



# Deployment Example 2: Federation Using SAML v2



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

Part No: 819-7664-10  
April 2007

Copyright 2007 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more U.S. patents or pending patent applications in the U.S. and in other countries.

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

This distribution may include materials developed by third parties.

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

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

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

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

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

---

Copyright 2007 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. Tous droits réservés.

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

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

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

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

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

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

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

# Contents

---

<b>Part I</b>	<b>About This Deployment Example</b>	19
<b>1</b>	<b>Key Features, System Architecture, and Process Flow</b>	21
1.1	Key Features	21
1.2	System Architecture	22
1.3	Illustrated Protocol Flows	25
1.4	Firewall Rules	26
<b>2</b>	<b>Before You Begin</b>	29
2.1	Using This Manual	29
2.1.1	Using the Companion Manual	30
2.1.2	Host Names and Functions Used in Examples	30
2.1.3	Related Third-Party Web Site References	31
2.1.4	Typographic Conventions	31
2.1.5	Shell Prompts in Command Examples	32
2.2	Downloading and Mounting the Java Enterprise System 2005Q4 Installer	32
	▼ To Download and Mount the Java Enterprise System 2005Q4 Installer	33
2.3	Obtaining the Federation Manager Program	34
2.4	Obtaining the SAMLv2 Plug-In	35
2.5	Obtaining the SAMLv2 Patch 2	35
2.6	Obtaining the Application Server Enterprise Ed 8.1 2005Q1 Patch	35
2.7	Obtaining Policy Agents Software	36
2.8	Resolving Host Names	36
2.9	Setting Up Load Balancer Hardware and Software	37
2.10	Obtaining Certificates for SSL and for XML Signing and Encryption	37
2.11	Obtaining and Using the Certificate Database Tool	38
2.12	Obtaining Instructions for Deploying the Identity Provider Site	38

2.13 Finding Help for SAMLv2 CLI Commands .....	38
<b>Part II Setting Up the Service Provider Site .....</b>	<b>39</b>
<b>3 Installing and Deploying the Federation Manager Servers .....</b>	<b>41</b>
3.1 Installing and Configuring Federation Manager 1 .....	41
▼ To Install the Web Server for Federation Manager 1 .....	41
▼ To Install Federation Manager Server 1 .....	44
▼ To Deploy the Federation Manager 1 WAR File .....	45
▼ To Install the SAMLv2 Plug-In on Federation Manager 1 .....	46
▼ To Install SAMLv2 Patch 2 on Federation Manager 1 .....	47
3.2 Installing and Configuring Federation Manager 2 .....	49
▼ To Install the Web Server for Federation Manager 2 .....	49
▼ To Install Federation Manager Server 2 .....	52
▼ To Deploy the Federation Manager 2 WAR File .....	53
▼ To Install the SAMLv2 Plug-In on Federation Manager 2 .....	54
▼ To Install the SAMLv2 Patch 2 on Federation Manager 2 .....	55
3.3 Configuring the Federation Manager Load Balancer .....	56
▼ To Configure Load Balancer 9 for the Federation Manager Servers .....	56
▼ To Configure Federation Manager 1 to Work with the Federation Manager Load Balancer .....	59
▼ To Configure Federation Manager 2 to Work with the Federation Manager Load Balancer .....	60
▼ To Verify that the Federation Manager Load Balancers are Working Properly .....	61
3.4 Configuring SSL Termination at the Federation Manager Load Balancer .....	62
▼ To Request an SSL Certificate .....	62
▼ To Install the SSL Certificate .....	63
▼ To Configure the Web Server 1 for SSL Termination .....	64
▼ To Configure the Web Server 2 for SSL Termination .....	65
▼ To Verify that SSL on the Federation Manager Load Balancer is Working Properly .....	65
<b>4 Installing and Configuring the Directory Servers .....</b>	<b>67</b>
4.1 Installing Two Directory Servers .....	67
▼ To Install Directory Server 3SP .....	67
▼ To Install Directory Server 4SP .....	71

---

4.2 Creating New Directory Server Instances .....	74
▼ To Create a New Configuration Instance in Directory Server 3SP .....	75
▼ To Create a New User Data Instance in Directory Server 3SP .....	76
▼ To Create a New Configuration Instance in Directory Server 4SP .....	77
▼ To Create a New User Data Instance in Directory Server 4SP .....	78
4.3 Enabling Multi-Master Replication of the Configuration Instances .....	79
▼ To Enable Multi-Master Replication of the Configuration Instance on Directory Server 3SP .....	80
▼ To Enable Multi-Master Replication of the Configuration Instance on Directory Server 4SP .....	81
▼ To Create a Replication Agreement for the Configuration Instance on Directory Server 3SP .....	82
▼ To Create a Replication Agreement for the Configuration Instance on Directory Server 4SP .....	84
▼ To Initialize the Configuration Instance Master Replica .....	85
4.4 Enabling Multi-Master Replication of the User Data Instances .....	86
▼ To Enable Multi-Master Replication for the User Data Instance on Directory Server 3SP .....	87
▼ To Enable Multi-Master Replication for the User Data Instance on Directory Server 4SP .....	88
▼ To Create a Replication Agreement for the User Data Instance on Directory Server 3SP ..	90
▼ To Create a Replication Agreement for the User Data Instance on Directory Server 4SP ..	91
▼ To Initialize the User Data Instance Master Replica .....	92
4.5 Configuring the Directory Server Load Balancers .....	93
4.5.1 Simple Persistence .....	94
▼ To Configure Load Balancer 7 for the Directory Server Configuration Instances .....	94
▼ To Configure Load Balancer 8 for the Directory Server User Data Instances .....	98
<b>5 Configuring Federation Manager Servers to Work with Directory Servers .....</b>	<b>103</b>
5.1 Migrating Federation Manager 1 Configuration from Flat Files to Directory Servers .....	103
▼ To Migrate Federation Manager 1 Services Schema into the Directory Servers .....	104
▼ To Update the Federation Manager 1 serverconfig.xml File .....	105
▼ To Update the Federation Manager 1 AMConfig.properties File .....	107
▼ To Regenerate and Redeploy the Federation Manager 1 WAR File .....	107
▼ To Update the Platform Server List .....	108
5.2 Migrating Federation Manager 1 User Data from Flat Files to Directory Servers .....	109

▼ To Load SAMLv2 Users Schema into the Directory Servers .....	109
▼ To Update the Federation Manager 1 AMConfig.properties File .....	110
▼ To Update the Federation Manager 1 serverconfig.xml File .....	111
5.3 Migrating Federation Manager 2 Configuration from Flat Files to Directory Servers .....	112
▼ To Update the Federation Manager 2 serverconfig.xml File .....	112
▼ To Update the Federation Manager 2 AMConfig.properties File .....	113
▼ To Regenerate and Redeploy the Federation Manager 2 WAR File .....	113
5.4 Migrating Federation Manager 2 User Data from Flat Files to Directory Servers .....	114
▼ To Update the Federation Manager 2 AMConfig.properties File .....	114
▼ To Update the Federation Manager 2 serverconfig.xml File .....	115
5.5 Configuring the Federation Manager Authentication Service to Work with the Directory Servers .....	116
▼ To Migrate the Federation Manager User Data to the Directory Server User Data Store ..	116
▼ To Verify that LDAP Authentication Works Properly .....	119
<b>6 Setting Up the Service Provider Keystores .....</b>	<b>121</b>
6.1 Configuring the Keystore for Federation Manager 1 .....	121
▼ To Obtain an XML Signing Certificate from a Trusted Certificate Authority .....	122
▼ To Obtain an Encryption Certificate from a Trusted Certificate Authority .....	126
6.2 Configuring Federation Manager 1 to Recognize the New Keystores and Key Files .....	130
▼ To Create the Federation Manager 1 Keystore Passwords .....	131
▼ To Modify the AMConfig.properties File .....	131
6.3 Configuring the Keystore for Federation Manager 2 .....	132
▼ To Install the Federation Manager 1 XML Signing Certificate on Federation Manager 2 ..	132
6.4 Configuring Federation Manager 2 to Recognize the New Keystores and Key Files .....	133
▼ To Create the Federation Manager 2 Keystore Passwords .....	134
▼ To Modify the AMConfig.properties File .....	134
6.5 Loading the Access Manager Root CA Certificates into the Federation Manager Servers ..	135
▼ To Load the Root CA Certificate into the Federation Manager 1 Web Container .....	135
▼ To Load the Root CA Certificate into the Federation Manager 2 Web Container .....	137
<b>7 Configuring SAMLv2 Metadata for the Federation Manager Servers .....</b>	<b>139</b>
7.1 Creating a Circle of Trust .....	139
▼ To Create a Circle of Trust .....	139
7.2 Configuring the SAMLv2 Service Provider Metadata .....	140

---

▼ To Generate and Customize the Service Provider Template Files .....	140
7.2.1 Sample Metadata Template Files .....	141
7.3 Loading the Service Provider SAMLv2 Metadata .....	146
7.3.1 To Load the Customized Service Provider Metadata .....	146
<b>Part III Setting Up the Identity Provider Site .....</b>	<b>147</b>
<b>8 Installing the SAMLv2 Plug-in on Access Manager Servers .....</b>	<b>149</b>
8.1 Installing the SAMLv2 Plug-In on the Access Manager Servers .....	149
▼ To Install the SAMLv2 Plug-In and the SAMLv2 Patch on Access Manager 1 .....	150
▼ To Install the SAMLv2 Plug-In and the SAMLv2 Patch on Access Manager 2 .....	153
8.2 Configuring the Access Manager Load Balancer for the SAMLv2 Protocols .....	156
8.3 Configuring the Access Manager Servers to Use SAMLv2 User Schema .....	156
▼ To Reconfigure the LDAPv3 Plug-In on the Access Manager User Instances .....	156
<b>9 Setting Up the Identity Provider Keystores .....</b>	<b>159</b>
9.1 Configuring the Keystore for Access Manager 1 .....	159
▼ To Obtain an XML Signing Certificate from a Trusted Certificate Authority .....	160
▼ To Obtain an Encryption Certificate from a Trusted Certificate Authority .....	163
9.2 Configuring Access Manager 1 to Recognize the New Keystores and Key Files .....	167
▼ To Create the Access Manager 1 Keystore Passwords .....	168
▼ To Modify the AMConfig.properties File .....	168
▼ To Modify the amsaml.properties File .....	169
9.3 Configuring the Keystore for Access Manager 2 .....	169
▼ To Install the Access Manager 1 XML Signing Certificate on Access Manager 2 .....	169
9.4 Configuring Access Manager 2 to Recognize the New Keystores and Key Files .....	170
▼ To Create the Access Manager 2 Keystore Passwords .....	171
▼ To Modify the AMConfig.properties File .....	171
▼ Modify the amSAML.properties File .....	172
9.5 Loading the Federation Manager Root CA Certificates into the Access Manager Servers ..	172
▼ To Load the Root CA Certificate into the Access Manager 1 Web Container .....	172
▼ To Load the Root CA Certificate into the Access Manager 2 Web Container .....	174

<b>10</b>	<b>Configuring SAMLv2 Metadata for the Access Manager Servers</b> .....	177
10.1	Creating a Circle of Trust .....	177
▼	To Create a Circle of Trust .....	177
10.2	Configuring the SAMLv2 Identity Provider Metadata .....	178
▼	To Generate and Customize the Identity Provider Template Files .....	178
10.3	Loading the SAMLv2 Metadata .....	179
▼	To Load Customized Identity Provider Configuration Files .....	180
10.4	Sample Identity Provider Metadata Template Files .....	180
<b>Part IV</b>	<b>Exchanging Metadata Between Identity Provider and Service Provider</b> .....	185
<b>11</b>	<b>Loading Identity Provider and Service Provider Metadata</b> .....	187
11.1	Loading Service Provider Metadata into the Access Manager Servers .....	187
▼	To Load the Service Provider Metadata into the Identity Provider Servers .....	187
▼	To Load the Identity Provider Metadata into the Service Provider Servers .....	189
<b>12</b>	<b>Verifying that SAMLv2 Protocols are Working Properly</b> .....	191
12.1	Creating Test Users .....	191
▼	To Create a Test Identity Provider User .....	191
▼	To Create a Test Service Provider User .....	192
12.2	Testing Basic SAMLv2 Protocols .....	193
▼	To Verify that Basic Login and Logout Work Properly .....	193
▼	To Verify that Single Sign-On Works Properly on Initial Login .....	193
▼	To Verify that Single Logout Works Properly .....	194
▼	To Verify that Single Sign-On Works Properly on Subsequent Login .....	194
<b>Part V</b>	<b>Setting Up Policy Agents in the Service Provider Site</b> .....	197
<b>13</b>	<b>Installing and Configuring J2EE Policy Agents</b> .....	199
13.1	Creating J2EE Policy Agent Profiles on the Federation Manager Servers .....	199
▼	To Create a J2EE Policy Agent Profile on Protected Resource 3 .....	200
▼	To Create an J2EE Policy Agent Profile on Protected Resource 4 .....	200
13.2	Installing Application Server 3 and J2EE Policy Agent 3 .....	201
▼	To Install Application Server 3 on Protected Resource 3 .....	201



▼ To Run the J2EE Policy Agent Installer on Application Server 3 .....	203
13.3 Completing the J2EE Policy Agent 3 Installation .....	205
▼ To Deploy the J2EE Policy Agent Housekeeping Application .....	205
▼ To Enable the J2EE Policy Agent 3 to Run in SSO-Only Mode .....	206
▼ To Initialize the Application Server 3 Certificate Database .....	206
▼ To Deploy the Sample Agent Application on Application Server 3 .....	207
▼ To Verify the Use of the Sample Agent Application on Application Server 3 .....	208
13.4 Installing Application Server 4 and J2EE Policy Agent 4 .....	208
▼ To Install Application Server 4 on Protected Resource 4 .....	208
▼ To Run the J2EE Policy Agent Installer on Application Server 4 .....	211
13.5 Completing the J2EE Policy Agent 4 Installation .....	212
▼ To Deploy the J2EE Policy Agent Housekeeping Application .....	213
▼ To Enable the J2EE Policy Agent 4 to Run in SSO-Only Mode .....	213
▼ To Initialize the Application Server 4 Certificate Database .....	214
▼ To Deploy the Sample Agent Application on Application Server 4 .....	215
▼ To Verify the Use of the Sample Agent Application on Application Server 4 .....	215
13.6 Configuring the J2EE Policy Agents Load Balancer .....	216
▼ To Configure the J2EE Policy Agents Load Balancer .....	216
▼ To Terminate SSL at the J2EE Policy Agents Load Balancer .....	219
13.7 Configuring the Application Servers for SSL Termination .....	220
▼ To Configure Application Server 3 for SSL Termination .....	220
▼ To Configure Application Server 4 for SSL Termination .....	221
13.8 Configuring the J2EE Policy Agents to Work with the J2EE Policy Agents Load Balancer .....	222
▼ To Configure J2EE Policy Agent 3 to Work with the J2EE Policy Agents Load Balancer ..	223
▼ To Configure J2EE Policy Agent 4 to Work with the J2EE Policy Agents Load Balancer ..	223
▼ To Verify that the J2EE Policy Agents Load Balancer Works Properly .....	224
13.9 Configuring the J2EE Policy Agents Load Balancer to Participate in SAMLv2 Protocols	225
▼ To Configure the J2EE Policy Agents Load Balancer to Participate in SAMLv2 Protocols .....	225
▼ To Verify that the J2EE Policy Agents Load Balancer Uses SAMLv2 Protocols .....	226
<b>14 Installing and Configuring Web Policy Agents .....</b>	<b>227</b>
14.1 Creating Web Agent Profiles on the Federation Manager Servers .....	227
▼ To Create the <code>UrlAccessAgent.properties</code> File on Federation Manager 1 .....	227
▼ To Create the <code>UrlAccessAgent.properties</code> File on Federation Manager 2 .....	228

14.2	Installing Web Server 3 and Web Policy Agent 3 .....	229
▼	To Install Web Server 3 on Protected Resource 3 .....	229
▼	To Install Web Policy Agent 3 .....	232
14.3	Completing the Web Policy Agent 3 Installation .....	234
▼	To Edit the AMAgent.Properties File .....	234
▼	To Verify that Web Policy Agent 3 is Working Properly .....	235
▼	To Import the Root CA Certificate into the Web Server 3 Key Store .....	235
▼	To Verify that Web Policy Agent 3 Can Access the Federation Manager Load Balancer .....	237
14.4	Installing Web Server 4 and Web Policy Agent 4 .....	237
▼	To Install Web Server 4 on Protected Resource 4 .....	237
▼	To Install Web Policy Agent 4 .....	240
14.5	Completing the Web Policy Agent 4 Installation .....	242
▼	To Edit the AMAgent.Properties File .....	242
▼	To Verify that Web Policy Agent 4 is Working Properly .....	243
▼	To Import the Root CA Certificate into the Web Server 4 Key Store .....	243
▼	To Verify that Web Policy Agent 4 Can Access the Federation Manager Load Balancer .....	245
14.6	Configuring the Web Policy Agents Load Balancer .....	245
▼	To Configure the Web Policy Agents Load Balancer .....	246
▼	To Configure the Web Policy Agents to Work with the Web Policy Agents Load Balancer .....	250
▼	To Verify that the Web Policy Agents Load Balancer is Working Properly .....	252
14.7	Configuring the Web Policy Agents Load Balancer to Participate in SAMLv2 Protocols .....	253
▼	To Enable the Web Policy Agents Load Balancer to Use SAMLv2 Protocols .....	253
▼	To Verify that the Web Policy Agents Load Balancer Uses SAMLv2 Protocols .....	254
<b>Part VI</b>	<b>Configuring Special Use Cases .....</b>	<b>255</b>
<b>15</b>	<b>Use Case 1: Testing Basic SAMLv2 Protocols .....</b>	<b>257</b>
15.1	Before You Begin .....	257
▼	To Create an index.jsp File .....	258
▼	To Create a Test User in the Identity Provider Site .....	258
15.2	Testing Requests Initiated by the Service Provider Using SOAP .....	259
▼	To Test Persistent Federation Using Browser Artifact .....	260
15.2.1	To Test Logout Using SOAP .....	260
▼	To Test Single Sign-On Using Browser Artifact .....	261

▼ To Test Federation Termination Using SOAP .....	262
15.3 Testing Requests Initiated by the Service Provider Using HTTP Redirect .....	262
▼ To Test Persistent Federation Using Browser POST .....	263
▼ To Test Logout Using HTTP .....	263
▼ To Test Single Sign-On Using Browser POST .....	264
▼ To Test Federation Termination Using HTTP .....	265
15.4 Testing Requests Initiated by the Identity Provider Using SOAP .....	265
▼ To Test Persistent Federation Using Browser Artifact .....	265
▼ To Test Logout Using SOAP .....	266
▼ To Test Single Sign-On Using Browser Artifact .....	267
▼ To Test Federation Termination Using SOAP .....	267
15.5 Testing Requests Initiated by the Identity Provider Using HTTP Redirect .....	268
▼ To Test Persistent Federation Using Browser POST .....	268
▼ To Test Logout Using HTTP .....	269
▼ To Test Single Sign-On Using Browser POST .....	270
▼ To Test Federation Termination Using HTTP .....	270
15.6 The Sample jsp.index File .....	271
<b>16 Use Case 2: User Attribute Mapping .....</b>	<b>277</b>
16.1 Mapping User Attributes from the Identity Provider to a Single User on the Service Provider .....	277
▼ To Modify the usersLDAP User Attributes .....	278
▼ To Create a New User .....	278
▼ To Edit the New User's Contact Information .....	279
▼ To Modify the Identity Provider Metadata .....	279
▼ To Modify the Service Provider Metadata .....	280
▼ To Modify the Agents Properties .....	281
▼ To Verify that Attribute Mapping is Working Properly .....	282

<b>Part VII</b>	<b>Reference: Summaries of Server and Component Configurations</b> .....	289
<b>A</b>	<b>Directory Servers</b> .....	291
<b>B</b>	<b>Federation Manager Servers</b> .....	297
<b>C</b>	<b>Sun Java System Application Servers and J2EE Policy Agents</b> .....	299
<b>D</b>	<b>Sun Java System Web Servers and Web Policy Agents</b> .....	303
<b>E</b>	<b>Load Balancers</b> .....	305
<b>F</b>	<b>Keystores and SSL Certificate Chains</b> .....	309

# Figures

---

FIGURE 1-1	Physical Architecture for Federation Using SAMLv2 .....	23
FIGURE 1-2	From <i>Access Manager Load Balancing, Distributed Authentication UI, and Session Failover</i> .....	24
FIGURE 1-3	SSO Protocol Flow .....	25
FIGURE 1-4	Single Logout Protocol Flow .....	26
FIGURE 16-1	Output from <code>snoop.jsp</code> .....	284



# Tables

---

TABLE 1-1	Software Products Used in Examples .....	22
TABLE 1-2	Firewall Rules .....	26
TABLE 2-1	Naming Conventions Used in This Manual .....	30
TABLE 2-2	Typographic Conventions .....	32
TABLE 2-3	Shell Prompts .....	32
TABLE 2-4	Local host File for Resolving Host Names .....	36
TABLE 8-1	Access Manager Load Balancer Settings .....	156
TABLE 15-1	SAMLv2 Profiles Illustrated in Use Case 1 .....	258
TABLE A-1	Directory Server 3SP Configuration .....	291
TABLE A-2	Directory Server 4SP Configuration .....	293
TABLE A-3	User Data Store Accounts .....	295
TABLE B-1	Federation Manager 1 Configuration .....	297
TABLE B-2	Federation Manager 2 Configuration .....	298
TABLE C-1	Protected Resource 3 Application Server and J2EE Policy Agent 3 Configurations .....	299
TABLE C-2	Protected Resource 4 Application Server and J2EE Policy Agent 4 Configurations .....	300
TABLE D-1	Protected Resource 3 Web Server and Web Policy Agent 3 Configurations ....	303
TABLE D-2	Protected Resource 4 Web Server and Web Policy Agent 4 Configurations ....	304
TABLE E-1	Load Balancer Configurations .....	305
TABLE F-1	Keystores .....	309
TABLE F-2	Certificate Chains .....	309





# Examples

---

EXAMPLE 7-1	Modified saml2-sp-template.xml File .....	141
EXAMPLE 7-2	Modified saml2-sp-metadata-template.xml File .....	143
EXAMPLE 10-1	Modified saml2-idp-template.xml File .....	180
EXAMPLE 10-2	Modified saml2-idp-metadata-template.xml File .....	182
EXAMPLE 15-1	Sample jsp.index File for Testing SAMLv2 Protocols .....	271
EXAMPLE 16-1	snoop.jsp .....	284



PART I

About This Deployment Example



# Key Features, System Architecture, and Process Flow

---

This document provides detailed instructions for enabling Security Assertion Markup Language (SAML) version 2 in a federated environment. You can adapt these instructions to suit your company's needs.

Sun Java™ System Access Manager and Federation Manager implement two important sets of standards: Identity Federation Framework (ID-FF), adopted by the Liberty Alliance Project, and SAML specifications adopted by the OASIS committee. These implementations enable business partners to form a Circle of Trust. The Circle of Trust enables individuals and organizations to easily conduct network transactions while protecting the individual's identity. For detailed information about the Liberty Alliance Project and about Access Manager implementations of federated identity and SAML protocols, see *Sun Java System Access Manager 7 2005Q4 Federation and SAML Administration Guide*.

## 1.1 Key Features

The setup instructions contained in this document use a specific environment to illustrate how to set up federation and SAMLv2 protocols. This environment is designed to highlight the following key features:

- Access Manager servers are deployed in high-availability mode.
- Federation Managers are deployed in high-availability mode and configured to work with Sun Java System Directory Server instead of the default flat files.
- XML Signing is enabled for all SAMLv2 protocols.
- SAML2 URL end points are exposed through load balancers with SSL termination.
- Web Policy Agents and J2EE Policy Agents are deployed in front of the Federation Manager instances, and the policy agents work only in single sign-on (SSO) mode.

## 1.2 System Architecture

In this system architecture, a Service Provider and a Identity Provider form a circle of trust in order to exchange user authentication information using SAMLv2. For these instructions, the circle of trust contains one identity provider, a service that maintains and manages identity information. Once the circle of trust is established, single sign-on is enabled between both providers.

The Service Provider domain is `siroe.com`. In this deployment, two Federation Managers are load-balanced for high availability, and each is configured for the SAMLv2 protocol. Each Federation Manager server uses a Directory Server user instance for user data.

The Identity Provider domain is `example.com`. Two Access Manager servers are configured for the SAMLv2 protocol and load-balanced for high availability.

TABLE 1-1 Software Products Used in Examples

Component	Versions
Sun Java Access Manager	7.0 JES 2005Q4
Sun Java Access Manager Patch	7.0_Patch_5
Sun Java Directory Server	5.2 JES 2005Q4
Sun Java Directory Server Patch	5.2_Patch_4
Sun Java System Federation Manager	7.0
Sun Java Web Server	6.1SP5 JES 2005Q4
Web Policy Agent (for Sun Java WebServer v6.1)	2.2
Web Policy Agent Patch	HotPatch_5
Sun Java Application Server	8.1 JES 2005Q4
Sun Java Application Server Patch	Enterprise Ed 8.1 2005Q1
J2EE Policy Agent (for Sun Java Application server 8.1 2005Q1)	2.2
SAML plug-in	2
SAML v2 plug-in Patch	2
Sun Solaris	10, Update 5

Figure 1-1 on the next page illustrates the Service Provider Site described in this document, *Deployment Example 2: Federation Using SAMLv2*.

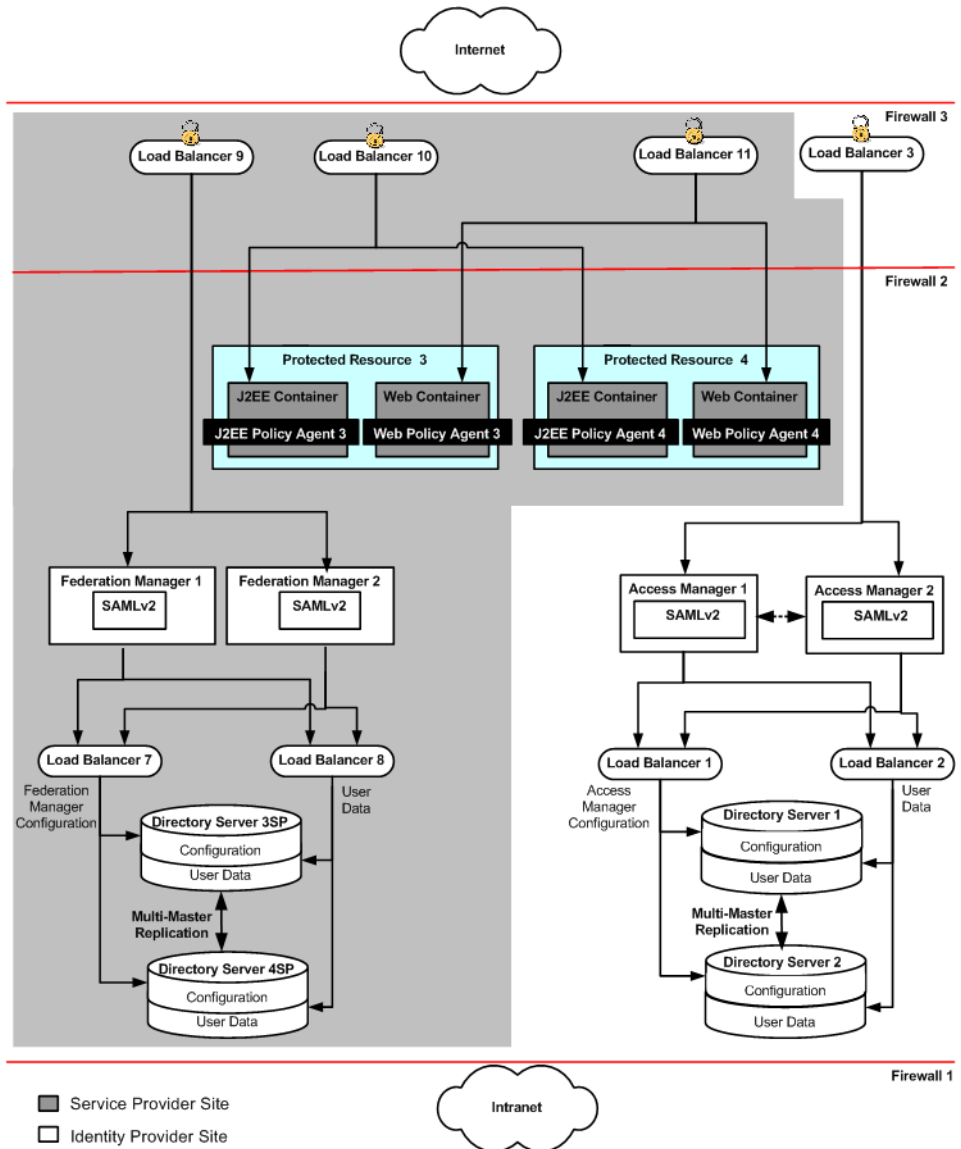


FIGURE 1-1 Physical Architecture for Federation Using SAMLv2

The Identity Provider Site shown here is a subset of a larger deployment example described in a companion document, *Deployment Example: Access Manager Load Balancing, Distributed Authentication, and Session Failover*. Use the two companion documents together to build both the Service Provider Site and the Identity Provider Site. See “2.12 Obtaining Instructions for Deploying the Identity Provider Site” on page 38.

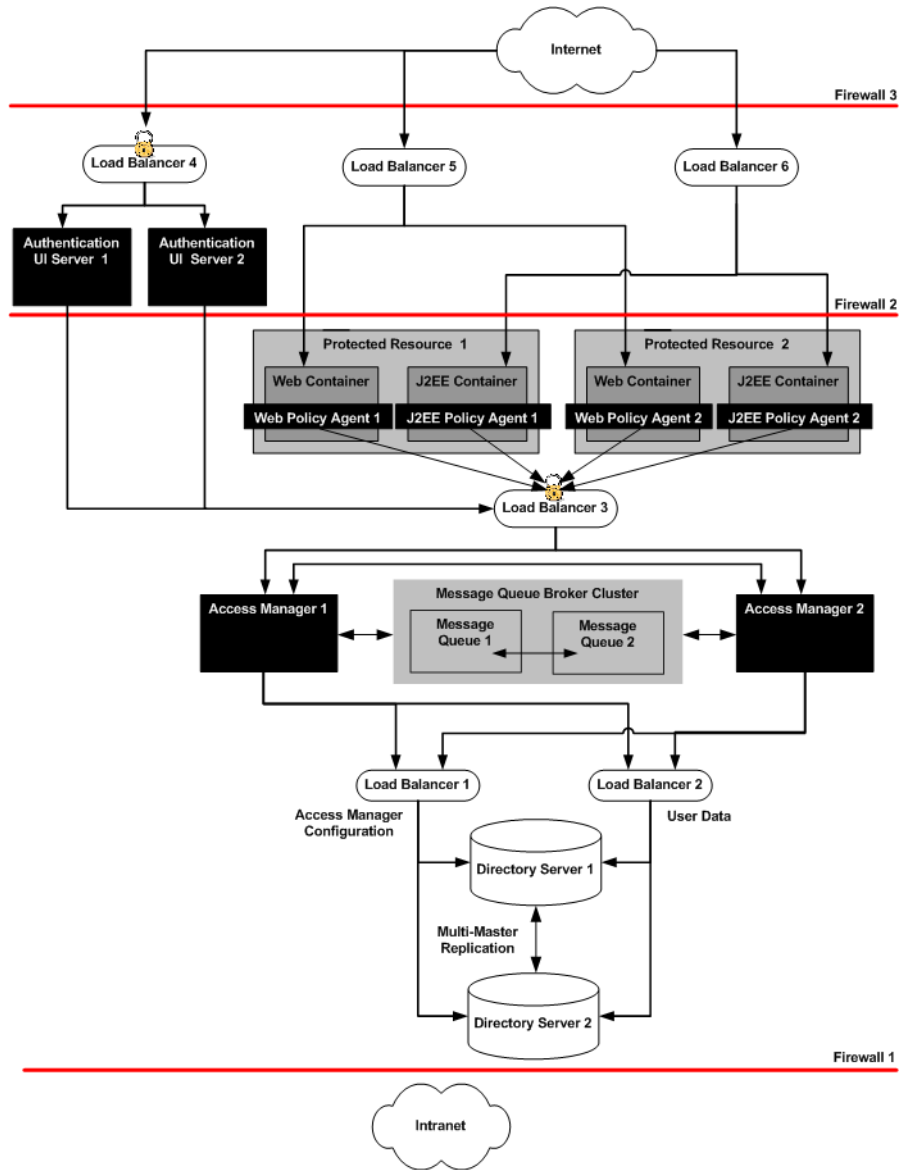


FIGURE 1-2 From *Access Manager Load Balancing, Distributed Authentication UI, and Session Failover*

To set up the Identity Provider Site, see *Deployment Example: Access Manager Load Balancing, Distributed Authentication, and Session Failover*. Follow the detailed instructions for setting up the Directory Servers, the Access Manager Servers, their respective load balancers, and session



failover. For the Federation Using SAMLv2 deployment example, it is not necessary to implement the Distributed Authentication UI or the Protected Resources and policy agents pictured here.

## 1.3 Illustrated Protocol Flows

The following figure describes one possible SAMLv2 transaction.

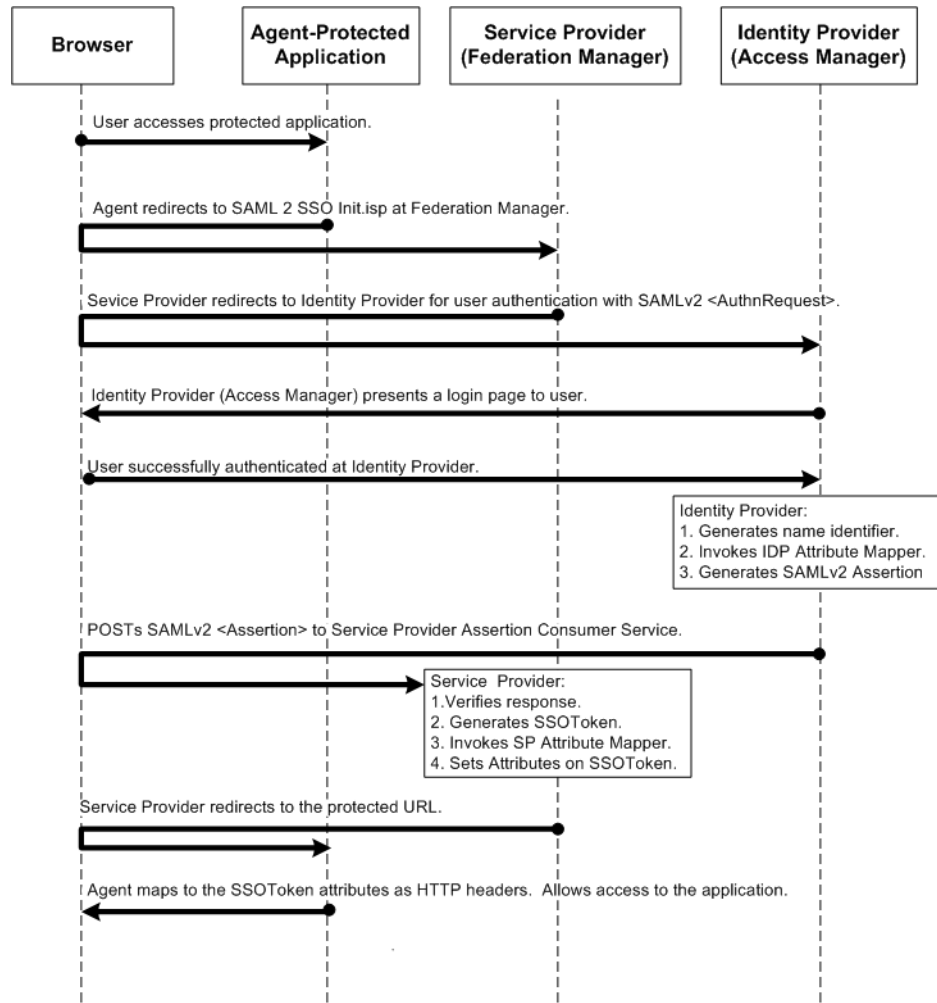


FIGURE 1-3 SSO Protocol Flow

The following figure describes the component interactions in an HTTP redirect-based single logout transaction.

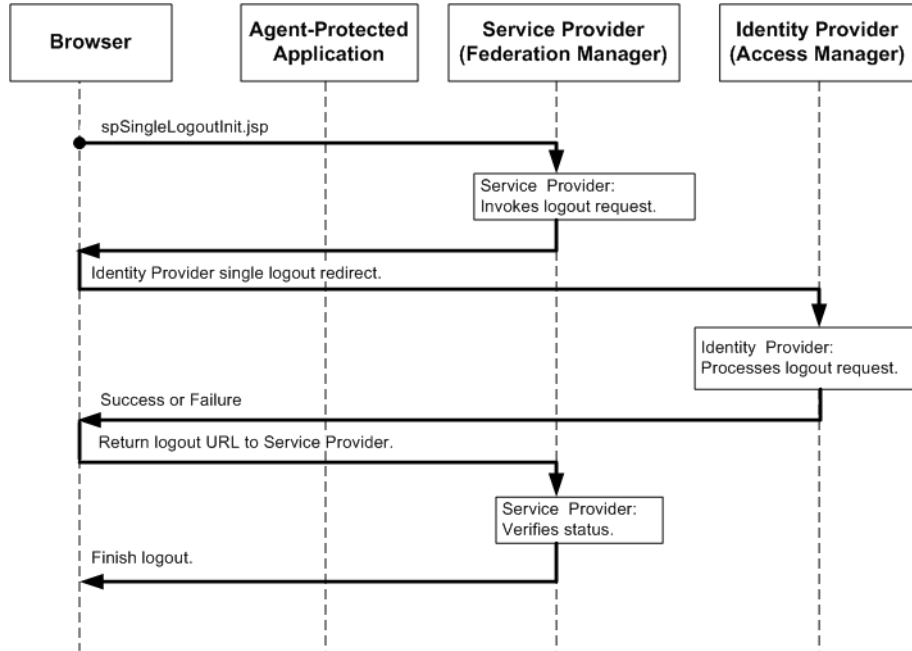


FIGURE 1-4 Single Logout Protocol Flow

## 1.4 Firewall Rules

Set up firewalls to allow traffic to flow as described in the following table.

TABLE 1-2 Firewall Rules

From	To	Protocol	Traffic Type
Internet User	LoadBalancer-9:3443	HTTPS	Internet metadata URLs access and user authentication at the Service Provider site
Internet User	LoadBalancer-10:4443	HTTPS	Service Provider application access
Internet User	LoadBalancer-11:6443	HTTPS	Service Provider application access
Internet User	LoadBalancer-3:9443	HTTPS	Internet metadata URLs access and user authentication at the Identity Provider site

TABLE 1-2 Firewall Rules (Continued)

From	To	Protocol	Traffic Type
LoadBalancer-10:4080	ProtectedResource-3:1080	HTTP	Service Provider application access by user
LoadBalancer-10:4080	ProtectedResource-4:1080	HTTP	Service Provider application access by user
LoadBalancer-11:5080	ProtectedResource-3:2080	HTTP	Service Provider application access by user
LoadBalancer-11:5080	ProtectedResource-4:2080	HTTP	Service Provider application access by user
Load Balancer-3:7070	AccessManager-1:8080	HTTP	Load balancer redirection to Access Manager
Load Balancer-3:7070	AccessManager-2:1080	HTTP	Load balancer redirection to Access Manager
LoadBalancer-9:1080	FederationManager-1:8080	HTTP	Load balancer redirection to Federation Manager
LoadBalancer-9:1080	FederationManager-2:8080	HTTP	Load balancer redirection to Federation Manager



## Before You Begin

---

This chapter provides the information about obtaining necessary software, tools, and third-party resources you'll need when implementing Federation using SAMLv2. The chapter also provides information about instructions that are outside the scope of this document, and how to obtain those instructions. You may want to resolve the issues described in this chapter before you begin building the Federation environment.

The following topics are discussed in this chapter:

- “2.1 Using This Manual” on page 29
- “2.2 Downloading and Mounting the Java Enterprise System 2005Q4 Installer” on page 32
- “2.3 Obtaining the Federation Manager Program” on page 34
- “2.4 Obtaining the SAMLv2 Plug-In ” on page 35
- “2.5 Obtaining the SAMLv2 Patch 2” on page 35
- “2.6 Obtaining the Application Server Enterprise Ed 8.1 2005Q1 Patch” on page 35
- “2.8 Resolving Host Names” on page 36
- “2.9 Setting Up Load Balancer Hardware and Software” on page 37
- “2.10 Obtaining Certificates for SSL and for XML Signing and Encryption” on page 37
- “2.11 Obtaining and Using the Certificate Database Tool” on page 38
- “2.12 Obtaining Instructions for Deploying the Identity Provider Site” on page 38
- “2.13 Finding Help for SAMLv2 CLI Commands” on page 38

### 2.1 Using This Manual

This manual provides instructions for building a Federation environment using SAMLv2. These instructions were used to build, deploy and test this deployment example in a lab facility. When using this manual, you'll obtain the best results if you perform the tasks in the exact sequence in which they are presented. Use the Table of Contents which begins on page 3 as a master task list. Groups of tasks are numbered for your convenience.

The last step in each task is a verification procedure. Be sure to verify the success of each task before moving on to the next task in the sequence.

This manual is designed to demonstrate just one way to implement Federation using SAMLv2. Although these instructions incorporate many recommended or “best practices,” and may be suitable in many different scenarios, this is not the only way to achieve the same results.



**Caution** – If you do plan to deviate from the task sequence or details described in this manual, you should refer to the relevant product documentation for information on differences in platforms, software versions or other requirement constraints.

## 2.1.1 Using the Companion Manual

This manual, *Deployment Example 2: Federation Using SAMLv2*, is designed to be used with its companion manual, *Deployment Example 1: Access Manager Load Balancing, Distributed Authentication UI, and Session Failover*. Use the Deployment Example 1 manual to set up the Identity Provider Site, and use this Deployment Example 2 manual to set up the Service Provider Site. For more information, see “[1.2 System Architecture](#)” on page 22 and “[2.12 Obtaining Instructions for Deploying the Identity Provider Site](#)” on page 38 in this manual.

## 2.1.2 Host Names and Functions Used in Examples

The following table lists naming conventions used in this manual.

TABLE 2-1 Naming Conventions Used in This Manual

Host Name :Port Number	Main Service URL
Directory Servers	
DirectoryServer-3SP:1391	ldap://DirectoryServer-3SP.siroe.com:1391
DirectoryServer-4SP:1391	ldap://DirectoryServer-4SP.siroe.com:1391
Access Managers	
AccessManager-1:58080	http://AccessManager-1.example.com:58080/amserver
AccessManager-2:58080	http://AccessManager-1.example.com:58080/amserver
Federation Managers	
FederationManager-1:8080	http://FederationManager-1.siroe.com:8080
FederationManager-1:8080	http://FederationManager-2.siroe.com:8080
Protected Resources — Application Servers	
ProtectedResource-3:8888	http://LoadBalancere-10.siroe.com:1080

TABLE 2-1 Naming Conventions Used in This Manual (Continued)

Host Name :Port Number	Main Service URL
ProtectedResource-4:8888	http://LoadBalancer-10.siroe.com:1080
Protected Resources — Web Servers	
ProtectedResource-3:8888	http://LoadBalancer-11.siroe.com:2080
ProtectedResource-4:8888	http://LoadBalancer-11.siroe.com:2080
Load Balancer for Access Manager-Servers	
LoadBalancer-3:9443	http://LoadBalancer-3.example.com:9443
Load Balancers for DirectoryServers	
LoadBalancer-7	http://LoadBalancer-7.siroe.com
LoadBalancer-8	http://LoadBalancer-8.siroe.com
Load Balancer for Federation Manager Servers	
LoadBalancer-9	http://LoadBalancer-9.siroe.com
Load Balancer for J2EE Policy Agents	
LoadBalancer-10	http://LoadBalancer-10.siroe.com
Load Balancer for Web Policy Agents	
LoadBalancer-11	http://LoadBalancer-11.siroe.com

## 2.1.3 Related Third-Party Web Site References

Third-party URLs are referenced in this document and provide additional, related information.

---

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

---

## 2.1.4 Typographic Conventions

The following table describes the typographic conventions that are used in this book.

TABLE 2-2 Typographic Conventions

Typeface	Meaning	Example
AaBbCc123	The names of commands, files, and directories, and onscreen computer output	Edit your <code>.login</code> file. Use <code>ls -a</code> to list all files. <code>machine_name% you have mail.</code>
<b>AaBbCc123</b>	What you type, contrasted with onscreen computer output	<code>machine_name% su</code> Password:
<i>aabbcc123</i>	Placeholder: replace with a real name or value	The command to remove a file is <i>rm filename</i> .
<i>AaBbCc123</i>	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the <i>User's Guide</i> . A <i>cache</i> is a copy that is stored locally. Do <i>not</i> save the file. <b>Note:</b> Some emphasized items appear bold online.

## 2.1.5 Shell Prompts in Command Examples

The following table shows the default UNIX® system prompt and superuser prompt for the C shell, Bourne shell, and Korn shell.

TABLE 2-3 Shell Prompts

Shell	Prompt
C shell	<code>machine_name%</code>
C shell for superuser	<code>machine_name#</code>
Bourne shell and Korn shell	<code>\$</code>
Bourne shell and Korn shell for superuser	<code>#</code>

## 2.2 Downloading and Mounting the Java Enterprise System 2005Q4 Installer

Installation as described in this document includes the installation and basic configuration of a Java Enterprise System (Java ES) solution. Installation, as used in this document, means using the Java ES 2004Q5 installer to copy the files for Java ES components to computer systems. You



can download and unpack the installer zip files onto one host computer system, and then mount the cd image on any remote host computer systems where you must install Directory Server, Access Manager, Web Server, or Application Server.

## ▼ To Download and Mount the Java Enterprise System 2005Q4 Installer

### 1 Download the Java ES installer zip files.

#### a. Start a browser, and go to

<http://www.sun.com/software/javaenterprisesystem/getit.jsp>.

#### b. Choose Java Enterprise System.

Follow the instructions for downloading two zip files that together will form the CD image.

### 2 Log in as a root user to a host computer system where you want to run the installer.

### 3 Copy the Java Enterprise System installer zip files to this host computer system.

### 4 Unzip each zipped file. Example:

```
#ls
java_es_05Q4-ga-solaris-sparc-1-iso.zip
java_es_05Q4-ga-solaris-sparc-2-iso.zip
# unzip java_es_05Q4-ga-solaris-sparc-1-iso.zip
inflating: java_es_05Q4-ga-solaris-sparc-1.iso...

# unzip java_es_05Q4-ga-solaris-sparc-2-iso.zip
inflating: java_es_05Q4-ga-solaris-sparc-2.iso...
```

### 5 Create three directories for mounting the .iso files. Example:

```
# mkdir /mnt
# mkdir /mnt2
# mkdir /jes-complete
```

### 6 Mount the .iso files.

In the following examples, replace */download-directory/* with the path to your .iso file:

```
# lofiadm -a /download-directory/java_es_05Q4-ga-solaris-sparc-1.iso /dev/lofi/1
# mount -F hsfs -o ro /dev/lofi/1 /mnt
```

**Tip** – If the `/dev/lofi/1` device is already in use, run this command:

```
# lofiadm -d /dev/lofi/1
```

and then retry using the `lofiad -a` command.

---

To mount the second iso file:

```
# lofiadm -a /download-directory/java_es_05Q4-ga-solaris-sparc-2.iso /dev/lofi/2
# mount -F hsfs -o ro /dev/lofi/2 /mnt2
# lofiadm
Block Device          File
dev/lofi/1            /export/temp/java_es_05Q4-ga-solaris-sparc-1.iso
/dev/lofi/2           /export/temp/java_es_05Q4-ga-solaris-sparc-2.iso
```

#### 7 Copy both mounted .iso files to the same directory.

The two .iso files together form the complete JES package, so you must copy both files into the same directory. As an alternative, you can burn each ISO onto a CD, and then run the installer from a CD drive.

```
# cd /mnt1
# cp -r * /jes-complete
# cd /mnt2
# cp -r * /jes-complete
```

**Next Steps** After you mount the .iso files, the installer is located in the following directory:

```
/jes-complete/Solaris_sparc
```

In this Deployment Example, you start the installer with the `-nodisplay` option:

```
# /jes-complete/Solaris_sparc/installer -nodisplay
```

## 2.3 Obtaining the Federation Manager Program

Download the Sun Java System Federation Manager program onto the Federation Manager 1 host and onto the Federation Manager 2 host. You can download the software from the following page on the Sun Microsystems website:

<http://www.sun.com/download/products.xml?id=44a5bbb5>

## 2.4 Obtaining the SAMLv2 Plug-In

Download the Sun Java System SAMLv2 Plug-in for Federation Services 1.0 onto the Federation Manager 1 host, the Federation Manager 2 host, the Access Manager 1 host, and the Access Manager 2 host. You can download the software from the following page on the Sun Microsystems website: <http://www.sun.com/download/products.xml?id=43e00414>

## 2.5 Obtaining the SAMLv2 Patch 2

Download the Sun Java System SAMLv2 Plug-in Patch 2 for Federation Services 1.0 onto the Federation Manager 1 host, the Federation Manager 2 host, the Access Manager 1 host, and the Access Manager 2 host. You can download the software using one of the following URLs:

Solaris (sparc) 122983-02	<a href="http://sunsolve.sun.com/search/document.do?assetkey=1-21-122983-02-1">http://sunsolve.sun.com/search/document.do?assetkey=1-21-122983-02-1</a>
Solaris (x86) 122984-02	<a href="http://sunsolve.sun.com/search/document.do?assetkey=1-21-122984-02-1">http://sunsolve.sun.com/search/document.do?assetkey=1-21-122984-02-1</a>
Linux 122985-02	<a href="http://sunsolve.sun.com/search/document.do?assetkey=1-21-122985-02-01">http://sunsolve.sun.com/search/document.do?assetkey=1-21-122985-02-01</a>

## 2.6 Obtaining the Application Server Enterprise Ed 8.1 2005Q1 Patch

A known problem exists that causes Application Server to replace the `https` string in URLs to `http` during redirection. You can eliminate this problem by installing this patch.

Download the Sun Java System Application Server Enterprise Ed 8.1 2005Q1 Patch onto the Application Server 3 host and onto the Application Server 4 host. You can download the software using one of the following URLs:

Solaris (sparc) 119166-22	<a href="http://sunsolve.sun.com/search/document.do?assetkey=1-21-119166">http://sunsolve.sun.com/search/document.do?assetkey=1-21-119166</a>
Solaris (x86) 119170-14	<a href="http://sunsolve.sun.com/search/document.do?assetkey=1-21-119170-14">http://sunsolve.sun.com/search/document.do?assetkey=1-21-119170-14</a>
Linux 119171-14	<a href="http://sunsolve.sun.com/search/document.do?assetkey=1-21-119171-14">http://sunsolve.sun.com/search/document.do?assetkey=1-21-119171-14</a>

## 2.7 Obtaining Policy Agents Software

- Download the Sun Java System Access Manager Policy Agent 2.2 for Sun Java System Application Server 8.1 onto the Protected Resource 3 host and onto the Protected Resource 4 host. You can download the software from the following Sun Microsystems website: <http://www.sun.com/download/products.xml?id=43543381>
- Download the Sun Java System Access Manager Policy Agent 2.2 for Sun Java System Web Server 6.1 onto the Protected Resource 3 host and onto the Protected Resource 4 host. You can download the software from the following Sun Microsystems website: <http://www.sun.com/download/products.xml?id=434ed995>

## 2.8 Resolving Host Names

There are many ways to resolve host names used in this deployment. For example, you can use a DNS naming service, or you can include the following DN entries in a DNS database. For this particular deployment, the following entries were added to the local host file on all Unix hosts. The entries were also added to equivalent files on Windows hosts, and on client machines for where browsers are used.

TABLE 2-4 Local host File for Resolving Host Names

SP

\*\*\*\*\*

192.18.69.135	DirectoryServer-3SP	DirectoryServer-3SP.siroe.com
192.18.72.136	DirectoryServer-4SP	DirectoryServer-4SP.siroe.com
192.18.72.89	FederationManager-1	FederationManager-1.siroe.com
192.18.72.86	FederationManager-2	FederationManager-2.siroe.com
192.18.69.16	LoadBalancer-7	LoadBalancer-7.siroe.com
	LoadBalancer-8	LoadBalancer-8.siroe.com
192.18.69.14	LoadBalancer-9	LoadBalancer-9.siroe.com
	LoadBalancer-10	LoadBalancer-10.siroe.com

IDP

\*\*\*\*\*

192.18.72.84	AccessManager-1	AccessManager-1.example.com
--------------	-----------------	-----------------------------

TABLE 2-4 Local host File for Resolving Host Names		(Continued)
192.18.72.85	AccessManager-2	AccessManager-2.example.com
192.18.69.14	LoadBalancer-3	LoadBalancer-3.example.com
192.18.72.122	DirectoryServer-1	DirectoryServer-1.example.com
192.18.72.121	DirectoryServer-2	DirectoryServer-2.example.com
192.18.69.14	LoadBalancer-1	LoadBalancer-1.example.com
	LoadBalancer-2	LoadBalancer-2.example.com

## 2.9 Setting Up Load Balancer Hardware and Software

All load balancers in this deployment example are BIG-IP load balancers made by f-5 Networks. If you are using BIG-IP load balancer hardware, use the documentation that comes with the product for the initial hardware setup. See <http://f5.com/products/bigip/#>. If you are using a load balancer made by another manufacturer, use the documentation that comes with that product.

## 2.10 Obtaining Certificates for SSL and for XML Signing and Encryption

For this deployment example, all SSL certificates were obtained from an internal certificate server. You may obtain SSL certificates from a recognized Certificate Authority (CA) such as VeriSign or Thawte. Follow the instructions provided by the certificate issuer. Be sure that you are familiar with SSL certificates and the procedures for requesting and obtaining certificates from your root Certificate Authority. The following groups of tasks require you to obtain SSL certificates:

- “6.1 Configuring the Keystore for Federation Manager 1” on page 121
- “6.3 Configuring the Keystore for Federation Manager 2” on page 132
- “9.1 Configuring the Keystore for Access Manager 1” on page 159
- “9.3 Configuring the Keystore for Access Manager 2” on page 169

## 2.11 Obtaining and Using the Certificate Database Tool

For this deployment example, you must have access to the Certificate Database Tool `certutil` utility. You need the `certutil` utility for setting up the SSL Client handshake on the J2EE Policy Agents. Use `certutil` to create and modify the Application Server trust database files. You can also use `certutil` to list, generate, modify, or delete certificates within the `cert8.db` file and to create or change the password, generate new public and private key pairs, display the contents of the key database, or delete key pairs within the `key3.db` file.

For information about obtaining and using the `certutil` utility, see the following URL on the Mozilla website:

<http://www.mozilla.org/projects/security/pki/nss/tools/certutil.html>.

## 2.12 Obtaining Instructions for Deploying the Identity Provider Site

In this manual, [Part III Setting Up the Identity Provider Site](#) is designed to build upon the instructions provided in another document, *Deployment Example 1: Access Manager Load Balancing, Distributed Authentication, and Session Failover*. Download this document from the following Sun Microsystems website: <http://docs.sun.com/app/docs/doc/819-6258>

The deployment described in *Deployment Example: Access Manager Load Balancing, Distributed Authentication, and Session Failover* is similar to the Identity Provider Site described in this document, *Deployment Example 2: Federation Using SAMLv2*. See “[1.2 System Architecture](#)” on page 22 in this manual.

## 2.13 Finding Help for SAMLv2 CLI Commands

When you need onscreen information for SAMLv2 commands, you can use the following `saml2meta` commands:

Syntax `saml2meta commandName --help`

Usage `saml2meta commandName`

PART II

Setting Up the Service Provider Site





# Installing and Deploying the Federation Manager Servers

---

This chapter contains detailed information about the following groups of tasks:

- “3.1 Installing and Configuring Federation Manager 1” on page 41
- “3.2 Installing and Configuring Federation Manager 2” on page 49
- “3.3 Configuring the Federation Manager Load Balancer” on page 56
- “3.4 Configuring SSL Termination at the Federation Manager Load Balancer” on page 62

## 3.1 Installing and Configuring Federation Manager 1

Use the following as your checklist for installing and configuring Federation Manager 1:

1. Install the Web Server for Federation Manager 1.
2. Install Federation Manager Server 1.
3. Deploy the Federation Manager 1 WAR file.
4. Install the SAMLv2 Plug-In on Federation Manager 1.
5. Install SAMLv2 Patch 2 on Federation Manager 1.

### ▼ To Install the Web Server for Federation Manager 1

**Before You Begin** The Java ES installer must be mounted on the host computer system where you will install Web Server. See the section “2.2 Downloading and Mounting the Java Enterprise System 2005Q4 Installer” on page 32 in this manual.

- 1 As a root user, log into the Web Server host.
- 2 Start the Java Enterprise System installer with the `-nodisplay` option.

```
# cd /mnt/Solaris_sparc
# ./installer -nodisplay
```
- 3 When prompted, provide the following information:

Welcome to the Sun Java(TM) Enterprise System; serious software made simple... <Press ENTER to Continue>	Press Enter.
<Press ENTER to display the Software License Agreement>	Press Enter.
Have you read, and do you accept, all of the terms of the preceding Software License Agreement [No]	Enter <b>y</b> .
Please enter a comma separated list of languages you would like supported with this installation [8]	Enter <b>8</b> for "English only."
Enter a comma separated list of products to install, or press R to refresh the list [ ]	Enter <b>3</b> to select Web Server.
Press "Enter" to Continue or Enter a comma separated list of products to deselect... [1]	Press Enter.
Enter 1 to upgrade these shared components and 2 to cancel [1]	You are prompted to upgrade shared components only if the installer detects that an upgrade is required.  Enter <b>1</b> to upgrade shared components.
Enter the name of the target installation directory for each product: Web Server [/opt/SUNWwbsvr] :	Accept the default value.
System ready for installation Enter 1 to continue [1]	Enter <b>1</b> .
1. Configure Now - Selectively override defaults or express through 2. Configure Later - Manually configure following installation Select Type of Configuration [1]	Enter <b>1</b> .
Common Server Settings Enter Host Name [FederationManager-1]	Accept the default value.
Enter DNS Domain Name [siroe.com]	Accept the default value.
Enter IP Address [192.18.87.180]	Accept the default value.
Enter Server admin User ID [admin]	Enter <b>admin</b> .
Enter Admin User's Password (Password cannot be less than 8 characters) [ ]	For this example, enter <b>admin123</b> .
Confirm Admin User's Password [ ]	Enter the same password to confirm it.

Enter System User [root]	Accept the default value.
Enter System Group [root]	Accept the default value.
Enter Server Admin User ID [admin]	Accept the default value.
Enter Admin User's Password []	For this example, enter <b>admin123</b> .
Enter Host Name [FederationManager-1.siroe.com]	Accept the default value.
Enter Administration Port [8888]	Accept the default value.
Enter Administration Server User ID [root]	Accept the default value.
Enter System User ID [webservd]	Enter <b>root</b> .
Enter System Group [webservd]	Enter <b>root</b> .
Enter HTTP Port [80]	Enter <b>8080</b> .
Enter content Root [/opt/SUNWwbsvr/docs]	Accept the default value.
Do you want to automatically start Web Server when system re-starts. (Y/N) [N]	Accept the default value.
Ready to Install 1. Install 2. Start Over 3. Exit Installation What would you like to do [1]	First, see the next numbered (Optional) step. When ready to install, enter <b>1</b> .

**4 (Optional) During installation, you can monitor the log to watch for installation errors. Example:**

```
# cd /var/sadm/install/logs
# tail -f Java_Enterprise_System_install.B xxxxxx
```

**5 Upon successful installation, enter ! to exit.**

**6 Verify that the Web Server is installed properly.**

**a. Start the Web Server administration server to verify it starts with no errors.**

```
# cd /opt/SUNWwbsvr/https-admserv
# ./stop; ./start
```

**b. Run the netstat command to verify that the Web Server ports are open and listening.**

```
# netstat -an | grep 8888
*.8888          *.*              0              0      49152          0      LISTEN
```

**c. Start a browser, and go to the Web Server administration URL.**

`http://FederationManager-1.siroe.com:8888`

**d. Log in to the Web Server console.**

Username     **admin**

Password     **admin123**

You should be able to see the Web Server console. You can log out of the console now.

**e. Start the Web Server instance.**

```
# cd /opt/SUNWwbsvr/https-FederationManager-1.siroe.com
# ./stop; ./start
```

**f. Go to the Web Server instance URL.**

`http://FederationManager-1.siroe.com:8080`

You should see the default Web Server index page.

## ▼ To Install Federation Manager Server 1

**Before You Begin** If you have installed Solaris 10 using a distribution package other than the Solaris Enterprise distribution package, then you must remove the `SUNWjas` and `SUNWjata` packages that were automatically installed for you. These packages are different versions than the `SUNWjas` and `SUNWjata` packages used by Federation Manager. The appropriate packages will be installed when you run the Federation Manager installer.

**1 Download the Sun Java System Federation Manager program from the following page on the Sun Microsystems website:** <http://www.sun.com/download/products.xml?id=44a5bbb5>

**2 Unpack the Federation Manager installer.**

```
# tar -xvf fm-7.0-domestic-us.sparc-sun-solaris2.8.tar

# ls
LICENSE.TXT
README.TXT
SUNWamfm
common
fm-7.0-domestic-us.sparc-sun-solaris2.8.tar
fmsetup
fmsilent-template
```

**3 Edit the `download_directory/fmsilent-template` file.**

Make a backup of the `fmsilent-template` file, and then set the following properties in the file:

```
FM_PROCESS_USER=root
FM_PROCESS_GROUP=root
INST_ORGANIZATION=o=siroe.com
SERVER_HOST=FederationManager-1.siroe.com
SERVER_PORT=8080
ADMINPASSWD=11111111
```

**4 Save the file as `/export/fmsilent`.****5 (Optional) For online help regarding the Federation Manager installer options, enter the following with no options:**

```
# ./fmsetup
```

**6 To start the Federation Manager installer, run the following command:**

```
# ./fmsetup install -s /export/fmsilent
```

**Next Steps** The Federation Manager installer creates the following web archive (WAR) file:

```
/var/opt/SUNWam/fm/war_staging/federation.war
```

You usually customize the Federation Manager WAR file for the environment before the WAR file can be deployed. In a deployment where SAMLv2 is not used, you could customize and deploy the Federation Manager WAR file now. However in this deployment example, you will install the SAMLv2 plug-in and the SAMLv2 patch *before* you customize the Federation Manager WAR file. So proceed directly to the next task, [“To Deploy the Federation Manager 1 WAR File” on page 45.](#)

## ▼ To Deploy the Federation Manager 1 WAR File

**1 Go to the Web Server directory that contains the `wdeploy` command:**

```
# cd /opt/SUNWwbsvr/bin/https/bin
```

**2 Run the `wdeploy` command:**

```
# ./wdeploy deploy -u /federation -i FederationManager-1.siroe.com
-v https-FederationManager-1.siroe.com
/var/opt/SUNWam/fm/war_staging/federation.war
```

### 3 Verify that the WAR file was successfully deployed.

- a. Verify that a directory has been created with the same name you specified during Federation Manager installation as the URI. In this deployment example, the directory is named federation.

```
# cd /opt/SUNWwbsvr/https-FederationManager-1.siroe.com/  
webapps/https-FederationManager-1.siroe.com/federation  
# ls  
META-INF      config      docs          html          js  
WEB-INF       console    fed_css      images        saml2  
com_sun_web_ui  css      fed_images  index.html   samples
```

- b. Restart the Federation Manager server, and verify that you can successfully access it.

```
# cd /opt/SUNWwbsvr/https-FederationManager-1.siroe.com  
# ./stop; ./start
```

- c. In a browser, go to the following URL:

```
http://FederationManager-1.siroe.com:8080/federation/UI/Login
```

- d. Log in to the Federation Manager console:

```
User Name:   amadmin  
Password:   11111111
```

If you can successfully log in, then the Federation Manager WAR file has been successfully deployed.

## ▼ To Install the SAMLv2 Plug-In on Federation Manager 1

**Before You Begin** You must download the SAMLv2 Plug-In and the SAMLv2 Patch 2 onto the Federation Manager 1 host.

To download the SAMLv2 Plug-In, go to the following URL and follow instructions for downloading the plug-in:

<http://www.sun.com/download/products.xml?id=43e00414>

- 1 As a root user, log in to the Federation Manager 1 host.

Change to the directory where you unpacked the SAMLv2 installation files. Example:

```
# cd /tmp/saml2  
# ls  
./                               SUNWsaml2/
```

```

../                                saml2setup*
ENTITLEMENT.TXT                    saml2silent
LICENSE.TXT                          samlv2-1.0-solaris-sparc.tar
README.TXT                           version

```

## 2 In a different directory, make a copy of the `saml2silent` file.

For this deployment example, no changes are made to the `saml2silent` file. All default values contained in the `saml2silent` file are used during installation. If you changed anything in the `fmsilent` other than the changes described in the section “[To Install Federation Manager Server 1](#)” on page 44, you should reflect the same changes in the `saml2silent` file.

## 3 Run the SAMLv2 installer.

```

# cd /tmp/saml2
# ./saml2setup install -s saml2silent

```

When installation is complete, you will see the following message:

```

To complete the installation of SAML2 you must deploy the war file.
Refer to the web container documentation
or the release notes for directions on deploying a war file.

```

Do not deploy the Federation Manager WAR file as instructed in the onscreen message. Instead, complete the following step and then proceed directly to the next task, “[To Install SAMLv2 Patch 2 on Federation Manager 1](#)” on page 47.

## 4 Restart the Federation Manager server, and verify that you can successfully access it.

```

# /opt/SUNWwbsvr/https-FederationManager-1.siroe.com
# ./stop; ./start

```

# ▼ To Install SAMLv2 Patch 2 on Federation Manager 1

**Before You Begin** To download the SAMLv2 Patch 2, go to one of the following URLs and follow instructions for downloading the patch for your operating system:

- Solaris (sparc) 122983-02  
<http://sunsolve.sun.com/search/document.do?assetkey=1-21-122983-02-1>
- Solaris (x86) 122984-02  
<http://sunsolve.sun.com/search/document.do?assetkey=1-21-122984-02-1>
- Linux 122985-02  
<http://sunsolve.sun.com/search/document.do?assetkey=1-21-122985-02-01>

**1 Go to the directory where you downloaded and unpacked the SAMLv2 patch installation file.**

```
#cd /temp/saml2patch/122983-02
#ls
LEGAL_LICENSE.TXT
LICENSE.TXT
patchinfo
postbackout
postpatch
prebackout
prepatch
README.122983-02
rel_notes.html
SUNWsaml2
```

**2 Run the SAMLv2 patch installer.**

The `—G` option in the following example is for Solaris 10 zones. The option is not necessary if you are not using the Solaris 10 platform.

```
# cd /temp/saml2patch
# patchadd -G 122983-02
```

When installation is complete, you will see the following message:

```
Patch packages installed:
        SUNWsaml2
```

**3 Go to the directory where the `saml2silent` file is located.**

```
# cd /opt/SUNWam/saml2/bin
```

**4 Run the update command.**

```
# ./saml2setup update -s /opt/SUNWam/saml2/bin/saml2silent
```

Any updates required because of the newly-installed patch are made in SAMLv2.

**5 Redeploy the Federation Manager 1 WAR file.**

At this point, the Federation Manager WAR file has been updated with SAMLv2 and SAMLv2 patch configurations. Once the WAR file is updated, you must deploy the WAR file.

See [“To Regenerate and Redeploy the Federation Manager 1 WAR File”](#) on page 107.



## 3.2 Installing and Configuring Federation Manager 2

Use the following as your checklist for installing and configuring Federation Manager 2:

1. [Install the Web Server for Federation Manager 2.](#)
2. [Install Federation Manager Server 2.](#)
3. [Deploy the Federation Manager 2 WAR file.](#)
4. [Install the SAMLv2 Plug-In on Federation Manager 2.](#)
5. [Install the SAMLv2 Patch 2 on Federation Manager 2.](#)

### ▼ To Install the Web Server for Federation Manager 2

**Before You Begin** The Java ES installer must be mounted on the host computer system where you will install Web Server. See the section [“2.2 Downloading and Mounting the Java Enterprise System 2005Q4 Installer” on page 32](#) in this manual.

- 1 **As a root user, log into the Web Server host.**
- 2 **Start the Java Enterprise System installer with the `-nodisplay` option.**

```
# cd /mnt/Solaris_sparc
# ./installer -nodisplay
```

- 3 **When prompted, provide the following information:**

Welcome to the Sun Java(TM) Enterprise System; serious software made simple... <Press ENTER to Continue>	Press Enter.
<Press ENTER to display the Software License Agreement>	Press Enter.
Have you read, and do you accept, all of the terms of the preceding Software License Agreement [No]	Enter <b>y</b> .
Please enter a comma separated list of languages you would like supported with this installation [8]	Enter 8 for “English only.”
Enter a comma separated list of products to install, or press R to refresh the list [ ]	Enter <b>3</b> to select Web Server.
Press "Enter" to Continue or Enter a comma separated list of products to deselect... [1]	Press Enter.

Enter 1 to upgrade these shared components and 2 to cancel [1]	You are prompted to upgrade shared components only if the installer detects that an upgrade is required.  Enter <b>1</b> to upgrade shared components.
Enter the name of the target installation directory for each product: Web Server [/opt/SUNWwbsvr] :	Accept the default value.
System ready for installation Enter 1 to continue [1]	Enter <b>1</b> .
1. Configure Now - Selectively override defaults or express through 2. Configure Later - Manually configure following installation Select Type of Configuration [1]	Enter <b>1</b> .
Common Server Settings Enter Host Name [FederationManager-2]	Accept the default value.
Enter DNS Domain Name [siroe.com]	Accept the default value.
Enter IP Address [192.18.87.180]	Accept the default value.
Enter Server admin User ID [admin]	Enter <b>admin</b> .
Enter Admin User's Password (Password cannot be less than 8 characters) []	For this example, enter <b>admin123</b> .
Confirm Admin User's Password []	Enter the same password to confirm it.
Enter System User [root]	Accept the default value.
Enter System Group [root]	Accept the default value.
Enter Server Admin User ID [admin]	Accept the default value.
Enter Admin User's Password []	For this example, enter <b>admin123</b> .
Enter Host Name [FederationManager-2.siroe.com]	Accept the default value.
Enter Administration Port [8888]	Accept the default value.
Enter Administration Server User ID [root]	Accept the default value.
Enter System User ID [webservd]	Enter <b>root</b> .
Enter System Group [webservd]	Enter <b>root</b> .

Enter HTTP Port [80]	Enter <b>8080</b> .
Enter content Root [/opt/SUNWwbsvr/docs]	Accept the default value.
Do you want to automatically start Web Server when system re-starts.(Y/N) [N]	Accept the default value.
Ready to Install 1. Install 2. Start Over 3. Exit Installation What would you like to do [1]	First, see the next numbered (Optional) step. When ready to install, enter <b>1</b> .

**4 (Optional) During installation, you can monitor the log to watch for installation errors. Example:**

```
# cd /var/sadm/install/logs
# tail -f Java_Enterprise_System_install.B xxxxxx
```

**5 Upon successful installation, enter ! to exit.**

**6 Verify that the Web Server is installed properly.**

**a. Start the Web Server administration server to verify it starts with no errors.**

```
# cd /opt/SUNWwbsvr/https-admserv
# ./stop; ./start
```

**b. Run the netstat command to verify that the Web Server ports are open and listening.**

```
# netstat -an | grep 8888
*.8888      *.*          0           0   49152       0   LISTEN
```

**c. Start a browser, and go to the Web Server administration URL.**

```
http://FederationManager-2.siroe.com:8888
```

**d. Log in to the Web Server console.**

```
Username    admin
Password    admin123
```

You should be able to see the Web Server console. You can log out of the console now.

**e. Start the Web Server instance.**

```
# cd /opt/SUNWwbsvr/https-FederationManager-2.siroe.com
# ./stop; ./start
```

**f. Go to the Web Server instance URL.**

```
http://FederationManager-2.siroe.com:8080
```

You should see the default Web Server index page.

## ▼ To Install Federation Manager Server 2

**Before You Begin** If you have installed Solaris 10 using a distribution package other than the Solaris Enterprise distribution package, then you must remove the SUNWjas and SUNWjato packages that were automatically installed for you. These packages are different versions than the SUNWjas and SUNWjato packages used by Federation Manager. The appropriate packages will be installed when you run the Federation Manager installer.

**1 Download the Sun Java System Federation Manager program from the following page on the Sun Microsystems website:** <http://www.sun.com/download/products.xml?id=44a5bbb5>

**2 Unpack the Federation Manager installer.**

```
# tar -xvf fm-7.0-domestic-us.sparc-sun-solaris2.8.tar
```

```
# ls
LICENSE.TXT
README.TXT
SUNWamfm
common
fm-7.0-domestic-us.sparc-sun-solaris2.8.tar
fmsetup
fmsilent-template
```

**3 Edit the `download_directory//fmfmsilent` file.**

Make a backup of the `fmsilent-template` file, and then set the following properties in the file:

```
FM_PROCESS_USER=root
FM_PROCESS_GROUP=root
INST_ORGANIZATION=o=siroe.com
SERVER_HOST=FederationManager-2.siroe.com
SERVER_PORT=8080
ADMINPASSWD=11111111
```

**4 Save the file as `/export/fmsilent`.**

**5 (Optional) For online help regarding the Federation Manager installer options, enter the following with no options:**

```
# ./fmsetup
```

**6 To start the Federation Manager installer, run the following command:**

```
# ./fmsetup install -s /export/fmsilent
```

**Next Steps** The Federation Manager installer creates the following web archive (WAR) file:

```
/var/opt/SUNWam/fm/war_staging/federation.war
```

You usually customize the Federation Manager WAR file for the environment before the WAR file can be deployed. In a deployment where SAMLv2 is not used, you could customize and deploy the Federation Manager WAR file now. However in this deployment example, you will install the SAMLv2 plug-in and the SAMLv2 patch *before* you customize the Federation Manager WAR file. So proceed directly to the next task, “[To Deploy the Federation Manager 2 WAR File](#)” on page 53.

## ▼ To Deploy the Federation Manager 2 WAR File

- 1 Go to the Web Server directory that contains the `wdeploy` command:

```
# cd /opt/SUNWwbsvr/bin/https/bin
```

- 2 Run the `wdeploy` command:

```
# ./wdeploy deploy -u /federation -i FederationManager-2.siroe.com
-v https-FederationManager-2.siroe.com
/var/opt/SUNWam/fm/war_staging/federation.war
```

- 3 Verify that the WAR file was successfully deployed.

- a. Verify that a directory has been created with the same name you specified during Federation Manager installation as the URI. In this deployment example, the directory is named `federation`.

```
# cd /opt/SUNWwbsvr/https-FederationManager-2.siroe.com/
webapps/https-FederationManager-2.siroe.com/federation
# ls
META-INF      config        docs          html          js
WEB-INF       console      fed_css      images        saml2
com_sun_web_ui  css        fed_images  index.html   samples
```

- b. Restart the Federation Manager server, and verify that you can successfully access it.

```
# cd /opt/SUNWwbsvr/https-FederationManager-2.siroe.com
# ./stop; ./start
```

- c. In a browser, go to the following URL:

```
http://FederationManager-2.siroe.com:8080/federation/UI/Login
```

- d. Log in to the Federation Manager console:

```
User Name:   amadmin
Password:   11111111
```

If you can successfully log in, then the Federation Manager WAR file has been successfully deployed.

## ▼ To Install the SAMLv2 Plug-In on Federation Manager 2

**Before You Begin** To download the SAMLv2 Plug-In, go to the following URL and follow instructions for downloading the plug-in:

<http://www.sun.com/download/products.xml?id=43e00414>

### 1 As a root user, log in to the Federation Manager 2 host.

Change to the directory where you unpacked the SAMLv2 installation files. Example:

```
# cd /tmp/saml2
# ls
./                SUNWsaml2/
../              saml2setup*
ENTITLEMENT.TXT  saml2silent
LICENSE.TXT       samlv2-1.0-solaris-sparc.tar
README.TXT        version
```

### 2 In a different directory, make a copy of the `saml2silent` file.

For this deployment example, no changes are made to the `saml2silent` file. All default values contained in the `saml2silent` file are used during installation. If you changed anything in the `fmsilent` other than the changes described in the section “[To Install Federation Manager Server 2](#)” on page 52, you should reflect the same changes in the `saml2silent` file.

### 3 Run the SAMLv2 installer.

```
# cd /tmp/saml2
# ./saml2setup install -s saml2silent
```

When installation is complete, you will see the following message:

```
To complete the installation of SAML2 you must deploy the war file.
Refer to the web container documentation
or the release notes for directions on deploying a war file.
```

Do not deploy the Federation Manager WAR file as instructed in the onscreen message. Instead, complete the following step and then proceed directly to the next task, “[To Install the SAMLv2 Patch 2 on Federation Manager 2](#)” on page 55.

**4 Restart the Federation Manager server, and verify that you can successfully access it.**

```
# /opt/SUNWwbsvr/https-FederationManager-2.siroe.com
# ./stop; ./start
```

## ▼ To Install the SAMLv2 Patch 2 on Federation Manager 2

**Before You Begin** To download the SAMLv2 Patch 2, go to the following URL and follow instructions for downloading the patch:

- Solaris (sparc) 122983-02  
<http://sunsolve.sun.com/search/document.do?assetkey=1-21-122983-02-1>
- Solaris (x86) 122984-02  
<http://sunsolve.sun.com/search/document.do?assetkey=1-21-122984-02-1>
- Linux 122985-02  
<http://sunsolve.sun.com/search/document.do?assetkey=1-21-122985-02-01>

**1 Go to the directory where you downloaded and unpacked the SAMLv2 patch installation file.**

```
#cd /temp/saml2patch/122983-02
#ls
LEGAL_LICENSE.TXT
LICENSE.TXT
patchinfo
postbackout
postpatch
prebackout
prepatch
README.122983-01
rel_notes.html
SUNWsaml2
```

**2 Run the SAMLv2 patch installer.**

The `—G` option is for Solaris 10 zones. If you are not using the Solaris 10 platform, do not use the `—G` option.

```
# cd /temp/saml2patch
# patchadd -G 122983-02
```

When installation is complete, you will see the following message:

```
Patch packages installed:
        SUNWsaml2
```

**3 Go to the directory where the SAMLv2 `saml2silent` file is located.**

```
# cd /opt/SUNWam/saml2/bin
```

**4 Run the `update` command.**

```
# ./saml2setup update -s /opt/SUNWam/saml2/bin/saml2silent
```

**5 Redeploy the Federation Manager 2 WAR file.**

At this point, the Federation Manager WAR file has been updated with SAMLv2 and SAMLv2 patch configurations. The next step is to deploy the WAR file.

See [“To Regenerate and Redeploy the Federation Manager 2 WAR File” on page 113.](#)

## 3.3 Configuring the Federation Manager Load Balancer

In this phase of the deployment, you set up Load Balancer 9 to manage Federation Manager requests. For more information about the f-5 Networks BIG-IP load balancers used in this deployment, see [“2.9 Setting Up Load Balancer Hardware and Software” on page 37](#) in this manual.

Use the following as your checklist for configuring the Federation Manager Load Balancer:

1. [Configure Load Balancer 9 for the Federation Manager Servers.](#)
2. [Configure Federation Manager 1 to work with the Federation Manager Load Balancer.](#)
3. [Configure Federation Manager 2 to work with the Federation Manager Load Balancer.](#)
4. [Verify that the Federation Manager load balancers are working properly.](#)

### ▼ To Configure Load Balancer 9 for the Federation Manager Servers

- Before You Begin**
- Contact your network administrator to obtain an available virtual IP address for the load balancer you want to configure.

You must also know the IP address of the load balancer hardware, the URL for the load balancer login page, and a username and password for logging in to the load balancer application.

---

**Note** – The load balancer hardware and software used in the lab facility for this deployment is BIG-IP® manufactured by F5 Networks. If you are using different load balancer software, see the documentation that comes with that product for detailed settings information.

---



- You must also have ready the IP addresses for Federation Manager 1 and Federation Manager 2.

To obtain these IP addresses, on each Federation Manager host, run the following command:

```
ifconfig -a
```

## 1 Create a Pool.

A pool contains all the backend server instances.

- a. Go to URL for the Big IP load balancer login page.

- b. Open the Configuration Utility.

Click “Configure your BIG-IP (R) using the Configuration Utility.”

- c. In the left pane, click Pools.

- d. On the Pools tab, click the Add button.

- e. In the Add Pool dialog, provide the following information:

Pool Name                      Example: fm\_server\_pool

Load Balancing Method      Round Robin

Resources                      Add the IP address of both Federation Manager hosts. In this example:

**192.18.72.89** (for Federation Manager 1)

**192.18.72.86** (for Federation Manager 2)

- f. Click the Done button.

## 2 Add a Virtual Server.

If you encounter Javascript errors or otherwise cannot proceed to create a virtual server, try using Microsoft Internet Explorer for this step.

- a. In the left frame, Click Virtual Servers.

- b. On the Virtual Servers tab, click the Add button.

- c. In the Add a Virtual Server dialog box, provide the following information:

Address      **192.18.69.14** (for LoadBalancer-9.siroe.com )

Service      **1080**

- d. **Continue to click Next until you reach the Select Physical Resources page.**

Select Pool, and then choose `fm_server_pool` from the drop-down list.

- e. **On the same page, set the Cookie Name property to `fm_lbcookie`.**

- f. **Click the Done button.**

**3 Configure the load balancer for persistence.**

- a. **In the left frame, click Pools.**

- b. **Click the name of the pool you want to configure.**

In this example, `fm_server_pool`.

- c. **Click the Persistence tab.**

- d. **On the Persistence tab, under Persistence Type, select Active HTTP Cookie and set the following:**

Method: **Insert**

When the Insert method is specified, the first time a server receives a request, the load balancer inserts a cookie and cookie value. On subsequent requests, when the load balancer sees the same cookie name and value, it redirects the request to the same server that received the initial request.

- e. **Click Apply.**

**4 Create a new monitor.**

This monitor will simply indicate whether the Federation Manager servers are running or stopped.

- a. **Click the Monitors tab.**

- b. **Click the Add.**

- c. **In the Name and Parent window, provide the following information, and then click Next.**

Name **fm\_servers\_monitor**

Inherits From **http**

- d. **In the Basic Properties window, accept the default values, and then click Next.**

Interval **5**

Timeout 16

- e. **In the Configure Destination Address and Service window, accept the default values and then click Done.**

The new monitor is added to the list on the Monitors tab.

**5 Click the Basic Associations tab.**

- a. **Find the IP addresses for Federation Manager 1 and for Federation Manager 2**

In this example: 192 . 18 . 72 . 89 for Federation Manager 1, and 192 . 18 . 82 . 86 for Federation Manager 2.

- b. **In the Node dropdown list, select `fm_servers_monitor`.**

- c. **Mark the ADD box for each IP address, and then click APPLY.**

When you click Nodes in the left frame of the console, you will be able to see if each server is running or stopped.

## ▼ To Configure Federation Manager 1 to Work with the Federation Manager Load Balancer

- 1 **As a root user, log in to the Federation Manager 1 host.**

- 2 **Go to the directory that contains the `AMConfig.properties` file.**

```
# cd /var/opt/SUNWam/fm/war_staging/web-src/WEB-INF/classes
```

- 3 **In the `AMConfig.properties` file, set the following property:**

```
com.sun.identity.server.fqdnMap[LoadBalancer-9.siroe.com]=LoadBalancer-9.siroe.com
```

- 4 **Add the following property:**

```
com.sun.identity.url.redirect=https,LoadBalancer-9.siroe.com
```

This property will be used when you terminate SSL at the Federation Manager load balancer.

- 5 **Add the Federation Manager load balancers to the Organization Aliases list.**

- a. **Go to the Federation Manager login URL:**

```
http://Federationmanager-1.siroe.com:8080/federation/UI/Login
```

- b. **Log in to the Federation Manager console:**

User Name: **amadmin**

Password: **11111111**

- c. **Click the Configuration tab. On the General Properties page, Under Organizational Attributes, add the Federation Manager load balancer to the DNS Aliases list.**

In the Add field, enter **LoadBalancer-9.siroe.com**, and then click Add.

Click Save.

- 6 **Regenerate the Federation Manager WAR file.**

```
#cd /opt/SUNWam/fm/bin
# ./fmwar -n federation -d /var/opt/SUNWam/fm/war_staging -s /export/fmsilent
```

- 7 **Redeploy the Federation Manager WAR file.**

See the section [“To Regenerate and Redeploy the Federation Manager 1 WAR File”](#) on page 107 in this manual.

## ▼ **To Configure Federation Manager 2 to Work with the Federation Manager Load Balancer**

- 1 **As a root user, log in to the Federation Manager 2 host.**

- 2 **Go to the directory that contains the AMConfig.properties file.**

```
# cd /var/opt/SUNWam/fm/war_staging/web-src/WEB-INF/classes
```

- 3 **In the AMConfig.properties file, set the following properties:**

```
com.sun.identity.server.fqdnMap[LoadBalancer-9.siroe.com]=LoadBalancer-9.siroe.com
```

- 4 **Add the following property:**

```
com.sun.identity.url.redirect=https,LoadBalancer-9.siroe.com
```

This property will be used when you terminate SSL at the Federation Manager load balancer.

- 5 **Add the Federation Manager load balancers to the Organization Aliases list.**

- a. **Go to the Federation Manager login URL:**

```
http://FederationManager-2.siroe.com:8080/federation/UI/Login
```

- b. **Log in to the Federation Manager console:**

User Name: **amadmin**

Password: **11111111**

- c. **Click the Organization tab. Under Organization Attributes, add the Federation Manager load balancers to the DNS Aliases list.**

In the Add field, enter **LoadBalancer-9.siroe.com**, and then click Add.

Click Save.

- 6 **Regenerate the Federation Manager 2 WAR file.**

See the section in this manual, [“To Regenerate and Redeploy the Federation Manager 2 WAR File” on page 113.](#)

## ▼ **To Verify that the Federation Manager Load Balancers are Working Properly**

- 1 **Use the tail command to monitor traffic requests to Federation Manager 1 and Federation Manager 2.**

- a. **As a root user, log in to the Federation Manager 1 host.**

- b. **Restart the Federation Manager 1 server:**

```
# cd / FederationManager-base/SUNWwbsvr/https-FederationManager-2.siroe.com
# ./stop; ./start
```

- c. **Use the tail command to monitor the Federation Manager access log.**

```
# tail -f logs/access
```

- d. **As a root user, log in to the Federation Manager 2 host.**

- e. **Start the Federation Manager 2 server:**

```
# cd FederationManager-base/SUNWwbsvr/https-FederationManager-2.siroe.com
# ./stop; ./start
```

- f. **Use the tail command to monitor the Directory Server access log.**

```
# tail -f logs/access
```

- 2 **Go to the following Federation Manager URL:**

<http://LoadBalancer-9.siroe.com:1080/federation/UI/Login>

- 3 **Log in to the Federation Manager console:**

User Name: **amadmin**

Password: **11111111**

As you log in and log out of the Federation Manager console, you should see in the access log that all requests are going to the same Federation Manager server. This indicates that the load balancer is working properly, and that the persistence setting is properly configured.

## 3.4 Configuring SSL Termination at the Federation Manager Load Balancer

In this deployment, SSL is not enabled at each Federation Manager server but is instead terminated at the load balancer. By terminating SSL at the load balancer, you can be sure that communication to the Federation Manager servers is secure while achieving the highest server availability and fastest response times.

Use the following as your checklist for configuring SSL termination at the Federation Manager load balancer:

1. [Request an SSL certificate.](#)
2. [Install the SSL certificate.](#)
3. [Configure the Web Server 1 for SSL termination.](#)
4. [Configure the Web Server 2 for SSL termination.](#)
5. [Verify that SSL on the Federation Manager load balancer is working properly.](#)

### ▼ To Request an SSL Certificate

- 1 **Log in to the BIG-IP load balancer.**
- 2 **Click Proxies in the left pane.**
- 3 **Click the Cert Admin tab, and then click the “Generate New Key Pair/ Certificate Request” button.**
- 4 **In the Create Certificate Request page, provide the following information:**
  - Key Identifier: **LoadBalancer-9.siroe.com**
  - Organization: **siroe.com**
  - Domain Name: **LoadBalancer-9.siroe.com**
  - Email Address: **jdoe@siroe.com**
- 5 **Click the Generate Request button.**

**6 In the Generate Request page, copy the request that looks similar to this:**

```

-----BEGIN CERTIFICATE REQUEST-----
Ubm77e50M63v1Z2A/505MA0GCSqGSIb3DQE0BAU
AMF8xCzAJBgNVBAYTAlVTMSAwHgYDVQKExdSU0
EgRGF0YSBTZW51cm10eSwgSW5jLjEuMCwGA1UEC
xMlU2VjdXJlIFNlcnZlciBDZXJ0aWZpY2F0aW9u
IEF1dGhvcml0eTAeFw0wMTA4MDIwMDAwMDBaFw0
wMzA4MDIyMzU5NTlaMIGQMqswCQYDVQGEwJVUz
ERMA8GA1UECBMlYmlyZ2luaWExETAPBgNVBACUC
FJpY2htb25kMSAwHgYDVQKFBdYXZhbGllciBU
ZWxlcGhvYm9uZGluZy5jYXZ0ZWwuY29tMIGfMA0
GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8x/1dxo
2YnblilQLmpiezi0qb7ArVfI1ymXo/MKcbKjnY2
-----END CERTIFICATE REQUEST-----

```

**7 Paste this text into a request form provided by a root certificate authority (CA) such as Verisign or Thwarte.**

See the certificate authority website such as <http://www.verisign.com/> or <http://www.thawte.com/> for detailed instructions on submitting a certificate request.

**▼ To Install the SSL Certificate**

After you receive the certificate from the issuer, install the SSL Certificate.

**1 Log in to the BIG-IP load balancer console.**

a. In the BIG-IP load balancer console, click the Cert Admin tab.

b. On the Cert Admin tab, click Install Certificate.

c. In the Install SSL Certificate page, paste the certificate text you received from the certificate issuer. Example:

```

-----BEGIN CERTIFICATE REQUEST-----
Ubm77e50M63v1Z2A/505MA0GCSqGSIb3DQE0BAU
AMF8xCzAJBgNVBAYTAlVTMSAwHgYDVQKExdSU0
EgRGF0YSBTZW51cm10eSwgSW5jLjEuMCwGA1UEC
xMlU2VjdXJlIFNlcnZlciBDZXJ0aWZpY2F0aW9u
IEF1dGhvcml0eTAeFw0wMTA4MDIwMDAwMDBaFw0
wMzA4MDIyMzU5NTlaMIGQMqswCQYDVQGEwJVUz
ERMA8GA1UECBMlYmlyZ2luaWExETAPBgNVBACUC
FJpY2htb25kMSAwHgYDVQKFBdYXZhbGllciBU
ZWxlcGhvYm9uZGluZy5jYXZ0ZWwuY29tMIGfMA0
GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8x/1dxo

```

```
2YnblilQLmpiEzi0qb7ArVfI1ymXo/MKcbKjnY2
-----END CERTIFICATE REQUEST-----
```

**d. Click Install Certificate.**

**2 In the left frame, click Proxies, and then click Add.**

**3 On the Add Proxy page, provide the following information:**

Proxy Type: SSL  
Proxy Address: Enter the IP address of LoadBalancer-9.siroe.com.  
Proxy Service: Enter 3443.  
Destination Address: Enter the IP address of LoadBalancer-9.siroe.com.  
Destination Service: Enter 1080.  
SSL Certificate: LoadBalancer-9.siroe.com  
SSL Key: LoadBalancer-9.siroe.com  
Enable ARP: Mark this box.  
Click Next, then provide the following information:  
Rewrite Redirects: Choose **Matching**.  
Click Done.

## ▼ To Configure the Web Server 1 for SSL Termination

**1 As a root user, log in to the Federation Manager 1 host.**

**2 Go to the following directory:**

```
/opt/SUNWwbsvr/https-FederationManager-1.siroe.com/config
```

**3 Modify the server.xml file.**

Make a backup of server.xml, and then modify the original file. Change this line:

```
<LS id="ls1" port="8080" servername="FederationManager-1.siroe.com" defaultvs ...
```

to:

```
<LS id="ls1" port="8080" servername="https://LoadBalancer-9.siroe.com" defaultvs ...
```

Save the file.



**4 Restart the Web Server.**

```
# cd /opt/SUNWwbsvr/https-FederationManager-1.siroe.com/
# ./stop ; ./start
```

**▼ To Configure the Web Server 2 for SSL Termination****1 As a root user, log in to the Federation Manager 2 host.****2 Go to the following directory:**

```
/opt/SUNWwbsvr/https-FederationManager-2.siroe.com/config
```

**3 Modify the server.xml file.**

Make a backup of server.xml, and then modify the original file. Change this line:

```
<LS id="ls1" port="8080" servername="FederationManager-2.siroe.com" defaultvs ...
```

to:

```
<LS id="ls1" port="8080" servername="https://LoadBalancer-9.siroe.com" defaultvs ...
```

Save the file.

**4 Restart the Web Server.**

```
# cd /opt/SUNWwbsvr/https-FederationManager-2.siroe.com/
# ./stop ; ./start
```

**▼ To Verify that SSL on the Federation Manager Load Balancer is Working Properly****1 Go to the Federation Manager URL:**

```
https://LoadBalancer-9.siroe.com:3443/federation/UI/Login
```

The following message is displayed:

“Unable to verify the identity of LoadBalancer-9.siroe.com as a trusted site.”

**2 Choose “Accept this certificate temporarily for this session,” and then click OK.****3 Log in to the Federation Manager console:**

User Name: **amadmin**

Password: **11111111**

If you can log in successfully, then SSL is configured properly.

# Installing and Configuring the Directory Servers

---

This chapter contains detailed information about the following groups of tasks:

- “4.1 Installing Two Directory Servers” on page 67
- “4.2 Creating New Directory Server Instances” on page 74
- “4.3 Enabling Multi-Master Replication of the Configuration Instances” on page 79
- “4.4 Enabling Multi-Master Replication of the User Data Instances” on page 86
- “4.5 Configuring the Directory Server Load Balancers” on page 93

## 4.1 Installing Two Directory Servers

The Java ES installer must be mounted on the host computer system where you will install Directory Server. See the section “2.2 Downloading and Mounting the Java Enterprise System 2005Q4 Installer” on page 32 in this manual.

Use the following as your checklist or installing two Directory Server:

1. [Install Directory Server 3SP.](#)
2. [Install Directory Server 4SP.](#)

### ▼ To Install Directory Server 3SP

- 1 As a root user, log in to the Directory Server 3SP host.
- 2 Start the installer with the `nodisplay` option. Example:

```
# cd /mnt/Solaris_sparc
# ./installer -nodisplay
```

### 3 When prompted, provided the following information:

Welcome to the Sun Java(TM) Enterprise System; serious software made simple... <Press ENTER to Continue>	Press Enter.
<Press ENTER to display the Software License Agreement>	Press Enter.
Have you read, and do you accept, all of the terms of the preceding Software License Agreement?	Enter <b>y</b> .
Please enter a comma separated list of languages you would like supported with this installation	Enter <b>8</b> to select "English only."
Enter a comma separated list of products to install, or press R to refresh the list.	Enter <b>6, 20</b> . Be sure you've specified Sun Java System Administration Server 5 2005Q4 and Sun Java System Directory Server 5 2005Q4.
Press "Enter" to Continue or Enter a comma separated list of products to deselect.	Press Enter.
Enter <b>1</b> to upgrade these shared components and <b>2</b> to cancel.	If upgrades are required, enter <b>1</b> to upgrade shared components.
Enter the name of the target installation directory for each product:	Accept the default value for each product.
System ready for installation...	Enter <b>1</b> to continue.
Select Type of Configuration	Enter <b>1</b> to configure now.
Enter Host Name [DirectoryServer-3SP]	Accept the default value.
Enter DNS Domain Name [siroe.com]	Accept the default value.
Enter IP Address [10.5.82.207]	Accept the default value.
Enter Server admin User ID [admin]	Accept the default value.
Enter Admin User's Password (Password cannot be less than 8 characters)	For this example, enter <b>admin123</b> .
Confirm Admin User's Password [ ]	Enter the same password again.
Enter System User [root]	Accept the default value.
Enter System Group [root]	Accept the default value.
Enter Server Admin ID [admin]	Accept the default value.

Enter Admin User's Password (At least 8 characters long)	For this example, enter <b>admin123</b> .
Retype Password []	Enter the same password again.
Enter Directory Manager DN [cn=Directory Manager]	Accept the default value.
Enter Directory Manager's Password (At least 8 characters long)	For this example, enter <b>11111111</b> .
Retype Password []	Enter the same password again.
Directory Server Root [/var/opt/mps/serverroot]	Accept the default value.
Enter Server Identifier [DirectoryServer-3SP]	Accept the default value.
Enter Server Port [390]	Enter <b>1390</b> .
Enter a valid Suffix [siroe.com]	Enter <b>dc=siroe,dc=com</b> .
Enter Administration Domain [siroe.com]	Accept the default value.
Enter System User [root]	Accept the default value.
Enter System Group [root]	Accept the default value.
This server's configuration can be stored in this new directory server or in another previously prepared configuration server.	Enter <b>1</b> to choose "The new instance will be the configuration directory server."
This server can store its own user data and group data, or it can access user data and group data from another instance of directory server.	Enter <b>1</b> to store data in the new directory server.
The new directory server can be populated with sample or real data.	Enter <b>4</b> to choose "Populate with no data."
Do you wish to disable Schema Checking when importing data?	Enter <b>n</b> .
Enter the Server Root [/var/opt/mps/serverroot]	Accept the default value.
Enter the Administration Port [390]	Enter <b>1391</b> .
Enter the Administration Domain [siroe.com]	Accept the default value.
Enter System User [root]	Accept the default value.

Enter System Group [root]	Accept the default value.
Enter Administration ID for Configuration Server Administration ID[admin]	Accept the default value.
Enter the admin Password []	For this example, enter <b>admin123</b> .
Enter the Configuration Directory Host [DirectoryServer-3SP.siroe.com]	Accept the default value.
Enter the Configuration Directory Port [1390]	Accept the default value.
Ready to Install. The following components will be installed: Directory Server Preparation Tool Directory Server 5 Administration Server	Enter <b>1</b> to install now.

**4 (Optional) During installation, you can monitor the log to watch for installation errors. Example:**

```
# cd /var/sadm/install/logs
# tail -f Java_Enterprise_System_install.B xxxxxx
```

**5 Upon successful installation, enter ! to exit.**

**6 Verify that Directory Server was successfully installed.**

**a. As a root user, log in to Directory Server 3SP.**

**b. Start the Directory Server.**

```
# cd /var/opt/mps/serverroot/slapd-DirectoryServer-3SP
# ./stop-slapd; ./start-slapd
```

**c. Use the tail command to monitor the Directory Server error log and see that the server successfully starts up.**

```
# tail -50 logs/errors
```

**d. Use the netstat command to verify that the Directory Server port is open and listening.**

```
# netstat -an | grep 1390
* 1390          *.*           0             0 49152         0 LISTEN
```

**e. Start the Administration Server that manages Directory Server.**

```
cd /var/opt/mps/serverroot
./stop-admin; ./start-admin
```

Installation is successful if the Administration Server displays a start-up message.

- f. Use the `netstat` command to verify that the Administration Server port is open and listening.

```
# netstat -an | grep 1391
* 1391          *.*          0           0 49152        0 LISTEN
```

## ▼ To Install Directory Server 4SP

- 1 As a root user, log in to the Directory Server 4SP host.
- 2 Start the installer with the `nodisplay` option. Example:
 

```
# cd /mnt/Solaris_sparc
# ./installer -nodisplay
```
- 3 When prompted, provided the following information:

Welcome to the Sun Java(TM) Enterprise System; serious software made simple... <Press ENTER to Continue>	Press Enter.
<Press ENTER to display the Software License Agreement>	Press Enter.
Have you read, and do you accept, all of the terms of the preceding Software License Agreement?	Enter <b>y</b> .
Please enter a comma separated list of languages you would like supported with this installation	Enter <b>8</b> to select "English only."
Enter a comma separated list of products to install, or press R to refresh the list.	Enter <b>6, 20</b> . Be sure you've specified Sun Java System Administration Server 5 2005Q4 and Sun Java System Directory Server 5 2005Q4.
Press "Enter" to Continue or Enter a comma separated list of products to deselect.	Press Enter.
Enter <b>1</b> to upgrade these shared components and <b>2</b> to cancel.	If upgrades are required, enter <b>1</b> to upgrade shared components.
Enter the name of the target installation directory for each product:	Accept the default value for each product.
System ready for installation...	Enter <b>1</b> to continue.

Select Type of Configuration	Enter <b>1</b> to configure now.
Enter Host Name [DirectoryServer-4SP]	Accept the default value.
Enter DNS Domain Name [siroe.com]	Accept the default value.
Enter IP Address [10.5.82.207]	Accept the default value.
Enter Server admin User ID [admin]	Accept the default value.
Enter Admin User's Password (Password cannot be less than 8 characters)	For this example, enter <b>admin123</b> .
Confirm Admin User's Password []	Enter the same password again.
Enter System User [root]	Accept the default value.
Enter System Group [root]	Accept the default value.
Enter Server Admin ID [admin]	Accept the default value.
Enter Admin User's Password (At least 8 characters long)	For this example, enter <b>admin123</b> .
Retype Password []	Enter the same password again.
Enter Directory Manager DN [cn=Directory Manager]	Accept the default value.
Enter Directory Manager's Password (At least 8 characters long)	For this example, enter <b>11111111</b> .
Retype Password []	Enter the same password again.
Directory Server Root [/var/opt/mps/serverroot]	Accept the default value.
Enter Server Identifier [DirectoryServer-4SP]	Accept the default value.
Enter Server Port [390]	Enter <b>1390</b> .
Enter a valid Suffix [siroe.com]	Enter <b>dc=siroe,dc=com</b> .
Enter Administration Domain [siroe.com]	Accept the default value.
Enter System User [root]	Accept the default value.
Enter System Group [root]	Accept the default value.
This server's configuration can be stored in this new directory server or in another previously prepared configuration server.	Enter <b>1</b> to choose "The new instance will be the configuration directory server."



This server can store its own user data and group data, or it can access user data and group data from another instance of directory server.	Enter <b>1</b> to store data in the new directory server.
The new directory server can be populated with sample or real data.	Enter <b>4</b> to choose “Populate with no data.”
Do you wish to disable Schema Checking when importing data?	Enter <b>n</b> .
Enter the Server Root [/var/opt/mps/serverroot]	Accept the default value.
Enter the Administration Port [390]	Enter <b>1391</b>
Enter the Administration Domain [siroe.com]	Accept the default value.
Enter System User [root]	Accept the default value.
Enter System Group [root]	Accept the default value.
Enter Administration ID for Configuration Server Administration ID[admin]	Accept the default value.
Enter the admin Password []	For this example, enter <b>admin123</b> .
Enter the Configuration Directory Host [DirectoryServer-4SP.siroe.com]	Accept the default value.
Enter the Configuration Directory Port [1390]	Accept the default value.
Ready to Install. The following components will be installed: Directory Server Preparation Tool Directory Server 5 Administration Server	Enter <b>1</b> to install now.

**4 (Optional) During installation, you can monitor the log to watch for installation errors. Example:**

```
# cd /var/sadm/install/logs
# tail -f Java_Enterprise_System_install.B xxxxxx
```

**5 Upon successful installation, enter ! to exit.**

**6 Verify that Directory Server was successfully installed.**

**a. As a root user, log in to Directory Server 4SP.**

**b. Start the Directory Server.**

```
# cd /var/opt/mps/serverroot/slapd-DirectoryServer-4SP
# ./stop-slapd; ./start-slapd
```

**c. Use the tail command to monitor the Directory Server error log and verify that the server successfully starts up.**

```
# tail -50 logs/errors
```

**d. Use the netstat command to verify that the Directory Server port is open and listening.**

```
# netstat -an | grep 1390
* 1390          *.*          0            0 49152        0 LISTEN
```

**e. Start the Administration Server that manages Directory Server.**

```
cd /var/opt/mps/serverroot
./stop-admin; ./start-admin
```

Installation is successful if the Administration Server displays a start-up message.

**f. Use the netstat command to verify that the Administration Server port is open and listening.**

```
# netstat -an | grep 1391
* 1391          *.*          0            0 49152        0 LISTEN
```

## 4.2 Creating New Directory Server Instances

On each Directory Server, create a new configuration instance and a new user data instance. When you're finished, Directory Server 3SP and Directory Server 4SP will each contain three instances. For example, Directory Server 3SP will contain three instances: `DirectoryServer-3SP`, `fm-config`, and `fm-users`. `DirectoryServer-3SP` stores Directory Server administration configuration. The instance named `fm-config` stores Federation Manager configuration, and the instance named `fm-users` stores Federation Manager user data. Directory Server 4SP will contain the identical directory structure.

Use the following as your checklist for creating new Directory Server instances:

1. [Create a new Configuration Instance in Directory Server 3SP.](#)
2. [Create a new User Data Instance in Directory Server 3SP.](#)
3. [Create a new Configuration Instance in Directory Server 4SP.](#)
4. [Create a new User Data Instance in Directory Server 4SP.](#)

## ▼ To Create a New Configuration Instance in Directory Server 3SP

Create a new data instance for storing Federation Manager configuration. This ensures that if you ever have to uninstall or restore Federation Manager configuration, the Directory Server configuration remains untouched and will not have to be restored.

### 1 As a root user, log in to Directory Server 3SP.

Set the X window display variable, and start the Directory Server 3SP console.

```
# cd /var/opt/mps/serverroot/
# export DISPLAY=DirectoryServer-3SP.siroe.com:1
# ./startconsole &
```

### 2 Log in to the Directory Server 3SP console.

```
Username          cn=Directory Manager
Password          11111111
Administration URL http://DirectoryServer-3SP.siroe.com:1391
```

### 3 In the Directory Server console, under the Servers and Applications tab, expand the Server Administration domain list until you see the Server Group item.

### 4 Right-click on Server Group, and choose "Create an instance of Sun Directory Server."

### 5 In the Create New Instance dialog box, provide the following information:

```
Server identifier:      Enter fm-config.
Network port:          Enter 1389.
Base suffix:           Enter o=siroe.com.
Directory Manager DN:  Enter cn=Directory Manager
Password:              For this example, enter 11111111.
Confirm Password:     Enter the same password to confirm it.
Server Runtime (UNIX) user ID:  Enter root.
```

### 6 Click OK, and then close the status window.

### 7 Verify that the new Directory Server instance named `fm-config` successfully starts up.

#### a. As a root user, log in to Directory Server 3SP.

**b. Start the new data Directory Server instance.**

```
# cd /var/opt/mps/serverroot/slapd-fm-config
# ./stop-slapd; ./start-slapd
```

**c. Use the tail command to monitor the Directory Server error log and see that the server starts up successfully.**

```
# tail -f logs/errors
```

## ▼ To Create a New User Data Instance in Directory Server 3SP

Create a new data instance for storing both Federation Manager configuration and user data. This ensures that if you ever have to uninstall or restore Federation Manager configuration, the Directory Server configuration remains untouched and will not have to be restored.

**1 As a root user, log in to Directory Server 3SP.**

Set the X window display variable, and start the Directory Server console.

```
# cd /var/opt/mps/serverroot/
# export DISPLAY=DirectoryServer-3SP.siroe.com:1
# ./startconsole &
```

**2 Log in to the Directory Server 3SP console.**

```
Username          cn=Directory Manager
Password          11111111
Administration URL http://DirectoryServer-3SP.siroe.com:1391
```

**3 In the Directory Server console, under the Servers and Applications tab, expand the Server Administration domain list until you see the Server Group item.****4 Right-click on Server Group, and choose "Create an instance of Sun Directory Server."****5 In the Create New Instance dialog box, provide the following information:**

```
Server identifier:      Enter fm-users.
Network port:          Enter 1489.
Base suffix:           Enter o=siroeusers.com.
Directory Manager DN:  Enter cn=Directory Manager
Password:              For this example, enter 11111111.
```

Confirm Password: Enter the same password to confirm it.

Server Runtime (UNIX) user ID: Enter **root**.

**6 Click OK, and then close the status window.**

**7 Verify that the new Directory Server instance named `fm-users` successfully starts up .**

**a. As a root user, log in to Directory Server 3SP.**

**b. Start the new data Directory Server instance.**

```
# cd /var/opt/mps/serverroot/slapd-fm-users
# ./stop-slapd; ./start-slapd
```

**c. Use the `tail` command to monitor the Directory Server error log and see that the server starts up successfully.**

```
# tail -f logs/errors
```

## ▼ To Create a New Configuration Instance in Directory Server 4SP

**1 As a root user, log in to Directory Server 4SP.**

Set the X window display variable, and start the Directory Server console.

```
# cd /var/opt/mps/serverroot/
# export DISPLAY=DirectoryServer-4SP.siroe.com:1
# ./startconsole &
```

**2 Log in to the Directory Server 4SP console.**

Username **cn=Directory Manager**

Password **11111111**

Administration URL **http://DirectoryServer-4SP.siroe.com:1391**

**3 In the Directory Server console, under the Servers and Applications tab, expand the Server Administration domain list until you see Server Group item.**

**4 Right-click on Server Group, and choose "Create an instance of Sun Directory Server."**

**5 In the Create New Instance dialog box, provide the following information:**

Server identifier: Enter **fm-config**.

Network port: Enter **1389**.

Base suffix: Enter **o=siroe.com**.

Directory Manager DN: Enter **cn=Directory Manager**

Password: For this example, enter **11111111**.

Confirm Password: Enter the same password to confirm it.

Server Runtime (UNIX) user ID: Enter **root**.

- 6 Click OK, and then close the status window.
- 7 Verify that the new Directory Server instance named `fm-config` successfully starts up .

a. As a root user, log in to Directory Server 4SP.

b. Start the new data Directory Server instance.

```
# cd /var/opt/mps/serverroot/slapd-fm-config
# ./stop-slapd; ./start-slapd
```

c. Use the `tail` command to monitor the Directory Server error log and see that the server starts up successfully.

```
# tail -f logs/errors
```

## ▼ To Create a New User Data Instance in Directory Server 4SP

- 1 As a root user, log in to Directory Server 4SP.

Set the X window display variable, and start the Directory Server console.

```
# cd /var/opt/mps/serverroot/
# export DISPLAY=DirectoryServer-4SP.siroe.com:1
# ./startconsole &
```

- 2 Log in to the Directory Server 4SP console.

```
Username          cn=Directory Manager
Password          11111111
Administration URL http://DirectoryServer-4SP.siroe.com:1391
```

- 3 In the Directory Server console, under the Servers and Applications tab, expand the Server Administration domain list until you see Server Group item.

**4 Right-click on Server Group, and choose “Create an instance of Sun Directory Server.”****5 In the Create New Instance dialog box, provide the following information:**

Server identifier:	Enter <b>fm-users</b> .
Network port:	Enter <b>1489</b> .
Base suffix:	Enter <b>o=siroeusers.com</b> .
Directory Manager DN:	Enter <b>cn=Directory Manager</b>
Password:	For this example, enter <b>11111111</b> .
Confirm Password:	Enter the same password to confirm it.
Server Runtime (UNIX) user ID:	Enter <b>root</b> .

**6 Click OK, and then close the status window.****7 Verify that the new Directory Server instance named `fm-users` successfully starts up .****a. Log in as root to Directory Server 4SP.****b. Start the new data Directory Server instance.**

```
# cd /var/opt/mps/serverroot/slapd-fm-users
# ./stop-slapd; ./start-slapd
```

**c. Use the `tail` command to monitor the Directory Server error log and see that the server starts up successfully.**

```
# tail -f logs/errors
```

## 4.3 Enabling Multi-Master Replication of the Configuration Instances

In this procedure you enable multi-master replication (MMR) between two directory masters. With MMR enabled, whenever a directory entry is changed in Directory Server 3SP, the change is automatically replicated in Directory Server 4SP. The reverse is also true.

Use the following as your checklist for enabling MMR among the configuration instances:

1. [Enable multi-master replication of the Configuration Instance on Directory Server 3SP.](#)
2. [Enable multi-master replication of the Configuration Instance on Directory Server 4SP.](#)
3. [Create a replication agreement for the Configuration Instance on Directory Server 3SP.](#)
4. [Create a replication agreement for the Configuration Instance on Directory Server 4SP.](#)

5. [Initialize the Configuration Instance master replica.](#)

## ▼ To Enable Multi-Master Replication of the Configuration Instance on Directory Server 3SP

**1 Start the Directory Server 3SP console.**

```
# cd /var/opt/mps/serverroot/  
# ./startconsole &
```

**2 Log in to the Directory Server 3SP console.**

```
Username          cn=Directory Manager  
Password          11111111  
Administration URL http://DirectoryServer-3SP.siroe.com:1391
```

**3 In the Directory Server console, under the Servers and Applications tab, expand the Server Administration domain list until you see the Server Group item.****4 Click to expand the Server Group.**

You should see three items: an Administration Server, a Directory Server (fm-config), and a Directory Server (fm-config).

**5 Double-click the instance name Directory Server (fm-config) to display the console for managing the instance fm-config.****6 Click the Configuration tab and navigate to the Replication pane.****a. Expand the Data node.****b. Expand the node for the suffix you want to be a master replica.**

In this example, double-click the suffix `o=siroe.com`.

**c. Click Replication.****7 Click the "Enable replication" button to start the Replication Wizard.****8 Select Master Replica, and then click Next to continue.****9 Enter a Replica ID, and then click Next.**

For this example, when enabling replication on DirectoryServer-3SP, assign the number 11.



- 10 If you have not already been prompted to select the change log file, you are prompted to select one now.**

The default change log file is shown in the text field. If you do not wish to use the default, type in a filename for the change log, or click Browse to display a file selector. If the change log has already been enabled, the wizard will skip this step.

- 11 If you have not already been prompted to enter and confirm a password for the default replication manager, you are prompted now.**

The replication manager is not used in the case of single-master replication, but you must still enter a password to proceed. For this example, enter **11111111**.

- a. Click Next.**

The Replication Wizard displays a status message while updating the replication configuration.

- 12 Click Close when replication is finished.**

## ▼ To Enable Multi-Master Replication of the Configuration Instance on Directory Server 4SP

- 1 Start the Directory Server 4SP console.**

```
# cd /var/opt/mps/serverroot/  
# ./startconsole &
```

- 2 Log in to the Directory Server 4SP console.**

```
Username          cn=Directory Manager  
Password          11111111  
Administration URL http://DirectoryServer-4SP.siroe.com:1391
```

- 3 In the Directory Server console, under the Servers and Applications tab, expand the Server Administration domain list until you see the Server Group item.**

- 4 Click to expand the Server Group.**

You should see three items: an Administration Server, a Directory Server (fm-config), and a Directory Server (fm-users).

- 5 Double-click the instance name Directory Server (fm-config) to display the console for managing the instance fm-config.**

**6 Click the Configuration tab and navigate to the Replication pane.**

**a. Expand the Data node.**

**b. Expand the node for the suffix you want to be a master replica.**

In this example, double-click the suffix `o=siroe.com`.

**c. Click Replication.**

**7 Click the “Enable replication” button to start the Replication Wizard.**

**8 Select Master Replica, and then click Next to continue.**

**9 Enter a Replica ID, and then click Next.**

For this example, when enabling replication on `DirectoryServer-4SP`, assign the number 22.

**10 If you have not already been prompted to select the change log file, you are prompted to select one now.**

The default change log file is shown in the text field. If you do not wish to use the default, type in a filename for the change log, or click `Browse` to display a file selector. If the change log has already been enabled, the wizard will skip this step.

**11 If you have not already been prompted to enter and confirm a password for the default replication manager, you are prompted now.**

The replication manager is not used in the case of single-master replication, but you must still enter a password to proceed. For this example, enter `11111111`.

**a. Click Next.**

The Replication Wizard displays a status message while updating the replication configuration.

**12 Click Close when replication is finished.**

## ▼ **To Create a Replication Agreement for the Configuration Instance on Directory Server 3SP**

**1 On DirectoryServer-3SP, in the Directory Server console, display the general properties for the Directory Server instance named `fm-config`.**

Navigate through the tree in the left panel to find the Directory Server instance named `fm-config`, and click on the instance name to display its general properties.

**2 Click the Open button to display the console for managing the `fm-config` instance.**

**3 Click the Configuration tab and navigate to the Replication pane.**

**a. Expand the Data node.**

**b. Expand the node for the suffix you want to be a master replica.**

In this example, double-click the suffix `o=siroe.com`.

**c. Click Replication.**

**4 Click the New button.**

**5 In the Replication Agreement dialog box, click the Other button.**

**6 In the Remote Server dialog box, provide the following information, and then click OK.**

Host            DirectoryServer-4SP.siroe.com

Port            1389

Secure Port    Leave this box unmarked.

**7 In the Replication Agreement dialog, for the distinguished name (DN) of the replication manager entry on the consumer server, accept the default value.**

By default, the DN is that of the default replication manager.

**8 For the password of the replication manager, enter 11111111.**

**9 (Optional) Provide a description string for this agreement.**

For this example, enter **Replication from DirectoryServer-3SP to DirectoryServer-4SP**.

**10 Click OK when done.**

**11 In the confirmation dialog, click Yes to test the connection to the server and port number.**

Use the given replication manager and password **11111111**.

If the connection fails, you will still have the option of using this agreement. For example, the parameters are correct but the server is offline. When you have finished, the agreement appears in the list of replication agreements for this master replica.

## ▼ To Create a Replication Agreement for the Configuration Instance on Directory Server 4SP

- 1 On DirectoryServer-4, in the Directory Server console, display the general properties for the Directory Server instance named `fm-config`.

Navigate through the tree in the left panel to find the Directory Server instance named `fm-config`, and click on the instance name to display its general properties.

- 2 Click the Open button to display the console for managing the `fm-config` instance.

- 3 Click the Configuration tab and navigate to the Replication pane.

- a. Expand the Data node.

- b. Expand the node for the suffix you want to be a master replica.

In this example, double-click the suffix `o=siroe.com`.

- c. Click Replication.

- 4 Click the New button.

- 5 In the Replication Agreement dialog box, click the Other button.

- 6 In the Remote Server dialog box, provide the following information, and then click OK.

Host            DirectoryServer-3SP.siroe.com

Port            1389

Secure Port    Leave this box unmarked.

- 7 In the Replication Agreement dialog, for the distinguished name (DN) of the replication manager entry on the consumer server, accept the default value.

By default, the DN is that of the default replication manager.

- 8 For the password of the replication manager, enter `11111111`.

- 9 (Optional) Provide a description string for this agreement.

For this example, enter **Replication from DirectoryServer-4SP to DirectoryServer-3SP**.

- 10 Click OK when done.

- 11 In the confirmation dialog, click Yes to test the connection to the server and port number.**

Use the given replication manager and password.

If the connection fails, you will still have the option of using this agreement. For example, the parameters are correct but the server is offline. When you have finished, the agreement appears in the list of replication agreements for this master replica.

## ▼ To Initialize the Configuration Instance Master Replica

- 1 In the Directory Server 3SP console, navigate through the tree in the left panel to find the Directory Server instance named `fm-config`.**

Click on the instance name to display its general properties.
- 2 Double-click the instance name Directory Server ( `fm-config` ) in the tree to display the console for managing the data.**
- 3 Click the Configuration tab and navigate to the Replication pane.**
  - a. Expand the Data node.**
  - b. Expand the node for the suffix you want to be a master replica.**

In this example, double-click the suffix `o=siroe.com`.
  - c. Click Replication.**
- 4 In the list of defined agreements, select the replication agreement corresponding to Directory Server 4SP, the consumer you want to initialize.**
- 5 Click Action > Initialize remote replica.**

A confirmation message warns you that any information already stored in the replica on the consumer will be removed.
- 6 In the Confirmation dialog, click Yes.**

Online consumer initialization begins immediately. The icon of the replication agreement shows a red gear to indicate the status of the initialization process.
- 7 Click Refresh > Continuous Refresh to follow the status of the consumer initialization.**

Any messages for the highlighted agreement will appear in the text box below the list.

- 8 Verify that replication is working properly.**
  - a. Log in to both Directory Server hosts as a root user, and start both Directory Server consoles.**
  - b. Log in to each Directory Server console.**
  - c. In each Directory Server console, enable the audit log on both Directory Server instances.**  
Go to Configuration > Logs > Audit Log. Check Enable Logging, and then click Save.
  - d. In separate terminal windows , use the `tail -f` command to watch the audit log files change.**
  - e. In the Directory Server 3SP console, create a new user entry.**
    - Go to the Directory tab, and right-click the suffix `o=siroue`. Then click New > Group. Name the new group People, and then click OK.
    - Click People, and then right-click to choose New > User.
    - In the Create New User dialog, enter a first name and last name, and then click OK.

Note the user entry is created in the instance audit log. Check to be sure the same entry is also created in Directory Server 4SP in the Directory Server instance audit log
  - f. On DirectoryServer-4SP, in the Directory Server console, create a new user entry.**
    - Go to the Directory tab, and right-click the suffix `o=siroue.com`. Click People, and then right-click to choose New > User.
    - In the Create New User dialog, enter a first name and last name, and then click OK.

Note the user entry is created in the instance audit log. Check to be sure the same entry is also created in Directory Server 3SP in the Directory Server instance audit log
  - g. Delete both new user entries in the Directory Server 4SP console.**  
Look in the Directory Server 3SP console to verify that both users have been deleted.

## 4.4 Enabling Multi-Master Replication of the User Data Instances

Use the following as your checklist for enabling MMR among the user data instances:

1. [Enable multi-master replication for the User Data Instance on Directory Server 3SP.](#)
2. [Enable multi-master replication for the User Data Instance on Directory Server 4SP.](#)
3. [Create a replication agreement for the User Data Instance on Directory Server 3SP.](#)

4. Create a replication agreement for the User Data Instance on Directory Server 4SP.
5. Initialize the User Data Instance master replica.

## ▼ To Enable Multi-Master Replication for the User Data Instance on Directory Server 3SP

- 1 On Directory Server 3SP, start the Directory Server console.

```
# cd /var/opt/mps/serverroot/
# ./startconsole &
```

- 2 Log in to the Directory Server 3SP console.

```
Username          cn=Directory Manager
Password          11111111
Administration URL http://DirectoryServer-3SP.siroe.com:1391
```

- 3 In the Directory Server console, under the Servers and Applications tab, expand the Server Administration domain list until you see the Server Group item.
- 4 Click to expand the Server Group.  
You should see three items: an Administration Server, a Directory Server (fm-config), and a Directory Server (fm-users).
- 5 Double-click the instance name Directory Server (fm-users) to display the console for managing the instance fm-users.
- 6 Click the Configuration tab and navigate to the Replication pane.
  - a. Expand the Data node.
  - b. Expand the node for the suffix you want to be a master replica.  
In this example, double-click the suffix o=siroeusers.com.
  - c. Click Replication.
- 7 Click the "Enable replication" button to start the Replication Wizard.
- 8 Select Master Replica, and then click Next to continue.

**9 Enter a Replica ID, and then click Next.**

For this example, when enabling replication on Directory Server 3SP, assign the number 33.

**10 If you have not already been prompted to select the change log file, you are prompted to select one now.**

The default change log file is shown in the text field. If you do not wish to use the default, type in a filename for the change log, or click Browse to display a file selector. If the change log has already been enabled, the wizard will skip this step.

**11 If you have not already been prompted to enter and confirm a password for the default replication manager, you are prompted now.**

The replication manager is not used in the case of single-master replication, but you must still enter a password to proceed. For this example, enter **11111111**.

**a. Click Next.**

The Replication Wizard displays a status message while updating the replication configuration.

**12 Click Close when replication is finished.**

## ▼ To Enable Multi-Master Replication for the User Data Instance on Directory Server 4SP

**1 Start the Directory Server 4SP console.**

```
# cd /var/opt/mps/serverroot/  
# ./startconsole &
```

**2 Log in to the Directory Server 4SP console.**

Username	<b>cn=Directory Manager</b>
Password	<b>11111111</b>
Administration URL	<b>http://DirectoryServer-4SP.siroe.com:1391</b>

**3 In the Directory Server console, under the Servers and Applications tab, expand the Server Administration domain list until you see the Server Group item.****4 Click to expand the Server Group.**

You should see three items: an Administration Server, a Directory Server (fm-config), and a Directory Server (fm-users).



- 5 **Double-click the instance name** Directory Server ( fm-users ) **to display the console for managing the instance** fm-users.
- 6 **Click the Configuration tab and navigate to the Replication pane.**
  - a. **Expand the Data node.**
  - b. **Expand the node for the suffix you want to be a master replica.**  
In this example, double-click the suffix o=siroeusers . com.
  - c. **Click Replication.**
- 7 **Click the “Enable replication” button to start the Replication Wizard.**
- 8 **Select Master Replica, and then click Next to continue.**
- 9 **Enter a Replica ID, and then click Next.**  
For this example, when enabling replication on Directory Server 4SP, assign the number 44.
- 10 **If you have not already been prompted to select the change log file, you are prompted to select one now.**  
The default change log file is shown in the text field. If you do not wish to use the default, type in a filename for the change log, or click Browse to display a file selector. If the change log has already been enabled, the wizard will skip this step.
- 11 **If you have not already been prompted to enter and confirm a password for the default replication manager, you are prompted now.**  
The replication manager is not used in the case of single-master replication, but you must still enter a password to proceed. For this example, enter **11111111** .
  - a. **Click Next.**  
The Replication Wizard displays a status message while updating the replication configuration.
- 12 **Click Close when replication is finished.**

## ▼ To Create a Replication Agreement for the User Data Instance on Directory Server 3SP

- 1 In the Directory Server 3SP console, display the general properties for the Directory Server instance named `fm-users`.

Navigate through the tree in the left panel to find the Directory Server instance named `fm-users`, and click on the instance name to display its general properties.

- 2 Click the **Open** button to display the console for managing the `fm-users` instance.

- 3 Click the **Configuration** tab and navigate to the **Replication** pane.

- a. Expand the **Data** node.

- b. Expand the node for the suffix you want to be a master replica.

In this example, double-click the suffix `o=siroeusers.com`.

- c. Click **Replication**.

- 4 Click the **New** button.

- 5 In the **Replication Agreement** dialog box, click the **Other** button.

- 6 In the **Remote Server** dialog box, provide the following information, and then click **OK**.

Host            `DirectoryServer-4SP.siroe.com`

Port            `1489`

Secure Port    Leave this box unmarked.

- 7 In the **Replication Agreement** dialog, for the distinguished name (DN) of the replication manager entry on the consumer server, accept the default value.

By default, the DN is that of the default replication manager.

- 8 For the password of the replication manager, enter `11111111`.

- 9 (Optional) Provide a description string for this agreement.

For this example, enter **Replication from DirectoryServer-3SP to DirectoryServer-4SP**.

- 10 Click **OK** when done.

- 11 In the confirmation dialog, click Yes to test the connection to the server and port number.**

Use the given replication manager and password **11111111**.

If the connection fails, you will still have the option of using this agreement. For example, the parameters are correct but the server is offline. When you have finished, the agreement appears in the list of replication agreements for this master replica.

## ▼ To Create a Replication Agreement for the User Data Instance on Directory Server 4SP

- 1 On DirectoryServer-4SP, in the Directory Server console, display the general properties for the Directory Server instance named fm-users.**

Navigate through the tree in the left panel to find the Directory Server instance named fm-users, and click on the instance name to display its general properties.

- 2 Click the Open button to display the console for managing the fm-users instance.**

- 3 Click the Configuration tab and navigate to the Replication pane.**

a. Expand the Data node.

b. Expand the node for the suffix you want to be a master replica.

In this example, double-click the suffix o=siroeusers.com.

c. Click Replication.

- 4 Click the New button.**

- 5 In the Replication Agreement dialog box, click the Other button.**

- 6 In the Remote Server dialog box, provide the following information, and then click OK.**

Host                    **DirectoryServer-3SP.siroe.com**

Port                    **1489**

Secure Port        Leave this box unmarked.

- 7 In the Replication Agreement dialog, for the distinguished name (DN) of the replication manager entry on the consumer server, accept the default value.**

By default, the DN is that of the default replication manager.

- 8 For the password of the replication manager, enter 11111111.**

**9 (Optional) Provide a description string for this agreement.**

For this example, enter **Replication from DirectoryServer-4SP to DirectoryServer-3SP**.

**10 Click OK when done.**

**11 In the confirmation dialog, click Yes to test the connection to the server and port number.**

Use the given replication manager and password.

If the connection fails, you will still have the option of using this agreement. For example, the parameters are correct but the server is offline. When you have finished, the agreement appears in the list of replication agreements for this master replica.

## ▼ **To Initialize the User Data Instance Master Replica**

**1 In the Directory Server 3SP console, navigate through the tree in the left panel to find the Directory Server instance named fm-users.**

Click on the instance name to display its general properties.

**2 Double-click the instance name Directory Server (fm-users) in the tree to display the console for managing the data.**

**3 Click the Configuration tab and navigate to the Replication pane.**

**a. Expand the Data node.**

**b. Expand the node for the suffix you want to be a master replica.**

In this example, double-click the suffix `o=siroeusers.com`.

**c. Click Replication.**

**4 In the list of defined agreements, select the replication agreement corresponding to Directory Server 4SP, the consumer you want to initialize.**

**5 Click Action > Initialize remote replica.**

A confirmation message warns you that any information already stored in the replica on the consumer will be removed.

**6 In the Confirmation dialog, click Yes.**

Online consumer initialization begins immediately. The icon of the replication agreement shows a red gear to indicate the status of the initialization process.

- 7 **Click Refresh > Continuous Refresh to follow the status of the consumer initialization.**  
Any messages for the highlighted agreement will appear in the text box below the list.
- 8 **Verify that replication is working properly.**
  - a. **As a root user, log in to both Directory Server hosts, and start both Directory Server consoles.**
  - b. **Log in to each Directory Server console.**
  - c. **In each Directory Server console, enable the audit log on both Directory Server instances.**  
Go to Configuration > Logs > Audit Log. Check Enable Logging, and then click Save.
  - d. **In separate terminal windows , use the `tail -f` command to watch the audit log files change.**
  - e. **In the Directory Server 3SP console, create a new user entry.**
    - Go to the Directory tab, and right-click the suffix `o=siroeusers.com`. Then click New > Group.  
Name the new group People, and then click OK.
    - Click People, and then right-click to choose New > User.
    - In the Create New User dialog, enter a first name and last name, an then click OK.

Note the user entry is created in the instance audit log. Check to be sure the same entry is also created in on DirectoryServer-4SP in the Directory Server instance audit log
  - f. **In the Directory Server 4SP console, create a new user entry.**
    - Go to the Directory tab, and right—click the suffix `o=siroeusers.com`Click People, and then right-click to choose New > User.
  - g. **Delete both new user entries in the Directory Server 4SP console.**  
Look in the Directory Server 3SP console to verify that both users have been deleted.

## 4.5 Configuring the Directory Server Load Balancers

In the following procedures, you configure one load balancer in front the Directory Server configuration instances, and one load balancer in front of the Directory Server user data instances.

Use the following as your checklist for configuring the Directory Server load balancers:

1. [Configure Load Balancer 7 for the Directory Server Configuration instances.](#)

2. [Configure Load Balancer 8 for the Directory Server User Data instances.](#)

## 4.5.1 Simple Persistence

In this deployment, both Directory Server load balancers are configured for simple persistence. When the load balancer is configured for simple persistence, all Federation Manager requests sent *within a specified interval* are sent to the same Directory Server for processing. Simple persistence ensures that within the specified interval, no errors or delays occur due to replication time or redirects when retrieving data.

When a request requires information to be written to Directory Server 3SP, that information is also replicated in Directory Server 4SP. But the replication takes time to complete. During that time, if a related request is directed by the load balancer to Directory Server 4SP, the request may fail.

For example, when simple persistence is not configured properly, creating a realm from the Federation Manager administration console could fail in the following way. A request for the parent entry creation is routed to Directory Server 3SP, and a second request to create the subentry is routed to Directory Server 4SP. But if the parent entry request is not yet fully replicated to Directory Server 4SP, the subentry request fails. The result is a partially created realm which may not contain all its subentries such as realm administration roles. Simple persistence eliminates this type of error. When persistence is properly configured, both the parent entry request and the subentry request are routed to Directory Server 3SP. The requests are processed in consecutive order. The parent entry is fully created before the subentry request begins processing.

### ▼ To Configure Load Balancer 7 for the Directory Server Configuration Instances

#### Before You Begin

- Contact your network administrator to obtain an available virtual IP address for the load balancer you want to configure.

You must also know the IP address of the load balancer hardware, the URL for the load balancer login page, and a username and password for logging in to the load balancer application.

---

**Note** – The load balancer hardware and software used in the lab facility for this deployment is BIG-IP® manufactured by F5 Networks. If you are using different load balancer software, see the documentation that comes with that product for detailed settings information.

---

- You must also have ready the IP addresses for Directory Server 3SP and Directory Server 4SP.

To obtain these IP addresses, on each Directory Server host, run the following command:

```
ifconfig -a
```

## 1 Create a Pool.

A pool contains all the backend server instances.

- a. Go to URL for the Big IP load balancer login page.

- b. Open the Configuration Utility.

Click “Configure your BIG-IP (R) using the Configuration Utility.”

- c. In the left pane, click Pools.

- d. On the Pools tab, click the Add button.

- e. In the Add Pool dialog, provide the following information:

Pool Name                      Example: federation\_ds\_pool

Load Balancing Method      Round Robin

Resources                      Add the IP address of both Directory Server hosts. In this example:

**192.18.69.135** (for DirectoryServer-3SP:1389)

192.18.72.136 (for DirectoryServer-4SP:1389)

- f. Click the Done button.

## 2 Add a Virtual Server.

If you encounter Javascript errors or otherwise cannot proceed to create a virtual server, try using Microsoft Internet Explorer for this step.

- a. In the left frame, Click Virtual Servers.

- b. On the Virtual Servers tab, click the Add button.

- c. In the Add a Virtual Server dialog box, provide the following information:

Address      192.18.69.16 (for LoadBalancer-7.siroe.com)

Service      389

Pool          federation\_ds\_pool

- d. **Continue to click Next until you reach the Pool Selection dialog box.**
- e. **In the Pool Selection dialog box, assign the Pool (federation\_ds\_pool) that you have just created.**
- f. **Click the Done button.**

### 3 Add Monitors

Monitors are required for the load balancer to detect the backend server failures.

- a. **In the left frame, click Monitors.**
- b. **Click the Basic Associations tab.**
- c. **Add an LDAP monitor for the Directory Server 3SP node.**  
Three columns exist on this page: Node, Node Address, and Service. In the Node column, locate the IP address and port number DirectoryServer - 3SP: 1389. Select the Add checkbox.
- d. **Add an LDAP monitor for the Directory Server 4SP node.**  
In the Node column, locate the IP address and port number for DirectoryServer - 4SP: 1389 . Select the Add checkbox.
- e. **At the top of the Node column, in the drop-down list, choose tcp .**
- f. **Click Apply.**

### 4 Configure the load balancer for simple persistence.

- a. **In the left frame, click Pools.**
- b. **Click the name of the pool you want to configure.**  
In this example, federation\_ds\_pool.
- c. **Click the Persistence tab.**
- d. **On the Persistence tab, under Persistence Type, select the Simple.**
- e. **Set the timeout interval.**  
In the Timeout field, enter 300 seconds.



f. Click Apply.

5 Verify the Directory Server load balancer configuration.

a. Log in as a root user to the host of each Directory Server.

b. On each Directory Server host, use the `tail` command to monitor the Directory Server access log.

```
# cd /var/opt/mps/serverroot/slapd-DirectoryServer-3SP/logs
# tail -f access
```

You should see connections to the load balancer IP address opening and closing. Example:

```
conn=54 op=-1 msgId=-1 - fd=22 slot=22 LDAP connection from
192.18.69.18 to 192.18.72.33
```

```
conn=54 op=-1 msgId=-1 - closing - B1
```

```
conn=54 op=-1 msgId=-1 - closed.
```

c. Execute the following LDAP search against the Directory Server load balancer:

```
# cd /var/opt/mps/serverroot/shared/bin/
# ./ldapsearch -h LoadBalancer-7.siroe.com -p 389 -b "o=siroe.com"
-D "cn=directory manager" -w 11111111 "(objectclass=*)"
```

The `ldapsearch` operation should return entries. Make sure the directory access entries display in only one Directory Server access log.

d. Stop Directory Server 3SP, and again perform the following LDAP search against the Directory Server load balancer:

```
# ./ldapsearch -h LoadBalancer-7.siroe.com -p 389 -b "o=siroeuers.com"
-D "cn=directory manager" -w 11111111 "(objectclass=*)"
```

The `ldapsearch` operation should return entries. Verify that the Directory Server access entries display in only one Directory Server access log.

e. If you encounter the following error message:

```
# ./ldapsearch -h 192.18.69.13 -p 1389 -b "o=siroeuers.com"
-D "cn=Directory Manager" -w 11111111
ldap_simple_bind: Cant' connect to the LDAP
server - Connection refused
```

You can reset the timeout properties to lower values:

- In the load balancer console, click the Monitors tab, and then click the `ldap-tcp` monitor name.

- In the Interval field, set the value to 5.
- In the Timeout field, set the value to 16.
- Click Apply.

Repeat the LDAP search.

**f. Restart the stopped Directory Server 3SP, and then stop Directory Server 4SP.**

Confirm that the requests are forwarded to the running Directory Server 4SP.

**g. Perform the following LDAP search against the Directory Server load balancer.**

```
# ./ldapsearch -h LoadBalancer-7.siroe.com -p 389 -b "o=siroe.com"  
-D "cn=Directory Manager" -w 11111111 "(objectclass=*)"
```

The `ldapsearch` operation should return entries. Make sure the directory access entries display in only the one Directory Server access log.

## ▼ To Configure Load Balancer 8 for the Directory Server User Data Instances

- Before You Begin**
- Contact your network administrator to obtain an available virtual IP address for the load balancer you want to configure.

You must also know the IP address of the load balancer hardware, the URL for the load balancer login page, and a username and password for logging in to the load balancer application.

---

**Note** – The load balancer hardware and software used in the lab facility for this deployment is BIG-IP® manufactured by F5 Networks. If you are using different load balancer software, see the documentation that comes with that product for detailed settings information.

---

- You must also have ready the IP addresses for Directory Server 3SP and Directory Server 4SP.

To obtain these IP addresses, on each Directory Server host, run the following command:

```
ifconfig -a
```

### 1 Create a Pool.

A pool contains all the backend server instances.

**a. Go to URL for the Big IP load balancer login page.**

**b. Open the Configuration Utility.**

Click “Configure your BIG-IP (R) using the Configuration Utility.”

**c. In the left pane, click Pools.****d. On the Pools tab, click the Add button.****e. In the Add Pool dialog, provide the following information:**

Pool Name	Example: federation_users_pool
Load Balancing Method	Round Robin
Resources	Add the IP address of both Directory Server hosts. In this example: .
	<b>192 . 18 . 69 . 135</b> (for DirectoryServer-3SP:1489)
	<b>192 . 18 . 72 . 136</b> (for DirectoryServer-4SP:1489)

**f. Click the Done button.****2 Add a Virtual Server.**

If you encounter Javascript errors or otherwise cannot proceed to create a virtual server, try using Microsoft Internet Explorer for this step.

**a. In the left frame, Click Virtual Servers.****b. On the Virtual Servers tab, click the Add button.****c. In the Add a Virtual Server dialog box, provide the following information:**

Address	192.18.69.16 (for LoadBalancer-8.siroe.com )
Service	1389
Pool	federation_users_pool

**d. Continue to click Next until you reach the Pool Selection dialog box.****e. In the Pool Selection dialog box, assign the Pool (federation\_users\_pool) that you have just created.****f. Click the Done button.**

### 3 Add Monitors

Monitors are required for the load balancer to detect the backend server failures.

a. In the left frame, click **Monitors**.

b. Click the **Basic Associations** tab.

c. **Add an LDAP monitor for the Directory Server 3SP node.**

Three columns exist on this page: Node, Node Address, and Service. In the Node column, locate the IP address and port number `DirectoryServer-3SP:1489`. Select the Add checkbox.

d. **Add an LDAP monitor for the Directory Server 4SP node.**

In the Node column, locate the IP address and port number for `DirectoryServer-4SP:1489`. Select the Add checkbox.

e. **At the top of the Node column, in the drop-down list, choose `ldap-tcp`.**

f. Click **Apply**.

### 4 Configure the load balancer for simple persistence.

a. In the left frame, click **Pools**.

b. **Click the name of the pool you want to configure.**

In this example, `federation_users_pool`.

c. Click the **Persistence** tab.

d. **On the Persistence tab, under Persistence Type, select the Simple.**

e. **Set the timeout interval.**

In the Timeout field, enter 300 seconds.

f. Click **Apply**.

### 5 Verify the Directory Server load-balancer configuration.

a. **Log in as a root user to the host of each Directory Server.**

- b. On each Directory Server host, use the `tail` command to monitor the Directory Server access log.**

```
# cd /var/opt/mps/serverroot/slapd-fm-users/logs
# tail -f access
```

You should see connections to the load balancer IP address opening and closing. Example:

```
conn=54 op=-1 msgId=-1 - fd=22 slot=22 LDAP connection from
192.18.69.18 to 192.18.72.33
```

```
conn=54 op=-1 msgId=-1 - closing - B1
```

```
conn=54 op=-1 msgId=-1 - closed.
```

- c. Execute the following LDAP search against the Directory Server load balancer:**

```
# cd /var/opt/mps/serverroot/shared/bin/
# ./ldapsearch -h LoadBalancer-8.siroe.com -p 1389 -b "o=siroeusers.com"
-D "cn=directory manager" -w 11111111 "(objectclass=*)"
```

The `ldapsearch` operation should return entries. Make sure the directory access entries display in only one Directory Server access log.

- d. Stop Directory Server 3SP, and again perform the following LDAP search against the Directory Server load balancer:**

```
# ./ldapsearch -h LoadBalancer-8.siroe.com -p 1389 -b "o=siroeusers.com"
-D "cn=directory manager" -w 11111111 "(objectclass=*)"
```

The `ldapsearch` operation should return entries. Verify that the Directory Server access entries display in only one Directory Server access log.

- e. If you encounter the following error message:**

```
# ./ldapsearch -h 192.18.69.13 -p 1389 -b "o=siroeusers.com"
-D "cn=Directory Manager" -w 11111111
ldap_simple_bind: Cant' connect to the LDAP
server - Connection refused
```

You can reset the timeout properties to lower values:

- In the load balancer console, click the Monitors tab, and then click the `ldap-tcp` monitor name.
- In the Interval field, set the value to 5.
- In the Timeout field, set the value to 16.
- Click Apply.

Repeat the LDAP search.

**f. Restart the stopped Directory Server 3SP, and then stop Directory Server 4SP.**

Confirm that the requests are forwarded to the running Directory Server 4SP.

**g. Perform the following LDAP search against the Directory Server load balancer.**

```
# ./ldapsearch -h LoadBalancer-8.siroe.com -p 389 -b "o=siroeusers.com"
-D "cn=Directory Manager" -w 11111111 "(objectclass=*)"
```

The ldapsearch operation should return entries. Make sure the directory access entries display in only the one Directory Server access log.

# Configuring Federation Manager Servers to Work with Directory Servers

---

This chapter contains detailed information about the following groups of tasks:

- “5.1 Migrating Federation Manager 1 Configuration from Flat Files to Directory Servers” on page 103
- “5.2 Migrating Federation Manager 1 User Data from Flat Files to Directory Servers” on page 109
- “5.3 Migrating Federation Manager 2 Configuration from Flat Files to Directory Servers” on page 112
- “5.4 Migrating Federation Manager 2 User Data from Flat Files to Directory Servers” on page 114
- “5.5 Configuring the Federation Manager Authentication Service to Work with the Directory Servers” on page 116

## 5.1 Migrating Federation Manager 1 Configuration from Flat Files to Directory Servers

Use the following as your checklist for migrating Federation Manager 1 configuration from flat files to the Directory Servers:

1. Migrate Federation Manager 1 services schema into the Directory Servers.
2. Update the Federation Manager 1 `serverconfig.xml` file.
3. Update the Federation Manager 1 `AMConfig.properties` file.
4. Regenerate and redeploy the Federation Manager 1 WAR file.
5. Update the Platform Server list.

## ▼ To Migrate Federation Manager 1 Services Schema into the Directory Servers

The Federation Manager LDIF files are located in the following directory:

```
/opt/SUNWam/fm/ldif
```

The file `fm_sm_sds_schema.ldif` is for use with Sun Directory Server. The file `fm_sm_ad_schema.ldif` is for use with Microsoft Active Directory.

- 1 **As a root user, log in to the Federation Manager 1 host.**
- 2 **Load the Federation Manager schema into the Directory Server configuration instance.**

```
# cd /opt/SUNWam/fm/ldif
# ldapmodify -D "cn=Directory Manager" -w 11111111 -h LoadBalancer-7.siroe.com
-p 389 -f ./fm_sm_sds_schema.ldif
```

The `ldapmodify` utility loads the object classes and service attributes required for Federation Manager services into the Directory Server schema.

- 3 **On each of the Directory Server hosts, you can watch the error logs for LDIF errors.**

```
# cd /var/opt/mps/serverroot/slapd-fm-config/logs
# tail -f errors
```

- 4 **Migrate the Federation Manager services schema from flat files to the Directory Server.**

```
# cd /opt/SUNWam/fm/bin
# ./fmff2ds -h LoadBalancer-7.siroe.com -p 389 -r "o=siroe.com"
-f /var/opt/SUNWam/fm/federation
-u "cn=Directory Manager" -w 11111111
-j /usr/jdk/instances/jdk.5.0
```

- 5 **Verify that Federation Manager schema was successfully moved to the Directory Server.**

- a. **Start the Directory Server 3SP console.**

```
# cd /var/opt/mps/serverroot/
# ./startconsole &
```

- b. **Log in to the Directory Server console.**

```
User ID:          cn=Directory Manager
Password         11111111
Administration URL: http://DirectoryServer-3SP.siroe.com:1391
```



- c. In the navigation pane, expand the DirectoryServer-3SP.siroe.com suffix, and expand the Server Group.
- d. Double-click the Directory Server (fm-config) instance, and open its console.
- e. Click the Directory tab.
- f. Under the o=siroe.com suffix, expand the Services object.  
All of the Federation Manager services are displayed.

## ▼ To Update the Federation Manager 1 serverconfig.xml File

- 1 Go to the following directory that contains the serverconfig.xml file:

```
# cd /var/opt/SUNWam/fm/war_staging/web-src/WEB-INF/config/
```

- 2 Make a backup of the file serverconfig.xml, and then make the following changes in serverconfig.xml:

- a. In the following entry, change the host name and port number attribute values.:

```
<iPlanetDataAccessLayer>
  <ServerGroup name="default" minConnPool="1" maxConnPool="10">
    <Server name="Server1" host="LoadBalancer-7.siroe.com"
      port="389" type="SIMPLE" />
    <User name="User1" type="proxy">
      <DirDN>
        uid=amadmin,ou=people,o=siroe.com
```

- b. Verify that the following user entries exist in the file:

```
<User name="User1" type="proxy">
  <DirDN>
    uid=amadmin,ou=people,o=siroe.com
  </DirDN>
  <DirPassword>
    AQICGmG7l+gzO6bjmbDBve/MqicBf/zR2I+P
  </DirPassword>
</User>
<User name="User2" type="admin"~
  <DirDN>
    uid=amadmin,ou=people,o=siroe.com
  </DirDN>
  <DirPassword>
```

```
                AQICGmG7l+gzO6bjmbDBve/MqicBf/zR2I+P
            </DirPassword>
    </User>
```

In this deployment example, the proxy user and administrative user have the same DN. In effect, these are the same user. They are both superusers contained in the `ou=service` branch of the Directory Server. These users have privileges to read, write, and search the Federation Manager configuration. The user `amadmin` does not exist in the Directory Server at this point.

### 3 Add the user `amadmin` to the Directory Server.

#### a. On the Federation Manager 1 host, go to the following directory:

```
/opt/SUNWam/fm/bin
```

#### b. Create a file named `amadminconfig.ldif` with the following entries:

```
dn=o=siroe.com
changetype:modify
add:aci

dn: ou=People,o=siroe.com
changetype: add
objectClass: top
objectClass: organizationalunit

dn: uid=amAdmin,ou=People,o=siroe.com
changetype: add
objectclass: inetuser
objectclass: inetorgperson
objectclass: organizationalperson
objectclass: person
objectclass: top
objectClass: iPlanetPreferences
objectclass: inetAdmin
inetuserstatus: Active
cn: amAdmin
sn: amAdmin
userPassword: 11111111

aci: (target="ldap:///ou=services,*o=siroe.com")
      (targetattr = "*" ) (version 3.0; acl "SIIS Top-level Admin Role
      access allow";
      allow (all) userdn = "ldap:///uid=amAdmin,ou=People,
      o=siroe.com";)
```

This LDIF creates a People container and the user amAdmin with the Top-level Admin Role. The user is assigned read, write, and search privileges.

- c. **Use the ldapmodify utility to load ./amadminconfig.ldif into the Directory Server 3SP.**

```
# ldapmodify -D "cn=Directory Manager" -w 11111111
-h LoadBalancer-7.siroe.com -f amadminconfig.ldif
```

## ▼ To Update the Federation Manager 1 AMConfig.properties File

- 1 **Go to the directory that contains the AMConfig.properties file:**

```
# cd /var/opt/SUNWam/fm/war_staging/web-src/WEB-INF/classes
```

- 2 **In AMConfig.properties, set the implementation class for the SM data store.**

Make a backup of the AMConfig.properties file, and then set the following property:

```
com.sun.identity.sm.sms_object_class_name=com.sun.identity.sm.ldap.SMSLDAPObject
```

## ▼ To Regenerate and Redeploy the Federation Manager 1 WAR File

- 1 **On the Federation Manager 1 host, run the fmwar command.**

```
#cd /opt/SUNWam/fm/bin
# ./fmwar -n federation -d /var/opt/SUNWam/fm/war_staging -s /export/fmsilent
```

- 2 **Undeploy the existing Federation Manager WAR 1 file.**

```
# cd /opt/SUNWwbsvr/bin/https/bin
# ./wdeploy delete -u /federation -i FederationManager-1.siroe.com
-v https-FederationManager-1.siroe.com -n hard
```

The `-n hard` option deletes the directory where Federation Manager is exported as well as the URI. If you use the `-n soft` option, only the URI is deleted.

- 3 **Deploy the customized Federation Manager 1 WAR file.**

```
# ./wdeploy deploy -u /federation -i FederationManager-1.siroe.com
-v https-FederationManager-1.siroe.com
/var/opt/SUNWam/fm/war_staging/federation.war
```

This WAR file contains all the SAMLv2 configuration and Directory Server configuration you completed in the previous tasks.

**4 Restart the Federation Manager web container.**

```
#cd /opt/SUNWwbsvr/https-FederationManager-1.siroe.com
# ./stop
# ./start
```

**5 Verify that you can access the Federation Manager 1 server.**

**a. In a browser, go to the Federation Manager URL:**

`http://FederationManager-1.siroe.com:8080/federation/UI/Login`

**b. Log in to the Federation Manager console:**

User Name: **amadmin**

Password: **11111111**

If you can log in successfully, the WAR file was deployed successfully.

## ▼ To Update the Platform Server List

**1 In a browser, go to the Federation Manager URL:**

`http://FederationManager-1.siroe.com:8080/federation/UI/Login`

**2 Log in to the Federation Manager console:**

User Name: **amadmin**

Password: **11111111**

**3 Click the Configuration tab, and then go to the “System properties | Platform” section of the page.**

**4 Add a new entry to the Server List.**

In the Server List field, enter the following:

`http://FederationManager-2.siroe.com:8080|02`

Click Add.

**5 Click Save, and then log out of the Federation Manager console.**

## 5.2 Migrating Federation Manager 1 User Data from Flat Files to Directory Servers

Use the following as your checklist for migrating Federation Manager 1 user data from flat files to Directory Servers:

1. [Load SAMLv2 users schema into the Directory Servers.](#)
2. [Update the Federation Manager 1 AMConfig.properties file.](#)
3. [Update the Federation Manager 1 serverconfig.xml file.](#)

### ▼ To Load SAMLv2 Users Schema into the Directory Servers

The Federation Manager LDIF files are located in the following directory:

```
/opt/SUNWam/saml2/ldif
```

The file `./saml2_sds_schema.ldif` is for use with Sun Directory Server. The file `saml2_ad_schema.ldif` is for use with Microsoft Active Directory.

#### 1 Load the Federation Manager schema into the Directory Servers.

```
# cd /opt/SUNWam/saml2/ldif
# ldapmodify -D "cn=Directory Manager" -w 11111111 -h LoadBalancer-8.siroe.com
-p 1389 -f saml2_sds_schema.ldif
```

The `ldapmodify` utility loads the object classes and user attributes required for Federation Manager users into the Directory Server schema.

#### 2 On each of the Directory Server hosts, you can watch the error logs for LDIF errors.

```
# cd /var/opt/mps/serverroot/slapd-fm-users/logs
# tail -f errors
```

#### 3 Create the `amadmin` suffix in the Directory Server.

##### a. Create a file named `amadminusers.ldif` with the following entries:

```
dn: ou=People,o=siroeusers.com
changetype: add
objectClass: top
objectClass: organizationalunit

dn: uid=amAdmin,ou=People,o=siroeusers.com
changetype: add
objectclass: inetuser
```

```
objectclass: inetorgperson
objectclass: organizationalperson
objectclass: person
objectclass: top
objectClass: iPlanetPreferences
objectclass: inetAdmin
inetuserstatus: Active
cn: amAdmin
sn: amAdmin
userPassword: 11111111
    dn:o=siroeusers.com
changetype:modify
add:aci
aci: (target="ldap:///ou=People,o=siroeusers.com")
    (targetattr = "*") (version 3.0;
    acl "SIIS Top-level Admin Role access allow";
    allow (all) userdn = "ldap:///uid=amAdmin,ou=People,
    o=siroeusers.com");)
```

This LDIF creates a People container and the suffix o=siroeusers.com.

**b. Use the ldapmodify utility to load amadminusers.ldif into the Directory Servers.**

```
# ldapmodify -D "cn=Directory Manager" -w 11111111
-h LoadBalancer-8.siroe.com -p 1389 -f amadminusers.ldif
```

## ▼ To Update the Federation Manager 1 AMConfig.properties File

**1 In the Federation Manager 1 host, go to the directory that contains the file AMConfig.properties:**

```
# cd /var/opt/SUNWam/fm/war_staging/web-src/WEB-INF/classes/
```

**2 Set the default datastore provider property:**

```
com.sun.identity.common.datastore.provider.default=
com.sun.identity.common.LDAPDataStoreProvider
```

Save the file.

## ▼ To Update the Federation Manager 1 serverconfig.xml File

- 1 Go to the directory that contains the file serverconfig.xml:

```
# cd /var/opt/SUNWam/fm/war_staging/web-src/WEB-INF/config
```

- 2 Make a backup of serverconfig.xml, and then modify the following entry.

Modify the host name, port, and user DNs as in the following example:

```
<ServerGroup name="userdefault" minConnPool="1"
  maxConnPool="10">
  <Server name="Server1" host="LoadBalancer-8.siroe.com"
    port="1389" type="SIMPLE" />
  <User name="User1" type="proxy">
    <DirDN>
      uid=amadmin,ou=people,o=siroeusers.com
    </DirDN>
    <DirPassword>
      AQICGmG7l+gz06bjmbDBve/MqicBf/zR2I+P
    </DirPassword>
  </User>
  <User name="User2" type="admin">
    <DirDN>
      uid=amadmin,ou=people,o=siroeusers.com
    </DirDN>
    <DirPassword>
      AQICGmG7l+gz06bjmbDBve/MqicBf/zR2I+P
    </DirPassword>
  </User>
  <BaseDN>
    ou=people,o=siroeusers.com
  </BaseDN>
</ServerGroup>
```

Save the file.

- 3 Regenerate and redeploy the Federation Manager 1 WAR file.

See [“To Regenerate and Redeploy the Federation Manager 1 WAR File”](#) on page 107 in this manual.

## 5.3 Migrating Federation Manager 2 Configuration from Flat Files to Directory Servers

Use the following as your checklist for migrating Federation Manager 2 configuration from flat files to Directory Servers:

1. Update the Federation Manager 2 `serverconfig.xml` file.
2. Update the Federation Manager 2 `AMConfig.properties` file.
3. Regenerate and redeploy the Federation Manager 2 WAR file.

### ▼ To Update the Federation Manager 2 `serverconfig.xml` File

- 1 Go the following directory that contains the `serverconfig.xml` file:

```
# cd /var/opt/SUNWam/fm/war_staging/web-src/WEB-INF/config/
```

- 2 Make a backup of the file `serverconfig.xml`, and then make the following changes in `serverconfig.xml`:

- a. In the following entry, change the host name and port number attribute values:

```
<iPlanetDataAccessLayer>
  <ServerGroup name="default" minConnPool="1" maxConnPool="10">
    <Server name="Server1" host="LoadBalancer-7.siroe.com"
      port="389" type="SIMPLE" />
    <User name="User1" type="proxy">
      <DirDN>
        uid=amadmin,ou=people,o=siroe.com
```

- b. Verify that the following user entries exist in the file:

```
<User name="User1" type="proxy">
  <DirDN>
    uid=amadmin,ou=people,o=siroe.com
  </DirDN>
  <DirPassword>
    AQICGmG7l+gz06bjmbDBve/MqicBf/zR2I+P
  </DirPassword>
</User>
<User name="User2" type="admin"~
  <DirDN>
    uid=amadmin,ou=people,o=siroe.com
  </DirDN>
  <DirPassword>
```



```

        AQICGmG7l+gzO6bjmbDBve/MqicBf/zR2I+P
    </DirPassword>
</User>

```

In this deployment example, the proxy user and administrative user have the same DN. In effect, these are the same user. They are both superusers contained in the `ou=service` branch of the Directory Server. These users have privileges to read, write, and search the Federation Manager configuration. The user `amadmin` does not exist in the Directory Server at this point.

## ▼ To Update the Federation Manager 2 AMConfig.properties File

- 1 **Go to the directory that contains the `AMConfig.properties` file:**

```
# cd /var/opt/SUNWam/fm/war_staging/web-src/WEB-INF/classes
```

- 2 **In `AMConfig.properties`, set the implementation class for the SM data store.**

Make a backup of the `AMConfig.properties` file, and then set the following property:

```
com.sun.identity.sm.sms_object_class_name=com.sun.identity.sm.ldap.SMSLDAPObject
```

## ▼ To Regenerate and Redeploy the Federation Manager 2 WAR File

- 1 **On the Federation Manager 2 host, run the `fmwar` command.**

```
#cd /opt/SUNWam/fm/bin
# ./fmwar -n federation -d /var/opt/SUNWam/fm/war_staging -s /export/fmsilent
```

- 2 **Undeploy the existing Federation Manager WAR 2 file.**

```
# cd /opt/SUNWwbsvr/bin/https/bin
# ./wdeploy delete -u /federation -i FederationManager-2.siroe.com
-v https-FederationManager-1.siroe.com -n hard
```

The `-n hard` option deletes the directory where Federation Manager is exported as well as the URI. If you use the `-n soft` option, only the URI is deleted.

- 3 **Deploy the customized Federation Manager 2 WAR file.**

```
# ./wdeploy deploy -u /federation -i FederationManager-2.siroe.com
-v https-FederationManager-2.siroe.com
/var/opt/SUNWam/fm/war_staging/federation.war
```

This WAR file contains all the SAMLv2 configuration and Directory Server configuration you completed in the previous tasks.

**4 Restart the Federation Manager web container.**

```
#cd /opt/SUNWwbsvr/https-FederationManager-2.siroe.com
# ./stop
# ./start
```

**5 Verify that you can access the Federation Manager 2 server.**

**a. In a browser, go to the Federation Manager URL:**

`http://FederationManager-2.siroe.com:8080/federation/UI/Login`

**b. Log in to the Federation Manager console:**

User Name: **amadmin**

Password: **11111111**

If you can log in successfully, the WAR file was deployed successfully.

## 5.4 Migrating Federation Manager 2 User Data from Flat Files to Directory Servers

Use the following as your checklist for migrating Federation Manager 2 user data from flat files to Directory Servers:

1. [Update the Federation Manager 2 AMConfig.properties file.](#)
2. [Update the Federation Manager 2 serverconfig.xml file.](#)

### ▼ To Update the Federation Manager 2 AMConfig.properties File

**1 In the Federation Manager 2 host, go to the directory that contains the file AMConfig.properties:**

```
# cd /var/opt/SUNWam/fm/war_staging/web-src/WEB-INF/classes/
```

**2 Make a backup AMConfig.properties, and then in the AMConfig.properties file, set the default datastore provider property:**

```
com.sun.identity.common.datastore.provider.default=
com.sun.identity.common.LDAPDataStoreProvider
```

Save the file.

## ▼ To Update the Federation Manager 2 serverconfig.xml File

- 1 **Go to the directory that contains the file** serverconfig.xml:

```
# cd /var/opt/SUNWam/fm/war_staging/web-src/WEB-INF/config
```

- 2 **Make a backup of serverconfig.xml, and then modify the following entry.**

Modify the host name, port, and user DNs as in the following example:

```
<ServerGroup name="userdefault" minConnPool="1"
  maxConnPool="10">
  <Server name="Server1" host="LoadBalancer-8.siroe.com"
    port="1389" type="SIMPLE" />
  <User name="User1" type="proxy">
    <DirDN>
      uid=amadmin,ou=people,o=siroeusers.com
    </DirDN>
    <DirPassword>
      AQICGmG7l+gz06bjmbDBve/MqicBf/zR2I+P
    </DirPassword>
  </User>
  <User name="User2" type="admin">
    <DirDN>
      uid=amadmin,ou=people,o=siroeusers.com
    </DirDN>
    <DirPassword>
      AQICGmG7l+gz06bjmbDBve/MqicBf/zR2I+P
    </DirPassword>
  </User>
  <BaseDN>
    ou=people,o=siroeusers.com
  </BaseDN>
</ServerGroup>
```

Save the file.

- 3 **Regenerate the redeploy the Federation Manager 2 WAR file.**

See [“To Regenerate and Redeploy the Federation Manager 2 WAR File”](#) on page 113.

**4 Restart the Federation Manager web container.**

```
#cd /opt/SUNWwbsvr/https-FederationManager-2.siroe.com
# ./stop
# ./start
```

**5 Verify that you can access the Federation Manager 2 server.**

**a. In a browser, go to the Federation Manager URL:**

`http://FederationManager-2.siroe.com:8080/federation/UI/Login`

**b. Log in to the Federation Manager console:**

User Name: **amadmin**

Password: **11111111**

If you can log in successfully, the WAR file was deployed successfully.

## 5.5 Configuring the Federation Manager Authentication Service to Work with the Directory Servers

Use the following as your checklist for configuring the Federation Manager authentication service:

1. [Migrate the Federation Manager User Data to the Directory Server User data store.](#)
2. [Verify that LDAP authentication works properly.](#)

### ▼ To Migrate the Federation Manager User Data to the Directory Server User Data Store

**1 Go to the Federation Manager 1 URL:**

`http://FederationManager-1.siroe.com:8080/federation/UI/Login`

Notice that above the User Name field, the text says “This server uses flat file authentication scheme.”

**2 Log in to the Federation Manager 1 console:**

User Name **amadmin**

Password **11111111**

- 3 **Add a new authentication service.**
  - a. **Click the Organization tab.**
  - b. **Click the Authentication subtab, and then click Add.**
  - c. **In the list of Authentication Modules, select LDAP, and then click Next.**
  - d. **On the LDAP page, provide the following information:**
    - Primary LDAP Server List:  
Add **LoadBalancer-8.siroe.com:1389**.
    - DN to Start User Search List:  
Add **o=sirousers.com**.
    - DN for Root User Bind:  
**cn=fmldapuser,ou=People,o=sirousers.com**

This root DN is used by the authentication module to create a connection to the Directory Server. This eliminates the need to authenticate each user by individual uid.
    - Password for Root User Bind:  
**00000000**
    - Password for Root User Bind (confirm):  
**00000000**
    - Attribute used to Retrieve User Profile:  
**uid**
    - Attribute User do Search for a User to be Authenticated:  
**uid**
  - e. **Click Assign.**
- 4 **On the Authentication page, locate the module named Core, and click its Edit link.**
- 5 **On the Core page, provide the following information:**
  - Organization Authentication Modules:     Choose Flatfile, LDAP and SAMLv2.
  - People Container for All Users:             Add to the list **ou=People,o=sirousers.com**.Click Save.
- 6 **Verify that LDAP is included as an Organizational Attribute.**

Click the Configuration tab. On the Configuration tab, under Authentication, click Core.

On the Core page, under Organization Attributes, verify that Flatfile, LDAP, and SAMLv2 are included in the list of Organization Authentication Modules.

**7 In the Directory Server, create a user named `fmldapuser`.**

This user is the Federation Manager user that can access the Directory Server. This user and has read, write, and search permissions in `o=siroeuers.com` branch of the Directory Server.

**a. Create an LDIF file named `fmldapuser.ldif` with the following entries:**

```
dn: cn=fmldapuser,ou=People,o=siroeuers.com
changetype: add
objectclass: inetuser
objectclass: organizationalperson
objectclass: person
objectclass: top
cn: fmldapuser
sn: fmldapuser
userPassword: 00000000

dn:o=siroeuers.com
changetype:modify
add:aci
aci: (target="ldap:///o=siroeuers.com")(targetattr="*"
(version 3.0; acl "FM special ldap auth user rights";
allow (read,search) userdn =
"ldap:///cn=fmldapuser,ou=People,o=siroeuers.com"); )
```

**b. Load `./fmldapuser.ldif` into Directory Server 1.**

```
# ldapmodify -D "cn=Directory Manager" -w d1rm4ngr
-h LoadBalancer-8.siroe.com -p 1389 -f ./fmldapuser.ldif
```

**8 Change the default authentication module from Flat File to LDAP.**

**a. Log in to the Federation Manager 1 host.**

**b. Go to the following directory:**

```
/opt/SUNWam/fm/bin
```

**c. Create a file named `ldap.xml` file that contains the following entries:**

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!--
  Copyright (c) 2005 Sun Microsystems, Inc. All rights reserved
  Use is subject to license terms.
-->
```

```

<!DOCTYPE Requests
  PUBLIC "-//iPlanet//Sun Java System Access Manager 2005Q4 Admin
    CLI DTD//EN" "jar://com/iplanet/am/admin/cli/amAdmin.dtd">

<!-- CREATE REQUESTS -->

<Requests>
<OrganizationRequests DN="o=siroe.com">
  <ModifyServiceTemplate serviceName="iPlanetAMAuthService"
    schemaType="Organization">
    <AttributeValuePair>
      Attribute name="iplanet-am-auth-org-config" />
    <Value>&lt;AttributeValuePair&gt;&lt;&lt;Value&gt;
      com.sun.identity.authentication.modules.ldap.LDAP REQUIRED&lt;
    /Value&gt;&lt;/AttributeValuePair&gt;</Value>
  </AttributeValuePair>
  </ModifyServiceTemplate>
</OrganizationRequests>
</Requests>

```

The attributes and AttributeValuePair in bold are the significant changes made to the configuration.

#### d. Load ldap.xml.

```
# ./amadmin -i /var/opt/SUNWam/fm/war-staging -u amadmin -w 11111111 -t ldap.xml
```

## ▼ To Verify that LDAP Authentication Works Properly

### 1 Go to the following Federation Manager URL:

<http://FederationManager-1.siroe.com:8080/federation/UI/Login>

The Federation Manager login page displays the following message: “This server uses LDAP Authentication.”

### 2 Log in to the Federation Manager console:

User Name: **amadmin**

Password: **11111111**

If you can log in successfully, then the LDAP Authentication module was able to successfully bind to the root user to the fm-config instance of Directory Server 3SP.

**3 Create a test user in the `fm-users` instance of Directory Server 3SP.**

**a. Start the Directory Server 3SP console.**

```
# cd /var/opt/mps/serverroot/  
# ./startconsole &
```

**b. In Directory Server 3SP, expand the Server Group, and open the `fm-users` instance.**

**c. Open the `fm-users` console, and click the Directory Tab.**

**d. On the Directory Tab, under the `o=siroeusers.com` suffix, right-click the People container.**

Choose New>User.

**e. In the Create New User dialog, provide the following information:**

First Name: Test  
Last Name: User  
User ID: testuser1  
Password: 11111111  
Click OK.

**4 Go to the following Federation Manager URL:**

<http://FederationManager-1.siroe.com:8080/federation/UI/Login>

**5 Log in to the Federation Manager console:**

User Name: **testuser1**  
Password: **11111111**

If you can log in successfully, then the LDAP Authentication module was able to successfully bind the new user to the `fm-users` instance of Directory Server 3SP.



## Setting Up the Service Provider Keystores

---

In this phase of the deployment, you create SAMLv2 metadata that is recognized by and required by the Liberty Identity protocols. Federation Manager provides sample templates that you can modify to suit your environment.

This chapter contains detailed information about the following groups of tasks:

- “6.1 Configuring the Keystore for Federation Manager 1” on page 121
- “6.2 Configuring Federation Manager 1 to Recognize the New Keystores and Key Files” on page 130
- “6.3 Configuring the Keystore for Federation Manager 2” on page 132
- “6.4 Configuring Federation Manager 2 to Recognize the New Keystores and Key Files” on page 133
- “6.5 Loading the Access Manager Root CA Certificates into the Federation Manager Servers” on page 135

### 6.1 Configuring the Keystore for Federation Manager 1

Use the `Java keytool` command to create private keys for XML signing and SAML encryption. Once the keys are stored in a keystore, you extract a certificate request from the keystore, and then submit the request to a trusted Certificate Authority (CA). The trusted CA sends you a certificate which will be used for XML signing.

Use the following as your checklist for configuring the keystore for Federation Manager 1:

1. Obtain an XML Signing Certificate from a trusted certificate authority.
2. Obtain an Encryption Certificate from a trusted certificate authority.

## ▼ To Obtain an XML Signing Certificate from a Trusted Certificate Authority

1 As a root user, log in to the Federation Manager 1 host.

2 Make a directory for creating a keystore. Example:

```
# cd /etc/opt/SUNWam/  
# mkdir config
```

3 Create a keystore with a private key.

A keystore is a database for storing XML signing certificates, your private keys, and your public keys. For detailed information about keystores and about using the `keytool` utility to create and manage keystores, see

<http://java.sun.com/j2se/1.5.0/docs/tooldocs/solaris/keytool.html>.

Use the `keytool` utility that comes with JDK and is installed with Federation Manager.

Example:

```
# cd /etc/opt/SUNWam/config  
# which keytool  
  /usr/jdk/instances/jdk/1.5.0_06/bin/keytool  
# keytool -genkey -alias LoadBalancer-9 -keyalg RSA -keysize 1024  
-dname "cn=LoadBalancer-9.siroe.com,o=siroe.com" -validity 365  
-keystore fmkeystore  
Enter keystore password: password  
Enter key password for <LoadBalancer-9>  
      (RETURN if same as keystore password): keypassword
```

---

**Note** – The keystore password you specify here must be identical to the keystore password you specify when you install a copy of this certificate onto Federation Manager 2. The two Federation Managers will be recognized as a single entity.

---

4 Verify that the keystore and private key were created properly.

You should be able to see `fmkeystore` in the following directory, and verify that the current date is within the certificate's valid date range.

```
# cd /etc/opt/SUNWam/config  
# ls -lrt  
-rw-r--r--      1 root      root      1261 Nov 2 11:03 fmkeystore  
# keytool -list -keystore fmkeystore -alias LoadBalancer-9 -v  
# Enter keystore password: password  
Alias name: LoadBalancer-9  
Creation date: Nov 2, 2006  
Entry type: keyEntry  
Certificate chain length: 1
```



```

Y29tMA0GCSqGSIb3DQEBAUAA0EAF+gzgerEagmbtjnpzPXkEdILm3vOXp008VOG
u8dZ2hcc2FytYkNbzAESjIw29fUBCSBCSmZQyuLku8jJX9ZxUjCCAo4wggI4oAMC
AQICAgMgMA0GCSqGSIb3DQEBBQUAMIGSMQswCQYDVQQGEwJVUzETMBEGA1UECBMK
Q2FsaWZvcn5pYTEUMBIGA1UEBxMLU2FudGEgQ2xhcmlExHjAcBgNVBAoTFVNB1biBN
aWNB3N5c3RlbnRlcjEjEaMBGGA1UECXMRSWRlbnRpdHkgU2VydmVjZXMxHDAa
BgNVBAMTE0NlcnRpb2mljYXRlIE1hbmFnZXIwHhcNMDQwODE2MDcwMDAwWhcNMzIw
ODE2MDcwMDAwWjCBKjELMAkGA1UEBhMCVVMxEzARBgNVBAGTCNhbGlm3JuaWEx
FDASBgNVBACTC1NhbRnRhIENsYXJhMR4wHAYDVQQKEwVUdW4gTWljcm9zeXN0ZW1z
IEluYy4xGjAYBgNVBAsteUlkZW50aXR5IFNlcjZpY2VzMRwwGgYDVQQDEwNDXJ0
aWZpY2F0ZSBNYW5hZ2VyMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBkz8xQGAbn86
19ouxv4QYtUbrI2AxwsteVlsrSumcG311DHshmnR8HqGZ4jgVN1SnR4YyAwo6jD
Dduf6xD0aM8CAwEAAAN2MHQwEQYJYIZIAyb4QgEBBAQDAgAHMA8GA1UdEwEB/wQF
MAMBAf8wHQYDVRO0BBYEFDugITfLTCfsWyNLTXDl7cMDUKuuMB8GA1UdIwQYMBaA
FDugITfLTCfsWyNLTXDl7cMDUKuuMA4GA1UdDwEB/wQEAwIBhjANBgkqhkiG9w0B
AQUFAANBAFR1D8PyX2k2E1PKx40ful6+hqjW2k+HmbTV70cCGJY8JR7y4y/wCE28
a4p6nxYjgdiQDlvoC8aOI+i1elvf9jMxAA==
-----END CERTIFICATE-----

```

In this deployment example, the certificate text was saved in a text file named `fm.certificate`.

## 7 Import the root CA certificate.

a. **Submit a request to the Certificate Authority for a root CA certificate.**

b. **After you receive the root CA certificate, copy the certificate to the following directory:**

```
/etc/opt/SUNWam/config
```

c. **Import the root CA certificate:**

```

# keytool -import -alias OpenSSL_CA_Cert -keystore fmkeystore -file ca.cert
Enter keystore password: password
...
Trust this certificate? [no]: yes
Certificate was added to keystore.

```

## 8 After you receive the certificate from the trusted CA, import the certificate into the Load Balancer 9 keystore.

The alias name that you specify here will be used later in the deployment when you configure the Federation protocols.

```

# keytool -import -alias LoadBalancer-9 -keystore fmkeystore
-file fm.certificate
Enter keystore password: password
Enter key password for <LoadBalancer-9>: keypassword

```

Top-level certificate in reply:

```
Owner: CN=Certificate Manager, OU=Identity Services,
```



```
o3YwdDARBg_lghkgBhvCAQEEBAMCAAcwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUO6AhN+VM
J+xbI0tNcOXtwNQq64wHwYDVR0jBBgwFoAUO6AhN+VMJ+xbI0tNcOXtwNQq64wDgYDVR0PAQH/
BAQDAgGGMA0GCSqGSIsB3DQEBBQUAA0EAVHUPw/JfaTYTU8rHjR+6Xr6GqNbaT4eZtNXs5wIYljwL
HvLjL/AITbxrinqfFiOB2JAOW+gLxo4j6LV6W9/2Mw==
-----END CERTIFICATE-----
```

Certificate [1] is the public key. This is the certificate that is presented to remote parties in a federated environment. Certificate [2] represents the certificate that authenticates the trusted authority or certificate issuer.

## ▼ To Obtain an Encryption Certificate from a Trusted Certificate Authority

The Liberty Identity specification requires all XML files to be signed. You can obtain and use one certificate to use for both signing and encryption. Or as an alternative, you can obtain one certificate to use for signing, and obtain a second certificate to use for encryption. In this deployment, for illustration purposes, one certificate is used for signing, and a second certificate is used for encryption.

### 1 As a root user, log in to the Federation Manager 1 host.

User Name: amadmin

Password: 11111111

### 2 Go to the following directory:

/etc/opt/SUNWam/config

### 3 Create a keystore with a private key.

```
# keytool -genkey -alias LoadBalancer-9-enc -keyalg RSA -keysize 1024
-dname "cn=LoadBalancer-9.siroe.com,o=siroe.com" -validity 365
-keystore fmkeystore
Enter keystore password: keypassword
Enter key password for <LoadBalancer-9-enc>
(RETURN if same as keystore password): keypassword
```

---

**Note** – The key password you specify here must be identical to the key password you specify for the encryption certificate.

---

#### 4 Verify that the keystore and private key were created properly.

You should be able to see `fmkeystore` in the following directory, and verify that the current date is within the certificate's valid date range.

```
# cd /etc/opt/SUNWam/config
# ls -lrt
-rw-r--r--      1 root      root      1261 Nov 2 11:03 fmkeystore
# keytool -list -keystore fmkeystore -alias LoadBalancer-9-enc -v
# Enter keystore password: password
Alias name: LoadBalancer-9-enc
Creation date: Nov 7, 2006
Entry type: keyEntry
Certificate chain length: 2
Certificate[1]:
Owner: CN=loadbalancer-9.siroe.com
Issuer: CN=Certificate Manager, OU=Identity Services,
O=Sun Microsystems Inc., L=Santa Clara, ST=California, C=US
Serial number: 68f
Valid from: Tue Nov 07 15:56:17 PST 2006 until: Tue Aug 03 16:56:17 PDT 2010
Certificate fingerprints:
    MD5:  69:9C:CF:F6:0D:7E:F4:A7:A8:C3:DC:CD:2F:EC:1A:F4
    SHA1: 29:2F:71:98:6B:AD:4C:27:F2:53:08:94:E0:4B:AF:62:96:1F:B0:F0
Certificate[2]:
Owner: CN=Certificate Manager, OU=Identity Services,
O=Sun Microsystems Inc., L=Santa Clara, ST=California, C=US
Issuer: CN=Certificate Manager, OU=Identity Services,
O=Sun Microsystems Inc., L=Santa Clara, ST=California, C=US
Serial number: 320
Valid from: Mon Aug 16 00:00:00 PDT 2004 until: Mon Aug 16 00:00:00 PDT 2032
Certificate fingerprints:
    MD5:  CD:07:DF:A6:CA:B9:AB:94:FF:CF:17:35:AB:C2:C2:51
    SHA1: 9A:B5:F7:54:DE:8A:BC:E9:F6:1D:F1:5B:71:46:72:9E:F0:4E:B8:7A
```

#### 5 Submit a request for an encryption certificate.

##### a. Create the request.

```
# cd /etc/opt/SUNWam/config
# keytool -certreq -alias LoadBalancer-9-enc
-file cert-enc.csr -keystore fmkeystore
Enter keystore password: password
Enter key password for <LoadBalancer-9-enc>: keypassword
```

##### b. Verify that the request text was successfully generated.

```
# vi cert-enc.csr
-----BEGIN NEW CERTIFICATE REQUEST-----
mllBdjCB4AlBADA3MR1wEAYDVQQKEWlzaXJvZs5jb20xLTAFBgNVBAMTGxvYWRiYkxhbmNlcj05
LnNpcm9IImNvbTcBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAozsGuaqGLL1Z5j6n+aXYACUh
```





## 7 Import the certificate into the Load Balancer 9 keystore.

```
# keytool -import -alias LoadBalancer-9-enc -keystore fmkeystore
-file fm-enc
```

Enter keystore password: **password**

Enter key password for <LoadBalancer-9-enc>: **keypassword**

Top-level certificate in reply:

```
Owner: CN=Certificate Manager, OU=Identity Services,
O=Sun Microsystems Inc., L=Santa Clara, ST=California, C=US
Issuer: CN=Certificate Manager, OU=Identity Services,
O=Sun Microsystems, Inc., L=Santa Clara, ST=California, C=US
Serial number:320
Valid from Mon Aug 16 00:00:00 PDT 2004 until: Mon Aug 16 00:00:00 PDT 2032
Certificate fingerprints:
    MDS:    CD:07:DF:A6:CA:B9:AB:94:FF:CF:17:35:AB:C2:C2:51
    SHA1:9A:B5:F7:54:DE:8A:BC:E9:F6:1D:F1:5B:71:46:72:9E:F0:4E:B8:7A
```

...is not trusted. Install reply anyway? [no]:**yes**

## 8 Verify that the certificate is properly installed.

When you run this command, note that the Entry Type must be keyEntry as in this example. The keyEntry type contains both private key and the public certificate chain. You will need both of these. The trustedcertEntry type contains only the public key and no private key.

```
# keytool -list -keystore fmkeystore -alias LoadBalancer-9-enc -rfc
```

Enter keystore password: **password**

Alias name: LoadBalancer-9-enc

Creation date: Nov 2, 2006

Entry type: keyEntry

Certificate chain length: 2

Certificate text similar to the following is displayed:

```
-----BEGIN CERTIFICATE-----
MIICYDCCAqggAwIBAgICBoowDQYJKoZIhvcNAQEEBQAwgZIXCzAJBgNVBAYTALVTMRMwEQYDVQKI
EwpDYWxpZm9ybmhMRQwEgYDVQQHEwtTYW50YSBDbGFyYU9EeMBwGA1UEChMVU3VvIE1pY3Jvc3lz
dGVtcyBJbmMuMR0wGAYDVQQLEXFJZGVudG10eSBTZXJ2aWNLczEcMBoGA1UEAxMTQ2VydgLmaWNh
dGUGTWFuY2Y2Lm91bnVnXm91bnVnXm91bnVnXm91bnVnXm91bnVnXm91bnVnXm91bnVnXm91bnVn
cm91bnVnXm91bnVnXm91bnVnXm91bnVnXm91bnVnXm91bnVnXm91bnVnXm91bnVnXm91bnVnXm91
AQUAA4GNADCBiQKBGQCjOwa5qoaUuVnknqf5pdgAJSEoWlvx/jnUYbkSDpXLzraEiy2UhwvpoBgB
EeTSUaPPbvboCItchakPI6Z/aFdH3Wmjuij9XD8r1C+q//7sU00IGn00RycddHhoo0aSdnnxGf9V
tREaqKm9dJ7Yn7kQHjo2eryMgYxtr/Z5I15F+wIDAQABo2AwXjARBglgkghkgBhvCAQEEBAMCBkAw
DgYDVRR0PAQH/BAQDAgTwMB8GA1UdIwQYMBaAFDugITfLTCfsWyNLTXD17cMDUKuuMBgGA1UdEQQR
MA+BDW1hbGxhQHN1bi5jb20wDQYJKoZIhvcNAQEEBQADQQB/6D0B6sRqCZu20enM9eQR0gube85e
nTTXu4a7x1naFxxYXK1iQ1vMARKMjDb19QEJIEJKZLdk4uS7yMlf1nFS
-----END CERTIFICATE-----
```

```

Certificate[2]:
-----BEGIN CERTIFICATE-----
MIICj j CCAj igAwIBAgICAYAwDQYJKoZIhvcNAQEFBQAwwZIx CzAJBgNVBAYTA l V T M R M w E Q Y D V Q Q I
EwpDYWxpZm9ybmlhMRQwEgYDVQQHEwTYW50YSBDbGFyYTEeMBwGA1UEChMVU3VvIE1pY3Jvc3lz
dGVt cy B J b m M u M R o w G A Y D V Q Q L E x F J Z G V u d G L 0 e S B T Z X J 2 a W N l c z E c M B o G A 1 U E A x M T Q 2 V y d G l m a W N h
dGUGtWFuYWdlc j AeFw0wNDA4MTYwNzAwMDBaFw0z M j A 4 M T Y w N z A w M D B a M I G S M Q s w C Q Y D V Q Q G E w J V
U z E T M B E G A 1 U E C B M K Q 2 F s a W Z v c m 5 p Y T E U M B I G A 1 U E B x M L U 2 F u d G E g Q 2 x h c m E x H j A c B g N V B A o T F V N 1
b i B N a W N y b 3 N 5 c 3 R l b X M g S W 5 j L j E a M B g G A 1 U E C x M R S W R l b n R p d H k g U 2 V y d m l j Z X M x H D A a B g N V B A M T
E 0 N l c n R p Z m l j Y X R l I E 1 h b m F n Z X I w X D A N B g k q h k i G 9 w 0 B A Q E F A A N L A D B I A k E A r P z F A Y B u f z r X 2 i 7 G
/ H h B i 1 R t E j Y D H C y 1 5 W w y t K 6 Z w b f X U M e y G a d H w e o Z n i O B U 3 V K d H h j I D C j q M M N 2 5 / r E M 5 o z w I D A Q A B
o 3 Y w d D A R B g l g h k g B h v h C A Q E E B A M C A A c w D w Y D V R 0 T A Q H / B A U w A w E B / z A d B g N V H Q 4 E F g Q U O 6 A h N + V M
J + x b I 0 t N c O X t w w N Q q 6 4 w H w Y D V R 0 j B B g w F o A U O 6 A h N + V M J + x b I 0 t N c O X t w w N Q q 6 4 w D g Y D V R 0 P A Q H /
B A Q D A g G G M A 0 G C S q G S I b 3 D Q E B B Q U A A 0 E A V H U P w / J f a T Y T U 8 r H j R + 6 X r 6 G q N b a T 4 e Z t N X s 5 w I Y l j w L
H v L j L / A I T b x r i n q f F i O B 2 J A O W + g L x o 4 j 6 L V 6 W 9 / 2 M w ==
-----END CERTIFICATE-----

```

Certificate [1] is the public key. This is the certificate that is presented to remote parties in a federated environment. Certificate [2] represents the certificate that authenticates the trusted authority or certificate issuer.

## 6.2 Configuring Federation Manager 1 to Recognize the New Keystores and Key Files

The XML signature provider, the XML encryption provider, and the Federation Manager servers use the keystore configuration in the `AMConfig.properties` file for signing purposes. By default, Federation Manager supports multiple XML signature algorithms. In this deployment example, you explicitly specify the RSA signature algorithm by setting the appropriate property in the `AMConfig.properties` file.

---

**Note** – Be sure that you are using the recommended version of the `keytool` utility. Example:

```
# which keytool
/usr/jdk/instances/jdk/1.5.0_06/bin/keytool
```

---

Use the following as your checklist for configuring Federation Manager 1:

1. [Create the Federation Manager 1 keystore passwords.](#)
2. [Modify the `AMConfig.properties` file.](#)

## ▼ To Create the Federation Manager 1 Keystore Passwords

### 1 Create a .storepass file.

```
# /opt/SUNWam/fm/bin/ampassword -i /var/opt/SUNWam/fm/war_staging -e
password >/etc/opt/SUNWam/config/.storepass
```

### 2 Create a .keypass file.

```
# /opt/SUNWam/fm/bin/ampassword -i /var/opt/SUNWam/fm/war_staging -e
keypassword >/etc/opt/SUNWam/config/.keypass
```

## ▼ To Modify the AMConfig.properties File

### 1 Go to the following directory:

```
/var/opt/SUNWam/fm/war_staging/web-src/WEB-INF/classes/
```

Make a backup of the AMConfig.properties file before you make changes.

### 2 In AMConfig.properties, set the following properties as in this example:

```
com.sun.identity.saml.xmlsig.keystore=/etc/opt/SUNWam/config/fmkeystore
com.sun.identity.saml.xmlsig.storepass=/etc/opt/SUNWam/config/.storepass
com.sun.identity.saml.xmlsig.keypass=/etc/opt/SUNWam/config/.keypass
com.sun.identity.saml.xmlsig.certalias=LoadBalancer-9
...
com.sun.identity.jss.donotInstallAtHighestPriority=true
```

### 3 Uncomment the following property, and set the value as in this example:

```
com.sun.identity.saml.xmlsig.xmlSigAlgorithm=
http://www.w3.org/2000/09/xmldsig#rsa-sha1
```

Save the file.

### 4 Regenerate and redeploy the Federation Manager 1 WAR file.

See [“To Regenerate and Redeploy the Federation Manager 1 WAR File”](#) on page 107 in this manual.



```

nTTxU4a7x1naFxzYXK1iQ1vMARKMjDb19QEJIEJKZLDK4uS7yMLf1nFS
-----END CERTIFICATE-----
Certificate[2]:
-----BEGIN CERTIFICATE-----
MIICjjCCAjjgAwIBAgICAYAwDQYJKoZIhvcNAQEFBQAwgZIx CzAJBgNVBAYTA1VTMRMwEQYDQKI
EwpDYWxpZm9ybmlhMRQwEgYDVQQHEwtTYW50YSBDbGFyYTEeMBwGA1UEChMVU3VuIE1pY3Jvc3l z
dGVtcyBJbmMuMR0wGAYDVQLExFjZGVudG0eSBTZj2aWNlczEcMBoGA1UEAxMTQ2VydGhmaWnh
dGUgTWFuYWdlcjAeFw0wNDA4MjYwNzAwMDBaFw0zMjA4MjYwNzAwMDBaMIGSMQswCQYDVQQGEwJV
UzETMBEGA1UECBMKQ2FsaWZvcn5pYTEUMBIGA1UEBxMLU2FudGEGQ2xhcmeXhjAcBgNVBAoTFVN1
biBNaW5yb3N5c3RlbXMgSW5jLjEaMBGGA1UECxMRSWRlbnRpdHkgU2VydmljZXMxHDAaBgNVBAMT
E0NlcnRpZmljYXRlIE1hbmFnZXIwXDANBgkqhkiG9w0BAQEFAANLADBIAkEARPzFAYBuzrX2i7G
/HhBi1RtEjYDHCy15WwytK6ZwbfxUMeyGadHweoZni0BU3VKdHhjIDCjqMMN25/rEM5ozwIDAQAB
o3YwdDARBglgghkgBhvCAQEEBAMCAAcwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUO6AhN+VM
J+xbI0tNcOXtwNnQ64wHwYDVR0jBBgwFoAU06AhN+VMJ+xbI0tNcOXtwNnQ64wDgYDVR0PAQH/
BAQDAgGGMA0GCSqGSIb3DQEBAQUAA0EAVHUPw/JfaTYTU8rHjR+6Xr6GqNbaT4eZtNXs5wIYLjwL
HvLjL/AITbxrinqfFi0B2JAOW+gLxo4j6LV6W9/2Mw==
-----END CERTIFICATE-----

```

Certificate [1] is the public key. This is the certificate that is presented to remote parties in a federated environment. Certificate [2] represents the certificate that authenticates the trusted authority or certificate issuer.

## 6.4 Configuring Federation Manager 2 to Recognize the New Keystores and Key Files

The XML signature provider, the XML encryption provider, and the Federation Manager servers use the keystore configuration in the `AMConfig.properties` file for signing purposes. By default, Federation Manager supports multiple XML signature algorithms. In this deployment example, you explicitly specify the RSA signature algorithm by setting the appropriate property in the `AMConfig.properties` file.

Use the following as your checklist for configuring Federation Manager 2 to recognize the new keystores and key files:

1. Create the Federation Manager 2 keystore passwords.
2. Modify the `AMConfig.properties` file.

## ▼ To Create the Federation Manager 2 Keystore Passwords

### 1 Create a .storepass file.

```
# /opt/SUNWam/fm/bin/ampassword -i /var/opt/SUNWam/fm/war_staging -e  
password >/etc/opt/SUNWam/config/.storepass
```

### 2 Create a .keypass file.

```
# /opt/SUNWam/fm/bin/ampassword -i /var/opt/SUNWam/fm/war_staging -e  
keypassword >/etc/opt/SUNWam/config/.keypass
```

## ▼ To Modify the AMConfig.properties File

### 1 Go to the following directory:

```
/var/opt/SUNWam/fm/war_staging/web-src/WEB-INF/classes/
```

Make a backup of the AMConfig.properties file before you make changes.

### 2 In AMConfig.properties, set the following properties as in this example:

```
com.sun.identity.saml.xmlsig.keystore=/etc/opt/SUNWam/config/fmkeystore  
com.sun.identity.saml.xmlsig.storepass=/etc/opt/SUNWam/config/.storepass  
com.sun.identity.saml.xmlsig.keypass=/etc/opt/SUNWam/config/.keypass  
com.sun.identity.saml.xmlsig.certalias=LoadBalancer-9  
...  
com.sun.identity.jss.donotInstallAtHighestPriority=true
```

### 3 Uncomment the following property, and set the value as in this example:

```
com.sun.identity.saml.xmlsig.xmlSigAlgorithm=  
http://www.w3.org/2000/09/xmldsig#rsa-sha1
```

Save the file.

### 4 Regenerate and redeploy the Federation Manager 2 WAR file.

See [“To Regenerate and Redeploy the Federation Manager 2 WAR File”](#) on page 113.

## 6.5 Loading the Access Manager Root CA Certificates into the Federation Manager Servers

In this procedure you import a root CA certificate from Access Manager 1 into the JDK trusted CA certificate for the Federation Manager servers. This step is not necessary if you are using one of the root CA certificates that come with JDK by default. The JDK default root CA certificates come from Verisign, Thwarte, and other major certificate issuers. In this deployment example, root CA certificates were obtained from certificate issuers that JDK does not recognize by default. So in this deployment example, the following procedure is necessary to establish trust among the local SSO provider (Federation Manager) and remote SSO providers (such as Access Manager).

1. [Load the root CA certificate into the Federation Manager 1 web container.](#)
2. [Load the root CA certificate into the Federation Manager 2 web container.](#)

### ▼ To Load the Root CA Certificate into the Federation Manager 1 Web Container

- 1 **As a root user, log into the Federation Manager 1 host.**
- 2 **Locate the JAVAHOME directory and JDK keystore directory for the Federation Manager 1 web container.**

```
#cd /opt/SUNWwbsvr/https-FederationManager-1.siroe.com/config
# view server.xml
```

Locate the following JAVA javahome entry. In this deployment example, it looks like this:

```
<JAVA javahome="/usr/jdk/entsys-j2se"
```

To find the JDK keystore file, append the following to the javahome path:

```
/jre/lib/security
```

For example, in this deployment example, the JDK keystore is in the following directory:

```
/usr/jdk/entsys-j2se/jre/lib/security
```

This directory contains the Federation Manager trusted CA files.

- 3 **Obtain a copy of the Access Manager 1 root CA certificate.**

You can obtain a copy from the certificate issuer. Or you can copy the certificate stored on the Access Manager 1 host.

In this deployment example, the Access Manager 1 root CA certificate has already been copied to the following directory on Federation Manager 1:

```
/net/slapd/export/share/cacert
```

#### 4 Import the Access Manager root CA certificate into the Federation Manager JDK keystore.

The alias rootCA represents the name of the root CA certificate you want to import.

```
# cd /usr/jdk/entsys-j2se/jre/lib/security
# keytool -import -keystore cacerts -alias rootCA
-file /net/slapd/export/share/cacert
Enter keystore password: changeit
Owner: CN=Certificate Manager, OU=Identity Services,
O=Sun Microsystems Inc., L=Santa Clara, ST=California, C=US
Issuer: CN=Certificate Manager, OU=Identity Services,
O=Sun Microsystems, Inc., L=Santa Clara, ST=California, C=US
Serial number:320
Valid from Mon Aug 16 00:00:00 PDT 2004 until: Mon Aug 16 00:00:00 PDT 2032
Certificate fingerprints:
    MDS:    CD:07:DF:A6:CA:B9:AB:94:FF:CF:17:35:AB:C2:C2:51
    SHA1:9A:B5:F7:54:DE:8A:BC:E9:F6:1D:F1:5B:71:46:72:9E:F0:4E:B8:7A
Trust this certificate? [no]: yes
Certificate was added to keystore.
```

#### 5 To verify that the root CA certificate was successfully imported, run the list command:

```
# cd /usr/jdk/instances/jdk1.5.0/jre/lib/security
# keytool -list -keystore cacerts -alias rootCA -rfc
Enter keystore password: changeit
Alias name: rootCA
Creation date: Mar 9, 2007
Entry type: trustedCertEntry

-----BEGIN CERTIFICATE-----
MIICjjCCAjjigAwIBAgICAYAwDQYJKoZIhvcNAQEFBQAwgZIx CzAJBgNVBAYTA lVTMRMwEYDVQQI
EwpDYWxpZm9ybmlhMRQwEgYDVQQHEwTYW50YSBDbGFyYTEeMBwGA1UEChMVU3V3UE1pY3Jvc3lz
dGVtcyBJbmMuMR0wGAYDVQQLExFJZGVudG l0eSBTZXJ2aWNLczEcMBoGA1UEAxMTQ2VydG lmaWNh
dGUgTWFuYWdlcjAeFw0wNDA4MTYwNzAwMDBaFw0zMjA4MTYwNzAwMDBaMIGSMQswCQYDVQQGEwJV
UzETMBEGA1UECBMKQ2FsaWZvc m5pYTEUMBIGA1UEBxMLU2FudGEgQ2xhc mExHjAcBgNVBAoTFVN1
biBNawNy b3N5c3RlbXMgSw5jLjEaMBGGA1UEC xMRSWRlbnRpdHkgU2Vydml jZXMxHDAaBgNVBAMT
E0NlcnRpZml jYXRlIE1hbmFnZXIwXDANBgkqhkiG9w0BAQEFAANLADBIAkEArPzFAYBUfzrX2i7G
/HhBi1RtEjYDHcy15WwytK6ZwbfXUMeyGadHweoZni0BU3VKdHhj IDCj qMMN25/ rEM5ozwIDAQAB
o3YwdDARBg lghkgBhv hCAQEEBAMCAAcwYDVR0TAQH/BAUwAwEB/ zAdBgNVHQ4EFgQUO6AhN+VM
J+xbI0tNcOXtwwNQ64wHwYDVR0 jBBgwFoAUO6AhN+VMJ+xbI0tNcOXtwwNQ64wDgYDVR0PAQH/
BAQDAgGGMA0GC SgSIB3DQEBBQUAA0EAVHUPw/ JfaTYTU8rHj r+6Xr6GqNbaT4eZtNXs5wIYljwL
HvLjL/AITbxrinqfFi0B2JAOW+gLxo4j6LV6W9/2Mw==
-----END CERTIFICATE-----
```



## ▼ To Load the Root CA Certificate into the Federation Manager 2 Web Container

- 1 As a root user, log into the Federation Manager 2 host.
- 2 Locate the JAVAHOME directory and JDK keystore directory for the Federation Manager 2 web container.

```
#cd /opt/SUNWwbsvr/https-FederationManager-2.siroe.com/config
# view server.xml
```

Locate the following JAVA javahome entry. In this deployment example, it looks like this:

```
<JAVA javahome="/usr/jdk/entsys-j2se"
```

To find the JDK keystore file, append the following to the javahome path:

```
/jre/lib/security
```

For example, in this deployment example, the JDK keystore is in the following directory:

```
/usr/jdk/entsys-j2se/jre/lib/security
```

This directory contains the Federation Manager JDK trusted CA files.

- 3 Obtain a copy of the Access Manager 1 root CA certificate.

You can obtain a copy from the certificate issuer. Or you can copy the certificate stored on the Access Manager 1 host.

In this deployment example, the Access Manager 1 root CA certificate has already been copied to the following directory on Federation Manager 1:

```
/net/slaped/export/share/cacert
```

- 4 Import the Access Manager 1 root CA certificate into the Federation Manager 2 JDK keystore.

The alias rootCA represents the name of the root CA certificate you want to import.

```
# cd /usr/jdk/entsys-j2se/jre/lib/security
# keytool -import -keystore cacerts -alias rootCA
-file /net/slaped/export/share/cacert
Enter keystore password: changeit
Owner: CN=Certificate Manager, OU=Identity Services,
O=Sun Microsystems Inc., L=Santa Clara, ST=California, C=US
Issuer: CN=Certificate Manager, OU=Identity Services,
O=Sun Microsystems, Inc., L=Santa Clara, ST=California, C=US
Serial number:320
Valid from Mon Aug 16 00:00:00 PDT 2004 until: Mon Aug 16 00:00:00 PDT 2032
Certificate fingerprints:
```

```

MDS:      CD:07:DF:A6:CA:B9:AB:94:FF:CF:17:35:AB:C2:C2:51
SHA1:9A:B5:F7:54:DE:8A:BC:E9:F6:1D:F1:5B:71:46:72:9E:F0:4E:B8:7A
Trust this certificate? [no]: yes
Certificate was added to keystore.

```

**5 To verify that the root CA certificate was successfully imported, run the list command:**

```

# cd /usr/jdk/instances/jdk1.5.0/jre/lib/security
# keytool -list -keystore cacerts -alias rootCA -rfc
Enter keystore password: changeit
Alias name: rootCA
Creation date: Mar 9, 2007
Entry type: trustedCertEntry

-----BEGIN CERTIFICATE-----
MIICjjCCAjigAwIBAgICAYAwDQYJKoZIhvcNAQEFBQAwgZIx CzAJBgNVBAYTA1VTMRMwEQYDVOQI
EwpDYWxpZm9ybmlhMRQwEgYDVOQHEwtTYW50YSBDbGFyYTEeMBwGA1UEChMVU3VuIE1pY3Jvc3lz
dGVtcyBJbmMuMRowGAYDVQQLEXZJZGVudGll0eSBTZXJ2aWNLczEcMBoGA1UEAxMTQ2VydgLmawNh
dGUgTWFuYWdlcjAeFw0wNDA4MTYwNzAwMDEBaFw0zMjA4MTYwNzAwMDEBaMIGSMQswCQYDVQQGEwJV
UzETMBEGA1UECBMkQ2FsaWZvcj5pYTEUMBIGA1UEBxMLU2FudGEGQ2xhcmlhcmExHjAcBgNVBAoTFVFN1
biBNawNyb3N5c3RlbXMGSw5jLjEaMBGGA1UECxMRSWRlbnRpdHkgU2VydmllZjZXMxHDAaBgNVBAMT
E0NlcnRpbmZlYXRlIE1hbmFnZXIwXDANBgkqhkiG9w0BAQEFAANLADBIAkEArPzFAYBufzrX2i7G
/HhBi1RtEjYDHCy15WwytK6ZwbfXUMeyGadHweoZni0BU3VKdHhjIDCj qMMN25/ rEM5ozwIDAQAB
o3YwdDARBgllghkgBhvCAQEEBAMCAAcwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUO6AhN+VM
J+xbI0tNcOXtwwNQq64wHwYDVR0jBBgwFoAUO6AhN+VMJ+xbI0tNcOXtwwNQq64wDgYDVR0PAQH/
BAQDAgGGMA0GCSqGSIb3DQEBBQUAA0EAVHUPw/JfaTYTU8rHjR+6Xr6GqNbaT4eZtNXs5wIYljwL
HvLjL/AITbxrinqfFiOB2JAOW+gLxo4j6LV6W9/2Mw==
-----END CERTIFICATE-----

```

# Configuring SAMLv2 Metadata for the Federation Manager Servers

---

Use the following as your checklist for configuring SAMLv2 metadata for the Federation Manager servers:

1. [Create a circle of trust.](#)
2. [Configure the SAMLv2 Service Provider metadata.](#)
3. [Load the SAMLv2 metadata.](#)

## 7.1 Creating a Circle of Trust

When you create metadata for the Service Provider, the Service Provider entity is added to a circle of trust. A circle of trust is used to group Service Providers and Identity Providers in a secure, trusted environment. Other remote provider entities can be added to the circle of trust. Whenever the SAMLv2 protocol is initiated, the SAMLv2 plug-in determines which circle of trust the requesting entity belongs to, and what other providers are available to interact with it. All entities within the same circle of trust can participate in the SAMLv2 protocols.

### ▼ To Create a Circle of Trust

- 1 **As a root user, log into the Federation Manager 1 host.**

- 2 **Run the `cotcreate` command:**

```
# /opt/SUNWam/saml2/bin/saml2meta -i /var/opt/SUNWam/fm/war_staging  
cotcreate -u amadmin -w 11111111 -t saml2_circle_of_trust  
Circle of trust "saml2_circle_of_trust" is created successfully.
```

## 7.2 Configuring the SAMLv2 Service Provider Metadata

Federation Manager provides two metadata templates you can customize to meet your needs. For examples of customized metadata templates, see “7.2.1 Sample Metadata Template Files” on page 141 at the end of this section.

---

**Note** – When you customize the metadata XML files, you must enter the `entityID` attribute using lowercase letters. For example, for the host `LoadBalancer-9.siroe.com`, enter the `entityID` as `loadbalancer-9.siroe.com`. The `entityID` will not be recognized if you use mixed case letters.

---

### ▼ To Generate and Customize the Service Provider Template Files

**1** Log in as a root user to the host `FederationManager-1`.

**2** Go to the following directory:

```
/opt/SUNWam/saml2/bin
```

**3** Generate the SAMLv2 template files.

```
# ./saml2meta -i /var/opt/SUNWam/fm/war_staging template -u amadmin
-w 11111111 -e loadbalancer-9.siroe.com -s /sp -a LoadBalancer-9
-f LoadBalancer-9-enc
-m /etc/opt/SUNWam/config/saml2-sp-template.xml
-x /etc/opt/SUNWam/config/saml2-sp-extended-template.xml
```

The `saml2-sp-extended-template.xml` is similar to the standard `saml2-sp-template.xml` file. However, the extended file contains data about the SAMLv2 plug-in that is specific to Federation Manager.

**4** Customize the `saml2-sp-template.xml` file.

When the file is first generated, default values are automatically generated and placed in the file. You must manually change these values to match the actual deployment environment. In this deployment example, a load balancer with SSL termination is being used. So you must modify the file to use the HTTPS protocol and the load balancer service URL.

```
# vi /etc/opt/SUNWam/config/saml2-sp-template.xml
```

**a.** In each `Location URL` and each `ResponseLocation URL`, change the protocol `http` to `https`.

Search for each occurrence of `Location` and `ResponseLocation` to be sure you have changed each URL.

- b. Globally change all occurrences of **FederationManager-1** to **loadbalancer-9**.
- c. Globally change all occurrences of **8080** to **3443**.

Save the file.

**5 Customize the saml2-sp-extended-template.xml file.**

```
# vi /etc/opt/SUNWam/config/saml2-sp-extended-template.xml
```

**a. Modify the following attribute-pair values to enable XML signing.**

```
<Attribute name="wantArtifactResponseSigned">
    <Value>true</Value>
<Attribute name="wantLogoutRequestSigned">
    <Value>true</Value>
<Attribute name="wantLogoutResponseSigned">
    <Value>true</Value>
<Attribute name="wantMNIRequestSigned">
    <Value>true</Value>
<Attribute name="wantMNIResponseSigned">
    <Value>true</Value>
<Attribute name="cotlist">
    <Value>saml2_circle_of_trust</Value>
```

**6 Load the metadata.**

See [“7.3 Loading the Service Provider SAMLv2 Metadata”](#) on page 146.

## 7.2.1 Sample Metadata Template Files

In the following examples, changes to the file are indicated in bold.

---

**Note** – When you customize the metadata XML files, you must enter the `entityID` attribute using lowercase letters. For example, for the host `LoadBalancer-9.siroe.com`, enter the `entityID` as **loadbalancer-9.siroe.com**. The `entityID` will not be recognized if you use mixed case letters.

---

EXAMPLE 7-1 Modified `saml2-sp-template.xml` File

```
<EntityDescriptor
  xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
  entityID="loadbalancer-9.siroe.com">
  <SPSSODescriptor
    AuthnRequestsSigned="false"
    WantAssertionsSigned="false"
```



## EXAMPLE 7-1 Modified saml2-sp-template.xml File (Continued)

```

        Location="https://LoadBalancer-9.siroe.com:3443/federation/
        SPSloRedirect/metaAlias/sp"
        ResponseLocation="https://LoadBalancer-9.siroe.com:3443/
        federation/SPSloRedirect/metaAlias/sp"/>
    <SingleLogoutService
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
        Location="https://LoadBalancer-9.siroe.com:3443/
        federation/SPSloSoap/metaAlias/sp"/>
    <ManageNameIDService
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
        Location="https://LoadBalancer-9.siroe.com:3443/federation/
        SPMniRedirect/metaAlias/sp"
        ResponseLocation="https://LoadBalancer-9.siroe.com:3443/
        federation/SPMniRedirect/metaAlias/sp"/>
    <ManageNameIDService
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
        Location="https://LoadBalancer-9.siroe.com:3443/
        federation/SPMniSoap/metaAlias/sp"
        ResponseLocation="https://LoadBalancer-9.siroe.com:3443/
        federation/SPMniSoap/metaAlias/sp"/>
    <NameIDFormat>
        urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
    </NameIDFormat>
    <NameIDFormat>
        urn:oasis:names:tc:SAML:2.0:nameid-format:transient
    </NameIDFormat>
    <AssertionConsumerService
        isDefault="true"
        index="0"
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"
        Location="https://LoadBalancer-9.siroe.com:3443/
        federation/Consumer/metaAlias/sp"/>
    <AssertionConsumerService
        index="1"
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
        Location="https://LoadBalancer-9.siroe.com:3443/
        federation/Consumer/metaAlias/sp"/>
</SPSSODescriptor>
</EntityDescriptor>

```

## EXAMPLE 7-2 Modified saml2-sp-metadata-template.xml File

```

<EntityConfig xmlns="urn:sun:fm:SAML:2.0:entityconfig"
  xmlns:fm="urn:sun:fm:SAML:2.0:entityconfig"
  hosted="1"
  entityID="loadbalancer-9.siroe.com">

```

EXAMPLE 7-2 Modified saml2-sp-metadata-template.xml File (Continued)

```
<SPSSOConfig metaAlias="/sp">
  <Attribute name="signingCertAlias">
    <Value>LoadBalancer-9</Value>
  </Attribute>
  <Attribute name="encryptionCertAlias">
    <Value>LoadBalancer-9-enc</Value>
  </Attribute>
  <Attribute name="basicAuthOn">
    <Value>>false</Value>
  </Attribute>
  <Attribute name="basicAuthUser">
    <Value></Value>
  </Attribute>
  <Attribute name="basicAuthPassword">
    <Value></Value>
  </Attribute>
  <Attribute name="autofedEnabled">
    <Value>>false</Value>
  </Attribute>
  <Attribute name="autofedAttribute">
    <Value></Value>
  </Attribute>
  <Attribute name="transientUser">
    <Value></Value>
  </Attribute>
  <Attribute name="spAccountMapper">
    <Value>com.sun.identity.saml2.plugins.DefaultSPAccountMapper</Value>
  </Attribute>
  <Attribute name="spAttributeMapper">
    <Value>com.sun.identity.saml2.plugins.DefaultSPAttributeMapper</Value>
  </Attribute>
  <Attribute name="spAuthncontextMapper">
    <Value>com.sun.identity.saml2.plugins.DefaultSPAuthnContextMapper</Value>
  </Attribute>
  <Attribute name="spAuthncontextClassrefMapping">
    <Value>PasswordProtectedTransport|0|default</Value>
  </Attribute>
  <Attribute name="spAuthncontextComparisonType">
    <Value>exact</Value>
  </Attribute>
  <Attribute name="attributeMap">
    <Value></Value>
  </Attribute>
  <Attribute name="saml2AuthModuleName">
    <Value></Value>
  </Attribute>
</SPSSOConfig>
```



EXAMPLE 7-2 Modified saml2-sp-metadata-template.xml File (Continued)

```

</Attribute>
<Attribute name="localAuthURL">
  <Value></Value>
</Attribute>
<Attribute name="intermediateUrl">
  <Value></Value>
</Attribute>
<Attribute name="defaultRelayState">
  <Value></Value>
</Attribute>
<Attribute name="assertionTimeSkew">
  <Value>300</Value>
</Attribute>
<Attribute name="wantAttributeEncrypted">
  <Value></Value>
</Attribute>
<Attribute name="wantAssertionEncrypted">
  <Value></Value>
</Attribute>
<Attribute name="wantNameIDEncrypted">
  <Value></Value>
</Attribute>
<Attribute name="wantArtifactResponseSigned">
  <Value>true</Value>
</Attribute>
<Attribute name="wantLogoutRequestSigned">
  <Value>true</Value>
</Attribute>
<Attribute name="wantLogoutResponseSigned ">
  <Value>true</Value>
</Attribute>
<Attribute name="wantMNIRequestSigned">
  <Value>true</Value>
</Attribute>
<Attribute name="wantMNIResponseSigned">
  <Value>true</Value>
</Attribute>
<Attribute name="cotlist">
  <Value>saml2_cirlce_of_trust</Value>
</Attribute>
</SPSSOConfig>
</EntityConfig>

```

## 7.3 Loading the Service Provider SAMLv2 Metadata

When you load the SAMLv2 metadata into Directory Server, the Service Provider entity configuration is created. The entity configuration enables the SAMLv2 plug-in to recognize all SAMLv2 protocol URLs. The SAMLv2 metadata is also used for exchanging data with remote parties.

### 7.3.1 To Load the Customized Service Provider Metadata

Load the customized `saml2-sp-template.xml` and `saml2-sp-extended-template.xml` configuration files using the following command:

```
# /opt/SUNWam/saml2/bin/saml2meta -i /var/opt/SUNWam/fm/war_staging import
-u amadmin -w 11111111 -m /etc/opt/SUNWam/config/saml2-sp-template.xml
-x /etc/opt/SUNWam/config/saml2-sp-extended-template.xml
```

---

**Note** – If the files do not load successfully, be sure that all `entityID` attributes in the files are entered using lowercase letters. The `entityID` attribute is not recognized if mixed case letters are used.

---

PART III

Setting Up the Identity Provider Site



# Installing the SAMLv2 Plug-in on Access Manager Servers

---

This chapter provides information about the following groups of tasks:

- “8.1 Installing the SAMLv2 Plug-In on the Access Manager Servers” on page 149
- “8.2 Configuring the Access Manager Load Balancer for the SAMLv2 Protocols” on page 156
- “8.3 Configuring the Access Manager Servers to Use SAMLv2 User Schema” on page 156

---

**Note** – The following instructions are designed to be used on an Identity Provider Site that is already deployed and running. See “1.2 System Architecture” on page 22 in this manual for information about deploying the Identity Provider Site. See also “2.12 Obtaining Instructions for Deploying the Identity Provider Site” on page 38 in this manual.

---

## 8.1 Installing the SAMLv2 Plug-In on the Access Manager Servers

You must obtain the Sun Java System SAMLv2 Plug-in for Federation Services 1.0.

The SAMLv2 Plug-in is an auxiliary program that works with either Sun Java System Access Manager or Sun Java System Federation Manager. The plug-in incorporates a subset of features based on the Security Assertion Markup Language (SAML) version 2 specifications. When installed, the plug-in allows support for interactions based on those specifications.

You can download the plug-in from the following Sun Microsystems

URL:<http://sunsolve.sun.com/search/document.do?assetkey=1-21-122983-02-1>.



---

**Caution** – If you have configured an Access Manager site, be sure to remove the site ID from the Access Manager instances before installing the SAMLv2 plug-in. If the site ID exists in the Access Manager instances, SAMLv2 installation may fail.

---

Use the following as your checklist for installing the SAMLv2 Plug-In:

1. [Install the SAMLv2 Plug-In and the SAMLv2 Patch on Access Manager 1.](#)
2. [Install the SAMLv2 Plug-In and the SAMLv2 Patch on Access Manager 2.](#)

## ▼ To Install the SAMLv2 Plug-In and the SAMLv2 Patch on Access Manager 1

### 1 As a root user, log in to the host Access Manager 1.

Change to the directory where you unpacked the SAMLv2 installation files. Example:

```
# cd /tmp/saml2
# ls
../
ENTITLEMENT.TXT          saml2silent
LICENSE.TXT              samlv2-1.0-solaris-sparc.tar
README.TXT               version
SUNWsaml2/
```

### 2 Modify the `saml2silent` file to reflect the location of the deployed Access Manager WAR file.

Make a backup copy of the `saml2silent` file before making any changes to it.

See changes in boldface in the following example:

```
##### START OF VARIABLE DEFINITIONS #####

STAGING_DIR=/opt/SUNWwbsvr/https-AccessManager-1.example.com/
is-web-apps/services
ADMINPASSWD=4m4dmin1
DEPLOY_SAMPLES=true

#
# SYSTEM
# AM if SAML2 will be deployed on Access Manager
# FM if SAML2 will be deployed on Federation Manager
# installer will auto detect if not specified.
#

SYSTEM=AM

# AM_INSTANCE
# SAML2 will be deployed on the specified AM instance.
# If it is not specified, SAML2 will be configured on the first AM instance.
#

AM_INSTANCE=
```

```

#
# LOAD_SCHEMA if true will load SAML2 SDS/AD schema
# DS_DIRMGRDN is the DN (distinguished name) of the directory manager,
#           the user who has unrestricted access to Directory Server.
# DS_DIRMGRPASSWD is the password for the directory manager
#
LOAD_SCHEMA=true
DS_DIRMGRDN="cn=Directory Manager"
DS_DIRMGRPASSWD=dirm4n4ger

#
# IDPDISCOVERY_ONLY set to true will only configure idpdiscovery service
# COMMON_COOKIE_DOMAIN IDP Discovery service cookie domain
# COOKIE_ENCODE set to true, common domain cookie will be encoded.
IDPDISCOVERY_ONLY=false
COMMON_COOKIE_DOMAIN=
COOKIE_ENCODE=true

##### END OF VARIABLE DEFINITIONS #####

```

### 3 Run the SAMLv2 installer.

```
# ./saml2setup install -s saml2silent
```

When installation is complete, you will see the following message:

```

Hosted entity descriptor for realm "/" was written to file
"idpMeta.xml" successfully.
Hosted entity config for realm "/" was written to file
"idpExtended.xml" successfully.
Hosted entity descriptor for realm "/" was written to file
"spMeta.xml" successfully.
Hosted entity config for realm "/" was written to file
"spExtended.xml" successfully.
Meta data created !!!

```

```
Circle of trust "samplecot" is created successfully.
```

```
Loading SAML2 schema...
```

```
The new AM server war /opt/SUNWam/amserver.war is ready for deploy!
```

In this deployment example, complete proceeding steps before deploying the WAR file.

### 4 Load the SAMLv2 users schema into the Access Manager users instance.

```

#cd /opt/SUNWam/saml2/ldif
# ldapmodify -h LoadBalancer-2.example.com -p 489 -D "cn=Directory Manager"

```

```
-w dirm4n4ger -f saml2_sds_schema.ldif  
modifying entry CN=schema
```

**5 Go to the directory where you downloaded and unpacked the SAMLv2 patch installation file.**

```
# cd /temp/saml2patch/122983-02  
# ls  
LEGAL_LICENSE.TXT  
LICENSE.TXT  
patchinfo  
postbackout  
postpatch  
prebackout  
prepatch  
README.122983-01  
rel_notes.html  
SUNWsaml2
```

**6 Run the SAMLv2 patch installer.**

```
# cd /temp/saml2patch  
# patchadd -G 122983-02
```

When installation is complete, you will see the following message:

```
Patch packages installed:  
                SUNWsaml2
```

**7 Go to the directory where the SAMLv2 update script is located.**

```
# cd /opt/SUNWam/saml2/bin
```

**8 Run the update script.**

```
# ./saml2setup update -s saml2silent
```

Any updates required because of the newly-installed patch are made in SAMLv2.

**9 Restart Access Manager 1.**

```
# cd /opt/SUNWwbsvr/https-AccessManager-1.example.com  
# ./stop; ./start
```

This deployment uses Sun Java System Web Server which does not require you to redeploy the Access Manager WAR file at this point. If you are using any other web container, you must redeploy the Access Manager WAR file before restarting the Access Manager 1 server.

**Troubleshooting** If you must uninstall and then re-install the SAMLv2 patch for any reason, when you run the update script the script may fail. Search the `saml2silent` file for the string `--` and delete all occurrences. The script may have inadvertently added the extraneous strings to the file.



## ▼ To Install the SAMLv2 Plug-In and the SAMLv2 Patch on Access Manager 2

### 1 As a root user, log in to the host Access Manager 2.

Change to the directory where you unpacked the SAMLv2 installation files. Example:

```
# cd /tmp/saml2
# ls
../
ENTITLEMENT.TXT          saml2silent
LICENSE.TXT              samlv2-1.0-solaris-sparc.tar
README.TXT               version
SUNWsaml2/
```

### 2 Modify the `saml2silent` file to reflect the location of the deployed Access Manager WAR file.

Make a backup copy of the `saml2silent` file before making any changes to it.

See changes in boldface in the following example:

```
##### START OF VARIABLE DEFINITIONS #####
```

```
STAGING_DIR=/opt/SUNWwbsvr/https-AccessManager-2.example.com/
is-web-apps/services
ADMINPASSWD=4m4dmin1
DEPLOY_SAMPLES=true
```

```
#
# SYSTEM
# AM if SAML2 will be deployed on Access Manager
# FM if SAML2 will be deployed on Federation Manager
# installer will auto detect if not specified.
#
```

```
SYSTEM=AM
```

```
# AM_INSTANCE
# SAML2 will be deployed on the specified AM instance.
# If it is not specified, SAML2 will be configured on the first AM instance.
#
```

```
AM_INSTANCE=
```

```
#
# LOAD_SCHEMA if true will load SAML2 SDS/AD schema
# DS_DIRMGRDN is the DN (distinguished name) of the directory manager,
#           the user who has unrestricted access to Directory Server.
# DS_DIRMGRPASSWD is the password for the directory manager
```

```
#
LOAD_SCHEMA=true
DS_DIRMGRDN="cn=Directory Manager"
DS_DIRMGRPASSWD=dirm4n4ger

#
# IDPDISCOVERY_ONLY set to true will only configure idpdiscovery service
# COMMON_COOKIE_DOMAIN IDP Discovery service cookie domain
# COOKIE_ENCODE set to true, common domain cookie will be encoded.
IDPDISCOVERY_ONLY=false
COMMON_COOKIE_DOMAIN=
COOKIE_ENCODE=true

##### END OF VARIABLE DEFINITIONS #####
```

### 3 Run the SAMLv2 installer.

```
# ./saml2setup install -s saml2silent
```

When installation is complete, you will see the following message:

```
Hosted entity descriptor for realm "/" was written to file
"idpMeta.xml" successfully.
Hosted entity config for realm "/" was written to file
"idpExtended.xml" successfully.
Hosted entity descriptor for realm "/" was written to file
"spMeta.xml" successfully.
Hosted entity config for realm "/" was written to file
"spExtended.xml" successfully.
Meta data created !!!
```

Circle of trust "samplecot" is created successfully.

Loading SAML2 schema...

The new AM server war /opt/SUNWam/amserver.war is ready for deploy!

In this deployment example, complete proceeding steps before deploying the WAR file.

### 4 Load the SAMLv2 users schema into the Access Manager users instance.

```
#cd /opt/SUNWam/saml2/ldif
# ldapmodify -h LoadBalancer-2.example.com -p 489 -D "cn=Directory Manager"
-w dirm4n4ger -f saml2_sds_schema.ldif
modifying entry CN=schema
```

### 5 Go to the directory where you downloaded and unpacked the SAMLv2 patch installation file.

```
# cd /temp/saml2patch/122983-02
# ls
```

```
LEGAL_LICENSE.TXT
LICENSE.TXT
patchinfo
postbackout
postpatch
prebackout
prepatch
README.122983-01
rel_notes.html
SUNWsaml2
```

## 6 Run the SAMLv2 patch installer.

```
# cd /temp/saml2patch
# patchadd -G 122983-02
```

When installation is complete, you will see the following message:

```
Patch packages installed:
                SUNWsaml2
```

## 7 Go to the directory where the SAMLv2 update script is located.

```
# cd /opt/SUNWam/saml2/bin
```

## 8 Run the update script.

```
# ./saml2setup update -s saml2silent
```

Any updates required because of the newly-installed patch are made in SAMLv2.

## 9 Restart Access Manager 2.

```
# cd /opt/SUNWwbsvr/https-AccessManager-2.example.com
# ./stop;./start
```

This deployment uses Sun Java System Web Server which does not require you to redeploy the Access Manager WAR file at this point. If you are using any other web container, you must redeploy the Access Manager WAR file before restarting the Access Manager 1 server.

**Troubleshooting** If you must uninstall and then re-install the SAMLv2 patch for any reason, when you run the update script the script may fail. Search the `saml2silent` file for the string `--` and delete all occurrences. The script may have inadvertently added the extraneous strings to the file.

## 8.2 Configuring the Access Manager Load Balancer for the SAMLv2 Protocols

Follow the instructions that come with your load balancer hardware and software for installing and setting up the load balancer. Set up Load Balancer 3 using the following settings:

TABLE 8-1 Access Manager Load Balancer Settings

Setting	Value
Load Balancing Method	Round Robin
Persistence	Active HTTP cookie with insert value
SSL Termination	Enabled

## 8.3 Configuring the Access Manager Servers to Use SAMLv2 User Schema

The final task in configuring the Access Manager servers is to configure them to use SAMLv2 user schema.

### ▼ To Reconfigure the LDAPv3 Plug-In on the Access Manager User Instances

#### 1 Log in to the Access Manager console:

User Name: `amadmin`

Password: `4m4dmin1`

#### 2 On the Realms page, click the users realm name.

#### 3 Click the Data Stores tab.

On the Data Stores tab, click the usersLDAP Data Store name.

#### 4 On the "LDAPv3 Repository Plugin" page, make the following changes:

##### a. Add a new LDAP User Object Class.

In the Add box for LDAP User Object Class, enter the following and then click Add:

`sunFMSAML2NameIdentifier`

**b. Add a new LDAP User Attribute.**

In the Add box for LDAP User Attributes, enter the following and then click Add:

`sun-fm-saml2-nameid-infokey`

**c. Add a second new LDAP User Attribute.**

In the Add box for LDAP User Attributes, enter the following and then click Add:

`sun-fm-saml2-nameid-info`

**5 Click Save.**



# Setting Up the Identity Provider Keystores

---

In this phase of the deployment, you create SAMLv2 metadata that is recognized by and required by the Liberty Identity protocols. Federation Manager provides sample templates that you can modify to suit your environment.

This chapter contains detailed information about the following groups of tasks:

- [“9.1 Configuring the Keystore for Access Manager 1” on page 159](#)
- [“9.2 Configuring Access Manager 1 to Recognize the New Keystores and Key Files” on page 167](#)
- [“9.3 Configuring the Keystore for Access Manager 2” on page 169](#)
- [“9.4 Configuring Access Manager 2 to Recognize the New Keystores and Key Files” on page 170](#)
- [“9.5 Loading the Federation Manager Root CA Certificates into the Access Manager Servers” on page 172](#)

## 9.1 Configuring the Keystore for Access Manager 1

Use the `Java keytool` command to create private keys for XML signing and SAML encryption. Once the keys are stored in a keystore, you extract a certificate request from the keystore, and then submit the request to a trusted Certificate Authority (CA). The trusted CA sends you a certificate which will be used for XML signing.

Use the following as your checklist for configuring the keystore for Federation Manager 1:

1. [Obtain an XML signing certificate from a trusted Certificate Authority.](#)
2. [Obtain an encryption certificate from a trusted Certificate Authority.](#)

## ▼ To Obtain an XML Signing Certificate from a Trusted Certificate Authority

1 As a root user, log in to the Access Manager 1 host.

2 Go to the following directory:

```
/etc/opt/SUNWam/config
```

3 Create a keystore with a private key.

A keystore is a database for storing XML signing certificates, your private keys, and your public keys. For detailed information about keystores and about using the `keytool` utility to create and manage keystores, see

<http://java.sun.com/j2se/1.5.0/docs/tooldocs/solaris/keytool.html>.

Use the `keytool` utility that comes with JDK and is installed with Access Manager. Example:

```
# cd /etc/opt/SUNWam/config
# which keytool
/usr/jdk/instances/jdk/1.5.0_06/bin/keytool
# keytool -genkey -alias LoadBalancer-3 -keyalg RSA -keysize 1024
-dname "cn=LoadBalancer-3.example.com,o=example.com" -validity 365
-keystore amkeystore
Enter keystore password: passwordam
Enter key password for <LoadBalancer-3>
(RETURN if same as keystore password): keypasswordam
```

---

**Note** – The keystore password you specify here must be identical to the keystore password you specify when you install a copy of this certificate onto Access Manager 2. The two Access Managers will be recognized as a single entity.

---

4 Verify that the keystore and private key were created properly.

You should be able to see `amkeystore` in the following directory, and verify that the current date is within the certificate's valid date range.

```
# cd /etc/opt/SUNWam/config
# ls -lrt
-rw-r--r-- 1 root root 1261 Nov 2 11:03 amkeystore
# keytool -list -keystore amkeystore -alias LoadBalancer-3 -v
# Enter keystore password: passwordam
Alias name: LoadBalancer-3
Creation date: Nov 2, 2006
Entry type: keyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=LoadBalancer-3.example.com, O=example.com
```









certificate to use for signing, and obtain a second certificate to use for encryption. In this deployment, for illustration purposes, one certificate is used for signing, and a second certificate is used for encryption.

**1 As a root user, log in to the Access Manager 1 host.**

**2 Go to the following directory:**

```
/etc/opt/SUNWam/config
```

**3 Create a keystore with a private key.**

```
# keytool -genkey -alias LoadBalancer-3-enc -keyalg RSA -keysize 1024
-dname "cn=LoadBalancer-3.example.com,o=siroe.com" -validity 365
-keystore amkeystore
Enter keystore password: passwordam
Enter key password for <LoadBalancer-3-enc>
(RETURN if same as keystore password): keypasswordam
```

---

**Note** – The key password you specify here must be identical to the key password you specify for the signing certificate.

---

**4 Verify that the keystore and private key were created properly.**

You should be able to see amkeystore in the following directory, and verify that the current date is within the certificate's valid date range.

```
# cd /etc/opt/SUNWam/config
# ls -lrt
-rw-r--r--      1 root      root      1261 Nov 2 11:03 amkeystore
# keytool -list -keystore amkeystore -alias LoadBalancer-3-enc -v
# Enter keystore password: passwordam
Alias name: LoadBalancer-3-enc
Creation date: Nov 7, 2006
Entry type: keyEntry
Certificate chain length: 2
Certificate[1]:
Owner: CN=loadbalancer-3.example.com
Issuer: CN=Certificate Manager, OU=Identity Services,
O=Sun Microsystems Inc., L=Santa Clara, ST=California, C=US
Serial number: 68f
Valid from: Tue Nov 07 15:56:17 PST 2006 until: Tue Aug 03 16:56:17 PDT 2010
Certificate fingerprints:
    MD5:  69:9C:CF:F6:0D:7E:F4:A7:A8:C3:DC:CD:2F:EC:1A:F4
    SHA1: 29:2F:71:98:6B:AD:4C:27:F2:53:08:94:E0:4B:AF:62:96:1F:B0:F0
Certificate[2]:
Owner: CN=Certificate Manager, OU=Identity Services,
O=Sun Microsystems Inc., L=Santa Clara, ST=California, C=US
Issuer: CN=Certificate Manager, OU=Identity Services,
```

```
O=Sun Microsystems Inc., L=Santa Clara, ST=California, C=US
Serial number: 320
Valid from: Mon Aug 16 00:00:00 PDT 2004 until: Mon Aug 16 00:00:00 PDT 2032
Certificate fingerprints:
    MD5:  CD:07:DF:A6:CA:B9:AB:94:FF:CF:17:35:AB:C2:C2:51
    SHA1: 9A:B5:F7:54:DE:8A:BC:E9:F6:1D:F1:5B:71:46:72:9E:F0:4E:B8:7A
```

## 5 Submit a request for an encryption certificate.

### a. Create the request.

```
# cd /etc/opt/SUNWam/config
# keytool -certreq -alias LoadBalancer-3-enc
-file am-enc.csr -keystore amkeystore
Enter keystore password: passwordam
Enter key password for <LoadBalancer-3-enc>: keypasswordam
```

### b. Verify that the request text was successfully generated.

```
# vi am-enc.csr
-----BEGIN NEW CERTIFICATE REQUEST-----
mLlBdjCB4ALBADA3MR1wEAYDVQQKEwIzaXJvZs5jb20xLTAFBgNVBAMTGxvYWRiYkxhbmNlci05
LnNpcm9IlnNvbTCBnzANBQkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAozsGuaqGLL1Z5j6n+aXYACU
hKFpb8f451GG5Eg6Vy862hIstlIb8KaAYARhk0lGjzwb26AiLXlWpDyOmf2hXR91po7oo/Vw/K9Qv
qv/+7FDtCBp9DkcnHXR4aKNGknZ58Rn/VBURGqipvXSe2J+5EB46Nnq8jIGMba/2eSJeRfsCAwEA
AaAMA0GCSqGS1b3DQEBBAUAA4GBAJ3u+f5mC7AVXErSDucNHZn4Li42LULQBEZmTK3K73U9Ar4wx
ex2Ee6lAsPdyb3g4jUmduBSkrSbKyxZhPutVZQTlfHkiLbd6vHWlK197DedLoWlt9nZa03xZyBym
6UCH0HYVly/TAL8fhsielElg8lsidlejis(hfkeowhkdlgile27uak9pwnbmqkdigleIDUekdo30
-----END OF NEW CERTIFICATE REQUEST-----
```

## 6 Follow the instructions provided by your Certificate Authority (CA) for submitting the cert-enc.csr file and sending the text to the CA.

The CA will process your request, and send you a certificate. When you open the certificate file with an editor, the certificate text will look similar to this:

```
-----BEGIN CERTIFICATE-----
MIIFJQYJKoZIhvcNAQcCoIIFfjCCBRICAQExADAPBgkqhkiG9w0BBwGgAgQAOIIE
9jCCAmAwggIKoAMCAQICAgAKMA0GCSqGS1b3DQEBBAUAMIGSMQswCQYDVQGEwJV
UzETMBEGA1UECBMKQ2FsaWZvcn5pYUeUMBIGA1UEBxMLU2FudGEGQ2xhcmeXhJAc
BgNVBAAoTFVn1b1BNawNyb3N5c3RlbnRlbnRpdHkgU2VydmljZXMTxHDAaBgnVBAMTE0NlcnRzmljYXRlIE1hbmFnZXIwHhcNMDYxMTAy
MTkxMTM0WWhcNMTAwNzISMTkxMTM0WjA3MR1wEAYDVQQKEwIzaXJvZs5jb20xITAF
BgNVBAMTGxvYWRiYkxhbmNlci05LnNpcm9lLnNvbTCBnzANBQkqhkiG9w0BAQEFA
AOBjQAwgYkCgYEAozsGuaqGLL1Z5j6n+aXYACUhhKFpb8f451GG5Eg6Vy862hIst
lIb8KaAYARhk0lGjzwb26AiLXIWpDyOmf2hXR91po7oo/Vw/K9Qvqv/+7FDtCBp9
DkcnHXR4aKNGknZ58Rn/VBURGqipvXSe2J+5EB46Nnq8jIGMba/2eSJeRfsCAwEA
AaNGMF4wEQYJYIZIAyb4QgEBBAQDAgZAMA4GA1UdDwEB/wQEAwIE8DAfBgNVHSME
GDAWgBQ70CE35Uwn7Fsjs01w5e3DA1CrrjAYBgNVHREETAPgQ1tYwxsYUBzdW4u
Y29tMA0GCSqGS1b3DQEBBAUAA0EAF+gzgerEagmbtjnpzPXkEdILm3vOXp08V0G
```



Entry type: keyEntry  
Certificate chain length: 2

Certificate text similar to the following is displayed:

```
-----BEGIN CERTIFICATE-----
MIICYDCCAqggAwIBAgICBoowDQYJKoZIhvcNAQEEBQAwgZIxZCzAJBgNVBAYTALVTMRMwEYQDVQQI
EwpDYWxpZm9ybmhMRQwEgYDVQQHEwTYW50YSBDbGFyYTEeMBwGA1UEChMVU3V3UE1pY3Jvc3lz
dGVtcyBjbMUMRowGAYDVQQLEwFJZGVudG10eSBTZjJ2aWNLczEcmBoGA1UEAxMTQ2VydGlmawNh
dGUGTWFuYWdlcjAeFw0wNjExMDIxOTExMzRaFw0xMDA3MjJkOTExMzRaMDcxZjAQBGNVBAoTCXNp
cm9lLmNvbTEhMB8GA1UEAxMYbG9hZGJhbGFuY2V2YyLTKuc2lyb2UuY29tMIGfMA0GCSqGSIb3DQEB
AQUAA4GNADCBiQKBQCj0wa5qoaUvUnknqf5pdgAJSEoWlvx/jnUYbkSDpXLzraEiy2UhwvpoBgB
EeTSUaPPbvboCItchakPI6Z/aFdH3Wmjuij9XD8r1C+q//7sU00IGn00RycddHhoo0aSdnnxGf9V
tREaqKm9dJ7Yn7kQHjo2eryMgYxtr/Z5I15F+wIDAQABo2AwXjARBglghkgBhvhCAQEEBAMCBKAw
DgYDVR0PAAQH/BAQDAgTWMB8GA1UdIwQYMBaAFDugITfLTCfswyNLTXDL7cMDUKuuMBGGA1UdEQQR
MA+BDW1hbGxhQHN1bi5jb20wDQYJKoZIhvcNAQEEBQADQBB/6D0B6sRqCZu20enM9eQR0gube85e
nTTxU4a7x1naFxxYXK1iQ1vMARKMjDb19QEJIEJKZlDK4uS7yMlf1nFS
-----END CERTIFICATE-----
Certificate[2]:
-----BEGIN CERTIFICATE-----
MIICj j CCAj igAwIBAgICAYAwDQYJKoZIhvcNAQEFBQAwgZIxZCzAJBgNVBAYTALVTMRMwEYQDVQQI
EwpDYWxpZm9ybmhMRQwEgYDVQQHEwTYW50YSBDbGFyYTEeMBwGA1UEChMVU3V3UE1pY3Jvc3lz
dGVtcyBjbMUMRowGAYDVQQLEwFJZGVudG10eSBTZjJ2aWNLczEcmBoGA1UEAxMTQ2VydGlmawNh
dGUGTWFuYWdlcjAeFw0wNDA4MjYwNzAwMDBaFw0zZmJ4MjYwNzAwMDBaMIGSMQswCQYDVQGEwJV
UzETMBEGA1UECBMKQ2FsaWZvcz5pYUeUMBIGA1UEBxMLU2FudGEGQ2xhcmeXhJAcBgNVBAoTFVN1
biBNawNyb3N5c3RlbXMGSw5jLjEaMBGGA1UECxMRSWRlbnRpdHkgU2VydmljZXMxHDAaBgNVBAMT
EONlcnRpZmljYXRlIE1hbmFnZXIwXDANBgkqhkiG9w0BAQEFAANLADBIAkEA rPzFAYBu f z rX2i7G
/HhBi1RtEjYDHCy15WwytK6ZwbFXUMeyGadHweoZni0BU3VKdHhJ IDCj qMMN25/ rEM5ozwIDAQAB
o3YwdDARBg lghkgBhvhCAQEEBAMCAAcwDwYDVR0T AQH/BAUwAwEB/zAdBgNVHQ4EFgQUO6AhN+VM
J+xbI0tNcOXtwwNQ64wHwYDVR0jBBgwFoAUO6AhN+VMJ+xbI0tNcOXtwwNQ64wDgYDVR0PAQH/
BAQDAgGGMA0GCSqGSIb3DQEBBQUAA0EAVHUPw/JfaTYTU8rHjR+6Xr6GqNbaT4eZtNXs5wIYLjwL
HvLjL/AITbxrinqfFiOB2JAOW+gLxo4j6LV6W9/2Mw==
-----END CERTIFICATE-----
```

Certificate [1] is the public key. This is the certificate that is presented to remote parties in a federated environment. Certificate [2] represents the certificate that authenticates the trusted authority or certificate issuer.

## 9.2 Configuring Access Manager 1 to Recognize the New Keystores and Key Files

The XML signature provider, the XML encryption provider, and the Access Manager servers use the keystore configuration in the `AMConfig.properties` file for signing purposes. By default, Access Manager supports multiple XML signature algorithms. In this deployment example, you explicitly specify the RSA signature algorithm by setting the appropriate property in the `AMConfig.properties` file.

Use the following as your checklist for configuring Access Manager 1:

1. [Create the Access Manager 1 keystore passwords.](#)
2. [Modify the `AMConfig.properties` file.](#)
3. [Modify the `amsaml.properties` file.](#)

## ▼ To Create the Access Manager 1 Keystore Passwords

- 1 **As a root user, log into the Access Manager host.**

- 2 **Create a `.storepass` file.**

```
# cd /etc/opt/SUNWam/config
# /opt/SUNWam/bin/ampassword -e passwordam > .storepass
```

- 3 **Create a `.keypass` file.**

```
# pwd /etc/opt/SUNWam/config
# /opt/SUNWam/bin/ampassword -e keypasswordam > .keypass
```

## ▼ To Modify the `AMConfig.properties` File

- 1 **Go to the following directory:**

```
/etc/opt/SUNWam/config
```

Make a backup of the `AMConfig.properties` file before you make changes.

- 2 **In `AMConfig.properties`, set the following properties as in this example:**

```
com.sun.identity.saml.xmlsig.keystore=/etc/opt/SUNWam/config/amkeystore
com.sun.identity.saml.xmlsig.storepass=/etc/opt/SUNWam/config/.storepass
com.sun.identity.saml.xmlsig.keypass=/etc/opt/SUNWam/config/.keypass
com.sun.identity.saml.xmlsig.certalias=LoadBalancer-3
...
com.sun.identity.jss.donotInstallAtHighestPriority=true
```

- 3 **Uncomment the following property, and set the value as in this example:**

```
com.sun.identity.saml.xmlsig.xmlSigAlgorithm=
http://www.w3.org/2000/09/xmldsig#rsa-sha1
```

Save the file.



## ▼ To Modify the `amsaml.properties` File

- 1 Go to the following directory:

```
/opt/SUNWam/locale
```

- 2 Open the `amsaml.properties` file and search for the following property:

```
xmlsigalgorithm=http://www.w3.org/2000/09/xmlsig#dsa-sha1
```

- 3 Change the method from `dsa-sha1` to `rsa-sha1`.

```
xmlsigalgorithm=http://www.w3.org/2000/09/xmlsig#dsa-sha1
```

- 4 Restart the Access Manager 1 server.

```
# cd /opt/SUNWwbsvr/https-AccessManager-1.example.com
```

```
# ./stop;./start
```

## 9.3 Configuring the Keystore for Access Manager 2

The XML signing certificates must be identical on both Access Manager instances. This ensures that when the SAMLv2 metadata is published, the metadata represents both Access Manager instances as a single entity. In this procedure you copy the XML signing certificate from Access Manager 1 and install the certificate on Access Manager 2.

### ▼ To Install the Access Manager 1 XML Signing Certificate on Access Manager 2

- 1 As a root user, log in to the Access Manager 2 host.

- 2 Go to the following directory:

```
/etc/opt/SUNWam/config
```

- 3 Copy into this directory the keystore files that were created for Access Manager 1.

- 4 Verify that the certificate is properly installed.

```
# keytool -list -keystore amkeystore -alias LoadBalancer-3 -rfc
```

```
Enter keystore password: password
```

```
Alias name: LoadBalancer-3
```

```
Creation date: Nov 2, 2006
```

```
Entry type: keyEntry
```

```
Certificate chain length: 2
```

Certificate text similar to the following is displayed:

```
Certificate[1]:
-----BEGIN CERTIFICATE-----
MIICYDCCAggqAwIBAgICBoowDQYJKoZIhvcNAQEEBQAwwZIxZCzAJBgNVBAYTALVTRMRWwEYDQVQKI
EwpDYWxpZm9ybmhMRQwEgYDVQQHEwtTYW50YSBDbGFyYTEeMBwGA1UEChMVU3VvIE1pY3Jvc3lz
dGVtcyBJbmMuMRowGAYDVQQLEXFlZGVudG10eSBTZjJ2aWNLczEcmBoGA1UEAxMTQ2VydGlmawNh
dGUgTWFuYWdlcjAeFw0wNjExMDIxOTExMzRaFw0xMDA3MjJkOTExMzRaMDcxZjAQBGNVBAoTCXNp
cm9lLmNvbTEhMB8GA1UEAxMYbG9hZGJhbGFuY2VyLTKuc2lyb2UuY29tMIGfMA0GCSqGSIb3DQEBA
QUAA4GNADCBiQKBgQCj0wa5qoaUuVnknqf5pdgAJSEoWlvx/jnUYbkSDpXLzraEiy2UhwvpoBgB
EeTSUaPPBvboCItchakPI6Z/aFdH3Wmjuij9XD8r1C+q//7sU00IGn00RycddHhoo0aSdnxGf9V
tREaqKm9dJ7Yn7kQHjo2eryMgYxtr/Z5I15F+wIDAQABo2AwXjARBglghkgBhvhCAQEEBAMCBkAw
DgYDVR0PAAQH/BAQDAgTWMB8GA1UdIwQYMBaAFDugITfLTCfsWyNLTXDL7cMDUKuuMBGGA1UdEQQR
MA+BDW1hbGxhQHN1bi5jb20wDQYJKoZIhvcNAQEEBQADQQB/6DOB6sRqCZu20enM9eQR0gube85e
nTTxU4a7x1naFxxYXK1iQ1vMARKMjDb19QEJIEJKZLDK4uS7yMlf1nFS
-----END CERTIFICATE-----

Certificate[2]:
-----BEGIN CERTIFICATE-----
MIICjjCCAjjigAwIBAgICAYAwDQYJKoZIhvcNAQEFBQAwwZIxZCzAJBgNVBAYTALVTRMRWwEYDQVQKI
EwpDYWxpZm9ybmhMRQwEgYDVQQHEwtTYW50YSBDbGFyYTEeMBwGA1UEChMVU3VvIE1pY3Jvc3lz
dGVtcyBJbmMuMRowGAYDVQQLEXFlZGVudG10eSBTZjJ2aWNLczEcmBoGA1UEAxMTQ2VydGlmawNh
dGUgTWFuYWdlcjAeFw0wNDA4MjYwNzAwMDBaFw0zAjA4MjYwNzAwMDBaMIGSMQswCQYDVQGEwJV
UzETMBEGA1UECBMKQ2FsaWZvcn5pYTEUMBIGA1UEBxMLU2FudGEGQ2xhcmlEAcBgNVBAoTFVFN1
biBNaWVyb3N5c3RlbXMGSw5jLjEAMBgGA1UECXMRSWRlbnRpdHkgU2VydmljZXMxHDAaBgNVBAMT
E0NlcnRzZmljYXRlIE1hbmFnZXIwXDAuNDBkqkqkiG9w0BAQEFAANLADBIAkEArPzFAYBuzrX2i7G
/HhBi1RtEjYDHCy15WwytK6ZwbfXUMeyGadHweoZni0BU3VKdHhJIDCjQMMN25/rEM5ozwIDAQAB
o3YwdDARBgIghkgBhvhCAQEEBAMCAAcwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQU06AhN+VM
J+xbI0tNcOXtwwNQq64wHwYDVR0jBBGwFoAU06AhN+VMJ+xbI0tNcOXtwwNQq64wDgYDVR0PAQH/
BAQDAgGGMAGCSqGSIb3DQEBBQUAA0EAVHUPw/JfaTYTU8rHjR+6Xr6GqNbaT4eZtNXs5wIYljwL
HvLjL/AITbxrinqfFi0B2JAOW+gLx04j6LV6W9/2Mw==
-----END CERTIFICATE-----
```

Certificate [1] is the public key. This is the certificate that is presented to remote parties in a federated environment. Certificate [2] represents the certificate that authenticates the trusted authority or certificate issuer.

## 9.4 Configuring Access Manager 2 to Recognize the New Keystores and Key Files

The XML signature provider, the XML encryption provider, and the Access Manager servers use the keystore configuration in the `AMConfig.properties` file for signing purposes. By default, Access Manager supports multiple XML signature algorithms. In this deployment example, you explicitly specify the RSA signature algorithm by setting the appropriate property in the `AMConfig.properties` file.

Use the following as your checklist for configuring Access Manager 2:

1. Create the Access Manager 1 keystore passwords.
2. Modify the `AMConfig.properties` file.
3. Modify the `amsaml.properties` file.

## ▼ To Create the Access Manager 2 Keystore Passwords

- 1 As a root user, log into the Access Manager 2 host.

- 2 Create a `.storepass` file.

```
# cd /etc/opt/SUNWam/config
# /opt/SUNWam/bin/ampassword -e passwordam > .storepass
```

- 3 Create a `.keypass` file.

```
# pwd /etc/opt/SUNWam/config
# /opt/SUNWam/bin/ampassword -e keypasswordam > .keypass
```

## ▼ To Modify the `AMConfig.properties` File

- 1 Go to the following directory:

```
/etc/opt/SUNWam/config
```

Make a backup of the `AMConfig.properties` file before you make changes.

- 2 In `AMConfig.properties`, set the following properties as in this example:

```
com.sun.identity.saml.xmlsig.keystore=/etc/opt/SUNWam/config/amkeystore
com.sun.identity.saml.xmlsig.storepass=/etc/opt/SUNWam/config/.storepass
com.sun.identity.saml.xmlsig.keypass=/etc/opt/SUNWam/config/.keypass
com.sun.identity.saml.xmlsig.certalias=LoadBalancer-3
...
com.sun.identity.jss.donotInstallAtHighestPriority=true
```

- 3 Uncomment the following property, and set the value as in this example:

```
com.sun.identity.saml.xmlsig.xmlSigAlgorithm=
http://www.w3.org/2000/09/xmldsig#rsa-sha1
```

Save the file.

## ▼ **Modify the `amsaml.properties` File**

- 1 **Go to the following directory:**

```
/opt/SUNWam/locale
```

- 2 **Open the `amsaml.properties` file and search for the following property:**

```
xmlsigalgorithm=http://www.w3.org/2000/09/xmlsig#dsa-sha1
```

- 3 **Change the method from `dsa-sha1` to `rsa-sha1`.**

```
xmlsigalgorithm=http://www.w3.org/2000/09/xmlsig#dsa-sha1
```

- 4 **Restart the Access Manager 2 server.**

```
# cd /opt/SUNWwbsvr/https-AccessManager-2.example.com  
# ./stop; ./start
```

## 9.5 Loading the Federation Manager Root CA Certificates into the Access Manager Servers

In this procedure you import a root CA certificate from Federation Manager 1 into the JDK trusted CA certificate for Access Manager 1. This step is not necessary if you are using one of the root CA certificates that come with JDK by default. The JDK default root CA certificates come from Verisign, Thwarte, and other major certificate issuers. In this deployment example, root CA certificates were obtained from certificate issuers that JDK does not recognize by default. So in this deployment example, the following procedure is necessary to establish trust among the local SSO provider (Federation Manager) and remote SSO providers (such as Access Manager).

Use the following as your checklist for loading the Federation Manager root CA certificates onto the Access Manager web containers:

1. [Load the root CA certificate into the Access Manager 1 web container.](#)
2. [Load the root CA certificate into the Access Manager 2 web container.](#)

## ▼ **To Load the Root CA Certificate into the Access Manager 1 Web Container**

- 1 **As a root user, log into the Access Manager 1 host.**

## 2 Locate the JAVAHOME directory and JDK keystore directory for the Access Manager 1 web container.

```
#cd /opt/SUNWwbsvr/https-AccessManager-1.example.com/config
# view server.xml
```

Locate the following JAVA javahome entry. In this deployment example, it looks like this:

```
<JAVA javahome="/usr/jdk/entsys-j2se"
```

To find the JDK keystore file, append the following to the javahome path:

```
/jre/lib/security
```

For example, in this deployment example, the JDK keystore is in the following directory:

```
/usr/jdk/entsys-j2se/jre/lib/security
```

This directory contains the Access Manager JDK trusted CA files.

## 3 Obtain a copy of the Federation Manager 1 JDK root CA certificate.

You can obtain a copy from the certificate issuer. Or you can copy the certificate stored on the Federation Manager 1 host.

In this deployment example, the Federation Manager 1 root CA certificate has already been copied to the following directory on Access Manager 1:

```
/net/slappd/export/share/cacert
```

## 4 Import the Federation Manager root CA certificate into the Access Manager JDK keystore.

The alias rootCA represents the name of the root CA certificate you want to import.

```
# cd /usr/jdk/entsys-j2se/jre/lib/security
# keytool -import -keystore cacerts -alias rootCA
-file /net/slappd/export/share/cacert
Enter keystore password: changeit
Owner: CN=Certificate Manager, OU=Identity Services,
O=Sun Microsystems Inc., L=Santa Clara, ST=California, C=US
Issuer: CN=Certificate Manager, OU=Identity Services,
O=Sun Microsystems, Inc., L=Santa Clara, ST=California, C=US
Serial number:320
Valid from Mon Aug 16 00:00:00 PDT 2004 until: Mon Aug 16 00:00:00 PDT 2032
Certificate fingerprints:
    MDS:    CD:07:DF:A6:CA:B9:AB:94:FF:CF:17:35:AB:C2:C2:51
    SHA1:9A:B5:F7:54:DE:8A:BC:E9:F6:1D:F1:5B:71:46:72:9E:F0:4E:B8:7A
Trust this certificate? [no]: yes
Certificate was added to keystore.
```

**5 To verify that the root CA certificate was successfully imported, run the list command:**

```
# cd /usr/jdk/instances/jdk1.5.0/jre/lib/security
# keytool -list -keystore cacerts -alias rootCA -rfc
Enter keystore password: changeit
Alias name: rootCA
Creation date: Mar 9, 2007
Entry type: trustedCertEntry

-----BEGIN CERTIFICATE-----
MIICjjCCAjjigAwIBAgICAYAwDQYJKoZIhvcNAQEFBQAwgZlxczAJBgNVBAYTA1VTRMRwEYDQYJ
EwpDYWxpZm9ybmlhMQRwEgYDVQQHEwTYW50YSBDbGFyYTEeMBwGA1UEChMVU3VvIE1pY3Jvc3lz
dGVtcyBJbmMuMURowGAYDVQQLExFJZGVudG10eSBTZjJ2aWNLczEcMBoGA1UEAxMTQ2VydgLmaWNh
dGUgTWFuYWdlcjAeFw0wNDA4MjYwNzAwMDBaFw0zMjA4MjYwNzAwMDBaMIGSMQswCQYDVQGEwJV
UzETMBEGA1UECBMKQ2FsaWZvcj5pYTEUMBIGA1UEBxMLU2FudGEGQ2xhcmeXhJAcBgNVBAoTFVFN1
biBNaW9yb3N5c3RlbXMGSw5jLjEaMBGGA1UECzMRSWRlbnRpdHkgU2VydmljZXMxHDAAgNBVBA
MT E0NlnRzmljYXRlIE1hbmFnZXIwXDANBgkqhkiG9w0BAQEFAANLADBIAkEArPzFAYBufzrX2i7G
/HhBi1RtEjYDHcy15WwytK6ZwbfXUMeyGadHweoZni0BU3VKdHhJIDCjqMMN25/rEM5ozwIDAQAB
o3YwdDARBgllghkgBhvhCAQEEBAMCAAcwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUO6AhN+VM
J+xbI0tNcOXtwwNQq64wHwYDVR0jBBgwFoAUO6AhN+VMJ+xbI0tNcOXtwwNQq64wDgYDVR0PAQH/
BAQDAgGGMA0GCSqGSIb3DQEBBQUAA0EAVHUPw/JfaTYTU8rHjR+6Xr6GqNbaT4eZtNXs5wIYljwL
HvLjL/AITbxrinqfFi0B2JAOW+gLxo4j6LV6W9/2Mw==
-----END CERTIFICATE-----
```

**▼ To Load the Root CA Certificate into the Access Manager 2 Web Container**

- 1 As a root user, log into the Access Manager 2 host.
- 2 Locate the JAVAHOME directory and JDK keystore directory for the Access Manager 2 web container.

```
#cd /opt/SUNWwbsvr/https-AccessManager-2.example.com/config
# view server.xml
```

Locate the following JAVA javahome entry. In this deployment example, it looks like this:

```
<JAVA javahome="/usr/jdk/entsys-j2se"
```

To find the JDK keystore file, append the following to the javahome path:

```
/jre/lib/security
```

For example, in this deployment example, the JDK keystore is in the following directory:

```
/usr/jdk/entsys-j2se/jre/lib/security
```

This directory contains the Access Manager JDK trusted CA files.

### 3 Obtain a copy of the Federation Manager 1 root CA certificate.

You can obtain a copy from the certificate issuer. Or you can copy the certificate stored on the Federation Manager 1 host.

In this deployment example, the Federation Manager 1 root CA certificate has already been copied to the following directory on Access Manager 1:

```
/net/slapd/export/share/cacert
```

### 4 Import the Federation Manager root CA certificate into the Access Manager JDK keystore.

The alias `rootCA` represents the name of the root CA certificate you want to import.

```
# cd /usr/jdk/entsys-j2se/jre/lib/security
# keytool -import -keystore cacerts -alias rootCA
-file /net/slapd/export/share/cacert
Enter keystore password: changeit
Owner: CN=Certificate Manager, OU=Identity Services,
O=Sun Microsystems Inc., L=Santa Clara, ST=California, C=US
Issuer: CN=Certificate Manager, OU=Identity Services,
O=Sun Microsystems, Inc., L=Santa Clara, ST=California, C=US
Serial number:320
Valid from Mon Aug 16 00:00:00 PDT 2004 until: Mon Aug 16 00:00:00 PDT 2032
Certificate fingerprints:
    MDS:    CD:07:DF:A6:CA:B9:AB:94:FF:CF:17:35:AB:C2:C2:51
    SHA1:9A:B5:F7:54:DE:8A:BC:E9:F6:1D:F1:5B:71:46:72:9E:F0:4E:B8:7A
Trust this certificate? [no]: yes
Certificate was added to keystore.
```

### 5 To verify that the root CA certificate was successfully imported, run the `list` command:

```
# cd /usr/jdk/instances/jdk1.5.0/jre/lib/security
# keytool -list -keystore cacerts -alias rootCA -rfc
Enter keystore password: changeit
Alias name: rootCA
Creation date: Mar 9, 2007
Entry type: trustedCertEntry

-----BEGIN CERTIFICATE-----
MIICjjCCAjigAwIBAgICAYAwDQYJKoZIhvcNAQEFBQAwZiExCzAJBgNVBAYTAlVTMRMwEQYDVQQKI
EwpDYWxpZm9ybmlhMRQwEgYDVQQHEwtTYW50YSBDbG9yYTEeMBwGA1UEChMVU3VvIE1pY3Jvc3lz
dGVtcyBJbmMuMUR0GAYDVQQLEXFJZGVudG10eSBTZjJ2aWNLczEcmBoGA1UEAxMTQ2VydGlmawNh
dGUgTWFuYwYwYDljAeFw0wNDA4MjYwNzAwMDBaFw0zZmJhMjYwNzAwMDBaMIGSMQswCQYDVQQGEwJV
UzETMBEGA1UECBMkQ2FsaWZvcm5pYTEUMBIGA1UEBxMLU2FudGEgQ2xhcmlhZjAcBgNVBAoTFVNI
biBNaW9yb3N5c3RlbXMGSw5jLjEaMBGGA1UECxMRSWRlbnRpdHkgU2VydmljZXhHDAaBgNVBAMT
E0NlcnRpdzmljYXRlIE1hbmFnZXIwXDAuNDAuNDAuNDAuNDAuNDAuNDAuNDAuNDAuNDAuNDAuNDAu
/HhBi1RtEjYDHcy15WytK6ZwbfXUMeyGadHweoZni0BU3VKdHhJIDCjQMMN25/rEM5ozwIDAQAB
o3YwdDARBgIghkgBhvCAQEBAAMCAAcwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUO6AhN+VM
J+xbI0tNcOXtwwNQq64wHwYDVR0jBBgwFoAUO6AhN+VMJ+xbI0tNcOXtwwNQq64wDgYDVR0PAQH/
BAQDAgGGMAGCSqGSIb3DQEBAQA0EAVHUPw/JfaTYTU8rHjR+6XR6GqNbaT4eZtNXs5wIYLjwL
```

```
HvLjL/AITbxrinqfFi0B2JAOW+gLxo4j6LV6W9/2Mw==  
-----END CERTIFICATE-----
```



# Configuring SAMLv2 Metadata for the Access Manager Servers

---

Use the following as your checklist for configuring SAMLv2 metadata for the Access Manager servers:

1. [Create a circle of trust.](#)
2. [Configure the SAMLv2 Service Provider metadata.](#)
3. [Load the SAMLv2 metadata.](#)

## 10.1 Creating a Circle of Trust

When you create metadata for the Identity Provider, the Identity Provider entity is added to a circle of trust. A circle of trust is used to group Service Providers and Identity Providers in a secure, trusted environment. Other remote provider entities can be added to the circle of trust. Whenever the SAMLv2 protocol is initiated, the SAMLv2 plug-in determines which circle of trust the requesting entity belongs to, and what other providers are available to interact with it. All entities within the same circle of trust can participate in the SAMLv2 protocols.

### ▼ To Create a Circle of Trust

- 1 **As a root user, log into the Access Manager 1 host.**

- 2 **Run the `cotcreate` command:**

```
# /opt/SUNWam/saml2/bin/saml2meta cotcreate -u amadmin  
-w 4m4dmin1 -r /users -t saml2_circle_of_trust  
Circle of trust "saml2_circle_of_trust" is created successfully.
```

## 10.2 Configuring the SAMLv2 Identity Provider Metadata

Federation Manager provides two metadata templates you can customize to meet your needs. For examples of customized metadata templates, see “7.2.1 Sample Metadata Template Files” on page 141 at the end of this chapter.

### ▼ To Generate and Customize the Identity Provider Template Files

1 As a root user, log into the Access Manager 1 host.

2 Go to the following directory:

```
/opt/SUNWam/saml2/bin
```

3 Generate the SAMLv2 template files.

```
# ./saml2meta template -u amadmin -w 4m4dmin1 -e loadbalancer-3.example.com
-d /users/idp -b LoadBalancer-3 -g LoadBalancer-3-enc
-m /etc/opt/SUNWam/config/saml2-idp-template.xml
-x /etc/opt/SUNWam/config/saml2-idp-extended-template.xml
Hosted entity descriptor for realm "/" was written to the file
"/etc/opt/SUNWam/config/saml2-idp-template.html" successfully.
Hosted entity config for realm "/" was written to the file
"/etc/opt/SUNWam/config/saml2-idp-extended-template.html" successfully.
```

The `saml2-idp-extended-template.xml` is similar to the standard `saml2-idp-template.xml` file. However, the extended file contains data about the SAMLv2 plug-in that is specific to Federation Manager.

4 Customize the `saml2-idp-template.xml` file.

When the file is first generated, default values are automatically generated and placed in the file. You must manually change these values to match the actual deployment environment. In this deployment example, a load balancer with SSL termination is being used. So you must modify the file to use the HTTPS protocol and the load balancer service URL.

```
# vi /etc/opt/SUNWam/config/saml2-idp-template.xml
```

a. In each location URL and each response location URL, change the protocol `http` to `https`.

Search for each occurrence of location and response location to be sure you have changed each URL.

b. Globally change all occurrences of `AccessManager-1` to `LoadBalancer-3`.

**c. Globally change all occurrences of 1080 to 9443.**

Save the file.

**5 Customize the saml2-sp-extended-template.xml file.**

```
# vi /etc/opt/SUNWam/config/saml2-idp-extended-template.xml
```

**a. Modify the following attribute-pair values to enable XML signing.**

```
<Attribute name="wantArtifactResponseSigned">
    <Value>true</Value>
<Attribute name="wantLogoutRequestSigned">
    <Value>true</Value>
<Attribute name="wantLogoutResponseSigned">
    <Value>true</Value>
<Attribute name="wantMNIRequestSigned">
    <Value>true</Value>
<Attribute name="wantMNIResponseSigned">
    <Value>true</Value>
<Attribute name="cotlist">
    <Value>saml2_circle_of_trust</Value>
```

**b. Set the following parameter value:**

```
<EntityConfig xmlns="urn:sun:fm:SAML:2.0:entityconfig"
    xmlns:fm="urn:sun:fm:SAML:2.0:entityconfig"
    hosted="1"
```

This indicates that you are using the local hosted configuration. A 0 value indicates that the configuration is provided by a remote host.

**6 Load the metadata.**

See [“7.3 Loading the Service Provider SAMLv2 Metadata”](#) on page 146.

## 10.3 Loading the SAMLv2 Metadata

When you load the SAMLv2 metadata into Directory Server, the Service Provider entity configuration is created. The entity configuration enables the SAMLv2 plug-in to recognize all SAMLv2 protocol URLs. The SAMLv2 metadata is also used for exchanging data with remote parties.



EXAMPLE 10-1 Modified saml2-idp-template.xml File (Continued)

```

    <KeyDescriptor use="encryption">
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <X509Data>
EwpDYWxpZm9ybmlhMRQwEgYDVQQHEwtTYW50YSBDbGFyYTEeMBwGA1UEChMVU3VuIE1pY3Jvc3lz
dGVtcyBJbmMuMR0wGAYDVQQLExFJZGVudG10eSBTZjJ2aWNlczEcMBoGA1UEAxMTQ2V4
dGUgTWFuYWdlcjAeFw0wNzAzMDcyMjAxMTVaFw0xMDEyMDEyMjAxMTVaMDsxFDASBgNVBAoTC2V4
YW1wbGUuY29tMSMwIQYDVQQDEExpM2FkQmFsYW5jZlItMy5leGFtcGxlLmNvbTcBnzANBgkqhkiG
HREETAPgQ1tYVxsYUBzdW4uY29tMA0GCSqGSIb3DQEBBAAUAA0EAegbmnOz2Rvpj9bludb9lEeVa
OA46zRiyt4BP1bgIaFyG6P7GWSddMi/14EimQjjDbr4ZfvLEdPJmimHEXZY3KQ==
        </KeyInfo>
      </EncryptionMethod>
    </KeyDescriptor>
    <ArtifactResolutionService
      index="0"
      isDefault="1"/>
    <SingleLogoutService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
    </SingleLogoutService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
    <ManageNameIDService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
      ResponseLocation="https://LoadBalancer-3.example.com:9443/
        amserver/IDPMniRedirect/metaAlias/idp"/>
    <ManageNameIDService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
      Location="https://LoadBalancer-3.example.com:9443/amserver/
        IDPMniSoap/metaAlias/idp"/>
    <NameIDFormat>
      urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
    </NameIDFormat>
    <NameIDFormat>
      urn:oasis:names:tc:SAML:2.0:nameid-format:transient
    </NameIDFormat>
    <SingleSignOnService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
      Location="https://LoadBalancer-3.example.com:9443/amserver/
        SSORedirect/metaAlias/idp"/>
    <SingleSignOnService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
      Location="https://LoadBalancer-3.example.com:9443/amserver/
        SSOSoap/metaAlias/idp"/>
  </IDPSSODescriptor>
</EntityDescriptor>

```

## EXAMPLE 10-2 Modified saml2-idp-metadata-template.xml File

```
<EntityConfig xmlns="urn:sun:fm:SAML:2.0:entityconfig"
  xmlns:fm="urn:sun:fm:SAML:2.0:entityconfig"
  hosted="1"
  entityID="loadbalancer-3.example.com">

  <IDPSSOConfig metaAlias="/users/idp">
    <Attribute name="signingCertAlias">
      <Value>LoadBalancer-3</Value>
      <Value>LoadBalancer-3-enc</Value>
    </Attribute>
  </Attribute>
  <Attribute name="basicAuthUser">
  <Attribute name="basicAuthPassword">
    <Value></Value>
    <Value>>false</Value>
  </Attribute>
  <Attribute name="autofedAttribute">
    <Value></Value>
  </Attribute>
  <Attribute name="assertionEffectiveTime">
    <Value>600</Value>
  </Attribute>
  <Attribute name="idpAuthncontextMapper">
  </Attribute>
  <Attribute name="idpAuthncontextClassrefMapping">
  </Attribute>
  <Attribute name="idpAccountMapper">
  </Attribute>
  <Attribute name="idpAttributeMapper">
  </Attribute>
  <Attribute name="attributeMap">
    <Value>EmailAddress=mail</Value>
    <Value>Telephone=telephonenumber</Value>
  </Attribute>
  <Attribute name="wantNameIDEncrypted">
    <Value></Value>
  </Attribute>
  <Attribute name="wantArtifactResolveSigned">
    <Value>>true</Value>
  </Attribute>
  <Attribute name="wantLogoutRequestSigned">
    <Value>>true</Value>
  </Attribute>
  <Attribute name="wantLogoutResponseSigned ">
    <Value>>true</Value>
  </Attribute>
```

EXAMPLE 10-2 Modified saml2-idp-metadata-template.xml File (Continued)

```
<Attribute name="wantMNIRequestSigned">
  <Value>true</Value>
</Attribute>
<Attribute name="wantMNIResponseSigned">
  <Value>true</Value>
</Attribute>
<Attribute name="cotlist">
  <Value>saml2_circle_of_trust</Value>
</Attribute>
</IDPSSOConfig>
</EntityConfig>
```





PART IV

Exchanging Metadata Between Identity  
Provider and Service Provider



# Loading Identity Provider and Service Provider Metadata

---

This chapter provides instructions for making Service Provider metadata available to the Identity Provider, and for making Identity Provider metadata available to the Service Provider.

## 11.1 Loading Service Provider Metadata into the Access Manager Servers

Use the following as your checklist for enabling the exchange of metadata between the Service Provider and Identity Provider:

1. [Load the Service Provider metadata into the Identity Provider servers.](#)
2. [Load the Identity Provider metadata into the Service Provider servers.](#)

### ▼ To Load the Service Provider Metadata into the Identity Provider Servers

- 1 As a root user, log into the Access Manager 1 host.
- 2 Copy the following Service Provider configuration files from the Federation Manager 1 host to the Access Manager 1 host:

```
/etc/opt/SUNWam/config/saml2-sp-template.xml  
/etc/opt/SUNWam/config/saml2-sp-extended-template.xml
```

In this deployment example, the files are copied to the following directory on the Access Manager host:

```
/etc/opt/SUNWam/config/
```

**3 Customize the saml2-sp-extended-template.xml file.****a. Go to the following directory:**

```
/etc/opt/SUNWam/config/
```

**b. Open the file saml2-sp-extended-template.xml.****c. Set the following parameter value:**

```
<EntityConfig xmlns="urn:sun:fm:SAML:2.0:entityconfig"
              xmlns:fm="urn:sun:fm:SAML:2.0:entityconfig"
              hosted="0"
```

This indicates that you are using the a configuration from a remote host. A 1 value indicates that the configuration is provided by the local host.

Save the file.

**4 Load the customized Service Provider configuration files.**

```
# /opt/SUNWam/saml2/bin/saml2meta
import -u amadmin -w 4m4dmin1 -r /users
-m /etc/opt/SUNWam/config/saml2-sp-template.xml
-x /etc/opt/SUNWam/config/saml2-sp-extended-template.xml
```

**5 Restart the Access Manager Servers****a. As a root user, log into the Access Manager 1 host.**

```
# cd /opt/SUNWwbsvr/https-AccessManager-1.example.com
# ./stop;./start
```

**b. As a root user, log into the Access Manager 2 host.**

```
# cd /opt/SUNWwbsvr/https-AccessManager-2.example.com
# ./stop;./start
```

**6 Verify that both Service Provider and Identity Provider belong to the same circle of trust.**

Run the cotmember command to display a list of entities in the circle of trust.

```
# /opt/SUNWam/saml2/bin/saml2meta cotmember -u amadmin -w 4m4dmin1
-r /users -t saml2_circle_of_trust
Entity ID:LoadBalancer-9.siroe.com
Entity ID:LoadBalancer-3.example.com
Circle of trust "saml2_circle_of_trust" is listed successfully.
```

## ▼ To Load the Identity Provider Metadata into the Service Provider Servers

- 1 As a root user, log into the Federation Manager 1 host.
- 2 Copy the following Identity Provider configuration files from the Access Manager host to the Federation Manager host:

```
/etc/opt/SUNWam/config/saml2-idp-template.xml
/etc/opt/SUNWam/config/saml2-idp-extended-template.xml
```

In this deployment example, the files are copied to the following directory on the Federation Manager host:

```
/etc/opt/SUNWam/config/
```

- 3 Customize the `saml2-idp-extended-template.xml` file.

```
# cd /etc/opt/SUNWam/config/
# vi saml2-idp-extended-template.xml
```

- a. Go to the following directory:
- b. Open the `saml2-idp-extended-template.xml` file.
- c. Set the following parameter value:

```
<EntityConfig xmlns="urn:sun:fm:SAML:2.0:entityconfig"
              xmlns:fm="urn:sun:fm:SAML:2.0:entityconfig"
              hosted="0"
```

This indicates that you are using the a configuration from a remote host. A 1 value indicates that the configuration is provided by the local host.

Save the file.

- 4 Load the customized Identity Provider configuration files.

```
# /opt/SUNWam/saml2/bin/saml2meta
-i /var/opt/SUNWam/fm/war_staging import -u amadmin -w 11111111
-m /etc/opt/SUNWam/config/saml2-idp-template.xml
-x /etc/opt/SUNWam/config/saml2-idp-extended-template.xml
File "/etc/opt/SUNWam/config/idp/saml2-idp-template.xml" was
imported successfully.
File "/etc/opt/SUNWam/config/idp/saml2-idp-extended-template.xml" was
imported successfully.
```

**5 Restart the Federation Manager Servers.**

**a. As a root user, log into the Federation Manager 1 host.**

```
# cd /opt/SUNWwbsvr/https-FederationManager-1.siroe.com
# ./stop; ./start
```

**b. As a root user, log into the Federation Manager 2 host.**

```
# cd /opt/SUNWwbsvr/https-FederationManager-2.siroe.com
# ./stop; ./start
```

**6 Verify that both Service Provider and Identity Provider belong to the same circle of trust.**

Run the cotmember command to display a list of entities in the circle of trust.

```
# /opt/SUNWam/saml2/bin/saml2meta -i /var/opt/SUNWam/fn/war_staging
cotmember -u amadmin -w 11111111 -t saml2_circle_of_trust
Entity ID:loadbalancer-9.siroe.com
Entity ID:loadbalancer-3.example.com
Circle of trust "saml2_circle_of_trust" is listed successfully.
```

# Verifying that SAMLv2 Protocols are Working Properly

---

You can perform simple tests to verify that Single Sign-On is working properly and that accounts are federated properly. This chapter provides detailed information about the following groups of tasks:

- “12.1 Creating Test Users” on page 191
- “12.2 Testing Basic SAMLv2 Protocols” on page 193

## 12.1 Creating Test Users

Use the following as your checklist for creating test users:

1. [Create a test Identity Provider user.](#)
2. [Create a test Service Provider user.](#)

### ▼ To Create a Test Identity Provider User

- 1 **Using a browser, go to the following URL:**

`https://LoadBalancer-3.example.com:9443/amserver`

- 2 **Log into the Access Manager 1 console:**

User Name: `amadmin`

Password: `4m4din1`

- 3 **On the Realms page, click the realm name users.**
- 4 **On the “Edit Realm-users” page, click the Subjects tab, and then click the Users subtab.**
- 5 **On the New User pager, provide the following information:**

ID: **idpuser**  
First Name: **idp**  
Last Name: **user**  
Full Name: **idp user**  
Password: **idpuser**  
Password confirm: **idpuser**

- 6 Click **Create**, and then log out.

## ▼ To Create a Test Service Provider User

- 1 Log into Directory Server 3SP console:

User Name: **cn=Directory Manager**

Password: **11111111**

- 2 Open the **DirectoryServer-3SP** console, and click the **Directory** tab.
- 3 Expand the **o=siroeusers.com** node.
- 4 Right-click the **People** object, and then choose **New > User**.
- 5 In the **Create New User** page, provide the following information:

First Name: **sp**

Last Name: **user**

Common Name: **sp user**

User ID: **spuser**

Password confirm: **spuser**

Password confirm: **spuser**

- 6 Click **OK**.

The user **spuser** is now listed in the list of users.



## 12.2 Testing Basic SAMLv2 Protocols

Use the following as your checklist for testing basic SAMLv2 protocols are working properly:

1. Verify that basic Login and Logout work properly.
2. Verify that Single Sign-On works properly.
3. Verify that Single Logout works properly.

### ▼ To Verify that Basic Login and Logout Work Properly

**1 Go to the following Federation Manager URL:**

<https://LoadBalancer-9.siroe.com:3443/federation/UI/Login>

**2 Log in to the Federation Manager console using the following information:**

User Name: **spuser**

Password: **spuser**

The following message is displayed:

Information: Welcome to Federation Manager. You have successfully authenticated.

**3 Close the Browser.**

This test verifies that Federation is configured properly and that basic login and logout operations work properly through the Federation Manager load balancer.

---

**Note** – Before proceeding with SSO testing, be sure that the cookie that contains session information is deleted. You can do this in one of two ways. You can clear the browser of all cookies (see your browser documentation for detailed instructions). Or you can close the browser and reopen it.

---

### ▼ To Verify that Single Sign-On Works Properly on Initial Login

**1 In the browser location field, enter the following URL:**

<https://LoadBalancer-9.siroe.com:3443/federation/saml2/jsp/spSSOInit.jsp?metaAlias=/sp&idpEntityID=loadbalancer-3.example.com>

The Access Manager login page is displayed.

**2 Log in to the Access Manager console using the following information:**

User Name: **idpuser**

Password: **idpuser**

The Service Provider (Federation Manager) login page is displayed.

**3 Log in to the Federation Manager console using the following information:**

User Name: **spuser**

Password: **spuser**

An HTML page is displayed and contains the following message, “Single Sign-on succeeded.” Notice that the user signs in to both Access Manager and Federation Manager only on the first login.

Do not log out or close the browser at this time. Proceed to the next task, “To Verify that Single Logout Works Properly.”

## ▼ To Verify that Single Logout Works Properly

● **In the browser location field, enter the following URL:**

<https://LoadBalancer-9.siroe.com:3443/federation/saml2/jsp/spSingleLogoutInit.jsp?metaAlias=/sp&idpEntityID=loadbalancer-3.example.com>

An HTML page is displayed and contains the following message, “SP initiated Single Logout succeeded.”

---

**Note** – Do not log out at this time. Proceed to the next task, “To Verify that Single Sign-On Works Properly on Subsequent Login.”

---

## ▼ To Verify that Single Sign-On Works Properly on Subsequent Login

**1 In the browser location field, enter the following URL:**

<https://LoadBalancer-9.siroe.com:3443/federation/saml2/jsp/spSSOinit.jsp?metaAlias=/sp&idpEntityID=loadbalancer-3.example.com>

The Access Manager login page is displayed.

**2 Log in to the Access Manager console using the following information:**

User Name: **idpuser**

Password: **idpuser**

An HTML page is displayed and contains the following message, “Single Sign-on succeeded.” Note that the user logs in to only Access Manager and is not prompted to log into Federation Manager. This verifies that SSO is working properly.



PART V

Setting Up Policy Agents in the Service  
Provider Site



# Installing and Configuring J2EE Policy Agents

---

This chapter contains detailed information about the following groups of tasks:

- “13.1 Creating J2EE Policy Agent Profiles on the Federation Manager Servers” on page 199
- “13.2 Installing Application Server 3 and J2EE Policy Agent 3” on page 201
- “13.3 Completing the J2EE Policy Agent 3 Installation” on page 205
- “13.4 Installing Application Server 4 and J2EE Policy Agent 4” on page 208
- “13.5 Completing the J2EE Policy Agent 4 Installation” on page 212
- “13.6 Configuring the J2EE Policy Agents Load Balancer” on page 216
- “13.8 Configuring the J2EE Policy Agents to Work with the J2EE Policy Agents Load Balancer” on page 222
- “13.9 Configuring the J2EE Policy Agents Load Balancer to Participate in SAMLv2 Protocols” on page 225

## 13.1 Creating J2EE Policy Agent Profiles on the Federation Manager Servers

When you install the J2EE Policy Agent, the agent profile is used to retrieve the J2EE Policy Agent user password. At this point, the J2EE Policy Agent authentication still occurs through flat files. This new account will be used by J2EE Policy Agent to authenticate to the Federation Manager servers.

Use the following as your checklist for creating J2EE Policy Agent profiles on the Federation Manager Servers:

1. [Create an Agent Profile on Federation Manager 1.](#)
2. [Create an Agent Profile on Federation Manager 2.](#)

## ▼ To Create a J2EE Policy Agent Profile on Protected Resource 3

**1 As a root user, log into the Protected Resource 3 host.**

**2 Create an agent profile.**

Create a text file named `agent_profile_password`, and add to it a name for the new agent profile. Example:

```
# cd /export
# vi agent_profile_password
asagent
```

Save the file.

**3 Generate an encrypted password for the new agent profile.**

```
# cd /var/opt/SUNWam/fm/federation/users
# /opt/SUNWam/fm/bin/ampassword -i /var/opt/SUNWam/fm/war_staging --hash asagent
EW1Ck/Yw4kpyYs9jbu5Dx5pJaH8=
```

**4 Create a text file named `asagent.properties`, and add the agent profile password to the file.**

The J2EE Policy Agent installer requires this file for installation.

```
# vi asagent.properties
password=EW1Ck/Yw4kpyYs9jbu5Dx5pJaH8=
```

Save the file.

## ▼ To Create an J2EE Policy Agent Profile on Protected Resource 4

**1 As a root user, log into the Protected Resource 4 host.**

**2 Create an agent profile.**

Create a text file named `agent_profile_password`, and add to it a name for the new agent profile. Example:

```
# cd /export
# vi agent_profile_password
asagent
```

Save the file.



**3 Generate an encrypted password for the new agent profile.**

```
# cd /var/opt/SUNWam/fm/federation/users
# /opt/SUNWam/fm/bin/ampassword -i /var/opt/SUNWam/fm/war_staging --hash asagent
EW1Ck/Yw4kpyYs9jbu5Dx5pJaH8=
```

**4 Create a text file named `asagent.properties`, and add the agent profile password to the file.**

The J2EE Policy Agent installer requires this file for installation.

```
# vi asagent.properties
password=EW1Ck/Yw4kpyYs9jbu5Dx5pJaH8=
```

Save the file.

## 13.2 Installing Application Server 3 and J2EE Policy Agent 3

You must have the Sun Java System Application Server installer and the Sun J2EE Policy Agent installer mounted on Protected Resource 1. See [Chapter 2](#) at the beginning of this manual.

### ▼ To Install Application Server 3 on Protected Resource 3

**1 As a root user, log into the Application Server 3 host.****2 Start the Java Enterprise System installer with the `-nodisplay` option.**

```
# cd /mnt/Solaris_sparc
# ./installer -nodisplay
```

**3 When prompted, provide the following information:**

Welcome to the Sun Java(TM) Enterprise System; serious software made simple... <Press ENTER to Continue>	Press Enter.
<Press ENTER to display the Software License Agreement>	Press Enter.
Have you read, and do you accept, all of the terms of the preceding Software License Agreement [No]	Enter <b>y</b> .
Please enter a comma separated list of languages you would like supported with this installation [8]	Enter 8 for "English only."

Do you want to install the full set of Sun Java (TM) Enterprise System Products and Services? [Yes]	Enter <b>No</b> .
Enter a comma separated list of products to install, or press R to refresh the list []	Enter <b>14</b> to install Sun Java (TM) Application Server Enterprise Edition 8.1 2005Q4.
Component Selection – Selected Product Sun Java (TM) Application Server Enterprise Edition 8.1 2005Q4. Enter a comma separated list of products to install, or press R to refresh the list []	Enter <b>1, 3, 5, 6</b> to install Domain Administration Server, Command Line Administration Tool, PointBase Database, and the Sample Applications.
Press "Enter" to Continue or Enter a comma separated list of products to deselect... [1]	Press Enter.
Enter 1 to upgrade these shared components and 2 to cancel [1]	You are prompted to upgrade shared components only if the installer detects that an upgrade is required. Enter <b>1</b> to upgrade shared components.
Enter the name of the target installation directory for each product: Web Server [/opt/SUNWappserver] :	Accept the default value.
Data and Server Configuration [/var/opt/SUNWappserver]	Accept the default value.
System ready for installation Enter 1 to continue [1]	Enter <b>1</b> .
1. Configure Now - Selectively override defaults or express through 2. Configure Later - Manually configure following installation Select Type of Configuration [1]	Enter <b>1</b> .
Common Server Settings Enter Host Name [ProtectedResource-3]	Accept the default value.
Enter DNS Domain Name [siroe.com]	Accept the default value.
Enter IP Address [192.18.72.151]	Accept the default value.
Enter Server admin User ID [admin]	Accept the default value.
Enter Admin User's Password (Password cannot be less than 8 characters) []	For this example, enter <b>11111111</b> .
Confirm Admin User's Password []	Enter the same password to confirm it.
Enter System User [root]	Accept the default value.

Enter System Group [root]	Accept the default value.
Admin User Name: [admin]	Accept the default value.
Password (min. 8 characters) []	For this example, enter <b>11111111</b> .
Re-enter Password []	For this example, enter <b>11111111</b> .
Admin Port [4849]	Accept the default value.
JMX Port [8686]	Accept the default value.
HTTP Port [8080]	Accept the default value.
HTTPS Port [8181]	Accept the default value.
Master Password (min. 8 characters) [ ]	For this example, enter <b>11111111</b> .
Re-enter Master Password (min. 8 characters) [ ]	For this example, enter <b>11111111</b> .
Ready to Install 1. Install 2. Start Over 3. Exit Installation What would you like to do [1]	When ready to install, enter <b>1</b> .

#### 4 After you have exited the installer, start Application Server 3:

```
# cd /opt/SUNWappserver/appserver/bin
# ./asadmin start-domain --user admin --password 11111111
Starting Domain domain1, please wait.
Log redirected to /var/opt/SUNWappserver/domains/domain1/logs/server.log.

Domain domain1 started.
```

#### 5 To verify that the Application Server 3 is successfully installed, go to the Application Server URL:

<http://ProtectedResource-3:8080/index.html>

The default Application Server page is displayed and contains the following message: “Your server is up and running!”

## ▼ To Run the J2EE Policy Agent Installer on Application Server 3

### Before You Begin

You must obtain and unpack the J2EE Policy Agent software from the following Sun Microsystems web page: <http://www.sun.com/download/products.xml?id=43543381>.

#### 1 In the directory where you downloaded the J2EE Policy Agent TAR file, unpack the J2EE Policy Agent bits using the GNU `untar` utility. Example:

```
# cd /export
# gunzip SJS_Appserver_81_agent_2.2.tar.zip
```

```
# gtar -xvf /usr/sfw/bin/SJS_Appserver_81_agent_2.2.tar
```

---

**Note** – For .tar.gz archives, do not use a program other than GNU\_tar to untar the contents of the J2EE agent deliverables. Using a different program, such as another tar program, can result in some files not being extracted properly. To learn more about the GNU\_tar program, visit the following web site: <http://www.gnu.org/software/tar/tar.html>

---

## 2 Start the J2EE Policy Agent installer.

```
# cd /export/j2ee_agents/am_as81_agent/bin
# ./agentadmin --install
```

## 3 When prompted, provide the following information:

Enter the Application Server Config Directory Path [/var/opt/SUNWappserver/domains/domain1/config]	Accept the default value.
Enter the Application Server Instance name: [server]	Accept the default value.
Access Manager Services Host:	Enter <b>LoadBalancer-9.siroe.com</b> .
Access Manager Services port: [80]	Enter <b>3443</b> .
Access Manager Services Protocol: [http]	Enter <b>https</b> .
Access Manager Services Deployment URI: [/amserver]	Enter <b>/federation</b> .
Enter the Agent Host name:	<b>ProtectedResource-3.siroe.com</b>
Is the Domain administration server host remote? [false]	Accept the default value.
Enter the port number for Application Server instance [80]:	Enter <b>8080</b> .
Enter the Preferred Protocol for Application instance [http]:	Accept the default value.
Enter the Deployment URI for the Agent Application [/agentapp]	Accept the default value.
Enter the Encryption Key [d1ui072LoDGSD5ZEz0Z4e3bvaJN2f3wz]:	Accept the default value.
Enter the Agent Profile name:	Enter <b>asagent</b> .
Enter the path to the password file:	Enter <b>/export/agent_profile_password</b> .

Is the agent being installed on the DAS host for a remote instant [false]	Accept the default value.
Are the Agent and Access Manager installed on the same instance of Application Server? [false]:	Accept the default value.
Verify your settings and decide from the choices below: 1. Continue with Installation 2. Back to the last interaction 3. Start Over 4. Exit Please make your selection [1]:	Accept the default value.

- 4 After the installer has finished installing the agent, verify that installation was successful. You check can for installation errors in the following log file:**

```
/export/j2ee_agents/am_as81_agent/logs/audit/install.log
```

## 13.3 Completing the J2EE Policy Agent 3 Installation

The J2EE Policy Agent is not yet ready to begin working. A number of these tasks must be completed before the agent can do its job. Use the following as your checklist for completing the J2EE Policy Agents installation and configuration:

1. [Deploy the J2EE Policy Agent housekeeping application.](#)
2. [Enable the J2EE Policy Agent 3 to run in SSO-Only mode.](#)
3. [Initialize the Application Server 3 certificate database.](#)
4. [Deploy the sample agent application on Application Server 3.](#)
5. [Verify the use of the sample agent application on Application Server 3.](#)

### ▼ To Deploy the J2EE Policy Agent Housekeeping Application

The J2EE Policy Agent uses the agent housekeeping application for notifications and other internal functionality. This application is bundled with the agent binaries.

- 1 As a root user, log into the Application Server 1 host.**
- 2 Go to the following directory:**

```
/export/j2ee-agents/am_as81_agent/etc
```

**3 Run the following command:**

```
# /opt/SUNWappserver/appserver/bin/asadmin deploy --user admin
--password 11111111 --contextroot /agentapp agentapp.war
Command deploy executed successfully.
```

**▼ To Enable the J2EE Policy Agent 3 to Run in SSO-Only Mode****1 Go to the following directory:**

```
/export/j2ee_agents/am_as81_agent/agent_001/config
```

Make a backup copy of `AMAgent.properties`, and then modify the original `AMAgent.properties` file.

**2 Set the following property as in the example:**

```
com.sun.identity.agents.config.filter.mode = SSO_ONLY
```

Federation Manager can run only in SSO-Only mode. In order to communicate with Federation Manager, the policy agent must also run in SSO-Only mode.

**3 Add the following property**

```
com.ipplanet.am.naming.ignoreNamingService=true
```

When set to `true`, the policy agent ignores the Federation Manager naming service for session validation purposes. Instead, the policy agent uses the local naming service URL defined in the `com.ipplanet.am.naming.url` property elsewhere in this file.

Save the file.

**▼ To Initialize the Application Server 3 Certificate Database**

**Before You Begin** You must have access to the `certutil` command to complete this task. See [“2.11 Obtaining and Using the Certificate Database Tool” on page 38](#).

**1 Log into the Protected Resource 3 host.****2 Copy into a temporary directory the root CA certificate from the Federation Manager load balancer.**

For example, in this deployment example, the JDK keystore is in the following directory:

```
/usr/jdk/entsys-j2se/jre/lib/security
```

This directory contains the Federation Manager trusted CA files, including `cacert`.

**3 Go to the following directory:**

```
/var/opt/SUNWappserver/domains/domain1/config
```

This directory contains two files you will need. The files are named `cert8.db` and `key3.db`, and are installed by default with Application Server 8.1. By default, Application Server 8.1 uses the NSS certificate databases for SSL purposes. You must import the Federation Manager load balancer root CA certificate to this Application Server certificate database.

**4 Obtain a copy of the Federation Manager 1 root CA certificate.**

You can obtain a copy from the certificate issuer. Or you can copy the certificate stored on the Federation Manager 1 host.

In this deployment example, the Federation Manager 1 root CA certificate has already been copied to the following directory on Protected Resource 3:

```
/net/slapp/export/share/cacert
```

**5 In the directory where you have deployed the certutil utility, run the certutil command. Example:**

```
# certutil -A -n rootCA -t T,c,c -i /net/slapp/export/share/cacert -d .
```

**6 To verify that the certificate was properly initialized, list the certificates in the database:**

```
# certutil -L -n rootCA -d .
```

A list of certificates is displayed, and the initialized certificate file is included in the list.

## ▼ To Deploy the Sample Agent Application on Application Server 3

**1 As a root user, log into the Protected Resource 3 host.****2 Go to the following directory:**

```
/export/j2ee_agents/am_as81_agent/sampleapp/dist
```

**3 Run the deploy command:**

```
//opt/SUNWappserver/appserver/bin/asadmin deploy --host localhost
--port 4849 --user admin --password 11111111 --contextroot /agentsample
--name agentsample agentsample.ear
Command deploy executed successfully.
```

**4 Restart Application Server 3.**

```
# cd /opt/SUNWappserver/appserver/bin
# ./asadmin stop-domain
Domain domain1 stopped.
```

```
# ./asadmin start-domain --user admin --password 11111111
Domain domain1 started.
```

## ▼ To Verify the Use of the Sample Agent Application on Application Server 3

### 1 Go to the Application Server 3 URL:

```
http://ProtectedResource-3.siroe.com:8080/agentsample/index.html
```

### 2 Log in to the Federation Manager console using the following information:

User Name: spuser

Password: spuser

The Sample Application welcome page is displayed.

## 13.4 Installing Application Server 4 and J2EE Policy Agent 4

You must have the Sun Java System Application Server installer and the Sun J2EE Policy Agent installer mounted on Protected Resource 1. See [Chapter 2](#) at the beginning of this manual.

## ▼ To Install Application Server 4 on Protected Resource 4

### 1 As a root user, log into the Application Server 4 host.

### 2 Start the Java Enterprise System installer with the `-nodisplay` option.

```
# cd /mnt/Solaris_sparc
# ./installer -nodisplay
```

### 3 When prompted, provide the following information:

Welcome to the Sun Java(TM) Enterprise System; serious software made simple... <Press ENTER to Continue>	Press Enter.
<Press ENTER to display the Software License Agreement>	Press Enter.



Have you read, and do you accept, all of the terms of the preceding Software License Agreement [No]	Enter <b>y</b> .
Please enter a comma separated list of languages you would like supported with this installation [8]	Enter 8 for "English only."
Do you want to install the full set of Sun Java (TM) Enterprise System Products and Services? [Yes]	Enter <b>No</b> .
Enter a comma separated list of products to install, or press R to refresh the list []	Enter <b>14</b> to install Sun Java (TM) Application Server Enterprise Edition 8.1 2005Q4.
Component Selection – Selected Product Sun Java (TM) Application Server Enterprise Edition 8.1 2005Q4. Enter a comma separated list of products to install, or press R to refresh the list []	Enter <b>1, 3, 5, 6</b> to install Domain Administration Server, Command Line Administration Tool, PointBase Database, and the Sample Applications.
Press "Enter" to Continue or Enter a comma separated list of products to deselect... [1]	Press Enter.
Enter 1 to upgrade these shared components and 2 to cancel [1]	You are prompted to upgrade shared components only if the installer detects that an upgrade is required. Enter <b>1</b> to upgrade shared components.
Enter the name of the target installation directory for each product: Web Server [/opt/SUNWappserver] :	Accept the default value.
Data and Server Configuration [/var/opt/SUNWappserver]	Accept the default value.
System ready for installation Enter 1 to continue [1]	Enter <b>1</b> .
1. Configure Now - Selectively override defaults or express through 2. Configure Later - Manually configure following installation Select Type of Configuration [1]	Enter <b>1</b> .
Common Server Settings Enter Host Name [ProtectedResource-4]	Accept the default value.
Enter DNS Domain Name [siroe.com]	Accept the default value.
Enter IP Address [192.18.72.152]	Accept the default value.

Enter Server admin User ID [admin]	Accept the default value.
Enter Admin User's Password (Password cannot be less than 8 characters) []	For this example, enter <b>11111111</b> .
Confirm Admin User's Password []	Enter the same password to confirm it.
Enter System User [root]	Accept the default value.
Enter System Group [root]	Accept the default value.
Admin User Name: [admin]	Accept the default value.
Password (min. 8 characters) []	For this example, enter <b>11111111</b> .
Re-enter Password []	For this example, enter <b>11111111</b> .
Admin Port [4849]	Accept the default value.
JMX Port [8686]	Accept the default value.
HTTP Port [8080]	Accept the default value.
HTTPS Port [8181]	Accept the default value.
Master Password (min. 8 characters) [ ]	For this example, enter <b>11111111</b> .
Re-enter Master Password (min. 8 characters) [ ]	For this example, enter <b>11111111</b> .
Ready to Install 1. Install 2. Start Over 3. Exit Installation What would you like to do [1]	When ready to install, enter <b>1</b> .

#### 4 After you have exited the installer, start Application Server 4:

```
# cd /opt/SUNWappserver/appserver/bin
# ./asadmin start-domain --user admin --password 11111111
Starting Domain domain1, please wait.
Log redirected to /var/opt/SUNWappserver/domains/domain1/logs/server.log.

Domain domain1 started.
```

#### 5 To verify that the Application Server 4 is successfully installed, go to the Application Server URL:

<http://ProtectedResource-4:8080/index.html>

The default Application Server page is displayed and contains the following message: “Your server is up and running!”

## ▼ To Run the J2EE Policy Agent Installer on Application Server 4

**Before You Begin** You must obtain and unpack the J2EE Policy Agent software from the following Sun Microsystems web page: <http://www.sun.com/download/products.xml?id=43543381>

- 1 In the directory where you downloaded the J2EE Policy Agent TAR file, unpack the J2EE Policy Agent bits using the GNU `untar` utility. Example:

```
# cd /export
# gunzip SJS_Appserver_81_agent_2.2.tar.zip
# gtar -xvf /usr/sfw/bin/SJS_Appserver_81_agent_2.2.tar
```

---

**Note** – For `.tar.gz` archives, do not use a program other than GNU `tar` to untar the contents of the J2EE agent deliverables. Using a different program, such as another `tar` program, can result in some files not being extracted properly. To learn more about the GNU `tar` program, visit the following web site: <http://www.gnu.org/software/tar/tar.html>

---

- 2 Start the J2EE Policy Agent installer.

```
# cd /export/j2ee_agents/am_as81_agent/bin
# ./agentadmin --install
```

- 3 When prompted, provide the following information:

Enter the Application Server Config Directory Path [/var/opt/SUNWappserver/domains/domain1/config]	Accept the default value.
Enter the Application Server Instance name: [server]	Accept the default value.
Access Manager Services Host:	Enter <b>LoadBalancer-9.siroe.com</b> .
Access Manager Services port: [80]	Enter <b>3443</b> .
Access Manager Services Protocol: [http]	Enter <b>https</b> .
Access Manager Services Deployment URI: [/amserver]	Enter <b>/federation</b> .
Enter the Agent Host name:	<b>ProtectedResource-4.siroe.com</b>
Is the Domain administration server host remote? [false]	Accept the default value.
Enter the port number for Application Server instance [80]:	Enter <b>8080</b> .

Enter the Preferred Protocol for Application instance [http]:	Accept the default value.
Enter the Deployment URI for the Agent Application [/agentapp]	Accept the default value.
Enter the Encryption Key [d1ui072LoDGSD5ZEz0Z4e3bvaJN2f3wz]:	Accept the default value.
Enter the Agent Profile name:	Enter <b>asagent</b> .
Enter the path to the password file:	Enter <b>/export/agent_profile_password</b> .
Is the agent being installed on the DAS host for a remote instant [false]	Accept the default value.
Are the Agent and Access Manager installed on the same instance of Application Server? [false]:	Accept the default value.
Verify your settings and decide from the choices below: 1. Continue with Installation 2. Back to the last interaction 3. Start Over 4. Exit Please make your selection [1]:	Accept the default value.

- 4 After the installer has finished installing the agent, verify that installation was successful. You can check for installation errors in the following log file:**

`/export/j2ee_agents/am_as81_agent/logs/audit/install.log`

## 13.5 Completing the J2EE Policy Agent 4 Installation

The J2EE Policy Agent is not yet ready to begin working. A number of these tasks must be completed before the agent can do its job. Use the following as your checklist for completing the J2EE Policy Agents installation and configuration:

1. [Deploy the J2EE Policy Agent housekeeping application.](#)
2. [Enable the J2EE Policy Agent 4 to run in SSO-Only mode.](#)
3. [Initialize the Application Server 4 certificate database.](#)
4. [Deploy the sample agent application on Application Server 4.](#)
5. [Verify the use of the sample agent application on Application Server 4.](#)

## ▼ To Deploy the J2EE Policy Agent Housekeeping Application

The J2EE Policy Agent uses the agent housekeeping application for notifications and other internal functionality. This application is bundled with the agent binaries.

**1 As a root user, log into the Application Server 4 host.**

**2 Go to the following directory:**

```
/export/j2ee-agents/am_as81_agent/etc
```

**3 Run the following command:**

```
# /opt/SUNWappserver/appserver/bin/asadmin deploy --user admin
--password 11111111 --contextroot /agentapp agentapp.war
Command deploy executed successfully.
```

## ▼ To Enable the J2EE Policy Agent 4 to Run in SSO-Only Mode

**1 Go to the following directory:**

```
/export/j2ee_agents/am_as81_agent/agent_001/config
```

Make a backup copy of `AMagent.properties`, and then modify the original `AMagent.properties` file.

**2 Set the following property as in the example:**

```
com.sun.identity.agents.config.filter.mode = SSO_ONLY
```

Federation Manager can run only in SSO-Only mode. In order to communicate with Federation Manager, the policy agent must also run in SSO-Only mode.

**3 Add the following property**

```
com.iplanet.am.naming.ignoreNamingService=true
```

When set to `true`, the policy agent ignores the Federation Manager naming service for session validation purposes. Instead, the policy agent uses the local naming service URL defined in the `com.iplanet.am.naming.url` property elsewhere in this file.

Save the file.

## ▼ To Initialize the Application Server 4 Certificate Database

**Before You Begin** You must have access to the `certutil` command to complete this task. See “2.11 Obtaining and Using the Certificate Database Tool” on page 38.

**1 Log into the Protected Resource 4 host.**

**2 Copy into a temporary directory the root CA certificate from the Federation Manager load balancer.**

For example, in this deployment example, the JDK keystore is in the following directory:

```
/usr/jdk/entsys-j2se/jre/lib/security
```

This directory contains the Federation Manager trusted CA files, including `cacert`.

**3 Go to the following directory:**

```
/var/opt/SUNWappserver/domains/domain1/config
```

This directory contains two files you will need. The files are named `cert8.db` and `key3.db`, and are installed by default with Application Server 8.1. By default, Application Server 8.1 uses the NSS certificate databases for SSL purposes. You must import the Federation Manager load balancer root CA certificate to this Application Server certificate database.

**4 Obtain a copy of the Federation Manager 1 root CA certificate.**

You can obtain a copy from the certificate issuer. Or you can copy the certificate stored on the Federation Manager 1 host.

In this deployment example, the Federation Manager 1 root CA certificate has already been copied to the following directory on Protected Resource 4:

```
/net/slapd/export/share/cacert
```

**5 In the directory where you deployed the `certutil` utility, run the `certutil` command.  
Example:**

```
# certutil -A -n rootCA -t T,c,c -i /net/slapd/export/share/cacert -d .
```

**6 To verify that the certificate was properly initialized, list the certificates in the database:**

```
# certutil -L -n rootCA -d .
```

A list of certificates is displayed, and the initialized certificate file is included in the list.

## ▼ To Deploy the Sample Agent Application on Application Server 4

**1 As a root user, log into the Protected Resource 4 host.**

**2 Go to the following directory:**

```
/export/j2ee_agents/am_as81_agent/sampleapp/dist
```

**3 Run the deploy command:**

```
//opt/SUNWappserver/appserver/bin/asadmin deploy --host localhost
--port 4849 --user admin --password 11111111 --contextroot /agentsample
--name agentsample agentsample.ear
Command deploy executed successfully.
```

**4 Restart Application Server 4.**

```
# cd /opt/SUNWappserver/appserver/bin
# ./asadmin stop-domain
Domain domain1 stopped.
# ./asadmin start-domain --user admin --password 11111111
Domain domain1 started.
```

## ▼ To Verify the Use of the Sample Agent Application on Application Server 4

**1 Go to the Application Server 4 URL:**

```
http://ProtectedResource-4.siroe.com:8080/agentsample/index.html
```

**2 Log in to the Federation Manager console using the following information:**

User Name: spuser

Password: spuser

The Sample Application welcome page is displayed.

## 13.6 Configuring the J2EE Policy Agents Load Balancer

Load Balancer 10 can be located in a less-secured zone, and handles traffic for the J2EE Policy Agents.

Load Balancer 10 is configured for simple persistence so that browser requests from the same IP address will always be directed to the same J2EE Policy Agent instance. This guarantees that the requests from the same user session will always be sent to the same J2EE Policy Agent instance. This is important from the performance perspective. Each J2EE Policy Agent must validate the user session and evaluate applicable policies. The results are subsequently cached on the individual J2EE Policy Agent to improve the performance. If no load balancer persistence is set, and the same user's requests are spread across two agents, then each agent must build up its own cache. To do so, both agents must validate the session and evaluate policies. This effectively doubles the workload on the Access Manager servers, and cuts the overall system capacity by half. The problem becomes even more acute as the number of J2EE Policy Agents increases further.

As a general rule, in situations where each J2EE Policy Agent instance is protecting identical resources, some form of load balancer persistence is highly recommended for the performance reasons. The actual type of persistence may vary when a different load balancer is used, as long as it achieves the goal of sending the requests from the same user session to the same J2EE Policy Agent instance.

Use the following as your checklist for Configuring the J2EE Policy Agents load balancer:

1. [Configure the J2EE Policy Agents load balancer.](#)
2. [Terminate SSL at the J2EE Policy Agents load balancer.](#)

### ▼ To Configure the J2EE Policy Agents Load Balancer

- 1 **Go to URL for the Big IP load balancer login page and log in.**

`https://ls-f5.siroe.com`

User name: **username**

Password: **password**

- 2 **Request an SSL Certificate for Load Balancer 10.**

- a. **Log in to the BIG-IP load balancer.**

- b. **Click Proxies in the left pane.**



c. Click the **Cert Admin** tab, and then click the **“Generate New Key Pair/ Certificate Request”** button.

d. In the **Create Certificate Request** page, provide the following information:

Key Identifier: **LoadBalancer-10.siroe.com**

Organization: **siroe.com**

Domain Name: **LoadBalancer-10.siroe.com**

Email Address: **jdoe@siroe.com**

e. Click the **Generate Request** button.

f. In the **Generate Request** page, copy the request that looks similar to this:

```
-----BEGIN CERTIFICATE REQUEST-----
UmM77e50M63v1Z2A/505MA0GCSqGSIb3DQE0BAU
AMF8xCzAJBgNVBAYTAlVTMSAwHgYDVQKExdSU0
EgRGF0YSBTZW50eSwgSW5jLjEuMCwGA1UEC
xMLU2VjdXJlIFNlcnZlciBDZXJ0aWZpY2F0aW9u
IEF1dGhvcml0eTAeFw0wMTA4MDIwMDAwMDBaFw0
wMzA4MDIyMzU5NTlaMIGQMswCQYDVQGEwJVUz
ERMA8GA1UECBMlYmlyZ2luaWEuXETAPBgNVBACU
CjFpY2htb25kMSAwHgYDVQKFBdYXZhbGllciBU
ZWxlGhVYm9uZGluZy5jYXZ0ZWwuY29tMIGfMA0
GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8x/ldxo
2YnblilQLmpiezi0qb7ArVfI1ymXo/MKcbKjnY2
-----END CERTIFICATE REQUEST-----
```

g. Paste this text into a request form provided by a root certificate authority (CA) such as **Verisign** or **Thwarte**.

See the certificate authority website such as <http://www.verisign.com/> or <http://www.thawte.com/> for detailed instructions on submitting a certificate request.

3 After you receive the certificate from the issuer, install the SSL Certificate.

a. In the **BIG-IP** load balancer console, click the **Cert Admin** tab.

b. On the **Cert Admin** tab, click **Install Certificate**.

c. In the **Install SSL Certificate** page, paste the certificate text you received from the certificate issuer. Example:

```
-----BEGIN CERTIFICATE REQUEST-----
UmM77e50M63v1Z2A/505MA0GCSqGSIb3DQE0BAU
AMF8xCzAJBgNVBAYTAlVTMSAwHgYDVQKExdSU0
```

```

EgRGF0YsBTZWw1cmL0eSwgSw5jLjEuMCwGA1UEC
xMlU2VjdXJlIFNlcnZlciBDZXJ0aWZpY2F0aW9u
IEF1dGhvcml0eTAeFw0wMTA4MDIwMDAwMDBaFw0
wMzA4MDIyMzU5NTlaMIGQMQswCQYDVQGEwJVUz
ERMA8GA1UECBMlYyZ2luaWEtAPBgNVBACUC
FJpY2htb25kMSAwHgYDVQKFBdYXZhbGllciBU
ZWxlYm9uZGluZy5jYXZ0ZWwuY29tMIGfMA0
GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8x/1dxo
2YnblilQLmpiEzi0qb7ArVfI1ymXo/MKcbKjnY2
-----END CERTIFICATE REQUEST-----

```

**d. Click Install Certificate.**

**4 Create a Pool.**

A pool contains all the backend server instances.

**a. Open the Configuration Utility.**

Click “Configure your BIG-IP (R) using the Configuration Utility.”

**b. In the left pane, click Pools.**

**c. On the Pools tab, click the Add button.**

**d. In the Add Pool dialog, provide the following information:**

Pool Name	<b>federation _j2ee_agents</b>
Load Balancing Method	<b>Round Robin</b>
Resources	Add the IP address of both Application Server hosts. In this example:  <b>192.18.72.152:8080</b> (for Application Server 3)  <b>192.18.72.151:8080</b> (for Application Server 4)

**e. Click the Done button.**

**f. In the List of Pools, click the name of the pool you just created (federation\_j2ee\_agents).**

**5 Add a Virtual Server.**

If you encounter Javascript errors or otherwise cannot proceed to create a virtual server, try using Microsoft Internet Explorer for this step.

**a. In the left frame, Click Virtual Servers.**

- b. On the **Virtual Servers** tab, click the **Add** button.
- c. In the **Add a Virtual Server** dialog box, provide the following information:
 

Address	192.18.69.14 (for LoadBalancer-10.siroe.com)
Services Port	1080
Pool	federation_j2ee_agents
- d. Continue to click **Next** until you reach the **Pool Selection** dialog box.
- e. Click the **Done** button.

## ▼ To Terminate SSL at the J2EE Policy Agents Load Balancer

You should still be logged into the BigIP load balancer program after the last task.

- 1 **Create an SSL Proxy.**
- 2 **Click the Proxies tab, and then click the Add button.**
- 3 **In the Add Proxy page, provide the following information:**

Proxy Type:	Mark the SSL box.
Proxy Address:	<b>192.18.49.14</b>
Proxy Service:	<b>4443</b>
Destination Address:	<b>192.18.69.14</b>
Destination Service:	<b>4080</b>
SSL Certificate:	<b>LoadBalancer-10.siroe.com</b>
SSL Key:	<b>LoadBalancer-10.siroe.com</b>
Server SSL Certificate:	<b>LoadBalancer-10.siroe.com</b>
Server SSL Key:	<b>LoadBalancer-10.siroe.com</b>

Click Next.

Rewrite Redirects:	<b>Matching</b>
--------------------	-----------------

Click Done.

## 13.7 Configuring the Application Servers for SSL Termination

Download the Sun Java System Application Server Enterprise Ed 8.1 2005Q1 Patch to the Application Server 3 host and to the Application 4 host using one of the following URLs:

Solaris (sparc) 119166-22	<a href="http://sunsolve.sun.com/search/document.do?assetkey=1-21-119166">http://sunsolve.sun.com/search/document.do?assetkey=1-21-119166</a>
Solaris (x86) 119170-14	<a href="http://sunsolve.sun.com/search/document.do?assetkey=1-21-119170-14">http://sunsolve.sun.com/search/document.do?assetkey=1-21-119170-14</a>
Linux 119171-14	<a href="http://sunsolve.sun.com/search/document.do?assetkey=1-21-119171-14">http://sunsolve.sun.com/search/document.do?assetkey=1-21-119171-14</a>

Use the following as you checklist for configuring the Application Servers for SSL Termination:

1. [Configure Application Server 3 for SSL termination.](#)
2. [Configure Application Server 4 for SSL termination.](#)

### ▼ To Configure Application Server 3 for SSL Termination

- 1 **As a root user, log into the Application Server 3 host.**

- 2 **Stop Application Server 3.**

```
# cd /opt/SUNWappserver/appserver/bin/
# ./asadmin stop-domain
```

- 3 **Install Patch 119166-22 as described in the file README.119166-22.**

Be sure to complete the patch post-installation instructions as described in that file.

```
# cd /tmp
# unzip 119166-21.zip
# patchadd -G /tmp/119166-22
```

- 4 **Verify that the patch was indeed installed successfully.**

```
# showrev -p | grep 119166-22
Patch: 119166-22 Obsoletes: Requires: Incompatibles: Packages: SUNWasuee,
SUNWaswbcr, SUNWascmnse, SUNWasacee, SUNWasdemdb, SUNWashdm, SUNWasdem,
SUNWascmn, SUNWasac, SUNWascm1, SUNWasu, SUNWasjdoc, SUNWasman, SUNWasut, SUNWasmanee
```

- 5 **Edit the following file:**

```
/var/opt/SUNWappserver/domains/domain1/applications/j2ee-apps/
agentsample/agentservlets_war/WEB-INF/sun-web.xml
```

Append the following directive to the end of the file:

```
...
<property name="relativeRedirectAllowed" value="true"/>
</sun-web-app>
```

Save the file and exit.

## 6 Edit the following file:

```
/var/opt/SUNWappserver/domains/domain1/applications/j2ee-modules/
agentapp/WEB-INF/sun-web.xml
```

Append this directive to the end of the file:

```
...
<property name="relativeRedirectAllowed" value="true"/>
</sun-web-app>
```

Save the file and exit.

## 7 Start the Application Server.

```
# cd /opt/SUNWappserver/appserver/bin/
# ./asadmin start-domain --user admin --password 11111111
```

# ▼ To Configure Application Server 4 for SSL Termination

## 1 As a root user, log into the Application Server 4 host.

## 2 Stop Application Server 4.

```
# cd /opt/SUNWappserver/appserver/bin/
# ./asadmin stop-domain
```

## 3 Install Patch 119166-22 as described in the file README.119166-22.

Be sure to complete the patch post-installation instructions as described in that file.

```
# cd /tmp
# unzip 119166-21.zip
# patchadd -G /tmp/119166-22
```

## 4 Verify that the patch was indeed installed successfully.

```
# showrev -p | grep 119166-22
Patch: 119166-21 Obsoletes: Requires: Incompatibles: Packages: SUNWasuee,
SUNWaswbcr, SUNWascmnse, SUNWasacee, SUNWasdemdb, SUNWashdm, SUNWasdem,
SUNWascmn, SUNWasac, SUNWascml, SUNWasu, SUNWasjdoc, SUNWasman, SUNWasut, SUNWasmanee
```

**5 Edit the following file:**

```
/var/opt/SUNWappserver/domains/domain1/applications/j2ee-apps/  
agentsample/agentservlets_war/WEB-INF/sun-web.xml
```

Append the following directive to the end of the file:

```
...  
<property name="relativeRedirectAllowed" value="true"/>  
</sun-web-app>
```

Save the file and exit.

**6 Edit the following file:**

```
/var/opt/SUNWappserver/domains/domain1/applications/j2ee-modules/  
agentapp/WEB-INF/sun-web.xml
```

Append this directive to the end of the file:

```
...  
<property name="relativeRedirectAllowed" value="true"/>  
</sun-web-app>
```

Save the file and exit.

**7 Start Application Server 4.**

```
# cd /opt/SUNWappserver/appserver/bin/  
# ./asadmin start-domain --user admin --password 11111111
```

## 13.8 Configuring the J2EE Policy Agents to Work with the J2EE Policy Agents Load Balancer

Use the following as your checklist for configuring the J2EE policy agents to work with the agents load balancer.

1. [Configure J2EE Policy Agent 3 to work with the J2EE Policy Agents load balancer.](#)
2. [Configure J2EE Policy Agent 4 to work with the J2EE Policy Agents load balancer.](#)
3. [Verify that the J2EE Policy Agents load balancer works properly.](#)

## ▼ To Configure J2EE Policy Agent 3 to Work with the J2EE Policy Agents Load Balancer

1 As a root user, log into the Protected Resource 3 host.

2 Go to the following directory:

```
# cd /export/j2ee_agents/am_as81_agent/agent_001/config
```

3 Update the `AMagents.properties` file.

Set the following properties as in this example:

```
# vi AMAgent.properties
com.sun.identity.agents.config.fqdn.mapping[LoadBalancer-10.siroe.com] =
LoadBalancer-10.siroe.com
com.sun.identity.agents.config.agent.host = LoadBalancer-10.siroe.com
com.sun.identity.agents.config.agent.port = 4443
com.sun.identity.agents.config.agent.protocol = https
```

Save the file.

4 Restart Application Server 3.

```
# cd /opt/SUNWappserver/appserver/bin
# ./asadmin stop-domain
Domain domain1 stopped.
# ./asadmin start-domain --user admin --password 11111111
Starting Domain domain1, please wait.
Log redirected to /var/opt/SUNWappserver/domains/domain1/logs/server.log.

Domain domain1 started.
```

## ▼ To Configure J2EE Policy Agent 4 to Work with the J2EE Policy Agents Load Balancer

1 As a root user, log into the Protected Resource 4 host.

2 Go to the following directory:

```
# cd /export/j2ee_agents/am_as81_agent/agent_001/config
```

### 3 Update the `AMagents.properties` file.

Set the following properties as in this example:

```
# vi AMAgent.properties
com.sun.identity.agents.config.fqdn.mapping[LoadBalancer-10.siroe.com] =
LoadBalancer-10.siroe.com
com.sun.identity.agents.config.agent.host = LoadBalancer-10.siroe.com
com.sun.identity.agents.config.agent.port = 4443
com.sun.identity.agents.config.agent.protocol = https
```

Save the file.

### 4 Restart Application Server 4.

```
# cd /opt/SUNWappserver/appserver/bin
# ./asadmin stop-domain
Domain domain1 stopped.
# ./asadmin start-domain --user admin --password 11111111
Starting Domain domain1, please wait.
Log redirected to /var/opt/SUNWappserver/domains/domain1/logs/server.log.
```

Domain domain1 started.

## ▼ To Verify that the J2EE Policy Agents Load Balancer Works Properly

### 1 Open a new browser.

### 2 Go to the J2EE Policy Agents load balancer URL:

<https://LoadBalancer-10.siroe.com:4443/agentsample>

The Federation Manager login page is displayed.

### 3 Log in to the Federation Manager console using the following information:

User Name: **spuser**

Password: **spuser**

The J2EE Policy Agent Sample Application welcome page is displayed.



## 13.9 Configuring the J2EE Policy Agents Load Balancer to Participate in SAMLv2 Protocols

Use the following as your checklist for configuring the J2EE Policy Agents load balancer to participate in SAMLv2 Protocols:

1. [Configure the J2EE Policy Agents load balancer to participate in SAMLv2 protocols.](#)
2. [Verify that the J2EE Policy Agents load balancer uses SAMLv2 protocols.](#)

### ▼ To Configure the J2EE Policy Agents Load Balancer to Participate in SAMLv2 Protocols

**1 As a root user, log into the Protected Resource 3 host.**

**2 Go to the following directory:**

```
/export/j2ee_agents/am_as81_agent/agent_001/config
```

**3 Make a backup of the AMagent.properties file, and then set the following properties:**

```
# vi AMagent.properties
com.sun.identity.agents.config.login.url[0] =
https://LoadBalancer-9.siroe.com:3443/federation/saml2/
jsp/spSSOInit.jsp?metaAlias=/sp&idpEntityID=loadbalancer-3.example.com
com.sun.identity.agents.config.redirect.param = RelayState
```

Save the file.

**4 Restart Application Server 3.**

```
# cd /opt/SUNWappserver/appserver/bin
# ./asadmin stop-domain
Domain domain1 stopped.
# ./asadmin start-domain --user admin --password 11111111
Starting Domain domain1, please wait.
Log redirected to /var/opt/SUNWappserver/domains/domain1/logs/server.log.
```

Domain domain1 started.

**5 As a root user, log into the Protected Resource 4 host.**

**6 Go to the following directory:**

```
/export/j2ee_agents/am_as81_agent/agent_001/config
```

**7 Make a backup of the AMagent.properties file, and then set the following properties:**

```
# vi AMagent.properties
com.sun.identity.agents.config.login.url[0] =
https://LoadBalancer-9.siroe.com:3443/federation/saml2/
jsp/spSSOInit.jsp?metaAlias=/sp&idpEntityID=loadbalancer-3.example.com
com.sun.identity.agents.config.redirect.param = RelayState
```

Save the file.

**8 Restart Application Server 4.**

```
# cd /opt/SUNWappserver/appserver/bin
# ./asadmin stop-domain
Domain domain1 stopped.
# ./asadmin start-domain --user admin --password 11111111
Starting Domain domain1, please wait.
Log redirected to /var/opt/SUNWappserver/domains/domain1/logs/server.log.
```

Domain domain1 started.

## ▼ To Verify that the J2EE Policy Agents Load Balancer Uses SAMLv2 Protocols

**1 Go to the following URL:**

<https://LoadBalancer-10.siroe.com:4443/agentssample>

The Access Manager login is displayed.

**2 Log in to the Access Manager console using the following information:**

User Name: **idp**

Password: **idp**

The J2EE Policy Agent Sample Application welcome page is displayed.

# Installing and Configuring Web Policy Agents

---

This chapter contains detailed information about the following groups of tasks:

- “14.1 Creating Web Agent Profiles on the Federation Manager Servers” on page 227
- “14.2 Installing Web Server 3 and Web Policy Agent 3” on page 229
- “14.3 Completing the Web Policy Agent 3 Installation” on page 234
- “14.4 Installing Web Server 4 and Web Policy Agent 4” on page 237
- “14.5 Completing the Web Policy Agent 4 Installation” on page 242
- “14.6 Configuring the Web Policy Agents Load Balancer” on page 245
- “14.7 Configuring the Web Policy Agents Load Balancer to Participate in SAMLv2 Protocols” on page 253

## 14.1 Creating Web Agent Profiles on the Federation Manager Servers

Use the following as your check list for creating Web Agent profiles on the Federation Manager servers:

1. Create the `UrlAccessAgent.properties` file on Federation Manager 1.
2. Create the `UrlAccessAgent.properties` file on Federation Manager 2.

### ▼ To Create the `UrlAccessAgent.properties` File on Federation Manager 1

- 1 Log into the Federation Manager 1 host.
- 2 Generate an encrypted password:

```
# /opt/SUNWam/fm/bin/ampassword -i /var/opt/SUNWam/fm/war_staging --hash 11111111  
BeUPgddAimR404ivWY6HPQ==
```

Make note of this encrypted password. You will use this password as the `UrlAccessAgent` encrypted password which is similar to a shared secret used by other web containers.

**3 Go to the following directory:**

```
/var/opt/SUNWam/fm/federation/users
```

**4 Create a file that contains the `UrlAccessAgent` encrypted password.**

```
# vi UrlAccessAgent.properties  
password=BeUPgddAimR404ivWY6HPQ==
```

Save the file.

**5 Restart the Federation Manager 1 server.**

```
# /opt/SUNWwbsvr/https-FederationManager-1.siroe.com  
# ./stop; ./start
```

## ▼ To Create the `UrlAccessAgent.properties` File on Federation Manager 2

**1 Log into the Federation Manager 2 host.**

**2 Generate an encrypted password:**

```
# /opt/SUNWam/fm/bin/ampassword -i /var/opt/SUNWam/fm/war_staging --hash 11111111  
BeUPgddAimR404ivWY6HPQ==
```

Make note of this encrypted password. You will use this password as the `UrlAccessAgent` encrypted password which is similar to a shared secret used by other web containers.

**3 Go to the following directory:**

```
/var/opt/SUNWam/fm/federation/users
```

**4 Create a file that contains the `UrlAccessAgent` encrypted password.**

```
# vi UrlAccessAgent.properties  
password=BeUPgddAimR404ivWY6HPQ==
```

Save the file.

**5 Restart the Federation Manager 2 server.**

```
# /opt/SUNWwbsvr/https-FederationManager-2.siroe.com  
# ./stop; ./start
```

## 14.2 Installing Web Server 3 and Web Policy Agent 3

For this part of the deployment, you must have the JES 5 installer and Web Policy Agent installer mounted on the host Protected Resource 1. See the section “2.2 Downloading and Mounting the Java Enterprise System 2005Q4 Installer” on page 32 in this manual.

Use the following as your checklist for installing Web Server 3 and Web Policy Agent 3:

1. [Install Web Server 3 on Protected Resource 3.](#)
2. [Install Web Policy Agent 3.](#)

### ▼ To Install Web Server 3 on Protected Resource 3

- 1 As a root user, log into the Protected Resource 3 host.
- 2 Start the Java Enterprise System installer with the `-nodisplay` option.
 

```
# cd /mnt/Solaris_sparc
# ./installer -nodisplay
```
- 3 When prompted, provide the following information:

Welcome to the Sun Java(TM) Enterprise System; serious software made simple... <Press ENTER to Continue>	Press Enter.
<Press ENTER to display the Software License Agreement>	Press Enter.
Have you read, and do you accept, all of the terms of the preceding Software License Agreement [No]	Enter <b>y</b> .
Please enter a comma separated list of languages you would like supported with this installation [8]	Enter <b>8</b> for “English only.”
Enter a comma separated list of products to install, or press R to refresh the list [ ]	Enter <b>3</b> to select Web Server.
Press "Enter" to Continue or Enter a comma separated list of products to deselect... [1]	Press Enter.

Enter 1 to upgrade these shared components and 2 to cancel [1]	You are prompted to upgrade shared components only if the installer detects that an upgrade is required.  Enter <b>1</b> to upgrade shared components.
Enter the name of the target installation directory for each product: Web Server [/opt/SUNWwbsvr] :	Accept the default value.
System ready for installation Enter 1 to continue [1]	Enter <b>1</b> .
1. Configure Now - Selectively override defaults or express through 2. Configure Later - Manually configure following installation Select Type of Configuration [1]	Enter <b>1</b> .
Common Server Settings Enter Host Name [ProtectedResource-3]	Accept the default value.
Enter DNS Domain Name [siroe.com]	Accept the default value.
Enter IP Address [192.18.72.151]	Accept the default value.
Enter Server admin User ID [admin]	Accept the default value.
Enter Admin User's Password (Password cannot be less than 8 characters) []	For this example, enter <b>11111111</b> .
Confirm Admin User's Password []	Enter the same password to confirm it.
Enter System User [root]	Accept the default value.
Enter System Group [root]	Accept the default value.
Enter Server Admin User ID [admin]	Accept the default value.
Enter Admin User's Password []	For this example, enter <b>11111111</b> .
Enter Host Name [ProtectedResource-3.siroe.com]	Accept the default value.
Enter Administration Port [8888]	Accept the default value.
Enter Administration Server User ID [root]	Accept the default value.
Enter System User ID [webservd]	Enter <b>root</b> .
Enter System Group [webservd]	Enter <b>root</b> .

Enter HTTP Port [80]	Enter <b>2080</b> .
Enter content Root [/opt/SUNWwbsvr/docs]	Accept the default value.
Do you want to automatically start Web Server when system re-starts. (Y/N) [N]	Accept the default value.
Ready to Install 1. Install 2. Start Over 3. Exit Installation What would you like to do [1]	First, see the next numbered (Optional) step. When ready to install, enter <b>1</b> .

**4 (Optional) During installation, you can monitor the log to watch for installation errors. Example:**

```
# cd /var/sadm/install/logs
# tail -f Java_Enterprise_System_install.B xxxxxx
```

**5 Upon successful installation, enter ! to exit.**

**6 Verify that the Web Server is installed properly.**

**a. Start the Web Server administration server to verify it starts with no errors.**

```
# cd /opt/SUNWwbsvr/https-admserv
# ./stop; ./start
```

**b. Run the netstat command to verify that the Web Server ports are open and listening.**

```
# netstat -an | grep 8888
*.8888          *.*            0              0      49152         0      LISTEN
```

**c. Go to the Web Server URL.**

```
http://ProtectedResource-3.siroe.com:8888
```

**d. Log in to the Web Server using the following information:**

```
Username    admin
Password    11111111
```

You should be able to see the Web Server console. You can log out of the console now.

**e. Start the Protected Resource 3 instance.**

```
# cd /opt/SUNWwbsvr/https-ProtectedResource-3.siroe.com
# ./stop; ./start
```

**f. Run the netstat command to verify that the Web Server ports are open and listening.**

```
# netstat -an | grep 2080
*.2080          *.*            0              0      49152         0      LISTEN
```

**g. Go to the instance URL.**

`http://ProtectedResource-3.siroe.com:1080`

You should see the default Web Server index page.

## ▼ To Install Web Policy Agent 3

### Before You Begin



**Caution** – If the Web Policy Agent installer is hosted on the same system where you are installing the Web Policy Agent, you can disregard this warning.

If the installer is hosted on a system other than the local system where you are installing the Web Policy Agent, you must start an X-display session on the system that hosts the installer. You must use an X-display program such as Reflections X or VNC even though you use the command-line installer. This is a known problem with this version of the Web Policy Agent. For more information about this known problem, see

<http://docs.sun.com/app/docs/doc/819-2796/6n52f1foq?a=view#adtcd>.

- 1 As a root user, log into the Protected Resource 3 host.**
- 2 Download the Java System Web Policy Agents 2.2 package from the following website:**

<http://www.sun.com/download/products.xml?id=434ed995>

- 3 Unpack the downloaded package.**

In this example, the package was downloaded into the directory `/temp`.

```
# cd /temp
# gunzip sun-one-policy-agent-2.2-es6-solaris_sparc.tar.gz
# tar -xvof sun-one-policy-agent-2.2-es6-solaris_sparc.tar
```

- 4 Start the Web Policy Agents installer.**

```
# ./setup -nodisplay
```

- 5 When prompted, provide the following information:**

When you are ready, press Enter to continue.  
<Press ENTER to Continue>

Press Enter.

Press ENTER to display the Sun Software  
License Agreement

Press Enter.



Have you read, and do you accept, all of the terms of the preceding Software License Agreement [no] y	Enter <b>y</b> .
Install the Sun Java(tm) System Access Manager Policy Agent in this directory [/opt] :	Accept the default value.
Enter information about the server instance this agent will protect. Host Name [ProtectedResource-3.siroe.com]:	Accept the default value.
Web Server Instance Directory []:	Enter <b>/opt/SUNWwbsvr/ https-ProtectedResource-9.siroe.com</b>
Web Server Port [80]:	Enter <b>2080</b> .
Web Server Protocol [http]	Enter <b>https</b> .
Agent Deployment URI [/amagent]:	Accept the default value.
Enter the Sun Java(tm) System Access Manager Information for this Agent. Primary Server Host [ProtectedResource-3.siroe.com] :	For this example, enter the external-facing load balancer host name. Example: <b>LoadBalancer-3.example.com</b>
Primary Server Port [1080]	Enter the load balancer HTTP port number. For this example, enter <b>3443</b> .
Primary Server Protocol [http]:	Enter <b>https</b> .
Primary Server Deployment URI [/amserver]:	Enter <b>/federation</b> .
Primary Console Deployment URI [/amconsole] :	Enter <b>/federation</b> .
Failover Server Host [] :	Accept the default value.
Agent-Access Manager Shared Secret:	Enter the amdapuser password that was entered when Access Manager was installed. For this example, enter <b>11111111</b> .
Re-enter Shared Secret:	Enter the <b>11111111</b> password again to confirm it.
CDSSO Enabled [false]:	Accept the default value.
Press "Enter" when you are ready to continue.	First, see the next (Optional) numbered step. When you are ready to start installation, press Enter.

**6 (Optional) During installation, you can monitor the log to watch for installation errors. Example:**

```
# cd /var/sadm/install/logs
# tail -f var/sadm/install/logs/
```

```
Sun_Java_tm_System_Access_Manager_Policy_Agent_install.Bxxxxxxxx
```

## 7 Restart the Web Server.

```
# cd /opt/SUNWwbsvr/https-ProtectedResource-3.siroe.com
# cd ./stop; ./start
```

Examine the Web Server log for startup errors.

```
# /opt/SUNWwbsvr/https-ProtectedResource-3.siroe.com/logs
# vi errors
```

# 14.3 Completing the Web Policy Agent 3 Installation

Use the following as your checklist for completing the Web Policy Agent 3 installation:

1. [Edit the AMAgent.Properties file.](#)
2. [Verify that Web Policy Agent 3 is working properly.](#)
3. [Import the root CA certificate into the Web Server 3 key store.](#)
4. [Verify that Web Policy Agent 3 can access the Federation Manager load balancer.](#)

## ▼ To Edit the AMAgent.Properties File

### 1 Log in to as a root user to Federation Manager 1 host.

### 2 Edit the AMAgent.properties file.

```
# cd /etc/opt/SUNWam/agents/es6/
config/_opt_SUNWwbsvr_https-ProtectedResource-3.siroe.com
```

#### a. Make a backup of AMAgent.properties, and then set the following properties:

```
com.sun.am.policy.am.username = UrlAccessAgent
com.sun.am.policy.am.password = BeVPgddAimR404ivWY6HPQ==
com.sun.am.policy.agents.config.do_sso_only = true
```

#### b. Add the following properties to the original file:

```
com.sun.am.ignore.naming.service = true
```

#### c. (Optional) Set the debug property as in this example:

```
com.sun.am.log.level = all:5
```

Save the file.

### 3 Restart Web Server 3.

```
# cd /opt/SUNWwbsvr/https-ProtectedResource-3.siroe.com
#./stop; ./start
```

## ▼ To Verify that Web Policy Agent 3 is Working Properly

### 1 Go to the following URL:

<http://ProtectedResource-3.siroe.com:2080>

### 2 Log in to Access Manager using the following information:

Username **spuser**

Password **spuser**

You should see the default `index.html` page for Web Server 3.

## ▼ To Import the Root CA Certificate into the Web Server 3 Key Store

The Web Policy Agent on Protected Resource 3 connects to Federation Manager servers through Load Balancer 9. The load balancer is SSL-enabled, so the agent must be able to trust the load balancer SSL certificate in order to establish the SSL connection. To do this, import the root CA certificate that issued the Load Balancer 3 SSL server certificate into the Web Policy Agent certificate store.

**Before You Begin** Obtain the root CA certificate, and copy it to the Protected Resource 3 host. Copy the certificate into the file `/export/software/ca.cert`.

### 1 Copy the root CA certificate to Protected Resource 3.

### 2 Open a browser, and go to the Web Server 3 administration console.

<http://ProtectedResource-3.siroe.com:8888>

### 3 Log in to the Web Server 3 console using the following information:

User Name: **admin**

Password: **11111111**

### 4 In the **Select a Server** field, select `ProtectedResource-3.siroe.com`, and then click **Manage**.

---

**Tip** – If a “Configuration files have not been loaded” message is displayed, it may be because the Web Server instance that is being accessed through the administration server has had its configuration files manually edited. This is the case when the Web Policy Agent is installed. The mirror configuration files are different from the current configuration files. In order to be sure the changes are not lost, you must apply the changes. First click Apply, and then click Apply Changes. The configuration files are read, and the server is stopped and restarted.

---

**5 Click the Security tab.**

**6 On the Initialize Trust Database page, enter a Database Password.**

Enter the password again to confirm it, and then click OK.

**7 In the left frame, click Install Certificate and provide the following information, and then click OK:**

Certificate For:                    Choose **Trusted Certificate Authority (CA)**.  
Key Pair File Password:        **password**  
Certificate Name:                **rootCA.cert**  
Message in this File:          **/export/software/ca.cert**

**8 Click Add Server Certificate.**

**9 Click Manage Certificates.**

The root CA Certificate name rootCA.cert is included in the list of certificates.

**10 Click the Preferences tab.**

**11 Restart Web Server 3.**

On the Server On/Off page, click Server Off. When the server indicates that the administration server is off, click Server On.

**12 Restart Web Server 3.**

```
# cd /opt/SUNWwbsvr/https-ProtectedResource-3.siroe.com
# ./stop; ./start
```

## ▼ To Verify that Web Policy Agent 3 Can Access the Federation Manager Load Balancer

### 1 Go to the Protected Resource 3 URL:

`http://ProtectedResource-3.siroe.com:2080/index.html`

### 2 Log into the Federation Manager console using the following information:

User Name: **spuser**

Password: **spuser**

The policy agent redirects the request, and the URL changes to `https://LoadBalancer-9.siroe.com:3443/federation/UI/Login`. The default Sun ONE Web Server page is displayed. This verifies that the web policy agent is properly configured to access the Federation Manager load balancer.

## 14.4 Installing Web Server 4 and Web Policy Agent 4

For this part of the deployment, you must have the JES 5 installer and Web Policy Agent installer mounted on the host Protected Resource 1. See the section [“2.2 Downloading and Mounting the Java Enterprise System 2005Q4 Installer”](#) on page 32 in this manual.

Use the following as you checklist for installing Web Server 4 and Web Policy Agent 4:

1. [Install Web Server 4 on Protected Resource 4.](#)
2. [Install Web Policy Agent 4.](#)

## ▼ To Install Web Server 4 on Protected Resource 4

### 1 As a root user, log into the Protected Resource 4 host.

### 2 Start the Java Enterprise System installer with the `-nodisplay` option.

```
# cd /mnt/Solaris_sparc
# ./installer -nodisplay
```

### 3 When prompted, provide the following information:

```
Welcome to the Sun Java(TM) Enterprise System;
serious software made simple...
<Press ENTER to Continue>
```

Press Enter.

<Press ENTER to display the Software License Agreement>	Press Enter.
Have you read, and do you accept, all of the terms of the preceding Software License Agreement [No]	Enter <b>y</b> .
Please enter a comma separated list of languages you would like supported with this installation [8]	Enter <b>8</b> for "English only."
Enter a comma separated list of products to install, or press R to refresh the list [ ]	Enter <b>3</b> to select Web Server.
Press "Enter" to Continue or Enter a comma separated list of products to deselect... [1]	Press Enter.
Enter <b>1</b> to upgrade these shared components and <b>2</b> to cancel [1]	You are prompted to upgrade shared components only if the installer detects that an upgrade is required.  Enter <b>1</b> to upgrade shared components.
Enter the name of the target installation directory for each product: Web Server [/opt/SUNWwbsvr] :	Accept the default value.
System ready for installation Enter <b>1</b> to continue [1]	Enter <b>1</b> .
1. Configure Now - Selectively override defaults or express through 2. Configure Later - Manually configure following installation Select Type of Configuration [1]	Enter <b>1</b> .
Common Server Settings Enter Host Name [ProtectedResource-4]	Accept the default value.
Enter DNS Domain Name [siroe.com]	Accept the default value.
Enter IP Address [192.18.72.152]	Accept the default value.
Enter Server admin User ID [admin]	Accept the default value.
Enter Admin User's Password (Password cannot be less than 8 characters) [ ]	For this example, enter <b>11111111</b> .
Confirm Admin User's Password [ ]	Enter the same password to confirm it.
Enter System User [root]	Accept the default value.
Enter System Group [root]	Accept the default value.

Enter Server Admin User ID [admin]	Accept the default value.
Enter Admin User's Password []	For this example, enter <b>11111111</b> .
Enter Host Name [ProtectedResource-4.siroe.com]	Accept the default value.
Enter Administration Port [8888]	Accept the default value.
Enter Administration Server User ID [root]	Accept the default value.
Enter System User ID [webservd]	Enter <b>root</b> .
Enter System Group [webservd]	Enter <b>root</b> .
Enter HTTP Port [80]	Enter <b>2080</b> .
Enter content Root [/opt/SUNWwbsvr/docs]	Accept the default value.
Do you want to automatically start Web Server when system re-starts.(Y/N) [N]	Accept the default value.
Ready to Install 1. Install 2. Start Over 3. Exit Installation What would you like to do [1]	First, see the next numbered (Optional) step. When ready to install, enter <b>1</b> .

**4 (Optional) During installation, you can monitor the log to watch for installation errors. Example:**

```
# cd /var/sadm/install/logs
# tail -f Java_Enterprise_System_install.B xxxxxx
```

**5 Upon successful installation, enter ! to exit.**

**6 Verify that the Web Server is installed properly.**

**a. Start the Web Server administration server to verify it starts with no errors.**

```
# cd /opt/SUNWwbsvr/https-admserv
# ./stop; ./start
```

**b. Run the netstat command to verify that the Web Server ports are open and listening.**

```
# netstat -an | grep 8888
*.8888          *.*            0             0      49152         0      LISTEN
```

**c. Go to the Web Server URL.**

```
http://ProtectedResource-4.siroe.com:8888
```

**d. Log in to the Web Server using the following information:**

```
Username    admin
Password    11111111
```

You should be able to see the Web Server console. You can log out of the console now.

**e. Start the Protected Resource 4 instance.**

```
# cd /opt/SUNWwbsvr/https-ProtectedResource-4.siroe.com
# ./stop; ./start
```

**f. Run the netstat command to verify that the Web Server ports are open and listening.**

```
# netstat -an | grep 2080
*.2080          *.*            0              0      49152         0      LISTEN
```

**g. Go to the instance URL.**

```
http://ProtectedResource-4.siroe.com:1080
```

You should see the default Web Server index page.

## ▼ To Install Web Policy Agent 4

### Before You Begin



**Caution** – If the Web Policy Agent installer is hosted on the same system where you are installing the Web Policy Agent, you can disregard this warning.

If the installer is hosted on a system other than the local system where you are installing the Web Policy Agent, you must start an X-display session on the system that hosts the installer. You must use an X-display program such as Reflections X or VNC even though you use the command-line installer. This is a known problem with this version of the Web Policy Agent. For more information about this known problem, see <http://docs.sun.com/app/docs/doc/819-2796/6n52flfoq?a=view#adtcd>.

---

- 1 As a root user, log into the Protected Resource 4 host.**
- 2 Download the Java System Web Policy Agents 2.2 package from the following website:**  
<http://www.sun.com/download/products.xml?id=434ed995>
- 3 Unpack the downloaded package.**

In this example, the package was downloaded into the directory /temp.

```
# cd /temp
# gunzip sun-one-policy-agent-2.2-es6-solaris_sparc.tar.gz
# tar -xvof sun-one-policy-agent-2.2-es6-solaris_sparc.tar
```



**4 Start the Web Policy Agents installer.**

```
# ./setup -nodisplay
```

**5 When prompted, provide the following information:**

When you are ready, press Enter to continue. <Press ENTER to Continue>	Press Enter.
Press ENTER to display the Sun Software License Agreement	Press Enter.
Have you read, and do you accept, all of the terms of the preceding Software License Agreement [no] y	Enter <b>y</b> .
Install the Sun Java(tm) System Access Manager Policy Agent in this directory [/opt] :	Accept the default value.
Enter information about the server instance this agent will protect. Host Name [ProtectedResource-4.siroe.com]:	Accept the default value.
Web Server Instance Directory []:	Enter <b>/opt/SUNWwbsvr/ https-ProtectedResource-4.siroe.com</b>
Web Server Port [80]:	Enter <b>2080</b> .
Web Server Protocol [http]	Accept the default value.
Agent Deployment URI [/amagent]:	Accept the default value.
Enter the Sun Java(tm) System Access Manager Information for this Agent. Primary Server Host [ProtectedResource-9.siroe.com] :	For this example, enter the load balancer host name. Example: <b>LoadBalancer-9.siroe.com</b>
Primary Server Port [1080]	Enter the load balancer HTTP port number. For this example, enter <b>3443</b> .
Primary Server Protocol [http]:	Enter <b>https</b> .
Primary Server Deployment URI [/amserver]:	Enter <b>/federation</b> .
Primary Console Deployment URI [/amconsole] :	Enter <b>/federation</b> .
Failover Server Host [] :	Accept the default value.
Agent-Access Manager Shared Secret:	Enter the amdapuser password that was entered when Access Manager was installed. For this example, enter <b>11111111</b> .

Re-enter Shared Secret:	Enter the <b>11111111</b> password again to confirm it.
CSSO Enabled [false]:	Accept the default value.
Press "Enter" when you are ready to continue.	First, see the next (Optional) numbered step. When you are ready to start installation, press Enter.

**6 (Optional) During installation, you can monitor the log to watch for installation errors. Example:**

```
# cd /var/sadm/install/logs
# tail -f var/sadm/install/logs/
Sun_Java_tm_System_Access_Manager_Policy_Agent_install.Bxxxxxxx
```

**7 Restart the Web Server.**

```
# cd /opt/SUNWwbsvr/https-ProtectedResource-4.siroe.com
# cd ./stop; ./start
```

Examine the Web Server log for startup errors.

```
# /opt/SUNWwbsvr/https-ProtectedResource-4.siroe.com/logs
# vi errors
```

## 14.5 Completing the Web Policy Agent 4 Installation

Use the following as your checklist for completing the Web Policy Agent 4 installation:

1. [Edit the AMAgent.Properties file.](#)
2. [Verify that Web Policy Agent 4 is working properly.](#)
3. [Import the root CA certificate into the Web Server 4 key store.](#)
4. [Verify that Web Policy Agent 4 can access the Federation Manager load balancer.](#)

### ▼ To Edit the AMAgent.Properties File

**1 Log in to as a root user to Federation Manager 1 host.**

**2 Edit the AMAgent.properties file.**

```
# cd /etc/opt/SUNWam/agents/es6/
config/_opt_SUNWwbsvr_https-ProtectedResource-4.siroe.com
```

**a. Make a backup of AMAgent.properties, and then set the following properties:**

```
com.sun.am.policy.am.username = UrlAccessAgent
com.sun.am.policy.am.password = BeVPgddAimR404ivWY6HPQ==
com.sun.am.policy.agents.config.do_sso_only = true
```

**b. Add the following properties to the original file:**

```
com.sun.am.ignore.naming.service = true
```

**c. (Optional) Set the debug property as in this example:**

```
com.sun.am.log.level = all:5
```

Save the file.

**3 Restart Web Server 4.**

```
# cd /opt/SUNWwbsvr/https-ProtectedResource-4.siroe.com
#./stop; ./start
```

**▼ To Verify that Web Policy Agent 4 is Working Properly****1 Go to the following URL:**

```
http://ProtectedResource-4.siroe.com:2080
```

**2 Log in to Access Manager using the following information:**

Username **spuser**

Password **spuser**

You should see the default `index.html` page for Web Server 4.

**▼ To Import the Root CA Certificate into the Web Server 4 Key Store**

The Web Policy Agent on Protected Resource 4 connects to Federation Manager servers through Load Balancer 9. The load balancer is SSL-enabled, so the agent must be able to trust the load balancer SSL certificate in order to establish the SSL connection. To do this, import the root CA certificate that issued the Load Balancer 3 SSL server certificate into the Web Policy Agent certificate store.

**Before You Begin** Obtain the root CA certificate, and copy it to the Protected Resource 4 host. Copy the certificate into the file `/export/software/ca.cert`.

**1 Copy the root CA certificate to Protected Resource 4.****2 Open a browser, and go to the Web Server 4 administration console.**

```
http://ProtectedResource-4.siroe.com:8888
```

**3 Log in to the Web Server 4 console using the following information:**User Name: **admin**Password: **11111111****4 In the Select a Server field, select ProtectedResource-4.siroe.com, and then click Manage.**

---

**Tip** – If a “Configuration files have not been loaded” message is displayed, it may be because the Web Server instance that is being accessed through the administration server has had its configuration files manually edited. This is the case when the Web Policy Agent is installed. The mirror configuration files are different from the current configuration files. In order to be sure the changes are not lost, you must apply the changes. First click Apply, and then click Apply Changes. The configuration files are read, and the server is stopped and restarted.

---

**5 Click the Security tab.****6 On the Initialize Trust Database page, enter a Database Password.**

Enter the password again to confirm it, and then click OK.

**7 In the left frame, click Install Certificate and provide the following information, and then click OK:**Certificate For: Choose **Trusted Certificate Authority (CA)**.Key Pair File Password: **password**Certificate Name: **rootCA.cert**Message in this File: **/export/software/ca.cert****8 Click Add Server Certificate.****9 Click Manage Certificates.**

The root CA Certificate name rooCA.cert is included in the list of certificates.

**10 Click the Preferences tab.****11 Restart Web Server 4.**

On the Server On/Off page, click Server Off. When the server indicates that the administration server is off, click Server On.

**12 Restart Web Server 4.**

```
# cd /opt/SUNWwbsvr/https-ProtectedResource-4.siroe.com
# ./stop; ./start
```

## ▼ To Verify that Web Policy Agent 4 Can Access the Federation Manager Load Balancer

### 1 Go to the Protected Resource 4 URL:

`http://ProtectedResource-4.siroe.com:2080/index.html`

### 2 Log into the Federation Manager console using the following information:

User Name: **spuser**

Password: **spuser**

The policy agent redirects the request, and the URL changes to `https://LoadBalancer-9.siroe.com:3443/federation/UI/Login`. The default Sun ONE Web Server page is displayed. This verifies that the web policy agent is properly configured to access the Federation Manager load balancer.

## 14.6 Configuring the Web Policy Agents Load Balancer

Load Balancer 11 can be located in a less-secured zone, and handles traffic for the Web Policy Agents.

Load Balancer 11 is configured for simple persistence so that browser requests from the same IP address will always be directed to the same Web Policy Agent instance. This guarantees that the requests from the same user session will always be sent to the same Web Policy Agent instance. This is important from the performance perspective. Each Web Policy Agent must validate the user session and evaluate applicable policies. The results are subsequently cached on the individual Web Policy Agent to improve the performance. If no load balancer persistence is set, and the same user's requests are spread across two agents, then each agent must build up its own cache. To do so, both agents must validate the session and evaluate policies. This effectively doubles the workload on the Access Manager servers, and cuts the overall system capacity by half. The problem becomes even more acute as the number of Web Policy Agents increases further.

As a general rule, in situations where each Web Policy Agent instance is protecting identical resources, some form of load balancer persistence is highly recommended for the performance reasons. The actual type of persistence may vary when a different load balancer is used, as long as it achieves the goal of sending the requests from the same user session to the same Web Policy Agent instance.

Use the following as your checklist for configuring the Web Policy Agents load balancer:

- [“To Configure the Web Policy Agents Load Balancer” on page 246](#)

- “To Configure the Web Policy Agents to Work with the Web Policy Agents Load Balancer” on page 250
- “To Verify that the Web Policy Agents Load Balancer is Working Properly” on page 252

## ▼ To Configure the Web Policy Agents Load Balancer

- 1 Go to URL for the Big IP load balancer login page and log in.

`https://ls-f5.siroe.com`

- 2 Log in using the following information:

User name: **username**

Password: **password**

- 3 Request an SSL Certificate for Load Balancer 11.

- a. Log in to the BIG-IP load balancer.

- b. Click Proxies in the left pane.

- c. Click the Cert Admin tab, and then click the “Generate New Key Pair/ Certificate Request” button.

- d. In the Create Certificate Request page, provide the following information:

Key Identifier: **LoadBalancer-11.siroe.com**

Organization: **siroe.com**

Domain Name: **LoadBalancer-11.siroe.com**

Email Address: **jdoe@siroe.com**

- e. Click the Generate Request button.

- f. In the Generate Request page, copy the request that looks similar to this:

```
-----BEGIN CERTIFICATE REQUEST-----
UbM77e50M63v1Z2A/505MA0GCSqGSIb3DQE0BAU
AMF8xCzAJBgNVBAYTAlVTMSAwHgYDVQKExdSU0
EgRGF0YSBTZWNIcmI0eSwgSW5jLjEuMCAwGA1UEC
xMLU2VjdXJlIFNlcnZlciBDZXJ0aWZpY2F0aW9u
IEF1dGhvcml0eTAeFw0wMTA4MDIwMDAwMDBaFw0
wMzA4MDIyMzU5NTlaMIGQMqswCQYDVQGEwJVUz
ERMA8GA1UECBMlYyZ2luaWEtETAPBgNVBACUC
FJpY2htb25kMSAwHgYDVQKFBDbDYXZhbGllciBU
```

```
ZWxlCghvYm9uZGluZy5jYXZ0ZWwuY29tMIGfMA0
GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8x/1dxo
2YnblilQLmpiezi0qb7ArVfI1ymXo/MKcbKjnY2
-----END CERTIFICATE REQUEST-----
```

- g. Paste this text into a request form provided by a root certificate authority (CA) such as Verisign or Thwarte.**

See the certificate authority website such as <http://www.verisign.com/> or <http://www.thawte.com/> for detailed instructions on submitting a certificate request.

- 4 After you receive the certificate from the issuer, install the SSL Certificate.**

- a. In the BIG-IP load balancer console, click the Cert Admin tab.**

- b. On the Cert Admin tab, click Install Certificate.**

- c. In the Install SSL Certificate page, paste the certificate text you received from the certificate issuer. Example:**

```
-----BEGIN CERTIFICATE REQUEST-----
UmM77e50M63v1Z2A/505MA0GCSqGSIb3DQE0BAU
AMF8xCzAJBgNVBAYTAlVTMSAwHgYDVQKExdSU0
EgRGF0YSBTZWN1cm10eSwgSW5jLjEuMCAwGA1UEC
xMlU2VjdxJlIFNlcnZlcjBDZXJ0aWZpY2F0aW9u
IEF1dGhvcml0eTAeFw0wMTA4MDIwMDAwMDBaFw0
wMzA4MDIyMzU5NTlaMIGQM0swCQYDVQGEwJVUz
ERMA8GA1UECBMlY2ZluaWExETAPBgNVBACUC
FJpY2htb25kMSAwHgYDVQKFBdYXZhbGllciBU
ZWxlCghvYm9uZGluZy5jYXZ0ZWwuY29tMIGfMA0
GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8x/1dxo
2YnblilQLmpiezi0qb7ArVfI1ymXo/MKcbKjnY2
-----END CERTIFICATE REQUEST-----
```

- d. Click Install Certificate.**

- 5 Create a Pool.**

A pool contains all the backend server instances.

- a. Open the Configuration Utility.**

Click “Configure your BIG-IP (R) using the Configuration Utility.”

- b. In the left pane, click Pools.**

- c. On the Pools tab, click the Add button.**

**d. In the Add Pool dialog, provide the following information:**

Pool Name	<b>federation_web_agents</b>
Load Balancing Method	<b>Round Robin</b>
Resources	<b>192.18.72.151:2080</b> (for Protected Resource 3) <b>192.18.72.152:2080</b> (for Protected Resource 4)

Click Done.

**6 Configure the load balancer for simple persistence.****a. In the left frame, click Pools.****b. Click the name of the pool you want to configure.**

In this example, `federation_web_agents`.

**c. Click the Persistence tab.****d. On the Persistence tab, under Persistence Type, select the Simple.****e. Set the timeout interval.**

In the Timeout field, enter 300 seconds.

Click Apply.

**7 Add a Virtual Server.**

If you encounter Javascript errors or otherwise cannot proceed to create a virtual server, try using Microsoft Internet Explorer for this step.

**a. In the left frame, Click Virtual Servers.****b. On the Virtual Servers tab, click the Add button.****c. In the Add Virtual Server dialog box, provide the following information:**

Address	<b>192.18.69.14</b> (for LoadBalancer-11.siroe.com)
Service	<b>5080</b>

Click Next.

**d. Continue to click Next until you reach the Select Physical Resources dialog box.**

Pool **federation\_web\_agents**



- e. In the Pool Selection dialog box, assign the Pool (`federation_web_agents`) that you have just created.
  - f. Click the Done button.
- 8 Create proxies.**
- a. In the left frame, click Proxies.
  - b. On the Proxies tab, click Add.
  - c. In the Add Proxy page, provide the following information:

Proxy Type:	Mark the SSL checkbox.
Proxy Address:	<b>192.18.69.14</b>
Proxy Service:	<b>6443</b>
Destination Address:	<b>192.18.69.14</b>
Destination Service:	<b>5080</b>
SSL Certificate:	<b>LoadBalancer-11.siroe.com</b>
SSL Key:	<b>LoadBalancer-11.siroe.com</b>
Server SSL Certificate:	<b>LoadBalancer-11.siroe.com</b>
Server SSL Key:	<b>LoadBalancer-11.siroe.com</b>

Click Done.
- 9 Add Monitors.**
- a. Click the Monitors tab, and then click the Add button.

In the Add Monitor dialog provide the following information:

Name:	<b>WebAgent-http</b>
Inherits From:	Choose <b>http</b> .
  - b. Click Next.

In the Configure Basic Properties page, click Next.
  - c. In the Configure ECV HTTP Monitor, in the Send String field, enter the following:  
GET /launch.html  
Click Next.

**d. In the Destination Address and Service (Alias) page, click Done.**

On the Monitors tab, the monitor you just added is now contained in the list of monitors.

**e. Click the Basic Associations tab.**

Look for the IP addresses for ProtectedResource-3:2080 and ProtectedResource-4:1080.

**f. Mark the Add checkbox for ProtectedResource-3 and ProtectedResource-4.****g. At the top of the Node column, choose the monitor that you just added, WebAgent-http.****h. Click Apply.**

## ▼ To Configure the Web Policy Agents to Work with the Web Policy Agents Load Balancer

In this procedure you modify the `AMAgent.properties` file. Map Protected Resource 3 and Protected Resource 4 to Load Balancer 11.

**1 Log in as a root user to Protected Resource 3.**

```
# cd etc/opt/SUNWam/agents/es6/
config/_opt_SUNWwbsvr_https-ProtectedResource-3.siroe.com
```

**2 Use a text editor to modify the `AMAgent.properties` file.**

For this property:

```
com.sun.am.policy.agents.config.notenforced_list
```

append the following to the end of the value string:

```
http://ProtectedResource-3.siroe.com:1080/launch.html
http://LoadBalancer-11.siroe.com:90/launch.html
```

**3 Set the following properties:**

```
com.sun.am.load_balancer.enable = true
com.sun.am.policy.agents.config.override_protocol = true
com.sun.am.policy.agents.config.override_host = true
com.sun.am.policy.agents.config.override_port = true
com.sun.am.policy.agents.config.agenturi.prefix =
https://LoadBalancer-11.siroe.com:6443/amagent
com.sun.am.policy.agents.config.fqdn.map =
[LoadBalancer-11.siroe.com|LoadBalancer-11.siroe.com]
```

```
com.sun.am.policy.agents.config.fqdn.default =
LoadBalancer-11.siroe.com
```

Save the file.

#### 4 Restart Web Server 3 on Protected Resource 3.

```
#cd /opt/SUNWwbsvr/https-ProtectedResource-3.siroe.com
./stop; ./start
```

#### 5 Log in as a root user to Protected Resource 4.

```
# cd etc/opt/SUNWam/agents/es6/
config/_opt_SUNWwbsvr_https-ProtectedResource-4.siroe.com
```

#### 6 Use a text editor to modify the AMAgent.properties file.

For this property:

```
com.sun.am.policy.agents.config.notenforced_list
```

append the following to the end of the value string :

```
http://ProtectedResource-4.siroe.com:1080/launch.html
http://LoadBalancer-11.siroe.com:90/launch.html
```

#### 7 Set the following properties:

```
com.sun.am.load_balancer.enable = true
com.sun.am.policy.agents.config.override_protocol = true
com.sun.am.policy.agents.config.override_host = true
com.sun.am.policy.agents.config.override_port = true
com.sun.am.policy.agents.config.agenturi.prefix =
https://LoadBalancer-11.siroe.com:6443/amagent
com.sun.am.policy.agents.config.fqdn.map =
[LoadBalancer-11.siroe.com|LoadBalancer-11.siroe.com]
com.sun.am.policy.agents.config.fqdn.default =
LoadBalancer-11.siroe.com
```

Save the file.

#### 8 Restart Web Server 4 on Protected Resource 4.

```
#cd /opt/SUNWwbsvr/https-ProtectedResource-4.siroe.com
./stop; ./start
```

## ▼ To Verify that the Web Policy Agents Load Balancer is Working Properly

### 1 In a browser, go to the following URL:

`https://LoadBalancer-11.siroe.com:6443/index.html`

The load balancer redirects the request to the Access Manager login page.

### 2 Log in to the Access Manager console using the following information:

Username **spuser**

Password **spuser**

If the default Web Server `index.html` page is displayed, then the load balancer is configured properly.

### 3 Verify that Load Balancer 11 monitors are monitoring the Web Servers properly.

#### a. Log in as a root user to Protected Resource 3.

#### b. Run the `tail` command.

```
# cd /opt/SUNWwbsvr/https-ProtectedResource-3.siroe.com/logs
# tail -f access
```

If you see frequent entries similar to this one:

```
192.18.69.18 - - [06/Oct/2006:13:53:07 -0700] "GET /launch.html" 200 8526
```

then the custom monitor is configured properly. If you do not see `"GET /launch.html"`, then you must troubleshoot the load balancer configuration.

#### c. Log in as root to Protected Resource 4.

#### d. Run the `tail` command.

```
# cd /opt/SUNWwbsvr/https-ProtectedResource-4.siroe.com/logs
# tail -f access
```

If you see frequent entries similar to this one:

```
192.18.69.18 - - [06/Oct/2006:13:53:07 -0700] "GET /launch.html" 200 8526
```

then the custom monitor is configured properly. If you do not see `"GET /launch.html"`, then you must troubleshoot the load balancer configuration.

## 14.7 Configuring the Web Policy Agents Load Balancer to Participate in SAMLv2 Protocols

Use the following as your checklist for configuring the Web Policy Agents load balancer to participate in SAMLv2 protocols:

1. [Enable the Web Policy Agents load balancer to use SAMLv2 protocols.](#)
2. [Verify that the Web Policy Agents load balancer uses SAMLv2 protocols.](#)

### ▼ To Enable the Web Policy Agents Load Balancer to Use SAMLv2 Protocols

**1 As a root user, log in to the Protected Resource 3 host.**

**2 Go to the following directory:**

```
/etc/opt/SUNWam/agents/es6/config/  
_opt_SUNWwbsvr_https-ProtectedResource-3.siroe.com
```

**3 Make a backup of `AMAgent.properties`, and then set the following properties:**

```
com.sun.am.policy.am.login.url =  
https://LoadBalancer-9.siroe.com:3443/federation/saml2/  
jsp/spSSOInit.jsp?metaAlias=/sp&idpEntityID=loadbalancer-3.example.com
```

**4 Add the following property:**

```
com.sun.am.policy.agents.config.url.redirect.param = RelayState
```

Save the file.

**5 As a root user, log in to the Protected Resource 4 host.**

**6 Go to the following directory:**

```
/etc/opt/SUNWam/agents/es6/config/  
_opt_SUNWwbsvr_https-ProtectedResource-4.siroe.com
```

**7 Make a backup of `AMAgent.properties`, and then set the following properties:**

```
com.sun.am.policy.am.login.url =  
https://LoadBalancer-9.siroe.com:3443/federation/saml2/  
jsp/spSSOInit.jsp?metaAlias=/sp&idpEntityID=loadbalancer-3.example.com
```

**8 Add the following property:**

```
com.sun.am.policy.agents.config.url.redirect.param = RelayState
```

Save the file.

**9 Restart the Protected Resource 3 host.**

```
# cd /opt/SUNWwbsvr/https-ProtectedResource-3.siroe.com
# ./stop; ./start
```

**10 Restart the Protected Resource 4 host.**

```
# cd /opt/SUNWwbsvr/https-ProtectedResource-4.siroe.com
# ./stop; ./start
```

## ▼ To Verify that the Web Policy Agents Load Balancer Uses SAMLv2 Protocols

**1 Go to the following URL:**

<https://LoadBalancer-11.siroe.com:6443/index.html>

**2 Log into the Access Manager console using the following information:**

User Name: **idpuser**

Password: **idpuser**

The Web Server default **index.html** page is displayed.

PART VI

## Configuring Special Use Cases





## Use Case 1: Testing Basic SAMLv2 Protocols

---

The three primary SAMLv2 protocols are Persistent Federation with SSO, Single Logout, and Federation Termination. SAMLv2 protocols can be initiated from the Service Provider site or from the Identity Provider site. Multiple variations exist. For example, the SSO protocol has two profiles, the browser artifact profile and browser POST profile. The profiles are among the many mechanisms described in the SAML specification.

Use Case 1 provides instructions for constructing and accessing URLs that use these profiles. Single logout uses two versions, SOAP and HTTP direct. Federation Termination uses two variations, HTTP data rate and SOAP.

### 15.1 Before You Begin

A sample JSP file is provided at the end of this chapter to help you run the four groups of test cases described in this chapter. Before you can begin running these test cases, you must complete the following tasks:

1. [Create an index.jsp file.](#)
2. [Create a test user in the Identity Provider Site.](#)

The following table summarizes the SAMLv2 profiles you can test in the Federation environment described in previous chapters of this document.

TABLE 15-1 SAMLv2 Profiles Illustrated in Use Case 1

Initiated by Service Provider	Initiated by Identity Provider
Use Case 1A <ol style="list-style-type: none"> <li>1. Persistent Federation (Browser Artifact)</li> <li>2. Logout (SOAP)</li> <li>3. Single Sign-On (Browser Artifact)</li> <li>4. Federation Termination Browser (SOAP)</li> </ol>	Use Case 1C <ol style="list-style-type: none"> <li>1. Persistent Federation (Browser Artifact)</li> <li>2. Logout (SOAP)</li> <li>3. Single Sign-On (Browser Artifact)</li> <li>4. Federation Termination Browser (SOAP)</li> </ol>
Use Case 1B <ol style="list-style-type: none"> <li>1. Persistent Federation (Browser POST)</li> <li>2. Logout (HTTP)</li> <li>3. Single Sign-On (Browser POST)</li> <li>4. Federation (Termination HTTP)</li> </ol>	Use Case 1D <ol style="list-style-type: none"> <li>1. Persistent Federation (Browser POST)</li> <li>2. Logout (HTTP)</li> <li>3. Single Sign-On (POST)</li> <li>4. Federation Termination (HTTP)</li> </ol>

## ▼ To Create an index.jsp File

- 1 As a root user, log into the Federation Manager 1 host.
- 2 Create a text file named `index.jsp` based on the sample below.
- 3 Copy the `index.jsp` file to the following directory:  

```
/opt/SUNWwbsver/https-FederationManager-1.siroe.com/webapps/
https-FederationManager-1.siroe.com/federation/saml2/jsp
```
- 4 As a root user, log into the Federation Manager 2 host.
- 5 Create a text file named `index.jsp` based on the sample below.
- 6 Copy the `index.jsp` file to the following directory:  

```
/opt/SUNWwbsver/https-FederationManager-2.siroe.com/webapps/
https-FederationManager-1.siroe.com/federation/saml2/jsp
```

## ▼ To Create a Test User in the Identity Provider Site

- 1 Go to the Access Manager URL:  

```
https://Loadbalancer-3.example.com:9443/amserver/UI/Login
```

**2 Log in to the Access Manager console using the following information:**User Name: **amadmin**Password: **4m4dmin1****3 On the Realms page, click the users realm name.****4 On the users-Properties page, click the Subjects tab and then click New.****5 On the New User page, provide the following information:**ID: **idp**First Name: **idp**Last Name: **idp**Full Name: **idp**Password: **idp**Password (confirm): **idp**

Click Save.

## 15.2 Testing Requests Initiated by the Service Provider Using SOAP

Use the following as your checklist for testing this use case:

1. [Test persistent Federation using browser artifact.](#)
2. [Test logout using SOAP.](#)
3. [Test Single Sign-On using browser artifact.](#)
4. [Test Federation termination using SOAP.](#)

---

**Note** – Conduct the four tests using the same browser window instance. The tests must be conducted in consecutive order to satisfy Use Case 1A.

---

## ▼ To Test Persistent Federation Using Browser Artifact

### 1 Access the Federation Manager server using one of the following alternatives:

- **Go to the `index.jsp` URL:**

`https://LoadBalancer-9-siroe.com:3443/federation/saml2/jsp/index.jsp`

On the SAML2 Use Cases page, in the SP Initiated Profiles section, click the following link:

Persistent Federation (Browser Artifact)

- **Go to the following URL:**

`https://loadbalancer-9.siroe.com:3443/federation/saml2/jsp/spSSOInit.jsp?metaAlias=/sp&idpEntityID=loadbalancer-3.example.com`

The login request is redirected to Access Manager.

### 2 Log in to the Access Manager console using the following information:

User Name: **idp**

Password: **idp**

The login request is redirected to Federation Manager.

### 3 Log in to the Federation Manager console using the following information:

User Name: **spuser**

User Name: **spuser**

The message “Single Sign-On succeeded” is displayed. You can view the debug file to see the actual assertion that was sent over the wire.

```
# vi /var/opt/SUNWam/fm/federation/debug/fmSAML2
```

## 15.2.1 To Test Logout Using SOAP

Access the Federation Manager server using one of the following alternatives:

- **Go to the `index.jsp` URL:**

`https://LoadBalancer-9-siroe.com:3443/federation/saml2/jsp/index.jsp`

On the SAML2 Use Cases page, in the SP Initiated Profiles section, click the following link:

Logout (SOAP)

- Go to the following URL:

```
https://loadbalancer-9.siroe.com:3443/federation/saml2/jsp/
spSingleLogoutInit.jsp?metaAlias=/sp&binding=
urn:oasis:names:tc:SAML:2.0:bindings:
SOAP&idpEntityID=loadbalancer-3.example.com
```

The message “SP initiated single logout succeeded” is displayed. You can view the debug file to see the actual assertion that was sent over the wire.

```
# vi /var/opt/SUNWam/fm/federation/debug/fmSAML2
```

## ▼ To Test Single Sign-On Using Browser Artifact

- 1 Access the Federation Manager server using one of the following options:

- Go to the `index.jsp` URL:

```
https://LoadBalancer-9-siroe.com:3443/federation/saml2/jsp/index.jsp
```

On the SAML2 Use Cases page, in the SP Initiated Profiles section, click the following link:

Single Sign-On (Browser Artifact)

- Go to the following URL:

```
https://loadbalancer-9.siroe.com:3443/federation/saml2/jsp/
spSSOInit.jsp?metaAlias=/sp&idpEntityID=
loadbalancer-3.example.com
```

- 2 The login request is redirected to Access Manager.

- 3 Log in to the Access Manager console using the following information:

User Name: **idp**

Password: **idp**

The message “Single Sign-On succeeded” is displayed. You can view the debug file to see the actual assertion that was sent over the wire.

```
# vi /var/opt/SUNWam/fm/federation/debug/fmSAML2
```

## ▼ To Test Federation Termination Using SOAP

- Access the Federation Manager server using one of the following alternatives:

- Go to the `index.jsp` URL:

`https://LoadBalancer-9-siroe.com:3443/federation/saml2/jsp/index.jsp`

On the SAML2 Use Cases page, in the SP Initiated Profiles section, click the following link:

Federation Termination (SOAP)

- Go to the following URL:

`https://loadbalancer-9.siroe.com:3443/federation/saml2/jsp/spMNIRRequestInit.jsp?metaAlias=/sp&idpEntityID=loadbalancer-3.example.com&requestType=Terminate&binding=urn:oasis:names:tc:SAML:2.0:bindings:SOAP`

The message “ManageNameID Request succeeded” is displayed. You can view the debug file to see the actual assertion that was sent over the wire.

```
# vi /var/opt/SUNWam/fm/federation/debug/fmSAML2
```

## 15.3 Testing Requests Initiated by the Service Provider Using HTTP Redirect

Use the following as your checklist for testing:

1. Test persistent Federation using browser POST.
2. Test logout using HTTP.
3. Test Single Sign-On Using Browser POST
4. Test Federation termination using HTTP.

---

**Note** – Conduct the four tests using the same browser window instance. The tests must be conducted in consecutive order to satisfy Use Case 1B.

---

## ▼ To Test Persistent Federation Using Browser POST

### 1 Access the Federation Manager server using one of the following alternatives:

- **Go to the `index.jsp` URL:**

`https://LoadBalancer-9-siroe.com:3443/federation/saml2/jsp/index.jsp`

On the SAML2 Use Cases page, in the SP Initiated Profiles section, click the following link:

Persistent Federation (Browser POST)

- **Go to the following URL:**

`https://loadbalancer-9.siroe.com:3443/federation/saml2/jsp/spSSOInit.jsp?metaAlias=/sp&idpEntityID=loadbalancer-3.example.com&binding=HTTP-POST`

The login request is redirected to Access Manager.

### 2 Log in to the Access Manager console using the following information:

User Name: **idp**

Password: **idp**

The login request is redirected to Federation Manager.

### 3 Log in to the Federation Manager console using the following information:

User Name: **spuser**

User Name: **spuser**

The message “Single Sign-On succeeded” is displayed. You can view the debug file to see the actual assertion that was sent over the wire.

```
# vi /var/opt/SUNWam/fm/federation/debug/fmSAML2
```

## ▼ To Test Logout Using HTTP

### ● Access the Federation Manager server using one of the following alternatives:

- **Go to the `index.jsp` URL:**

`https://LoadBalancer-9-siroe.com:3443/federation/saml2/jsp/index.jsp`

On the SAML2 Use Cases page, in the SP Initiated Profiles section, click the following link:

Logout (HTTP)

- **Go to the following URL:**

```
https://loadbalancer-9.siroe.com:3443/federation/saml2/jsp/spSingleLogoutInit.jsp?metaAlias=/sp&idpEntityID=loadbalancer-3.example.com
```

The message “SP initiated single logout succeeded” is displayed. You can view the debug file to see the actual assertion that was sent over the wire.

```
# vi /var/opt/SUNWam/fm/federation/debug/fmSAML2
```

## ▼ To Test Single Sign-On Using Browser POST

### 1 Access the Federation Manager using one of the following options:

- Go to the `index.jsp` URL:

```
https://LoadBalancer-9-siroe.com:3443/federation/saml2/jsp/index.jsp
```

On the SAML2 Use Cases page, in the SP Initiated Profiles section, click the following link:

Single Sign-On (Browser POST)

- Configure and go to the following URL:

```
https://loadbalancer-9.siroe.com:3443/federation/saml2/jsp/spSSOInit.jsp?metaAlias=/sp&idpEntityID=loadbalancer-3.example.com&binding=HTTP-POST
```

The login request is redirected to Access Manager.

### 2 Log in to the Access Manager console using the following information:

User Name: **idp**

Password: **idp**

The message “Single Sign-On succeeded” is displayed. You can view the debug file to see the actual assertion that was sent over the wire.

```
# vi /var/opt/SUNWam/fm/federation/debug/fmSAML2
```



## ▼ To Test Federation Termination Using HTTP

- Access the Federation Manager server using one of the following alternatives:

- Go to the `index.jsp` URL:

`https://LoadBalancer-9-siroe.com:3443/federation/saml2/jsp/index.jsp`

On the SAML2 Use Cases page, in the SP Initiated Profiles section, click the following link:

Federation Termination (HTTP)

- Go to the following URL:

`https://loadbalancer-9.siroe.com:3443/federation/saml2/jsp/spMNIRequestInit.jsp?metaAlias=/sp&idpEntityID=loadbalancer-3.example.com&requestType=Terminate`

The message “ManageNameID Request succeeded” is displayed. You can view the debug file to see the actual assertion that was sent over the wire.

```
# vi /var/opt/SUNWam/fm/federation/debug/fmSAML2
```

## 15.4 Testing Requests Initiated by the Identity Provider Using SOAP

Use the following as your checklist for testing:

1. [Test persistent Federation using browser artifact.](#)
2. [“To Test Logout Using SOAP” on page 266](#)
3. [“To Test Single Sign-On Using Browser Artifact” on page 267](#)
4. [“To Test Federation Termination Using SOAP” on page 267](#)

---

**Note** – Conduct the four tests using the same browser window instance. The tests must be conducted in consecutive order to satisfy Use Case 1C.

---

## ▼ To Test Persistent Federation Using Browser Artifact

- 1 Access the Federation Manager server using one of the following alternatives:

- Go to the `index.jsp` URL:

`https://LoadBalancer-9-siroe.com:3443/federation/saml2/jsp/index.jsp`

On the SAML2 Use Cases page, in the IDP Initiated Profiles section, click the following link:

Persistent Federation (Browser Artifact)

- Go to the following URL:

```
https://loadbalancer-3.example.com:9443/amserver/saml2/jsp/
idpSSOInit.jsp?metaAlias=/users/idp&spEntityID=
loadbalancer-9.siroe.com
```

The login request is redirected to Access Manager.

## 2 Log in to the Access Manager console using the following information:

User Name: **idp**

Password: **idp**

The login request is redirected to Federation Manager.

## 3 Log in to the Federation Manager console using the following information:

User Name: **spuser**

User Name: **spuser**

The message “Single Sign-On succeeded” is displayed. You can view the debug file to see the actual assertion that was sent over the wire.

```
# vi /var/opt/SUNWam/fm/federation/debug/fmSAML2
```

# ▼ To Test Logout Using SOAP

## ● Access the Federation Manager server using one of the following alternatives:

- **Go to the index.jsp URL:**

```
https://LoadBalancer-9-siroe.com:3443/federation/saml2/jsp/index.jsp
```

On the SAML2 Use Cases page, in the IDP Initiated Profiles section, click the following link:

Logout (HTTP)

- **Go to the following URL:**

```
https://loadbalancer-3.example.com:9443/amserver/saml2/jsp/
idpSingleLogoutInit.jsp?metaAlias=/users/idp&spEntityID=
loadbalancer-9.siroe.com&binding=
urn:oasis:names:tc:SAML:2.0:bindings:SOAP
```

The message “IDP initiated single logout succeeded” is displayed. You can view the debug file to see the actual assertion that was sent over the wire.

```
# vi /var/opt/SUNWam/fm/federation/debug/fmSAML2
```

## ▼ To Test Single Sign-On Using Browser Artifact

### 1 Access the Federation Manager server using one of the following alternatives:

- **Go to the index.jsp URL:**

```
https://LoadBalancer-9-siroe.com:3443/federation/saml2/jsp/index.jsp
```

On the SAML2 Use Cases page, in the IDP Initiated Profiles section, click the following link:

Single Sign-On (Browser Artifact)

- **Go to the following URL:**

```
https://loadbalancer-3.example.com:9443/amserver/saml2/jsp/idpSSOInit.jsp?metaAlias=/users/idp&spEntityID=loadbalancer-9.siroe.com
```

The login request is redirected to Access Manager.

### 2 Log in to the Access Manager console using the following information:

User Name: **idp**

Password: **idp**

The message “Single Sign-On succeeded” is displayed. You can view the debug file to see the actual assertion that was sent over the wire.

```
# vi /var/opt/SUNWam/fm/federation/debug/fmSAML2
```

## ▼ To Test Federation Termination Using SOAP

### ● Access the Federation Manager server using one of the following alternatives:

- **Go to the index.jsp URL:**

```
https://LoadBalancer-9-siroe.com:3443/federation/saml2/jsp/index.jsp
```

On the SAML2 Use Cases page, in the IDP Initiated Profiles section, click the following link:

Federation Termination (HTTP)

- **Go to the following URL:**

```
https://loadbalancer-3.example.com:9443/amserver/saml2/jsp/  
idpMNIRequestInit.jsp?metaAlias=/users/idp&spEntityID=  
loadbalancer-9.siroe.com&binding=  
urn:oasis:names:tc:SAML:2.0:bindings:SOAP&requestType=Terminate
```

The message “ManageNameID Request succeeded” is displayed. You can view the debug file to see the actual assertion that was sent over the wire.

```
# vi /var/opt/SUNWam/fm/federation/debug/fmSAML2
```

## 15.5 Testing Requests Initiated by the Identity Provider Using HTTP Redirect

Use the following as your checklist for testing:

1. Test persistent Federation using browser POST.
2. Test logout using HTTP.
3. Test Single Sign-On using browser POST.
4. Test Federation termination using HTTP.

---

**Note** – Conduct the four tests using the same browser window instance. The tests must be conducted in consecutive order to satisfy Use Case 1D.

---

### ▼ To Test Persistent Federation Using Browser POST

#### 1 Access the Federation Manager server using one of the following alternatives:

- **Go to the index.jsp URL:**

```
https://LoadBalancer-9-siroe.com:3443/federation/saml2/jsp/index.jsp
```

On the SAML2 Use Cases page, in the SP Initiated Profiles section, click the following link:

Persistent Federation (Browser POST)

- **Go to the following URL:**

```
https://loadbalancer-3.example.com:9443/amserver/saml2/jsp/  
/idpSSOInit.jsp?metaAlias=/users/idp&spEntityID=  
loadbalancer-9.siroe.com&binding=HTTP-POST
```

The login request is redirected to Access Manager.

**2 Log in to the Access Manager console using the following information:**User Name: **idp**Password: **idp**

The login request is redirected to Federation Manager.

**3 Log in to the Federation Manager console using the following information:**User Name: **spuser**User Name: **spuser**

The message “Single Sign-On succeeded” is displayed. You can view the debug file to see the actual assertion that was sent over the wire.

```
# vi /var/opt/SUNWam/fm/federation/debug/fmSAML2
```

**▼ To Test Logout Using HTTP****● Access the Federation Manager server using one of the following alternatives:****■ Go to the index.jsp URL:**

```
https://LoadBalancer-9-siroe.com:3443/federation/saml2/jsp/index.jsp
```

On the SAML2 Use Cases page, in the SP Initiated Profiles section, click the following link:

Logout (HTTP)

**■ Go to the following URL:**

```
https://loadbalancer-3.example.com:9443/amserver/saml2/jsp/
idpSingleLogoutInit.jsp?metaAlias=/users/idp&spEntityID=
loadbalancer-9.siroe.com
```

The message “SP initiated single logout succeeded” is displayed. You can view the debug file to see the actual assertion that was sent over the wire.

```
# vi /var/opt/SUNWam/fm/federation/debug/fmSAML2
```

## ▼ To Test Single Sign-On Using Browser POST

### 1 Access the Federation Manager server using one of the following alternatives:

- **Go to the index.jsp URL:**

`https://LoadBalancer-9-siroe.com:3443/federation/saml2/jsp/index.jsp`

On the SAML2 Use Cases page, in the SP Initiated Profiles section, click the following link:

Single Sign-On (Browser POST)

- **Configure the following URL:**

`https://loadbalancer-3.example.com:9443/amserver/saml2/jsp/idpSSOInit.jsp?metaAlias=/users/idp&spEntityID=loadbalancer-9.siroe.com&binding=HTTP-POST`

The login request is redirected to Access Manager.

### 2 Log in to the Access Manager console using the following information:

User Name: **idp**

Password: **idp**

The message “Single Sign-On succeeded” is displayed. You can view the debug file to see the actual assertion that was sent over the wire.

```
# vi /var/opt/SUNWam/fm/federation/debug/fmSAML2
```

## ▼ To Test Federation Termination Using HTTP

### ● Access the Federation Manager server using one of the following alternatives:

- **Access the index.jsp URL:**

`https://LoadBalancer-9-siroe.com:3443/federation/saml2/jsp/index.jsp`

On the SAML2 Use Cases page, in the SP Initiated Profiles section, click the following link:

Federation Termination (HTTP)

- **Go to the following URL:**

`https://loadbalancer-3.example.com:9443/amserver/saml2/jsp/idpMNIRRequestInit.jsp?metaAlias=/users/idp&spEntityID=loadbalancer-9.siroe.com&requestType=Terminate`

The message “ManageNameID Request succeeded” is displayed. You can view the debug file to see the actual assertion that was sent over the wire.

```
# vi /var/opt/SUNWam/fm/federation/debug/fmSAML2
```

## 15.6 The Sample jsp.index File

EXAMPLE 15-1 Sample jsp.index File for Testing SAMLv2 Protocols

```
<%--
  Copyright © 2004 Sun Microsystems, Inc. All rights reserved
  Use is subject to license terms.
--%>

<html>
<head>
<title>SAML2 Usecases (index)</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">

<link rel="stylesheet" href="samples/liberty/sso/css/styles.css"
type="text/css">

</head>

<body bgcolor="#FFFFFF" text="#000000" leftmargin="9" marginwidth="9"
  topmargin="9" marginheight="9" >
<br>

<table width="30%" border="0" cellspacing="0" cellpadding="0" >

  <tr>
  <td colspan="2">&nbsp;</td>
  <td width="100%">
  <table border="0" cellspacing="0" cellpadding="0" align=center>
  <tr>
  <td>
    <P ALIGN=CENTER>
      <FONT FACE="Arial Narrow, sans-serif">
      <FONT SIZE=2 STYLE="font-size: 11pt">
        <B>SAML2 Usecases</B>
      </FONT>
    </FONT>
  </td>
  </tr>
  </table>
  </td>
  </tr>
  </table>
```

## EXAMPLE 15-1 Sample jsp.index File for Testing SAMLv2 Protocols (Continued)

```

        </P>
</td>
</tr>

<tr><td colspan="3">&nbsp;</td></tr>
<tr>
  <td>
<p>
  <B>SP Initiated Profiles</B>
</p>
</td>
</tr>

<tr><td colspan="3">&nbsp;</td></tr>
<tr>
  <td>
<p>
  <a href="https://loadbalancer-9.siroe.com:3443/federation/saml2/jsp/
    /spSSOInit.jsp?metaAlias=/sp&idpEntityID=loadbalancer-3.example.com">
    Persistent Federation (Browser Artifact) </a>
</p>
</td>
</tr>

<tr><td colspan="3">&nbsp;</td></tr>
<tr>
  <td>
<p>
  <a href="https://loadbalancer-9.siroe.com:3443/federation/saml2/jsp/
    spSingleLogoutInit.jsp?metaAlias=/sp&binding=urn:oasis:names:tc:SAML:
    2.0:bindings:SOAP&idpEntityID=loadbalancer-3.example.com">Logout (SOAP) </a>
</p>
</td>
</tr>

<tr><td colspan="1">&nbsp;</td></tr>
<tr>
  <td>
<p>
  <a href="https://loadbalancer-9.siroe.com:3443/federation/saml2/jsp/
    spSSOInit.jsp?metaAlias=/sp&idpEntityID=loadbalancer-3.example.com">
    Single Sign-On (Browser Artifact) </a>
</p>
</td>
</tr>

```



## EXAMPLE 15-1 Sample jsp.index File for Testing SAMLv2 Protocols (Continued)

```

<tr><td colspan="1">&nbsp;</td></tr>
<tr>
  <td>
    <p>
      <a href="https://loadbalancer-9.siroe.com:3443/federation/saml2/jsp/
        spMNIRequestInit.jsp?metaAlias=/sp&idpEntityID=
        loadbalancer-3.example.com&requestType=Terminate&binding=
        urn:oasis:names:tc:SAML:2.0:bindings:SOAP">
          Federation Termination(SOAP)</a>
    </p>
  </td>
</tr>

<tr><td colspan="1">&nbsp;</td></tr>
<tr>
  <td>
    <p>
      <a href="https://loadbalancer-9.siroe.com:3443/federation/saml2/jsp
        /spSSOInit.jsp?metaAlias=/sp&idpEntityID=
        loadbalancer-3.example.com&binding=
        HTTP-POST">Persistent Federation (Browser POST) </a>
    </p>
  </td>
</tr>

<tr><td colspan="1">&nbsp;</td></tr>
<tr>
  <td>
    <p>
      <a href="https://loadbalancer-9.siroe.com:3443/federation/saml2/jsp/
        spSingleLogoutInit.jsp?metaAlias=/sp&idpEntityID=
        loadbalancer-3.example.com">
          Logout(HTTP)</a>
    </p>
  </td>
</tr>

<tr><td colspan="1">&nbsp;</td></tr>
<tr>
  <td>
    <p>
      <a href="https://loadbalancer-9.siroe.com:3443/federation/saml2/jsp
        /spSSOInit.jsp?metaAlias=/sp&idpEntityID=
        loadbalancer-3.example.com&binding=

```

## EXAMPLE 15-1 Sample jsp.index File for Testing SAMLv2 Protocols (Continued)

```

        HTTP-POST">Single Sign-On (Browser POST) </a>
    </p>
</td>
</tr>

<tr><td colspan="1">&nbsp;</td></tr>
<tr>
    <td>
<p>
    <a href="https://loadbalancer-9.siroe.com:3443/federation/saml2/jsp
        /spMNIRRequestInit.jsp?metaAlias=/sp&idpEntityID=
        loadbalancer-3.example.com&requestType=Terminate">
        Federation Termination(HTTP)</a>
    </p>
</td>
</tr>

<tr><td colspan="1">&nbsp;</td></tr>
<tr>
    <td>
<p>
    <B>IDP Initiated Profiles </B>
    </p>
</td>
</tr>

<tr><td colspan="1">&nbsp;</td></tr>
<tr>
    <td>
<p>
    <a href="https://loadbalancer-3.example.com:9443/amserver/saml2/jsp
        /idpSSOInit.jsp?metaAlias=/users/idp&spEntityID=
        loadbalancer-9.siroe.com">
        Persistent Federation (Browser Artifact)</a>
    </p>
</td>
</tr>

<tr><td colspan="1">&nbsp;</td></tr>
<tr>
    <td>
<p>
    <a href="https://loadbalancer-3.example.com:9443/amserver/saml2/jsp
        /idpSingleLogoutInit.jsp?metaAlias=/users/idp&spEntityID=
        loadbalancer-9.siroe.com&binding=

```

## EXAMPLE 15-1 Sample jsp.index File for Testing SAMLv2 Protocols (Continued)

```

        urn:oasis:names:tc:SAML:2.0:bindings:SOAP">Logout (SOAP)</a>
    </p>
</td>
</tr>

<tr><td colspan="1">&nbsp;</td></tr>
<tr>
    <td>
<p>
    <a href="https://loadbalancer-3.example.com:9443/amserver/saml2/jsp
        /idpSSOInit.jsp?metaAlias=/users/idp&spEntityID=
        loadbalancer-9.siroe.com">
        Single Sign-On (Browser Artifact)</a>
    </p>
</td>
</tr>

<tr><td colspan="1">&nbsp;</td></tr>
<tr>
    <td>
<p>
    <a href="https://loadbalancer-3.example.com:9443/amserver/saml2/jsp
        /idpMNIRquestInit.jsp?metaAlias=/users/idp&spEntityID=
        loadbalancer-9.siroe.com&binding= urn:oasis:names:tc:SAML:2.0:
        bindings:SOAP&requestType=Terminate">Federation Termination (SOAP)</a>
    </p>
</td>
</tr>

<tr><td colspan="1">&nbsp;</td></tr>
<tr>
    <td>
<p>
    <a href="https://loadbalancer-3.example.com:9443/amserver/saml2/jsp
        /idpSSOInit.jsp?metaAlias=/users/idp&spEntityID=
        loadbalancer-9.siroe.com&binding=
        HTTP-POST">Persistent Federation (Browser POST)</a>
    </p>
</td>
</tr>

<tr><td colspan="1">&nbsp;</td></tr>
<tr>
    <td>
<p>

```

## EXAMPLE 15-1 Sample jsp.index File for Testing SAMLv2 Protocols (Continued)

```
<a href="https://loadbalancer-3.example.com:9443/amserver/saml2/jsp
    /idpSingleLogoutInit.jsp?metaAlias=/users/idp&spEntityID=
    loadbalancer-9.siroe.com">Logout (HTTP)</a>
</p>
</td>
</tr>

<tr><td colspan="1">&nbsp;</td></tr>
<tr>
  <td>
<p>
  <a href="https://loadbalancer-3.example.com:9443/amserver/saml2/jsp
    /idpSSOInit.jsp?metaAlias=/users/idp&spEntityID=
    loadbalancer-9.siroe.com&binding=
    HTTP-POST">Single Sign-On (Browser POST)</a>
</p>
</td>
</tr>

<tr><td colspan="1">&nbsp;</td></tr>
<tr>
  <td>
<p>
  <a href="https://loadbalancer-3.example.com:9443/amserver/saml2/jsp
    /idpMNIRequestInit.jsp?metaAlias=/users/idp&spEntityID=
    loadbalancer-9.siroe.com&requestType=Terminate">
    Federation Termination (HTTP)</a>
</p>
</td>
</tr>

<tr><td colspan="1">&nbsp;</td></tr>

</table>
</td>
</tr>
</table>

</body>
</html>
```

## Use Case 2: User Attribute Mapping

---

In this use case, no user repository exists in the Service Provider site. All users in the Identity Provider site are mapped to an anonymous user. The anonymous user represents all users in the Identity Provider site when it presents itself to the Service Provider site. The anonymous user is used to map transient-based federation attributes.

This use case illustrates how you can pass user profile attributes from the Identity Provider site to the to Service Provider site, and the from Service Provider site to all of its Service Provider agent-protected applications. Communication from the Identity Provider site to the Service Provider site takes place using SAMLv2 protocols. Communication from Federation Manager site to all Service Provider agent-protected applications takes place using agent-to- LDAP attribute mapping.

### 16.1 Mapping User Attributes from the Identity Provider to a Single User on the Service Provider

Use the following as your checklist for mapping user attributes to a single user:

1. [Modify the user's LDAP user attributes.](#)
2. [Create a new user.](#)
3. [Edit the new user's contact information.](#)
4. [Modify the Identity Provider metadata.](#)
5. [Modify the Service Provider metadata.](#)
6. [Modify the agents properties.](#)
7. [Verify that attribute mapping is working properly.](#)

## ▼ To Modify the usersLDAP User Attributes

**1 Go to the Access Manager URL:**

`https://LoadBalancer-3.example.com:9443/amserver/UI/Login`

**2 Log in to the Access Manager console using the following information:**

User name: `amadmin`

Password: `4m4dmin1`

**3 Add the usersLDAP user attributes that will be set for the user entry.**

In this example, you will add the `mail` and `telephone number` attributes.

a. On the **Realms** page, click the `users` realm name, and then click **Data Stores**.

b. On the `users` — **Data Stores** page, click the `usersLDAP` data store name.

c. On the **Edit Data Store** page, add `givenname` to the **LDAP User Attributes** list.

In the **LDAP User Attributes** field, enter `givenname`, and then click **Add**.

d. In the same manner, add `mail` to the **LDAP User Attributes** list.

e. In the same manner, add `telephonenumber` to the **LDAP User Attributes** list.

f. Click **Save**.

## ▼ To Create a New User

**1 Go to the Access Manager URL:**

`https://LoadBalancer-3.example.com:9443/amserver/UI/Login`

**2 Log in to the Access Manager console using the following information:**

User name: `amadmin`

Password: `4m4dmin1`

**3 On the Realms page, click the users realm name, and then click the Subject tab.**

**4 On the User tab, click New.**

**5 On the New User page, provide the following information:**

ID: **jsmith**  
First Name: **John**  
Last Name: **Smith**  
Full Name: **John Smith**  
Password: **jsmith**  
Password (confirm): **jsmith**

Click Create, and then log out of the Access Manager console.

## ▼ To Edit the New User's Contact Information

### 1 Go to the Access Manager URL:

<https://LoadBalancer-3.example.com:9443/amserver/UI/Login>

### 2 Log in to the Access Manager console using the following information:

User name: **amadmin**

Password: **4m4dmin1**

### 3 On the Realms page, click the users realm name, and then click the Subject tab.

### 4 On the User tab, in the list of users, click `jsmith`.

### 5 On the Edit User page, provide the following information:

Email Address: `jsmith@example.com`

Telephone Number: `408-555-5454`

Click Save, and then log out of the Access Manager console.

## ▼ To Modify the Identity Provider Metadata

### 1 As a root user, log into the Access Manager 1 host.

## 2 In the Identity Provider extended metadata file, map the Email Address and Telephone Number attributes.

For example, in the first value-pair mapping, `mail` is the LDAP attribute name, and `EmailAddress` is the information to be sent over the wire using SAMLv2 protocols.

```
# cd /etc/opt/SUNWam/config
# vi saml2-idp-extended-metadata.xml
...
<Attribute name="attributeMap">
    <Value>EmailAddress=mail</Value>
    <Value>Telephone=telephonenumber</Value>
...
```

Save the file.

## 3 Delete the existing metadata.

```
# /opt/SUNWam/saml2/bin/saml2meta delete -u amadmin -w 4m4dmin1
-r /users -e loadbalancer3.example.com
Descriptor and config fore entity "loadbalancer-3.example" was deleted successfully.
```

## 4 Load the modified metadata file into the Directory Server.

```
#/opt/SUNWam/saml2/bin/saml2meta import -u amadmin -w 4m4dmin1 -r /users
-m saml2-idp-metadata.xml -x saml2-idp-extended-metadata.xml
File "saml2-idp-metadata.xml" was imported successfully.
File "saml2-idp-extended-metadata.xml" was imported successfully.
```

When you map the attributes on one Access Manager server, the mapping is also made available to the second Access Manager. So you do not have to modify metadata on the Access Manager 2 server. The metadata will also be made available to the Federation Manager servers.

# ▼ To Modify the Service Provider Metadata

## 1 As a root user, log into the Federation Manager 1 host .

## 2 In the Service Provider extended metadata file, map the Email Address and Telephone Number attributes.

```
# cd /etc/opt/SUNWam/config
# vi saml2-sp-extended-metadata.xml
...
<Attribute name="attributeMap">
    <Value>EmailAddress=EmailAddress</Value>
    <Value>Telephone=Telephone</Value>
...
```



Notice that the value `mail` in the `EmailAddress` attribute—value pair does not have to be identical to the value `EmailAddress` specified in the Identity Provider metadata.

### 3 Add anonymous to the transient user list.

```
<Attribute name="transientUser">
    <Value>anonymous</Value>
```

Save the file.

### 4 Delete the existing metadata.

```
# /opt/SUNWam/saml2/bin/saml2meta -i /var/opt/SUNWam/fm/war_staging
delete -u amadmin -w 11111111 -e loadbalancer-9.siroe.com
```

### 5 Load the modified metadata file into the Directory Server.

```
#/opt/SUNWam/saml2/bin/saml2meta -i /var/opt/SUNWam/fn/war_staging import
-u amadmin -w 11111111 -m saml2-sp-metadata.xml -x saml2-sp-extended-metadata.xml
File "saml2-sp-metadata.xml" was imported successfully.
File "saml2-sp-extended-metadata.xml" was imported successfully.
```

Save the file.

### 6 Restart Federation Manager 1.

```
# cd /opt/SUNWwbsvr/https-FederationManager-1.siroe.com
# ./stop; ./start
```

### 7 Restart Federation Manager 2.

```
# cd /opt/SUNWwbsvr/https-FederationManager-2.siroe.com
# ./stop; ./start
```

## ▼ To Modify the Agents Properties

### 1 Modify the Web Policy Agents properties.

### 2 As a root user, log into the Protected Resource 3 host.

### 3 Add the transient attribute to the property `com.sun.am.policy.am.login.url`.

```
# cd /etc/opt/SUNWam/agents/es6/config/
_opt_SUNWwbsvr_https-ProtectedResource-3.siroe.com
# vi AMAgent.properties
com.sun.am.policy.am.login.url =
https://LoadBalancer-9.siroe.com:3443/federation/
saml2/jsp/spSSOInit.jsp?metaAlias=sp&idpEntityID=
loadbalancer-3.example.com&NameIDFormat=transient
```

**4 Modify the following properties:**

```
com.sun.am.policy.agents.config.session.attribute.fetch.mode=HTTP_HEADER
com.sun.am.policy.agents.config.session.attribute.map=
EmailAddress|EmailAddress,Telephone|Telephone
```

Save the file.

**5 Restart the Protected Resource 3 host.**

```
# cd /opt/SUNWwbsvr/https-ProtectedResource-3.siroe.com
# ./stop; ./start
```

**6 As a root user, log into the Protected Resource 4 host.****7 Add the transient NameID format to the property com.sun.am.policy.am.login.url.**

```
# cd /etc/opt/SUNWam/agents/e6/config/
_opt_SUNWwbsvr_https-ProtectedResource-4.siroe.com
# vi AMAgent.properties
com.sun.am.policy.am.login.url =
https://LoadBalancer-9.siroe.com:3443/federation/
saml2/jsp/spSSOInit.jsp?metaAlias=sp&idpEntityID=
loadbalancer-4.example.com&NameIDFormat=transient
```

**8 Modify the following properties:**

```
com.sun.am.policy.agents.config.session.attribute.fetch.mode=HTTP_HEADER
com.sun.am.policy.agents.config.session.attribute.map=
EmailAddress|EmailAddress,Telephone|Telephone
```

Save the file.

**9 Restart the Protected Resource 4 host.**

```
# cd /opt/SUNWwbsvr/https-ProtectedResource-4.siroe.com
# ./stop; ./start
```

## ▼ To Verify that Attribute Mapping is Working Properly

The file `snoop.jsp` is provided at the end of this chapter for you to use with this deployment example. The `snoop.jsp` file reads each of the HTTP headers and reads a number of query parameters in the SAMLv2 metadata. In this use case, the JSP determines which headers are being passed from the Service Provider to the agent. When you will initiate SAMLv2 for Federation, the user attribute mapping from the Identity Provider to the Service Provider takes place using the SAMLv2 protocol. The mapping from the Service Provider to the Identity Provider takes place using LDAP attribute mapping from Federation Manager to the Web Policy Agent.

- 1 **As a root user, log into the Protected Resource 3 host.**
- 2 **Copy the `snoop.jsp` file to the following directory on both the Protected Resource 3 host and the Protected Resource 4 host:**

`/opt/SUNWwbsvr/docs`

- 3 **Access `snoop.jsp` through the Web Policy Agents URL:**

`https://LoadBalancer-11.siroe.com:6443/snoop.jsp`

The Web Policy Agent redirects the request, and the Access Manager login page is displayed.

- 4 **Log in to the Access Manager console using the following information:**

User Name: `jsmith`

Password: `jsmith`

The JSP Snoop Page is displayed. John Smith's telephone number and email address are included in the request headers section of the file. Also notice that the Remote user is anonymous. This is the user that serves as confirmation of the `transientUser` you configured in the `saml2-sp-extended-metadata.xml` file on the Service Provider.

## Request information

**Requested URL:** http://loadbalancer-11.siroe.com:6443/snoop.jsp  
**Request method:** GET  
**Request URI:** /snoop.jsp  
**Request protocol:** HTTP/1.1  
**Servlet path:** /snoop.jsp  
**Path info:** null  
**Path translated:** null  
**Query string:** null  
**Content length:** -1  
**Content type:** null  
**Server name:** loadbalancer-11.siroe.com  
**Server port:** 6443  
**Remote user:** anonymous  
**Remote address:** 192.18.69.17  
**Remote host:** 192.18.69.17  
**Authorization scheme:** DSAME

## Request headers

Header:	Value:
accept-encoding	gzip,deflate
connection	keep-alive
accept-language	en-us,en;q=0.5
host	loadbalancer-11.siroe.com:6443
telephone	408-276-5555
accept-charset	ISO-8859-1,utf-8;q=0.7,*;q=0.7
user-agent	Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.8.1.3) Gecko/20070309
emailaddress	jsmith@sun.com

FIGURE 16-1 Output from snoop.jsp

### Example 16-1 snoop.jsp

```

sr1-usca-43 7 > view snoop.jsp
"snoop.jsp" [Read only] 171 lines, 3825 characters
<HTML>
<HEAD>
    <TITLE>JSP snoop page</TITLE>
    <%@ page import="javax.servlet.http.
        HttpUtils,java.util.Enumeration" %>
</HEAD>
<BODY>
    <H1>JSP Snoop page</H1>

```

## <H2>Request information</H2>

```

<TABLE>
<TR>
  <TH align=right>Requested URL:</TH>
  <TD><%= HttpUtils.getRequestURL(request) %></TD>
</TR>
<TR>
  <TH align=right>Request method:</TH>
  <TD><%= request.getMethod() %></TD>
</TR>
<TR>
  <TH align=right>Request URI:</TH>
  <TD><%= request.getRequestURI() %></TD>
</TR>
<TR>
  <TH align=right>Request protocol:</TH>
  <TD><%= request.getProtocol() %></TD>
</TR>
<TR>
  <TH align=right>Servlet path:</TH>
  <TD><%= request.getServletPath() %></TD>
</TR>
<TR>
  <TH align=right>Path info:</TH>
  <TD><%= request.getPathInfo() %></TD>
</TR>
<TR>
  <TH align=right>Path translated:</TH>
  <TD><%= request.getPathTranslated() %></TD>
</TR>
<TR>
  <TH align=right>Query string:</TH>
  <TD><%= request.getQueryString() %></TD>
</TR>
<TR>
  <TH align=right>Content length:</TH>
  <TD><%= request.getContentLength() %></TD>
</TR>
<TR>
  <TH align=right>Content type:</TH>
  <TD><%= request.getContentType() %></TD>
</TR>
<TR>
  <TH align=right>Server name:</TH>
  <TD><%= request.getServerName() %></TD>

```

```

<TR>
<TR>
    <TH align=right>Server port:</TH>
    <TD><%= request.getServerPort() %></TD>
<TR>
<TR>
    <TH align=right>Remote user:</TH>
    <TD><%= request.getRemoteUser() %></TD>
<TR>
<TR>
    <TH align=right>Remote address:</TH>
    <TD><%= request.getRemoteAddr() %></TD>
<TR>
<TR>
    <TH align=right>Remote host:</TH>
    <TD><%= request.getRemoteHost() %></TD>
<TR>
<TR>
    <TH align=right>Authorization scheme:</TH>
    <TD><%= request.getAuthType() %></TD>
<TR>
</TABLE>

<%
    Enumeration e = request.getHeaderNames();
    if(e != null && e.hasMoreElements()) {
%>
<H2>Request headers</H2>

<TABLE>
<TR>
    <TH align=left>Header:</TH>
    <TH align=left>Value:</TH>
</TR>
<%
        while(e.hasMoreElements()) {
            String k = (String) e.nextElement();
%>
<TR>
    <TD><%= k %></TD>
    <TD><%= request.getHeader(k) %></TD>
</TR>
<%
        }
%>
</TABLE>
<%

```

```

    }
%>

<%
    e = request.getParameterNames();
    if(e != null && e.hasMoreElements()) {
%>
<H2>Request parameters</H2>
<TABLE>
<TR valign=top>
    <TH align=left>Parameter:</TH>
    <TH align=left>Value:</TH>
    <TH align=left>Multiple values:</TH>
</TR>
<%
        while(e.hasMoreElements()) {
            String k = (String) e.nextElement();
            String val = request.getParameter(k);
            String vals[] = request.getParameterValues(k);
%>
<TR valign=top>
    <TD><%= k %></TD>
    <TD><%= val %></TD>
    <TD><%
            for(int i = 0; i < vals.length; i++) {
                if(i > 0)
                    out.print("<BR>");
                out.print(vals[i]);
            }
        %></TD>
</TR>
<%
        }
%>
</TABLE>
<%
    }
%>

<%
    e = getServletConfig().getInitParameterNames();
    if(e != null && e.hasMoreElements()) {
%>
<H2>Init parameters</H2>
<TABLE>
<TR valign=top>

```

```
        <TH align=left>Parameter:</TH>
        <TH align=left>Value:</TH>
    </TR>
    <%
        while(e.hasMoreElements()) {
            String k = (String) e.nextElement();
            String val = getServletConfig().getInitParameter(k);
    %>
    <TR valign=top>
        <TD><%= k %></TD>
        <TD><%= val %></TD>
    </TR>
    <%
        }
    %>
</TABLE>
<%
}
%>
</BODY>
</HTML>
```



PART VII

Reference: Summaries of Server and  
Component Configurations



# Directory Servers

---

TABLE A-1 Directory Server 3SP Configuration

Component	Description
Host	Computer system that hosts the Directory Server.
	Host Name            DirectoryServer-3SP.siroe.com
Directory Server Administration Instance	Administration server that manages Directory Server and all its instances.
	Port Number            1391
	Service URL            http://DirectoryServer-3SP.siroe.com:1391
	Instance Directory    /var/opt/mps/serverroot/admin-serv
Directory Server Configuration Instance	Instance that stores Directory Server configuration data.
	Instance name            DirectoryServer-3SP
	Port Number            1390
	Service URL            http://DirectoryServer-3SP.siroe.com:1390
	Base suffix              dc=siroe,dc=com
	Super User                cn=Directory Manager
	Super User password    admin123
	Administrative User    admin
	Administrative User Password    admin123
	Instance Directory    /var/opt/mps/serverroot/slaped-DirectoryServer-3SP

TABLE A-1 Directory Server 3SP Configuration (Continued)

Component	Description
Federation Manager Configuration Instance	Stores Federation Manager configuration data.
	Instance name fm-config
	Port Number 1389
	Service URL http://DirectoryServer-3SP.siroe.com:1389
	Base Suffix o=siroe.com
	Replication Manager cn=replication manager,cn=replication,cn=config
	Replication Manager Password 11111111
	Instance Directory /var/opt/mps/serverroot/slapd-fm-config
User Data Store	Stores Federation Manager user data. In this deployment example, the user data store is located on the same computer system as the Federation Manager configuration data store. The user data store could also be installed on a different computer system.
	Instance Name fm-users
	Port Number 1489
	Service URL http://DirectoryServer-3SP.siroe.com:1489
	Base Suffix dc=siroe, dc=com
	Users Suffix o=siroeusers
	Replication Manager cn=replication manager, cn=replication,cn=config
	Replication Manager Password 11111111
	Instance Directory /var/opt/mps/serverroot/slapd-fm-users

TABLE A-2 Directory Server 4SP Configuration

Component	Description
Host	Computer system that hosts the Directory Server.
	Host Name            DirectoryServer-4SP.siroe.com
Directory Server Administration Instance	Administration server that manages Directory Server and all its instances.
	Port Number            1391
	Service URL            http://DirectoryServer-4SP.siroe.com:1391
	Instance Directory    /var/opt/mps/serverroot/admin-serv
Directory Server Configuration Instance	Instance that stores Directory Server configuration data.
	Instance name            DirectoryServer-4SP
	Port Number            1390
	Service URL            http://DirectoryServer-4SP.siroe.com:1390
	Base suffix             dc=siroe,dc=com
	Super User              cn=Directory Manager
	Super User password    admin123
	Administrative User    admin
	Administrative User Password    admin123
	Instance Directory    /var/opt/mps/serverroot/slapd-DirectoryServer-4SP
Federation Manager Configuration Instance	Stores Federation Manager configuration data.
	Instance name            fm-config
	Port Number            1389
	Service URL            http://DirectoryServer-4SP.siroe.com:1389
	Base Suffix             o=siroe.com
	Replication Manager    cn=replication manager,cn=replication,cn=config
	Replication Manager Password    11111111
	Instance Directory    /var/opt/mps/serverroot/slapd-fm-config

TABLE A-2 Directory Server 4SP Configuration (Continued)

Component	Description
User Data Store	Stores Federation Manager user data. In this deployment example, the user data store is located on the same computer system as the Federation Manager configuration data store. The user data store could also be installed on a different computer system.
Instance Name	fm-users
Port Number	1489
Service URL	http://DirectoryServer-4 SP.siroe.com:1489
Base Suffix	dc=siroe, dc=com
Users Suffix	o=siroeuers
Replication Manager	cn=replication manager, cn=replication, cn=config
Replication Manager Password	11111111
Instance Directory	/var/opt/mps/serverroot/slapd-fm-users

TABLE A-3 User Data Store Accounts

UserID	Description
spuser	Used for testing Federation Manager login.
	Password                  spuser
	DN                          uid=spuser,o=siroeusers,dc=siroe,dc=com
idpuser	Used for testing single sign-on configuration and Web Policy Agents configuration.
	Password                  idpuser
	DN                          uid=idpuser,o=siroeusers,dc=siroe,dc=com
testuser1	Used to verify fm-users data store configuration.
	Password                  11111111
	DN                          uid=testuser1,o=siroeusers,dc=siroe,dc=com
idp	Used to verify that the configuration of Application Server sample application with J2EE Policy Agents.
	Password                  idp
	DN                          uid=idp,o=siroeusers,dc=siroe,dc=com





# Federation Manager Servers

---

TABLE B-1 Federation Manager 1 Configuration

Component	Description
Host	Computer system that hosts the Federation Manager 1 server.
	Host Name                  FederationManager-1.siroe.com
Web Server Administration	Manages the entire Web Server an all its instances.
	Instance name              admserv
	Port Number                8888
	Service URL                http://FederationManager-1.siroe.com:8888
	Administrative User        admin
	Administrative User Password    11111111
	Instance Directory        /opt/SUNWwbsvr/https-admserv
Federation Manager Web Server	Contains the Federation Manager applications.
	Instance name              FedeartionManager-1.siroe.com
	Port Number                8080
	Service URL                http://FederationManager-1.siroe.com:1080
	Administrative User        amadmin
	Administrative User Password    11111111
	Instance Directory        /opt/SUNWwbsvr/https-FederationManager-1.siroe.com

TABLE B-2 Federation Manager 2 Configuration

Component	Description
Host	Computer system that hosts the Federation Manager 2 server.
	Host Name                      FederationManager-2.siroe.com
Web Server Administration	Manages the entire Web Server and all its instances.
	Instance name                  admserv
	Port Number                    8888
	Service URL                    http://FederationManager-2.siroe.com:8888
	Administrative User          admin
	Administrative User Password                      11111111
	Instance Directory            /opt/SUNWwbsvr/https-admserv
Federation Manager Web Server	Contains the Federation Manager applications.
	Instance name                  FedartionManager-2.siroe.com
	Port Number                    8080
	Service URL                    http://FederationManager-2.siroe.com:1080
	Administrative User          amadmin
	Administrative User Password                      11111111
	Instance Directory            /opt/SUNWwbsvr/https-FederationManager-2.siroe.com

# Sun Java System Application Servers and J2EE Policy Agents

---

**TABLE C-1** Protected Resource 3 Application Server and J2EE Policy Agent 3 Configurations

Component	Description
Host	Computer system that hosts Application Server 3
	Host Name                      ProtectedResource-3.siroe.com
Application Server Administration	Manages the entire Application Server and all its instances
	Instance Name                  AdminServer
	Port Number                      8080
	Administrative User            admin
	Administrative User Password    11111111
	Instance Directory            /opt/SUNWappserver/ ProtectedResource-3
Application Server	Stores configuration information for this Application Server instance.
	Instance Name                  ProtectedResource-3
	Instance Directory            /opt/SUNWappserver/ ProtectedResource-3
J2EE Policy Agent Instance	Server instance which contains the Application Server and J2EE policy agent.
	Instance Name                  ProtectedResource-3
	Port Number                      8080

**TABLE C-1** Protected Resource 3 Application Server and J2EE Policy Agent 3 Configurations  
(Continued)

Component	Description
	Instance Directory     /export/j2ee_agents/ am_as81_agent/agent_001
J2EE Policy Agent Profile	
	Administrative User     asagent
	Administrative User Password     This encrypted password is generated using ampassword.

**TABLE C-2** Protected Resource 4 Application Server and J2EE Policy Agent 4 Configurations

Component	Description
Host	Computer system that hosts Application Server 4
	Host Name                 ProtectedResource-4.siroe.com
Application Server Administration	Manages the entire Application Server and all its instances
	Instance Name             AdminServer
	Port Number                8080
	Administrative User        admin
	Administrative User Password     11111111
	Instance Directory        /opt/SUNWappserver/ ProtectedResource-4
Application Server	Stores configuration information for this Application Server instance.
	Instance Name             ProtectedResource-4
	Instance Directory        /opt/SUNWappserver/ ProtectedResource-4
J2EE Policy Agent Instance	Server instance which contains the Application Server and J2EE policy agent.
	Instance Name             ProtectedResource-4
	Port Number                8080
	Instance Directory        /export/j2ee_agents/ am_as81_agent/agent_001

**TABLE C-2** Protected Resource 4 Application Server and J2EE Policy Agent 4 Configurations  
(Continued)

Component	Description
J2EE Policy Agent Profile	
	Administrative User asagent
	Administrative User Password This encrypted password is generated using ampassword.



# Sun Java System Web Servers and Web Policy Agents

---

TABLE D-1 Protected Resource 3 Web Server and Web Policy Agent 3 Configurations

Component	Description
Host	Computer system that hosts Web Server 3
	Host Name            ProtectedResource-3.siroe.com
Web Server Administration	Manages the entire Web Server and all its instances.
	Instance Name        admserv
	Port Number           8888
	Administrative User   admin
	Administrative User Password   web4admin
	Instance Directory   /opt/SUNWwbsvr/https-admserv
Web Policy Agent Instance	Server instance that contains the web server and web policy agent.
	Instance Name        ProtectedResource-3.siroe.com
	Port Number           2080
	Instance Directory   /opt/SUNWwbsvr/ https-ProtectedResource-3.siroe.com
Web Agent Profile	
	Administrative User   webagent
	Administrative User Password   web4gent

TABLE D-2 Protected Resource 4 Web Server and Web Policy Agent 4 Configurations

Component	Description
Host	Computer system that hosts Web Server 4
	Host Name            ProtectedResource-4.siroe.com
Web Server Administration	Manages the entire Web Server and all its instances.
	Instance Name        admserv
	Port Number           8888
	Administrative User   admin
	Administrative User Password   web4admin
	Instance Directory    /opt/SUNWwbsvr/https-admserv
Web Policy Agent Instance	Server instance that contains the web server and web policy agent.
	Instance Name        ProtectedResource-4.siroe.com
	Port Number           2080
	Instance Directory    /opt/SUNWwbsvr/ https-ProtectedResource-4.siroe.com
Web Agent Profile	
	Administrative User   webagent
	Administrative User Password   web4gent



# Load Balancers

---

TABLE E-1 Load Balancer Configurations

Component	Description
Host	Computer system that hosts all virtual servers in this deployment example.  Host Name            is-f5.siroe.com
Load Balancer 1 Load Balancer 2	These load balancers are not discussed in this manual. See <a href="#">“1.2 System Architecture” on page 22</a> and <a href="#">“1.2 System Architecture” on page 22</a> for more information.
Load Balancer 3 Access Manager Servers	Virtual Service Address for the Access Manager Web Server instances.  SSL is terminated at this at this load balancer before the request is forwarded to the Access Manager Servers. This load-balancer is the single point-of-failure for Access Manager and can be considered a limitation of this deployment example.  Configured for cookie and IP— based stickiness and TCP (HTTP and LDAP) load balancing.  External users access port 9443, while internal users will access port 90.  Instance Name        LoadBalancer-3 Port Number            90 and 9443 Pool Name                AccessManager-Pool Virtual Server and Port Number    LoadBalancer-3.example.com:90 Monitor                    HTTP

TABLE E-1 Load Balancer Configurations (Continued)

Component	Description	
Load Balancer 4	These load balancers are not discussed in this manual. See “1.2 System Architecture” on page 22 and “1.2 System Architecture” on page 22 for more information.	
Load Balancer 5		
Load Balancer 6		
Load Balancer 7	Virtual Service Address for the Federation Manager configuration store.	
Federation Manager Configuration Stores	Configured for cookie and IP-based stickiness and TCP (HTTP and LDAP) load balancing.	
	Instance Name	LoadBalancer-7
	Port Number	389
	Pool Name	federation_ds_pool
	Virtual Server and Port Number	LoadBalancer-7.siroe.com:389
	Monitor	LDAP-tcp
Load Balancer 8	Virtual Service Address for the Federation Manager User Data store.	
Federation Manager User Data Stores	Configured for cookie and IP-based stickiness and TCP (HTTP and LDAP) load balancing.	
	Instance Name	LoadBalancer-8
	Port Number	1389
	Pool Name	DirectoryServer-UserData-Pool
	Virtual Server and Port Number	LoadBalancer-8.siroe.com:1389
	Monitor	LDAP-tcp
Load Balancer 9	Virtual Service Address for the Federation Manager Web Server instances.	
Federation Manager Web Servers	SSL is terminated at this load balancer before the request is forwarded to the Access Manager servers.	
	Configured for cookie and IP-based stickiness and TCP (HTTP and LDAP) load balancing.	
	External users will access port 3443, while non-SSL port 1080 is used for proxying.	
	Instance Name	LoadBalancer-9
	Port Number	1080
	Pool Name	fm_server_pool

TABLE E-1 Load Balancer Configurations (Continued)

Component	Description
	Virtual Server and Port Number LoadBalancer-9.siroe.com:1080
	Monitor HTTP
Load Balancer 10	Virtual Service Address for J2EE Policy Agents
J2EE Policy Agents	SSL is terminated at this load balancer before the request is forwarded to J2EE Policy Agents.  Configured for cookie and IP-based stickiness and TCP (HTTP and LDAP) load balancing.
	Instance Name LoadBalancer-10
	Port Number 4080
	Pool Name federation_j2ee_agents
	Virtual Server and Port Number LoadBalancer-10.siroe.com:1080 LoadBalancer-10.siroe.com:2443
	Monitor HTTP
Load Balancer 11	Virtual Service Address for Web Policy Agents.
Web Policy Agents	SSL is terminated at this load balancer before the request is forwarded to Web Policy Agents.  Configured for cookie and IP— based stickiness and TCP (HTTP and LDAP) load balancing.
	Instance Name LoadBalancer-11
	Port Number 5080
	Pool Name federation_web_agents
	Virtual Server and Port Number LoadBalancer-11.siroe.com:2080 LoadBalancer-11.siroe.com:5443
	Monitor HTTP



# Keystores and SSL Certificate Chains

---

TABLE F-1 Keystores

Keystore	Description
Identity Provider Keystore	/etc/opt/SUNWam/config/amkeystore
	Keystore Password      passwordam
	Key Password              keypasswordam
	Key Algorithm              RSA
	Strength                    1024
Service Provider Keystore	/etc/opt/SUNWam/config/fmkeystore
	Keystore Password      password
	Key Password              keypassword
	Key Algorithm              RSA
	Strength                    1024

TABLE F-2 Certificate Chains

Root CA	Server	Certificate Type	Certificate ID
OpenSSL	Self	Root CA	OpenSSL_CA_Cert
OpenSSL	LoadBalancer-9.siroe.com	Server SSL	LoadBalancer-9.siroe.com_OpenSSL
OpenSSL	LoadBalancer-10.siroe.com	Server SSL	LoadBalancer-10.siroe.com_OpenSSL
OpenSSL	LoadBalancer-11.siroe.com	Server SSL	LoadBalancer-11.siroe.com_OpenSSL

