理 UNIX® 系统及 TCP/IP 网络的经验。您负责安装、配置及管理 SRA。

要安装 SRA 的各种组件，需要对所需机器进行根访问。您还需要所需的管理权限以执行其他其他操作，如配置用户和服务。

## 您需要了解哪些内容

在管理 SRA 之前，您需要熟悉以下内容：

- Solaris 的基本管理步骤
- LDAP
- Sun Java™ System Directory Server
- Sun Java™ System Web Server
- Sun Java™ System Portal Server

您还需具备下列能力以编写“重写器”规则：

- 了解 HTML 及 HTML 标记
- 精通 JavaScript
- XML 的基本知识

## 本书的组织结构

本书包括以下各章及附录：

关于本指南（本章）

第 1 章，“[Portal Server Secure Remote Access 简介](#)”

本章介绍 SRA 以及 Sun Java™ System Portal Server 产品与 SRA 组件之间的关系。它同时提供管理和配置 SRA 的信息。

第 2 章 “[网关](#)”

本章介绍顺利运行“网关”所需的“网关”相关概念及信息。

第 3 章 “[Proxylet 和重写器](#)”

本章介绍 Proxylet 和“重写器”。对于“重写器”，本章将提供其规则示例及最佳作法。

第 4 章 “[NetFile](#)”

本章介绍 NetFile 并对其操作进行说明。

第 5 章 “[Netlet](#)”

本章介绍如何使用 Netlet 在用户远程标准“门户桌面”与内部网内联网中正运行应用程序的服务器之间安全地运行应用程序。

## 第 6 章 “具有 PDC 的 Netlet”

本章介绍如何配置客户机浏览器的 Java Plugin 插件，以使 Netlet 能够与 PDC 一起使用。

## 第 7 章 “证书”

本章介绍证书管理并说明如何安装自签名证书或来自“证书授权机构”的证书。

## 第 8 章 “配置 URL 访问控制”

本章介绍如何允许或拒绝最终用户通过网关对特定 URL 的访问。

## 第 9 章 “配置网关”

本章介绍如何通过 Sun Java™ System Identity Server 管理控制台配置“网关”属性。

## 第 10 章 “配置 NetFile”

本章介绍如何通过 Sun Java™ System Identity Server 管理控制台配置 NetFile。

## 第 11 章 “配置 Netlet”

本章介绍如何通过 Sun Java™ System Identity Server 管理控制台配置 Netlet 属性。

## 第 12 章 “配置 Proxylet”

本章介绍如何通过 Sun Java™ System Identity Server 管理控制台配置 Proxylet。

## 第 13 章 “配置 SSL 加速器”

本章介绍如何为 Portal Server Secure Remote Access 配置各种加速器。

## 附录 A “日志文件”

本附录列出了所有 Portal Server Secure Remote Access 日志文件及其说明。

## 附录 B “配置属性”

本附录列出了用户在 Sun Java™ System Identity Server 管理控制台中需为 Portal Server Secure Remote Access 设置的属性。

## 附录 C “国家代码”

本附录列出了需在证书管理期间指定的两字母国家代码。

## 术语表

本术语表包含到 Sun Java System 的全局术语表的链接。

# 本指南所使用的文档约定

## 等宽字体

计算机屏幕上显示的所有文本或应键入的文本均采用等宽字体。文件名、区别名、函数和示例亦采用等宽字体。

## 斜体字体

*斜体字体*用于表示使用安装过程中专用的信息输入的文本（例如，变量）。它用于服务器路径、名称和帐户 ID。

## 方括号

方括号 [] 用于将可选参数括在其中。例如，在本文档中您将看到 `xx` 命令的如下用法：

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

出现的 [options]、[arguments] 和 [component] 表明存在可以添加到 `xx` 命令中的可选参数。

## 命令行提示符

示例中未显示命令行提示符（例如，C shell 的 % 表示 C shell，K shell 或 B shell 的 \$ 表示 K shell 或 B shell）。根据所使用的操作系统环境的不同，您将会看到各种不同的命令行提示符。但是，除非另有特殊说明，否则应按命令在文档中出现的形式输入。

## 在何处查找相关信息

### SRA 文档

下面列出的是附加其他 SRA 文档。

- *Portal Server Secure Remote Access 属性联机帮助*
- *Portal Server Secure Remote Access Netlet 联机（客户机）帮助*
- *Portal Server Secure Remote Access NetFile Java1 联机（客户机）帮助*
- *Portal Server Secure Remote Access NetFile Java2 联机（客户机）帮助*
- *Portal Server Secure Remote Access Proxylet 联机（客户机）帮助*

### Portal Server 文档

全套 Sun Java™ System Portal Server 文档还包括下列几项：

- *Portal Server 管理指南*
- *Portal Server Migration Guide*
- *Portal Server Desktop Customization Guide*
- *Portal Server Developer's Guide*

### 本指南中引用的文档

本指南中引用的其他其他文档：

- *Identity Server 管理指南*
- *Sun Crypto Accelerator 1000 Board Installation and User's Guide*

本指南位于：

<http://www.sun.com/products-n-solutions/hardware/docs/pdf/816-2450-11.pdf>

## 相关第三方站点引用

您可从访问 <http://docs.sun.com> 站点在线访问查看 Sun 技术文档。您可以浏览档案归档文件或搜索指定的书籍标题或主题。

---

### 注意

对于本文档中所提及的第三方 Web 站点，Sun 不负责其可用性。此类站点或资源直接或间接提供的的任何内容、广告、产品或其他资料未经 Sun 正式认可，Sun 对此不负任何责任。对于因使用或信任此类站点或资源提供的任何内容、商品或服务，而直接或间接造成任何实际或所谓的损害或损失，Sun 概不负责。

---

## 在哪里可找到本在线指南

您可访问 <http://docs.sun.com> 站点，在线访问查看 Sun 技术文档。您可以浏览档案归档文件或搜索指定的书籍标题或主题。

# Portal Server Secure Remote Access 简介

本章介绍 Sun Java™ System Portal Server Secure Remote Access（之前的 Sun ONE™ Portal Server, Secure Remote Access）以及 Sun Java™ System Portal Server (Portal Server) 软件与 Sun Java System Portal Server Secure Remote Access (SRA) 组件之间的关系。

本章包括以下主题：

- [SRA 软件概述](#)
- [SRA 服务](#)
- [管理 SRA 产品](#)
- [配置 SRA 属性](#)
- [支持的应用程序](#)

## SRA 软件概述

SRA 软件使远程用户可通过 Internet 安全地访问其组织的网络及网络服务。此外，可为贵组织提供一个安全的 Internet 门户，从而使所有目标观众 - 雇员、商业合作伙伴以及普通公众能够访问其内容、应用程序和数据。

SRA 软件可提供对门户内容和服务的基于浏览器的安全远程访问（自任一远程设备）。它是一种节省成本的安全访问解决方案，用户可从任意设备通过启用了 Java 技术的浏览器对其进行访问，从而省去了对客户机软件的需要。与 Portal Server 的集成可确保用户对具有访问许可权的内容和服务进行安全加密式的访问。

SRA 软件所面向的目标是那些部署高度安全的远程访问门户的企业。这些门户强调安全、保护性以及内部网资源的保密性。SRA 体系结构非常适合此类门户的要求。SRA 软件使用户能够通过 Internet 安全地访问内部网资源，同时不将这些资源在 Internet 上公开。

驻留在“隔离区”(DMZ)的网关可提供对全部的内部网 URL、文件系统及应用程序的单个安全访问点。其他所有非 SRA 的服务(如“会话”、“验证”和标准“门户桌面”)均驻留在安全内部网中 DMZ 的后面。从客户机浏览器到网关的通信采用 HTTPS 进行加密。从网关到服务器和内部网资源的通信既可以是 HTTP，也可以是 HTTPS。

SRA 软件使用两种方法

Netlet applet 和 NetFile applet 会被下载到客户机中，而支持文件可驻留在网关上，也可驻留在 Portal Server 主机上。

Portal Server 可在以下两种模式下工作：

- 开放模式
- 安全模式

## 开放模式

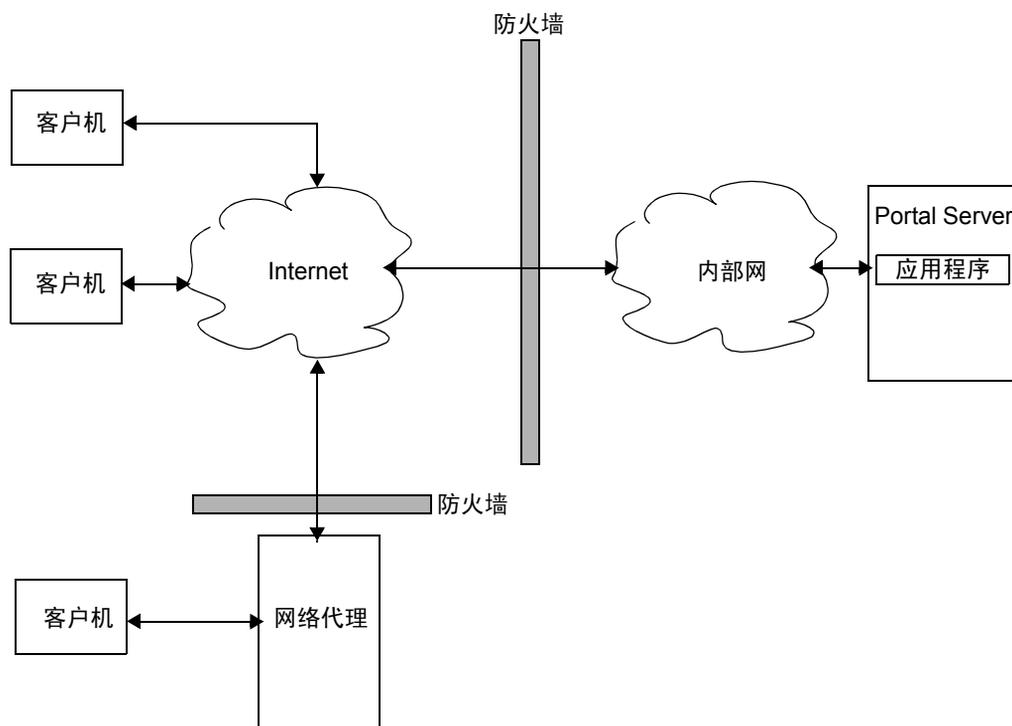
在开放模式中，安装 Portal Server 时不带 SRA 软件。尽管在此模式下 HTTPS 通信仍可进行，但无法实现安全远程访问。这就意味着用户不能访问安全的远程文件系统和应用程序。

开放门户和安全门户的主要区别是，由开放门户提供的服务通常驻留在隔离区(DMZ)内，而不是驻留在安全的内部网中。DMZ 是公共 Internet 和专用内部网之间的一个小型受保护网络，通常在其两端以防火墙来划界。

如果门户不包含敏感信息(部署公用信息和允许访问自由应用程序)，则对大量用户所发出的访问请求的响应速度比使用安全模式更快。

图 1-1 显示开放模式下的 Portal Server。在此，Portal Server 被安装在防火墙后的单台服务器上。多台客户机穿过单面防火墙在 Internet 上访问 Portal Server。

图 1-1 开放模式下的 Portal Server



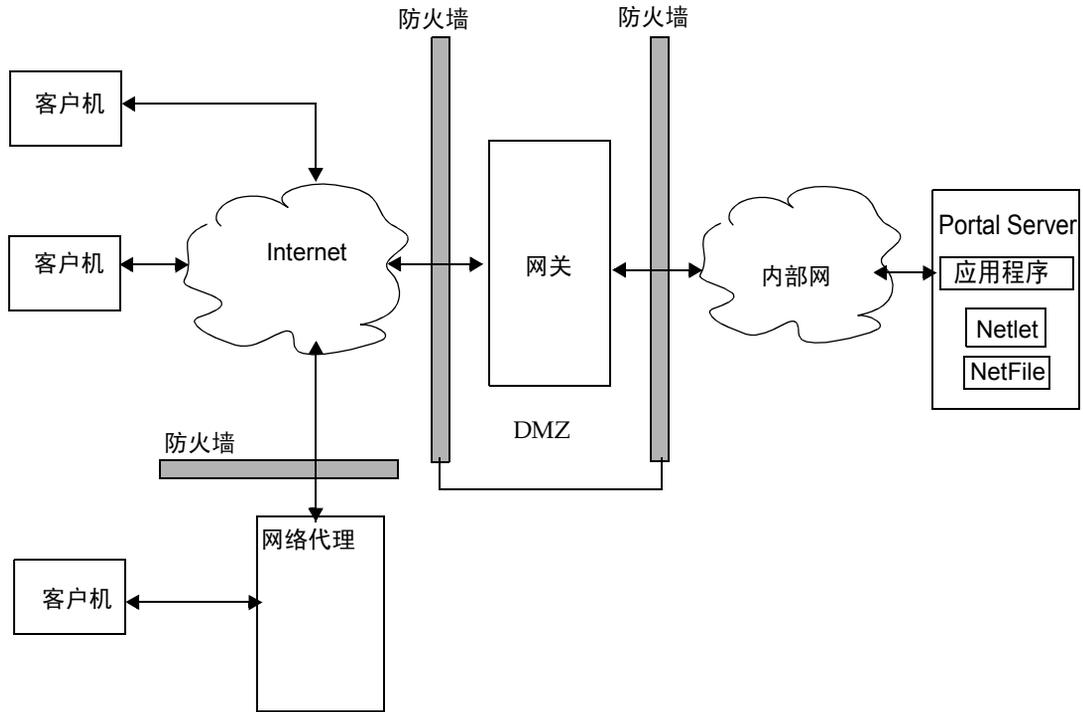
## 安全模式

安全模式可使用户对所需的内部网文件系统和应用程序进行安全远程访问。

网关驻留在隔离区 (DMZ) 内。网关可提供对所有内部网 URL 和应用程序的单个安全访问点，这便减少了防火墙中要打开端口的数目。其他所有 Portal Server 服务（如“会话”、“验证”和标准“门户桌面”）均驻留在安全内部网中 DMZ 的后面。从客户机浏览器到网关的通信采用“安全套接字层” (SSL) 基础之上的 HTTP 进行加密。从网关到服务器和内部网资源的通信既可以是 HTTP，也可以是 HTTPS。

图 1-2 显示具有 SRA 软件的 Portal Server。SSL 用于在 Internet 上加密客户机和网关之间的连接。SSL 也可用于加密网关与服务器之间的连接。在内部网和 Internet 之间出现的网关使客户机和 Portal Server 之间的安全路径得到延伸。

图 1-2 安全模式下的 Portal Server（具有 SRA 软件）



可添加附加服务器和网关以用于站点扩充。根据业务需要，可通过多种方式配置 SRA 软件。

## SRA 服务

SRA 软件有五个主要组件：

- [网关](#)
- [重写器](#)
- [NetFile](#)
- [Netlet](#)
- [Proxylet](#)

## 网关

SRA 网关在源自 **Internet** 与公司内部网的远程用户会话之间提供界面和安全屏障。网关可通过单个接口将来自内部 **Web** 服务器和应用程序服务器的内容安全地呈现给远程用户。

**Web** 服务器使用基于网络的资源（如 **HTML**、**JavaScript** 和 **XML**）在客户机和网关之间进行通信。重写器是一个网关组件，用于使网络内容变为可用。

应用程序服务器使用二进制协议（如 **telnet** 和 **FTP**）在客户机和网关之间通信。驻留在网关上的 **Netlet** 便是针对此目的而应用的。有关详细信息，请参阅第 2 章“[网关](#)”。

## 重写器

重写器使最终用户可以浏览内部网，并使这些页上的链接和其他 **URL** 引用正确运行。重写器会预先考虑网络浏览器位置字段中的“网关 **URL**”，从而通过网关重定向内容请求。有关详细信息，请参阅第 3 章“[Proxylet 和重写器](#)”。

## NetFile

**NetFile** 是一个文件管理器应用程序，它允许对文件系统和目录进行远程访问和操作。**NetFile** 包括 **NetFile Java™**（**Java** 的用户界面）。它可用于 **Java 1** 和 **Java 2**。详细信息请参阅第 4 章“[NetFile](#)”。

## Netlet

**Netlet** 有利于以安全方式在远程桌面上运行常用的或公司特定的应用程序。在您的站点实现 **Netlet** 后，用户可安全地运行公共 **TCP/IP** 服务（如 **Telnet** 和 **SMTP**）及基于 **HTTP** 的应用程序（如 **pcANYWHERE** 或 **Lotus Notes**）。有关详细信息，请参阅第 5 章“[Netlet](#)”。

## Proxylet

Proxylet 是一个在客户机上运行的动态代理服务器。Proxylet 将 URL 重定向到网关。它通过阅读和修改客户机上浏览器的代理设置以使其指向本地代理服务器或 Proxylet 来完成这项工作。

## 管理 SRA 产品

SRA 软件有两个用于管理的界面：

- Identity Server 管理控制台
- 命令行

大多数管理任务都是通过基于网络的 Sun Java System Identity Server 管理控制台执行的。管理控制台可通过网络浏览器进行本地或远程访问。但是，某些任务（如文件修改）必须通过 UNIX 命令行界面进行管理。

## 配置 SRA 属性

您可在组织级、角色级和用户级配置与 SRA 有关的属性，以下情况除外：

- 不能在用户级设置“冲突解决级别”。同样在“服务配置”选项卡中也不提供该项。请参阅第 35 页的“设置冲突解决”。
- 只能在组织级别设置“MIME 类型配置文件定位”属性。请参阅第 302 页的“指定 MIME 类型配置文件位置”。

在组织级设置的值将由该组织以下的所有角色和用户继承。在用户级设置的值会覆盖在组织级或角色级设置的相应值。

大多数属性可在 Identity Server 选项卡中进行设置，也可在 Identity Server 上的“服务配置”选项卡中进行设置。在“服务配置”级设置的属性会用作模板。默认情况下，所创建的任何组织或用户均会继承这些值。

您可在“服务配置”级对属性值进行更改。只有添加了新的组织后，才反映这些新的属性值。在“服务配置”选项卡中对属性值所作的更改不会影响现有的组织或用户。有关详细信息，请参阅《*Identity Server 管理指南*》。

您可在“SRA 配置”下的 Identity Server 管理控制台中使用以下服务配置 SRA 属性：

- 访问列表

此服务可使您准许或限制对特定 URL 的访问，并可管理单点登录功能。有关详细信息，请参阅第 8 章“配置 URL 访问控制”。

- 网关

此服务允许您配置所有与网关相关的属性，如代理管理、cookie 管理、日志、重写器管理和密码。有关详细信息，请参阅第 9 章“配置网关”。

- NetFile

此服务允许您配置所有与 NetFile 相关的属性，如公共主机、MIME 类型，以及对不同类型主机的访问。有关详细信息，请参阅第 10 章“配置 NetFile”。

- Netlet

此服务允许您配置所有与 Netlet 相关的属性，如 Netlet 规则、对所需规则的访问、组织和主机，以及默认算法。有关详细信息，请参阅第 11 章“配置 Netlet”。

- Proxylet

此服务允许您配置与 Proxylet 相关的属性，如 Proxylet Applet 绑定 IP 地址及端口号。有关详细信息，请参阅第 12 章“配置 Proxylet”。

---

**警告**

网关不会收到有关在其运行期间对属性所作更改的通知。

重启网关以确保网关使用已更新的配置文件属性（属于网关或任何其他服务）。请参阅第 76 页的“使用验证链”。

---

# 设置冲突解决

## ► 设置冲突解决级别

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 从“查看”下拉列表中选择“服务”。
6. 单击“SRA 配置”下方相应服务（访问列表、NetFile 或 Netlet）旁的箭头。
7. 从“冲突解决级别”字段下拉列表中选择所需的级别。
8. 单击 NetFile 页顶部或底部的“保存”，记录此项更改。

# 支持的应用程序

SRA 软件支持下列应用程序：

- SRA 软件支持安装 Outlook Web Access (OWA) 的 MS Exchange 2000 SP3 和 MS Exchange 2003。  
OWA 页所需的规则集已按名称 `exchange_2003_owa_ruleset` 以非标准方式安装。要查看 OWA 的实例研究，请参阅第 272 页的“[Outlook Web Access 规则集](#)”。
- iNotes - Notes 5.0.11
- 日历 - Sun ONE 日历服务器 5.1.1 版及更高版本
- Messenger Express - iPlanet Messaging Server 5.2 及更高版本

支持的应用程序

本章介绍顺利运行网关所需的网关相关概念及信息。有关配置网关的信息，请参阅第 9 章“配置网关”。

本章包括以下主题：

- 网关概述
- 创建网关配置文件
- 了解 `platform.conf` 文件
- 运行 `chroot` 环境中的网关
- 在 `chroot` 环境重新启动网关
- 创建网关的多个实例
- 启动和停止网关
- 重新启动网关
- 指定虚拟主机
- 指定联系 Identity Server 的代理
- 使用网络代理
- 使用自动代理配置
- 使用 Netlet 代理
- 使用重写器代理
- 与网关一起使用反向代理
- 获取客户机信息
- 使用验证链

- [使用通配符证书](#)
- [禁用浏览器高速缓存](#)
- [自定义网关服务用户界面](#)
- [使用联合管理](#)

## 网关概述

网关在源自 **Internet** 与公司内联网的远程用户会话之间提供界面和安全屏障。网关可通过单个接口将来自内联网服务器和应用程序服务器的内容安全地呈现给远程用户。

## 创建网关配置文件

网关配置文件含有与网关配置相关的所有信息，诸如网关侦听所在端口、SSL 选项及代理选项。

安装网关时，如果选择缺省值，就会创建一个名为 “**default**” 的缺省网关配置文件。与缺省配置文件相对应的配置文件位于：

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

其中 `/etc/opt/SUNWps` 是所有 `platform.conf.*` 文件的缺省位置。

有关 `platform.conf` 文件内容的详细信息，请参阅第 40 页的 “[了解 platform.conf 文件](#)”。

您可以：

- 创建多个配置文件、定义每个配置文件的属性，并根据需要将这些配置文件分配给不同的网关。
- 将单个配置文件分配给在不同机器上安装的网关。

- 将不同的配置文件分配给在同一机器上运行的单个网关实例。

---

**警告** 不要将同一配置文件分配给在同一机器上运行的不同网关实例。由于端口号相同，这会导致冲突。

不要在为同一网关创建的不同配置文件中指定相同的端口号。运行具有相同端口的同一网关的多个实例将导致冲突。

---

## ► 创建网关配置文件

1. 以管理员身份登录到 Sun Java™ System Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。

网关页出现在右侧窗格中。

4. 单击“新建”。

显示“创建新网关配置文件”页。

5. 输入新网关配置文件的名称。
6. 从下拉列表中选择用于创建新配置文件的配置文件。

缺省情况下，您创建的任何新配置文件都基于预封装的缺省配置文件。如果已创建一个自定义配置文件，则可以从下拉列表中选择该配置文件。新配置文件会继承所选配置文件的全部属性。

7. 单击“创建”。

新配置文件创建完成并返回到网关页，该页将列出新配置文件。

8. 如果要使更改生效，请重新启动使用此网关配置文件的网关：

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

要配置网关，请参阅第 9 章“配置网关”。

# 了解 platform.conf 文件

缺省情况下， platform.conf 文件位于：

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

platform.conf 文件包含网关所需要的详细信息。本部分提供了一个 platform.conf 文件示例，并且描述了所有条目。

在配置文件中包含所有机器特定细节的优势在于：一个通用的配置文件可以被多个机器上运行的各个网关共享。

示例如下：

```
#  
# 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=siroe1.india.sun.com 10.13.147.81  
gateway.virtualhost.defaultOrg=o=root,dc=test,dc=com  
gateway.notification.url=/notification  
gateway.retries=6  
gateway.debug=error  
gateway.debug.dir=/var/opt/SUNWps/debug
```

```

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

```

表 2-1 列出并介绍了 platform.conf 文件中的所有字段。

**表 2-1** platform.conf 文件属性

表项	缺省值	说明
gateway.user	noaccess	以该用户身份运行网关。 必须以 root 用户身份启动网关，在初始化之后将丧失 root 用户权限而成为该用户。
gateway.jdk.dir		这是网关使用的 JDK 目录的位置。
gateway.dsame.agent		这是 Identity Server 的 URL，该服务器是网关启动时为获取其配置文件所联系的服务器。

表 2-1 platform.conf 文件属性

表项	缺省值	说明
portal.server.protocol portal.server.host portal.server.port		这是 Portal Server 缺省安装正在使用的协议、主机和端口。
gateway.protocol gateway.host gateway.port		这是网关的协议、主机和端口。这些值与您在安装期间所指定的模式和端口相同。这些值用于构造通知用的 URL。
gateway.trust_all_server_certs	true	该项指示网关是否必须信任所有服务器证书，或者仅信任那些位于网关证书数据库中的证书。
gateway.trust_all_server_cert_domains	false	只要在网关和服务器间有 SSL 通讯，服务器证书就会被提交至网关。缺省情况下，网关检查服务器主机名是否与服务器证书 CN 相同。 如果该属性值被设为 true，则网关将禁止对所接收的服务器证书进行域检查。
gateway.virtualhost		如果网关机器具有多个已配置的主机名，则可以在此字段中指定一个不同的名称和身份提供者地址。

表 2-1 platform.conf 文件属性

表项	缺省值	说明
gateway.virtualhost.defaultOrg=org		<p>该项指定用户将登录的缺省 <b>Org</b>。</p> <p>例如，假设虚拟主机字段条目如下所示：</p> <pre>gateway.virtualhost=test.com employee.test.com Managers.test.com</pre> <p>而缺省 <b>Org</b> 条目为：</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>用户可以使用 <code>https://manager.test.com</code> 登录到管理人员的 <b>Org</b>，而不是 <code>https://test.com/o=Manager,dc=test,dc=com</code></p> <p>注意：<b>virtualhost</b> 和 <b>defaultOrg</b> 在 <code>platform.conf</code> 文件中区分大小写，但是在 <b>URL</b> 中使用时却不用区分大小写。</p>
gateway.notification.url		<p>网关主机、协议和端口的组合用于构造通知用的 <b>URL</b>。这用于从 <b>Identity Server</b> 接收会话通知。</p> <p>请确保通知用的 <b>URL</b> 与任何组织名称都不相同。如果通知用的 <b>URL</b> 与组织名匹配，则试图连接至该组织的用户就会得到一个空白页，而不是登录页。</p>
gateway.retries		这是启动时网关试图联系 <b>Portal Server</b> 的次数。

表 2-1 platform.conf 文件属性

表项	缺省值	说明
gateway.debug	error	<p>该项可设置网关的调试级别。调试日志文件位于 <i>debug-directory/files</i>。调试文件的位置在 <i>gateway.debug.dir</i> 条目中指定。</p> <p>调试级别为：</p> <p><b>error</b> - 只有严重的错误才会记录到调试文件中。当出现此类错误时，网关通常停止运行。</p> <p><b>warning</b> - 记录警告消息。</p> <p><b>message</b> - 记录所有调试消息。</p> <p><b>on</b> - 在控制台上显示所有调试信息。</p> <p>调试文件为：</p> <p><i>srapGateway.gateway-profile-name</i> - 包含网关调试消息。</p> <p><i>Gateway_to_from_server.gateway-profile-name</i> - 在消息模式中，该文件包含网关和内部服务器间的所有请求和响应报头。</p> <p>要生成该文件，请更改 <i>/var/opt/SUNWps/debug</i> 目录的写权限。</p> <p><i>Gateway_to_from_browser.gateway-profile-name</i> - 在消息模式中，该文件包含网关和客户机浏览器间的所有请求和响应报头。</p> <p>要生成该文件，请更改 <i>/var/opt/SUNWps/debug</i> 目录的写权限。</p>
gateway.debug.dir		<p>这是生成所有调试文件的目录。</p> <p>在 <i>gateway.user</i> 中所提及的用户应当具有足够的权限以便对目录中的文件进行写入操作。</p>
gateway.logdelimiter		当前未使用。

表 2-1 platform.conf 文件属性

表项	缺省值	说明
gateway.external.ip		对于多宿主网关机器（一部机器具有多个 IP 地址），需要在此指定外部 IP 地址。Netlet 使用该 IP 用于运行 FTP。
gateway.certdir		该项指定证书数据库的位置。
gateway.allow.client.caching	true	允许或禁止客户机高速缓存。 如果允许，则客户机浏览器就可以为实现更好的性能而高速缓存静态页和图像（通过已缩减的网络通信量）。 如果禁止，由于在客户机端没有高速缓存任何内容，因此安全性会更高，但是性能会下降，网络负载会更大。
gateway.userProfile.cacheSize		这是在网关获取高速缓存的用户配置文件条目数。如果条目数超过了该值，则会出现频繁重试以便清除高速缓存。
gateway.userProfile.cacheSleepTime		设置清除高速缓存的睡眠时间（以秒为单位）。
gateway.userProfile.cacheCleanupTime		以秒为单位的最大时间，超过该时间后就可以删除一个配置文件条目。
gateway.bindipaddress		在多宿主机器上，这是 IP 地址，网关将其 serversocket 绑定到该地址。要配置网关以侦听所有接口，请替换该 IP 地址使 gateway.bindipaddress=0.0.0.0
gateway.sockretries	3	当前未使用。
gateway.enable.accelerator	false	如果设置为 true，则允许支持外部加速器。
gateway.enable.customurl	false	如果设置为 true，则允许管理员为网关指定一个自定义的 URL 以便将页重写至该 URL。

表 2-1 platform.conf 文件属性

表项	缺省值	说明
gateway.httpurl		输入 HTTP 反向代理 URL，为网关设置一个自定义的 URL，以便将页重写至该 URL。
gateway.httpsurl		输入 HTTPS 反向代理 URL，为网关设置一个自定义的 URL，以便将页重写至该 URL。
gateway.favicon		该项指定一个 URL，网关将对 favicon.ico 文件的请求重定向至该 URL。 这用于 Internet Explore 和 Netscape 7.0 中及更高版本中首选项和收藏的“收藏图标”。 如果留为空白，网关会将一条 404 未找到的消息发送回浏览器。
gateway.logging.password		该字段包含用户“amService-srapGateway”的 LDAP 口令（网关使用它创建应用程序会话）。 该字段既可以是加密文本，也可以是明文。
http.proxyHost		此代理主机用于联系 Portal Server。
http.proxyPort		这是主机用于联系 Portal Server 的端口。
http.proxySet		如果需要代理主机，将此属性设置为 true。如果将该属性设置为 false，则忽略 http.proxyHost 和 http.proxyPort。
portal.server.instance		此特性值是相应的 /etc/opt/SUNWam/config/AMConfig-instance-name.properties 文件。如果此值为缺省值，则它指向 AMConfig-default.properties。
gateway.cdm.cacheSleepTime		Identity Server 将高速缓存的“客户机检测模块”回应发送到网关的超时值。
gateway.cdm.cacheCleanupTime		Identity Server 将高速缓存的“客户机检测模块”回应发送到网关的超时值。

## 运行 chroot 环境中的网关

要在 chroot 环境中提供高安全性，必须使 chroot 目录内容尽可能小。例如，如果存在任何允许用户修改 chroot 目录下文件的程序，则 chroot 将不会阻止攻击者修改服务器 chroot 目录树下的文件。不应当用解释性语言（如 bourne shell、c-shell、korn shell 或 perl 等）编写 CGI 程序，而应使用编译的二进制代码，这样就不需要将解释程序放在 chroot 目录树下。

---

**注意** chroot 环境不支持监视器功能。

---

### ► 安装 chroot

1. 在终端窗口中，以 root 用户身份将下列文件复制到外部源中，例如网络中的计算机、备份磁带或软盘。

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

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

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

2. 在以下目录中运行 mkchroot 脚本：

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

---

**注意** 执行开始后，不能通过按 Ctrl-C 来中断 mkchroot 脚本的执行。

如果执行 mkchroot 脚本期间出现错误事件，请参阅第 49 页的“mkchroot 脚本执行失败”。

---

系统会提示您使用不同的根目录 (new\_root\_directory)。该脚本将创建新目录。

在下面的示例中，/safedir/chroot 就是 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.
```

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

3. 使用以下命令将在 platform.conf 文件中提及的 Java 目录手动安装到 chroot 目录:

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

对于 Solaris 9, 请执行以下命令:

```
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
```

要在系统启动时安装该目录, 请在 /etc/vfstab 文件中添加相应的条目:

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

对于 Solaris 9:

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

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

4. 键入下面的命令以重新启动网关:

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

## mkchroot 脚本执行失败

如果执行 mkchroot 脚本期间出现错误事件, 该脚本会将文件恢复至其初始状态。

在以下示例中, /safedir/chroot 就是 chroot 目录。

如果收到以下错误消息:

不是一次干净的退出

1. 请将在 [安装 chroot](#) 过程的步骤 1 中所备份的文件复制回其原始位置, 并执行以下命令:

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

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

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

2. 删除 /safedir/chroot 目录。

# 在 chroot 环境重新启动网关

只要重新启动网关机器, 就请按照以下步骤在 chroot 环境中启动网关。

## ► 在 chroot 环境中重新启动网关

1. 停止 '/' 目录中运行的网关。

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

2. 启动要从 chroot 目录运行的网关:

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

---

**注意** 需要对 `/safedir/chroot/etc` 文件（例如 `passwd` 和 `hosts`）进行管理（就像管理 `/etc` 文件那样），但是仅包括正在 `chroot` 树中运行的程序所需的主机和帐户信息。

例如，如果更改了系统的身份提供者地址，也要更改文件 `/safedir/chroot/etc/hosts`。

---

## 创建网关的多个实例

使用 `gwmultiinstance` 脚本创建网关的新实例。最好在创建网关配置文件之后再运行该脚本。

1. 以 `root` 用户身份登录并导航到以下目录：

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

2. 运行多实例脚本：

```
./gwmultiinstance
```

**3. 选择以下一个安装选项：**

- 1) 创建新网关实例
- 2) 删除网关实例
- 3) 删除所有网关实例
- 4) 退出

如果选择 1，请回答以下问题：

新网关实例的名称是什么？

新网关实例将使用什么协议？ [https]

新网关实例将监听哪个端口？

Portal Server 的全限定主机名是什么？

应当使用哪个端口访问 Portal Server？

应当使用哪个协议访问 Portal Server？ [http]

Portal Server 部署 URI 是什么？

组织 DN 是什么？ [dc=iportal,dc=com]

Identity Server URI 是什么？ [/amserver]

Identity Server 口令加密密钥是什么？

请提供下列创建自签名证书所需的信息：

您的组织名是什么？

您的部门名是什么？

您所在的城市名或地区名是什么？

您所在州名或省名是什么？

两字母国家代码是什么？

“证书数据库”的口令是什么？ 重试吗？

登录用户的口令是什么？ 重试吗？

是否已在管理控制台创建新的网关配置文件？ [y]/n

安装后启动网关吗？ [y]/n

4. 启动使用新网关配置文件名的新网关实例。

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

其中， *gateway-profile-name* 是新的网关实例。

除创建网关配置文件之外，还应在 `/etc/opt/SUNWam/config` 目录中创建 `AMConfig-instance-name.properties` 文件。

如果 `platform.conf` 文件中存在 `portal.server.instance` 属性，则网关会读取相应的 `AMConfig-instance-name.properties` 文件。如果 `platform.conf` 文件中不存在 `portal.server.instance` 属性，则网关会读取缺省 `AMConfig` 文件 (`AMConfig.properties`)。

## 创建多宿主网关实例

如果您要创建多宿主网关实例（即一个 Portal Server 上多个网关），则必须按以下方式修改 `platform.conf` 文件：

```
gatewaybindipaddress = 0.0.0.0
```

## 使用同一 LDAP 创建网关实例

如果您要创建使用同一 LDAP 的多个网关实例，请在创建第一个网关之后，在所有后续网关上执行以下操作：

在 `/etc/opt/SUNWam/config/` 中，修改 `AMConfig-instance-name.properties` 中的以下内容，以便与安装的第一个网关实例同步：

1. 使用与第一个网关相同的字符串替换用于加密和解密口令的密钥。

```
am.encryption.pwd= string_key_specified_in_gateway-install
```

2. 替换应用程序验证模块的共享密钥

```
com.ipplanet.am.service.secret= string_key_specified_in_gateway-install
```

3. 在 `/etc/opt/SUNWam/config/ums` 中，修改 `serverconfig.xml` 文件中的以下内容，以便与安装的第一个 Portal-Identity Server 实例同步：

```
<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. 重新启动 `amservice` 服务。

## 启动和停止网关

缺省情况下，网关以用户 `noaccess` 启动。

### ► 启动网关

1. 安装网关并创建所需的配置文件之后，请运行下面的命令启动网关：

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

`default` 为安装期间所创建的缺省网关配置文件。可在以后创建自己的配置文件，然后用新的配置文件重新启动网关。请参阅第 38 页的“创建网关配置文件”。

如果有多个网关实例，请使用：

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

此命令可启动在该特定机器上配置的所有网关实例。

---

**注意**      重新启动服务器（已配置网关实例的机器）将重新启动所有已配置的网关实例。

请确保在 `/etc/opt/SUNWps` 目录中没有旧的或者备份的配置文件。

---

2. 运行以下命令，检查网关是否在指定的端口上运行：

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

缺省网关端口为 443。

### ► 停止网关

1. 请使用以下命令停止网关：

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

如果有多个网关实例，请使用：

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

此命令可停止在该特定机器上运行的所有网关实例。

2. 运行以下命令，检查网关进程是否已停止：

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

## 重新启动网关

通常，您无需重新启动网关。仅当发生以下任何事件时，才需要重新启动网关：

- 已创建一个新的配置文件并且需要将新配置文件分配给网关。
- 已修改现有配置文件中的某些属性并要使更改生效。

### ► 用不同的配置文件重新启动网关

重新启动网关：

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

### ► 重新启动网关

在终端窗口中，以超级用户 (root) 身份连接并执行以下步骤之一：

- 启动监视器进程：

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

此操作将在当前处于活动状态的 `crontab` 和监视器进程中创建一个条目。监视器监控正在特定机器上运行的所有网关实例和网关端口，并在网关停机时重新启动它。

### ► 配置网关监视器

可以配置监视器监控网关状态的时间间隔。该时间间隔缺省设置为 60 秒。要更改时间间隔，请在 `crontab` 中编辑以下行：

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

请参阅 `crontab` 的手册页以便配置 `crontab` 条目。

## 指定虚拟主机

虚拟主机是一个指向同一机器 IP 和主机名的附加主机名。例如，如果某一主机名 `a.b.c` 指向主机 IP 地址 `192.155.205.133`，则您可以添加指向同一 IP 地址的另一主机名 `c.d.e`。

### ► 指定虚拟主机

1. 以 `root` 用户身份登录并编辑所需网关实例的 `platform.conf` 文件：

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

2. 添加下列条目：

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

```
gateway.enable.customurl=true （该值缺省设置为 false。）
```

3. 重新启动网关：

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

如果未指定这些值，则网关将设置为缺省值。

## 指定联系 Identity Server 的代理

您可以指定一个主机代理，网关将使用它联系 Portal Server 上部署的“SRA 核心”(RemoteConfigServlet)。网关使用此代理联系 Portal Server 和 Identity Server。

### ► 指定代理

1. 在命令行中编辑以下文件：

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

2. 添加下列条目：

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

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

```
http.proxySet=true
```

3. 重新启动网关以使用指定的代理处理发往服务器的请求。

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

## 使用网络代理

使用第三方的网络代理，可配置用于联系 HTTP 资源的网关。网络代理位于客户机和 Internet 之间。

### 网络代理配置

不同的代理可能用于不同的域和子域。这些条目告诉网关使用哪个代理去联系特定域中的特定子域。在网关中指定的代理配置具有如下功能：

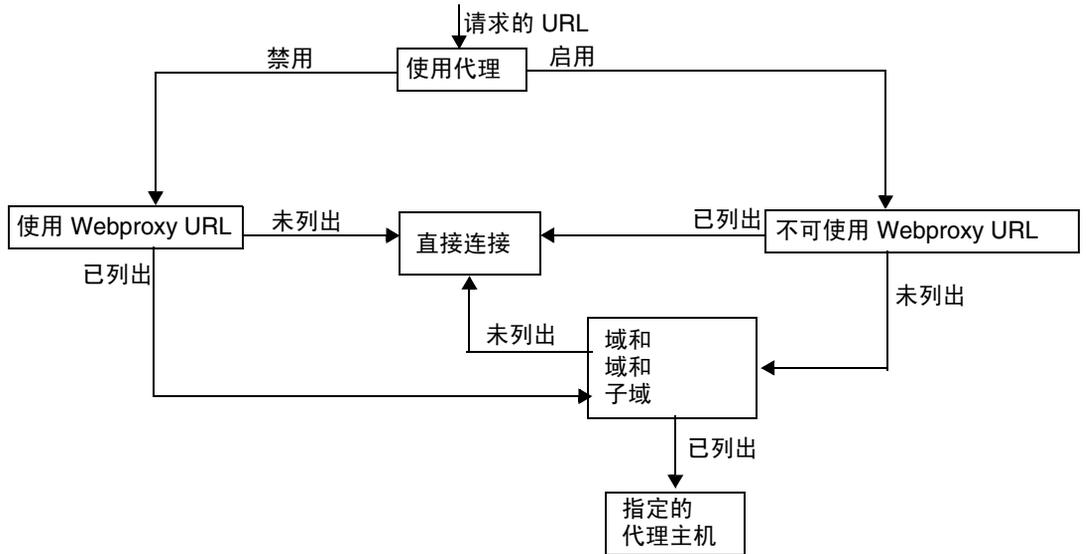
- 创建域和子域列表，同时在网关服务中的“域和子域代理”字段中创建所需的代理。  
有关配置域和子域代理的信息，请参阅第 256 页的“创建域和子域代理列表”。
- 启用“使用代理”选项：
  - 在“域和子域代理”字段中指定的代理被用于指定的主机。
  - 要实现直接连接“域和子域代理”列表中指定的域和子域内的特定 URL，请在“不使用 Web 代理 URL”字段中指定这些 URL。
- 禁用“使用代理”选项：

- 要确保代理被用于在“域和子域代理”字段中指定的域和子域内的特定 URL，请在“使用 WebProxy URL”列表中指定这些 URL。虽然已禁用“使用代理”选项，但是代理仍用于连接在“使用 Webproxy URL”下列出的 URL。这些 URL 的代理从“域和子域代理”列表中获得。

要配置“使用代理”选项，请参阅第 254 页的“启用“使用网络代理””。

图 2-1 显示基于网关服务中的代理配置来分析网络代理信息的方法。

图 2-1 网络代理管理



在图 2-1 中，如果启用“使用代理”，并且请求的 URL 在“不可使用 Webproxy URL”列表中列出，则网关直接连接到目标主机。

如果启用“使用代理”，并且请求的 URL 未在“不可使用 Webproxy URL”列表中列出，则网关通过指定的代理连接到目标主机。如果已经指定代理，则可以在“域和子域代理”列表中查寻。

如果禁用“使用代理”，并且请求的 URL 在“使用 Webproxy URL”列表中列出，则网关使用在“域和子域代理”列表中的代理信息连接到目标主机。

如果禁用“使用代理”，并且请求的 URL 未在“使用 Webproxy URL”列表中列出，则网关直接连接到目标主机。

如果上述条件都无法满足，则不可能进行直接连接，网关显示一条错误信息，说明不可能进行连接。

---

**注意** 如果您正通过标准“门户桌面”的“书签”频道访问 URL，但未满足上述任一条件，则网关将向浏览器发送一条重定向指令。浏览器使用它自己的代理设置访问 URL。

---

### 语法

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

### 示例

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

\* 是一个匹配任何内容的通配符

其中：

sesta.com 是域名而 wp1 是在端口 8080 上用于联系的代理。

red 是子域而 wp2 是在端口 8080 上用于联系的代理。

yellow 是子域。由于没有指定代理，因此使用为域指定的代理，即端口 8080 上的 wp1。

\* 指示对于所有其他子域端口 8080 上都需要使用 wp3。

---

**注意** 如果未指定端口，则缺省使用 8080 端口。

---

## 处理网络代理信息

当客户机试图访问一个特定 URL 时，系统使用“域和子域代理”列表中的条目匹配 URL 中的主机名。要考虑与所请求主机名的最长后缀相匹配的条目。例如，考虑所请求的主机名是 `host1.sesta.com`

- 在“域和子域代理”列表中扫描 `host1.sesta.com`。如果发现匹配的条目，则根据该条目所指定的代理将用于连接该主机。
- 或者，在列表中扫描 `*.sesta.com`。如果找到一个条目，则使用相应的代理。
- 或者，在列表中搜索 `sesta.com`。如果找到一个条目，则使用相应的代理。
- 或者，在列表中搜索 `*.com`。如果找到一个条目，则使用相应的代理。
- 或者，在列表中搜索 `com`。如果找到一个条目，则使用相应的代理。
- 或者，在列表中搜索 `*`。如果找到一个条目，则使用相应的代理。
- 或者，尝试直接连接。

考虑以下“域和子域代理”列表中的条目：

```
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
```

网关在内部将这些条目映射到如表 2-2 所显示的表中。

**表 2-2** 域和子域代理列表中条目的映射

数量	域和子域代理列表中的条目	代理	说明
1	com	p1	如列表中指定。
2	host1.com	p2	如列表中指定。
3	host2.com	p1	由于没有为 host2 指定代理，因此使用域的代理。
4	*.com	p3	如列表中指定。
5	sesta.com	p4	如列表中指定。
6	host5.sesta.com	p5	如列表中指定。
7	*.sesta.com	p6	如列表中指定。
8	florizon.com	直接	有关详细信息，请参阅条目 14 的说明。
9	host6.florizon.com	-	有关详细信息，请参阅条目 14 的说明。
10	abc.sesta.com	p8	如列表中指定。
11	host7.abc.sesta.com	p7	如列表中指定。
12	host8.abc.sesta.com	p8	如列表中指定。
13	*.abc.sesta.com	p9	如列表中指定。对于所有主机（在 abc.sesta.com 域下面的 host7 和 host8 除外），使用 p9 作为代理。
14	host6.florizon.com	p10	此条目与条目 9 相同。条目 9 指示直接连接，但是此条目指示应当使用代理 p10。在有两种条目的情况下（例如此项），具有代理信息的条目被认为是有效的条目。另一个条目将被忽略。
15	host9.sesta.com	p11	如列表中指定。
16	siroe.com	直接	由于没有为 siroe.com 指定代理，因此尝试执行直接连接。
17	host12.siroe.com	p12	如列表中指定。
18	host13.siroe.com	p13	如列表中指定。
19	host14.siroe.com	直接	由于没有为 host14 或 siroe.com 指定代理，因此尝试执行直接连接。

**表 2-2** 域和子域代理列表中条目的映射

数量	域和子域代理列表中的条目	代理	说明
20	*.siroe.com	p14	请参阅表项 23 的说明。
21	host15.siroe.com	p15	如列表中指定。
22	host16.siroe.com	直接	由于没有为 host16 或 siroe.com 指定代理，因此尝试执行直接连接。
23	*.siroe.com	p16	这类似于表项 20。但是指定的代理却不同。在此情况下，无法知道网关的确切行为。可使用两个代理中的任意一个。
24	*	p17	如果没有其他条目与所请求的 URL 匹配，则使用 p17 作为代理。

**注意** 与其使用符号 | 分开“域和子域代理”列表中的代理条目，在列表中拥有单独的条目也许更简单一些。例如，不使用一个条目：

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

可以将其指定为：

```
sesta.com p1
```

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

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

这更容易捕获重复的条目和任何其他多义条目。

### 基于域和子域代理列表进行重写

“重写器”也使用“域和子域代理”列表中的条目。重写器重写所有 URL（它们的域与“域和子域代理”列表中列出的域相匹配）。

**警告** 不会考虑重写“域和子域代理”列表中的 \* 条目。例如，在表 2-2 所提供的示例中，条目 24 就不会被考虑。

有关重写器的信息，请参阅第 3 章 “Proxylet 和重写器”。

### 默认域和子域

当 URL 中的目标主机不是全限定主机名时，缺省的域和子域将用于到达全限定名。

假设管理控制台的 “缺省域” 字段中的值是：

```
red.sesta.com
```

---

**注意** 需要在 “域和子域代理” 列表中具有相应的条目。

---

在上面的示例中，sesta.com 是缺省域而缺省子域是 red。

如果请求的 URL 是 host1，则使用缺省的域和子域将该 URL 解析至 host1.red.sesta.com。随后在 “域和子域代理” 列表中查寻 host1.red.sesta.com。

## 使用自动代理配置

要忽略 “域和子域代理” 列表中的信息，请启用 “自动代理配置” 功能。要配置该功能，请参阅第 258 页的 “启用自动代理配置支持”。

当使用 “代理自动配置” (PAC) 文件时，请注意以下各项：

- js.jar 必须位于网关机器上的 \$JRE\_HOME/lib/ext 目录中，否则网关将不能分析 PAC 文件。
- 启动时，网关从网关配置文件 “自动代理配置文件” 位置字段中所指定的位置获取 PAC 文件。要配置位置，请参阅第 258 页的 “指定自动代理配置文件位置”。
- Portal Server、网关、Netlet、Proxylet 和 Jchardet 使用 Rhino 软件分析 PAC 文件。您可以从 SUNWrhino 软件包安装该软件。

此软件包包含 /usr/share/lib 目录中必须存在的 js.jar 文件。将此目录添加到网关和 Portal Server 机器上的 webserver/appserver 类路径中，否则，Portal Server、网关、Netlet、Proxylet 和 Jchardet 将无法分析 PAC 文件。

- 网关使用 URLConnection API 到达该位置。如果需要将代理配置为到达该位置，则需要按以下方法配置代理。

- a. 在命令行中编辑以下文件：

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

- b. 添加下列条目：

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

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

```
http.proxySet=true
```

- c. 重新启动网关以使用指定的代理：

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

- 如果 PAC 文件初始化失败，则网关使用“域和子域代理”列表中的信息。
- 如果从 PAC 文件返回 ""（空字符串）或“null”，则网关假设该主机不属于内联网。这类似于主机不在“域和子域代理”列表中。

如果要网关使用直接到主机的连接，将返回“DIRECT”。请参阅第 64 页的“返回 DIRECT 或 NULL 的示例”。

- 当指定多个代理时，网关仅使用返回的第一个代理。它不会在为主机指定的各个代理中尝试执行故障切换或负载平衡。
- 网关忽略 SOCKS 代理并且尝试直接连接，并假设主机是内联网的一部分。
- 要指定用于到达任何不属于内联网的主机的代理，请使用代理类型“STARPROXY”。这是 PAC 文件格式的扩展，类似于网关配置文件的“域和子域代理”节中的条目 \*proxyHost:port。请参阅第 64 页的“返回 STARPROXY 的示例”

## PAC 文件用法示例

以下示例显示在“域和子域代理”列表中列出的 URL 及相应的 PAC 文件。

### 返回 DIRECT 或 NULL 的示例

使用这些域和子域代理：

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

相应的 PAC 文件是：

```
// 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
```

### 返回 STARPROXY 的示例

使用这些域和子域代理：

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

相应的 PAC 文件是：

```
// 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

```

在此情况中，如果请求用于 .intranet2.com 域中的主机，则网关将联系 proxy.intranet1.com:8080。如果 proxy.intranet1.com:8080 关机，则请求将失败。网关将不会执行故障切换并联系 proxy1.intranet1.com:8080。

## 使用 Netlet 代理

Netlet 信息包在网关处解码并被发送至目标服务器。然而，网关需要通过隔离区 (DMZ) 和内联网之间的防火墙，才能访问所有的 Netlet 目标主机。这需要在防火墙处打开许多端口。Netlet 代理可于将防火墙中打开的端口数量降至最低。

Netlet 代理通过延展客户机至网关最终至内联网中的 Netlet 代理之间的安全通道，从而增强了网关和内联网之间的安全性。通过使用代理，Netlet 信息包将被代理解码然后发送到目标服务器地。

由于以下原因，Netlet 代理非常有用：

- 添加了额外的安全层。
- 在大规模的部署环境中，通过内部防火墙最小化了来自网关的额外 IP 地址和端口的使用。
- 将网关和 Portal Server 之间的打开端口数限制为 1。该端口数可以在安装期间配置。
- 扩展了客户机和网关之间的安全通道，直到如在图 2-2 的“使用配置的 Netlet 代理”部分中所显示的 Portal Server。通过数据加密 Netlet 代理提供的安全性得到改善，但是可能会增加系统资源的使用量。有关安装 Netlet 代理的信息，请参阅《Sun Java Enterprise System 安装指南》。

您可以：

- 选择在 Portal Server 节点或在单独的节点上安装 Netlet 代理。

- 使用管理控制台安装多个 Netlet 代理并且为单个网关配置这些代理。这有利于负载均衡。有关详细信息，请参阅第 239 页的“启用和创建 Netlet 代理列表”。
- 在单个机器上配置 Netlet 代理的多个实例。
- 将多个网关实例指向单个安装的 Netlet 代理。
- 通过网络代理开通 Netlet 通道。要配置该功能，请参阅第 259 页的“通过网络代理启用 Netlet 隧穿”。

图 2-2 显示三个实现示例：网关以及安装和未安装 Netlet 代理的 Portal Server。组件包括一台客户机、两个防火墙、驻留在两个防火墙之间的网关、Portal Server 和 Netlet 目标服务器。

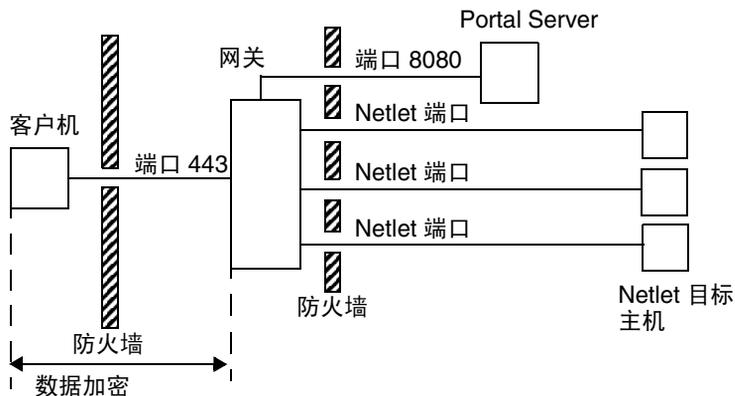
第一种方案显示网关和未安装 Netlet 代理的 Portal Server。在此方案中，数据加密仅从客户机扩展至网关。对于每个 Netlet 连接请求，都会在第二个防火墙中打开一个端口。

第二种方案显示网关和 Portal Server，此时在 Portal Server 上安装了 Netlet 代理。在此情况下，数据加密从客户机一直扩展到 Portal Server。由于所有 Netlet 连接都通过 Netlet 代理路由，因此在第二个防火墙中仅需为 Netlet 请求打开一个端口。

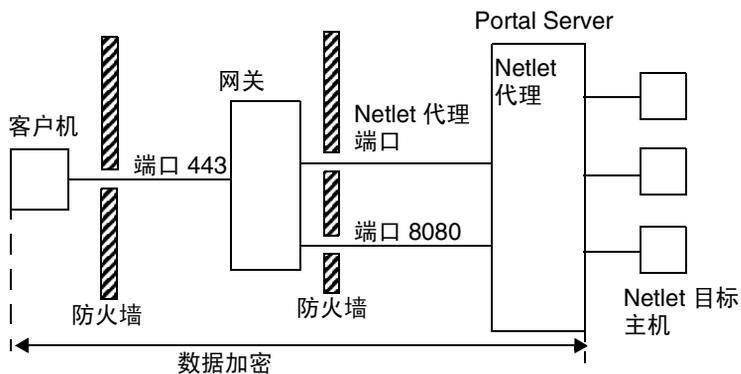
第三种方案显示网关和 Portal Server，以及在单独节点上安装的 Netlet 代理。在单独节点上安装 Netlet 代理将减少 Portal Server 节点上的负载。在此方案中，仅需在第二个防火墙中打开两个端口。一个端口将请求送至 Portal Server，另一个端口将 Netlet 请求发送至 Netlet 代理服务器。

图 2-2 Netlet 代理的实现

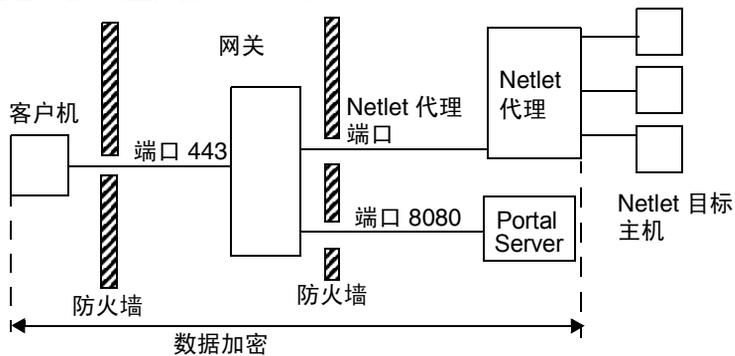
## 未配置 Netlet 代理



## 已在 Portal Server 上安装“Netlet 代理”



## 已在单独节点上安装“Netlet 代理”



## 创建 Netlet 代理的实例

使用 `nlpmultiinstance` 脚本在 Portal Server 节点或单独节点上创建新的 Netlet 代理实例。最好在创建网关配置文件之后再运行该脚本：

1. 以 root 用户身份登录并导航到以下目录：

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

2. 运行多实例脚本：

```
./nlpmultiinstance
```

3. 回答由 `nlpmultiinstance` 脚本提出的问题：

- 新 netlet 代理实例的名称是什么？
- 如果此节点上已配置一个同名的实例，脚本将会询问您是否要为该 Netlet 代理实例使用相同的配置。
- 如果回答是肯定的，请回答以下两个问题：
  - 新 netlet 代理实例将监听哪个端口？
  - 安装后启动 netlet 代理吗？
- 如果回答是否定的，请回答以下问题：
  - 新 netlet 代理实例将使用什么协议？
  - 新 netlet 代理实例将监听哪个端口？
  - 您的组织名是什么？
  - 您的部门名是什么？
  - 您所在的城市名或地区名是什么？
  - 您所在州名或省名是什么？
  - 两字母国家代码是什么？
  - 证书数据库的口令是什么？
  - 登录用户的口令是什么？
  - 是否已在管理控制台创建新的网关配置文件？
  - 如果回答是肯定的，要在安装之后启动 netlet 代理吗？

4. 启动使用所需网关配置文件名的新 netlet 代理实例：

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

其中，*gateway-profile-name* 是与所需网关实例相对应的配置文件名。

## 启用 Netlet 代理

通过 Identity Server 管理控制台中“SRA 配置”下的网关服务可启用 Netlet 代理。请参阅第 239 页的“启用和创建 Netlet 代理列表”。

## 重新启动 Netlet 代理

可将 Netlet 代理配置为只要代理被意外终止就重新启动。可以计划一个监视器进程时间表来监控 Netlet 代理，只要它停止运行就重新启动。

也可以手动重新启动 Netlet 代理。

### ► 重新启动 Netlet 代理

在终端窗口中，以 root 用户身份连接并执行以下步骤之一：

- 启动监视器进程：

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

此操作将在当前处于活动状态的 crontab 和监视器进程中创建一个条目。监视器监控 Netlet 代理端口，只要它停止运行就重新启动。

- 手动启动 Netlet 代理：

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

其中，*gateway-profile-name* 是与所需网关实例相对应的配置文件名。

### ► 配置 Netlet 代理监视器

可以配置监视器监控 Netlet 代理状态的时间间隔。该时间间隔缺省设置为 60 秒。要执行此配置，请在 crontab 中编辑下列行：

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

## 使用重写器代理

重写器代理安装于内联网中。网关会将所有请求转发至网关，“重写器”代理将获取内并将内容返回至网关，网关不会直接尝试检索内容。

使用“重写器”代理有两个优点：

- 如果网关和服务器之间有防火墙，则防火墙只需要打开两个端口 - 一个端口连接网关和“重写器”代理，另一个连接网关和 Portal Server。
- 现在，HTTP 通信在网关和内联网之间是安全的，即使目标服务器仅支持 HTTP 协议（不是 HTTPS）。

如果未指定“重写器”代理，那么当用户试图访问内联网中一台计算机时，网关组件将会直接连接到内联网计算机。

如果您将“重写器”代理用作负载均衡器，请确保“重写器”的 `platform.conf.instance_name` 指向负载均衡器的 URL。同时要确保 Portal Server 列表中已指定负载均衡器主机。

如果您的每个网关实例有多个“重写器”代理实例（无需在门户节点上）。在 `platform.conf` 中，无需为“重写器”代理设置单个端口条目，而是采用 `host-name:port` 的形式输入每个“重写器”代理的详细信息。

## 创建重写器代理的实例

使用 `rwpmultiinstance` 脚本在 Portal Server 节点上创建新的“重写器”代理实例。最好在创建网关配置文件之后再运行该脚本。

1. 以 root 用户身份登录并导航到以下目录：

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

2. 运行多实例脚本：

```
./rwpmultiinstance
```

3. 回答由脚本提出的问题：

- 新重写器代理实例的名称是什么？
  - 如果已在此节点上配置一个同名的重写器代理实例，脚本将会询问您是否要为该重写器代理实例使用相同的配置。
  - 如果回答是肯定的，请回答以下两个问题：
    - 新重写器代理实例将监听哪个端口？
    - 安装后启动重写器代理吗？
  - 如果回答是否定的，请回答以下问题：
    - 新重写器代理实例将使用什么协议？
    - 新重写器代理实例将监听哪个端口？
    - 您的组织名是什么？
    - 您的部门名是什么？
    - 您所在的城市名或地区名是什么？
    - 您所在州名或省名是什么？
    - 两字母国家代码是什么？
    - 证书数据库的口令是什么？
    - 登录用户的口令是什么？
    - 是否已在管理控制台创建新的网关配置文件？
    - 如果回答是肯定的，要在安装之后启动重写器代理吗？
4. 启动使用所需网关配置文件名的新重写器代理实例：
- ```
rewriter-proxy-install-root/SUNWps/bin/rwproxyd -n gateway-profile-name start
```
- 其中， *gateway-profile-name* 是与所需网关实例相对应的配置文件名。

## 启用重写器代理

在 Identity Server 管理控制台中，通过“SRA 配置”下的网关服务启用“重写器”代理。请参阅第 237 页的“启用和创建重写器代理列表”。

## 重新启动重写器代理

可以将“重写器”代理配置为只要代理被意外终止就重新启动。可以计划一个监视器进程时间表来监控“重写器”代理，只要它停止运行就重新启动。

也可以手动重新启动“重写器”代理。

### ► 重新启动重写器代理

在终端窗口中，以 root 用户身份连接并执行以下步骤之一：

- 启动监视器进程：

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

此操作将在当前处于活动状态的 `crontab` 和监视器进程中创建一个条目。监视器监控端口，只要它停止运行就重新启动代理。

- 手动启动：

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

其中，`gateway-profile-name` 是与所需网关实例相对应的配置文件名。

### ► 配置重写器代理监视器

可以配置监视器监控“重写器”代理状态的时间间隔。该时间间隔缺省设置为 60 秒。要执行此配置，请在 `crontab` 中编辑下列行：

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

## 与网关一起使用反向代理

代理服务器将 Internet 内容传送至内联网，而反向代理将内联网内容传送至 Internet。可将反向代理的部署配置为传送 Internet 内容，以实现负载均衡和高速缓存。

如果部署中网关前面有第三方反向代理，必须用反向代理的 URL 重写响应内容，而不是网关的 URL。对此，需要进行下列配置。

### ► 启用反向代理

1. 以 root 用户身份登录并编辑所需网关实例的 platform.conf 文件：

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

2. 添加下列条目：

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

```
gateway.enable.customurl=true （该值缺省设置为 false。）
```

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

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

gateway.httpurl 将用于重写对在某端口所接收请求的响应，该端口在网关配置文件中列为 HTTP 端口。

gateway.httpsurl 将用于重写对在某端口所接收请求的响应，该端口在网关配置文件中列为 HTTPS 端口。

3. 重新启动网关：

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

如果未指定这些值，则网关将设置为缺省值。

## 获取客户机信息

当网关将客户机请求转发至任何内部服务器时，它将 HTTP 报头添加到 HTTP 请求中。可以使用这些报头来获取额外的客户机信息并检测网关是否存在。

要查看 HTTP 请求报头，请将 platform.conf 文件中的条目设置为 gateway.error=message，然后使用来自 servlet API 的 request.getHeader()。下表列出了 HTTP 报头中的信息

**表 2-3** HTTP 报头中的信息

| 报头        | 语法                                      | 说明                                                                                                                                                                                                                                                                              |
|-----------|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PS-GW-PDC | X-PS-GW- PDC:true/false                 | 指示是否已在网关启用 PDC。                                                                                                                                                                                                                                                                 |
| PS-Netlet | X-PS-Netlet:enabled=true/false          | 指示网关是否已启用或禁用 Netlet。<br>如果已启用，则加密选项被填充，指示网关是以 HTTPS (encryption=ssl) 模式运行还是以 HTTP 模式 (encryption=plain) 运行<br>例如：<br>PS-Netlet:enabled=false<br>Netlet 已禁用。<br>PS-Netlet:enabled=true; encryption=ssl<br>Netlet 已启用，网关以 SSL 模式运行。<br>当未启用 Netlet 时， encryption=ssl/plain 不会被填充。 |
| PS-GW-URL | X-PS-GW-URL:http(s)://gatewayURL(:port) | 指示客户机连接的 URL。<br>如果它是非标准端口（即网关处于 HTTP/HTTPS 模式而端口不是 80/443），则 ":port" 也被填充。                                                                                                                                                                                                     |

表 2-3 HTTP 报头中的信息

| 报头                  | 语法                                                   | 说明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PS-GW-Rewriting-URL | X-PS-GW-URL:http(s)://gatewayURL(:port)[SessionInfo] | <p>指示网关将全部页重写至的 URL。</p> <ol style="list-style-type: none"> <li>当浏览器支持 <b>cookie</b> 时，该报头的值与 PS-GW-URL 报头相同。</li> <li>当浏览器不支持 <b>cookie</b> 时： <ul style="list-style-type: none"> <li>如果目标主机列于“用户会话 <b>Cookie</b> 被转发到的用户会话”字段中，则该值是网关将要重写页的实际 URL（其中包括已编码的 <b>SessionID</b> 信息）。</li> <li>如果目标主机未列于“用户会话 <b>Cookie</b> 被转发到的用户会话”字段中，则 <b>SessionInfo</b> 字符串将为 “<b>\$SessionID</b>”</li> </ul> </li> </ol> <p>注意：作为响应的一部分，如果用户的 <b>Identity Server</b> 的 <b>sessionId</b> 发生变化（就像来自验证页的响应一样），则使用该值重新写入页（而不是先前在报头中所指示的值）。</p> <p>例如：</p> <ul style="list-style-type: none"> <li>如果浏览器支持 <b>cookie</b>：<br/>PS-GW-Rewriting-URL:https://siroe.india.sun.com:10443/</li> <li>如果浏览器不支持 <b>cookie</b>，但是端服务器列于“用户会话 <b>Cookie</b> 被转发到的用户会话”字段中。<br/>PS-GW-Rewriting-URL:https://siroe.india.sun.com:10443/SessionID/alCustomEncodedValue/</li> <li>如果浏览器不支持 <b>cookie</b> 且端服务器未列于“用户会话 <b>Cookie</b> 被转发到的用户会话”字段中。<br/>PS-GW-Rewriting-URL:https://siroe.india.sun.com:10443/\$SessionID</li> </ul> |
| PS-GW-ClientIP      | X-PS-GW-ClientIP:IP                                  | <p>这是网关从 <code>receivedSocket.getNetAddress().getHostAddress()</code> 获取的 IP。</p> <p>如果客户机直接连接至网关，这可提供客户机的 IP。</p> <p>注意：由于 JSS/NSS 的错误，该功能目前尚不可用。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## 使用验证链

验证链在整个常规验证机制中提供了高级别安全。可用多个验证机制验证用户。

这里所描述的过程仅用于在网关同时启用验证链和“个人数字证书”(PDC)验证。有关在网关启用验证链(但不启用PDC验证)的信息,请参阅《*Identity Server 管理指南*》。

例如,如果您将PDC、Unix和Radius验证模块链接在一起,用户则将不得不通过全部三个模块的验证以便访问标准“门户桌面”。

---

**注意** 如果启用PDC,则它总是为用户验证的第一个验证模块。

---

### ► 向现有PDC实例添加验证模块

1. 以管理员身份登录到Identity Server管理控制台。
2. 选择所需的组织。
3. 在“查看”下拉菜单中选择“服务”。  
服务显示在左侧窗格中。
4. 单击“验证配置”旁的箭头。  
显示“服务实例列表”。
5. 单击gatewaypdc。  
显示Gatewaypdc特性页。
6. 单击“验证配置”前的“编辑”。  
显示“添加模块”。
7. 选择“模块名称”并将“标志”设置为“必填”。选项可以为空。
8. 单击“确定”。
9. 添加一个或多个模块之后,单击“保存”。
10. 单击gatewaypdc特性页中的“保存”。
11. 要使更改生效,需要重新启动网关:

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

## 使用通配符证书

通配符证书接受具有主机名的全限定 DNS 名中通配符的单个证书。

这允许证书保护相同域内的多个主机。例如，`*.domain.com` 的证书可用于 `abc.domain.com` 和 `abc1.domain.com`。事实上，该证书对于 `domain.com` 域中的任何主机都有效。

您需要在全限定主机名中指定一个 `*`。例如，如果全限定主机名是 `abc.florizon.com`，则将其指定为 `*.florizon.com`。现在，生成的证书对 `florizon.com` 域中的所有主机名都有效。

## 禁用浏览器高速缓存

由于网关组件为来自任何位置且仅使用网络浏览器的用户提供对后端公司数据的安全访问，因此可能必须禁止客户机在本地对信息进行高速缓存。

通过修改特定网关的 `platform.conf` 文件中的属性，可以禁止通过网关将重定向页存入高速缓存。

禁用该选项会影响网关性能。每当标准“门户桌面”被刷新，网关就必须检索该页所引用的所有内容，例如可能先前已经被浏览器高速缓存的图像。然而，通过启用该功能，远程访问安全内容将不会在客户端留下高速缓存的痕迹。如果从不受公司 IT 控制的网吧或类似的远程位置访问公司网络，这样做的价值有可能超过性能方面的蕴义。

### ► 禁用浏览器高速缓存

1. 以 `root` 用户身份登录并编辑所需网关实例的 `platform.conf` 文件：

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

2. 编辑以下行：

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

该值缺省设置为 `true`。将该值更改为 `false` 可禁用客户端的浏览器高速缓存。

3. 重新启动网关：

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

# 自定义网关服务用户界面

本部分讨论可以编辑的各种属性文件。

## srpGateway.properties 文件

您可以编辑该文件用于以下目的：

- 自定义网关运行时可能会出现的错误消息。
  - HTML-CharSets=ISO-8859-1 指定用于创建此文件的字符集。
  - 括号中的数字（例如 {0}）表示值将在运行时显示。可以更改与该数字关联的标签，或者按照需要重新排列选项卡。确保选项卡对应于将要显示的消息，因为数字和消息是关联的。
- 自定义日志信息。

缺省情况下，srpGateway.properties 文件位于 *portal-server-install-root/SUNWps/locale* 目录之下。网关机器（与消息相关的网关）上出现的所有消息都在该文件中，而与消息语言无关。

如果需要更改在客户机标准“门户桌面”上显示的消息的语言，请将该文件复制到相应语言环境的目录中，例如 *portal-server-install-root/SUNWps/locale\_en\_US*。

## srpadminmsg.properties 文件

您可以出于以下目的编辑该文件：

- 定制在管理控制台中网关服务的按钮上显示的标签。
- 定制配置网关时所显示的状态消息和错误消息。

# 使用联合管理

“联合管理”允许用户汇总其本地标识以便他们能够拥有统一的网络标识。“联合管理”使用网络标识以允许用户在一个服务提供者的站点上登录，并访问其他服务提供者的站点而不必重新认证其标识。这称为单点登录。

在 Portal Server 上，可在开放模式和安全模式中配置联合管理。*Portal Server 管理指南*描述了如何在开放模式中配置联合管理。在用“安全远程访问”配置安全模式中的“联合”管理之前，请确保它工作于开放模式。如果要使用户既在开放模式中、又在安全模式中使用来自同一浏览器的“联合管理”，则他们必须清除 cookie 并从浏览器进行高速缓存。

有关“联合管理”的详细信息，请参阅 *Identity Server Customization and API Guide*。

## 联合管理方案

初始服务提供者对用户进行验证。服务提供者是提供网络服务的商业性或非盈利性组织。这一广泛的范畴可以包括网络门户、零售商、运输供应商、金融机构、娱乐公司、图书馆、高等院校和政府机构。

服务提供者使用 cookie 存储客户机浏览器中用户的会话信息。cookie 也包括用户的身份提供者。

身份提供者是专门提供验证服务的提供者。在管理验证服务的同时，他们也维护和管理标识信息。由身份提供者完成的验证将获得所有服务提供者的认可，而不管它属于哪个机构。

当用户试图访问不属于该身份提供者的服务时，身份提供者将 cookie 发往相应的服务提供者。该服务提供者随后可以访问在 cookie 中调用的身份提供者。

然而，不能跨越不同的 DNS 域读取 cookie。因此“通用域 Cookie 服务”被用于将服务提供者重定向到正确的身份提供者，从而启用用户的单点登录。

## 配置联合管理资源

可基于要配置内容所在的位置，在网关配置文件中配置联合资源、服务提供者、身份提供者和通用域 Cookie 服务 (CDCS)。本部分介绍如何配置以下三种方案：

1. 全部资源都在公司内联网内
2. 全部资源都不在公司内联网内或者身份提供者驻留在 Internet 上。
3. 全部资源都不在公司内联网内，或者身份提供者被网关保护而服务提供者又是驻留在 Internet 上的第三方。

### 配置 1

在此配置中，服务提供者、身份提供者和“通用域 Cookie 服务”被部署在同一个公司内联网中并且不在 Internet “域名服务器” (DNS) 中发布身份提供者。CDCS 是可选的。

在此配置中，网关指向服务提供者 Portal Server。此配置对于多个 Portal Server 实例有效。

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 在管理控制台中，选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 单击“核心”选项卡。
6. 选中“启用 Cookie 管理”复选框以启用 cookie 管理。

7. 滚动至 Portal Server 字段并输入 Portal Server 名，以便能够使用相对 URL，如在“非验证 URL”列表中列出的 /amserver 或 /portal/dt。例如：

```
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. 滚动到 Portal Server 字段，然后输入 Portal Server 名。例如 /amserver。
9. 单击“保存”。
10. 单击“安全”选项卡。
11. 滚动至“非验证 URL”列表并添加“联合”资源。例如：

```
/amserver/config/federation
```

```
/amserver/IntersiteTransferService
```

```
/amserver/AssertionConsumerservice
```

```
/amserver/fed_images
```

```
/amserver/preLogin
```

```
/portal/dt
```

12. 单击“添加”。
13. 单击“保存”。
14. 如果到达“非验证 URL”列表中列出的 URL 需要使用网络代理，请单击“代理”选项卡。
15. 滚动至“域和子域代理”字段并输入所需的网络代理。
16. 单击“添加”。
17. 单击“保存”。
18. 从终端窗口重新启动网关：

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

## 配置 2

在此配置中，服务提供者、身份提供者和“通用域 Cookie 提供者” (CDCP) 未部署在公司内联网中，或者身份提供者是驻留在 Internet 上的第三方提供者。

在此配置中，网关指向服务提供者 Portal Server。此配置对于多个 Portal Server 实例有效。

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 在管理控制台中，选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 单击“核心”选项卡。
6. 选中“启用 Cookie 管理”复选框以启用 cookie 管理。
7. 滚动至 Portal Server 字段并输入服务提供者的 Portal Server 名，以便能够使用相对 URL，如在“非验证 URL”列表中列出的 /amserver 或 /portal/dt。

`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. 单击“保存”。
9. 单击“安全”选项卡。

- 滚动至“非验证 URL”列表并添加“联合”资源。例如：

```

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

```

- 单击“添加”。
- 单击“保存”。
- 如果到达“非验证 URL”列表中列出的 URL 需要使用网络代理，请单击“代理”选项卡。
- 滚动至“域和子域代理”字段并输入所需的网络代理。
- 单击“添加”。
- 单击“保存”。
- 从终端窗口重新启动网关：

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

### 配置 3

在此配置中，服务提供者、身份提供者和“通用域 Cookie 提供者” (CDCP) 未部署在公司内联网中，或者服务提供者是驻留在 Internet 上的第三方提供者并且身份提供者受网关保护。

在此配置中，网关指向身份提供者 Portal Server。

此配置对于多个 Portal Server 实例有效。这种配置不可能在 Internet 上，然而，一些公司网络可能在其内联网具有这种配置，即身份提供者驻留在被防火墙保护的子网中，并且可以从公司网络内部直接访问服务提供者。

- 以管理员身份登录到 Identity Server 管理控制台。
- 在管理控制台中，选择“服务配置”选项卡。
- 单击“SRA 配置”下网关旁边的箭头。

显示网关页面。

4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 单击“核心”选项卡。
6. 选中“启用 Cookie 管理”复选框以启用 cookie 管理。
7. 滚动至 Portal Server 字段并输入身份提供者的 Portal Server 名，以便能够使用相对 URL，如在“非验证 URL”列表中列出的 /amserver 或 /portal/dt。

`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. 单击“保存”。
9. 单击“安全”选项卡。
10. 滚动至“非验证 URL”列表并添加“联合”资源。例如：

`/amserver/config/federation`

`/amserver/IntersiteTransferService`

`/amserver/AssertionConsumerservice`

`/amserver/fed_images`

`/amserver/preLogin`

`/portal/dt`

11. 单击“添加”。
12. 单击“保存”。

13. 如果到达“非验证 URL”列表中列出的 URL 需要使用网络代理，请单击“代理”选项卡。
14. 滚动至“域和子域代理”字段并输入所需的网络代理。
15. 单击“添加”。
16. 单击“保存”。
17. 从终端窗口重新启动网关：

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



# Proxylet 和重写器

本章介绍 Proxylet 和“重写器”。这些组件使用户能够通过网关访问内部网网页。它们通过不同的方法来实现此目的。Proxylet 不能分析网页，而“重写器”则可以。

Proxylet 涵盖下列主题：

- [Proxylet 概述](#)

“重写器”涵盖下列主题：

- [重写器概述](#)
- [字符集编码](#)
- [重写器使用方案](#)
- [编写规则集](#)
- [公共接口（规则集 DTD）](#)
- [在网关服务中配置重写器](#)
- [使用调试日志排除故障](#)
- [公共接口（规则集 DTD）](#)
- [工作示例](#)
- [实例研究](#)
- [6.x 与 3.0 的规则集映射](#)

## Proxylet 概述

Proxylet 是一个在客户机上运行的动态代理服务器。Proxylet 将 URL 重定向到网关。它通过阅读和修改客户机上浏览器的代理设置以使其指向本地代理服务器或 Proxylet 来完成这项工作。

它支持 HTTP 和 SSL，从而从网关继承传输模式。如果将网关配置为在 SSL 上运行，则 Proxylet 会在客户机和网关之间建立一个安全通道。如果客户机 JVM 为 1.4 或更高版本，或者所需的 jar 文件驻留在客户机上，Proxylet 将使用 JSSE API。否则使用 KSSL API。

在网关配置文件中指定定向到网关的 URL 的域和子域。如果 URL 不是网关处理的域的一部分，则请求将定向到 Internet。如果在网关配置文件中列出了一个特定 URL 域，则 Proxylet 会重置客户机代理设置以指向该网关。

Proxylet 通过指定客户机 IP 地址和端口的 Identity Server 管理控制台启用。如果启用了 Proxylet，则它将检查客户机的以下各项：

- 适当的浏览器权限。
- JVM 版本 2（适用于 Netscape 浏览器）。
- 浏览器为 Netscape 7.0、Mozilla 1.4.1、Internet Explorer 5.0 或更高版本。
- 计算机或设备可以运行服务器应用程序。

如果满足上述要求，则会下载一个小型 applet 并在客户机上启动。如果客户机未安装 JRE 1.3.1 或更高版本，则自动使用 Proxylet 下载 JRE。

它会从“代理自动配置”(PAC)文件（如果使用）或代理配置列表中检索代理设置。

## 使用 Proxylet 的优点

与“重写器”不同，Proxylet 是一种非常规的解决方案，安装后极少或不需要进行任何更改。与第三方软件（如 Microsoft Exchange Server）的集成非常简单。同时，由于 Proxylet 未涉及网络内容，因此网关性能有所提高。

## 配置 Proxylet

有关启用和配置 Proxylet 的信息，请参阅第 321 页第 12 章的“配置 Proxylet”。

## 重写器概述

SRA 的“重写器”组件允许最终用户通过在网页上修改“统一资源标识符”(URI) 以使其指向网关来浏览内部网。URI 定义了一种方法，可将名称封装在任何已注册的名称空间中并用该名称空间来标示它。最常见的 URI 类型是“统一资源定位符”(URL)。URL 可以有各种不同的协议，如 http、ftp、邮件发送协议、文件协议以及新闻协议。

“重写器”可识别和重写在 RFC-1738 中指定、使用 HTTP 或 HTTPS 协议的所有标准 URL。这些协议不区分大小写。例如，hTtP、HTTp 和 http 都有效。下面列出了一些 URL 示例：

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

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

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

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

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

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

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

对于 Internet Explore 和 Netscape 所支持的一些基本的非标准 URL，“重写器”也支持对其进行重写。将非标准 URL 转化成标准格式所需的信息取自该 URL 所在页的基 URL。该信息可能包括：

- 协议
- 主机名
- 端口
- 路径

“重写器”仅支持出现在相对 URL 中的反斜线符号。

例如，

`http://abc.sesta.com\index.html` 会被重写，

而以下这些 URL 不会被重写：

`http:\\abc.sesta.com。`

`http:/abc.com`

## 字符集编码

HTTP 标准要求 HTTP 文件头或 HTML 元标记为网页指定一个字符集。但有时无法获得此信息。字符集必须已知，以便设置数据编码并按照创建者的意图显示数据。

Sun Microsystems 提供了检测字符集的第三方产品。要启用此产品，请安装 SUNWjchdt 软件包。如果安装了此产品，“重写器”会检测到它，并在需要时使用。

---

**注意**      使用此产品可能会影响性能，因此应在有需要时才安装。有关安装、配置以及用法的详细信息，请参阅 `jcharset_readme.txt`。

---

## 重写器使用方案

当用户试图通过网关访问内部网网页时，可使用“重写器”来获得网页。下列组件使用了“重写器”：

- [URLScrapper](#)
- [网关](#)

### URLScrapper

URL Scrapper 提供者从已配置的 URI 中获取内容，在将内容发送到浏览器之前，它会将所有相对 URI 扩展成绝对 URI。

例如，如果用户想要访问具有如下内容的站点：

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

“重写器”会将其转换为：

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

其中 `http://yahoo.com/test/` 为页的基 URL。

有关 URLScrapper 供应商的详细信息，请参阅 *Portal Server 管理指南*。

## 网关

网关从 Internet 门户获得内容，并且在将内容发送到浏览器之前，它会将网关 URI 加在现有 URI 之前，以便来自浏览器的后续 URI 请求可以到达网关。

例如，如果有某位用户想要访问某台 Internet 机器上具有如下内容的 HTML 页：

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

“重写器”会在该 URL 前加上一个指向网关的引用，如下所示：

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

当用户单击与该锚定点相关联的某个链接时，浏览器便会与网关联络。网关会从 `mymachine.intranet.com` 中获取 `mypage.html` 的内容。

网关使用若干规则来确定要重写已获取网页的哪些要素。

## 编写规则集

可在“服务配置选项卡”下的“Portal Server 配置”部分定义规则集。

有关定义规则集的详细信息，请参阅 *Portal Server 管理指南*。在创建了新的规则集后，需要定义所需的规则。

本部分涵盖下列主题：

- [公共接口（规则集 DTD）](#)
- [XML DTD 示例](#)
- [规则编写步骤](#)

- 规则集指导原则
- 定义规则集根元素
- 使用递归功能
- HTML 内容规则
- JavaScript 内容规则
- XML 内容规则
- 层叠样式表规则
- WML 规则

## 公共接口（规则集 DTD）

以下为规则集 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 "*"
>

```

---

**注意** 可将 \* 作为规则值的一部分。但并非所有强制属性值都可以只是 \*。此类规则会被忽略，但会将消息记录在 `RuleSetInfo` 日志文件中。有关该日志文件的信息，请参阅第 134 页的“调试文件名称”。

---

## XML DTD 示例

本部分包含一个示例规则集。第 140 页的“实例研究”用于举例说明“重写器”是如何解释这些规则的。

```

<?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>
```

## 规则编写步骤

下面列出了编写规则时可以遵循的一般步骤。

- 确定哪些目录包含内容需重写的 HTML 页。
- 在这些目录中，确定需重写的页。
- 确定各页需重写的 URL。确定大多数 URL 的简便方法是搜索“http”和“/”。
- 确定 URL 的内容类型：HTML、JavaScript 或 XML。
- 编写上述各 URL 所需的重写规则，这可通过在 Identity Server 管理控制台中编辑“Portal Server 配置”下的“重写器”服务必需规则集来完成。
- 将上述所有规则合并成该域的一个规则集。

## 规则集指导原则

请记住以下几点：

- 特定主机的优先顺序以匹配最长的 URL 为基础。例如，对于以下规则集

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

由于 sfbay\_ruleset 匹配最长，因此使用它。

- 规则集中的规则会依次应用于页中的每条语句，直到有一项规则与某条语句相匹配为止。

编写规则时，切记不要忘了规则的顺序。规则是按它们在规则集中的出现顺序应用于页中的语句的。如果既有特定规则又有包含 "\*" 的一般规则，要先定义特定规则，然后再定义一般规则。否则，一般规则将先于特定规则应用于所有语句。

- 所有规则都需包括在 <RuleSet> </RuleSet> 标记内。
- 在规则集的 <HTMLRules> </HTMLRules> 部分加入需要重写 HTML 内容的所有规则。

- 在规则集的 `<JSRules>` `</JSRules>` 部分加入需要重写 JavaScript 内容的所有规则。
- 在规则集的 `<XMLRules>` `</XMLRules>` 部分加入需要重写 XML 内容的所有规则。
- 在内部网页中，确定需要重写的 URL，并在规则集的适当部分（HTML、JSRules 或 XMLRules）加入所需规则。
- 将规则集分配给所需的域。有关详细信息，请参阅第 270 页的“创建 URI 到规则集映射列表”。
- 重新启动网关以使所有更改生效：

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

## 定义规则集根元素

规则集根元素有两个属性：

- **RuleSetName**。例如，`default_ruleset`。在规则集到 URI 的映射中会引用这个名称。
- **Extends**。该属性是指规则集的继承功能。扩展值指向一个规则集，欲从该规则集中派生出某个规则集。

可使用扩展值 `none` 表示这个新的独立规则集不依赖于其他任何规则集，或者指定 `RuleSetName` 表示您的规则集依赖于另一规则集。

## 使用递归功能

“重写器”使用递归功能，对同一模式进行搜索，直到匹配字符串模式的结尾。

例如，“重写器”分析以下字符串时：

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

规则

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

仅重写首先出现的模式，形式如下：

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

但是，如果您使用如下递归选项，

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

“重写器”将对同一模式进行搜索，直到匹配字符串模式的结尾，因此输出为：

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

## 定义基于语言的规则（定义规则）

规则建立在下列语言基础上：

- HTML
- JavaScript
- XML

### HTML 内容规则

网页中的 HTML 内容可进一步分成属性、表单和 applet。相应地，HTML 内容规则分为以下几类：

- [HTML 内容属性规则](#)
- [HTML 内容的表单规则](#)
- [HTML 内容的 Applet 规则](#)

#### HTML 内容属性规则

该规则用于确定标记都有哪些属性的值需要重写。属性值可以是简单 URL，也可以是 JavaScript 或 DHTML 内容。例如：

- “img” 标记的 src 属性指向某个图像位置（简单 URL）
- href 属性的 onClick 属性用于处理链接单击操作 (DJS)

本部分分为下列各小部分：

- [属性规则语法](#)
- [属性规则示例](#)
- [DJS 属性示例](#)

### 属性规则语法

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

其中：

attributeName 是属性的名称（强制项）

tag 是属性所属的标记（可选项，默认值是 \*，指任何标记）

valuePatterns 参见第 104 页的“在规则中使用模式匹配”。

source 指定在其中定义该属性的页的 URI（可选项，默认值是 \*，指在任何页中）

type 指定值的类型（可选项）。它们可以是：

URL - 简单 URL（默认值）。

DHTML - DHTML 内容。这种内容见于标准的 HTML 内容，并在 Microsoft 的 HTC 格式文件中会使用这种内容。

DJS - JavaScript 内容。所有 HTML 事件处理程序（如 onClick 和 onMouseover）都用此 HTML 属性嵌入 JavaScript。

### 属性规则示例

假定页的基 URL 为：

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

页内容

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

规则

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

或

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

输出

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

说明

由于要重写的 URL 已是一个绝对 URL，所以只在此 URL 前加上“网关 URL”。

## DJS 属性示例

假定页的基 URL 为：

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

### 页内容

< 表单 >

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

### 规则

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

### 输出

< 表单 >

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

### 说明

需要两项规则来重写指定的页内容。第一项规则确定 onClick JavaScript 标志。第二项规则确定 check 函数需要重写的参数。在本例中，只会重写第一个参数，因为 paramPatterns 用值 y 代替了第一个参数。

会在所需参数前加上“网关 URL”以及这些 JavaScript 标志所在页的基 URL。

## HTML 内容的表单规则

用户浏览的 HTML 页可能会包含表单。一些表单元素可能会以 URL 作为值。

本部分分为下列各小部分：

- [表单规则语法](#)
- [表单规则示例](#)

### 表单规则语法

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

其中

name 是表单的名称（强制项）

field 是表单中值需重写的字段（强制项）

valuePatterns 参见第 104 页的“在规则中使用模式匹配”

source 是该表单定义所在 html 页的 URL（可选项，默认值是 \*，指在任何页中）

### 表单规则示例

假定页的基 URL 为：

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

#### 页内容

假定页 URI 是 form.html，并且它位于服务器的根目录下。

```
<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>
```

要重写 form1 中名为 abc1 的隐藏字段值中出现的 /text.html，需要下列规则：

#### 规则

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

#### 输出

```
<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>
```

#### 说明

action 标记是用某项已定义的 HTML 属性规则进行重写的。

输入标记属性值的 value 会如输出中所示的那样被重写。将会查找所指定的 valuePatterns，并通过在前面加上“网关 URL”以及页的基 URL 来重写紧随在匹配的 valuePatterns 之后的所有内容。请参阅第 104 页的“在规则中使用模式匹配”。

## HTML 内容的 Applet 规则

单个网页可以包含许多 applet，而且每个 applet 可以包含许多参数。“重写器”将用规则中指定的值与 applet 的 HTML 定义进行匹配，然后修改 applet 参数定义中出现的 URL 值。此替换在服务器处执行，用户浏览特定网页时并不会执行。此项规则会确定并重写 applet 以及 HTML 内容对象标记中的参数。

本部分分为下列各小部分：

- [Applet 规则语法](#)
- [Applet 规则示例](#)

### *Applet 规则语法*

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

其中

code 是 applet 或对象类的名称（强制项）

param 是值需重写的参数的名称（强制项）

valuePatterns 参见第 104 页的“在规则中使用模式匹配”。

source 是包含 applet 定义的页的 URL（可选项，默认值是 \*，指在任何页中）

### *Applet 规则示例*

假定页的基 URL 为：

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

页内容

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

规则

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

## 输出

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

## 说明

由于 `<Attribute name="codebase"/>` 是 `default_gateway_ruleset` 中的一项已定义规则，所以会重写 `codebase` 属性。

名称以 `Test` 开头的参数均会被重写。并且，会在 `param` 标记的 `value` 属性前加上显示 `applet` 代码的页面的基 URL 以及“网关 URL”。

## 在规则中使用模式匹配

可以使用 `valuePatterns` 字段实现模式匹配并指定语句中需重写的特定部分。

如果已在规则中指定了 `valuePatterns`，将会重写紧随在匹配模式之后的所有内容。

请考虑下面的表单规则示例。

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

其中

`source` 是表单所在 `html` 页的 URL

`name` 是表单的名称

`field` 是表单中值需重写的字段

`valuePatterns` 指示需要重写字符串中的哪个部分。将会重写 `valuePatterns` 后出现的所有内容（可选项，默认值是“”，指需要重写整个值）。

### 在 `valuePatterns` 中指定专用字符

可以通过使用反斜杠转义指定专用字符。例如：

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

### 在 *valuePatterns* 中使用通配符

可以使用 \* 字符来实现重写时的模式匹配。

但不能在 *valuePatterns* 字段中仅仅指定一个 \*。由于 \* 表示与一切内容匹配，所以 *valuePattern* 后不会跟有任何内容，从而不会留下任何内容让“重写器”重写。可将 \* 与另一字符串连起来使用，如 \*abc。此时，会重写紧随在 \*abc 之后的所有内容。

---

**注意** 可在规则的任何字段中使用星号 (\*) 作为通配符。但并非规则中的所有字段都能包含 \*。如果所有字段都包含 \*，则会忽略该规则。不会显示任何错误消息。

---

可以与原始语句中出现的分隔符（分号或逗号）联合使用 \* 或 \*\* 来分隔多个字段。单通配符 (\*) 匹配任何不进行重写的字段，双通配符 (\*\*) 匹配任何需要重写的字段。

表 3-1 列出了 \* 通配符的一些用法示例。

表 3-1 \* 通配符用法示例

URL	valuePatterns	说明
url1, url2, url3, url4	valuePatterns = "**, *, **, *"	在本例中，由于 ** 表示要重写的部分，所以会重写 url1 和 url3
XYZABCh <code>http://host1.sesta.com/dir1.html</code>	valuePatterns = "*ABC"	在本例中，只会重写 <code>http://host1.sesta.com/dir1.html</code> 部分。需要重写 *ABC 后的所有内容。
"0 dir1 dir2 dir3 dir4 test url1	valuePatterns = "* * ** * ** * "	在本例中，会重写 dir2、dir4 和 url1。最后一个需要重写的字段不必用 ** 指出。

## JavaScript 内容规则

JavaScript 可以在各种不同位置包含 URL。“重写器”不能直接分析 JavaScript 并确定出 URL 部分。需要编写一组特殊的规则来帮助 JavaScript 处理器确定和转换 URL。

具有 URL 类型的 JavaScript 元素分类如下：

- 变量
- 函数参数

## 变量

### 一般语法

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

根据 JavaScript 变量所含值的类型，可将它们细分为以下 5 类：

- [URL 变量](#)
- [EXPRESSION 变量](#)
- [DHTML（动态 HTML）变量](#)
- [DJS（动态 JavaScript）变量](#)
- [SYSTEM 变量](#)

### URL 变量

变量值为可作为 URL 对待的简单字符串。

本部分分为下列各小部分：

- [URL 变量语法](#)
- [URL 变量示例](#)

### URL 变量语法

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

其中

`variableName` 是变量的名称。`variableName` 的值会被重写（强制项）。

`type` 是 URL 变量（强制项，其值必须是 URL）

`source` 是该 JavaScript 变量所在页的 URI（可选项，默认值是 \*，指在任何页中）

### URL 变量示例

假定基 URL 为：

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

## 页内容

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

## 规则

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

## 输出

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

## 说明

会重写所有为 URL 类型并且名称以 `imgsrc` 开头的变量。对于输出中的第一行，在其前面加上了“网关 URL”以及变量所在页的基 URL。第二行已包含绝对路径，因此只在其前面加上了“网关 URL”。由于第三行的 `var imgsrc2` 的值不是字符串，而是其他 JavaScript 值，所以不会对其进行重写。

## *EXPRESSION* 变量

表达式变量的右侧是一个表达式。该表达式的结果是一个 URL。由于“重写器”无法对服务器上的此类表达式求值，所以它会向 HTML 页追加一个 JavaScript 函数 (`psSRAPRewriter_convert_expression`)。该函数将此表达式视为一个参数，并在客户机浏览器中对其进行求值以得出所需的 URL。

如果不确定语句中包含的是简单 URL 还是 EXPRESSION URL，推荐使用 EXPRESSION 规则，因为它两种情形都可以处理。

本部分分为下列各小部分：

- [EXPRESSION 变量语法](#)
- [EXPRESSION 变量示例](#)

### *EXPRESSION 变量语法*

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

其中

variableName 是值为表达式的 JavaScript 变量的名称（强制项）

type 是 JavaScript 变量的类型（可选项，默认值是 EXPRESSION）

source 是页的 URI（可选项，默认值是 \*，指任何源）

### *EXPRESSION 变量示例*

假定页的基 URL 为：

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

页内容

```
<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>
```

规则

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

或

```
<Variable name="expvar"/>
```

## 输出

```
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";
```

## 说明

会在第一行的表达式变量 `expvar` 的右侧前面加上函数 `psSRAPRewriter_convert_expression`。该函数会在运行时处理此表达式并重写相应内容。在第三行中，值被重写为一个简单的 URL。

## *DHTML*（动态 HTML）变量

这些变量是包含 HTML 内容的 JavaScript 变量。

本部分分为下列各小部分：

- [DHTML 语法](#)
- [DHTML 示例](#)

### *DHTML 语法*

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

其中

`variableName` 是具有 DHTML 内容的 JavaScript 变量的名称（强制项）

`type` 是变量的类型（强制项，其值必须是 DHTML）

`source` 是页的 URL（可选项，默认值是 \*，指在任何页中）

### *DHTML 示例*

假定页的基 URL 为：

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

### 页内容

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

```
var dhtmlVar=""
//-->
</SCRIPT>
```

### 规则

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

### 或

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

### 输出

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

### 说明

JavaScript 分析器会读取 dhtmlVar 的值作为 HTML 内容，并通过 HTML 分析器发送此内容。HTML 分析器会应用其中有 href 属性规则匹配的 HTML 规则，因而它会被重写。

### *DJS*（动态 JavaScript）变量

这些变量是包含 JavaScript 内容的 JavaScript 变量。

本部分分为下列各小部分：

- [DJS 语法](#)
- [DJS 示例](#)

### DJS 语法

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

其中

variable 是值为 javascript 的 JavaScript 变量。

### DJS 示例

假定页的基 URL 为：

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

页内容

```
//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';"
```

规则

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

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

输出

```
//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.jpg';"
```

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

说明

这里需要两项规则。第一项规则用于查找动态 JavaScript 变量 dJSVar。该变量的值同样是 URL 类型的 JavaScript。第二项规则用于重写该 JavaScript 变量的值。

### SYSTEM 变量

这些变量是指不是由用户声明而是作为 JavaScript 标准一部分提供的变量。例如，window.location.pathname。对于这些变量的支持是有限的。

本部分分为下列各小部分：

- [SYSTEM 变量语法](#)
- [SYSTEM 变量示例](#)

### *SYSTEM 变量语法*

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

其中

variableName 是 JavaScript 系统变量（强制项，其值可以是与以下模式匹配的任何值：document.URL、document.domain、location、document.location、location.pathname、location.href、location.protocol、location.hostname、location.host 和 location.port。上述所有模式都存在于 generic\_ruleset 中。不要修改这些系统变量规则。）

type 指定系统类型值（强制项，且值为 DJS）

source 是这类页的 URI（可选项，默认值是 \*，指在任何页中）

### *SYSTEM 变量示例*

假定页的基 URL 为：

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

页内容

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

规则

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

输出

```
</SCRIPT>
<SCRIPT LANGUAGE="Javascript">
<!--
//SYSTEM Var
```

```
alert(psSRAPRewriter_convert_pathname(window.location.pathname));
//-->
</SCRIPT>
```

## 说明

“重写器”会查找与规则匹配的系统变量，然后在其前面加上 `psSRAPRewriter_convert_system` 函数。该函数会在运行时处理此系统变量并相应地重写最终得到的 URL。

## 函数参数

值需重写的函数参数分为以下 4 类：

- URL 参数
- EXPRESSION 参数
- DHTML 参数
- DJS 参数

### 一般语法

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

其中

`name` 是 JavaScript 函数的名称（强制项）

`paramPatterns` 指定需要重写的参数（强制项）

`y` 和 `y` 的位置指示需要重写的参数。例如，在语法中，第一个参数需要重写，但不能重写第二个参数。

`type` 指定该参数所需值的类型（可选项，默认值是 EXPRESSION 类型）

`source` 是页的源 URI（可选项，默认值是 \*，指在任何页中）

### URL 参数

函数将该参数视为一个字符串并且该字符串可以作为 URL 对待。

本部分分为下列各小部分：

- URL 参数语法
- URL 参数示例

### URL 参数语法

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

其中

name 是具有 URL 类型参数的函数的名称（强制项）

paramPatterns 指定需要重写的参数（强制项）

y 和 y 的位置指示需要重写的参数。例如，在语法中，第一个参数需要重写，但不能重写第二个参数。

type 是函数的类型（强制项，其值必须是 URL）

source 是具有该函数调用的页的 URL（可选项，默认值是 \*，指在任何 URL 中）

### URL 参数示例

假定页的基 URL 为：

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

页内容

```
<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>
```

规则

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

输出

```
<SCRIPT language="JavaScript">
<!--
function test(one,two,three) {
```

```

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

```

### 说明

第一项规则指定需要重写名为 `test` 的函数中的前两个参数。因此会重写 `test` 函数的前两个参数。第二项规则指定需要重写 `window.open` 函数的第一个参数。会在 `window.open` 函数中的 URL 前面加上“网关 URL”以及包含这些函数参数的页的基 URL。

### *EXPRESSION* 参数

这些参数接受表达式值，表达式计算结果为 URL。

本部分分为下列各小部分：

- [EXPRESSION 参数语法](#)
- [EXPRESSION 参数示例](#)

### *EXPRESSION* 参数语法

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

其中

`name` 是函数的名称（强制项）。

`paramPatterns` 指定需要重写的参数（强制项）

`y` 和 `y` 的位置指示需要重写的函数参数。在上述语法中，只会重写第一个参数。

`type` 指定 *EXPRESSION* 值（可选项）

`source` 是其中调用了该函数的页的 URI。

### *EXPRESSION* 参数示例

假定页的基 URL 为：

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

页内容

```
<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>
```

规则

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

或

```
<Function name="jstest1" paramPatterns="y"/>
```

输出

```
<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>

```

### 说明

此规则将 `jstest1` 函数的第一个参数视为一个 `EXPRESSION` 函数参数，以此来指定需要重写该参数。在示例页内容中，第一个参数是一个表达式，只会在运行时对其进行求值。“重写器”会在该表达式前加上 `psSRAPRewriter_convert_expression` 函数。此表达式要进行求值，并且 `psSRAPRewriter_convert_expression` 函数会在运行时重写输出结果。

---

**注意**      在上述示例中，不需要在 JavaScript 变量规则中包含变量 `test1`。  
`jstest1` 的函数规则会负责执行重写工作。

---

### DHTML 参数

值为 HTML 的函数参数

本地 JavaScript 方法，如可动态生成 HTML 页的 `document.write()`，归属于这一类别。

本部分分为下列各小部分：

- [DHTML 参数语法](#)
- [DHTML 参数示例](#)

### DHTML 参数语法

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

其中

`name` 是函数的名称。

`paramPatterns` 指定需要重写的参数（强制项）

y 和 Y 的位置指示需要重写的函数参数。在上述语法中，只会重写第一个参数。

### *DHTML* 参数示例

假定页的基 URL 为：

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

页内容

```
<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>
```

规则

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

输出

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

## 说明

第一项规则指定需要重写函数 `document.write` 中的第一个参数。第二项规则指定需要重写函数 `document.writeln` 中的第一个参数。第三项规则是一项简单的 HTML 规则，它指定需要重写名为 `href` 的所有属性。在示例中，DHTML 参数规则将会确定函数中需要重写的参数。然后会应用 HTML 属性规则来实际重写已确定的参数。

### DJS 参数

值为 JavaScript 的函数参数。

本部分分为下列各小部分：

- [DJS 参数语法](#)
- [DJS 参数示例](#)

### DJS 参数语法

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

其中

`name` 是其中有一个参数为 DJS 的函数的名称（强制项）

`paramPatterns` 指定上述函数中的哪个参数是 DJS（强制项）

`y` 和 `y` 的位置指示需要重写的函数参数。在上述语法中，只会重写第一个参数。

`type` 为 DJS（强制项）

`source` 是页的 URI（可选项，默认值为 `*`，指任何 URI）

### DJS 参数示例

假定页的基 URL 为：

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

页内容

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

## 规则

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

## 输出

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

## 说明

第一项规则指定需要重写函数 `NavBarMenuItem` 中的第二个包含 JavaScript 的参数。在此 JavaScript 中，变量 `top.location` 也需要重写。该变量是使用第二项规则来重写的。

# XML 内容规则

网页可以包含 XML 内容，而后者又可以包含 URL。需要重写的 XML 内容分为以下两类：

- 标记文本（与标记的 `PCDATA` 或 `CDATA` 相同）
- 属性

## 标记文本

本规则用于重写标记元素的 `PCDATA` 或 `CDATA`。

本部分分为下列各小部分：

- 标记文本语法
- 标记文本示例

### 标记文本语法

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

其中

`tagName` 是标记的名称。

attributePatterns 是与该标记相应的属性及其值模式（可选项，指该标记根本无任何属性）

source 是该 xml 文件的 URI（可选项，默认值是 \*，指任何 xml 页）

### 标记文本示例

假定页的基 URL 为：

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

### 页内容

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

### 规则

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

### 输出

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

### 说明

页内容中的第一行有一个[属性示例](#)。页内容中的第二行不包含属性称为 name 且属性名称值为 src 的属性，因此不会进行任何重写。要重写该属性，也需要有 `<TagText tag="attribute"/>`

### 属性

XML 属性规则与 HTML 的属性规则类似。请参阅第 118 页的“[HTML 内容的属性规则](#)”。二者的区别在于，XML 的属性规则区分大小写，而 HTML 属性规则不区分大小写。这同样是因为在 XML 中内置而没有在 HTML 中内置大小写敏感性所造成的。

“重写器”会基于属性名称来转换属性值。

本部分分为下列各小部分：

- [属性语法](#)
- [属性示例](#)

### 属性语法

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

其中

`attributeName` 是属性的名称（强制项）

`tag` 是该属性所在标记的名称（可选项，默认值是 \*，指任何标记）

`valuePatterns` 参见第 104 页的“在规则中使用模式匹配”。

`source` 是该 XML 页的 URI（可选项，默认值是 \*，指在任何 XML 页中）

### 属性示例

假定页的基 URL 为：

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

页内容

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

规则

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

输出

```
<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.html"/>
</xml>
```

### 说明

在上述示例中，只会重写第四行，因为它满足规则中指定的所有条件。请参阅第 116 页的“在规则中使用模式匹配”。

## 层叠样式表规则

HTML 页中的“层叠样式表”（包括 CCS2）会进行转换。由于 URL 只在 CSS 的 `url()` 函数和导入语法中出现，因此没有为这种转换定义任何规则。

## WML 规则

WML 与 HTML 类似，因此 HTML 规则适用于 WML 内容。可对 WML 内容使用一般规则集。请参阅第 99 页的“HTML 内容规则”。

## 使用递归功能

“重写器”使用递归功能，对同一模式进行搜索，直到匹配字符串模式的结尾。

例如，“重写器”分析以下字符串时：

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

规则

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

仅重写首先出现的模式，形式如下：

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

但是，如果您使用如下递归选项，

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

“重写器”将对同一模式进行搜索，直到匹配字符串模式的结尾，因此输出为：

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

## 在网关服务中配置重写器

使用“重写器”选项卡下的网关服务，可以在两类（“基本”和“高级”）范围内执行下列任务：

- 基本任务
  - 启用全部 URL 重写
  - 创建 URI 到规则集映射列表
  - 创建要分析的 MIME 类型列表
  - 指定默认域
- 高级任务
  - 创建禁止重写的 URI 列表
  - 启用 MIME 推测
  - 创建要分析的 URI 映射列表
  - 启用屏蔽
  - 指定屏蔽种子字符串
  - 创建禁止屏蔽的 URI 列表
  - 使网关协议与原始 URI 协议相同

## 基本任务

### 启用全部 URL 重写

如果您启用了网关服务中的“启用全部 URL 重写”选项，“重写器”会重写任何 URL，而不检查“域和子域代理”列表中的条目。“域和子域代理”列表中的条目将被忽略。

### ► 允许网关重写所有 URL

1. 以管理员身份登录到 Sun Java™ System Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
会显示“网关配置文件”页。
4. 单击与想要为其设置属性的网关配置文件相应的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 单击“重写器”选项卡。
6. 选中“启用全部 URL 重写”复选框，以允许网关重写所有 URL。
7. 单击页顶部或底部的“保存”，记录此项更改。
8. 从终端窗口中重新启动网关：

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

### 创建 URI 到规则集映射列表

规则集是在 Identity Server 管理控制台中，在“Portal Server 配置”下的“重写器”服务中创建的。有关详细信息，请参阅 *Portal Server 管理指南*。

创建了规则集之后，可使用“将 URI 映射至规则集”字段将某个域与此规则集相关联。默认情况下，会将以下两个条目添加到“将 URI 映射至规则集”字段中：

- `*://*.Sun.COM/portal/*|default_gateway_ruleset`  
其中，`sun.com` 是门户的安装域，`/portal` 是门户安装环境
- `*|generic_ruleset`

此条目表示，对于域为 sun.com 的门户目录中的所有页，都会应用 default\_gateway\_ruleset。对于其他所有页，将会应用一般规则集。 default\_gateway\_ruleset 和 generic\_ruleset 是预先打包好的规则集。

---

**注意** 对于标准“门户桌面”上出现的所有内容，不管内容取自何处，均会使用与 default\_gateway\_ruleset 对应的规则集。

例如，假定将标准“门户桌面”配置成凑集来自 URL yahoo.com 的内容。Portal Server 位于 sesta.com 中。此时会将与 sesta.com 相应的规则集应用于所取得的内容。

---

---

**注意** 为其指定规则集的域必须在“域和子域代理”列表中列出。

---

### 在语法中使用通配符

可以在规则集中使用星号来映射全限定 URI 或部分 URI。

例如，可以将 java\_index\_page\_ruleset 应用于 index.html 页，如下所示：

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

也可以将 java 目录中的所有页应用于 java\_directory\_ruleset，如下所示：

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

### ► 将 URI 映射至规则集

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
会显示“网关配置文件”页。
4. 单击需要设置属性的网关配置文件。  
会显示“网关 - gateway-profile-name”页。
5. 单击“重写器”选项卡。
6. 滚动到“将 URI 映射至规则集”字段。

- 在“将 URI 映射至规则集”字段中，键入所需的域或主机名和规则集，然后单击“添加”。

会将此条目添加到“将 URI 映射至规则集”字段中。

指定域或主机名以及规则集时采用的格式如下：

域名 | 规则集名

例如：

`eng.sesta.com|default`

## 创建要分析的 MIME 类型列表

“重写器”有 4 个不同的分析器，可用来根据内容类型（HTML、JAVASCRIPT、CSS 和 XML）对网页进行分析。默认情况下，这些分析器与常见的 MIME 类型相关联。您可以在网关服务的“将分析器映射至 MIME 类型”字段中，将新的 MIME 类型与这些分析器相关联。这会将“重写器”功能扩展到其他 MIME 类型。

可用分号或逗号（“;”或“,”）分隔多个条目。例如：

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

它表示会将含有上述 MIME 的任何内容发送到 HTML 重写器，并且会应用 HTML 规则来重写这些 URL。

---

**提示** 从 MIME 映射列表中删除不必要的分析器可以提高操作速度。例如，如果您确信来自某个内部网的内容不会含有任何 JavaScript，便可从 MIME 映射列表中删除 JAVASCRIPT 条目。

---

### ► 指定 MIME 映射

- 以管理员身份登录到 Identity Server 管理控制台。
- 选择“服务配置”选项卡。
- 单击“SRA 配置”下网关旁边的箭头。  
会显示“网关配置文件”页。
- 单击需要设置属性的网关配置文件。  
会显示“网关 - *gateway-profile-name*”页。
- 单击“重写器”选项卡。

6. 滚动到“将分析器映射至 MIME 类型”字段，然后将所需 MIME 类型添加到编辑框中。可使用分号或逗号分隔多个条目。

以 `HTML=text/html;text/htm` 格式指定该条目

7. 单击“添加”，将所需条目添加到列表中。
8. 单击页顶部或底部的“保存”，记录此项更改。
9. 从终端窗口中重新启动网关：

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

## 创建禁止重写的 URI 列表

### ► 指定禁止重写的 URI

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。

会显示“网关配置文件”页。

4. 单击需要设置属性的网关配置文件。
5. 单击“重写器”选项卡、“基本”子部分。

会显示“网关 - *gateway-profile-name*”页。

6. 滚动到“禁止重写的 URI”字段，然后将 URI 添加到编辑框中。

注意：即使此 href 规则包括在规则集中，在该列表中添加 `#*` 也会允许重写 URI。

7. 单击页顶部或底部的“保存”，记录此项更改。
8. 从终端窗口中重新启动网关：

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

## 指定默认域

当 URL 仅包含没有域和子域的主机名时，默认的域和子域会非常有用。在这种情况下，网关将假定主机名在默认的域和子域中，并进行相应处理。

例如，如果 URL 中的主机名为 `host1`，并且将默认的域和子域指定为 `red.sesta.com`，则主机名会被解析为 `host1.red.sesta.com`。

### ► 指定默认域

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 单击“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的右箭头。  
会显示“网关配置文件”页。
4. 单击与想要为其设置属性的网关配置文件相应的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 滚动到“默认域”字段，然后以 `subdomain.domain name` 格式键入所需默认值。
6. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。
7. 从终端窗口中重新启动网关：

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

## 高级任务

### 启用 MIME 推测

重写器根据页面的 MIME 类型选择分析器。某些 Web 服务器（如 WebLogic 和 Oracle）不发送 MIME 类型。要解决这个问题，可通过在“将分析器映射至 URI”列表框中添加数据来启用 MIME 推测功能。

### ► 启用 MIME 推测

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
会显示“网关配置文件”页。
4. 单击需要设置属性的网关配置文件。  
会显示“网关 - *gateway-profile-name*”页。

5. 单击“重写器”选项卡、“高级”子部分。
6. 选中“启用 MIME 推测”复选框，以启用“MIME 推测”。
7. 单击页顶部或底部的“保存”，记录此项更改。
8. 从终端窗口中重新启动网关：

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

## 创建要分析的 URI 映射列表

如果启用了“MIME 推测”复选框，并且服务器尚未发送 MIME 类型，可使用该列表框映射要分析的 URI。

多个 URI 以分号进行分隔。

例如，HTML=\*.html;\*.htm;\*Servlet

它表示会使用“HTML 重写器”来重写具有 html、htm 或 Servlet 扩展名的任何页的内容。

### ► 分析 URI 映射

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
会显示“网关配置文件”页。
4. 单击需要设置属性的网关配置文件。  
会显示“网关 - gateway-profile-name”页。
5. 单击“重写器”选项卡、“高级”子部分。
6. 滚动到“将分析器映射至 MIME 类型”字段，然后将相应数据添加到编辑框中。
7. 单击页顶部或底部的“保存”，记录此项更改。
8. 从终端窗口中重新启动网关：

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

## 启用屏蔽

屏蔽功能允许“重写器”重写 URI 以便使人们看不到页的内部网 URL。

### ► 启用屏蔽

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
会显示“网关配置文件”页。
4. 单击需要设置属性的网关配置文件。  
会显示“网关 - *gateway-profile-name*”页。
5. 单击“重写器”选项卡、“高级”子部分。
6. 选中“启用屏蔽”复选框以启用“屏蔽”功能。
7. 单击页顶部或底部的“保存”，记录此项更改。
8. 从终端窗口中重新启动网关：

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

## 指定屏蔽种子字符串

种子字符串用于屏蔽 URI。它是由屏蔽算法生成的一个随机字符串。

---

**注意** 如果该种子字符串已更改或是重启了网关，则可能无法为屏蔽后的 URI 加书签。

---

### ► 指定屏蔽种子字符串

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
会显示“网关配置文件”页。
4. 单击需要设置属性的网关配置文件。  
会显示“网关 - *gateway-profile-name*”页。
5. 单击“重写器”选项卡、“高级”子部分。

6. 滚动到“屏蔽种子字符串”字段，然后在编辑框中添加一个字符串。
7. 单击页顶部或底部的“保存”，记录此项更改。
8. 从终端窗口中重新启动网关：

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

## 创建禁止屏蔽的 URI 列表

一些应用程序（如 applet）需要一个 Internet URI，而且不能对其进行屏蔽。要指定这些应用程序，可将 URI 添加到列表框中。

例如，如果添加了

**\*/Applet/Param\***

到列表框中，则当内容 URI `http://abc.com/Applet/Param1.html` 与规则集中的规则匹配时，将不会屏蔽此 URI。

### ► 指定禁止屏蔽 URI 列表

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
会显示“网关配置文件”页。
4. 单击需要设置属性的网关配置文件。  
会显示“网关 - *gateway-profile-name*”页。
5. 单击“重写器”选项卡、“高级”子部分。
6. 滚动到“禁止屏蔽 URI”字段，然后在编辑框中添加 URI。
7. 单击页顶部或底部的“保存”，记录此项更改。
8. 从终端窗口中重新启动网关：

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

## 使网关协议与原始 URI 协议相同

当网关同时运行于 HTTP 和 HTTPS 模式下时，您可以允许“重写器”使用一致的协议来访问 HTML 内容中引用的资源。

例如，如果原始 URL 是 `http://intranet.com/Public.html`，则添加 HTTP 网关。如果原始 URL 是 `https://intranet.com/Public.html`，则添加 HTTPS 网关。

---

**注意**           这样做只适用于静态 URI，不适用于 Javascript 中生成的动态 URI。

---

### ► 使网关协议与原始 URI 协议相同

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
会显示“网关配置文件”页。
4. 单击需要设置属性的网关配置文件。  
会显示“网关 - *gateway-profile-name*”页。
5. 单击“重写器”选项卡、“高级”子部分。
6. 选中“使网关协议与原始 URI 协议相同”复选框。
7. 单击页顶部或底部的“保存”，记录此项更改。
8. 从终端窗口中重新启动网关：

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

## 使用调试日志排除故障

要排除“重写器”故障，需要启用调试日志。

“调试消息”分为以下几类。

- **错误** - 重写器无法从中恢复的错误。
- **警告** - 该文件包含有关警告消息的日志。“重写器”能够恢复这类错误，但无法保证是否会造成异常行为。例如，“禁止重写图像内容”会作为警告消息被记录下来。这是合理的，因为“重写器”不应该重写这些图像。这些仅仅是警告，不会严重影响“重写器”的功能。警告中显示的一些消息是为了提供信息。
- **消息** - 这是“重写器”所提供的最高级信息。

## 设置重写器调试级别

### ► 设置重写器调试级别

1. 以根用户身份登录到网关机器并编辑以下文件：

*网关安装根目录* /SUNWam/config/AMConfig- *instance-name* .properties

2. 设置调试级别：

com.ipplanet.services.debug.level=

调试级别为：

error - 只将严重错误记录到调试文件中。出现此类错误时，“重写器”通常会停止工作。

warning - 记录警告消息。

message - 记录所有调试消息。

off - 不记录任何调试消息。

3. 在 AMConfig- *instance-name*.properties 文件的以下属性中，为调试文件指定目录。

com.ipplanet.services.debug.directory=/var/opt/SUNWam/debug

其中， /var/opt/SUNWam/debug 是默认调试目录。

4. 从终端窗口中重新启动网关：

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

## 调试文件名称

当将调试级别设置为消息时，调试时会生成一组文件。表 3-2 列出了“重写器”文件以及其中包含的信息。

表 3-2 重写器调试文件

文件名	信息
RuleSetInfo	本文件记录重写时已使用的所有规则集。
Original Pages	包含页 URI、解析 URI（如果它与页 URI 不同）、内容 MIME、已应用于此页的规则集、分析器 MIME，以及原始内容。 与分析有关的特定错误 / 警告 / 消息也出现在本文件中。 在消息模式下，会记录全部内容；在警告和错误模式下，只记录重写期间出现的异常。

表 3-2 重写器调试文件

文件名	信息
Rewritten Pages	包含页 URI、解析 URI（如果它与页 URI 不同）、内容 MIME、已应用于此页的规则集、分析器 MIME，以及重写后的内容。 当将调试模式设置为消息时，将会填写本文件。
Unaffected Pages	包含未经修改的页列表。
URIInfo Pages	本文件包含已找到并经过转换的 URL。该文件会记录内容仍与原始数据相同的所有页的详细信息。 所记录的详细信息有：页 URI、MIME 及编码数据、重写时所用的规则集 ID，以及分析器 MIME。

除了上述文件以外，“重写器”还会为调试消息生成一个文件，该文件未收入上述文件中。其文件名由两部分组成：第一部分是 `pwRewriter` 或 `psSRARewriter`；第二部分为扩展名，使用 `portal` 或 `gateway-profile-name`。

调试文件在门户或网关中显示。这些文件在 `AMConfig-instance-name.properties` 文件指定的目录中。

“重写器”组件会生成下面的一组文件来帮助进行调试：

`prefix_RuleSetInfo.extension`

`prefix_OriginalPages.extension`

`prefix_RewrittenPages.extension`

`prefix_UnaffectedPages.extension`

`prefix_URIInfo.extension`

其中

`prefix` 对于 `URLScrapper` 使用日志为 `psRewriter`，对于网关使用日志为 `psSRAPRewriter`。

`extension` 在使用 `URLScrapper` 时为 `portal`，在使用网关时为 `gateway-profile-name`。

例如，如果使用网关上的“重写器”来转换页并且使用了默认网关配置文件，则调试时会创建下列文件：

```
psSRAPRewriter_RuleSetInfo.default
psSRAPRewriter_OriginalPages.default
psSRAPRewriter_RewrittenPages.default
psSRAPRewriter_UnaffectedPages.default
psSRAPRewriter_URIInfo.default
psSRAPRewriter.default
```

## 工作示例

本部分包括：

- 含有需重写内容的简单 HTML 页
- 重写内容所需的规则
- 相应的重写后的 HTML 页

这些示例页可在 *portal-server-URL/rewriter* 目录下获得。在应用规则之前可以先浏览页面，然后再通过网关查看含有已重写输出的文件，以了解规则的工作方式。在一些示例中，规则已包含在 `default_gateway_ruleset` 中。在一些示例中，您可能得将规则加入到 `default_gateway_ruleset` 中。这一点会在适当的地方提及。

---

**注意**            某些语句以粗体形式出现，表示已对它们进行了重写。

---

提供了下列示例：

- HTML
  - [HTML 属性示例](#)
  - [HTML 表单示例](#)
  - [HTML Applet 示例](#)

- JavaScript
  - 变量
    - [JavaScript URL 变量示例](#)
    - [JavaScript 内容示例](#)
    - [JavaScript DHTML 变量示例](#)
    - [JavaScript DJS 变量示例](#)
    - [JavaScript SYSTEM 变量示例](#)
  - 函数
    - [JavaScript URL 函数示例](#)
    - [JavaScript EXPRESSION 函数示例](#)
    - [JavaScript DHTML 函数示例](#)
    - [JavaScript DJS 函数示例](#)
- XML
  - [XML 属性示例](#)

## HTML 内容示例

### HTML 属性示例

#### ► 使用 HTML 属性示例

1. 可从以下位置访问本示例：

*portal-server-URL/rewriter/HTML/attrib/attribrule.html*

2. 确保在网关服务的“域和子域代理”列表中定义了 `abc.sesta.com` 和 `host1.siroe.com`。

如果没有定义该项，则假定采用直接连接，不会在其前面加“网关 URL”。

不需要将本示例中指定的规则添加到 `default_gateway_ruleset` 中，因为它已经定义。

### 重写前的 HTML

```
<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>
```

### 规则

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

### 重写后的 HTML

```
<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>
```

// 由于已在 default\_gateway\_ruleset 中定义了 <Attrib name="href"/> 规则，所以会重写这个 URL。由于此 URL 已是绝对 URL，因此只在其前面加上了“网关 URL”。确保在网关服务的“域和子域代理”列表中定义了 abc.sesta.com。否则，不会在其前面加“网关 URL”，因为此时将假定采用直接连接。

## 2. href <a

```
href="gateway-URL/https://host1.siroe.com">https://../a>
```

// 同样，需要在网关服务的“域和子域代理”列表中定义 host1.siroe.com。否则，不会在其前面加“网关 URL”，因为此时将假定采用直接连接。

```
<br><br>
```

## 3. href <a

```
href="gateway-URL/portal-server-URL/rewriter/HTML/images/logo.gif">../images/</a>
```

// 由于指定了相对路径，因此会随所需子目录一同在其前面加上“网关 URL”和 portal-server-URL。该链接不会起作用，因为在所提供的示例结构中，HTML 目录下并不存在名为 images 的目录。

```
<br><br>
```

## 4 href <a

```
href="gateway-URL/portal-server-URL/rewriter/HTML/attrib/images/logo.gif">images/../a> <br><br>
```

// 由于指定了相对路径，因此会随所需子目录一同在其前面加上“网关 URL”和 Portal Server URL。

## 5. href <a

```
href="gateway-URL/portal-server-URL/rewriter/images/logo.gif">../../images/</a> <br><br>
```

// 由于指定了相对路径，因此会随所需子目录一同在其前面加上“网关 URL”和 Portal Server URL。该链接不会起作用，因为在所提供的示例结构中，重写器目录下并不存在名为 images 的目录。

```
Rewriting ends
```

```
</html>
```

## HTML 动态 JavaScript 标志示例

### ► 使用 HTML JavaScript 标志示例:

1. 可从以下位置访问本示例:

```
portal-server-URL/rewriter/HTML/jstokens/JStokens.html
```

2. 将本示例中指定的规则添加到 “JavaScript 源重写规则” 部分的 default\_gateway\_ruleset 中。
3. 在 Identity Server 管理控制台中, 编辑 “Portal Server 配置” 下的 “重写器” 服务中的 default\_gateway\_ruleset。
4. 从终端窗口中重新启动网关:

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

### 重写前的 HTML

```
<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>

```

### 规则

```

<Attribute name="onClick" type="DJS"/>
<Function type="URL" name="Check" paramPatterns="y"/>

```

---

**注意** <Function name="URL" name="Check" paramPatterns="y"/> 是 JavaScript 函数规则，在 JavaScript 函数示例中对其进行了详细解释。

---

### 重写后的 HTML

```

<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;">

```

// 在本示例中所有语句均会被重写。并且在每种情况下都会在前面加上“网关 URL”和 Portal Server URL。这是因为在 default\_gateway\_ruleset 文件中定义了 onAbort、onBlur、onFocus、onChange 和 onClick 的相应规则。“重写器”会检测 JavaScript 标志，并将其传递给 JavaScript 函数规则以便做进一步处理。示例中所列的第二项规则会通知“重写器”要重写哪个参数。

```

</body>

<br>

Rewriting ends

</html>

```

## HTML 表单示例

### ► 使用表单示例

1. 从以下位置访问此示例：

*portal-server-URL/rewriter/HTML/forms/formrule.html*

2. 确保在网关服务的“域和子域代理”列表中定义了 abc.sesta.com。  
如果没有定义该项，则假定采用直接连接，不会在其前面加“网关 URL”。

3. 将本示例中指定的规则添加到“HTML 属性重写规则”部分的 default\_gateway\_ruleset 中。

4. 在 Identity Server 管理控制台中，编辑“Portal Server 配置”下的“重写器”服务中的 default\_gateway\_ruleset。

5. 从终端窗口中重新启动网关：

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

*重写前的 HTML 页*

```

<!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>

```

*规则*

```

<Form source="*" name="form1" field="name1" valuePatterns="0|1234|"/>

```

*重写后的 HTML 页*

```

<HTML>
<HEAD>
RW_START
</HEAD>
<BODY>
<P>
<FORM name=form1 method=POST
action="gateway-URL/http://abc.sesta.com/casestudy/html/form.htm
1">

```

// 由于在 default\_gateway\_ruleset 的 HTML 规则中定义了 <Attribute name="action"/>, 所以会重写这个 URL。由于此 URL 已是绝对 URL, 因此只需在其前面加上“网关 URL”。确保在网关服务的“域和子域代理”列表中定义了 abc.sesta.com。否则, 不会在其前面加“网关 URL”, 因为此时将假定采用直接连接。

```
<input type=hidden name=name1 value="0|1234|gateway
URL/portal-server-URL/test.html">
```

// 这里, 表单名是 form1, 字段名是 name1。这与规则中指定的表单名和字段名相匹配。规则将 valuePatterns 规定为 0|1234|, 该值与本语句中的 value 相匹配。因此, 会重写 valuePattern 后出现的 URL。在其前面加上 Portal Server URL 和“网关 URL”。有关 valuePatterns 的详细信息, 请参阅第 116 页的“在规则中使用模式匹配”。

```
<input type=hidden name=name3 value="../../../html/test.html">
```

// 由于 name 不匹配规则中指定的 field 名称, 所以不会重写这个 URL。

```
</FORM>
```

```
<FORM name=form2 method=POST
action="gateway-URL/http://abc.sesta.com/casestudy/html/form.htm
l"><BR>
```

// 由于在默认规则集的 HTML 规则中定义了 <Attribute name="action"/>, 所以会重写这个 URL。由于此 URL 已是绝对 URL, 因此只需在其前面加上“网关 URL”。

```
<input type=hidden name=name1 value="0|1234|../../../html/test.html">
```

// 由于表单名不匹配规则中指定的名称, 所以不会重写这个 URL。

```
</FORM>
```

```
</BODY>
```

```
RW_END
```

```
</HTML>
```

## HTML Applet 示例

### ► 使用 Applet 示例

1. 获得 applet 类文件。RewriteURLinApplet.class 文件位于以下位置：

*portal-server-URL/rewriter/HTML/applet/appletcode*

applet 代码所在页的基 URL 是：

*portal-server-URL/rewriter/HTML/applet/rule1.html*

2. 将本示例中指定的规则添加到 “HTML 属性重写规则” 部分的 default\_gateway\_ruleset 中。
3. 在 Identity Server 管理控制台中，编辑 “Portal Server 配置” 下的 “重写器” 服务中的 default\_gateway\_ruleset。
4. 重新启动网关：

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

### 重写前的 HTML

```
<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>
```

### 规则

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

### 重写后的 HTML

```
<HTML>
Rewriting starts
```

```
<BR>
```

```
<APPLET
```

```
codebase=gateway-URL/portal-server-URL/rewriter/HTML/applet/appl
etcode=RewriteURLinApplet.class archive=/test>
```

// 由于规则 `<Attribute name="codebase"/>` 已存在于 `default_gateway_ruleset` 文件中，所以会重写这个 URL。“网关 URL”和 Portal Server URL 会连同到 `appletcode` 目录的路径一起被加在其前面。

```
<param name=Test1
```

```
value="gateway-URL/portal-server-URL/index.html">
```

// 由于页的基 URL 是 `rule1.html`，并且参数名与规则中指定的参数 `Test*` 相匹配，所以会重写这个 URL。由于 `index.html` 被指定位于根级，因此会直接在其前面加上“网关 URL”和 Portal Server URL。

```
<param name=Test2
```

```
value="gateway-URL/portal-server-URL/rewriter/HTML/index.html">
```

// 由于页的基 URL 是 `rule1.html`，并且参数名与规则中指定的参数 `Test*` 相匹配，所以会重写这个 URL。会根据需要在其前面加上相应的路径。

```
<param name=Test3
```

```
value="gateway-URL/portal-server-URL/rewriter/index.html">
```

// 由于页的基 URL 是 `rule1.html`，并且参数名与规则中指定的参数 `Test*` 相匹配，所以会重写这个 URL。会根据需要在其前面加上相应的路径。

```
</APPLET>
```

```
Rewriting ends
```

```
</HTML>
```

## JavaScript 内容示例

### JavaScript URL 变量示例

#### ► 使用 JavaScript URL 变量示例

1. 可从以下位置访问本示例：

```
portal-server-URL/rewriter/JavaScript/variables/url/js_urls.html
```

2. 确保在网关服务的“域和子域代理”列表中定义了 abc.sesta.com。  
如果没有定义该项，则假定采用直接连接，不会在其前面加“网关 URL”。
3. 将本示例中指定的规则添加到“JavaScript 源重写规则”部分的 default\_gateway\_ruleset 中。
4. 在 Identity Server 管理控制台中，编辑“Portal Server 配置”下的“重写器”服务中的 default\_gateway\_ruleset。
5. 如果添加了此规则，请重新启动网关：

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

### 重写前的 HTML 页

```
<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>
```

*规则*

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

*重写后的 HTML 页*

```
<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";

// 如规则中指定的那样,所有上述 URL 都是 URL 类型且名称为 imgsrc 的 JavaScript
// 变量。因此会在它们前面加上“网关 URL”和 Portal Server URL。根据需要,会在
// 其前面加上跟在 Portal Server URL 后面的路径。

/-->
</SCRIPT>

<br>
Testing JavaScript variables!

<br>

// 由于在 default_gateway_ruleset 中定义了规则 <Attribute name="src"/>, 所以
// 会重写该行

<br>
Image
</body>

<br>
Rewriting ends
</html>

```

## JavaScript EXPRESSION 变量示例

### ► 使用 JavaScript 表达式变量示例

1. 可从以下位置访问本示例:

*portal-server-URL/rewriter/JavaScript/variables/expr/expr.html*

2. 将本示例中指定的规则（如果它尚不存在）添加到“JavaScript 源重写规则”部分的 `default_gateway_ruleset` 中。
3. 在 Identity Server 管理控制台中,编辑“Portal Server 配置”下的“重写器”服务中的 `default_gateway_ruleset`。

4. 如果添加了此规则，请重新启动网关：

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

#### 重写前的 HTML 页

```
<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>
```

#### 规则

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

#### 重写后的 HTML 页

```
<html>
<head>
<title>JavaScript EXPRESSION Variables Test Page</title>
</head>
```

```

<body>
<SCRIPT>
// 重写器在此附加包裹函数 psSRAPRewriter_convert_expression。
</SCRIPT>
<script LANGUAGE="Javascript">
<!--
//Expression variables
var expvar1="images";
var expvar2="/logo.gif";
var expvar =psSRAPRewriter_convert_expression( expvar1 +
expvar2);

// “重写器”会将该语句的右侧部分识别为一个 JavaScript EXPRESSION 变量。
“重写器”不能在服务器端求解该表达式的值。因此，会在此表达式前面加上函数
psSRAPRewriter_convert_expression。在客户端对此表达式进行求值，并根据需
要对其进行重写。

document.write("<A HREF="+expvar+">EXPRESSION</A><P>")

// 使用了上一语句中 expvar 重写后的值来得出该表达式的值。由于结果是一个有效
的 URL（在示例中，该位置有图形存在），因此链接将会起作用。

var expvar="gateway URL/portal-server-URL/images/logo"+" .gif";

// “重写器”会将 expvar 的右侧部分识别为一个字符串表达式。该表达式可以在服
务器一方求解，因而会直接对其进行重写。

document.write("<A HREF="+expvar+">EXPRESSION</A><P>")

// 使用了上一语句中 expvar 重写后的值来得出该表达式的值。由于结果不是一个有
效的 URL（在最终得出的位置不存在图形），因此链接将不起作用。

//-->
</SCRIPT>

Testing JavaScript EXPRESSION variables
</body>
</html>

```

## JavaScript DHTML 变量示例

### ► 使用 JavaScript DHTML 变量示例

1. 可从以下位置访问本示例：

```
portal-server-URL/rewriter/JavaScript/variables/dhtml/dhtml.html
```

2. 确保在网关服务的“域和子域代理”列表中定义了 `abc.sesta.com`。如果没有定义该项，则假定采用直接连接，不会在其前面加“网关 URL”。
3. 将本示例中指定的规则（如果它尚不存在）添加到“JavaScript 源重写规则”部分的 `default_gateway_ruleset` 中。在 Identity Server 管理控制台中，编辑“Portal Server 配置”下的“重写器”服务中的 `default_gateway_ruleset`。
4. 如果添加了此规则，请重新启动网关：

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

### 重写前的 HTML 页

```
<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>

```

*规则*

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

*重写后的 HTML 页*

```

<html>
<head>
<title>JavaScript DHTML Variable Test Page</title>
</head>
<body>
<script LANGUAGE="Javascript">
<!--
//DHTML Var
var dhtmlVar="<a
href=gateway-URL/portal-server-URL/rewriter/JavaScript/images/test.html>"

```

// JavaScript DHTML 规则将 dhtmlVar 的右侧部分确定为动态 HTML 内容。因而，会应用 default\_gateway\_ruleset 文件中的 HTML 规则。动态 HTML 包含一个 href 属性。default\_gateway\_ruleset 定义了规则 <Attribute name="href"/>。因而，会重写 href 属性的值。但此 URL 不是绝对 URL；因此，会用页的基 URL 以及所需子目录来替换这个相对 URL。接着在其前面加上“网关 URL”以得出最终重写后的输出。

```

var dhtmlVar="<a
href=gateway-URL/portal-server-URL/./images/test.html>"

```

// 虽然附加了页的基 URL，并且在前面加上了“网关 URL”，但最终得到的 URL 不会起作用。这是因为初始 URL ./images/test.html 是错误的。

```

var dhtmlVar="<a
href=gateway-URL/portal-server-URL/images/test.html>"

```

// 这里，JavaScript DHTML 规则同样将右侧部分确定为动态 HTML 内容，并将其传递给 HTML 规则。因此，会应用 default\_gateway\_ruleset 中的 HTML 规则 <Attribute name="href"/>，并且会按所示方式重写此语句。在其前面加上“网关 URL”和 Portal Server URL。

```
var dhtmlVar="

```

```
var dhtmlVar="

```

```
var dhtmlVar="

```

// JavaScript DHTML 规则会确定出右侧的动态 HTML 内容，并将此语句传递给 HTML 规则。此时会应用 default\_gateway\_ruleset 中的 <Attribute name="src"/> 规则。由于此 URL 是绝对 URL，因此只需在其前面加上“网关 URL”。为重写该 URL，请确保在“域和子域代理”列表中定义了 abc.sesta.com。

```
//-->
```

```
</SCRIPT>
```

```
<br><br>
```

```
Testing DHTML Variables
```

```
<br><br>
```

```

```

// 由于在 default\_gateway\_ruleset 中定义了规则 <Attribute name="src"/>，所以会重写该行。

```
<br><br>
```

```
Image
```

```
</body>
```

```
</html>
```

## JavaScript DJS 变量示例

### ► 使用 JavaScript DJS 变量示例

1. 可从以下位置访问本示例：

```
portal-server-URL/rewriter/JavaScript/variables/djs/djs.html
```

2. 确保在网关服务的“域和子域代理”列表中定义了 abc.sesta.com。如果没有定义该项，则假定采用直接连接，不会在其前面加“网关 URL”。
3. 将本示例中指定的这两项规则（如果它们尚不存在）添加到“JavaScript 源重写规则”部分的 default\_gateway\_ruleset 中。在 Identity Server 管理控制台中，编辑“Portal Server 配置”下的“重写器”服务中的 default\_gateway\_ruleset。
4. 重新启动网关：

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

### 重写前的 HTML 页

```
<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>**

*规则*

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

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

*重写后的 HTML 页*

**<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';"
```

// 会用“网关 URL”和 Portal Server URL 重写上面的所有语句。还会适当地在前面加上所需的路径。第一项规则将 dJSVar 的右侧部分确定为一个动态 JavaScript 变量。然后将其传递给第二项规则，后者将 dJSimgsrc 的右侧部分确定为一个 URL 类型的 JavaScript 变量。并且会相应地对其进行重写。

**//-->**

**</SCRIPT>**

**<br>**

**Testing Dynamic JavaScript Variables**

**<br>**

```



// 由于在 default_gateway_ruleset 中定义了规则 <Attribute name="src"/>, 所以
会重写该行。

<br>
Image
</body>
</html>

```

## JavaScript SYSTEM 变量示例

### ► 使用 JavaScript 系统变量示例

1. 可从以下位置访问本示例:

```
portal-server-URL/rewriter/JavaScript/variables/system/system.html
```

2. 将本示例中指定的规则（如果它尚不存在）添加到“JavaScript 源重写规则”部分的 default\_gateway\_ruleset 中。
3. 在 Identity Server 管理控制台中，编辑“Portal Server 配置”下的“重写器”服务中的 default\_gateway\_ruleset。
4. 重新启动网关:

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

### 重写前的 HTML 页

```

<html>
<head>
<title>JavaScript SYSTEM Variables Test Page</title>
</head>
<body>
<script LANGUAGE="Javascript">
<!--
//SYSTEM Var
alert(window.location.pathname);

```

```
//document.write("<A
href="+window.location.pathname+">SYSTEM</A><P>")
//-->
</SCRIPT>

Testing JavaScript SYSTEM Variables

<br>

This page displays the path where the current page is located
when it is loaded.

</body>
</html>
```

### 规则

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

### 重写后的 HTML

```
<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"));

// “重写器”将 window.location.pathname 确定为一个 JavaScript SYSTEM 变量。
无法在服务器端确定该变量的值。因此，“重写器”会在此变量前加上
psSRAPRewriter_convert_pathname 函数。这个包裹函数将在客户端确定变量的
值，并根据需要进行重写。

//-->
```

```

</SCRIPT>
Testing JavaScript SYSTEM Variables
<br>
This page displays the path where the current page is located
when it is loaded.
</body>
</html>

```

## JavaScript URL 函数示例

### ► 使用 JavaScript URL 函数示例

1. 可从以下位置访问本示例：

```
portal-server-URL/rewriter/JavaScript/functions/url/url.html
```

2. 将本示例中指定的规则（如果它尚不存在）添加到“JavaScript 源重写规则”部分的 default\_gateway\_ruleset 中。在 Identity Server 管理控制台中，编辑“Portal Server 配置”下的“重写器”服务中的 default\_gateway\_ruleset。

3. 重新启动网关：

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

### 重写前的 HTML 页

```

<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>
```

*规则*

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

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

*重写后的 HTML 页*

```
<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>
```

## JavaScript EXPRESSION 函数示例

### ► 使用 JavaScript 表达式函数示例

1. 可从以下位置访问本示例:

*portal-server-URL/rewriter/JavaScript/functions/expr/expr.html*

2. 将本示例中指定的规则（如果它尚不存在）添加到“JavaScript 源重写规则”部分的 `default_gateway_ruleset` 中。
3. 在 Identity Server 管理控制台中，编辑“Portal Server 配置”下的“重写器”服务中的 `default_gateway_ruleset`。
4. 重新启动网关：

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

### 重写前的 HTML 页

```
<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>
```

*规则*

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

*重写后的 HTML 页*

```
<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()));
// 此规则规定需要重写函数 jstest1 中类型为 EXPRESSION 的第一个参数。该表
达式的值是 /test/images/test.html。会在该值前面加上 Portal Server URL 和 “网
关 URL”。
document.write("<a HREF="+test1+">Test</a>");
```

```

alert(test1);
//-->
</SCRIPT>
</body>
</html>

```

## JavaScript DHTML 函数示例

### ► 使用 JavaScript DHTML 函数示例

1. 可从以下位置访问本示例：

*portal-server-URL/rewriter/JavaScript/functions/dhtml/dhtml.html*

2. 将本示例中指定的规则（如果它尚不存在）添加到“JavaScript 源重写规则”部分的 `default_gateway_ruleset` 中。
3. 在 Identity Server 管理控制台中，编辑“Portal Server 配置”下的“重写器”服务中的 `default_gateway_ruleset`。
4. 重新启动网关：

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

### 重写前的 HTML 页

```

<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>

```

### 规则

```

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

```

### 重写后的 HTML 页

```

<html>
<head>
Testing JavaScript DHTML Functions
<br>
<br>
<script>
<!--
document.write('<a
href="gateway-URL/portal-server-URL/index.html">write</a><BR>')
// 第一项规则指定需要重写 DHTML JavaScript 函数 document.write 的第一个参
数。“重写器”将第一个参数确定为一个简单 HTML 语句。
default_gateway_ruleset 中的 HTML 规则部分具有规则 <Attribute name="href"
/>，该规则指示需要重写此语句。
document.writeln('<a
href="gateway-URL/portal-server-URL/rewriter/JavaScript/function
s/dhtml/index.html">writeln</a><BR>')
// 第二项规则指定需要重写 DHTML JavaScript 函数 document.writeln 的第一个
参数。“重写器”将第一个参数确定为一个简单 HTML 语句。
default_gateway_ruleset 中的 HTML 规则部分具有规则 <Attribute name="href"
/>，该规则指示需要重写此语句。

```

```

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

// 虽然此 DHTML 规则确定出了 document.write 和 document.writeln 函数，但是
// 不会重写上述语句。这是因为本例中的第一个参数不是简单 HTML。它可以是任意
// 的字符串，因而“重写器”不知道该如何重写这个参数。

//-->
</SCRIPT>
</head>
<body BGCOLOR=white>
<br><br>
Testing document.write and document.writeln
</body>
</html>

```

## JavaScript DJS 函数示例

### ► 使用 JavaScript DJS 函数示例

1. 可从以下位置访问本示例：

```
portal-server-URL/rewriter/JavaScript/functions/djs/djs.html
```

2. 确保在网关服务的“域和子域代理”列表中定义了 abc.sesta.com。

如果没有定义该项，则假定采用直接连接，不会在其前面加“网关 URL”。

3. 将本示例中指定的规则（如果它尚不存在）添加到“JavaScript 源重写规则”部分的 default\_gateway\_ruleset 中。在 Identity Server 管理控制台中，编辑“Portal Server 配置”下的“重写器”服务中的 default\_gateway\_ruleset。
4. 重新启动网关：

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

### 重写前的 HTML 页

```

<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>

```

### 规则

```

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

```

### 重写后的 HTML 页

```

<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 是网关服务的“域和子域代理”列表中的一项。因此“重写器”需要重写这个 URL。但由于它是一个绝对 URL，所以不需要在其前面加 Portal Server URL。此 DJS 规则规定需要重写 DJS 函数 NavBarMenuItem 的第二个参数。但第二个参数还是一个 JavaScript 变量。此时还需要一项规则来重写该变量的值。第二项规则指定需要重写 JavaScript 变量 top.location 的值。由于满足上述所有条件，所以会重写此 URL。

```

//menu.addItem(new NavBarMenuItem("All Available
Information", "http://abc.sesta.com"));

```

// 虽然此 DJS 规则指定需要重写函数 NavBarMenuItem 的第二个参数，但在本语句中这种事情是不会发生的。这是因为“重写器”不会将第二个参数识别为简单 HTML。

```

</script>
</html>

```

## XML 属性示例

### ► 使用 XML 属性示例

1. 可从以下位置访问本示例：

*portal-server-URL/rewriter/XML/attrib.html*

2. 将本示例中指定的规则（如果它尚不存在）添加到“XML 源重写规则”部分的 `default_gateway_ruleset` 中。
3. 在 Identity Server 管理控制台中，编辑“Portal Server 配置”下的“重写器”服务中的 `default_gateway_ruleset`。
4. 重新启动网关：

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

#### 重写前的 XML

```
<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>
```

*规则*

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

*重写后的 HTML*

```
<html>
```

```
  Rewriting starts
```

```
    <br>
```

```
    <br>
```

```
  <body>
```

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

```
    <xml><img href="image.html"/></xml>
```

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

```
    <xml><check
```

```
href="1234|gateway-URL/portal-server-URL/rewriter/XML/string.html"/></xml>
```

// 由于本语句符合规则中指定的条件，所以会重写它。Attribute name 为 href, tag 为 check, valuePatterns 为 1234 会重写跟在 valuePatterns 后面的字符串。有关 valuePatterns 的详细信息，请参阅第 116 页的“在规则中使用模式匹配”。

```
  </body>
```

```
  Rewriting ends
```

```
</html>
```

## 实例研究

本部分包括一个邮件客户机示例的源 HTML 页。本实例研究并未涵盖所有可能的方案和规则。它只是一个规则集示例，目的是为了帮助您将自己内部网页的相应规则合在一起。

### 假设

本实例研究作了如下假设：

- 假定邮件客户机的基 URL 为 abc.siroe.com
- 假定“网关 URL”为 gateway.sesta.com
- 假定网关服务的“域和子域代理”列表中有相关条目

## 示例页 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>

```

## 说明

表 3-3 展示了示例规则集与实例研究之间的映射。

表 3-3 示例规则集与实例研究间的映射

页内容	应用的规则	重写器输出	说明
<pre> var g_szVirtualRoot=" http://abc.siroe. com/mailweb"; </pre>	<pre> &lt;Variable name="URL"&gt; g_szVirtualRoot &lt;/Variable&gt; </pre>	<pre> var g_szVirtualRoot= "http://gateway.sesta .com/http://abc.siroe .com/mailweb"; </pre>	<p>g_szVirtualRoot 是一个值为简单 URL 的变量。</p> <p>该规则通知“重写器”搜索 URL 类型的变量 g_szVirtualRoot。如果网页中存在这样的变量，“重写器”会将其转换成一个绝对 URL，并在其前加上“网关 URL”。</p>
<pre> src="/destin_file s/logo-ie5.gif" </pre>	<pre> &lt;Attribute name="src" /&gt; </pre>	<pre> src="http://gateway.s esta.com/http://abc.s iroe.com/destin_files /logo-ie5.gif" </pre>	<p>src 是属性的名称，它没有附带任何标记或 valuePattern。</p> <p>该规则通知“重写器”搜索名称带 src 的所有属性，并重写该属性的值。</p>

表 3-3 示例规则集与实例研究间的映射

页内容	应用的规则	重写器输出	说明
<code>href="http://abc.siroe.com/mailclient/destin/Inbox/?Cmd=contents&amp;Page=1"</code>	<code>&lt;Attribute name="href"/&gt;</code>	<code>href="http://gateway.sesta.com/http://abc.siroe.com/mailclient/destin/Inbox/?Cmd=contents&amp;Page=1"</code>	href 是属性的名称，它没有附带任何标记或 <code>valuePattern</code> 。 该规则通知“重写器”搜索名称带 href 的所有属性，并重写该属性的值。

**注意** 规则集应用优先顺序为 hostname-subdomain-domain。

例如，假定在基于域的规则集列表中有下列条目：

`sesta.com | ruleset1`

`eng.sesta.com | ruleset2`

`host1.eng.sesta.com | ruleset3`

ruleset3 将应用于 host1 上的所有页。

除了从 host1 中检索到的页之外，ruleset2 将应用于 eng 子域中的所有页。

除了从 eng 子域和 host1 中检索到的页之外，ruleset1 将应用于 sesta.com 域中的所有页。

5. 单击页顶部或底部的“保存”，记录此项更改。

6. 从终端窗口中重新启动网关：

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

### Outlook Web Access 规则集

SRA 软件支持在 Sun Java System Web Server（即之前的 Sun™ ONE Web Server）及 IBM 应用程序服务器上安装 Outlook Web Access (OWA) 的 MS Exchange 2000 SP3 和 MS Exchange 2003。

#### ► 配置 OWA 规则集

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
会显示“网关配置文件”页。
4. 单击想要为其设置属性的网关配置文件。  
会显示“网关 - *gateway-profile-name*”页。
5. 在“将 URI 映射至规则集”字段中，输入安装了 Exchange 2000 的服务器名称，其后跟随 Exchange 2000 Service Pack 4 OWA 规则集。

例如：

`exchange.domain.com|exchange_2000sp3_owa_ruleset。`

## 6.x 与 3.0 的规则集映射

下表列出了 SRA “重写器”规则与 Portal Server 产品先前版本的映射。

表 3-4 与 SP3 的规则映射

Rewriter 6.0 DTD 元素	Rewriter 3.0 列表框名称
<b>HTML 内容规则</b>	
属性 - URL	重写 HTML 属性
属性 - DJS	重写包含 JavaScript 的 HTML 属性
表单	重写表输入标记列表
Applet	重写 Applet/Object 参数值列表

表 3-4 与 SP3 的规则映射

Rewriter 6.0 DTD 元素	Rewriter 3.0 列表框名称
<b>JavaScript 内容规则</b>	
变量 - URL	重写 URL 中的 JavaScript 变量
变量 - EXPRESSION	重写 JavaScript 变量函数
变量 - DHTML	重写 HTML 中的 JavaScript 变量
变量 - DJS	重写 JavaScript 中的 JavaScript 变量
变量 - SYSTEM	重写 JavaScript 系统变量
函数 - URL	重写 JavaScript 函数参数
函数 - EXPRESSION	重写 JavaScript 函数参数功能
函数 - DHTML	重写 HTML 中的 JavaScript 函数参数
函数 - DJS	重写 JavaScript 中的 JavaScript 函数参数
<b>XML 内容规则</b>	
属性 - URL	重写 XML 文档的属性值
TagText	重写“XMI 文档”的“文本”数据
<b>CSS 内容规则</b>	
无需任何规则。默认情况下，会转换所有 URL	
<b>WML 内容规则</b>	
未定义任何规则。WML 以 HTML 方式处理，并应用 HTML 规则。	
<b>WMLScript 内容规则</b>	
不支持 WML 脚本	

# NetFile

本章介绍 NetFile 并对其操作进行说明。有关配置 NetFile 的信息，请参阅第 283 页的第 10 章“配置 NetFile”。

本章包括以下主题：

- [NetFile 概述](#)
- [支持的文件访问协议](#)
- [启用对 NetFile 的访问](#)
- [启用 NetFile 的日志](#)
- [配置 UNIX 验证](#)

## NetFile 概述

NetFile 是一个文件管理器应用程序，它允许用户对远程文件系统和目录进行访问和操作。

SRA 的 NetFile 组件以 Java1 和 Java2 applet 形式提供。如果用户的浏览器无 Java2 插件，可以使用 Java1 applet。Java2 applet 具有更加理想的界面，同时使访问更轻松。

NetFile 提供了以下关键功能：

- 添加或删除共享或文件夹的工具
- 文件上载与下载
- 搜索文件与文件夹
- 使用 GZIP 和 ZIP 压缩文件

- NetFile 环境中的邮件工具
- 保存当前的 NetFile 会话信息
- 拖放文件

有关配置 NetFile 的信息，请参阅第 10 章“配置 NetFile”。

## 支持的文件访问协议

NetFile 允许您使用 FTP、JCIFS (Windows) 以及 NFS 协议访问远程系统。它包括以下文件访问协议功能：

- 如果用户指定使用“自动检测”来添加系统，NetFile 会按照以下顺序自动检测要使用的协议：
  - 检查端口 21 上 FTP 服务器的主机。如果 FTP 响应包含字符串 "NetWare"，则将其视为 NETWARE 主机。
  - 检查端口 2049 上 NFS 服务器的主机。
  - 检查端口 139 上 Windows 主机。
  - 如果上述操作均失败，将显示消息：无法确定主机类型。

检测到的第一个文件系统类型将被用于连接所请求的主机。主机检测顺序可在 Identity Server 管理控制台 中进行更改。

---

**注意** 如果服务器正在非标准端口上运行，则连接会失败。

---

- NetFile 允许用户选择所喜爱的文件服务器和协议。  
针对这些协议中的每一项，下面列出了所支持的平台。

**表 4-1** 文件系统和支持的协议

文件系统 / 协议	平台
NFS	Solaris 2.6 及更高版本
JCIFS	Windows 95/98/NT/2000/ME/XP

表 4-1 文件系统和支持的协议

文件系统 / 协议	平台
FTP	运行于 Novell Netware 上的 Novell FTP 5.1 Server 运行于 Win NT 4.0 上的 MS FTP Server 4.0 运行于 Win NT 2000 上的 MS FTP Server 5.0 Solaris FTP Server WU_FTP 2.6.1 ProFTPD 1.2.8 vsFTPd 1.2.0

**注意** 只有通过 FTP 服务器才支持 Novell Netware，本地访问不支持。

**注意** 要使用 NetFile 将文件上传到 ProFTPD 服务器，需要在运行 ProFTPD 服务器的主机中将 `proftpd.conf` 文件中的 "AllowStoreRestart" 设置为 "on"。

## 启用对 NetFile 的访问

安装 SRA 时，仅会为您在安装期间所指定的组织注册 NetFile 服务。

### ► 为组织与用户启用 NetFile

1. 向要求 NetFile 访问的组织注册 NetFile 服务。
2. 基于 NetFile 服务创建 NetFile 策略，并为要求访问 NetFile 的组织角色指定 NetFile 策略。
3. 为要求访问 NetFile 的每位用户分配 NetFile 服务。

有关创建并分配策略与服务的详细信息，请参阅《*Identity Server 管理指南*》。

## 启用 NetFile 的日志

使用“Identity Server 日志”服务指定日志位置以启用 NetFile 的日志。日志文件的名称为 `srapNetFile`。默认情况下，它位于 `/var/opt/SUNWam/logs` 目录中。

## 配置 UNIX 验证

### ► 启用 Unix 验证

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 从管理控制台中选择“身份认证管理”选项卡。
3. 从左边视图窗格中的“视图”下拉菜单中选择“服务”。  
如果 UNIX 显示在右边的视图窗格中，则它需要注册。
4. 可通过选择 UNIX 旁边的复选框注册服务，请单击“注册”。
5. 单击左边视图窗格中 UNIX 旁边的箭头并单击“创建”。  
创建服务模板。
6. 单击“保存”。
7. 注销管理控制台。
8. 以超级用户 (root) 身份或配置为运行 Identity Server 的用户的身份重新启动 Identity Server:

```
/etc/init.d/amserver startall
```

9. 验证 doUnix 进程是否正在运行:

```
ps -ef | grep doUnix
```

### ► 配置 Unix 验证

1. 远程登录到配置端口上的本地主机，如下所示：  

```
telnet localhost 58946
```
2. 键入“Unix Helper 监听端口”号。  
为“监听端口”指定默认值 57946。
3. 键入“Unix Helper 会话超时”值（以秒为单位）。

4. 键入 “Unix Helper 最大会话数” 值。  
显示消息 “doUnix 配置成功”。



# Netlet

本章介绍如何使用 Netlet 在用户远程桌面与内部网中正运行应用程序的服务器之间安全地运行应用程序。要配置 Netlet，请参阅第 305 页的第 11 章“配置 Netlet”。

本章包括以下主题：

- [Netlet 概述](#)
- [从远程主机下载 Applet](#)
- [定义 Netlet 规则](#)
- [Netlet 规则示例](#)
- [启用 Netlet 日志](#)
- [在 Sun Ray 环境中运行 Netlet](#)

## Netlet 概述

Sun Java™ System Portal Server 软件用户可能希望以安全方式在其远程桌面上运行流行的或公司所特定的应用程序。通过在您的平台上设置 Netlet，可提供对这些应用程序的安全访问。

Netlet 使用户可以在不安全的网络上（如 Internet）安全地运行常用 TCP/IP 服务。您可以运行 TCP/IP 应用程序（如 Telnet 和 SMTP）、HTTP 应用程序及任何固定端口应用程序。

如果应用程序基于 TCP/IP 或者使用固定端口，则可以通过 Netlet 运行。

---

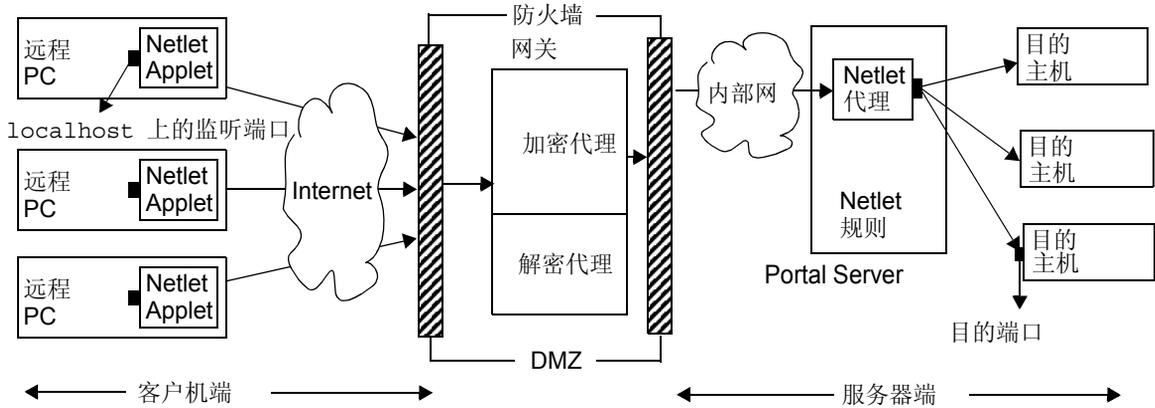
**注意** 仅当使用 FTP 时才支持动态端口。要使用 Microsoft Exchange，请使用 OWA (Outlook Web Access)。

---

# Netlet 组件

Netlet 使用的各种组件如图 5-1 所示。

图 5-1 Netlet 组件



## localhost 上的监听端口

这是 Netlet applet 在其上进行监听的客户机中的端口。客户机为 localhost。

## Netlet Applet

Netlet applet 负责在远程客户机与内部网应用程序（如 Telnet、Graphon 或 Citrix）之间设置加密 TCP/IP 通道。applet 将信息包加密，并将其发送至网关，然后解密来自网关的响应信息包，并将其发送至本地应用程序。

对于静态规则，当用户登录到门户时，将自动下载 Netlet applet。对于动态规则，当用户单击对应于动态规则的链接时，会下载 applet。有关静态和动态规则的详细信息，请参阅第 188 页的“规则类型”。

要在“Sun Ray 环境”中运行 Netlet，请参阅第 201 页的“在 Sun Ray 环境中运行 Netlet”。

## Netlet 规则

Netlet 规则会将需要在客户机上运行的应用程序映射到相应的目的主机中。这意味着 Netlet 仅适用于发送至在 Netlet 规则中所定义端口的信息包。这将确保更高的安全性。

作为管理员，您需要为 Netlet 的运行配置特定规则。这些规则指定各种细节，如要使用的密码、要调用的 URL、要下载的 applet、目的端口以及目的主机。当客户机上的用户通过 Netlet 发出请求时，这些规则有助于确定建立连接必须采用的方式。有关详细信息，请参阅第 185 页的“定义 Netlet 规则”。

## Netlet 提供者

这是 Netlet 的 UI 组件。提供者允许用户从 Portal Server, Secure Remote Access 桌面配置所需的应用程序。提供者中创建了一个链接，用户单击此链接可运行所需的应用程序。用户也可针对桌面 Netlet 提供者的动态规则指定目的主机。请参阅第 185 页的“定义 Netlet 规则”。

## 加密代理

所有客户机请求均通过“加密代理”进行发送。“加密代理”仅处理 Netlet 请求，并将其他所有请求传递至“解密代理”。“加密代理”分析 Netlet 请求，并将其传递至 Netlet 代理（如果已启用），或直接传递至目的主机。

## Netlet 代理（可选）

网关可确保远程客户机与网关之间的通道安全。Netlet 代理是可选的，在安装期间可以选择不安装此代理。有关 Netlet 代理的信息，请参阅第 65 页的“使用 Netlet 代理”。

## 目的端口

这是目的应用程序的主机在其上进行监听的端口。

# Netlet 使用方案

Netlet 的使用涉及下列一系列事件：

1. 远程用户登录至 Portal Server, Secure Remote Access 桌面。

2. 如果已为用户、角色或组织定义了静态 Netlet 规则，则自动将 Netlet applet 下载到远程客户机中。

如果已为用户、角色或组织定义了动态规则，则用户需要在 Netlet 提供者中配置所需的应用程序。当用户单击 Netlet 提供者中的应用程序链接时，将下载 Netlet applet。有关静态和动态规则的详细信息，请参阅第 185 页的“定义 Netlet 规则”。

3. Netlet 将监听在 Netlet 规则中定义的本地端口。
4. Netlet 将通过 Netlet 规则中指定的端口在远程客户机与主机之间设置一个通道。

## 使用 Netlet

为了使 Netlet 能够根据不同组织中各个用户的需要进行工作，您需要完成以下操作：

1. 根据用户要求，确定需要创建静态规则还是动态规则。请参阅第 188 页的“规则类型”。
2. 从 Identity Server 管理控制台上的“服务配置”选项卡中定义 Netlet 模板中的全局选项。请参阅第 305 页的第 11 章“配置 Netlet”。
3. 确定规则应基于组织、角色还是用户，并按照需要在每一级别进行修改。有关组织、角色以及用户的详细信息，请参阅 *Portal Server 管理指南*。

---

**注意** 请勿本地化 `srapNetletServlet.properties` 文件中框架集参数的值。

---

## 从远程主机下载 Applet

有时，URL 会返回一个页面，该页面包含需要从远程机器获取的嵌入式 applet。但是，Java 安全性只允许 applet 与作为其下载来源的主机进行通信。要允许 applet 通过本地网络端口与网关进行通信，您需要检查 Identity Server 管理控制台上的“下载 Applet”字段，并指定以下语法：

*local-port:server-host:server-port*

其中

*local-port* 是 Netlet 监听来自 applet 的通信量的本地端口

*server-host* 是 applet 的下载源

*server-port* 是用于下载 applet 的端口

## 定义 Netlet 规则

Netlet 配置通过 Netlet 规则进行定义，而这些规则在“SRA 配置”部分下的 Identity Server 管理控制台中配置。可以为组织、角色或用户配置 Netlet 规则。如果为角色或用户配置 Netlet 规则，请在选择组织后选择所需的角色或用户。

---

**警告** Netlet 规则不支持多字节条目。请勿为 Netlet 规则中的任何可编辑字段指定多字节字符。

Netlet 规则不可包含任何高于 64000 的端口号。

---

表 5-1 列出了 Netlet 规则中的字段。

**表 5-1** Netlet 规则中的字段

参数	说明	值
规则名	指定 Netlet 规则的名称。需要为每一规则指定一个唯一的名称。这在定义用户对指定规则的访问权限时是很有用的。有关详细信息，请参阅第 314 页的“定义 Netlet 访问规则”。	
加密密码	定义加密密码，或指定用户可从中进行选择的密码列表。	您所选择的密码会以列表形式出现在 Netlet 提供者中。用户可从选定列表中选择所需的密码。 默认值 - 使用在 Netlet 管理控制台中指定的“默认 VM 本地密码”和“默认 Java Plugin 密码”。

表 5-1 Netlet 规则中的字段

参数	说明	值
URL	指定当用户在 Netlet 提供者中单击相关链接时浏览器所打开的 URL。浏览器打开应用程序的窗口，并连接到本地端口号（稍后在规则中指定）处的 localhost。 您需要指定相关的 URL。	由 Netlet 规则所调用的应用程序的 URL。例如， telnet://localhost:30000。 如果应用程序使用 applet 调用应用程序，请指定一个 URL。 空 - 当应用程序不是由 URL 启动或者由桌面进行控制时，用户所设定的值。对于不基于网络的应用程序而言该项通常为 true。
下载 Applet	指示是否有必要为本规则下载 applet。	False - 不下载 applet。 True - 使用回环端口从 Portal Server 机器下载 applet。 以 local-port:server-host:server-port 格式指定 applet 详细信息，其中： <ul style="list-style-type: none"> <li>local-port 表示客户机上的目的端口。该端口必须不同于默认回环端口。有关详细信息，请参阅第 11 章“配置 Netlet”。为每一规则指定一个唯一的 local port。</li> <li>server-host 是从中下载 applet 的服务器名称。</li> <li>server-port 代表服务器上用于下载 applet 的端口。</li> </ul> 如果要下载 applet，且未指定服务器，则从 Portal Server 主机下载 applet。
扩展会话	当 Netlet 处于活动状态时，它控制 Portal Server 会话的空闲超时。	启用 - 当只有 Netlet 处于活动状态而其余门户应用程序空闲时，该项为门户会话保持活动状态所必需。 禁用 - 即使 Netlet 应用程序处于活动状态而其余门户应用程序空闲，在会话空闲超时的时候门户会话空闲也会超时。

表 5-1 Netlet 规则中的字段

参数	说明	值
本地端口	Netlet 进行监听的客户机上的端口。	<p><i>local-port</i> 的值必须是唯一的。不能在一个以上的规则中指定特定端口号。</p> <p>如果要为多个连接指定多台主机，需指定多个本地端口。有关语法，请参阅第 193 页的“具有多个主机连接的静态规则”。</p> <p>对于 FTP 规则，本地端口值必须是 30021</p>
目的主机	Netlet 连接的收件人。	<p><i>host</i> - 接收 Netlet 连接的主机名。它用于静态规则中。使用简单主机名，如 <i>siroe</i>，或全限定 DNS 样式的主机名，如 <i>siroe.mycompany.com</i>。下列情况请指定多台主机：</p> <ul style="list-style-type: none"> <li>与指定的每一台主机建立连接。需要为指定的每一台主机指定相应的客户机与目的端口。有关语法，请参阅第 193 页的“具有多个主机连接的静态规则”。</li> <li>尝试连接到指定主机列表中的任何一台可用主机。有关语法，请参阅第 194 页的“具有多主机选择的静态规则”。</li> </ul> <p>TARGET - 在语法中指定 TARGET 的规则为动态规则。TARGET 表示最终用户可在桌面 Netlet 提供者中指定所需目的主机或主机。</p> <p>单个规则中不能同时具有静态主机和 TARGET。</p>

表 5-1 Netlet 规则中的字段

参数	说明	值
目的端口	目的主机上的端口	<p>除主机与目的主机外，还必须要指定一个目的端口。在有多台目的主机的情况下，可以指定多个目的端口。以 <code>port1+port2+port3-port4+port5</code> 格式指定多个端口。</p> <p>端口号之间的加号 (+) 表示某单一主机的备选端口。</p> <p>端口号之间的减号 (-) 是不同目的主机端口号之间的分隔符。</p> <p>在此，Netlet 按顺序依次使用 <code>port1</code>、<code>port2</code> 和 <code>port3</code>，以尝试连接到指定的第一台目的主机。如果失败，Netlet 使用 <code>port4</code> 和 <code>port5</code>（按此顺序）以尝试连接到第二台主机。</p> <p>只可为静态规则配置多个端口。</p>

对于要从 Portal Server 获得会话通知的网关，需添加以下内容：

```
com.ipplanet.am.jassproxy.trustAllServerCerts=true
```

至以下属性文件

```
/etc/opt/SUNWam/config/AMConfig.properties（在 Portal Server 上）
```

2. 重新启动 Identity Server。

## 规则类型

根据规则中目的主机的指定方式，将 Netlet 规则分为两种类型。

## 静态规则

静态规则将目的主机指定为规则的一部分。如果创建静态规则，用户就无权指定所需的目的主机。在下面的示例中，`sesta` 是目的主机。

规则名称	加密密码	URL	下载 Applet	扩展会话	本地端口	目的主机	目的端口
ftpstatic	SSL_RSA_WITH_RC4_128_MD5	null	false	true	30021	sesta	21

可为静态规则配置多台目的主机和多个端口。有关示例，请参阅第 193 页的“具有多个主机连接的静态规则”。

## 动态规则

在动态规则中，目的主机不指定为规则的一部分。用户可以在 Netlet 提供者中指定所需的目的主机。在下面的示例中，`TARGET` 是目的主机的占位符。

规则名称	加密密码	URL	下载 Applet	扩展会话	本地端口	目的主机	目的端口
ftpdynamic	SSL_RSA_WITH_RC4_128_MD5	null	false	true	30021	TARGET	21

## 加密密码

根据加密密码，可将 Netlet 规则进一步分类如下：

- **用户可配置密码规则** - 在此规则中，您可以指定一个用户可从中进行选择的密码列表。这些可选密码以列表形式出现在 Netlet 提供者中。用户可从该列表中选择所需的密码。在下面的示例中，用户可从多个密码中进行选择。

规则名称	加密密码	URL	下载 Applet	扩展会话	本地端口	目的主机	目的端口
Telnet	SSL_RSA_WITH_RC4_128_SHA SSL_RSA_WITH_RC4_128_MD5	null	false	true	30000	TARGET	23

---

**注意** 尽管 Portal Server 主机可能启用了多个不同的密码，但用户可以从作为 Netlet 规则一部分而配置的密码列表中进行选择。

---

有关 Netlet 所支持的密码列表，请参阅第 190 页的“支持的密码”。

- **管理员配置密码规则** - 在此规则中，密码被定义为 Netlet 规则的一部分。用户无权选择所需的密码。在下面的示例中，密码被配置为 SSL\_RSA\_WITH\_RC4\_128\_MD5。

规则名称	加密密码	URL	下载 Applet	扩展会话	本地端口	目的主机	目的端口
Telnet	SSL_RSA_WITH_RC4_128_MD5	null	false	true	30000	TARGET	23

有关 Netlet 所支持的密码列表，请参阅第 190 页的“支持的密码”。

## 支持的密码

表 5-2 列出了 Netlet 所支持的密码列表。

**表 5-2** 支持密码的列表

### 密码

#### 本地 VM 密码

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 密码

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

---

**表 5-2** 支持密码的列表**密码**

SSL\_RSA\_WITH\_DES\_CBC\_SHA

SSL\_RSA\_WITH\_NULL\_MD5

**向后兼容性**

Portal Server 的早期版本不支持将密码作为 Netlet 规则的一部分。考虑到不带密码的现有规则的向后兼容性，这些规则将使用默认密码。不带密码的现有规则，如：

规则名称	加密密码	URL	下载 Applet	扩展会话	本地端口	目的主机	目的端口
Telnet		telnet://localhost:3000	false	true	30000	TARGET	23

会被解释为：

规则名称	加密密码	URL	下载 Applet	扩展会话	本地端口	目的主机	目的端口
Telnet	默认密码	telnet://localhost:30000	false	true	30000	TARGET	23

这与将“加密密码”字段选为“默认值”的“管理员配置规则”相似。有关详细信息，请参阅第 309 页的“指定默认加密密码”。

**注意** Netlet 规则不可包含任何高于 64000 的端口号。

## Netlet 规则示例

本部分包含 Netlet 规则的几个示例以说明 Netlet 语法的作用机理。

- 基本静态规则
- 具有多个主机连接的静态规则
- 调用 URL 的动态规则
- 下载 Applet 的动态规则

### 基本静态规则

该规则支持客户机与 `sesta` 机器之间的 Telnet 连接。

规则名称	加密密码	URL	下载 Applet	扩展会话	本地端口	目的主机	目的端口
myrule	SSL_RSA_WITH_RC4_128_MD5	null	false	true	1111	sesta	23

其中

`myrule` 是规则名称。

`SSL_RSA_WITH_RC4_128_MD5` 表示要使用的密码。

`null` 表示该应用程序并非由 URL 调用或通过桌面运行。

`false` 表示客户机在运行该应用程序时并不下载 applet。

`true` 表示当 Netlet 连接处于活动状态时 Portal Server 不应超时。

`1111` 是客户机上的端口，Netlet 在此监听来自目的主机的连接请求。

`sesta` 是 Telnet 连接中的接收方主机名称。

`23` 是目的主机的连接端口号，在本例中为众所周知的 Telnet 端口。

桌面 Netlet 提供者不显示链接，但 Netlet 会自动启动，并监听指定端口 (1111)。指示用户启动连接到端口 1111 上的 localhost 的客户机软件（在本例中为 Telnet 会话）。

例如，要启动 Telnet 会话，客户需要在终端的 UNIX 命令行中键入以下内容：

```
telnet localhost 1111
```

## 具有多个主机连接的静态规则

该规则支持从客户机到两台主机 `sesta` 与 `siroe` 的 Telnet 连接。

规则名称	加密密码	URL	下载 Applet	扩展会话	本地端口	目的主机	目的端口
myrule	SSL_RSA_WITH_RC4_128_MD5	null	false	true	1111	sesta	23
					1234	siroe	23

其中

23 是目的主机的连接端口号 `n` 即 Telnet 的保留端口。

1111 是客户机上的端口，Netlet 在此监听来自第一台目的主机 `sesta` 的连接请求。

1234 是客户机上的端口，Netlet 在此监听来自第二台目的主机 `siroe` 的连接请求。

该规则中的前六个字段与第 192 页的“基本静态规则”中的字段相同。区别在于标识第二台目的主机的另外三个字段。

在向规则中添加附加目标时，必须为每一台新目的主机添加三个字段，即 `local port`、`destination host` 以及 `destination port`。

---

**注意** 您可以用多组三字段来描述与每一目的主机的连接。如果远程客户机是基于 UNIX 的，切不可使用小于 2048 的监听端口号，因为编号较低的端口将受限制，而且您必须是根用户才能启动监听器。

---

该规则与前一规则作用相同。Netlet 提供者不显示任何链接，但 Netlet 会自动启动，并监听指定的两个端口（1111 和 1234）。用户需要启动客户机软件（在本例中为 Telnet 会话），它将连接至端口 1111 上的 localhost 或端口 1234 上的 localhost，以便连接到主机 example2。

### 具有多主机选择的静态规则

使用该规则可指定多台备选主机。如果与规则中第一台主机连接失败，Netlet 会尝试连接指定的第二台主机，依此类推。

规则名称	加密密码	URL	下载 Applet	扩展会话	本地端口	目的主机	目的端口
gojoe	SSL_RSA_WITH_RC4_128_MD5	/gojoe.html	8000:gojoeserver:8080	true	10491	siroe+sesta	35+26+491-35+491

其中

10491 是客户机上的端口，Netlet 在此监听来自目的主机的连接请求。

依据端口的可用性，Netlet 将依次尝试通过端口 35、端口 26 和端口 491 与 siroe 建立连接。

如果无法连接到 siroe，Netlet 会依次尝试通过端口 35 和 491 连接 sesta。

主机之间的加号 (+) 表示备选主机。

端口号之间的加号 (+) 表示某单一目的主机的备选端口。

端口号之间的减号 (-) 是不同目的主机端口号之间的分隔符。

## 调用 URL 的动态规则

该规则允许用户配置所需的目的地主机，从而使用户可通过 Netlet 远程登录到各个主机上。

规则名称	加密密码	URL	下载 Applet	扩展会话	本地端口	目的地主机	目的地端口
myrule	SSL_RSA_WITH_RC4_128_MD5	telnet://localhost:30000	false	true	30000	TARGET	23

其中

myrule 是规则名称。

SSL\_RSA\_WITH\_RC4\_128\_MD5 表示要使用的密码。

telnet://localhost:30000 是由规则所调用的 URL。

false 表示将不会下载任何 applet。

Extend Session(true) 表示当 Netlet 连接处于活动状态时 Portal Server 不应超时。

30000 是客户机上的端口，Netlet 在此监听针对该规则的连接请求。

TARGET 表示目的地主机需要由用户使用 Netlet 提供者进行配置。

23 是由 Netlet 打开的目的地主机上的端口，在本例中为众所周知的用于 Telnet 的端口。

### † 在添加规则之后运行 Netlet

添加该规则之后，用户必须要完成一些步骤才能使 Netlet 按照预期方式运行。用户需要在客户端执行以下操作：

1. 在标准 Portal Server 桌面的 Netlet 提供者部分单击“编辑”。  
在“添加新目标”部分的“规则名称”下面会列出新的 Netlet 规则。
2. 选择规则名称，并键入目的地主机的名称。
3. 保存更改。

用户返回桌面，同时在 Netlet 提供者部分会看到新的链接。

#### 4. 单击新链接。

将会启动一个新的浏览器，转至 Netlet 规则中给出的 URL。

---

**注意** 通过重复以上步骤可以为同一规则添加多台目的主机。

---

### 下载 Applet 的动态规则

该规则将在客户机与动态分配的主机之间定义 GO-Joe 连接。它会从 applet 所处的服务器上将 GO-Joe applet 下载到客户机中。

规则名称	加密密码	URL	下载 Applet	扩展会话	本地端口	目的主机	目的端口
gojoe	SSL_RSA_WITH_RC4_128_MD5	/gojoe.html	8000:gojoe serve:8080	true	3399	TARGET	58

其中

gojoe 是规则名称。

SSL\_RSA\_WITH\_RC4\_128\_MD5 表示要使用的密码。

例如，/gojoe.html 是包含 applet 的 HTML 页的路径，该路径应相对于部署门户的网络容器的文档根。

8000:server:8080 指明端口 8000 是用于接收 applet 的客户机上的目的端口，gojoeserve 是提供 applet 的服务器的名称，8080 则是自其下载 applet 的服务器上的端口。

Extended Session (true) 表示当 Netlet 连接处于活动状态时 Portal Server 不应超时。

3399 是客户机上的端口，Netlet 在此监听该类型的连接请求。

TARGET 表示目的主机需要由用户使用 Netlet 提供者进行配置。

58 是由 Netlet 所打开的目的主机上的端口，在本例中为 GoJoe 的端口。端口 58 是目的主机监听其自身通信量的端口。Netlet 将信息从新 applet 传递至该端口。

# Netlet 规则示例

表 5-3 列出了一些常见应用程序的 Netlet 规则示例。

该表由 7 列组成，分别对应于 Netlet 规则中的以下字段：规则名称、URL、下载 Applet、本地端口、目的主机、目的端口。最后一列中包括对规则的描述。

**注意** 表 5-3 未列出 Netlet 规则的“密码”与“扩展会话”字段。对于所提供的示例，假定这两个字段分别为 "SSL\_RSA\_WITH\_RC4\_128\_MD5" 和 "true"。

表 5-3 Netlet 规则示例

规则	URL	下载 Applet	本地端口	目的主机	目的端口	说明
IMAP	null	false	10143	imapserver	143	客户机端的 Netlet local port 不必与服务器端的 destination port 相同。如果您使用的不是标准的 IMAP 和 SMTP 端口，请确保配置客户机以将其连接在不同于标准端口的端口上。  Solaris 客户机用户在连接到端口号小于 1024 的端口时会遇到麻烦，除非他们以根用户身份运行。
SMTP	null	false	10025	smtpserver	25	
Lotus 网络客户机	null	false	80	lotus-server	80	该规则将指示 Netlet 监听端口 80 上的客户机，并连接到端口 80 上的 lotus-server 服务器。“Lotus 网络客户机”要求客户机监听端口必须与服务器端口匹配。

表 5-3 Netlet 规则示例

规则	URL	下载 Applet	本地端口	目的主机	目的端口	说明
Lotus Notes 非网络客户机	null	false	1352	lotus-domino	1352	<p>利用此项规则，Lotus Notes 客户机可以通过 Netlet 连接到 Lotus Domino 服务器。需确保在客户机尝试连接到服务器时，它切不可指向作为服务器名称的 localhost。它必须指向 Lotus Domino 服务器的实际服务器名称。服务器名称必须与服务器的系统名称相同。当使用 Netlet 时，客户机必须将该名称解析为 127.0.0.1。有两种方法可实现此目的：</p> <ul style="list-style-type: none"> <li>• 在客户机主机表中设置服务器名称使其指向 127.0.0.1。</li> <li>• 导出指向 127.0.0.1 的服务器名称的 DNS 条目。</li> </ul> <p>服务器名称必须是安装期间用于配置 Domino 服务器的同一服务器名称。</p>

表 5-3 Netlet 规则示例

规则	URL	下载 Applet	本地端口	目的主机	目的端口	说明
Microsoft Outlook 与 Exchange Server 它不适用于 Windows NT、2000 和 XP。对于 Windows NT、2000 和 XP，请借助于“重写器”使用 Outlook Web Access。	null	false	135	exchange	135	<p>该规则指示 Netlet 在客户机的端口 135 上监听，并连接到端口 135 上的服务器 exchange。Outlook 客户机使用此端口进行联系 Exchange 服务器的首次尝试，并确定和该服务器通话时要使用的后续端口。</p> <p>在客户机上：</p> <ul style="list-style-type: none"> <li>• 用户必须将 Exchange 服务器（在 Outlook 客户机中进行配置）的主机名更改为 localhost。该选项的位置随 Outlook 版本的不同而不同。</li> <li>• 用户必须使用主机文件将 Exchange 服务器的主机名（单一且全限定）映射到 IP 地址 127.0.0.1。</li> <li>• 在 Windows 95 或 98 中，该文件位于 \Windows\Hosts 下</li> <li>• 在 Windows NT4 中，该文件位于 \WinNT\System32\drivers\etc\Hosts 下。</li> </ul> <p>该项形式如下：</p> <pre>127.0.0.1 exchange exchange.company.com</pre> <p>Exchange 服务器将其本身的名称发送回 Outlook 客户机。该映射可确保 Outlook 客户机使用 Netlet 客户机连接回服务器。</p>

表 5-3 Netlet 规则示例

规则	URL	下载 Applet	本地端口	目的主机	目的端口	说明
FTP	null	false	30021	<i>your-ftp_server.your-domain</i>	21	您可以利用所控制的最终用户帐户为“FTP 服务器”提供 FTP 服务。这可确保在最终用户系统和单一位置之间进行安全的远程 FTP 传输。若无用户名，则将 FTP URL 解释为一个匿名的 FTP 连接。 您必须将端口 30021 定义为 Netlet FTP 规则的本地端口。 使用 Netlet 连接不支持动态 FTP。
Netscape 4.7 邮件客户机	null	false	30143, 30025.	TARGET TARGET	10143 10025	在 Netscape 客户机中，用户需要指定： 用于 IMAP 或接收邮件的 localhost:30143 用于 SMTP 或发送邮件的 localhost:30025
Graphon	third_party/xsession_start.html	true	10491	TARGET	491	这是用于通过 Netlet 访问 Graphon 的规则。 xsession_start.html 与 Graphon 捆绑在一起。
Citrix	third_party/citrix_start.html	true	1494	TARGET	1494	这是用于通过 Netlet 访问 Citrix 的规则。citrix_start.html 与 Citrix 捆绑在一起。
远程控制	third_party/pca_start.html	true	5631 5632	TARGET TARGET	5631 5632	这是用于通过 Netlet 访问“远程控制”的规则。pca_start.html 与“远程控制”捆绑在一起。

## 启用 Netlet 日志

您可以在网关服务中启用 Netlet 相关活动的日志。请参阅第 280 页的“启用 Netlet 日志”。在“日志位置”属性中指定的目录内将会创建日志文件，作为“Identity Server 配置”属性“日志”的一部分。

日志文件命名惯例如下：

*srapNetlet\_gateway-hostname\_gateway-profile-name*

Netlet 日志会捕捉以下信息:

- 开始时间
- 源地址
- 源端口
- 服务器地址
- 服务器端口
- 停止时间
- 状态 (开始或停止)

## 在 Sun Ray 环境中运行 Netlet

如果您要在 Sun Ray 环境中运行需要将 applet 下载到客户机上的应用程序, 就需要更改 HTML 文件。这里是一个示例文件, 向您显示需要完成的必要修改。

### 新 HTML 文件

```
<!-- @(#)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>

```

## 弃用的 HTML 文件:

```

<html>
<body>
<applet code="com.citrix.JICA.class" archive="JICAEngN.jar" width=800 height=600>
<param name="cabbase" value="JICAEngM.cab">
<param name="address" value="localhost">
<param name=ICAPortNumber value=1494>
</applet>
</body></html>

```

在 Sun Ray 环境中运行 Netlet

## 具有 PDC 的 Netlet

本章介绍如何配置客户机浏览器的 Java Plugin，以使 Netlet 能够与 PDC 一起使用。

---

**注意** 只有具有 JSSE 的“虚拟机”(VM)才支持具有 PDC 的 Netlet。

---

### 为 PDC 配置 Netlet

#### † 为 PDC 配置 Netlet

1. 用下列格式之一从浏览器中导出客户机证书：

- PKCS
- JKS

导出客户机证书后，Java Plugin 应该具有以下允许 VM 使用该证书的 JVM 参数：

```
javax.net.ssl.keyStoreType
```

```
javax.net.ssl.keyStorePassword
```

```
javax.netl.ssl.keyStore
```

2. 转至“控制面板”然后转至“启动 Java Plugin”
3. 选择“高级”选项卡，然后选择“Java 运行时环境”

4. 指定“Java 运行时参数”。例如：  
Djavax.net.ssl.keyStoreType=pkcs  
Djavax.net.ssl.keyStorePassword=testing123  
Djavax.netl.ssl.keyStore="C:\dir\test.cert"
5. 单击“应用”。
6. 关闭 Java plugin，然后重新启动相关的浏览器。

# 证书

本章介绍证书管理并说明如何安装自签名证书和来自“证书授权机构”的证书。

本章包括以下主题：

- [SSL 证书概述](#)
- [证书文件](#)
- [证书委托属性](#)
- [CA 委托属性](#)
- [certadmin 脚本](#)
- [生成自签名证书](#)
- [安装来自证书授权机构的 SSL 证书](#)
- [添加根 CA 证书](#)
- [修改证书的委托属性](#)
- [列出根 CA 证书](#)
- [列出所有证书](#)
- [删除证书](#)
- [打印证书](#)

## SSL 证书概述

Portal Server Secure Remote Access 软件为远程用户提供基于证书的验证。SRA 使用“加密套接字层”(SSL)启用安全通信。SSL 协议可在两台机器之间实现安全通信。

SSL 证书使用公共和私有密钥对提供加密和解密功能。

有两种类型的证书：

- 自签名证书（也称为根 CA 证书）
- 由证书授权机构 (CA) 签发的证书

默认情况下，当安装网关时，将会生成并安装自签名证书。

在安装后，您可随时生成、获取或替换证书。

SRA 也支持以“个人数字证书”(PDC)进行客户机验证。PDC 是一个通过 SSL 客户机验证来验证用户的机制。进行 SSL 客户机验证时，SSL 信号交换将在网关结束。网关抽取用户的 PDC 并将其传递给已验证的服务器。该服务器使用 PDC 验证用户。要同时配置 PDC 与“验证链”，请参阅第 76 页的“使用验证链”。

SRA 提供名为 `certadmin` 的工具，可使用它来管理 SSL 证书。请参阅第 214 页的“`certadmin` 脚本”。

## 证书文件

证书相关文件位于 `/etc/opt/SUNWps/cert/default/gateway-profile-name`。默认情况下，此目录包含 5 个文件。

表 7-1 列出这些文件及其说明。

表 7-1 证书文件

文件名	类型	说明
cert8.db, key3.db, secmod.db	二进制	包含证书、密钥和加密模块的数据。 可使用 certadmin 脚本处理。 和 Sun Java™ System Web Server 所使用的数据库文件具有相同的格式，并且位于 <i>portal-server-install-root/SUNWwbsvr/alias</i> 。 如有必要，可在 Portal Server 主机和网关组件或网关之间共享这些文件。
.jsspass	隐藏文本文件	包含 SRA 密钥数据库的加密口令。
.nickname	隐藏文本文件	存储网关需要在 <i>token-name:certificate-name</i> 格式中使用的令牌和证书名。 如果您使用的是默认令牌（默认内部软件加密模块上的令牌），则省略令牌名。多数情况下，.nickname 文件仅存储证书名。 作为管理员，您可在此文件中修改证书名。您指定的证书此时将由网关使用。

## 证书委托属性

证书的委托属性表明以下信息：

- 该证书（如客户机或服务器证书）是否由“委托 CA”发放。
- 证书（如根证书）是否可受委托作为服务器或客户机证书的签发人。

对于每一证书均有三种可用的委托类别，按如下顺序表示：“SSL、电子邮件、对象登记”。对于网关，仅第一类别有用。在每一类别位置中，将使用多个或不使用任何委托属性代码。

类别的属性代码以逗号分隔，并且整个属性组由引号括在其中。例如，在网关安装期间生成并安装的自签名证书被标记为“u,u,u”，它表示该证书是与根 CA 证书相对的服务器证书（用户证书）。

表 7-2 列出可能的属性值及每个值的含义。

**表 7-2** 证书委托属性

属性	说明
p	有效同级
P	委托同级（暗示 p）
c	有效 CA
T	签发客户机证书的委托 CA（暗示 c）
C	签发服务器证书的委托 CA（仅限 SSL）（暗示 c）
u	证书可用于验证或登记
w	发送警告（当证书在该环境中使用时，与其他属性一起使用以包括警告）

## CA 委托属性

证书数据库中包含大多数众所周知的公共 CA。有关修改公共 CA 之委托属性的信息，请参阅第 225 页的“修改证书的委托属性”。

表 7-3 列出带有委托属性的最常见“证书授权机构”。

**表 7-3** 公共证书授权机构

证书授权机构名	委托属性
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

表 7-3 公共证书授权机构

Thawte Personal Premium CA	CPp,CPp,CPp
Thawte Personal Freemail CA	CPp,CPp,CPp
Thawte Server CA	CPp,CPp,CPp
Thawte Premium Server CA	CPp,CPp,CPp
American Express CA	CPp,CPp,CPp
American Express Global CA	CPp,CPp,CPp
Equifax Premium CA	CPp,CPp,CPp
Equifax Secure CA	CPp,CPp,CPp
BelSign Object Publishing CA	CPp,CPp,CPp
BelSign Secure Server CA	CPp,CPp,CPp
TC TrustCenter, Germany, Class 0 CA	CPp,CPp,CPp
TC TrustCenter, Germany, Class 1 CA	CPp,CPp,CPp
TC TrustCenter, Germany, Class 2 CA	CPp,CPp,CPp
TC TrustCenter, Germany, Class 3 CA	CPp,CPp,CPp
TC TrustCenter, Germany, Class 4 CA	CPp,CPp,CPp
ABAecom (sub., Am. Bankers Assn.)Root CA	CPp,CPp,CPp
Digital Signature Trust Co. Global CA 1	CPp,CPp,CPp
Digital Signature Trust Co. Global CA 3	CPp,CPp,CPp
Digital Signature Trust Co. Global CA 2	CPp,CPp,CPp
Digital Signature Trust Co. Global CA 4	CPp,CPp,CPp
Deutsche Telekom AG Root CA	CPp,CPp,CPp
Verisign Class 1 Public Primary Certification Authority	CPp,CPp,CPp
Verisign Class 2 Public Primary Certification Authority	CPp,CPp,CPp
Verisign Class 3 Public Primary Certification Authority	CPp,CPp,CPp
Verisign Class 1 Public Primary Certification Authority - G2	CPp,CPp,CPp

**表 7-3** 公共证书授权机构

Verisign Class 2 Public Primary Certification Authority - G2	CPp,CPp,CPp
Verisign Class 3 Public Primary Certification Authority - G2	CPp,CPp,CPp
Verisign Class 4 Public Primary Certification Authority - G2	CPp,CPp,CPp
GlobalSign Root CA	CPp,CPp,CPp
GlobalSign Partners CA	CPp,CPp,CPp
GlobalSign Primary Class 1 CA	CPp,CPp,CPp
GlobalSign Primary Class 2 CA	CPp,CPp,CPp
GlobalSign Primary Class 3 CA	CPp,CPp,CPp
ValiCert Class 1 VA	CPp,CPp,CPp
ValiCert Class 2 VA	CPp,CPp,CPp
ValiCert Class 3 VA	CPp,CPp,CPp
Thawte Universal CA Root	CPp,CPp,CPp
Verisign Class 1 Public Primary Certification Authority - G3	CPp,CPp,CPp
Verisign Class 2 Public Primary Certification Authority - G3	CPp,CPp,CPp
Verisign Class 3 Public Primary Certification Authority - G3	CPp,CPp,CPp
Verisign Class 4 Public Primary Certification Authority - G3	CPp,CPp,CPp
Entrust.net Secure Server CA	CPp,CPp,CPp
Entrust.net Secure Personal CA	CPp,CPp,CPp
Entrust.net Premium 2048 Secure Server CA	CPp,CPp,CPp
ValiCert OCSP Responder	CPp,CPp,CPp
Baltimore CyberTrust Code Signing Root	CPp,CPp,CPp
Baltimore CyberTrust Root	CPp,CPp,CPp
Baltimore CyberTrust Mobile Commerce Root	CPp,CPp,CPp
Equifax Secure Global eBusiness CA	CPp,CPp,CPp
Equifax Secure eBusiness CA 1	CPp,CPp,CPp

表 7-3 公共证书授权机构

Equifax Secure eBusiness CA 2	CPp,CPp,CPp
Visa International Global Root 1	CPp,CPp,CPp
Visa International Global Root 2	CPp,CPp,CPp
Visa International Global Root 3	CPp,CPp,CPp
Visa International Global Root 4	CPp,CPp,CPp
Visa International Global Root 5	CPp,CPp,CPp
beTRUSTed Root CA	CPp,CPp,CPp
Xcert Root CA	CPp,CPp,CPp
Xcert Root CA 1024	CPp,CPp,CPp
Xcert Root CA v1	CPp,CPp,CPp
Xcert Root CA v1 1024	CPp,CPp,CPp
Xcert EZ	CPp,CPp,CPp
CertEngine CA	CPp,CPp,CPp
BankEngine CA	CPp,CPp,CPp
FortEngine CA	CPp,CPp,CPp
MailEngine CA	CPp,CPp,CPp
TraderEngine CA	CPp,CPp,CPp
USPS Root	CPp,CPp,CPp
USPS Production 1	CPp,CPp,CPp
AddTrust Non-Validated Services Root	CPp,CPp,CPp
AddTrust External Root	CPp,CPp,CPp
AddTrust Public Services Root	CPp,CPp,CPp
AddTrust Qualified Certificates Root	CPp,CPp,CPp
Verisign Class 1 Public Primary OCSP Responder	CPp,CPp,CPp
Verisign Class 2 Public Primary OCSP Responder	CPp,CPp,CPp

**表 7-3** 公共证书授权机构

Verisign Class 3 Public Primary OCSP Responder	CPp,CPp,CPp
Verisign Secure Server OCSP Responder	CPp,CPp,CPp
Verisign Time Stamping Authority CA	CPp,CPp,CPp
Thawte Time Stamping CA	CPp,CPp,CPp
E-Certify CA	CPp,CPp,CPp
E-Certify RA	CPp,CPp,CPp
Entrust.net Global Secure Server CA	CPp,CPp,CPp
Entrust.net Global Secure Personal CA	CPp,CPp,CPp

## certadmin 脚本

您可使用 certadmin 脚本完成以下证书管理任务：

- 生成自签名证书
- 生成证书签名请求 (CSR)
- 添加根 CA 证书
- 安装来自 CA 的证书
- 删除证书
- 修改证书的委托属性
- 列出根 CA 证书
- 列出所有证书
- 打印证书

# 生成自签名证书

您需要针对每个服务器和网关之间的 SSL 通信生成证书。

## † 在安装后生成自签名证书

1. 以根用户身份，在您要为其生成证书的网关机器上运行 certadmin 脚本。

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

显示证书管理菜单。

- 1) 生成自签名证书
- 2) 生成证书签名请求 (CSR)
- 3) 添加根 CA 证书
- 4) 安装来自证书授权机构 (CA) 的证书
- 5) 删除证书
- 6) 修改证书的委托属性 (例如, 用于 PDC)
- 7) 请列出根 CA 证书
- 8) 列出所有证书
- 9) 打印证书内容
- 10) 退出

选择: [10] 1

2. 选择证书管理菜单上的选项 1。

证书管理脚本询问您是否要保留现有数据库文件。

3. 输入组织特定信息、令牌名和证书名。

---

**注意**

对于通配符证书，在主机的全限定 DNS 名中指定一个 \*。例如，如果主机的全限定 DNS 名为 `abc.sesta.com`，则将其指定为 `*.sesta.com`。现在，生成的证书对 `sesta.com` 域中的所有主机名均有效。

---

此主机的全限定 DNS 名称是什么? [host\_name.domain\_name]

您所属的组织（如公司）的名称是什么? []

您所属的组织单位（如部门）的名称是什么? []

您所在的城市或地区的名称是什么? []

您所在的洲名或省名是什么（请勿使用缩写）? []

此单位的两字国家代码是什么? []

仅当您不使用默认内部（软件）加密模块时才需要令牌名，例如，如果您想使用加密卡（令牌名可使用以下形式列出：`modutil -dbdir /etc/opt/SUNWps/cert/gateway-profile-name -list`）；否则，只需点击下面的回车键。

请输入令牌名。 []

请为此证书输入您想要的名称？

输入证书的有效期（按月） [6]  
将生成一自签名证书并提示返回。

令牌名（默认值为空）和证书名存储在  
`/etc/opt/SUNWps/cert/gateway-profile-name` 下面的 `.nickname` 文件中。

#### 4. 重新启动网关以使证书生效：

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

## 生成证书签名请求 (CSR)

在您可从 CA 订购证书之前，需要生成将包含 CA 所需信息的证书签名请求。

## † 生成 CSR

1. 以根用户身份，运行 certadmin 脚本：

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

显示证书管理菜单。

- 1) 生成自签名证书
- 2) 生成证书签名请求 (CSR)
- 3) 添加根 CA 证书
- 4) 安装来自证书授权机构 (CA) 的证书
- 5) 删除证书
- 6) 修改证书的委托属性 (例如，用于 PDC)
- 7) 请列出根 CA 证书
- 8) 列出所有证书
- 9) 打印证书内容
- 10) 退出

选择: [10] 2

2. 选择证书管理菜单上的选项 2。

脚本提示您输入组织指定的信息、令牌名和网站管理员的电子邮件和电话号码。

确保指定主机的全限定 DNS 名。

此主机的全限定 DNS 名称是什么? [snape.sesta.com]

您所属的组织 (如公司) 的名称是什么? []

您所属的组织单位 (如部门) 的名称是什么? []

您所在的城市或地区的名称是什么? []

您所在的洲名或省名是什么 (请勿使用缩写)? []

此单位的两字国家代码是什么? []

仅当您不使用默认内部 (软件) 加密模块时才需要令牌名, 例如, 如果您想使用加密卡 (令牌名可使用以下形式列出: `modutil -dbdir /etc/opt/SUNWps/cert -list`); 否则, 只需点击下面的回车键。

请输入令牌名 []

对于要为其生成证书的机器, 请输入其网站管理员的一些联系信息。

该服务器的管理员 / 网站管理员的电子邮件地址是什么 []?

该服务器的管理员 / 网站管理员的电话号码 []?

### 3. 键入全部所需信息。

---

**注意** 请勿将网站管理员的电子邮件和电话号码留为空白。此信息对于获取有效 CSR 是必需的。

---

在 `portal-server-install-root/SUNWps/bin/csr.hostname.datetimestamp` 文件中将生成并存储 CSR。CSR 也会打印在屏幕上。当您从 CA 订购证书时, 可直接复制并粘贴 CSR。

## 添加根 CA 证书

如果客户机站点所提供的经 CA 签名的证书不为网关证书数据库所知，则 SSL 信号交换将失败。

为防止出现此情况，您需要向证书数据库中添加根 CA 证书。这将确保使 CA 为网关所知。

浏览到 CA 的网站并获取该 CA 的根证书。当您使用 certadmin 脚本时，指定根 CA 证书的文件名和路径。

### † 添加根 CA 证书

1. 以根用户身份，运行 certadmin 脚本。

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

显示证书管理菜单。

- 1) 生成自签名证书
  - 2) 生成证书签名请求 (CSR)
  - 3) 添加根 CA 证书
  - 4) 安装来自证书授权机构 (CA) 的证书
  - 5) 删除证书
  - 6) 修改证书的委托属性 (例如，用于 PDC)
  - 7) 请列出根 CA 证书
  - 8) 列出所有证书
  - 9) 打印证书内容
  - 10) 退出
- 选择: [10] 3

2. 选择证书管理菜单上的选项 3。
3. 输入包含根证书的文件名，并输入证书名。  
根 CA 证书会被添加到证书数据库。

## 安装来自证书授权机构的 SSL 证书

在安装网关过程中，默认情况下将创建并安装自签名证书。在安装之后，您可随时安装由供应商（提供官方证书授权机构 (CA) 服务）或您公司的 CA 签名的 SSL 证书。

此项任务涉及三个步骤：

- [生成证书签名请求 \(CSR\)](#)
- [从 CA 订购证书](#)
- [安装来自 CA 的证书](#)

### 从 CA 订购证书

在生成证书签名请求 (CSR) 后，您需要使用 CSR 从 CA 订购证书。

#### † 从 CA 订购证书

1. 转到“证书授权机构”的网站，并订购您的证书。
2. 提供 CA 所需的 CSR。提供 CA 所需的其他信息（如果需要）。

您会收到来自 CA 的证书。将其保存到文件中。在文件中需包括连同证书在内的 "BEGIN CERTIFICATE" 和 "END CERTIFICATE" 行。

以下示例省略了实际的证书数据。

```
-----BEGIN CERTIFICATE-----  
  
The certificate contents...  
  
-----END CERTIFICATE-----
```

## 安装来自 CA 的证书

使用 `certadmin` 脚本，在 `/etc/opt/SUNWps/cert/gateway-profile-name` 下的本地数据库文件中安装从 CA 获取的证书。

### † 安装来自 CA 的证书

1. 以根用户身份，运行 `certadmin` 脚本。

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

显示证书管理菜单。

- 1) 生成自签名证书
- 2) 生成证书签名请求 (CSR)
- 3) 添加根 CA 证书
- 4) 安装来自证书授权机构 (CA) 的证书
- 5) 删除证书
- 6) 修改证书的委托属性 (例如, 用于 PDC)
- 7) 请列出根 CA 证书
- 8) 列出所有证书

9) 打印证书内容

10) 退出

选择: [10] 4

## 2. 选择证书管理菜单上的选项 4。

脚本要求您输入证书文件名、证书名和令牌名。

包含证书的文件名（包括路径）是什么？  
创建证书的 CSR 时请输入您使用的令牌名。 []

## 3. 提供全部所需的信息。

证书被安装在 `/etc/opt/SUNWps/cert/gateway-profile-name` 中，并且返回屏幕提示。

## 4. 重新启动网关以使证书生效：

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

# 删除证书

通过使用证书管理脚本可删除证书。

## † 删除证书

### 1. 以根用户身份，运行 certadmin 脚本。

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

其中， *gateway-profile-name* 是网关实例名。  
显示证书管理菜单。

- 1) 生成自签名证书
  - 2) 生成证书签名请求 (CSR)
  - 3) 添加根 CA 证书
  - 4) 安装来自证书授权机构 (CA) 的证书
  - 5) 删除证书
  - 6) 修改证书的委托属性 (例如, 用于 PDC)
  - 7) 请列出根 CA 证书
  - 8) 列出所有证书
  - 9) 打印证书内容
  - 10) 退出
- 选择: [10] 5

2. 选择证书管理菜单上的选项 5。
3. 输入要删除证书的名称。

# 修改证书的委托属性

证书的委托属性需要修改的一种情况便是对网关应用客户机验证。PDC（个人数字证书）是客户机验证的一个示例。签发 PDC 的 CA 必须要受网关委托，并且必须将 CA 证书标记为 "T" 以满足 SSL。

如果设置了与 HTTPS 站点通信的网关，则 HTTPS 站点服务器证书的 CA 必须要受网关委托，并且必须将 CA 证书标记为 "C" 以满足 SSL。

## † 修改证书的委托属性

1. 以根用户身份，运行 certadmin 脚本。

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

其中，*gateway-profile-name* 是网关实例名。

显示证书管理菜单。

- 1) 生成自签名证书
- 2) 生成证书签名请求 (CSR)
- 3) 添加根 CA 证书
- 4) 安装来自证书授权机构 (CA) 的证书
- 5) 删除证书
- 6) 修改证书的委托属性 (例如，用于 PDC)
- 7) 请列出根 CA 证书
- 8) 列出所有证书

9) 打印证书内容

10) 退出

选择: [10] 6

2. 选择证书管理菜单上的选项 6。
3. 输入证书名称。例如, Thawte Personal Freemail C。

请输入证书名?  
Thawte Personal Freemail CA

4. 输入证书的委托属性。

请输入要使证书具有的委托属性 [CT,CT,CT]

证书委托属性将被更改。

## 列出根 CA 证书

通过使用证书管理脚本可查看所有根 CA 证书。

### † 查看根 CA 的列表

1. 以根用户身份, 运行 certadmin 脚本。

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

其中， *gateway-profile-name* 是网关实例名。

显示证书管理菜单。

- 1) 生成自签名证书
- 2) 生成证书签名请求 (CSR)
- 3) 添加根 CA 证书
- 4) 安装来自证书授权机构 (CA) 的证书
- 5) 删除证书
- 6) 修改证书的委托属性 (例如, 用于 PDC)
- 7) 请列出根 CA 证书
- 8) 列出所有证书
- 9) 打印证书内容
- 10) 退出

选择: [10] 7

## 2. 选择证书管理菜单上的选项 7。

显示所有根 CA 证书。

# 列出所有证书

通过使用证书管理脚本可查看所有证书及其相应的委托属性。

## † 列出所有证书

1. 以根用户身份，运行 certadmin 脚本。

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

其中， *gateway-profile-name* 是网关实例名。

显示证书管理菜单。

- 1) 生成自签名证书
  - 2) 生成证书签名请求 (CSR)
  - 3) 添加根 CA 证书
  - 4) 安装来自证书授权机构 (CA) 的证书
  - 5) 删除证书
  - 6) 修改证书的委托属性 (例如, 用于 PDC)
  - 7) 请列出根 CA 证书
  - 8) 列出所有证书
  - 9) 打印证书内容
  - 10) 退出
- 选择: [10] **8**

2. 选择证书管理菜单上的选项 8。  
显示所有 CA 证书。

## 打印证书

通过使用证书管理脚本可打印证书。

### † 打印证书

1. 以根用户身份，运行 certadmin 脚本。

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

其中，*gateway-profile-name* 是网关实例名。

显示证书管理菜单。

- 1) 生成自签名证书
- 2) 生成证书签名请求 (CSR)
- 3) 添加根 CA 证书
- 4) 安装来自证书授权机构 (CA) 的证书
- 5) 删除证书
- 6) 修改证书的委托属性 (例如，用于 PDC)
- 7) 请列出根 CA 证书
- 8) 列出所有证书

9) 打印证书内容

10) 退出

选择: [10] 9

2. 选择证书管理菜单上的选项 9。
3. 输入证书名称。

## 配置 URL 访问控制

本章介绍如何用 Sun Java™ System Identity Server 管理控制台中“SRA 配置”下的“访问列表”来允许或拒绝最终用户通过网关访问特定 URL。

---

**注意** 单击 Identity Server 管理控制台右上角的“文档”，然后单击“SRA 帮助”以获取所有 Sun Java System Portal Server Secure Remote Access (SRA) 属性的快速参考。

---

### ► 配置 URL 访问控制

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 在管理控制台中，选择“服务配置”选项卡。
3. 在“SRA 配置”下，单击“访问列表”旁边的箭头。  
会显示“访问列表”页面。

从这里，您可以执行下列任务：

- [设置拒绝的 URL 列表](#)
- [设置允许的 URL 列表](#)
- [管理单点登录](#)

---

**注意** 当您安装 SRA 时，缺省情况下“访问列表”服务对所有用户均不可用。该服务仅适用于安装过程期间在缺省情况下创建的 amadmin 用户。不具有此项服务的其他用户将无法通过网关访问桌面。以 amadmin 身份登录，并将此项服务分配给所有用户。

---

## 设置拒绝的 URL 列表

可使用此字段指定最终用户不能通过网关访问的 URL 列表。

网关在检查“允许的 URL”列表之前要先检查“拒绝的 URL”列表。

### ► 设置拒绝的 URL 列表

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 在“SRA 配置”下，单击“访问列表”旁边的箭头。  
会显示“访问列表”页面。
4. 在“拒绝的 URL”字段中指定希望拒绝通过网关访问的 URL。输入 URL 的格式为：  
`http://abc.siroe.com`
5. 单击“添加”。  
该 URL 将被添加到“拒绝的 URL 列表”。  
也可使用正则表达式，如 `http://*.siroe.com`。在这种情况下，用户不能访问 `siroe.com` 域的所有主机。
6. 单击“保存”记录更改。

## 设置允许的 URL 列表

可指定最终用户可通过网关访问的所有 URL。缺省情况下，此列表有一通配符项 (\*)，表示可以访问所有 URL。如果要允许访问所有 URL，仅限制访问特定 URL，可将受限 URL 添加到“拒绝的 URL”列表中。用同样的方法，如果希望仅允许访问特定 URL，则将“拒绝的 URL”字段留为空白，在“允许的 URL”字段中指定所需的 URL。

网关会先检查“拒绝的 URL”，然后再检查“允许的 URL”。

### ► 设置允许的 URL 列表

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。

3. 在“SRA 配置”下，单击“访问列表”旁边的箭头。  
会显示“访问列表”页面。
4. 在“允许的 URL”字段中指定希望允许通过网关访问的 URL。输入 URL 的格式为：  
`http://abc.siroe.com`
5. 单击“添加”。  
该 URL 将被添加到“允许的 URL”。

---

**注意** 缺省情况下，“允许的 URL”字段具有一个\*，它表示可通过网关访问所有的 URL。

---

6. 单击“保存”记录更改。

## 管理单点登录

SRA 软件中的“访问列表”服务允许您控制各个主机的单点登录功能。但要想使用单点登录功能，必须在网关服务中启用“启用 HTTP 基本验证”选项。请参阅第 237 页的“启用 HTTP 和 HTTPS 连接”。

通过“访问列表”服务，可禁用某些主机的单点登录功能。这意味着最终用户在每次连接到需要 HTTP 基本验证的主机时都需要进行验证，除非为每一会话启用单点登录。

如果已禁用某台主机的单点登录，用户可在单一 Portal Server 会话中重新连接到该主机。例如，假定已禁用至 `abc.sesta.com` 的单点登录。第一次连接到此站点时，需要对用户进行验证。用户可以浏览其他页面，并稍后返回此页面，而且如果这些页面在同一 Portal Server 会话中，则无需验证。

用户也可使用受限的管理控制台配置这些属性。

### ► 禁用主机的单点登录

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 在“SRA 配置”下，单击“访问列表”旁边的箭头。  
会显示“访问列表”页面。

4. 在“SSO 被禁用的主机”字段中指定要禁用 SSO 的主机。  
以 `abc.siroe.com` 格式指定主机名称。
5. 单击“添加”。  
该主机名被添加到列表。
6. 单击“保存”记录更改。

► **启用每一会话的单点登录**

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 在“SRA 配置”下，单击“访问列表”旁边的箭头。  
会显示“访问列表”页面。
4. 选中“在每一会话中启用单点登录”复选框以启用会话的单点登录。
5. 单击“保存”记录更改。

► **指定验证级别**

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 在“SRA 配置”下，单击“访问列表”旁边的箭头。  
会显示“访问列表”页面。
4. 滚动到“允许的验证级别”字段。
5. 输入允许的验证。用星号可表示允许所有级别。
6. 单击“保存”记录更改。

# 配置网关

本章介绍如何通过 Sun Java™ System Identity Server 管理控制台配置网关属性。

---

**注意** 单击 Identity Server 管理控制台右上角的“帮助”，然后单击“SRA 帮助”，以获取所有 Sun Java System Portal Server Secure Remote Access (SRA) 属性的快速参考。

---

要设置网关，请参阅第 38 页的“创建网关配置文件”。

在创建网关配置文件后，需要配置网关属性。

► **配置网关属性**

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 在管理控制台中，选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑 ...”。  
会显示“编辑网关配置文件”页。

在此处单击相应选项卡：

- [核心选项卡](#)
- [代理选项卡](#)
- [安全选项卡](#)

- [重写器选项卡](#)
- [记录选项卡](#)

下面列出了每个选项卡及其包含的可配置属性。

## 核心选项卡

使用“核心”选项卡，可在网关服务中执行以下任务：

- [启用 HTTP 和 HTTPS 连接](#)
- [启用和创建重写器代理列表](#)
- [启用 Netlet](#)
- [启用和创建 Netlet 代理列表](#)
- [启用 Proxylet](#)
- [启用 Cookie 管理](#)
- [启用 HTTP 基本验证](#)
- [启用持久性 HTTP 连接](#)
- [指定每个持久性连接的最大请求数量](#)
- [指定持久套接字连接超时](#)
- [指定周转时间的宽限期超时](#)
- [创建将用户会话 Cookie 转发到 URL 列表](#)
- [指定最大连接队列长度](#)
- [指定网关超时](#)
- [指定线程池容量最大值](#)
- [指定高速缓存套接字超时](#)
- [创建 Portal Server 列表](#)
- [指定服务器重试间隔](#)
- [启用存储外部服务器 Cookie](#)
- [从 URL 获取会话](#)
- [启用将 Cookie 标记为安全](#)

## 启用 HTTP 和 HTTPS 连接

如果安装时选择在 HTTPS 模式下运行网关，安装完成后，网关将以 HTTPS 模式运行。在 HTTPS 模式中，网关接受来自浏览器的 SSL 连接，而拒绝非 SSL 连接。

不过，您也可以将网关配置为在 HTTP 模式下运行。这样将提高网关性能，因为管理 SSL 会话以及加密、解码 SSL 通信的开销均未涉及到。

### ► 将网关配置为在 HTTP 或 HTTPS 模式运行

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 在管理控制台中，选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 在“核心”选项卡下执行以下操作。
  - 根据需要选择“启用 HTTP 连接”、“启用 HTTPS 连接”，或者选中这两个复选框。
  - 在“HTTPS 端口”字段中指定所需的 HTTPS 端口。
  - 在“HTTP 端口”字段中指定所需的 HTTP 端口。
6. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。
7. 从终端窗口中重新启动网关：

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

## 启用和创建重写器代理列表

“重写器”代理可以使网关与内部网计算机之间安全地进行 HTTP 通信。如果未指定“重写器”代理，那么当用户试图访问其中一台内部网计算机时，网关组件将会直接连接到内部网计算机。

“重写器”代理在安装后不会自动运行。您需要按照以下步骤启用“重写器”代理。

► 启用“重写器代理”和创建“重写器代理”列表

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。

---

**注意** 确保“重写器”代理和网关使用相同的网关配置文件。

---

会显示“编辑网关配置文件”页。

5. 单击“核心”选项卡。
6. 选中“启用重写器代理”复选框以启用“重写器”代理。
7. 在“重写器代理”编辑框中，使用 `hostname:port` 格式键入所需的主机和端口。
8. 单击“添加”。
9. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。
10. 在服务器上运行 `portal-server-install-root/SUNWps/bin/certadmin` 以创建“重写器”代理证书。

只有当您在安装“重写器”代理过程中未选择创建证书时，才需要执行此步骤。

11. 以根用户身份登录至安装“重写器”代理的机器，并启动“重写器”代理：

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

12. 以根用户的身份登录至安装网关的机器，并重新启动网关：

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

## 启用 Netlet

Netlet 使用户可以在不安全的网络上（如 Internet）安全地运行常用 TCP/IP 服务。您可以运行 TCP/IP 应用程序（如 Telnet 和 SMTP）、HTTP 应用程序及任何固定端口应用程序。

如果启用了 Netlet，网关就需要判断接收的通信是 Netlet 通信还是 Portal Server 通信。由于网关假定所有接收的通信都是 HTTP 通信或 HTTPS 通信，所以禁用 Netlet 可以减少此类开销。只有在确信不需要与 Portal Server 一同使用任何应用程序时，才可以禁用 Netlet。

### ► 启用 Netlet

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 单击“核心”选项卡。
6. 选中“启用 Netlet”复选框。默认情况下此复选框已选中。取消选中该选项将禁用 Netlet。
7. 选中“启用 Netlet 代理”复选框以启用 Netlet 代理。
8. 在“Netlet 代理列表”编辑框中，使用 hostname:port 格式键入所需的主机和端口。
9. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。
10. 从终端窗口中重新启动网关：

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

## 启用和创建 Netlet 代理列表

Netlet 代理通过将安全隧道从客户机经网关扩展到内部网中驻留的 Netlet 代理，提高了网关和内部网之间 Netlet 通信的安全性。

如果已启用 Netlet 代理，Netlet 信息包将由 Netlet 代理解码，然后发送到目的服务器。这将减少需要在防火墙中打开的端口数量。

► 启用 “Netlet 代理” 和创建 “Netlet 代理” 列表

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择 “服务配置” 选项卡。
3. 在左框中，单击 “SRA 配置” 下网关旁边的右箭头。  
网关页显示在右侧窗格中。
4. 单击所需配置文件旁边的 “编辑”。  
“编辑网关配置文件” 页显示在右侧窗格中。
5. 选中 “启用 Netlet 代理” 复选框以启用 Netlet 代理。
6. 在 “Netlet 代理主机” 字段中，使用 `host hostname:port` 格式键入所需的 Netlet 代理主机和端口。

---

**提示** 要确定所需端口是否可用或未使用，在命令行中输入：

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

*port-number* 是所需的端口。

---

7. 单击 “添加”。
8. 单击页面顶部或底部的 “保存”，保存更改。
9. 从终端窗口中重新启动网关：  
`gateway-install-root/SUNWps/bin/gateway -n gateway-profile-name start`

## 启用 Proxylet

► 启用 Proxylet

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择 “服务配置” 选项卡。

3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 单击“核心”选项卡。
6. 单击“SRA 配置”下网关旁边的箭头。
7. 选中“启用 Proxylet”复选框。
8. 单击“代理”选项卡。向下滚动到“域和子域代理”字段，然后输入定向到网关的 URL 的域。
9. 单击“保存”。

## 启用 Cookie 管理

许多网站使用 cookie 对用户会话进行跟踪和管理。当网关向网站发送在 HTTP 报头中设置 cookie 的请求时，网关以下述方式丢弃或传送这些 cookie：

- 如果未在网关服务中选中“启用 Cookie 管理”属性，则不会重写 cookie。因此，来自浏览器的 cookie 可能不会到达内部网主机，反之亦然。
- 如果选择了“启用 Cookie 管理”属性，网关将重写 cookie。网关会确保来自浏览器的 cookie 到达内部网的目的主机，反之亦然。

此设置不适用于 Portal Server 用来跟踪 Portal Server 用户会话的 cookie。它由“用户会话 Cookie 转发目标用户会话”选项的配置控制。请参阅第 246 页的“创建将用户会话 Cookie 转发到 URL 列表”。

此设置适用于用户可以访问的所有网站（即不能选择丢弃某些网站的 cookie，而保留其他网站的 cookie）。

---

**注意** 即使在无 cookie 的网关中，也不要从“Cookie 域”列表中删除 URL。有关“Cookie 域”列表的详细信息，请参阅《Identity Server 管理指南》。

---

### ► 启用 Cookie 管理

1. 以管理员身份登录到 Identity Server 管理控制台。

1. 选择“服务配置”选项卡。
2. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
3. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
4. 单击“核心”选项卡。
5. 选中“启用 Cookie 管理”复选框以启用 cookie 管理。
6. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。
7. 从终端窗口中重新启动网关：

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

## 启用 HTTP 基本验证

HTTP 基本验证可在网关服务中设置。

网站可以使用“HTTP 基本验证”，要求访问者在浏览网站之前输入用户名和口令（HTTP 响应代码为 401 和 WWW 验证：BASIC），从而获得保护。Portal Server 可以保存用户名和口令，这样用户在重新访问受 BASIC 保护的网站时，无需重新输入其身份验证信息。这些身份验证信息保存在 Directory Server 的用户配置文件中。

此设置不决定用户能否访问受 BASIC 保护的网站，它只确定是否将用户输入的验证信息保存到该用户的配置文件中。

此设置适用于用户可以访问的所有网站（即 HTTP 基本验证高速缓冲功能不能对某些网站可用，而对其他网站不可用）。

---

**注意** 不支持对由 Microsoft Internet Information Server (IIS) 提供服务、由 Windows NT 质询 / 响应（HTTP 响应代码为 401，WWW 验证：NTLM）而非 BASIC 验证提供保护的 URL 的浏览。

---

您也可使用管理控制台中的“访问列表”服务来启用单点登录。有关启用单点登录的详细信息，请参阅第 233 页的“管理单点登录”。

### ► 启用 HTTP 基本验证

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 单击“核心”选项卡。
6. 选中“启用 HTTP 基本验证”复选框，以启用 HTTP 基本验证。
7. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。
8. 从终端窗口中重新启动网关：

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

## 启用持久性 HTTP 连接

可在网关启用 HTTP 持久性连接，以防套接字为网页中的每个对象（如图像和样式表）均打开。

### ► 启用持久性 HTTP 连接

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 单击“核心”选项卡。

6. 选中“启用持久性 HTTP 连接”复选框，以启用 HTTP 连接。
7. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。
8. 从终端窗口中重新启动网关：

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

## 指定每个持久性连接的最大请求数量

### ► 指定每个持久性连接的最大请求数量

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 单击“核心”选项卡。
6. 滚动到“每个持久性连接的最大请求数量”字段，然后键入所需的请求数量。
7. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。
8. 从终端窗口中重新启动网关：

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

## 指定持久套接字连接超时

### ► 指定持久套接字连接超时

1. 以管理员身份登录到 Identity Server 管理控制台。

2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 单击“核心”选项卡。
6. 滚动到“持久连接套接字超时”字段，然后键入所需的超时值（以秒为单位）。
7. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。
8. 从终端窗口中重新启动网关：

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

## 指定周转时间的宽限期超时

宽限期超时周转时间是下列时间之和：

- 浏览器发送请求之后，该请求到达网关所需时间。
- 网关发送响应和浏览器实际接收到该响应之间的时间。

这取决于诸多因素，如网络条件和客户机连接速度。

### ► 指定周转时间的超时

这是客户机（浏览器）与网关之间的网络通信的往返时间。

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。

4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 单击“核心”选项卡。
6. 滚动到“Grace 超时，以解决周转时间”字段，然后键入所需的超时时间（以秒为单位）。
7. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。
8. 从终端窗口中重新启动网关：

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

## 创建将用户会话 Cookie 转发到 URL 列表

portal server 利用 cookie 跟踪用户会话。当网关向服务器提出 HTTP 请求时（例如，当调用桌面 servlet 以生成用户桌面页时），此 cookie 将被转发到服务器。服务器上的应用程序使用该 cookie 来确认并标识用户。

Portal Server 的 cookie 不会被转发到针对服务器以外机器的 HTTP 请求，除非那些机器上的 URL 已在“用户会话 Cookie 转发目标用户会话”列表中指定。因此向此列表中添加 URL 可使 servlet 和 CGI 接收 Portal Server 的 cookie，并使用 API 来标识用户。

URL 使用隐含的后缀通配符进行匹配。例如，列表的默认条目：

```
http://server:8080
```

将 cookie 转发到所有以 http://server:8080 开始的 URL。

添加：

```
http://newmachine.eng.siroe.com/subdir
```

将 cookie 转发到所有开头与该字符串完全相同的 URL。

在此例中，cookie 不会转发到任何以 "http://newmachine.eng/subdir" 开始的 URL，因为该字符串与转发列表中的字符串不完全一致。要将 cookie 转发到以这个改变的机器名开始的 URL，必须向转发列表添加新的条目。

同样，cookie 也不会转发到以 "https://newmachine.eng.siroe.com/subdir" 开始的 URL，除非向转发列表中添加相应的条目。

### ► 添加转发 Cookie URL

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 单击“核心”选项卡。
6. 滚动到“用户会话 Cookie 转发目标用户会话”编辑框，然后键入所需的 URL。
7. 单击“添加”，将此条目添加到“用户会话 Cookie 转发目标用户会话”列表中。
8. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。
9. 从终端窗口中重新启动网关：

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

## 指定最大连接队列长度

可以指定网关可接受的最大并发连接数量。网关不接受任何超出此数量的连接。

### ► 指定最大连接队列长度

1. 以管理员身份登录到 Identity Server 管理控制台。

2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 单击“核心”选项卡。
6. 滚动到“最大连接队列长度”字段，然后指定所需的连接数量。
7. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。
8. 从终端窗口中重新启动网关：

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

## 指定网关超时

可以指定网关与浏览器断开连接的超时时间间隔（以毫秒为单位）。

### ► 指定网关超时

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 单击“核心”选项卡。
6. 滚动到“网关超时”（毫秒）字段，然后指定所需的时间间隔（以毫秒为单位）。
7. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。
8. 从终端窗口中重新启动网关：

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

## 指定线程池容量最大值

可在网关线程池中指定可以预先创建的最大线程数量。

### ► 指定线程池容量最大值

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 单击“核心”选项卡。
6. 滚动到“线程组合容量最大值”字段，然后指定所需的线程数量。
7. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。
8. 从终端窗口中重新启动网关：

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

## 指定高速缓存套接字超时

可指定网关与 Portal Server 断开连接的超时时间间隔（以毫秒为单位）。

### ► 指定高速缓存套接字超时

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。

4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 单击“核心”选项卡。
6. 滚动到“高速缓存套接字超时”字段，然后指定所需的时间间隔（以毫秒为单位）。
7. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。
8. 从终端窗口中重新启动网关：

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

## 创建 Portal Server 列表

可以为网关配置多个 Portal Server 以为请求提供服务。安装网关时，可能已经指定需要和网关协同工作的 Portal Server。默认情况下，此 Portal Server 会在 Portal Server 字段中列出。可向列表中添加更多的 Portal Server，格式为 `http://portal server name:port number`。网关试图联系每个以循环方式列出的 Portal Server 来为请求提供服务。

### ► 指定 Portal Server

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 单击“核心”选项卡。
6. 滚动到 Portal Server 字段，然后指定 Portal Server。  
在编辑字段中，使用 `http://portal server name:port number` 格式指定 Portal Server，然后单击“添加”。
7. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。

8. 从终端窗口中重新启动网关:

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

## 指定服务器重试间隔

此属性指定在 Portal Server、“重写器”代理或 Netlet 代理无法使用（如，崩溃或死机）时，尝试启动它们的各个请求之间的时间间隔。

### ► 指定 Portal Server 重试间隔

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 单击“核心”选项卡。
6. 滚动到“Portal Server 重试间隔”字段，然后指定秒数。
7. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。
8. 从终端窗口中重新启动网关:

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

## 启用存储外部服务器 Cookie

当启用“存储外部服务器 Cookie”选项时，网关存储并管理通过网关访问的任何第三方应用程序或服务器的 cookie。即使应用程序或服务不能服务于 cookieless 设备或（由于历史遗留原因）需要依赖 cookie 进行状态管理，此选项也可以透明地屏蔽应用程序或服务对其服务的 cookieless 设备的了解。有关 cookieless 设备和客户机检测的信息，请参阅 *Identity Server Customization and API Guide*。

### ► 存储外部服务器 Cookie

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 单击“核心”选项卡。
6. 选中“存储外部服务器 Cookie”复选框以启用存储外部服务器 cookie。
7. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。
8. 从终端窗口中重新启动网关：

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

## 从 URL 获取会话

选择“从 URL 获取会话”选项后，不管是否支持 cookie，会话信息都将作为 URL 的一部分进行编码。这意味着网关使用在 URL 中找到的会话信息进行验证，而不使用客户机浏览器发出的会话 cookie。

### ► 从 URL 获取会话

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 单击“核心”选项卡。
6. 选中“从 URL 获取会话”复选框以便从 URL 获取会话。

7. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。
8. 从终端窗口中重新启动网关：

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

## 启用将 Cookie 标记为安全

将 cookie 标记为安全 cookie 时，浏览器以额外的安全对待该 cookie。安全的实现方式取决于浏览器。如果要使用此功能，必须启用“启用 Cookie 管理”属性。

### ► 将 Cookie 标记为安全

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 单击“核心”选项卡。
6. 选中“将 Cookie 标记为安全”复选框以将 cookie 标记为安全 cookie。  
确保启用了“启用 Cookie 管理”属性。
7. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。
8. 从终端窗口中重新启动网关：

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

## 代理选项卡

使用“代理”选项卡，可在网关服务中执行以下任务：

- 启用“使用网络代理”
- 创建网络代理的 URL 列表

- 创建不使用代理的 URL 列表
- 创建域和子域代理列表
- 创建代理口令列表
- 启用自动代理配置支持
- 指定自动代理配置文件位置
- 通过网络代理启用 Netlet 隧穿

## 启用“使用网络代理”

### ► 启用“使用网络代理”

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 单击“代理”选项卡。
6. 选中“使用代理”复选框以启用“使用网络代理”。
7. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。
8. 从终端窗口中重新启动网关：

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

## 创建网络代理的 URL 列表

可以指定即使在禁用“使用代理”选项时，网关也只能通过在“域和子域代理”列表中列出的网络代理与某些 URL 联系。您需要在“使用 Webproxy URL”字段中指定这些 URL。有关此字段值如何影响代理使用的详细说明，请参阅第 56 页的“指定联系 Identity Server 的代理”。

### ► 指定 Webproxy 的 URL

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 单击“代理”选项卡。
6. 在“使用 Webproxy URL”编辑框中，使用 `http://host name.subdomain.com` 格式键入所需的 URL。单击“添加”。  
该 URL 添加到“使用 Webproxy URL”列表中。
7. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。
8. 从终端窗口中重新启动网关：  

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

## 创建不使用代理的 URL 列表

网关会尝试直接连接到在“不可使用 Webproxy URL”列表中列出的 URL。webproxy 将不用于连接到这些 URL。

### ► 指定不使用代理的 URL

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 单击“代理”选项卡。

- 在“不可使用 Webproxy URL”编辑框中键入所需的 URL，然后单击“添加”。

该 URL 添加到“不可使用 Webproxy URL”列表中。

- 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。
- 从终端窗口中重新启动网关：

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

## 创建域和子域代理列表

### ► 指定域和子域的代理

有关代理信息如何应用于不同主机的详细信息，请参阅第 56 页的“指定联系 Identity Server 的代理”。

- 以管理员身份登录到 Identity Server 管理控制台。
- 选择“服务配置”选项卡。
- 单击“SRA 配置”下网关旁边的右箭头。  
会显示“网关配置文件”页。
- 单击与想要为其设置属性的网关配置文件相应的“编辑...”。  
会显示“编辑网关配置文件”页。
- 单击“代理”选项卡。
- 滚动到“域和子域代理”编辑框并键入所需信息，然后单击“添加”。该条目添加到“域和子域代理”列表框中。

输入代理信息的格式如下：

```
domainname proxy1:port1|subdomain1 proxy2:port2|subdomain2  
proxy3:port3|* proxy4:port4
```

\* 表示在 \* 后定义的代理需要用于所有域和子域，特别指出的除外。

如果未指定代理端口，默认使用端口 8080。

7. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。
8. 从终端窗口中重新启动网关：

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

## 创建代理口令列表

如果代理服务器在访问某些或所有站点时需要验证，那么您必须为网关指定特定代理服务器验证所需的用户名和口令。

### ► 指定代理口令

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 单击“代理”选项卡。
6. 滚动到“代理口令列表”字段，键入每个代理服务器的相应信息，然后单击“添加”

输入代理信息的格式如下：

```
proxyserver|username|password
```

`proxyserver` 与在“域和子域代理”列表中定义的代理服务器相对应。

7. 为所有需要验证的代理重复步骤 6。
8. 单击页顶部或底部的“保存”，记录这些更改。
9. 从终端窗口中重新启动网关：

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

## 启用自动代理配置支持

如果您选择了“启用自动代理配置”选项，“域和子域代理”字段中的信息将被忽略。网关仅使用“代理自动配置”(PAC)文件配置内部网。有关 PAC 文件的信息，请参阅第 62 页的“使用自动代理配置”。

### ► 启用自动代理配置支持

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 单击“代理”选项卡。
6. 选中“启用自动代理配置支持”复选框以启用 PAC 支持。
7. 单击页顶部或底部的“保存”，记录这些更改。
8. 从终端窗口中重新启动网关：

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

## 指定自动代理配置文件位置

### ► 指定自动代理配置文件位置

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。

4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 单击“代理”选项卡。
6. 滚动到“自动代理配置文件位置”字段，然后键入 PAC 文件的名称和位置。
7. 单击页顶部或底部的“保存”，记录这些更改。
8. 从终端窗口中重新启动网关：

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

## 通过网络代理启用 Netlet 隧穿

### ► 通过网络代理启用隧道 Netlet

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 单击“代理”选项卡。
6. 选中“通过网络代理启用 Netlet 隧穿”复选框以启用隧穿。
7. 单击页顶部或底部的“保存”，记录这些更改。
8. 从终端窗口中重新启动网关：

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

## 安全选项卡

使用“安全”选项卡，可在网关服务中执行以下任务：

- 创建非验证 URL 列表

- 创建已启用证书的网关主机列表
- 允许 40 位加密连接
- 启用 SSL 2.0 版本
- 启用 SSL 密码选择
- 启用 SSL 3.0 版本
- 启用空密码
- 创建信任的 SSL 域列表
- 配置个人数字证书 (PDC) 验证

## 创建非验证 URL 列表

可以指定一些不需要任何验证的 URL。它们通常是包含图像的目录和文件夹。

### ► 指定非验证 URL 路径

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 滚动到“非验证 URL”字段，然后以文件夹 / 子文件夹格式键入所需的文件夹路径。  
未全限定的 URL（例如， /images）被视为门户 URL。  
要添加非门户 URL，请完全限定该 URL。
6. 单击“添加”，将此条目添加到“非验证 URL”列表中。
7. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。
8. 从终端窗口中重新启动网关：

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

## 创建已启用证书的网关主机列表

### ► 将网关添加到“已启用证书的网关主机”列表

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。  
所有服务显示在左侧窗格中。
3. 单击“SRA 配置”下网关旁边的箭头。  
“网关配置文件”页显示在右侧窗格中。
4. 单击需要启用基于证书验证的配置文件的“编辑...”。
5. 单击“安全”选项卡。
6. 将网关名称添加到“已启用证书的网关主机”。  
以 `host1.sesta.com` 格式添加网关。
7. 单击“添加”。

## 允许 40 位加密连接

如果要允许 40 位（弱）“加密套接字层”（SSL）连接，请选择此选项。如果不选择此选项，则只支持 128 位连接。

如果禁用此选项，用户需要确保浏览器的配置支持所需的连接类型。

---

### 注意

对于 Netscape Navigator 4.7x，用户需要执行以下操作：

- 在“通讯器”菜单中，选择“工具”下的“安全性信息”。
  - 在左侧窗格中单击“导航器”链接。
  - 在“高级安全性 (SSL) 配置”下单击“配置 SSL v2”或“配置 SSL v3”。
  - 启用所需的密码。
-

### ► 允许 40 位加密连接

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 选中“允许 40 位加密”复选框以启用 40 位浏览器连接。
6. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。
7. 从终端窗口中重新启动网关：

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

## 启用 SSL 2.0 版本

可启用或禁用 SSL 版本 2.0。禁用 SSL 2.0 表示仅支持旧版 SSL 2.0 的浏览器将无法进行 SRA 验证。这将确保更高级别的安全性。

### ► 启用 SSL 2.0 版本

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 选中“启用 SSL 2.0 版本”复选框以启用 2.0 版本。  
默认情况下，该选项已启用。
6. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。

7. 从终端窗口中重新启动网关:

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

## 启用 SSL 密码选择

SRA 支持许多标准密码。您可选择支持所有预封装的密码或单独选择所需的密码。您可以为每个网关实例指定特定的 SSL 密码。只要客户机站点中存在任一选定的密码，SSL 信号交换即可成功。

### ► 启用 “单个密码选择”

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择 “服务配置” 选项卡。
3. 单击 “SRA 配置” 下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的 “编辑 ...”。  
会显示 “编辑网关配置文件” 页。
5. 滚动到 “启用 SSL 密码选择” 字段，然后选择该选项。  
此选项允许从 SSL2、SSL3 和 TLS 密码列表中选择所需的密码。
6. 单击 “编辑网关配置文件” 页顶部或底部的 “保存”，保存此项更改。
7. 从终端窗口中重新启动网关:

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

## 启用 SSL 3.0 版本

可启用或禁用 SSL 版本 3.0。禁用 SSL 3.0 表示仅支持 SSL 3.0 版本的浏览器将无法进行 SRA 软件验证。这将确保更高级别的安全性。

### ► 启用 SSL 3.0 版本

1. 以管理员身份登录到 Identity Server 管理控制台。

2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 选中“启用 SSL 3.0 版本”复选框以启用 3.0 版本。
6. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。
7. 从终端窗口中重新启动网关：

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

## 启用空密码

### ► 启用空密码

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 选中“启用空密码”复选框以启用空密码。
6. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。
7. 从终端窗口中重新启动网关：

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

## 创建信任的 SSL 域列表

### ► 创建信任的 SSL 域列表

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 滚动到“信任的 SSL 域列表”并输入域名，然后单击“添加”。
6. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。
7. 从终端窗口中重新启动网关：

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

## 配置个人数字证书 (PDC) 验证

PDC 由“认证机构”(CA) 发放，并使用该认证机构的私有密钥签名。CA 在发放证书前要验证申请方的身份。因此，PDC 的出现提供了一种功能更加强大的验证机制。

PDC 含有所有者的公共密钥、所有者名称、到期日期、发放“数字证书”的认证机构名称、序列号以及可能包含的其他信息。

用户可以将 PDC 和编码设备（如 Smart 卡和 Java 卡）用于 Portal Server 中的验证。编码设备带有一个与存储在卡上的 PDC 相同的电子信息。如果用户使用其中任何一种方式登录，将不会显示“登录”屏幕和验证屏幕。

PDC 验证过程涉及以下步骤：

1. 用户在浏览器中键入一个连接请求，例如 `https://my.sesta.com`。  
对此请求的响应取决于到 `my.sesta.com` 的网关是否已经配置为接受证书。

---

**注意** 如果网关配置为接受证书，它将仅接受以证书方式进行的登录，其他类型的登录将被拒绝。

---

网关检查证书是否由已知的“认证机构”发放，是否尚未过期，以及是否未经篡改。如果证书有效，网关将允许用户进入验证过程的下一步。

2. 网关将证书传递给服务器中的 PDC 验证模块。

### ► 配置 PDC 和编码设备

配置 PDC 和编码设备涉及以下步骤：

1. 将下面一行添加到 Portal Server 机器上的 `portal-server-install-root/SUNWam/config/AMConfig-instance-name.properties` 文件中：  

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

（添加到文件内的任意位置）
2. 将“需要的证书”导入希望启用 PDC 的网关的证书数据库。  
有关详细信息，请参阅第 7 章“证书”。
3. 注册证书：
  - a. 以管理员身份登录到 Identity Server 管理控制台。
  - b. 选择“身份认证管理”选项卡。
  - c. 选择您的组织。
  - d. 在“查看”下拉菜单中单击“服务”。
  - e. 单击“核心”旁的箭头。

- f. 在“组织验证模块”列表框 LDAP 中选择“证书”和 LDAP。
        - g. 从“用户配置文件”下拉菜单中选择“动态创建”。
        - h. 单击“保存”。
4. 创建“信任的远程主机”列表。
  - a. 单击“服务配置”选项卡。
  - b. 单击证书下面“验证配置”旁的箭头。
  - c. 滚动到“信任的远程主机”列表框。
  - d. 突出显示“无”，然后单击“删除”。
  - e. 在文本框中键入 "any"
  - f. 单击“添加”。
  - g. 单击“保存”。
5. 创建新实例。
  - a. 单击“身份管理”选项卡。
  - b. 在“查看”下拉菜单中选择“服务”。
  - c. 单击“验证配置”旁的箭头。
  - d. 显示“服务实例列表”。
  - e. 单击“新建”。
  - f. 显示“新服务实例”页面。
  - g. 输入服务实例名称 gatewaypdc。
  - h. 注意：必须使用此名称。
  - i. 单击“提交”。
  - j. 显示“gatewaypdc 服务实例列表”。
  - k. 单击 gatewaypdc 编辑服务。
  - l. 出现 gatewaypdc 显示特性页。
  - m. 单击“验证配置”旁的“编辑”链接。
  - n. 出现弹出窗口。



# 重写器选项卡

使用“重写器”选项卡，可在网关服务中执行以下任务：

- 启用全部 URL 重写
- 创建 URI 到规则集映射列表
- 创建要分析的 MIME 类型列表
- 指定默认域和子域
- 创建禁止重写的 URI 列表
- 启用 MIME 推测
- 创建要分析的 URI 映射列表
- 启用屏蔽
- 指定屏蔽种子字符串
- 创建禁止屏蔽的 URI 列表
- 使网关协议与原始 URI 协议相同

## 启用全部 URL 重写

如果您启用了网关服务中的“启用全部 URL 重写”选项，“重写器”会重写任何 URL，而不检查“域和子域代理”列表中的条目。“域和子域代理”列表中的条目将被忽略。

### ► 允许网关重写所有 URL

1. 以管理员身份登录到 Sun Java™ System Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
会显示“网关配置文件”页。
4. 单击与想要为其设置属性的网关配置文件相应的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 单击“重写器”选项卡、“基本”子部分。

6. 选中“启用全部 URL 重写”复选框，以允许网关重写所有 URL。
7. 单击页顶部或底部的“保存”，记录此项更改。
8. 从终端窗口中重新启动网关：

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

## 创建 URI 到规则集映射列表

规则集是在 Identity Server 管理控制台中，在“Portal Server 配置”下的“重写器”服务中创建的。有关详细信息，请参阅 *Portal Server 管理指南*。

创建了规则集之后，可使用“将 URI 映射至规则集”字段将域与规则集相关联。默认情况下，会将以下两个条目添加到“将 URI 映射至规则集”字段中：

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

其中，`sun.com` 是门户的安装域，`/portal` 是门户的安装环境

- `*|generic_ruleset`

这表示默认域的所有页都应用默认网关规则集。对于其他所有页，将会应用一般规则集。默认网关规则集和一般规则集都是预封装的规则集。

---

**注意** 对于所有在桌面上显示的内容，不管内容取自何处，均使用默认域规则集。

例如，假定将桌面配置为凑集来自 URL `yahoo.com` 的内容。Portal Server 位于 `sesta.com` 中。此时会将与 `sesta.com` 相应的规则集应用于所取得的内容。

---

---

**注意** 为其指定规则集的域必须在“域和子域代理”列表中列出。

---

### ► 将 URI 映射至规则集

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
会显示“网关配置文件”页。
4. 单击需要设置属性的网关配置文件。  
会显示“网关 - *gateway-profile-name*”页。
5. 单击“重写器”选项卡、“基本”子部分。
6. 滚动到“将 URI 映射至规则集”字段。
7. 在“将 URI 映射至规则集”字段中，键入所需的域或主机名和规则集，然后单击“添加”。

会将此条目添加到“将 URI 映射至规则集”字段中。

指定域或主机名以及规则集时采用的格式如下：

域名 | 规则集名

例如：

`eng.sesta.com|default`

---

### 注意

规则集应用优先顺序为 `hostname-subdomain-domain`。

例如，假定在基于域的规则集列表中有下列条目：

`sesta.com|ruleset1`

`eng.sesta.com|ruleset2`

`host1.eng.sesta.com|ruleset3`

`ruleset3` 将应用于 `host1` 上的所有页。

除了从 `host1` 中检索到的页之外，`ruleset2` 将应用于 `eng` 子域中的所有页。

除了从 `eng` 子域和 `host1` 中检索到的页之外，`ruleset1` 将应用于 `sesta.com` 域中的所有页。

---

8. 单击页顶部或底部的“保存”，记录此项更改。
9. 从终端窗口中重新启动网关：

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

## Outlook Web Access 规则集

SRA 软件支持 Outlook Web Access (OWA) 的 MS Exchange 2000 SP3 安装和 MS Exchange 2003。

### ► 配置 OWA 规则集

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
会显示“网关配置文件”页。
4. 单击需要设置属性的网关配置文件。  
会显示“网关 - gateway-profile-name”页。
5. 在“将 URI 映射至规则集”字段中，先输入安装 Exchange 2000 的服务器名称，紧接着输入 Exchange 2000 Service Pack 4 OWA 规则集。

例如：

```
exchange.domain.com|exchange_2000sp3_owa_ruleset。
```

## 创建要分析的 MIME 类型列表

“重写器”有 4 个不同的分析器，用来根据内容类型（HTML、JAVASCRIPT、CSS 和 XML）对网页进行分析。默认情况下，这些分析器与常见的 MIME 类型相关联。您可以在网关服务的“将分析器映射至 MIME 类型”字段中，将新的 MIME 类型与这些分析器相关联。这会将“重写器”功能扩展到其他 MIME 类型。

可用分号或逗号（“;”或“,”）分隔多个条目。

例如：

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

它表示会将含有上述 MIME 的任何内容发送到“HTML 重写器”，并且会应用“HTML 规则”来重写这些 URL。

---

**提示** 从 MIME 映射列表中删除不必要的分析器可以提高操作速度。例如，如果您确信来自某个内部网的内容不会含有任何 JavaScript，便可从 MIME 映射列表中删除 JAVASCRIPT 条目。

---

### ► 指定 MIME 映射

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
会显示“网关配置文件”页。
4. 单击需要设置属性的网关配置文件。  
会显示“网关 - *gateway-profile-name*”页。
5. 单击“重写器”选项卡、“基本”子部分。
6. 滚动到“将分析器映射至 MIME 类型”字段，然后将所需 MIME 类型添加到编辑框中。可使用分号或逗号分隔多个条目。  
以 HTML=text/html;text/htm 格式指定该条目
7. 单击“添加”，将所需条目添加到列表中。
8. 单击页顶部或底部的“保存”，记录此项更改。
9. 从终端窗口中重新启动网关：

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

## 指定默认域和子域

当 URL 仅包含没有域和子域的主机名时，默认的域和子域会非常有用。在这种情况下，网关将假定主机名在默认的域和子域中，并进行相应处理。

例如，如果 URL 中的主机名为 host1，并且将默认的域和子域指定为 red.sesta.com，则主机名会被解析为 host1.red.sesta.com。

► 指定默认的域和子域

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 单击“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的右箭头。  
会显示“网关配置文件”页。
4. 单击与想要为其设置属性的网关配置文件相应的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 单击“重写器”选项卡、“基本”子部分。
6. 滚动到“默认域”字段，然后以 `subdomain.domain name` 格式键入所需默认值。
7. 单击“编辑网关配置文件”页顶部或底部的“保存”，保存此项更改。
8. 从终端窗口中重新启动网关：

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

## 创建禁止重写的 URI 列表

► 指定默认的域和子域

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
会显示“网关配置文件”页。
4. 单击需要设置属性的网关配置文件。  
会显示“网关 - *gateway-profile-name*”页。
5. 单击“重写器”选项卡、“高级”子部分。
6. 滚动到“禁止重写的 URI”字段，然后将 URI 添加到编辑框中。  
注意：即使此 href 规则包括在规则集中，在该列表中添加 `#*` 也会允许重写 URI。
7. 单击页顶部或底部的“保存”，记录此项更改。

8. 从终端窗口中重新启动网关:

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

## 启用 MIME 推测

重写器根据页面的 MIME 类型选择分析器。某些 Web 服务器（如 WebLogic 和 Oracle）不发送 MIME 类型。要解决这个问题，可通过在“将分析器映射至 URI”列表框中添加数据来启用 MIME 推测功能。

### ► 启用 MIME 推测

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
会显示“网关配置文件”页。
4. 单击需要设置属性的网关配置文件。  
会显示“网关 - gateway-profile-name”页。
5. 单击“重写器”选项卡、“高级”子部分。
6. 选中“启用 MIME 推测”复选框，以启用“MIME 推测”。
7. 单击页顶部或底部的“保存”，记录此项更改。
8. 从终端窗口中重新启动网关:

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

## 创建要分析的 URI 映射列表

如果启用了“MIME 推测”复选框，并且服务器尚未发送 MIME 类型，可使用该列表框将分析器映射到 URI。

多个 URI 以分号进行分隔。

例如，HTML=\*.html;\*.htm;\*.Servlet

它表示会使用“HTML 重写器”来重写具有 html、htm 或 Servlet 扩展名的任何页的内容。

### ► 分析 URI 映射

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
会显示“网关配置文件”页。
4. 单击需要设置属性的网关配置文件。  
会显示“网关 - *gateway-profile-name*”页。
5. 单击“重写器”选项卡、“高级”子部分。
6. 滚动到“将分析器映射至 MIME 类型”字段，然后将相应数据添加到编辑框中。
7. 单击页顶部或底部的“保存”，记录此项更改。
8. 从终端窗口中重新启动网关：

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

## 启用屏蔽

屏蔽功能允许“重写器”重写 URI 以便使人们看不到页面的内部网 URL。

### ► 启用屏蔽

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
会显示“网关配置文件”页。
4. 单击需要设置属性的网关配置文件。  
会显示“网关 - *gateway-profile-name*”页。
5. 单击“重写器”选项卡、“高级”子部分。
6. 选中“启用屏蔽”复选框以启用屏蔽功能。
7. 单击页顶部或底部的“保存”，记录此项更改。
8. 从终端窗口中重新启动网关：

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

## 指定屏蔽种子字符串

种子字符串用于屏蔽 URI。它是由屏蔽算法生成的一个随机字符串。

---

**注意** 如果该种子字符串已更改或是重启了网关，则可能无法为屏蔽后的 URI 加书签。

---

### ► 指定屏蔽种子字符串

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
会显示“网关配置文件”页。
4. 单击需要设置属性的网关配置文件。  
会显示“网关 - *gateway-profile-name*”页。
5. 单击“重写器”选项卡、“高级”子部分。
6. 滚动到“屏蔽种子字符串”字段，然后在编辑框中添加一个字符串。
7. 单击页顶部或底部的“保存”，记录此项更改。
8. 从终端窗口中重新启动网关：

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

## 创建禁止屏蔽的 URI 列表

一些应用程序（如 applet）需要一个 Internet URI，而且不能对其进行屏蔽。要指定这些应用程序，可将 URI 添加到列表框中。

例如，如果添加

```
*/Applet/Param*
```

到列表框中，则当内容 URI `http://abc.com/Applet/Param1.html` 在规则集的规则中匹配时，将不会屏蔽此 URI。

### ► 指定禁止屏蔽 URI

1. 以管理员身份登录到 Identity Server 管理控制台。

2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
会显示“网关配置文件”页。
4. 单击需要设置属性的网关配置文件。  
会显示“网关 - *gateway-profile-name*”页。
5. 单击“重写器”选项卡、“高级”子部分。
6. 滚动到“禁止屏蔽 URI 列表”字段，然后在编辑框中添加 URI。
7. 单击页顶部或底部的“保存”，记录此项更改。
8. 从终端窗口中重新启动网关：

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

## 使网关协议与原始 URI 协议相同

当网关同时运行于 HTTP 和 HTTPS 模式下时，您可以允许“重写器”使用一致的协议来访问 HTML 内容中引用的资源。

例如，如果原始 URL 是 `http://intranet.com/Public.html`，则添加 **http** 网关。如果原始 URL 是 `https://intranet.com/Public.html`，则添加 **https** 网关。

---

**注意** 这样做只适用于静态 URI，不适用于 Javascript 中生成的动态 URI。

---

### ► 使网关协议与原始 URI 协议相同

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
会显示“网关配置文件”页。
4. 单击需要设置属性的网关配置文件。  
会显示“网关 - *gateway-profile-name*”页。
5. 单击“重写器”选项卡、“高级”子部分。

6. 选中“使网关协议与原始 URI 协议相同”复选框。
7. 单击页顶部或底部的“保存”，记录此项更改。
8. 从终端窗口中重新启动网关：

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

## 记录选项卡

使用“记录”选项卡，可在网关服务中执行以下任务：

- 启用记录
- 启用 Netlet 日志

### 启用记录

可指定网关日志文件以捕获关于每个会话的最少信息或详细信息。日志信息保存在“日志位置”属性中指定的目录，作为“Identity Server 配置”属性中“记录”的一部分。此日志位于 Portal Server 机器上。

日志使用以下命名惯例：

```
srapGateway_gatewayhostname_gateway-profile-name
```

根据“Identity Server 配置”中的设置，日志信息可以保存为文件或数据库。日志中的字段是由逗号分隔的 ASCII 值，可以导出到其他数据分析工具支持的格式。

#### ► 启用网关日志

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。

显示网关页面。

4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 选中“启用日志”复选框以启用网关日志。
6. 选中“启用每会话日志”复选框以捕获最基本的日志信息，如“客户机地址”、“请求类型”和“目的主机”。

---

**注意** 只有启用“启用日志”字段，才能捕获日志信息。

---

7. 选择“启用详细的每会话日志”，使网关捕获详细的日志信息，如“客户机”、“请求类型”、“目的主机”、“请求的类型”、“客户请求的 URL”、“客户发布数据大小”、“会话 ID”、“应答结果代码”以及“完成应答的大小”等。

---

**注意** 只有选中“启用每会话日志”复选框，才能捕获详细的日志信息。

---

8. 单击页顶部或底部的“保存”，记录这些更改。
9. 从终端窗口中重新启动网关：

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

## 启用 Netlet 日志

可通过选择此选项来启用 Netlet 相关活动的记录功能。Netlet 日志将包含以下有关 Netlet 会话的详细信息：

- 开始时间
- 源地址
- 源端口
- 服务器地址
- 服务器端口
- 停止时间
- 状态（开始或停止）

► 启用 Netlet 日志

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 单击“SRA 配置”下网关旁边的箭头。  
显示网关页面。
4. 单击需要设置属性的网关配置文件旁的“编辑...”。  
会显示“编辑网关配置文件”页。
5. 选中“启用 Netlet 日志”复选框以启用 Netlet 日志。
6. 单击页面底部的“保存”，记录这些更改。
7. 从终端窗口中重新启动网关：

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

记录选项卡

# 配置 NetFile

本章介绍如何通过 Sun Java™ System Identity Server 管理控制台配置 NetFile。

---

**注意** 单击 Identity Server 管理控制台右上角的“帮助”，然后单击“SRA 帮助”以获取所有 SRA 属性的快速参考。

---

## ► 配置 NetFile 属性

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 从“查看”下拉列表中选择“组织”。
6. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
7. 从“查看”列表框中选择“服务”。
8. 单击“SRA 配置”下 NetFile 旁边的箭头。

在此处单击相应选项卡。

- [主机选项卡](#)
- [权限选项卡](#)
- [查看选项卡](#)
- [操作选项卡](#)
- [常规选项卡](#)

下面列出了各个选项卡以及每个选项卡下可以配置的属性。

# 主机选项卡

使用“主机”选项卡，可在 NetFile 服务中执行下列任务：

- 指定 OS 字符集
- 指定主机侦测顺序
- 配置公共主机列表
- 指定默认域
- 指定 Windows 域 / 工作组
- 指定默认 WINS/DNS 服务器
- 指定对不同类型主机的访问
- 配置允许的主机列表
- 配置拒绝的主机列表

## 指定 OS 字符集

可指定在与主机通信时用作默认编码的字符集。默认值为 UTF-8。

---

**警告** 如果未正确指定字符集，则无法预测机器及错误消息的表现行为。

---

### ► 指定 OS 字符集

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。

5. 从“查看”下拉列表中选择“组织”。
6. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
7. 从“查看”下拉列表中选择“组织”。
8. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
9. 从“查看”列表框中选择“服务”。
10. 单击“SRA 配置”下 NetFile 旁边的箭头。  
会显示 NetFile 页。
11. 单击“主机”选项卡、“配置”子部分。
12. 滚动到“OS 字符集”字段并选择字符集代码。
13. 单击 NetFile 页顶部或底部的“保存”，记录此项更改。

## 指定主机侦测顺序

### ► 指定主机侦测顺序

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 从“查看”下拉列表中选择“组织”。
6. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
7. 从“查看”下拉列表中选择“组织”。
8. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
9. 从“查看”列表框中选择“服务”。
10. 单击“SRA 配置”下 NetFile 旁边的箭头。  
会显示 NetFile 页。

11. 单击“主机”选项卡、“配置”子部分。
12. 滚动到“主机侦测顺序”字段并选择主机类型。
13. 使用“上移”及“下移”按钮更改主机侦测顺序。
14. 单击 NetFile 页顶部或底部的“保存”，记录此项更改。

## 配置公共主机列表

可配置通过 NetFile 对所有远程 NetFile 用户都可用主机列表。需要为所添加的每个主机指定以下信息：

**主机名** — 既可以键入简单主机名，也可以键入全限定名称。如果您提供的主机名与用户配置的主机名匹配，则会合并这两组信息，并且用户指定的值会覆盖您指定的值。

例如，假定您已配置了 4 个公共主机 - `sesta`、`siroe`、`florizon` 和 `abc`。某位用户配置了 3 个主机，其中有 2 个为 `sesta` 和 `siroe`。在这种冲突情况下，用户指定的值会覆盖管理员指定的值。在用户的 NetFile 中，也会列出 `florizon` 和 `abc`，而且此用户能对这些主机执行各种操作。纵使您已将 `florizon` 列入了“拒绝的主机列表”，`florizon` 仍会在用户的 NetFile 中列出，只是不能对 `florizon` 执行任何操作。

**主机类型** — 如果用户所添加的主机已在“公共主机”列表中列出，用户设置优先。如果存在类型冲突，不会为该用户添加管理员所添加的共享组件。如果用户与管理员所添加的共享组件相同，则会添加此共享组件，但用户设置的口令优先。

**编码** — 如果此处指定的值与用户设置之间有冲突，用户设置优先。如果您指定的设置为空或无效，则会使用客户机 OS（用户的机器）的字符集。

---

**注意** 用户可以编辑 NetFile 客户机应用程序中的任何值。但编辑后的值仅对当前会话有效。如果用户注销后又重新登录，不会保留这些编辑后的值。

---

► **配置公共主机列表**

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 从“查看”下拉列表中选择“组织”。
6. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
7. 从“查看”下拉列表中选择“组织”。
8. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
9. 从“查看”列表框中选择“服务”。
10. 单击“SRA 配置”下 NetFile 旁边的箭头。  
会显示 NetFile 页。
11. 单击“主机”选项卡、“配置”子部分。  
会显示“NetFile > 添加 NetFile 主机”页。
12. 要添加公共主机，请执行以下步骤：
  - a. 在下列字段中输入所需信息：
    - 主机名
    - 主机类型
    - 编码
    - Windows 域 / 工作组
    - 用户名
    - 口令
  - b. 在下列字段中，为想要添加的每个共享组件输入所需信息，然后单击“添加到列表”：
    - 共享列表
    - 共享名
    - 共享口令

- c. 单击“确定”。
  - d. 为想要添加或删除的每个公共主机重复上述信息设置。
13. 要从“公共主机”列表中删除公共主机，请执行以下步骤：
- a. 单击“删除”，然后从“共享列表”中选择“主机名”。接着单击“移除”。
  - b. 单击 NetFile 页顶部或底部的“保存”，记录此项更改。

## 指定默认域

可以指定 NetFile 联络允许的主机时需要使用的默认域。

仅当用户在使用 NetFile 添加主机时指定的不是全限定主机名时，该默认域值才适用。

---

**警告** 确保“默认域”字段不为空，并且其中包含有效的域名。

---

### ► 指定默认域

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 从“查看”下拉列表中选择“组织”。
6. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
7. 从“查看”下拉列表中选择“组织”。
8. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
9. 从“查看”列表框中选择“服务”。

10. 单击“SRA 配置”下 NetFile 旁边的箭头。  
会显示 NetFile 页。
11. 单击“主机”选项卡、“配置”子部分。
12. 滚动到“默认域”字段，然后键入默认域名。
13. 单击 NetFile 页顶部或底部的“保存”，记录此项更改。

## 指定 Windows 域 / 工作组

这是用户访问 Windows 主机时选择的默认 Windows 域或工作组。

用户可以在添加机器时指定不同的值来覆盖该值。

### ► 指定默认 Windows 域或工作组

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 从“查看”下拉列表中选择“组织”。
6. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
7. 从“查看”下拉列表中选择“组织”。
8. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
9. 从“查看”列表框中选择“服务”。
10. 单击“SRA 配置”下 NetFile 旁边的箭头。  
会显示 NetFile 页。
11. 单击“主机”选项卡、“配置”子部分。
12. 滚动到“默认 Windows 域 / 工作组”字段，然后键入默认域名或工作组名。
13. 单击 NetFile 页顶部或底部的“保存”，记录此项更改。

## 指定默认 WINS/DNS 服务器

这是 NetFile 用来访问 windows 主机的 WINS/DNS 服务器。

### ► 指定默认 WINS/DNS 服务器

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 从“查看”下拉列表中选择“组织”。
6. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
7. 从“查看”下拉列表中选择“组织”。
8. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
9. 从“查看”列表框中选择“服务”。
10. 单击“SRA 配置”下 NetFile 旁边的箭头。  
会显示 NetFile 页。
11. 单击“主机”选项卡、“配置”子部分。
12. 滚动到“默认 WINS/DNS 服务器”字段，然后键入默认的 Windows 或 DNS 服务器名。
13. 单击 NetFile 页顶部或底部的“保存”，记录此项更改。

## 指定对不同类型主机的访问

可指定用户是否可以访问特定的主机，如 Windows、FTP、NFS 或 Netware 主机。还可以设置相应的选项来允许或拒绝对每一类型主机的访问。默认情况下，所有这些选项均已启用。

### ► 指定对不同类型主机的访问

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份管理”选项卡。从“查看”下拉列表中选择“组织”。
3. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
4. 从“查看”下拉列表中选择“组织”。
5. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
6. 从“查看”列表框中选择“服务”。
7. 单击“SRA 配置”下 NetFile 旁边的箭头。  
会显示 NetFile 页。
8. 单击“主机”选项卡、“配置”子部分。
9. 单击允许访问的主机类型。您可以选择启用下列选项：
  - 允许访问 Windows 主机
  - 允许访问 FTP 主机
  - 允许访问 NFS 主机
  - 允许访问 Netware 主机选择相应的选项可使用户访问该特定类型的主机。清除相应的复选框将禁止用户访问该类型的主机。
10. 单击页顶部或底部的“保存”，记录此项更改。

## 配置允许的主机列表

默认情况下，由于列表中有 \* 条目，所以允许用户通过 NetFile 访问所有主机。如果您想要改变这种情况，可在列表中删除 \* 条目，然后只在其中指定用户需要通过 NetFile 来进行访问的那些主机。另一种做法是，保留此处的 \* 条目，而在“拒绝的主机”列表中指定想要拒绝访问的主机。在这种情况下，除了“拒绝的主机”列表中指定的主机以外，允许访问所有主机。

有关详细信息，请参阅第 292 页的“配置拒绝的主机列表”。

---

**注意** 如果“允许的主机”列表和“拒绝的主机”列表均为空，则不允许访问任何主机。

---

► **创建允许的主机列表**

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 从“查看”下拉列表中选择“组织”。
6. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
7. 从“查看”下拉列表中选择“组织”。
8. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
9. 从“查看”列表框中选择“服务”。
10. 单击“SRA 配置”下 NetFile 旁边的箭头。  
会显示 NetFile 页。
11. 单击“主机”选项卡、“配置”子部分。
12. 滚动到“允许的主机”字段。在编辑字段键入想要允许访问的主机的名称，然后单击“添加”。  
该主机名会添加到“允许的主机”列表框中。
13. 单击页顶部或底部的“保存”，记录这些更改。

## 配置拒绝的主机列表

在第 286 页的“配置公共主机列表”下指定了可公用的主机列表后，您还可以通过 NetFile 指定拒绝用户访问的主机列表。

---

**注意** 如果您拒绝访问某一主机，而某位用户已将该主机添加到 NetFile 窗口中，被拒绝的主机仍会在该用户的 NetFile 窗口中显示。但该用户将不能对此主机执行任何操作。

在 NetFile Java2 中，被拒绝的主机在应用程序中显示时标有红色的叉，指示它们是不可访问的。

---

---

**注意** 如果“允许的主机”列表和“拒绝的主机”列表均为空，则不允许访问任何主机。

---

► **创建拒绝的主机列表**

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 从“查看”下拉列表中选择“组织”。
6. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
7. 从“查看”下拉列表中选择“组织”。
8. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
9. 从“查看”列表框中选择“服务”。
10. 单击“SRA 配置”下 NetFile 旁边的箭头。  
会显示 NetFile 页。
11. 单击“主机”选项卡、“配置”子部分。
12. 滚动到“拒绝的主机”字段。在编辑字段键入想要拒绝访问的主机的名称。
13. 单击“添加”。  
该主机名会添加到“拒绝的主机”列表框中。
14. 单击页顶部或底部的“保存”，记录这些更改。

# 权限选项卡

使用“权限”选项卡，可以在 NetFile 服务中允许或拒绝用户从远程主机执行下列任务的权限：

- 重命名文件
- 删除文件和文件夹
- 上载文件
- 下载文件和文件夹
- 搜索文件
- 邮寄文件
- 压缩文件
- 更改用户 Id

此选项允许您指定用户是否可用不同的 ID 连接到使用 NetFile 的主机。在大型组织中，用户可能会有多个用户 ID。您或许希望限制用户使用单个用户 ID。此时，可禁用“允许改变用户 ID”选项。这将防止特定组织中的所有用户更改其用户 ID，并限制他们只能通过 NetFile 使用单个 ID（桌面登录 ID）连接到主机。在另一种情况下，用户可能在不同的机器上有不同的登录 ID，此时，您或许希望允许用户根据需要更改 ID。

- 更改 Windows 域

该选项适用于 NT 域。

如果用户在添加某个系统时，在“用户 NT 域名”字段中指定了一个无效域名，会显示一条错误消息。如果用户在以后编辑主机信息时指定了一个无效的域名，则不会显示错误信息。

如果用户指定了域名，还需要为该域指定用户名和口令。如果需要使用主机用户名和口令，用户需从“用户 NT 域名”字段中删除此域。

默认情况下，权限选项已启用。

### ► 启用 / 禁用权限

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 从“查看”下拉列表中选择“组织”。
6. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
7. 从“查看”下拉列表中选择“组织”。
8. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
9. 从“查看”列表框中选择“服务”。
10. 单击“SRA 配置”下 NetFile 旁边的箭头。  
会显示 NetFile 页。
11. 单击“权限”选项卡。
12. 滚动到所需“允许”字段，然后单击相应的复选框以允许权限。
13. 单击 NetFile 页顶部或底部的“保存”，记录此项更改。

---

**注意** 如果您在用户开始使用 NetFile 后禁用了这些选项，则仅当用户从 NetFile 中注销并重新登录时，此更改才会生效。

---

## 查看选项卡

使用“查看”选项卡，可在 NetFile 服务中执行下列任务：

- [指定 NetFile 窗口大小](#)
- [指定 NetFile 窗口位置](#)

## 指定 NetFile 窗口大小

可在用户桌面上以像素为单位指定 NetFile 窗口的大小。默认值是 700|400（像素）。如果输入了无效值，NetFile 会使用默认值。

---

**注意** 用户也可以在其可以使用的受限管理控制台中编辑该值。如果用户重新在桌面上调整了 NetFile 窗口的大小，会用新值替换您指定的值。

---

### ► 指定 NetFile 窗口的大小

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 从“查看”下拉列表中选择“组织”。
6. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
7. 从“查看”列表框中选择“服务”。
8. 单击“SRA 配置”下 NetFile 旁边的箭头。  
会显示 NetFile 页。
9. 单击“查看”选项卡。
10. 滚动到“窗口大小”字段，然后键入所需的窗口大小（像素）。  
以 700|400 格式键入该值，不带空格。坐标形如 x|y。不能用其他字符作为分隔符。
11. 单击 NetFile 页顶部或底部的“保存”，记录此项更改。

## 指定 NetFile 窗口位置

可以指定 NetFile 窗口在用户桌面上的显示位置。默认值是 100|50（像素）。如果输入了无效值，NetFile 会使用默认值。

---

**注意** 用户也可以在其可以使用的受限管理控制台中编辑该值。如果用户重新在桌面上调整了 NetFile 窗口的位置，会用新值替换您指定的值。

---

### ► 指定 NetFile 窗口的位置

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 从“查看”下拉列表中选择“组织”。
6. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
7. 从“查看”下拉列表中选择“组织”。
8. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
9. 从“查看”列表框中选择“服务”。
10. 单击“SRA 配置”下 NetFile 旁边的箭头。  
会显示 NetFile 页。
11. 单击“查看”选项卡。
12. 滚动到“窗口位置”字段，然后键入所需的窗口位置坐标。  
以 100|50 格式键入该值，不带空格。坐标形如 x|y。不能用其他字符作为分隔符。
13. 单击 NetFile 页顶部或底部的“保存”，记录此项更改。

## 操作选项卡

使用“操作”选项卡，可在 NetFile 服务中执行下列任务：

- 指定临时文件目录
- 设置文件上传大小限制
- 指定搜索目录限制
- 指定压缩

### 指定临时文件目录

NetFile 需要一个临时目录来进行某些文件操作，如邮寄文件。默认临时目录是 /tmp。在执行完所需操作后，会删除这些临时文件。

如果所指定的临时目录在服务器上不存在，则会创建它。

确保运行 Web 服务器的 ID（如 nobody 或 noaccess）对所指定的目录具有 rwx 权限。还要确保此 ID 对于到所需临时目录的完整路径具有 rx 权限。

---

**提示** 最好为 NetFile 创建一个单独的临时目录。如果所指定的临时目录是 Portal Server 的所有模块公用的，磁盘空间可能很快就会用完。如果临时目录没有空间，NetFile 中的部分操作（如邮寄文件）将无法工作。

---

#### ► 指定临时目录

1. 以管理员身份登录到 Sun Java™ System Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 从“查看”下拉列表中选择“组织”。

6. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
7. 从“查看”列表框中选择“服务”。
8. 单击“SRA 配置”下 NetFile 旁边的箭头。  
会显示 NetFile 页。
9. 单击“操作”选项卡、“通信量”子部分。
10. 滚动到“临时目录位置”字段，然后键入所需的临时目录位置。
11. 单击 NetFile 页顶部或底部的“保存”，记录此项更改。

## 设置文件上传大小限制

可在这个字段中指定所能上载的最大文件大小。如果要上载的文件大小超出此处指定的限制，将显示一条错误消息并且不会上载该文件。默认值为 5 MB。如果输入无效值，NetFile 会将其重置为默认值。

可为不同用户指定不同的文件上传大小限制。

---

**注意** 要以兆字节为单位指定最大文件上传大小。确保键入的是整数。

---

### ► 设置文件上传大小限制

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 从“查看”下拉列表中选择“组织”。
6. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
7. 从“查看”列表框中选择“服务”。

8. 单击“SRA 配置”下 NetFile 旁边的箭头。  
会显示 NetFile 页。
9. 单击“操作”选项卡、“通信量”子部分。
10. 滚动到“文件上传限制 (MB)”字段。键入所需大小限制（兆字节）。
11. 单击 NetFile 页顶部或底部的“保存”，记录此项更改。

## 指定搜索目录限制

可以配置在单次搜索操作中将要搜索的最大目录数。在大量用户同时登录的情况下，此限制有助于减少网络阻塞，提高访问速度。默认值为 100。如果键入无效值，NetFile 会将其重置为默认值。

假设用户有一个名为 A 的目录。同时，假定 A 有 100 个子目录。如果指定要搜索的最大目录数为 100，搜索操作将会从头至尾搜索目录 A，然后停止。由于在目录 A 中已达到 100 这一限制，所以不会继续在用户机器的其他目录中进行搜索。达到搜索限制时积累的搜索结果显示给用户，并显示一条错误消息，表明已超出搜索限制。要继续搜索，用户必须在下一目录手动重新启动搜索。

搜索操作以深度优先方式进行。这就意味着，搜索操作在转移到下一目录之前，会先在用户所选目录的所有子目录中进行。

### ► 指定搜索目录限制

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 从“查看”下拉列表中选择“组织”。
6. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
7. 从“查看”下拉列表中选择“组织”。

8. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
9. 从“查看”列表框中选择“服务”。
10. 单击“SRA 配置”下 NetFile 旁边的箭头。  
会显示 NetFile 页。
11. 单击“操作”选项卡、“搜索”子部分。
12. 滚动到“搜索目录限制”字段，然后键入所需数目。

---

**注意** 确保在该字段中键入一个整数值。

---

13. 单击 NetFile 页顶部或底部的“保存”，记录此项更改。

## 指定压缩

这些压缩属性仅适用于 NetFile Java2。

### ► 指定默认压缩类型

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 从“查看”列表框中选择“服务”。
6. 单击“SRA 配置”下 NetFile 旁边的箭头。  
会显示 NetFile 页。
7. 单击“操作”选项卡、“压缩”子部分。
8. 滚动到“默认压缩类型”字段。  
选择 Zip 或 GZip
9. 单击 NetFile 页顶部或底部的“保存”，记录此项更改。

## 常规选项卡

使用“常规”选项卡，可以在 NetFile 服务中指定 MIME 类型配置文件位置。

### 指定 MIME 类型配置文件位置

该信息是确定发送到客户机浏览器的响应内容类型所必需的。浏览器需要该信息来确定在执行 NetFile 打开或下载操作期间，需要将文件与哪个应用程序相关联。这是在安装期间配置的。

如果需要使用 Portal Server Web 服务器的 MIME 类型文件，请指定此位置：

```
portal-server-install-root/SUNWam/servers/instance-name-of-web-server-machine/config
```

---

**注意** 只能在组织级别设置“MIME 类型配置文件定位”属性。

---

#### ► 指定 MIME 类型配置文件的位置

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 从“查看”下拉列表中选择“组织”。
6. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
7. 从“查看”列表框中选择“服务”。
8. 单击“SRA 配置”下 NetFile 旁边的箭头。  
会显示 NetFile 页。

9. 单击“常规”选项卡。
10. 滚动到“MIME 类型配置文件定位”字段，然后键入到 MIME 类型配置文件所在位置的完整路径。
11. 单击 NetFile 页顶部或底部的“保存”，记录此项更改。

## 启用 NetFile 的调试功能

调试信息的位置取决于 `com.ipplanet.services.debug.directory` 属性的设置，该属性在 Portal Server 节点上的 `AMConfig-instance-name.properties` 文件中。

例如，如果 `com.ipplanet.services.debug.directory` 属性的值为：

```
/var/opt/SUNWam/debug/
```

则 NetFile 的调试信息将可以在 `/var/opt/SUNWam/debug` 目录下的 `srapNetFile` 文件中获得。

有关详细信息，请参阅《*Identity Server 管理指南*》。

常规选项卡

## 配置 Netlet

本章介绍如何通过 Sun Java™ System Identity Server 管理控制台配置 Netlet 属性。

---

**注意** 单击 Identity Server 管理控制台右上角的“帮助”，然后单击“SRA 帮助”以获取所有 SRA 属性的快速参考。

---

可在组织级别配置的所有属性也可以在用户级别配置。有关组织、角色以及用户级属性的详细信息，请参阅《Identity Server 管理指南》。

要配置 Netlet 属性，请按以下步骤在组织级别配置属性：

1. 以管理员身份登录到 Sun Java™ System Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 从“查看”下拉列表中选择“服务”。
6. 单击“SRA 配置”下 Netlet 旁边的箭头。

从这里，您可以执行下列任务：

- [添加 Netlet 规则](#)
- [为用户分配 Netlet 服务](#)
- [添加 Netlet 规则](#)

- 修改现有 Netlet 规则
- 删除 Netlet 规则

除了配置用户配置文件以及创建 Netlet 规则以外，您还需要根据自己站点的要求配置下列属性。这些属性可以在组织或用户级别进行配置。

- 指定默认加密密码
- 分配默认回环端口
- 启用连接时重新验证
- 启用连接时弹出警告对话框
- 启用在端口警告对话框中显示复选框
- 设置保活间隔
- 设置门户注销时终止 Netlet 选项
- 定义 Netlet 访问规则
- 拒绝 Netlet 访问规则
- 允许访问主机拒绝访问主机

## 为用户分配 Netlet 服务

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。  
所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 从“查看”下拉列表中为所选的组织选择“用户”。
6. 单击左窗格中所需用户旁边的箭头。
7. 如果 Netlet 服务对该用户尚不可用，请从“查看”下拉列表中为该用户选择“服务”。
8. 单击“添加”。

9. 从“可用服务”列表中选择 Netlet。
10. 单击“保存”
11. 从“查看”下拉列表中选择 Netlet 服务，可以为该用户修改 Netlet 属性。

## 添加 Netlet 规则

在 Identity Server 管理控制台的“身份认证管理”选项卡中，可以在全局级别添加或创建 Netlet 规则。您新创建的任何组织都会继承这些规则。

还可以在组织、角色或用户级别创建新规则或修改现有规则。

### ► 添加 Netlet 规则

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 选择想要为其创建规则的“组织”。
4. 从“查看”下拉列表中选择“服务”。
5. 单击“SRA 配置”下 Netlet 旁边的箭头。  
在右窗格中会显示 Netlet 页。
6. 在“Netlet 规则”字段中单击“添加”。  
会显示“添加 Netlet 规则”页。规则的所有字段均填充了示例值，您可以根据需要更改这些值。
7. 在“规则名称”字段中为规则键入一个唯一的名称。
8. 指定所需的密码。选择“默认”可保留默认的加密密码。选择“其他”可从可用密码列表中进行选择。  
有关默认密码的详细信息，请参阅第 310 页的“指定默认密码”。
9. 在 URL 字段中键入指向要调用的应用程序的 URL。
10. 如果需要下载某个 applet，请选中“下载 Applet”复选框。以本地端口：服务器主机：服务器端口的格式，在关联的编辑框中键入 applet 详细信息。

---

**注意** 为每一规则指定一个唯一的本地端口。

---

仅当需要从 Portal Server 主机以外的某个主机下载 applet 时，才需要指定 applet 详细信息。如果没有选中此复选框，上述编辑框将被禁用。有关详细信息，请参阅第 184 页的“从远程主机下载 Applet”。

11. 选中“扩展会话”复选框，确保在该规则相应的 Netlet 会话运行期间，延长 Portal Server 会话时间。
12. 在“本地端口”字段中键入 Netlet 监听的本地端口。  
对于 FTP 规则，本地端口值必须是 30021。
13. 在“目标主机”字段中键入一个输入项。  
对于静态规则，输入 Netlet 要连接的目标机器的主机名。  
对于动态连接，输入 "TARGET"。
14. 在“目标端口”字段中键入目标主机上的端口。
15. 单击“添加到列表”，以便在“本地端口到目的端口”字段中反映最新输入的三项信息。
16. 单击“保存”。  
将会保存规则并返回到 Netlet 页。在“Netlet 规则”列表中会显示新的规则名。

## 修改现有 Netlet 规则

通过管理控制台中的“身份管理”选项卡，可以在组织、角色或用户级别修改现有规则。您新创建的任何组织都会继承这些规则。

### ► 修改 Netlet 规则

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 选择想要为其修改规则的“组织”。
4. 从“查看”下拉列表中选择“服务”。

5. 单击“SRA 配置”下 Netlet 旁边的箭头。  
在右窗格中会显示 Netlet 页。
6. 单击想要修改的规则的名称。  
会显示“编辑 Netlet 规则”页。
7. 根据需要进行更改，然后单击“保存”。  
将会保存修改后的规则并返回到 Netlet 页。

## 删除 Netlet 规则

在管理控制台的“身份认证管理”选项卡中，可以在全局级别删除 Netlet 规则。

### ► 删除 Netlet 规则

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 选择想要为其删除规则的“组织”。
4. 单击“SRA 配置”下 Netlet 旁边的箭头。  
在右窗格中会显示 Netlet 页。
5. 选中要从“Netlet 规则”列表中删除的规则旁边的复选框。
6. 单击“删除”。  
会从“Netlet 规则”列表中删除所选规则。

---

**注意** 本部分介绍所有组织级属性的配置。

---

## 指定默认加密密码

需要为 Netlet 规则指定默认密码。这在使用其中未包括密码的现有规则时非常有用。该字段是强制字段。请参阅第 191 页的“向后兼容性”。

► **指定默认密码**

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 从“查看”下拉列表中选择“服务”。
6. 单击“SRA 配置”下 Netlet 旁边的箭头。  
在右窗格中会显示 Netlet 页。
7. 滚动到“默认本地 VM 密码”或“默认 Java Plugin 密码”字段，然后从下拉列表中选择所需密码。要获得所支持密码的列表，请参阅第 190 页的“支持的密码”。
8. 单击 Netlet 页顶部或底部的“保存”，记录此项更改。

## 分配默认回环端口

当通过 Netlet 下载 applet 时，此属性指定用于本地计算机的端口。所使用的默认值为 58000，除非在 Netlet 规则中取代了该值。

► **分配默认回环端口**

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 从“查看”下拉列表中选择“服务”。
6. 单击“SRA 配置”下 Netlet 旁边的箭头。  
在右窗格中会显示 Netlet 页。
7. 滚动到“默认回环端口”字段，然后键入所需的端口号。
8. 单击 Netlet 页顶部或底部的“保存”，记录此项更改。

## 启用连接时重新验证

如果希望用户在每次需要建立 Netlet 连接时都要输入 Netlet 口令，请启用该选项。如果启用了该选项，在用户桌面上将不会显示连接警告弹出窗口。有关详细信息，请参阅第 311 页的“启用连接时弹出警告对话框”。

启用该选项后，将允许用户使用 Netlet 频道编辑选项更改重新验证口令。默认情况下，初始口令是 srap-Netlet。

### ► 启用连接时重新验证

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 从“查看”下拉列表中选择“服务”。
6. 单击“SRA 配置”下 Netlet 旁边的箭头。  
在右窗格中会显示 Netlet 页。
7. 滚动到“连接时重新验证”字段，然后选择此选项。
8. 单击 Netlet 页顶部或底部的“保存”，记录此项更改。

## 启用连接时弹出警告对话框

当有人试图通过监听端口连接到 Netlet，并且用户正使用 Netlet 运行应用程序时，该属性会在用户桌面上显示弹出警告对话框。如果您不希望出现在用户桌面上出现弹出窗口，可取消选择该属性。

### ► 启用连接时弹出警告

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。

4. 单击所需的组织名。所选组织名会在管理控制台左上角的“位置”信息中反映出来。
5. 从“查看”下拉列表中选择“服务”。
6. 单击“SRA 配置”下 Netlet 旁边的箭头。  
在右窗格中会显示 Netlet 页。
7. 选中“显示连接时弹出警告”复选框以启用弹出警告。
8. 单击 Netlet 页顶部或底部的“保存”，记录此项更改。

## 启用在端口警告对话框中显示复选框

如果在管理控制台中启用了弹出警告，则当 Netlet 试图通过本地机上可自由使用的端口连接到目的主机时，该属性会在用户桌面上的弹出警告中显示复选框。通过选中或取消选中桌面上相应的复选框，用户可选择启用或禁用弹出窗口。

在管理控制台中禁用“在端口警告对话框中显示复选框”选项，可允许用户禁止该弹出警告。

### ► 允许用户禁止端口警告对话框

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 从“查看”下拉列表中选择“服务”。
6. 单击“SRA 配置”下 Netlet 旁边的箭头。  
在右窗格中会显示 Netlet 页。
7. 滚动到“在端口警告对话框中显示复选框”字段，然后取消选中相应的方框。
8. 单击 Netlet 页顶部或底部的“保存”，记录此项更改。

## 设置保活间隔

如果客户机正通过网络代理连接到网关，则由于代理超时将断开空闲的 Netlet 连接。为防止出现此情况，请为此参数指定一个小于代理超时值的值。

### ► 设置保活间隔

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 从“查看”下拉列表中选择“服务”。
6. 单击“SRA 配置”下 Netlet 旁边的箭头。  
在右窗格中会显示 Netlet 页。
7. 滚动到“保活间隔（分钟）”字段，然后键入所需的时间间隔。
8. 单击 Netlet 页顶部或底部的“保存”，记录此项更改。

## 设置门户注销时终止 Netlet 选项

如果希望确保在用户从 Portal Server 中注销时终止所有连接，请启用该选项。这将确保更高的安全性。默认情况下，该选项已启用。

禁用该选项可确保即使在用户已从 Portal Server 桌面中注销后，活动的 Netlet 连接仍会起作用。

---

**注意** 禁用该选项后，将不允许用户在从 Portal Server 中注销后进行新的 Netlet 连接。而是只保持现有的连接。

---

### ► 设置门户注销时终止 Netlet 选项

1. 以管理员身份登录到 Identity Server 管理控制台。

2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 从“查看”下拉列表中选择“服务”。
6. 单击“SRA 配置”下 Netlet 旁边的箭头。  
在右窗格中会显示 Netlet 页。
7. 滚动到“门户注销时终止 Netlet”字段，然后根据需要选择或取消选取此选项。
8. 单击 Netlet 页顶部或底部的“保存”，记录此项更改。  
另请参阅在 [Sun Ray 环境中运行 Netlet](#)。

## 定义 Netlet 访问规则

可为某些组织、角色或用户定义对特定 Netlet 规则的访问。

### ► 定义 Netlet 访问规则

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 从“查看”下拉列表中选择“服务”。
6. 单击“SRA 配置”下 Netlet 旁边的箭头。  
在右窗格中会显示 Netlet 页。
7. 滚动到“Netlet 访问规则”字段。
8. 在“Netlet 访问规则”字段中，键入想要为所选组织提供使用的规则名称。  
该字段中的星号 (\*) 表示所有已定义的 Netlet 规则都可用于所选组织。

9. 单击“添加”。  
会将指定的规则添加到“Netlet 访问规则”列表中。
10. 对想要提供使用的每一项 Netlet 规则重复步骤 7、8 和 9。
11. 单击 Netlet 页顶部或底部的“保存”，记录此项更改。

## 拒绝 Netlet 访问规则

可以拒绝某些组织、角色或用户对特定 Netlet 规则的访问。

### ► 拒绝 Netlet 访问规则

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 从“查看”下拉列表中选择“服务”。
6. 单击“SRA 配置”下 Netlet 旁边的箭头。  
在右窗格中会显示 Netlet 页。
7. 滚动到“Netlet 拒绝规则”字段。
8. 在“Netlet 拒绝规则”字段中，键入想要拒绝所选组织访问的规则名称。  
该字段中的星号 (\*) 表示拒绝所选组织访问所有已定义的 Netlet 规则。
9. 单击“添加”。  
会将指定的规则添加到“Netlet 拒绝规则”列表中。
10. 对想要拒绝访问的每一项 Netlet 规则重复步骤 7、8 和 9。
11. 单击 Netlet 页顶部或底部的“保存”，记录此项更改。

## 允许访问主机

可为某些组织、角色或用户定义对特定主机的访问。这使您可以允许对某些主机的访问。例如，您可以建立一个含有五个主机的“允许”列表，使用户可以远程登录到这些主机。

### ► 允许访问主机

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 从“查看”下拉列表中选择“服务”。
6. 单击“SRA 配置”下 Netlet 旁边的箭头。

在右窗格中会显示 Netlet 页。

7. 滚动到“允许的主机”字段。
8. 在“允许的主机”字段中，键入想要允许访问的主机的名称。

该字段中的星号 (\*) 表示指定域中的所有主机都是可以访问的。例如，如果指定 \*.sesta.com，则用户可以执行 sesta.com 域中的所有 Netlet 目标。也可指定一个含有通配符的 IP 地址，如 xxx.xxx.xxx.\*。

9. 单击“添加”。  
会将指定的主机添加到“允许的主机”列表中。
10. 对想要提供使用的每个主机重复步骤 7 和 8。
11. 单击 Netlet 页顶部或底部的“保存”，记录此项更改。

## 拒绝访问主机

可拒绝对组织内特定主机的访问。在“拒绝的主机”列表中，指定想要拒绝访问的主机。

### ► 拒绝访问主机

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“身份认证管理”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 从“查看”下拉列表中选择“服务”。
6. 单击“SRA 配置”下 Netlet 旁边的箭头。  
在右窗格中会显示 Netlet 页。
7. 滚动到“拒绝的主机”字段。
8. 在“拒绝的主机”字段中，键入想要拒绝访问的主机的名称。  
该字段中的星号 (\*) 表示拒绝用户访问所选组织中的所有主机。例如，要拒绝访问 sesta 组织中的所有主机，请在“拒绝的主机”字段中键入 \*.sesta.com。  
要拒绝访问特定的主机，请指定相应的全限定名。例如，要拒绝访问主机 abc，请键入 abc.sesta.com。
9. 单击“添加”。  
会将指定的域添加到“域访问”列表中。
10. 对想要提供使用的每个域重复步骤 7 和 8。
11. 单击 Netlet 页顶部或底部的“保存”，记录此项更改。

## 代理配置

可以在用户级别配置以下属性：

- 浏览器代理类型
- 浏览器代理主机
- 浏览器代理端口
- 浏览器代理忽略列表

如果您没有在管理控制台中指定这些值并且 Netlet 无法确定浏览器代理的设置，则在首次通过 Netlet 建立连接时，将会请求用户提供该信息。该信息被存储起来并由用户在将来建立连接时使用。

Netlet 无法确定以下场景中的浏览器代理的设置：

- 用户使用的是装有 Java 插件（1.4.0 版本以下）的 Internet Explorer 4.x、5.x 或 6.x，已在“Java 插件控制面板”的“代理”选项卡中启用了“使用浏览器设置”选项，并且已在 Internet Explorer 的“局域网设置”对话框的“使用自动配置脚本”字段中指定了一个附加产品或 INS 文件。
- 用户使用的是装有 Java 插件（1.3.1\_01 版或更高版本）的 Netscape 6.2，并且已在“Java 插件控制面板”的“代理”选项卡中启用了“使用浏览器设置”选项。

在这两种情况下，Netlet 有可能无法确定浏览器设置，因而会请求用户提供以下信息：

- 浏览器代理类型  
该属性可取的值为“直接”或“手动”。如果用户从下拉列表中选择“直接”，Netlet 会直接连接到网关主机。
- 浏览器代理主机  
指定所需的代理主机，Netlet 需要通过该主机进行连接。
- 浏览器代理端口  
指定代理主机上的端口，Netlet 需要通过该端口进行连接。
- 浏览器代理忽略列表（用逗号分隔）  
指定不想让 Netlet 通过代理进行连接的主机。该列表可以包含多个以逗号分隔的主机名。

## 启用调试日志

调试信息的位置取决于 `com.ipplanet.services.debug.directory` 属性的设置，该属性在 Portal Server 节点上的 `AMConfig-instance-name.properties` 文件中。

例如，如果 `com.ipplanet.services.debug.directory` 属性的值为：

```
/var/opt/SUNWam/debug/
```

则 Netlet 的调试信息将可以在 `/var/opt/SUNWam/debug` 目录下的 `srappNetlet` 文件中获得。

有关详细信息，请参阅 《*Identity Server 管理指南*》。

启用调试日志

## 配置 Proxylet

本章介绍如何通过 Sun Java™ System Identity Server 管理控制台配置 Proxylet。

---

**注意** 单击 Identity Server 管理控制台右上角的“帮助”，然后单击“SRA 帮助”以获取所有 SRA 属性的快速参考。

---

### 配置 Proxylet

通过选中 Proxylet 频道编辑页中的“自动下载 Proxylet Applet”复选框，可以将 Proxylet 配置为当用户登录时自动启动。如果未选中“自动下载 Proxylet”复选框，则用户可通过单击标准“门户桌面”的 Proxylet 频道中的“启动 Proxylet”链接随时启动 Proxylet。

#### ► 配置 Proxylet 属性

1. 以管理员身份登录到 Identity Server 管理控制台。
2. 选择“服务配置”选项卡。
3. 从“查看”下拉列表中选择“组织”。
4. 单击所需的组织名。所选组织名会在管理控制台左上角的位置信息中反映出来。
5. 单击“SRA 配置”下 Proxylet 旁边的箭头。
6. 如果需要，选中“自动下载 Proxylet Applet”复选框。
7. 输入将运行 Proxylet 的“默认 Proxylet Applet 绑定 IP”地址。

8. 在“默认 Proxylet Applet 端口”字段中输入 Proxylet 进行监听所需的端口号。
9. 单击“保存”。

---

**注意** 如果用户登录到 Portal Server 并调用 Proxylet，然后安装 Java Plugin，则用户必须重新启动 Netscape 浏览器。

---

## 配置 SSL 加速器

本章介绍如何为 Sun Java™ System Portal Server Secure Remote Access 配置各种加速器。

本章包括以下主题：

- [Sun Crypto Accelerator 1000](#)
- [Sun Crypto Accelerator 4000](#)
- [外部 SSL 设备和代理加速器](#)

### 概述

外部加速器是专用的硬件协处理器，用于从服务器 CPU 卸载 SSL 功能，借此释放 CPU 空间以使其执行其他任务，同时提高对 SSL 事务的处理速度。

### Sun Crypto Accelerator 1000

Sun™ Crypto Accelerator 1000 (Sun CA1000) 板是一块短 PCI 板，它可作为加密协处理器以加速公共密钥和对称加密。本产品无外部接口。该板通过内部 PCI 总线接口与主机通信。采用此板卡的目的是针对电子商务应用程序中的安全协议，加速各种在计算上较为密集的加密算法。

许多关键的加密功能，如 RSA [7] 和 Triple-DES (3DES) [8]，都可从应用程序中卸载到 Sun CA1000 并以并行方式执行。这样便可释放中央处理器空间以执行其他任务，同时提高对 SSL 事务的处理速度。

## 启用 Crypto Accelerator 1000

确保已安装了 Portal Server Secure Remote Access，并安装了网关服务器证书（自签名或由任一 CA 所签发）。有关详细信息，请参阅[证书](#)一章。

[表 13-1](#) 是一个清单，有助于您在安装“SSL 加速器”之前熟悉所需信息。它列出了 Crypto Accelerator 1000 的参数和相应值。

**表 13-1** Crypto Accelerator 1000 安装清单

参数	值
SRA 安装基本目录	/opt
SRA 证书数据库路径	/etc/opt/SUNWps/cert/default
SRA 服务器证书昵称	server-cert
区域	sra-keystore
区域用户	crypta

## 配置 Crypto Accelerator 1000

### ► 配置 Crypto Accelerator 1000

1. 按照用户指南中的说明安装硬件。请参阅：

<http://www.sun.com/products-n-solutions/hardware/docs/pdf/816-2450-11.pdf>

2. 从光盘安装以下软件包。

SUNWcrypm、SUNWcrypu、SUNWcrysus、SUNWdcar、SUNWcrypr、SUNWcrysl、SUNWdcamn、SUNWdcav

3. 安装以下修补程序。（您可从 <http://sunsolve.sun.com> 获取这些程序）

110383-01、108528-05、112438-01

4. 确保您拥有 `pk12util` 和 `modutil` 工具。

这些工具安装在 `/usr/sfw/bin` 目录下面。如果工具不位于 `/usr/sfw/bin` 目录中，则需要手动从 Sun Java System 分发媒体中添加 SUNWt1su 数据包：  
`Solaris_[sparc/x86]/Product/shared_components/`

5. 创建插槽文件：

```
vi /etc/opt/SUNWconn/crypto/slots
```

然后将 `"crypta@sra"` 作为第一行而且是唯一一行放在文件中。

6. 创建和设置区域。

- a. 以根用户身份登录。

- b. 键入以下命令：

```
cd /opt/SUNWconn/bin/secadm
```

```
secadm> create realm=sra
```

已成功创建区域 `sra`。

7. 创建一个用户：

- a. 键入并回应以下命令：

```
secadm> set realm=sra
```

```
secadm{srap}> su
```

```
secadm{root@sra}>create user=crypta
```

初始口令：

确认口令：

已成功创建用户 `crypta`。

8. 以您创建的用户身份登录。

```
secadm{root@sra}> login user=crypta
```

口令：

```
secadm{crypta@sra}> show key
```

不存在此用户的密钥。

**9. 载入 Sun Crypto 模块。**

环境变量 `LD_LIBRARY_PATH` 必须指向 `/usr/lib/mps/secv1/`

类型:

```
modutil -dbdir /etc/opt/SUNWps/cert/default -add "Sun Crypto Module"
-libfile /opt/SUNWconn/crypto/lib/libpkcs11.so
```

使用以下命令验证是否已载入此模块:

```
modutil -list -dbdir /etc/opt/SUNWps/cert /default
```

**10. 将网关证书和密钥导出到 “Sun Crypto 模块” 中。**

环境变量 `LD_LIBRARY_PATH` 必须指向 `/usr/lib/mps/secv1/`

类型:

```
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"
```

现在, 运行显示密钥命令:

```
secadm{crypta@sra}> show key
```

应该可以看到此用户的两个密钥。

**11. 更改 `/etc/opt/SUNWps/cert/default/.nickname` 文件中的昵称。**

```
vi /etc/opt/SUNWps/cert/default/.nickname
```

用 `crypta@sra:server-cert` 替换 `server-cert`

**12. 启用加速密码。**

请参阅第 263 页的 “启用 SSL 密码选择”

SUN CA1000 可加速 RSA 功能, 但只支持对 DES 和 3DES 密码的加速。

**13. 修改 `/etc/opt/SUNWps/platform.conf.gateway-profile-name` 以启用加速器:**

```
gateway.enable.accelerator=true
```

**14. 从终端窗口重新启动网关:**

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

---

**注意** 网关会绑定到端口（在配置文件中被称为 `https` 端口）上的一个普通 `ServerSocket`（非 SSL）。

不对收到的客户机通信进行任何 SSL 加密或解密操作。此操作会由加速器来执行。

PDC 在此模式下不起作用。

---

## Sun Crypto Accelerator 4000

Sun™ Crypto Accelerator 4000 板是一个基于以太网的千兆网卡，它支持 Sun 服务器上 IPsec 和 SSL（对称和不对称）的加密硬件加速。

除了作为用于未加密网络通信的标准千兆以太网网卡之外，该板还包含加密硬件以支持加密 IPsec 通信实现更高的通过量。

Crypto Accelerator 4000 板可同时在硬件和软件上加速加密算法。它也支持密码 DES 和 3DES 的整体加密。

## 启用 Crypto Accelerator 4000

确保已安装了 SRA，并安装了网关服务器证书（自签名或由任一 CA 所签发）。以下清单有助于您在安装“SSL 加速器”之前熟悉所需信息。

表 13-1 列出了 Crypto Accelerator 4000 的参数和相应值。

**表 13-2** Crypto Accelerator 4000 安装清单

参数	值
Secure Remote Access 安装基本目录	/opt
SRA 实例	default
SRA 证书数据库路径	/etc/opt/SUNWps/cert/default
SRA 服务器证书昵称	server-cert
CA4000 keystore	srap
CA4000 keystore 用户	crypta

---

## 配置 Crypto Accelerator 4000

### ► 配置 Crypto Accelerator 4000

1. 按用户指南中的说明安装硬件和软件包。请参阅：

<http://www.sun.com/products-n-solutions/hardware/docs/pdf/816-2450-11.pdf>

2. 安装以下修补程序。（您可从 <http://sunsolve.sun.com> 处获取这些程序）：  
114795

3. 确保您拥有 `certutil`、`pk12util` 和 `modutil` 工具。

这些工具安装在 `/usr/sfw/bin` 目录下面

如果工具不位于 `/usr/sfw/bin` 目录中，则需要

手动从 Sun Java System 分发媒体中添加 SUNWtisu 数据包：  
`Solaris_[sparc/x86]/Product/shared_components/`

4. 初始化该板。

运行 `/opt/SUNWconn/bin/vcadm` 工具初始化密码板，并设置下列值。

初始安全主管名：`sec_officer`

Keystore 名称：`sra-keystore`

以 FIPS 140-2 模式下运行：否

5. 创建一个用户。

```
vcaadm{vca0@localhost, sec_officer}> create user
```

新用户名 :crypta

输入新的用户口令:

确认口令:

已成功创建用户 crypta。

6. 将令牌映射到 key store。

```
vi /opt/SUNWconn/cryptov2/tokens
```

然后, 将 sra-keystore 追加到文件中。

7. 启用整体加密。

```
touch /opt/SUNWconn/cryptov2/sslreg
```

8. 载入 Sun Crypto 模块。

环境变量 LD\_LIBRARY\_PATH 必须指向 /usr/lib/mps/secv1/

类型:

```
modutil -dbdir /etc/opt/SUNWps/cert/default -add "Sun Crypto Module"
-libfile /opt/SUNWconn/cryptov2/lib/libvpkcs11.so
```

您可使用以下命令检验是否已载入此模块:

```
modutil -list -dbdir /etc/opt/SUNWps/cert /default
```

9. 将网关证书和密钥导出到 “Sun Crypto 模块” 中。

环境变量 LD\_LIBRARY\_PATH 必须指向 /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"
```

您可使用以下命令检验是否已经导出密钥:

```
certutil -K -h "sra-keystore" -d /etc/opt/SUNWps/cert/default
```

10. 更改 /etc/opt/SUNWps//cert/default/.nickname 文件中的昵称:

```
vi /etc/opt/SUNWps/cert/default/.nickname
```

用 sra-keystore:server-cert 替换 server-cert

**11. 启用加速密码。**

请参阅第 263 页的“启用 SSL 密码选择”

**12. 从终端窗口重新启动网关：**

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

网关会提示您输入 keystore 口令。

为 "sra-keystore":crypta:crypta-password 输入口令或 Pin

---

**注意** 网关会绑定到端口（在配置文件中被称为 https 端口）上的一个普通 ServerSocket（非 SSL）。

不对收到的客户机通信进行任何 SSL 加密或解密操作。此操作会由加速器来执行。

PDC 在此模式下不起作用。

---

## 外部 SSL 设备和代理加速器

外部 SSL 设备可在开放模式下于 Sun Java System Portal Server Secure Remote Access (SRA) 前端运行。它在客户机和 SRA 之间提供了 SSL 链接。

### 启用外部 SSL 设备加速器

确保已安装了 SRA，并且网关在安全模式下（HTTPS 模式）运行：

网关 >> 启用 HTTPS 连接

网关 >> HTTP 端口：880

表 13-3 列出了 SSL 设备和代理加速器的参数及相应的值。

**表 13-3** 外部 SSL 设备和代理加速器清单

参数	值
SRA 实例	default
网关模式	https

**表 13-3** 外部 SSL 设备和代理加速器清单

参数	值
网关端口	880
外部设备 / 代理端口	443

## 配置外部 SSL 设备加速器

### ► 配置外部 SSL 设备加速器

1. 按用户指南中的说明安装硬件和软件包。
2. 安装必需的修补程序（如果有）。
3. 通过在 `platform.conf` 文件中输入值，启用“SSL 设备 / 代理”支持：

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

```
gateway.enable.accelerator=true
```

如果外部设备 / 代理主机名与网关主机名不同：

```
gateway.enable.customurl=true
```

```
gateway.httpsurl=external-device.domain.subdomain/proxy-URL
```

4. 可以两种方式配置网关通知：
  - 当 Identity Server 可在端口 880 连接网关计算机时（会话通知将为 http 形式），在 `platform.conf` 文件中输入值。

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

```
gateway.protocol=http
```

```
gateway.port=880
```

- 当 Identity Server 可在端口 443 连接外部设备 / 代理时（会话通知将为 HTTPS 形式），在 `platform.conf` 文件中输入值。

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

```
gateway.host=External Device/Proxy Host Name
```

```
gateway.protocol=https
```

```
gateway.port=443
```

5. 确保 SSL 设备 / 代理就绪并处于运行状态，而且经过配置以便将通信引向网关端口。

6. 从终端窗口重新启动网关：

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

## 日志文件

以下日志文件位于默认目录 `/var/opt/SUNWps/debug` 中，并且包含调试信息及其他类型的信息。

**表 A-1** 信息文件和调试文件

文件名	内容
以下日志文件由默认目录 <code>/etc/opt/SUNWam/config/ file</code> 下的 <code>AMConfig-instance-name.properties</code> 文件中的调试参数控制：	
<code>amconsole</code>	Netfile、Netlet 及网关管理文件
<code>srapNetFile</code>	NetFile 信息文件
<code>srapNetlet</code>	Netlet 信息文件
以下日志文件由默认目录 <code>/etc/opt/SUNWps</code> 下的 <code>platform.conf.gateway-profile-name</code> 文件中的调试参数 <code>gateway.debug</code> 控制：	
<code>srapGateway.gateway-profile-name</code>	网关信息
<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>	
<code>rwproxy.log.rewriter-proxy-instance-name</code>	重写器代理的开始时间和停止时间
<code>nlproxy.log.netlet-proxy-instance-name</code>	Netlet 代理的开始时间和停止时间
<code>gateway.log.gateway.instance.name</code>	网关的开始时间和停止时间
以下日志文件由默认目录 <code>/var/opt/SUNWam/config/ file</code> 下的 <code>AMConfig-instance-name.properties</code> 文件中的调试参数控制。有关详细信息，请参阅第 133 页的“使用调试日志排除故障”。	

**表 A-1** 信息文件和调试文件

文件名	内容
RuleSetInfo	本文件记录重写时已使用的所有规则集。
Original Pages	包含页 <b>URI</b> 、解析 <b>URI</b> （如果它与页 <b>URI</b> 不同）、内容 <b>MIME</b> 、已应用于此页的规则集、分析器 <b>MIME</b> ，以及原始内容。 与分析有关的特定错误 / 警告 / 消息也出现在本文件中。 在消息模式下，会记录全部内容；在警告和错误模式下，只记录重写期间出现的异常。
Rewritten Pages	包含页 <b>URI</b> 、解析 <b>URI</b> （如果它与页 <b>URI</b> 不同）、内容 <b>MIME</b> 、已应用于此页的规则集、分析器 <b>MIME</b> ，以及重写后的内容。 当将调试模式设置为消息时，将会填写本文件。
Unaffected Pages	包含未经修改的页列表。
URLInfo Pages	本文件包含已找到并经过转换的 <b>URL</b> 。该文件会记录内容仍与原始数据相同的所有页的详细信息。 所记录的详细信息有：页 <b>URI</b> 、 <b>MIME</b> 及编码数据、重写时所用的规则集 <b>ID</b> ，以及分析器 <b>MIME</b> 。

## 配置属性

本附录介绍可通过每个 Secure Remote Access 组件的“服务配置”中的 Identity Server 管理控制台为 Portal Server Secure Remote Access 配置的属性：

- [访问列表服务](#)
- [网关服务](#)
- [NetFile 服务](#)
- [Netlet 服务](#)
- [Proxylet 服务](#)

## 访问列表服务

表 B-1 列出“访问列表”服务属性。

**表 B-1** 访问列表服务属性

属性	默认值	说明
拒绝的 URL		最终用户不能通过网关访问的 URL 列表。
允许的 URL	*	最终用户可通过网关访问的 URL 列表。
单点登录禁用的主机		禁用一系列主机的单点登录。
在每一会话中启用单点登录		启用会话的单点登录。
允许的验证级别	*	表示对验证的信任度。使用星号以允许所有验证级别。有关验证级别的信息，请参阅《 <i>Identity Server 管理指南</i> 》。

# 网关服务

单击网关服务时，右侧窗格显示用于创建新配置文件的按钮和已创建的所有网关配置文件的列表。

如果单击“新建”，下一个窗格要求输入新网关配置文件名。可选择使用默认模板或者使用先前创建的网关配置文件作为模板。

如果单击所列出的网关配置文件名之一，将提供一个选项卡列表。分别是：

- [核心](#)
- [代理](#)
- [安全](#)
- [重写器](#)
- [日志](#)

## 核心

表 B-2 列出网关服务核心属性。

**表 B-2** 网关服务核心属性

属性	默认值	说明
启用 HTTPS 连接		启用 HTTPS 连接。
HTTPS 端口	443	指定 HTTPS 端口。
启用 HTTP 连接	*	启用 HTTP 连接。
HTTP 端口	80	指定 HTTP 端口。
启用重写器代理	*	实现网关与内部网之间的安全 HTTP 通信。“重写器”代理和网关使用相同的网关配置文件。
重写器代理列表		“重写器”代理列表。若“重写器”代理有多个实例，采用 <i>host-name:port</i> 形式输入每个代理的详细信息
启用 Netlet	选中	实现 TCP/IP（如 Telnet 和 SMTP）、HTTP 应用程序及固定端口应用程序的安全性。
启用 Proxylet	选中	启用客户机上的 Proxylet 下载。
启用 Netlet 代理		通过将安全通道从客户机经网关扩展到驻留在内部网中的 Netlet 代理，增强网关和内部网之间 Netlet 通信的安全性。如果不需要与 Portal Server 一同使用应用程序，请禁用此功能。

表 B-2 网关服务核心属性

属性	默认值	说明
Netlet 代理主机		以 host hostname:port 格式列出 Netlet 代理主机
启用 Cookie 管理		跟踪和管理允许用户访问的所有网站的用户会话。 (不适用于 Portal Server 用来跟踪 Portal Server 用户会话的 cookie)。
启用 HTTP 基本验证	选中	保存用户名和口令, 这样用户在重新访问受 BASIC 保护的网站时, 就无需重新输入其身份验证信息。
启用持久的 HTTP 连接	选中	在网关启用 HTTP 持久性连接, 以防套接字对网页中的每个对象 (如图像和样式表) 均打开。
每个持久性连接的最大请求数量	10	指定每个持久性连接的请求数量。
持久套接字连接超时	50	指定套接字关闭之前需要的时间长短。
Grace 超时, 以解决周转时间	20	指定浏览器在发送请求之后该请求到达网关需要的宽限时间, 以及网关发送响应和浏览器实际接收到响应之间的时间。
用户会话 Cookie 转发目标 URL		可使 servlet 和 CGI 接收 Portal Server 的 cookie 并使用 API 来标识用户。
最大连接队列长度	50	指定网关可接受的最大并发连接数量。
网关超时 (毫秒)	120000	指定网关与浏览器断开连接之前的时间间隔 (以毫秒为单位)。
线程组合容量最大值	200	指定可在网关线程池中预先创建的最大线程数量。
高速缓存套接字超时	200000	指定网关与 Portal Server 断开连接之前的时间间隔 (以毫秒为单位)。

表 B-2 网关服务核心属性

属性	默认值	说明
Portal Server		以格式 <code>http://portal server name:port -number</code> 指定 Portal Server。网关试图联系每个以循环方式列出的 Portal Server 来为请求提供服务。
服务器重试间隔（分）	2	指定在 Portal Server、“重写器”代理或 Netlet 代理不可用（如，崩溃或死机）之后，尝试启动它们的请求之间的时间间隔。
存储外部服务器 Cookie		允许网关存储和管理通过网关访问的任何第三方应用程序或服务器的 cookie。
从 URL 获取会话信息		无论支持 cookie 与否，均将会话信息作为 URL 的一部分进行编码。网关验证时使用在 URL 中找到的会话信息，而非客户机浏览器发出的会话 cookie。
把 Cookie 标记为安全		将 cookie 标记为安全。必须启用“启用 Cookie 管理”选项。

## 代理

表 B-3 列出网关服务代理属性。

表 B-3 网关服务代理属性

属性	默认值	说明
使用代理		启用网络代理的应用。
使用 Webproxy URL		列出网关只能通过“域和子域代理”列表中列出的网络代理进行联系的 URL（即使禁用“使用代理”选项）。
不可使用 Webproxy URL		列出网关可以直接连接到的 URL。
域和子域代理	iportal.com sun.com	指定用于联系特定域中的特定子域的代理。
代理口令列表		如果代理服务器需要验证才能访问某些或所有站点，须为网关指定验证指定代理服务器所需的用户名和口令。

**表 B-3** 网关服务代理属性

属性	默认值	说明
启用自动代理配置支持		指定“域和子域的代理”字段中的信息将被忽略。
自动代理配置文件位置		指定要用于 PAC 支持的文件的位置。
启用通过网络代理开通 Netlet 通道		将安全通道从客户机经由网关扩展到驻留在内部网中的网络代理。

## 安全

表 B-4 列出网关服务安全属性。

**表 B-4** 网关服务安全属性

属性	默认值	说明
没有已验证的 URL	/portal/desktop/images /amserver/login_images /portal/desktop/css /amserver/jss /amconsole/console/css /portal/searchadmin/console/js /amconsole/console/js /amserver/css	指定不需要任何验证的 URL，如包含图像的目录。
已启用证书的网关主机		列出启用证书的网关主机。
允许 40 位加密		允许 40 位（弱）“加密套接字层”(SSL) 连接。如果不选择此选项，则只支持 128 位连接。
启用 SSL 2.0 版本	选中	启用 SSL 2.0 版本。 禁用 SSL 2.0 意味着仅支持旧版 SSL 2.0 的浏览器将无法进行 SRA 验证。如此可提高安全级别。
启用 SSL 密码选择		启用 SSL 密码选择。您可选择支持所有预封装的密码，或者可以单独选择所需的密码。您可以为每个网关实例指定特定的 SSL 密码。

**表 B-4** 网关服务安全属性

属性	默认值	说明
SSL2 密码		列出可以选择的 SSL 2 版密码。
SSL3 密码		列出可以选择的 SSL 3.0 版密码。
TLS 密码		列出 TLS 密码。
启用 SSL 3.0 版本	选中	启用 SSL 3.0 版本。 禁用 SSL 3.0 表示仅支持 SSL 3.0 版本的浏览器将无法进行 SRA 验证。这将确保更高级别的安全性。
启用空密码		启用空密码。
信任的 SSL 域		列出信任的 SSL 域。

## 重写器

“重写器”选项卡有两个子部分：

- [基本](#)
- [高级](#)

### 基本

[表 B-5](#) 列出网关服务“重写器”基本属性。

**表 B-5** 网关服务重写器属性 - 基本

属性	默认值	说明
启用全部 URI 重写		指定重写任何 URL，而不检查“域和子域代理”列表中的条目。

表 B-5 网关服务重写器属性 - 基本

属性	默认值	说明
将 URI 映射至规则集	<pre> *://*.iportal.com*/portal/* default_gateway_ruleset */portal/NetFileOpenFileServlet* null_ruleset * generic_ruleset REPLACE_WITH_IPLANET_MAIL_SERVER_NAME iplanet_mail_ruleset REPLACE_WITH_EXCHANGE_SERVER_NAME exchange_2000sp3_owa_ruleset *://*.iportal.com*/amconsole/* default_gateway_ruleset REPLACE_WITH_INOTES_SERVER_NAME inotes_ruleset http*://*/portal/NetFileController* null_ruleset </pre>	使用“将 URI 映射至规则集”列表将域和规则集相关联。规则集在 Identity Server 管理控制台中的“Portal Server 配置”下创建。
将分析器映射至 MIME 类型	<pre> JAVASCRIPT=application/x-javascript XML=text/xml HTML=text/html;text/html;text/x-component;text/wml;text/vnd.wap.wml CSS=text/css </pre>	使新 MIME 类型和 HTML、JAVASCRIPT、CSS 或 XML 关联。用分号或逗号分隔多个条目。
禁止重写的 URI		列出禁止重写的 URI。注意：即使此 href 规则包括在规则集中，在该列表中添加 #* 也会允许重写 URI。
默认域		将主机名解析为默认域和子域。它在安装期间指定

## 高级

表 B-6 列出网关服务“重写器”高级属性。

**表 B-6** 网关服务重写器属性 - 高级

属性	默认值	说明
启用 MIME 推测		未发送 MIME 时, 启用 MIME 推测。必须将数据添加到“将分析器映射至 URI”列表框中。
将分析器映射至 URI 映射		将分析器映射到 URI。多个 URI 以分号进行分隔。 例如, HTML=*.html; *.htm;*Servlet 表示使用“重写器”来重写具有 html、htm 或 Servlet 扩展名的任何页的内容。
启用屏蔽		允许“重写器”重写 URI 以便使人们看不到页的“内部网 URL”。
屏蔽的种子字符串		指定用于屏蔽 URI 的种子字符串。它是由屏蔽算法生成的随机字符串。
禁止屏蔽的 URI		指定不进行屏蔽的 Internet URI。应用程序 (如 applet) 需要 Internet URI 时, 使用此项。 例如, 如果添加 */Applet/Param* 到列表框中, 则当内容 URI http://abc.com/Applet/Param1.html 在规则集的规则中匹配时, 将不会屏蔽此 URI。
使网关协议与原始 URI 协议相同		使“重写器”能以一致的协议访问 HTML 内容中的引用资源。 这样做只适用于静态 URI, 不适用于 Javascript 中生成的动态 URI。

## 日志

表 B-7 列出网关服务日志属性。

**表 B-7** 网关服务日志属性

属性	默认值	说明
启用日志		启用日志。
启用每会话日志		启用捕获最基本的日志信息, 如“客户机地址”、“请求类型”以及“目的主机”。

表 B-7 网关服务日志属性

属性	默认值	说明
启用详细的每会话日志		启用捕获详细日志信息，如“客户机”、“请求类型”、“目的主机”、“请求的类型”、“客户请求的 URL”、“客户发布数据大小”、“会话 ID”、“应答结果代码”和“完成应答的大小”。 注意：必须启用“启用每会话日志”。
启用 Netlet 日志		启用日志的情况下指定。假若如此，则捕获下列信息：开始时间、源、地址、源端口、服务器地址、服务器端口、停止时间以及状态（开始或停止）

## NetFile 服务

单击“NetFile 服务”时，右侧窗格显示选项卡。分别是：

- [主机](#)
- [权限](#)
- [视图](#)
- [操作](#)
- [常规](#)

### 主机

“主机”选项卡有两个子部分：

- [配置](#)
- [访问](#)

## 配置

表 B-8 列出 NetFile 主机配置属性。

**表 B-8** NetFile 服务主机配置属性

属性	默认值	说明
OS 字符集	Unicode(UTF-8)	指定与主机进行通信时用作默认编码的字符集。
主机侦测顺序	WIN、NETWARE、FTP、NFS	指定主机侦测顺序。
通用主机		指定所有远程 NetFile 用户均可通过 NetFile 使用的主机。
默认域		指定 NetFile 联络允许的主机时需要使用的默认域。
默认 Windows 域 / 工作组		指定用户访问 Windows 主机时选择的默认 Windows 域或工作组。
默认 WINS/DNS 服务器		指定 NetFile 用于访问 windows 主机的 WINS/DNS 服务器。

## 访问

表 B-9 列出 NetFile 服务主机访问属性。

**表 B-9** NetFile 服务主机访问属性

属性	默认值	说明
允许访问 Windows 主机	选中	允许访问 windows 主机。
允许访问 FTP 主机	选中	允许访问 FTP 主机。
允许访问 NFS 主机	选中	允许访问 NFS 主机。
允许访问 Netware 主机	选中	允许访问 Netware 主机。
允许的主机	*	指定用户可通过 NetFile 访问的主机。
拒绝的主机		指定用户不能通过 NetFile 访问的主机。

## 权限

如果您在用户开始使用 NetFile 后禁用这些选项，则仅当用户从 NetFile 中注销并重新登录时，此更改才会生效。

表 B-10 列出 NetFile 服务权限属性。

表 B-10 NetFile 服务权限属性

属性	默认值	说明
允许文件更名	选中	允许用户重命名文件。
允许删除文件 / 文件夹	选中	允许用户删除文件和文件夹。
允许文件上载	选中	允许用户上传文件。
允许文件 / 文件夹下载	选中	允许用户下载文件和文件夹。
允许文件搜索	选中	允许用户进行搜索。
允许文件邮件	选中	允许邮寄文件。
允许文件压缩	选中	允许文件压缩。
允许改变用户 Id	选中	允许用户使用不同的 ID。
允许改变 Windows 域	选中	允许用户更改 windows 域。

## 视图

表 B-11 列出 NetFile 服务视图属性。

表 B-11 NetFile 服务视图属性

属性	默认值	说明
窗口大小	700 400	在用户桌面上以像素为单位指定 NetFile 窗口的大小。如果输入了无效值，NetFile 会使用默认值。
Window 位置	100 50	指定 NetFile 窗口在用户桌面上的显示位置。如果输入了无效值，NetFile 会使用默认值。

## 操作

“操作”选项卡有下列子部分：

- 通信
- 搜索
- 压缩

## 通信

表 B-12 列出 NetFile 服务操作通信属性。

**表 B-12** NetFile 服务操作 - 通信属性

属性	默认值	说明
临时目录位置	/tmp	<p>指定各种 NetFile 文件操作的临时目录。</p> <p>确保运行 Web 服务器的 ID（如 nobody 或 noaccess）对所指定的目录具有 rwx 权限。还要确保此 ID 对于到所需临时目录的完整路径具有 rx 权限。</p> <p>最好为 NetFile 创建一个单独的临时目录。如果所指定的临时目录是 Portal Server 的所有模块公用的，磁盘空间可能很快就会用完。如果临时目录没有空间，NetFile 将无法工作。</p>
文件上传限制 (MB)	5	<p>指定可以上传的最大文件大小。如果输入无效值，NetFile 会将其重置为默认值。确保键入的是整数。</p> <p>可为不同用户指定不同的文件上传大小限制。</p>

## 搜索

表 B-13 列出 NetFile 服务操作搜索属性。

**表 B-13** NetFile 服务操作 - 搜索属性

属性	默认值	说明
搜索目录限制	100	<p>指定在单次搜索操作中将要搜索的最大目录数。</p>

## 压缩

表 B-14 列出 NetFile 服务操作压缩属性。

**表 B-14** NetFile 服务操作 - 压缩属性

属性	默认值	说明
默认压缩类型	Zip	指定 Zip 或 Gzip 压缩类型。
默认压缩级别	6	指定压缩级别，1 和 9 之间的一个数字。

## 常规

表 B-15 列出 NetFile 服务常规属性。

**表 B-15** NetFile 服务 - 常规属性

属性	默认值	说明
MIME 类型配置文件定位	/opt/S1PS62/SUNWps/samples/config/netfile	指定要发送到客户机浏览器的响应内容类型。

# Netlet 服务

表 B-16 列出 Netlet 服务属性。

**表 B-16** Netlet 服务属性

属性	默认值	说明
Netlet 规则		选择添加或删除规则。
如果添加规则，下列九个属性是必需的：		
-- 规则名称		为规则指定唯一名称。
-- 加密密码		指定所需密码。
--URL		指定要调用的应用程序的 URL。
-- 下载 Applet		需要下载 applet 时指定。如果使用 applet，相关编辑框中的语法为： <i>local-port:server-host:server-port</i>
-- 扩展会话		确保与该规则相对应的 Netlet 会话运行期间，延长 Portal Server 会话时间。

表 B-16 Netlet 服务属性

属性	默认值	说明
-- 将本地端口映射至目的服务器端口		指定本地端口、目标主机和目标端口。输入这些值（在此表的后三行中）之后，单击添加，使其出现在列表中。
-- 本地端口		指定 Netlet 进行监听时所在的本地端口。对于 FTP 规则，本地端口值必须是 30021。
-- 目的主机		静态规则包含用于 Netlet 连接的目的机器的主机名。 动态规则包含单词 "TARGET"。
-- 目的端口		指定目的主机上的端口。
默认本地 VM 密码		为 Netlet 规则指定默认密码。这在使用其中未包括密码的现有规则时非常有用。
默认 Java Plugin 密码		为 Netlet 规则指定默认密码。这在使用其中未包括密码的现有规则时非常有用。
默认回环端口	58000	当通过 Netlet 下载 applet 时，指定要使用的客户机端口。在 Netlet 规则中，可以覆盖默认值。
连接时重新验证		确保用户在每次需要建立 Netlet 连接时，均输入 Netlet 口令。
显示连接时弹出警告	选中	当用户通过 Netlet 运行应用程序或是有入侵者企图通过监听端口访问桌面时，显示消息。
在端口警告对话框中显示复选框	选中	当 Netlet 试图连接到用户的标准“门户桌面”上的目的主机时，为用户提供取消“弹出警告对话框”的选项。
保活间隔（分钟）	0	如果客户机正通过网络代理连接到网关，则由于代理超时将断开空闲的 Netlet 连接。为防止出现此情况，请为此参数指定一个小于代理超时值的值。
端口注销时中止 Netlet	选中	用户从 Portal Server 注销时，确保所有连接均终止。
Netlet 访问规则	*	为某些组织、角色或用户定义对特定 Netlet 规则的访问。
Netlet 拒绝规则		为某些组织、角色或用户定义对特定 Netlet 规则的访问。
允许的主机	*	为某些组织、角色或用户定义对特定主机的访问。
拒绝的主机		拒绝对组织内特定主机的访问。

# Proxylet 服务

表 B-17 列出 Proxylet 服务属性。

**表 B-17** Proxylet 服务属性

属性	默认值	说明
自动下载 Proxylet Applet	127.0.0.1	如果选中复选框，用户登录时 Proxylet 会被下载到客户机上。
默认 Proxylet Applet 绑定 IP	127.0.0.1	驻留 Proxylet Applet 的 IP 地址。
默认 Proxylet Applet 端口	58080	这是 Proxylet 进行监听的端口。



## 国家代码

下表列出了需在证书管理期间指定的两个字母的国家代码。

**表 C-1** 两字母国家代码 (第 1 页, 共 10 页)

ad	安道尔公国
ae	阿拉伯联合酋长国
af	阿富汗伊斯兰共和国
ag	安提瓜和巴布达
ai	安圭拉
al	阿尔巴尼亚
am	亚美尼亚
an	荷属安的列斯群岛
ao	安哥拉
aq	南极洲
ar	阿根廷
arpa	老式阿帕网
as	美属萨摩亚
at	奥地利
au	澳大利亚
aw	阿鲁巴
az	阿塞拜疆
ba	波斯尼亚 - 黑塞哥维纳

**表 C-1** 两字母国家代码 (第2页, 共10页)

bb	巴巴多斯
bd	孟加拉国
be	比利时
bf	布基纳法索
bg	保加利亚
bh	巴林
bi	布隆迪
bj	贝宁
bm	百慕大
bn	文莱达鲁萨兰国
bo	玻利维亚
br	巴西
bs	巴哈马
bt	不丹
bv	博维特岛
bw	博茨瓦纳
by	白俄罗斯
bz	伯利兹
ca	加拿大
cc	科科斯 (基灵) 群岛
cf	中非共和国
cd	刚果民主共和国
cg	刚果
ch	瑞士
ci	象牙海岸
ck	库克群岛
cl	智利

**表 C-1** 两字母国家代码 (第3页, 共10页)

cm	喀麦隆
cn	中国
co	哥伦比亚
com	商业
cr	哥斯达黎加
cs	前捷克斯洛伐克
cu	古巴
cv	佛得角
cx	圣诞岛
cy	塞浦路斯
cz	捷克共和国
de	德国
dj	吉布提
dk	丹麦
dm	多米尼加
do	多米尼加共和国
dz	阿尔及利亚
ec	厄瓜多尔
edu	教育
ee	爱沙尼亚
eg	埃及
eh	西撒哈拉
er	厄立特里亚
es	西班牙
et	埃塞俄比亚
fi	芬兰
fj	斐济

**表 C-1** 两字母国家代码 (第4页, 共10页)

fk	福克兰群岛
fm	密克罗尼西亚
fo	法罗群岛
fr	法国
fx	法国 (欧洲领土)
ga	加蓬
gb	大不列颠
gd	格林纳达
ge	格鲁吉亚
gf	法属圭亚那
gh	加纳
gi	直布罗陀
gl	格陵兰
gm	冈比亚
gn	几内亚
gov	美国政府
gp	瓜德罗普 (法属)
gq	赤道几内亚
gr	希腊
gs	南乔治亚和南桑德韦奇群岛
gt	危地马拉
gu	关岛 (美属)
gw	几内亚比绍
gy	圭亚那
hk	中国香港特别行政区
hm	赫德岛和麦克唐纳群岛
hn	洪都拉斯

**表 C-1** 两字母国家代码 (第5页, 共10页)

hr	克罗地亚
ht	海地
hu	匈牙利
id	印度尼西亚
ie	爱尔兰
il	以色列
in	印度
int	国际
io	英属印度洋地区
iq	伊拉克
ir	伊朗
is	冰岛
it	意大利
jm	牙买加
jo	约旦
jp	日本
ke	肯尼亚
kg	吉尔吉斯共和国 (吉尔吉斯斯坦)
kh	柬埔寨王国
ki	基里巴斯
km	科摩罗
kn	圣基茨和尼维斯安圭拉
kp	朝鲜
kr	韩国
kw	科威特
ky	开曼群岛
kz	哈萨克斯坦

**表 C-1** 两字母国家代码 (第6页, 共10页)

la	老挝
lb	黎巴嫩
lc	圣卢西亚
li	列支敦士登
lk	斯里兰卡
lr	利比里亚
ls	莱索托
lt	立陶宛
lu	卢森堡
lv	拉脱维亚
ly	利比亚
ma	摩洛哥
mc	摩纳哥
md	摩尔达维亚
mg	马达加斯加
mh	马绍尔群岛
mil	美国军方
mk	马其顿
ml	马里
mm	缅甸
mn	蒙古
mo	中国澳门特别行政区
mp	北马里亚纳群岛
mq	马提尼克 (法属)
mr	毛里塔尼亚
ms	蒙特塞拉特
mt	马耳他

**表 C-1** 两字母国家代码 (第7页, 共10页)

mu	毛里求斯
mv	马尔代夫
mw	马拉维
mx	墨西哥
my	马来西亚
mz	莫桑比克
na	纳米比亚
nato	北约 (1996年清除了此项 - 参见 <a href="http://hq.nato.int">hq.nato.int</a> )
nc	新喀里多尼亚 (法属)
ne	尼日尔
net	网络
nf	诺福克岛
ng	尼日利亚
ni	尼加拉瓜
nl	荷兰
no	挪威
np	尼泊尔
nr	瑙鲁
nt	中立区
nu	纽埃
nz	新西兰
om	阿曼
org	非盈利组织 (原文)
pa	巴拿马
pe	秘鲁
pf	玻利尼西亚 (法属)
pg	巴布亚新几内亚

**表 C-1** 两字母国家代码 (第8页, 共10页)

ph	菲律宾
pk	巴基斯坦
pl	波兰
pm	圣皮埃尔和密克隆
pn	皮特克恩岛
pr	波多黎各
pt	葡萄牙
pw	帕劳
py	巴拉圭
qa	卡塔尔
re	留尼旺 (法属)
ro	罗马尼亚
ru	俄罗斯联邦
rw	卢旺达
sa	沙特阿拉伯
sb	所罗门群岛
sc	塞舌尔
sd	苏丹
se	瑞典
sg	新加坡
sh	圣赫勒拿
si	斯洛文尼亚
sj	斯瓦尔巴特和扬马延群岛
sk	斯洛伐克共和国
sl	塞拉利昂
sm	圣马力诺
sn	塞内加尔

**表 C-1** 两字母国家代码 (第9页, 共10页)

so	索马里
sr	苏里南
st	圣多美和普林西比
su	前苏联
sv	萨尔瓦多
sy	叙利亚
sz	斯威士兰
tc	特克斯和凯科斯群岛
td	乍得
tf	法属南部领土
tg	多哥
th	泰国
tj	塔吉克斯坦
tk	托克劳
tm	土库曼斯坦
tn	突尼斯
to	汤加
tp	东帝汶
tr	土耳其
tt	特立尼达和多巴哥
tv	图瓦卢
tw	中国台湾
tz	坦桑尼亚
ua	乌克兰
ug	乌干达
uk	英国
um	美国边远小岛

**表 C-1** 两字母国家代码 (第10页, 共10页)

us	美国
uy	乌拉圭
uz	乌兹别克斯坦
va	圣座 (梵蒂冈城国)
vc	圣文森特和格林纳丁斯
ve	委内瑞拉
vg	维尔京群岛 (英属)
vi	维尔京群岛 (美属)
vn	越南
vu	瓦努阿图
wf	瓦利斯和富图纳群岛
ws	萨摩亚
ye	也门
yt	马约特
yu	南斯拉夫
za	南非
zm	赞比亚
zr	扎伊尔
zw	津巴布韦

# 术语表

有关本文档集中所使用术语的完整列表，请参阅 《Java Enterprise System Glossary》 (<http://docs.sun.com/doc/816-6873>)。



## A

applet 182  
  下载 196  
安全模式 29

## B

保活间隔  
  设置 313  
报头  
  HTTP 73

## C

certadmin 脚本 214  
chroot 47  
Citrix  
  html 文件 201  
cookie  
  标记为安全 253  
  存储外部 251  
  启用 241  
层叠样式表  
  重写器中 123  
超时  
  高速缓存套接字 249

宽限期 245  
套接字连接 244  
网关 248

### 重写器

6.x 与 3.0 规则集映射 173  
编写规则 97  
创建 URI 到规则集映射列表 270  
创建 URI 映射分析器列表 130  
创建禁止重写的 URI 列表 126  
工作示例 136  
规则集 DTD 92  
规则中的模式匹配 104  
HTML 规则 99  
和域和子域代理列表 61  
JavaScript 规则 105  
  配置 124  
  启用屏蔽 131  
  启用全部 URL 重写 269  
  示例 136  
  实例研究 168  
  使用调试日志 133  
  使用通配符 126  
URLScraper 90  
XML 规则 120  
  一致的协议 278  
  重写所有 URL 124

### 重写器代理

创建 70  
启用 72  
优点 70

## D

- 重新启动 72
- 重写器服务 32
- 重新启动 54
  - Netlet 代理 69
  - 网关 54
  - 重写器代理 72
- 重新验证
  - 连接 311
- 冲突解决 35
- 处理顺序
  - 代理 59
- 创建
  - 重写器代理 70
  - 非验证 URL 列表 260
  - hostproxy 56
  - 禁止屏蔽的 URI 列表 277
  - 禁止重写的 URI 列表 126, 274
  - portal server 列表 250
  - URI 到规则集映射列表 270
  - URI 映射分析器列表 130
  - 网关配置文件 38, 50
  - 信任的 SSL 域列表 265
  - 要分析的映射列表 275
  - 已启用证书的网关主机列表 261
- 窗口大小
  - NetFile 的 296
- 窗口位置
  - NetFile 的 297

## D

- default
  - Windows 工作组 289
  - Windows 域 289, 290
  - 网关配置文件 38
  - 域 62
- DMZ 28
- DNS 198
- 代理
  - 重写器 237

- 反向 73
- 加密代理 183
- 加速器 330
- 解密代理 183
- 口令 257
- Netlet 183, 239
- 网络 56
- 验证 257
- 指定 254
  - 指定 hostproxy 56
- 代理自动配置 62
- 弹出警告对话框 311
- 单点登录 233
- 第三方
  - 站点引用 26
- 动态规则
  - 调用 195
  - Netlet 189
  - 下载 applet 196
- 端口
  - 回环 310
  - 目的 183
  - Netlet 182
- 端口号
  - Netlet 191
- 多个实例
  - 网关 50
- 多宿主网关 52
- 调试
  - NetFile 303
  - 信息位置 318
- 调试日志
  - 重写器 133

## F

- 反向代理 73
  - 启用 73
- 访问
  - 拒绝访问主机 316

- 允许访问主机 316
- 访问列表
  - 单点登录 233
  - 拒绝的 URL 232
  - 允许的 URL 232
- 分配
  - 默认回环端口 310
  - 为用户分配 Netlet 服务 306
- 服务
  - SRA 31
- 服务器重试间隔 251
- 复选框
  - 在端口警告对话框中启用 312

## G

- gwmultiinstance 脚本 50
- 高速缓存套接字超时 249
- 隔离区 28
- 公共主机列表
  - 配置 286
- 管理控制台 33
- 管理员配置密码 190
- 规则
  - 层叠样式表 123
  - Netlet 185
  - 添加 307
  - WML 123
  - 重写器 97
  - 重写器中的 HTML 99
  - 重写器中的 JavaScript 105
- 规则集
  - OWA 272
  - 一般 125
- 规则集映射
  - 创建 URI 列表 270
- 国家代码
  - 两字母值 351

## H

- hostproxy
  - 创建 56
- HTML
  - 重写器规则 99
- HTTP
  - 报头 73
  - 基本验证 242
  - 使用网络代理的资源 56
  - 资源, 联系 56
- 回环端口
  - 分配 310

## J

- JavaScript
  - 重写器规则 105
- 记录
  - NetFile 178
  - Netlet 200
  - 网关 279
  - 重写器 133
- iNotes 35
- 加密代理 183
- 加密套接字层 30
- 加速器
  - 代理 330
  - Sun Crypto 1000 323
  - Sun Crypto 4000 327
  - 外部 SSL 设备 330
- 监视器
  - Netlet 代理 69
  - 重写器代理 72
- 解密代理 183
- 禁用
  - 单点登录 233
  - 浏览器高速缓存 77
  - Netlet 代理 239
  - SSL 2.0 版本 262
- 禁止

## K

- 端口警告 312
- 静态规则 189
- 拒绝
  - URL 232

## K

- 开放模式 28
- 口令
  - 代理 257
- 宽限期超时 245

## L

- 联合管理 79
- 连接
  - 持久性 243
  - 启用弹出警告对话框 311
- 临时文件目录 298
- 浏览器高速缓存
  - 禁用 77

## M

- Messenger Express 35
- Microsoft Exchange Server 199
- MIME
  - 推测 129, 275
  - 要分析的类型 272
- MIME 类型
  - 创建列表 272
  - 指定 302
- 密码
  - 管理员配置 190
  - 默认加密 309
  - null 264
  - 选择 263

- 用户可配置的 189
  - 支持的 190
- 命令行提示符 25
- 默认加密密码 309
- 默认域
  - 指定 273, 288
- 模式
  - 安全 29
  - HTTP 237
  - HTTPS 237
  - 开放 28
- 目的端口 183

## N

- NetFile 175
  - 窗口大小 296
  - 窗口位置 297
  - 访问主机 290
  - 公共主机列表 286
  - 记录 178
  - 简介 175
  - 拒绝访问主机 292
  - 临时文件目录 298
  - 配置 283
  - 启用访问 177
  - 上传大小限制 299
  - 调试 303
  - Unix 验证 178
  - 压缩 301
  - 允许访问主机 291
  - 支持的协议 176
- NetFile 服务 32
- Netfile 中 176
- Netlet 182
  - applet 182
  - 保活间隔 313
  - 从远程主机下载 applet 184
  - 端口号 191
  - 访问主机 316

- 规则 183, 185
- 记录 200, 280
- 简介 181
- 监听端口 182
- 拒绝访问主机 316
- 配置 305
- 启用 239
- 启用连接时重新验证 311
- 使用方案 183
- 提供者 183
- 添加规则 307
- 通过网络代理的隧穿 259
- 为 PDC 配置 205
- 下载 applet 复选框 307
- 在 Sun Ray 环境中 201
- 注销时终止 313
- 组件 182
- Netlet 代理 183
  - 创建 68
  - 重新启动 69
  - 启用 69
  - 使用 65
  - 优点 65
- Netlet 服务 32
  - 为用户分配 306
- Netlet 规则 308
  - 动态 189
  - 静态规则 189
  - 拒绝访问 315
  - 删除 309
  - 示例 197
  - 修改 308
  - 指定访问 314
- Netlet 规则示例
  - FTP 200
  - IMAP 197
  - Lotus Notes 非网络客户机 198
  - Lotus 网络客户机 197
  - Microsoft Outlook 与 Exchange Server 199
  - Netscape 4.7 邮件客户机 200
  - SMTP 197
- nlpmultiinstance 脚本 68

- Novell Netware
  - 协议 177

## O

- OS 字符集 284
- Outlook Web Access 199
  - 规则集 173, 272
  - 配置 173

## P

- PAC
  - 配置 62
- PDC 265
  - 配置 205, 265
  - 验证 208
  - 验证链 76
- platform.conf 40
  - 属性 41
- portal server
  - 创建列表 250
- ProFTPD
  - 上载文件 177
- Proxylet
  - 简介 88
  - 配置 321
  - 启用 240
  - 优点 88
- Proxylet 服务 33
- 排除故障 133
- 配置
  - 持久性 HTTP 连接 243
  - 重写器 124
  - 个人数字证书 265
  - 公共主机列表 286
  - 拒绝的 URL 232
  - 拒绝的主机列表 292
  - Netlet 305

## Q

- Outlook Web Access 173
- Proxylet 321
- Secure Remote Access 33
- 网关 235
- 允许的主机列表 291

### 屏蔽

- 启用 131, 276
- 种子字符串 277

## Q

### 启动

- 网关 53

### 启用

- 40 位浏览器连接 261
- cookie 241
- 重写器代理 72, 237
- 重写所有 URL 124
- 存储外部服务器 cookie 251
- 单点登录 233
- 反向代理 73
- HTTP 基本验证 242
- HTTP 连接 243
- 记录 279
- 将 cookie 标记为安全 253
- 空密码 264
- 连接 237
- 连接时重新验证 311
- MIME 推测 129, 275
- 密码选择 263
- NetFile 访问 177
- Netlet 代理 69, 239
- Netlet 日志 200, 280
- PDC 验证 265
- Proxylet 240
- 屏蔽 131, 276
- SSL 2.0 版本 262
- SSL 3.0 版本 263
- 使用网络代理 254
- 弹出警告对话框 311
- 调试 303

- 网络代理 254

- 验证链 76

- 在端口警告对话框中显示复选框 312

### 缺省域

- 重写 62

## R

- rwpmultiinstance 70

- 日历 35

### 日志

- 启用调试 318

### 日志文件

- 文件名 333

## S

- SMTP 239

### SRA

- 服务 31
- 联系支持 56
- 软件 27
- 所有属性列表 335

- SSL 208

- SSL 3.0 版本 263

- SSO 233

### 删除

- Netlet 规则 309

### 上传大小限制

- NetFile 的 299

### 生成

- 自签名证书 215

### 示例

- 重写器 136

### 实例研究

- 重写器 168

### 属性

- platform.conf 41
- 配置 33

SRA 335

搜索

目录限制 300

## T

TCP/IP 181, 239

Telnet 239

套接字

连接超时 244

提示符

命令行 25

停止

网关 54

通配符

重写器中 126

在网络代理中 58

通配符证书 77

通知 34

## W

Windows

域 289, 290

Windows 域

指定 289

WINS/DNS 服务器

指定 290

WML

重写器规则 123

UNIX

命令行 33

验证 178

URI 映射分析器 130

URL

创建网络代理列表 254

非验证 260

获取会话 252

禁止重写 274

启用重写 269

已拒绝 232

已允许的 232

用户会话 cookie 246

由动态 Netlet 规则调用 195

URLScaper 90

网关 54

chroot 模式 47

超时 248

从 URL 获取会话 252

多个实例 50

多宿主 52

HTTP 模式 237

HTTPS 模式 237

记录 279

简介 37

配置 235

启动 53

启用连接 237

停止 54

网关配置文件 38

已启用证书 261

指定线程池 249

网关服务 32

网关配置文件

创建 50

网络代理 56

Netlet 隧穿 259

启用 254

委托属性 209

文件上载限制 299

## X

XML 规则

重写器中 120

协议

NetFile 176

信任的 SSL 域 265

## Y

- 修改
  - Netlet 规则 308
- 选择
  - 密码 263

## Y

- 压缩
  - NetFile 的 301
- 验证
  - 链 76
  - PDC 76, 208
  - UNIX 178
- 验证级别 234
- 一致性 278
- 应用程序
  - 运行 181
  - 支持的 35
- 用户可配置密码 189
- 域和子域代理 59
- 运行
  - HTTP 模式 237
  - HTTPS 模式 237
  - 应用程序 181
- 允许
  - 40 位浏览器连接 261
- 允许的 URL 232

## Z

- 证书
  - certadmin 脚本 214
  - 从 CA 安装 221
  - 打印 229
  - 订购 221
  - 根 CA 证书 220
  - 公共证书 210
  - 列出根 CA 证书 226
  - 列出所有 228

- SSL 208
- 删除 223
- 通配符 77
- 委托属性 209, 210
- 文件 208
- 修改委托属性 225
- 证书签名请求 217
- 自签名 215
- 支持的密码 190
- 指定 234
  - 保活间隔 313
  - 冲突解决 35
  - 代理 254
  - 代理验证 257
  - 访问主机 290
  - 高速缓存套接字超时 249
  - 回环端口 310
  - 临时目录 298
  - MIME 类型文件 302
  - 默认 WINS/DNS 290
  - 默认域 273, 288
  - NetFile 窗口大小 296
  - NetFile 窗口位置 297
  - OS 字符集 284
  - 搜索目录限制 300
  - Windows 域 289
  - 网关超时 248
  - 网关线程池容量 249
  - 验证级别 234
  - 直接连接 255
  - 最大连接队列长度 247
- 终止
  - Netlet 313
- 主机
  - 拒绝访问 316
  - 配置允许的主机列表 291, 292
  - 允许访问 316
  - 指定访问 290
- 转发用户会话 cookie 246
- 自定义
  - 网关用户界面 78
- 自动代理配置

文件位置 258  
自动检测 176  
自签名证书 215  
组件  
    Netlet 182  
最大请求数量 244

**Z**