

Oracle® WebLogic Server

Securing WebLogic Server

10g Release 3 (10.3)

July 2008

ORACLE®

Oracle WebLogic Server Securing WebLogic Server, 10g Release 3 (10.3)

Copyright © 2007, 2008, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

1. Introduction and Roadmap

Document Scope	1-1
Document Audience	1-1
Guide to This Document	1-2
Related Information	1-4
Security Samples and Tutorials	1-5
Security Examples in the WebLogic Server Distribution	1-5
New and Changed Security Features	1-5

2. Overview of Security Management

Security Realms in WebLogic Server	2-1
Security Providers	2-2
Security Policies and WebLogic Resources	2-4
WebLogic Resources	2-5
Deployment Descriptors and the WebLogic Server Administration Console	2-6
The Default Security Configuration in WebLogic Server	2-7
Configuring WebLogic Security: Main Steps	2-7
Methods of Configuring Security	2-9
What Is Compatibility Security?	2-10
Management Tasks Available in Compatibility Security	2-10

3. Customizing the Default Security Configuration

Why Customize the Default Security Configuration?	3-1
---	-----

Before You Create a New Security Realm	3-2
Creating and Configuring a New Security Realm: Main Steps	3-3

4. Configuring WebLogic Security Providers

When Do You Need to Configure a Security Provider?	4-2
Reordering Security Providers	4-3
Configuring an Authorization Provider	4-3
Configuring the WebLogic Adjudication Provider	4-4
Configuring a Role Mapping Provider	4-4
Configuring the WebLogic Auditing Provider	4-5
Auditing ContextHandler Elements	4-8
Configuration Auditing	4-10
Enabling Configuration Auditing	4-11
Configuration Auditing Messages	4-11
Audit Events and Auditing Providers	4-15
Configuring a WebLogic Credential Mapping Provider	4-16
Configuring a PKI Credential Mapping Provider	4-17
PKI Credential Mapper Attributes	4-18
Credential Actions	4-18
Configuring a SAML Credential Mapping Provider for SAML 1.1	4-19
Configuring Assertion Lifetime	4-19
Relying Party Registry	4-20
Configuring a SAML 2.0 Credential Mapping Provider for SAML 2.0	4-20
SAML 2.0 Credential Mapping Provider Attributes	4-21
Service Provider Partners	4-22
Partner Lookup Strings Required for Web Service Partners	4-23
Management of Partner Certificates	4-26
Java Interface for Configuring Service Provider Partner Attributes	4-26

Configuring the Certificate Lookup and Validation Framework	4-26
CertPath Provider	4-27
Certificate Registry	4-27
Configuring a WebLogic Keystore Provider	4-28

5. Configuring Authentication Providers

Choosing an Authentication Provider	5-2
Using More Than One Authentication Provider	5-3
Setting the JAAS Control Flag Option	5-3
Changing the Order of Authentication Providers	5-4
Configuring the WebLogic Authentication Provider	5-4
Configuring LDAP Authentication Providers	5-5
Requirements for Using an LDAP Authentication Provider	5-6
Configuring an LDAP Authentication Provider: Main Steps	5-6
Accessing Other LDAP Servers	5-7
Dynamic Groups and WebLogic Server	5-7
Configuring Failover for LDAP Authentication Providers	5-8
LDAP Failover Example 1	5-8
LDAP Failover Example 2	5-9
Improving the Performance of WebLogic and LDAP Authentication Providers	5-9
Optimizing the Group Membership Caches	5-10
Configuring Dynamic Groups in the iPlanet Authentication Provider to Improve Performance	5-11
Optimizing the Principal Validator Cache	5-12
Configuring the Active Directory Authentication Provider to Improve Performance	5-12
Configuring RDBMS Authentication Providers	5-13
Common RDBMS Authentication Provider Attributes	5-13

Data Source Attribute	5-14
Group Searching Attributes	5-14
Group Caching Attributes	5-14
Configuring the SQL Authentication Provider	5-14
Password Attributes	5-14
SQL Statement Attributes	5-15
Configuring the Read-Only SQL Authenticator	5-15
Configuring the Custom DBMS Authenticator	5-15
Plug-In Class Attributes	5-16
Configuring a Windows NT Authentication Provider	5-16
Domain Controller Settings	5-16
LogonType Setting	5-17
UPN Names Settings	5-18
Configuring the SAML Authentication Provider	5-18
Configuring the Password Validation Provider	5-19
Password Composition Rules for the Password Validation Provider	5-20
Using the Password Validation Provider with the WebLogic Authentication Provider	5-23
Using WLST to Create and Configure the Password Validation Provider	5-24
Creating an Instance of the Password Validation Provider	5-24
Specifying the Password Composition Rules	5-25
Configuring Identity Assertion Providers	5-25
How an LDAP X509 Identity Assertion Provider Works	5-27
Configuring an LDAP X509 Identity Assertion Provider: Main Steps	5-28
Configuring a Negotiate Identity Assertion Provider	5-29
Configuring a SAML Identity Assertion Provider for SAML 1.1	5-30
Asserting Party Registry	5-31
Certificate Registry	5-31

Configuring a SAML 2.0 Identity Assertion Provider for SAML 2.0	5-31
Identity Provider Partners	5-32
Ordering of Identity Assertion for Servlets	5-37
Configuring Identity Assertion Performance in the Server Cache	5-38
Configuring a User Name Mapper	5-39
Configuring a Custom User Name Mapper	5-40

6. Configuring Single Sign-On with Microsoft Clients

Overview of Single Sign-On with Microsoft Clients	6-1
System Requirements for SSO with Microsoft Clients	6-2
Single Sign-On with Microsoft Clients: Main Steps	6-3
Configuring Your Network Domain to Use Kerberos	6-4
Creating a Kerberos Identification for WebLogic Server	6-5
Configuring Microsoft Clients to Use Windows Integrated Authentication	6-7
Configuring a .NET Web Service	6-7
Configuring an Internet Explorer Browser	6-8
Configure Local Intranet Domains	6-8
Configure Intranet Authentication	6-8
Verify the Proxy Settings	6-9
Set Integrated Authentication for Internet Explorer 6.0	6-9
Creating a JAAS Login File	6-9
Configuring the Identity Assertion Provider	6-11
Using Startup Arguments for Kerberos Authentication with WebLogic Server	6-11
Verifying Configuration of SSO with Microsoft Clients	6-11

7. Configuring Single Sign-On with Web Browsers and HTTP Clients

Configuring SAML 1.1 Services	7-2
---	-----

Enabling Single Sign-on with SAML 1.1: Main Steps	7-2
Configuring a Source Site: Main Steps.	7-2
Configuring a Destination Site: Main Steps	7-2
Configuring a SAML 1.1 Source Site for Single Sign-On	7-3
Configure the SAML 1.1 Credential Mapping Provider	7-3
Configure the Source Site Federation Services	7-3
Configure Relying Parties.	7-4
Replacing the Default Assertion Store	7-5
Configuring a SAML 1.1 Destination Site for Single Sign-On	7-5
Configure SAML Identity Assertion Provider	7-5
Configure Destination Site Federation Services.	7-5
Configuring Asserting Parties.	7-7
Configuring Relying and Asserting Parties with WLST	7-7
Configuring SAML 2.0 Services.	7-9
Configuring SAML 2.0 Services: Main Steps	7-9
Configuring SAML 2.0 General Services	7-11
About SAML 2.0 General Services	7-11
Publishing and Distributing the Metadata File	7-13
Configuring an Identity Provider Site for SAML 2.0 Single Sign-On	7-14
Configure the SAML 2.0 Credential Mapping Provider	7-14
Configure SAML 2.0 Identity Provider Services	7-14
Create and Configure Web Single Sign-On Service Provider Partners	7-15
Configuring a Service Provider Site for SAML 2.0 Single Sign-On.	7-18
Configure the SAML 2.0 Identity Assertion Provider	7-18
Configure the SAML Authentication Provider.	7-19
Configure SAML 2.0 General Services	7-19
Configure SAML 2.0 Service Provider Services	7-19
Create and Configure Web Single Sign-On Identity Provider Partners	7-20

Viewing Partner Site, Certificate, and Service Endpoint Information	7-23
Web Application Deployment Considerations for SAML 2.0	7-24
Deployment Descriptor Recommendations	7-24
Login Application Considerations for Clustered Environments	7-25

8. Migrating Security Data

Overview of Security Data Migration	8-1
Migration Concepts	8-2
Formats and Constraints Supported by WebLogic Security Providers	8-3
Migrating Data with WLST	8-6
Migrating Data Using weblogic.admin	8-6

9. Managing the Embedded LDAP Server

Configuring the Embedded LDAP Server	9-1
Embedded LDAP Server Replication	9-2
Viewing the Contents of the Embedded LDAP Server from an LDAP Browser	9-3
Exporting and Importing Information in the Embedded LDAP Server	9-4
LDAP Access Control Syntax	9-6
The Access Control File	9-6
Access Control Location	9-7
Access Control Scope	9-7
Access Rights	9-7
Attribute Permissions	9-8
Entry Permissions	9-9
Attributes Types	9-11
Subject Types	9-11
Grant/Deny Evaluation Rules	9-12

10.Managing the RDBMS Security Store

Security Providers that Use the RDBMS Security Store	10-2
Configuring the RDBMS Security Store.	10-3
Create a Domain with the RDBMS Security Store	10-3
Specifying Database Connection Properties.	10-4
Testing the Database Connection	10-6
Create RDBMS Tables in the Security Datastore	10-7
Configure a JMS Topic for the RDBMS Security Store	10-8
Configuring JMS Connection Recovery in the Event of Failure	10-10
Upgrading a Domain to Use the RDBMS Security Store	10-11

11.Configuring Identity and Trust

Private Keys, Digital Certificates, and Trusted Certificate Authorities	11-1
Configuring Identity and Trust: Main Steps	11-2
Supported Formats for Identity and Trust	11-3
Obtaining Private Keys, Digital Certificates, and Trusted Certificate Authorities	11-4
Common Keytool Commands	11-5
Using the CertGen Utility	11-6
Using Your Own Certificate Authority	11-7
Converting a Microsoft p7b Format to PEM Format.	11-8
Obtaining a Digital Certificate for a Web Browser	11-9
Using Certificate Chains (Deprecated)	11-9
Storing Private Keys, Digital Certificates, and Trusted Certificate Authorities	11-11
Guidelines for Using Keystores	11-11
Creating a Keystore and Loading Private Keys and Trusted Certificate Authorities into the Keystore	11-12
Configuring Demo Certificates for Clients	11-13
How WebLogic Server Locates Trust.	11-13

Configuring Keystores for Production.	11-13
---	-------

12. Configuring SSL

SSL: An Introduction.	12-2
One-Way and Two-Way SSL	12-2
Setting Up SSL: Main Steps	12-2
Using Host Name Verification	12-3
Enabling SSL Debugging	12-4
SSL Session Behavior	12-5
Configuring RMI over IIOP with SSL	12-6
SSL Certificate Validation.	12-7
Controlling the Level of Certificate Validation	12-7
Accepting Certificate Policies in Certificates.	12-8
Checking Certificate Chains.	12-9
Using Certificate Lookup and Validation Providers.	12-10
How SSL Certificate Validation Works in WebLogic Server.	12-10
Troubleshooting Problems with Certificate Validation	12-11
Using the nCipher JCE Provider with WebLogic Server	12-12
Specifying the Version of the SSL Protocol	12-14

13. Configuring Security for a WebLogic Domain

Important Information Regarding Cross-Domain Security Support	13-1
Enabling Trust Between WebLogic Server Domains	13-2
Enabling Cross Domain Security Between WebLogic Server Domains	13-2
Configuring Cross-Domain Security.	13-3
Configuring a Cross-Domain User	13-3
Configure a Credential Mapping for Cross-Domain Security	13-4
Enabling Global Trust	13-5

Using Connection Filters	13-6
Using the Java Authorization Contract for Containers	13-8
Viewing MBean Attributes	13-8
How Passwords Are Protected in WebLogic Server.	13-8
Protecting User Accounts	13-9

14.Using Compatibility Security

Running Compatibility Security: Main Steps	14-2
Limited Visibility of Compatibility Security MBeans	14-2
The Default Security Configuration in the CompatibilityRealm	14-3
Configuring a Realm Adapter Authentication Provider	14-4
Configuring the Identity Assertion Provider in the Realm Adapter Authentication Provider 14-5	
Configuring a Realm Adapter Auditing Provider	14-5
Protecting User Accounts in Compatibility Security	14-5
Accessing 6.x Security from Compatibility Security	14-6

15.Security Configuration MBeans

SSLMBean	15-1
ServerMBean.	15-2
EmbeddedLDAPMBean	15-2
SecurityMBean	15-2
SecurityConfigurationMBean	15-3
RealmMBean.	15-3
WindowsNTAuthenticatorMBean	15-3
CustomDBMSAuthenticatorMBean	15-3
ReadOnlySQLAuthenticatorMBean	15-4
SQLAuthenticatorMBean	15-4
DefaultAuditorMBean.	15-4

Compatibility Security MBeans	15-4
UserLockoutManagerMBean	15-5
Other Security Provider MBeans.....	15-5

Introduction and Roadmap

The following sections describe the contents and organization of this guide, *Securing WebLogic Server*, as well as new and changed security features in this release.

- “Document Scope” on page 1-1
- “Document Audience” on page 1-1
- “Guide to This Document” on page 1-2
- “Related Information” on page 1-4
- “Security Samples and Tutorials” on page 1-5
- “New and Changed Security Features” on page 1-5

Document Scope

This document explains how to configure WebLogic Server® security, including settings for security realms, providers, identity and trust, SSL, and Compatibility security. See [Related Information](#) for a description of other WebLogic security documentation.

Document Audience

This document is intended for the following audiences:

- Application Architects—Architects who, in addition to setting security goals and designing the overall security architecture for their organizations, evaluate WebLogic Server security

features and determine how to best implement them. Application Architects have in-depth knowledge of Java programming, Java security, and network security, as well as knowledge of security systems and leading-edge, security technologies and tools.

- **Security Developers**—Developers who define the system architecture and infrastructure for security products that integrate with WebLogic Server and who develop custom security providers for use with WebLogic Server. They work with Application Architects to ensure that the security architecture is implemented according to design and that no security holes are introduced, and work with Server Administrators to ensure that security is properly configured. Security Developers have a solid understanding of security concepts, including authentication, authorization, auditing (AAA), in-depth knowledge of Java (including Java Management eXtensions (JMX)), and working knowledge of WebLogic Server and security provider functionality.
- **Application Developers**—Java programmers who focus on developing client applications, adding security to Web applications and Enterprise JavaBeans (EJBs), and working with other engineering, quality assurance (QA), and database teams to implement security features. Application Developers have in-depth/working knowledge of Java (including J2EE components such as servlets/JSPs and JSEE) and Java security.
- **Server Administrators**—Administrators work closely with Application Architects to design a security scheme for the server and the applications running on the server; to identify potential security risks; and to propose configurations that prevent security problems. Related responsibilities may include maintaining critical production systems; configuring and managing security realms, implementing authentication and authorization schemes for server and application resources; upgrading security features; and maintaining security provider databases. Server Administrators have in-depth knowledge of the Java security architecture, including Web services, Web application and EJB security, Public Key security, SSL, and Security Assertion Markup Language (SAML).
- **Application Administrators**—Administrators who work with Server Administrators to implement and maintain security configurations and authentication and authorization schemes, and to set up and maintain access to deployed application resources in defined security realms. Application Administrators have general knowledge of security concepts and the Java Security architecture. They understand Java, XML, deployment descriptors, and can identify security events in server and audit logs.

Guide to This Document

This document is organized as follows:

- This chapter describes the audience, organization, and related information for this guide.

- [Chapter 2, “Overview of Security Management,”](#) describes the default security configuration in WebLogic Server; lists the configuration steps for security, and describes Compatibility security.
- [Chapter 3, “Customizing the Default Security Configuration,”](#) explains when to customize the default security configuration, the configuration requirements for a new security realm, and how to set a security realm as the default security realm.
- [Chapter 4, “Configuring WebLogic Security Providers,”](#) describes the available configuration options for the security providers supplied by WebLogic Server and how to configure a custom security provider.
- [Chapter 5, “Configuring Authentication Providers,”](#) describes the Authentication providers supplied by WebLogic Server, including information about how to configure them.
- [Chapter 6, “Configuring Single Sign-On with Microsoft Clients,”](#) describes how to configure authentication between a WebLogic Server domain and .NET Web Service clients or browser clients (for example, Internet Explorer) in a Microsoft domain, using Windows authentication based on the Simple and Protected Negotiate (SPNEGO) mechanism.
- [Chapter 7, “Configuring Single Sign-On with Web Browsers and HTTP Clients,”](#) describes how to configure authentication between a WebLogic Server domain and Web browsers or other HTTP clients, using authentication based on the Security Assertion Markup Language (SAML).
- [Chapter 8, “Migrating Security Data,”](#) provides information about exporting and importing security data between security realms and security providers.
- [Chapter 9, “Managing the Embedded LDAP Server,”](#) describes the management tasks associated with the embedded LDAP server used by the WebLogic security providers.
- [Chapter 10, “Managing the RDBMS Security Store,”](#) describes the steps required to configure the RDBMS security store, which enables you to store the security data managed by several security providers in an external RDBMS system rather than in the embedded LDAP server. The use of the RDBMS security store is required for SAML 2.0 services when configured on multiple servers in a domain, such as in a cluster.
- [Chapter 11, “Configuring Identity and Trust,”](#) describes how to configure identity and trust for WebLogic Server.
- [Chapter 12, “Configuring SSL,”](#) describes how to configure SSL for WebLogic Server.

- [Chapter 13, “Configuring Security for a WebLogic Domain,”](#) describes how to set security configuration options for a WebLogic Server domain.
- [Chapter 14, “Using Compatibility Security,”](#) describes how to use Compatibility security, a security configuration mode designed for backwards compatibility with security realms developed under WebLogic Server 6.x.
- [Chapter 15, “Security Configuration MBeans,”](#) describes which WebLogic Security MBeans and MBean attributes are dynamic (can be changed without restarting the server) and which are non-dynamic (changes require a server restart).

Related Information

The following Oracle WebLogic Server documents contain information that is relevant to the WebLogic Security Service:

- [Understanding WebLogic Security](#)—Summarizes the features of the WebLogic Security Service, including an overview of its architecture and capabilities. It is the starting point for understanding WebLogic security.
- [Developing Security Providers for WebLogic Server](#)—Provides security vendors and application developers with the information needed to develop custom security providers that can be used with WebLogic Server.
- [Securing a Production Environment](#)—Highlights essential security measures for you to consider before you deploy WebLogic Server in a production environment.
- [Securing WebLogic Resources Using Roles and Policies](#)—Introduces the various types of WebLogic resources, and provides information about how to secure these resources using WebLogic Server. This document focuses primarily on securing URL (Web) and Enterprise JavaBean (EJB) resources.
- [Programming WebLogic Security](#)—Describes how to develop secure Web applications.
- [WebLogic Web Services: Security](#)—Describes how to develop and configure secure Web Services.
- [Administration Console Online Help](#)—Many security configuration tasks can be performed using the WebLogic Administration Console. The console’s online help describes configuration procedures and provides a reference for configurable attributes.
- [Upgrading WebLogic Application Environments](#)—Provides procedures and other information you need to upgrade from earlier versions of WebLogic Server to this release. It also provides information about moving applications from an earlier version of

WebLogic Server to this release. For specific information on upgrading WebLogic Server security, see *Upgrading a Security Provider* in *Upgrading WebLogic Application Environments*.

- *Javadocs for WebLogic Classes*—Provides reference documentation for the WebLogic security packages that are provided with and supported by this release of WebLogic Server.

Security Samples and Tutorials

In addition to the documents listed in [Related Information](#), Oracle provides a variety of code samples for developers, some packaged with WebLogic Server and others available at the Oracle Technology Network (OTN) at

<http://www.oracle.com/technology/community/welcome-bea/index.html>.

Security Examples in the WebLogic Server Distribution

WebLogic Server optionally installs API code examples in

`WL_HOME\samples\server\examples\src\examples\security`, where `WL_HOME` is the top-level directory of your WebLogic Server installation. You can start the examples server, and obtain information about the samples and how to run them from the WebLogic Server Start menu.

The following examples illustrate WebLogic security features:

- Java Authentication and Authorization Service
- Outbound and Two-way SSL

New and Changed Security Features

For a comprehensive listing of the new WebLogic Server features introduced in this release, see “[What’s New in WebLogic Server](#)” in *Release Notes*.

Introduction and Roadmap

Overview of Security Management

The following sections provide an overview of the security system for WebLogic Server. For a broader overview, see *Understanding WebLogic Security*.

- “Security Realms in WebLogic Server” on page 2-1
- “Security Providers” on page 2-2
- “Security Policies and WebLogic Resources” on page 2-4
- “The Default Security Configuration in WebLogic Server” on page 2-7
- “Configuring WebLogic Security: Main Steps” on page 2-7
- “Methods of Configuring Security” on page 2-9
- “What Is Compatibility Security?” on page 2-10
- “Management Tasks Available in Compatibility Security” on page 2-10

Note: Throughout this document, the term *6.x* refers to WebLogic Server 6.0 and 6.1 and their associated service packs.

Security Realms in WebLogic Server

The security service in WebLogic Server simplifies the configuration and management of security while offering robust capabilities for securing your WebLogic Server deployment. Security realms act as a scoping mechanism. Each security realm consists of a set of configured security providers, users, groups, security roles, and security policies. You can configure multiple

security realms in a domain; however, only one can be the active security realm. WebLogic Server provides two default security realms:

- `myrealm`—Has the WebLogic Adjudication, Authentication, Identity Assertion, Authorization, Role Mapping, and Credential Mapping providers configured by default.
- `CompatibilityRealm`—Provides backward compatibility for 6.x security configurations. You can access an existing 6.x security configuration through the `CompatibilityRealm`.

You can customize authentication and authorization functions by configuring a new security realm to provide the security services you want and then set the new security realm as the default security realm.

For information about the default security configuration in WebLogic Server, see [“The Default Security Configuration in WebLogic Server” on page 2-7](#)

For information about configuring a security realm and setting it as the default security realm, see [Chapter 3, “Customizing the Default Security Configuration.”](#)

For information about Compatibility security, see [Chapter 14, “Using Compatibility Security.”](#)

Security Providers

Security providers are modular components that handle specific aspects of security, such as authentication and authorization. Although applications can leverage the services offered by the default WebLogic security providers, the WebLogic Security Service’s flexible infrastructure also allows security vendors to write their own custom security providers for use with WebLogic Server. WebLogic security providers and custom security providers can be mixed and matched to create unique security solutions, allowing organizations to take advantage of new technology advances in some areas while retaining proven methods in others. The WebLogic Administration Console allows you to administer and manage all your security providers through one unified management interface.

The WebLogic Security Service supports the following types of security providers:

- **Authentication**—Authentication is the process whereby the identity of users or system processes are proved or verified. Authentication also involves remembering, transporting, and making identity information available to various components of a system when that information is needed. Authentication providers supported by the WebLogic Security Service supply the following types of authentication:
 - Username and password authentication
 - Certificate-based authentication directly with WebLogic Server

- HTTP certificate-based authentication proxied through an external Web server
- **Identity Assertion**—An Authentication provider that performs perimeter authentication—a special type of authentication using tokens—is called an Identity Assertion provider. Identity assertion involves establishing a client's identity through the use of client-supplied tokens that may exist outside of the request. Thus, the function of an Identity Assertion provider is to validate and map a token to a username. Once this mapping is complete, an Authentication provider's LoginModule can be used to convert the username to a principal (an authenticated user, group, or system process).
- **Authorization**—Authorization is the process whereby the interactions between users and WebLogic resources are limited to ensure integrity, confidentiality, and availability. In other words, once a user's identity has been established by an authentication provider, authorization is responsible for determining whether access to WebLogic resources should be permitted for that user. An Authorization provider supplies these services.
- **Role Mapping**—You can assign one or more roles to multiple users and then specify access rights for users who hold particular roles. A Role Mapping provider obtains a computed set of roles granted to a requestor for a given resource. Role Mapping providers supply Authorization providers with this information so that the Authorization provider can answer the “is access allowed?” question for WebLogic resources that use role-based security (for example, Web applications and Enterprise JavaBeans (EJBs)).
- **Adjudication**—When multiple Authorization providers are configured in a security realm, each may return a different answer to the “is access allowed” question for a given resource. Determining what to do if multiple Authorization providers do not agree is the primary function of an Adjudication provider. Adjudication providers resolve authorization conflicts by weighing each Authorization provider's answer and returning a final access decision.
- **Credential Mapping**—A credential map is a mapping of credentials used by WebLogic Server to credentials used in a legacy or remote system, which tell WebLogic Server how to connect to a given resource in that system. In other words, credential maps allow WebLogic Server to log into a remote system on behalf of a subject that has already been authenticated. Credential Mapping providers map credentials in this way.
- **Keystore**—A keystore is a mechanism for creating and managing password-protected stores of private keys and certificates for trusted certificate authorities. The keystore is available to applications that may need it for authentication or signing purposes. In the WebLogic Server security architecture, the WebLogic Keystore provider is used to access keystores.

Note: The WebLogic Server Keystore provider is deprecated and is only supported for backward compatibility. Use keystores instead. For more information about configuring keystores, see [“Configuring Keystores for Production” on page 11-13](#).

- **Certificate Lookup and Validation (CLV)**—X.509 certificates need to be located and validated for purposes of identity and trust. CLV providers receive certificates, certificate chains, or certificate references, complete the certificate path (if necessary), and validate all the certificates in the path. There are two types of CLV providers:
 - A CertPath Builder looks up and optionally completes the certificate path and validates the certificates.
 - A CertPath Validator looks up and optionally completes the certificate path, validates the certificates, and performs extra validation (for example, revocation checking).
- **Certificate Registry**—A certificate registry is a mechanism for adding certificate revocation checking to a security realm. The registry stores a list of valid certificates. Only registered certificates are valid. A certificate is revoked by removing it from the certificate registry. The registry is stored in the embedded LDAP server. The Certificate Registry is both a CertPath Builder and a CertPath Validator.
- **Auditing**—Auditing is the process whereby information about security requests and the outcome of those security requests is collected, stored, and distributed for the purpose of non-repudiation. In other words, auditing provides an electronic trail of computer activity. An Auditing provider supplies these services.

For information about the functionality provided by the WebLogic security providers, see [Chapter 4, “Configuring WebLogic Security Providers”](#) and [Chapter 5, “Configuring Authentication Providers.”](#)

For information about the default security configuration, see [“The Default Security Configuration in WebLogic Server” on page 2-7](#).

For information about writing custom security providers, see [Developing Security Providers for WebLogic Server](#).

Security Policies and WebLogic Resources

WebLogic Server uses security policies (which replace the ACLs and permissions used in WebLogic Server 6.x) to protect WebLogic resources. Security policies answer the question “who has access” to a WebLogic resource. A security policy is created when you define an association between a WebLogic resource and a user, group, or security role. You can also

optionally associate a time constraint with a security policy. A WebLogic resource has no protection until you assign it a security policy.

Creating security policies is a multi-step process with many options. To fully understand this process, read *Securing WebLogic Resources Using Roles and Policies*. That document should be used in conjunction with *Securing WebLogic Security* to ensure security is completely configured for a WebLogic Server deployment.

WebLogic Resources

A WebLogic resource is a structured object used to represent an underlying WebLogic Server entity, which can be protected from unauthorized access. WebLogic Server defines the following resources:

- Administrative resources such as the WebLogic Server Administration Console and WebLogic Scripting Tool.
- Application resources that represent Enterprise applications. This type of resource includes individual EAR (Enterprise Application aRchive) files and individual components, such as EJB JAR files contained within the EAR.
- Component Object Model (COM) resources that are designed as program component objects according to Microsoft's framework. This type of resource includes COM components accessed through the Oracle bidirectional COM-Java (jCOM) bridging tool.
- Enterprise Information System (EIS) resources that are designed as resource adapters, which allow the integration of Java applications with existing enterprise information systems. These resource adapters are also known as connectors.
- Enterprise JavaBean (EJB) resources including EJB JAR files, individual EJBs within an EJB JAR, and individual methods on an EJB.
- Java DataBase Connectivity (JDBC) resources including groups of connection pools, individual connection pools, and multipools.
- Java Naming and Directory Interface (JNDI) resources.
- Java Messaging Service (JMS) resources.
- Server resources related to WebLogic Server instances, or servers. This type of resource includes operations that start, shut down, lock, or unlock servers.

- URL resources related to Web applications. This type of resource can be a Web Application Archive (WAR) file or individual components of a Web application (such as servlets and JSPs).

Note: Web resources are deprecated. Use the URL resource instead.

- Web Services resources related to services that can be shared by and used as components of distributed, Web-based applications. This type of resource can be an entire Web service or individual components of a Web service (such as a stateless session EJB, particular methods in that EJB, the Web application that contains the `web-services.xml` file, and so on).
- Remote resources.

Deployment Descriptors and the WebLogic Server Administration Console

WebLogic Server offers a choice of models for configuring security roles and policies. Under the standard Java Enterprise Edition model, you define role mappings and policies in the Web application or EJB deployment descriptors. The WebLogic Security Service can use information defined in deployment descriptors to grant security roles and define security policies for Web applications and EJBs. When WebLogic Server is booted for the first time, security role and security policy information stored in `web.xml`, `weblogic.xml`, `ejb-jar.xml`, or `weblogic-ejb-jar.xml` deployment descriptors is loaded into the Authorization and Role Mapping providers configured in the default security realm. You can then make changes to the information through the Administration Console.

To use information in deployment descriptors, at least one Authorization and Role Mapping provider in the security realm must implement the `DeployableAuthorizationProvider` and `DeployableRoleProvider` Security Service Provider Interface (SSPI). This SSPI allows the providers to store (rather than retrieve) information from deployment descriptors. By default, the WebLogic Authorization and Role Mapping providers implement this SSPI.

If you change security role and security policy in deployment descriptors through the Administration Console and want to continue to modify this information through the Administration Console, you can set configuration options on the security realm to ensure changes made through the Console are not overwritten by old information in the deployment descriptors when WebLogic Server is rebooted.

For more information, see [Options for Securing Web Application and EJB Resources](#) in *Securing WebLogic Resources Using Roles and Policies*.

The Default Security Configuration in WebLogic Server

To simplify the configuration and management of security, WebLogic Server provides a default security configuration. In the default security configuration, `myrealm` is set as the default security realm and the WebLogic Adjudication, Authentication, Identity Assertion, XACML Authorization, Credential Mapping, XACML Role Mapping, and CertPath providers are defined as the security providers. WebLogic Server's embedded LDAP server is used as the data store for these default security providers. To use the default security configuration, you need to define users, groups, and security roles for the security realm, and create security policies to protect the WebLogic resources in the domain.

Note: WebLogic Server includes the WebLogic Authorization provider, which is referred to in the Administration Console and elsewhere as the Default Authorizer, and the WebLogic Role Mapping provider, which is referred to in the Administration Console and elsewhere as the Default RoleMapper. Beginning with WebLogic Server 9.1, these providers are no longer the default providers in newly-created security realms. Instead, the XACML Authorization provider and the XACML Role Mapping provider are the default providers.

For a description of the functionality provided by the WebLogic Security providers, see [Understanding WebLogic Security](#). If the WebLogic security providers do not fully meet your security requirements, you can supplement or replace them. See [Developing Security Providers for WebLogic Server](#).

If the default security configuration does not meet your requirements, you can create a new security realm with any combination of WebLogic and custom security providers and then set the new security realm as the default security realm. See [Chapter 3, "Customizing the Default Security Configuration."](#)

Configuring WebLogic Security: Main Steps

Because WebLogic Server's security features are closely related, it is difficult to determine where to start when configuring security. In fact, configuring security for your WebLogic Server deployment may be an iterative process. Although more than one sequence of steps may work, Oracle recommends the following procedure:

1. Determine whether or not to use the default security configuration by reading ["Why Customize the Default Security Configuration?"](#) on page 3-1.
 - If you are using the default security configuration, begin at step 3.
 - If you are not using the default security configuration, begin at step 2.

2. Configure additional security providers (for example, configure an LDAP Authentication provider instead of using the WebLogic Authentication provider) or configure custom security providers in the default security realm. This step is optional. By default, WebLogic Server configures the WebLogic security providers in the default security realm (`myrealm`). For information about the circumstances that require you to customize the default security configuration, see [“Why Customize the Default Security Configuration?”](#) on page 3-1. For information about creating custom security providers, see [Developing Security Providers for WebLogic Server](#).

Note: You can also create a new security realm, configure security providers (either WebLogic or custom) in the security realm and set the new security realm as the default security realm. See [Chapter 3, “Customizing the Default Security Configuration.”](#)

3. Optionally, configure the embedded LDAP server. WebLogic Server’s embedded LDAP server is configured with default options. However, you may want to change those options to optimize the use of the embedded LDAP server in your environment. See [Chapter 9, “Managing the Embedded LDAP Server.”](#)
4. Ensure that user accounts are properly secured. WebLogic Server provides a set of configuration options for protecting user accounts. By default, they are set for maximum security. However, during the development and deployment of WebLogic Server, you may need to weaken the restrictions on user accounts. Before moving to production, check that the options on user accounts are set for maximum protection. If you are creating a new security realm, you need to set the user lockout options. See [“How Passwords Are Protected in WebLogic Server”](#) on page 13-8 and [“Protecting User Accounts”](#) on page 13-9.
5. Protect WebLogic resources with security policies. Creating security policies is a multi-step process with many options. To fully understand this process, read [Securing WebLogic Resources Using Roles and Policies](#). This document should be used in conjunction with [Securing WebLogic Resources Using Roles and Policies](#) to ensure security is completely configured for a WebLogic Server deployment.
6. Configure identity and trust for WebLogic Server. (This step is optional but recommended.) See [Chapter 11, “Configuring Identity and Trust.”](#)
7. Enable SSL for WebLogic Server. (This step is optional but recommended.) See [Chapter 12, “Configuring SSL.”](#)
8. When you have moved to production, review and implement the additional security options described in [Securing a Production Environment](#).

In addition, you can:

- Configure a connection filter. See [“Using Connection Filters” on page 13-6](#).
- Enable interoperability between WebLogic domains. See [“Enabling Cross Domain Security Between WebLogic Server Domains” on page 13-2](#).

Methods of Configuring Security

In many cases, this document describes how to configure WebLogic security by using the WebLogic Server Administration Console. Generally, any configuration task you can accomplish through the Console you can also accomplish by using the WebLogic Scripting Tool or the Java Management Extensions (JMX) APIs. For information about using WLST to manage WebLogic security, see [Managing Security Data](#) in *WebLogic Scripting Tool*. For information about using JMX APIs, see [Choosing an MBean Server to Manage Security Realms](#) in *Developing Custom Management Utilities with JMX*.

When you manage security realms, you must use two different MBean servers depending on your task:

- To set the value of a security MBean attribute, you must use the Edit MBean Server.
- To add users, groups, roles, and policies, or to invoke other operations in a security provider MBean, you must use a Runtime MBean Server or the Domain Runtime MBean Server.

In addition, to prevent the possibility of incompatible changes, you cannot invoke operations in security provider MBeans if your client or another JMX client has an edit session currently active. The Administration Console automatically enforces this limitation and automatically accesses the proper MBean server. When you use the Console, you can override this limitation by enabling Allow Security Management Operations if Non-dynamic Changes have been Made on the Domain → Security → General page. Setting this attribute to true permits users to perform security management operations without restarting the server. Note that this attribute is reset to false when a new MBean edit session begins.

For example, the value of the `MinimumPasswordLength` attribute in `DefaultAuthenticatorMBean` is stored in the domain’s configuration document. Because all modifications to this document are controlled by WebLogic Server, to change the value of this attribute you must use the Edit MBean Server and acquire a lock on the domain’s configuration. The `createUser` operation in `DefaultAuthenticatorMBean` adds data to an LDAP server, which is not controlled by WebLogic Server. To prevent incompatible changes between the `DefaultAuthenticatorMBean`’s configuration and the data that it uses in the LDAP server, you cannot invoke the `createUser` operation if you or other users are in the process of modifying the

`MinimumPasswordLength` attribute. In addition, because changing this attribute requires you to restart WebLogic Server, you cannot invoke the `createUser` operation until you have restarted the server.

What Is Compatibility Security?

Compatibility security refers to the capability to run security configurations developed under WebLogic Server 6.x in this release of WebLogic Server. In Compatibility security, you manage 6.x security realms, users, groups, and ACLs, protect user accounts, and configure the Realm Adapter Auditing provider and optionally the Identity Assertion provider in the Realm Adapter Authentication provider.

The only security realm available in Compatibility security is the `CompatibilityRealm`. The Realm Adapter providers (Auditing, Adjudication, Authorization, and Authentication) in the Compatibility realm allow backward compatibility with the authentication, authorization, and auditing services in 6.x security realms. For more information, see [Chapter 14, “Using Compatibility Security.”](#)

Note: Compatibility security is deprecated and will not be supported in future major releases. Oracle strongly recommends upgrading your WebLogic Server deployment to the security features in this release of WebLogic Server. You should only use Compatibility security pending such an upgrade.

Management Tasks Available in Compatibility Security

Because Compatibility security allows you to access only authentication, authorization, and custom auditing implementations supported in WebLogic Server 6.x, not all 6.x security tasks are allowed in Compatibility security. Use Compatibility security to:

- Configure the Realm Adapter Auditing provider. For more information, see [“Configuring a Realm Adapter Auditing Provider” on page 14-5.](#)
- Configure the Identity Assertion provider in the Realm Adapter Authentication provider so that implementations of the `weblogic.security.acl.CertAuthenticator` class can be used. For more information, see [“Configuring the Identity Assertion Provider in the Realm Adapter Authentication Provider” on page 14-5.](#)

Note: The Realm Adapter Adjudication and Authorization providers are configured by default in the `CompatibilityRealm` using information in an 6.x existing `config.xml` file. These providers can only be used in the `CompatibilityRealm`. The Realm Adapter Authentication provider is also automatically configured in the `CompatibilityRealm`. However, this provider can also be configured in other realms to provide access to users

and groups stored in 6.x security realms. For more information, see [“Configuring RDBMS Authentication Providers” on page 5-13](#).

- Change the password of the `system` user to protect your WebLogic Server deployment.
- Manage the security realm in the `CompatibilityRealm`.
- Define additional users for the security realm in the `CompatibilityRealm`. Organize users further by implementing groups in the security realm.
- Manage ACLs and permissions for the resources in your WebLogic Server deployment.
- Create security roles and security policies for WebLogic resources you add to the `CompatibilityRealm`. For more information, see [Securing WebLogic Resources Using Roles and Policies](#).

You can still configure identity and trust, use SSL, configure connection filters, and enable interoperability between domains; however, you use the security features available in this release of WebLogic Server to perform these tasks. See:

- [Chapter 11, “Configuring Identity and Trust”](#)
- [Chapter 12, “Configuring SSL”](#)
- [Chapter 13, “Configuring Security for a WebLogic Domain”](#)

Overview of Security Management

Customizing the Default Security Configuration

The following sections provide information about customizing the default security configuration by creating a new security realm:

- [“Why Customize the Default Security Configuration?”](#) on page 3-1
- [“Before You Create a New Security Realm”](#) on page 3-2
- [“Creating and Configuring a New Security Realm: Main Steps”](#) on page 3-3

For information about configuring security providers, see [Chapter 4, “Configuring WebLogic Security Providers”](#) and [Chapter 5, “Configuring Authentication Providers.”](#)

For information about migrating security data to a new security realm, see [Chapter 8, “Migrating Security Data.”](#)

Why Customize the Default Security Configuration?

To simplify the configuration and management of security, WebLogic Server provides a default security configuration. In the default security configuration, `myrealm` is set as the default (active) security realm, and the WebLogic Adjudication, Authentication, Identity Assertion, Credential Mapping, CertPath, XACML Authorization and XACML Role Mapping providers are defined as the security providers in the security realm.

Customize the default security configuration if you want to do any of the following:

- Replace one of the security providers in the default realm with a different security provider.

- Configure additional security providers in the default security realm. (For example, if you want to use two Authentication providers, one that uses the embedded LDAP server and one that uses a Windows NT store of users and groups.)
- Use an Authentication provider that accesses an LDAP server other than WebLogic Server's embedded LDAP server.
- Use an existing store of users and groups (for example, a DBMS database) instead of defining users and groups in the WebLogic Authentication provider.
- Add an Auditing provider to the default security realm.
- Use an Identity Assertion provider that handles SAML assertions or Kerberos tokens.
- Use the Certificate Registry to add certificate revocation to the security realm.
- Change the default configuration settings of the security providers.

For information about configuring different types of security providers in a security realm, see [Chapter 4, “Configuring WebLogic Security Providers”](#) and [Chapter 5, “Configuring Authentication Providers.”](#)

The easiest way to customize the default security configuration is to add the security providers you want to the default security realm (`myrealm`). However, Oracle recommends instead that you customize the default security configuration by creating an entirely new security realm. This preserves your ability to revert more easily to the default security configuration. You configure security providers for the new realm; migrate any security data, such as users as groups, from the existing default realm; and then set the new security realm as the default realm. See [“Creating and Configuring a New Security Realm: Main Steps”](#) on page 3-3.

Before You Create a New Security Realm

Before creating a new security realm, you need to decide:

- Which security providers you want to use. WebLogic Server includes a wide variety of security providers and, in addition, allows you to create or obtain custom security providers. A valid security realm requires an Authentication provider, an Authorization provider, an Adjudication provider, a Credential Mapping provider, a Role Mapping provider, and a CertPathBuilder. In addition, a security realm can optionally include Identity Assertion, Auditing, and Certificate Registry providers. If your new security realm includes two or more providers of the same type (for example, more than one Authentication provider or more than one Authorization provider), you need to determine

how these providers should interact with each other. See [“Using More Than One Authentication Provider”](#) on page 5-3.

- What model to use to set security roles and security policies for Web application and EJB resources. These security roles and policies can be set through deployment descriptors or through the WebLogic Administration Console. See [Options for Securing Web Application and EJB Resources](#) in *Securing WebLogic Resources Using Roles and Policies*.
- Whether or not to use the Web resource.

The Web resource is deprecated. If you are configuring a custom Authorization provider that uses the Web resource (instead of the URL resource) in the new security realm, enable Use Deprecated Web Resource on the new security realm. This option changes the runtime behavior of the Servlet container to use a Web resource rather than a URL resource when performing authorization.

Note: When you create a new security realm, you must configure at least one of the Authentication providers to return asserted LoginModules. Otherwise, `run-as` tags defined in deployment descriptors will not work.

For more information, see [Configure new security realms](#) in the *Administration Console Online Help*.

Creating and Configuring a New Security Realm: Main Steps

To create a new security realm:

1. Define a name and set the configuration options for the security realm. See [“Before You Create a New Security Realm”](#) on page 3-2 and [Configure new security realms](#) in the *Administration Console Online Help*.
2. Configure the required security providers for the security realm. A valid security realm requires an Authentication provider, an Authorization provider, an Adjudication provider, a Credential Mapping provider, a Role Mapping provider, and a CertPathBuilder. See [Chapter 4, “Configuring WebLogic Security Providers”](#) and [Chapter 5, “Configuring Authentication Providers.”](#)
3. Optionally, define Identity Assertion, Auditing, and Certificate Registry providers. See [Chapter 4, “Configuring WebLogic Security Providers”](#) and [Chapter 5, “Configuring Authentication Providers.”](#)

4. If you configured the WebLogic Authentication, Authorization, Credential Mapping or Role Mapping provider or the Certificate Registry in the new security realm, verify that the settings of the embedded LDAP server are appropriate. See [Chapter 9, “Managing the Embedded LDAP Server.”](#)
5. Optionally, configure caches to improve the performance of the WebLogic or LDAP Authentication providers in the security realm. See [“Improving the Performance of WebLogic and LDAP Authentication Providers” on page 5-9.](#)
6. Protect WebLogic resources in the new security realm with security policies. Creating security policies is a multi-step process with many options. To fully understand this process, read [Securing WebLogic Resources Using Roles and Policies](#). This document should be used in conjunction with *Securing WebLogic Server* to ensure security is completely configured for a WebLogic Server deployment.
7. If the security data (users and groups, roles and policies, and credential maps) defined in the existing security realm will also be valid in the new security realm, you can export the security data from the existing realm and import it into the new security realm. See [Chapter 8, “Migrating Security Data.”](#)
8. Protect user accounts in the new security realm from dictionary attacks by setting lockout attributes. See [“Protecting User Accounts” on page 13-9.](#)
9. Set the new realm as the default security realm for the WebLogic domain. See [Change the default security realm](#) in the *Administration Console Online Help*.

Note: You can also use the WebLogic Scripting Tool or Java Management Extensions (JMX) APIs to create a new security configuration. See [WebLogic Scripting Tool](#).

Configuring WebLogic Security Providers

The following sections describe how to configure the security providers supplied by WebLogic Server.

Note: WebLogic Server includes so many Authentication providers and Identity Assertion providers that they are better handled in a separate section. See [Chapter 5, “Configuring Authentication Providers.”](#)

- [“When Do You Need to Configure a Security Provider?”](#) on page 4-2
- [“Reordering Security Providers”](#) on page 4-3
- [“Configuring an Authorization Provider”](#) on page 4-3
- [“Configuring the WebLogic Adjudication Provider”](#) on page 4-4
- [“Configuring a Role Mapping Provider”](#) on page 4-4
- [“Configuring the WebLogic Auditing Provider”](#) on page 4-5
- [“Configuring a WebLogic Credential Mapping Provider”](#) on page 4-16
- [“Configuring a PKI Credential Mapping Provider”](#) on page 4-17
- [“Configuring a SAML Credential Mapping Provider for SAML 1.1”](#) on page 4-19
- [“Configuring a SAML 2.0 Credential Mapping Provider for SAML 2.0”](#) on page 4-20
- [“Configuring the Certificate Lookup and Validation Framework”](#) on page 4-26

When Do You Need to Configure a Security Provider?

By default, most WebLogic security providers are generally configured to run after you install WebLogic Server. However, the following circumstances require you to supply configuration information:

- Before using the WebLogic Identity Assertion provider, define the active token type. See [“Configuring Identity Assertion Providers” on page 5-25.](#)
- To map tokens to a user in a security realm, configure the user name mapper in the WebLogic Identity Assertion provider. See [“Configuring a WebLogic Credential Mapping Provider” on page 4-16.](#)
- To use auditing in the default (active) security realm, configure either the WebLogic Auditing provider or a custom Auditing provider. See [“Configuring the WebLogic Auditing Provider” on page 4-5.](#)
- To use HTTP and Kerberos-based authentication in conjunction with WebLogic Server. See [Chapter 6, “Configuring Single Sign-On with Microsoft Clients.”](#)
- To use identity assertion based on SAML assertions. See [Chapter 7, “Configuring Single Sign-On with Web Browsers and HTTP Clients.”](#)
- To use certificate revocation. See [“Certificate Registry” on page 4-27.](#)
- To use an LDAP server other than the embedded LDAP server, configure one of the LDAP Authentication providers. An LDAP authentication provider can be used instead of or in addition to the WebLogic Authentication provider. See [“Configuring LDAP Authentication Providers” on page 5-5.](#)
- To access user, password, group, and group membership information stored in databases for authentication purposes. See [“Configuring RDBMS Authentication Providers” on page 5-13](#) The RDBMS Authentication providers can be used to upgrade from the RDBMS security realm.
- To use Windows NT users and groups for authentication purposes. See [“Configuring a Windows NT Authentication Provider” on page 5-16.](#) The Windows NT Authentication provider is the upgrade path for the Window NT security realm.
- When you create a new security realm, configure security providers for that realm. See [“Creating and Configuring a New Security Realm: Main Steps” on page 3-3.](#)
- When you add a custom security provider to a security realm or replace a WebLogic security provider with a custom security provider, configure options for the custom security

provider. When you create a custom security provider, you can implement options that are configurable through the Administration Console. However, those options are implementation-specific and are not addressed in this manual. See [Extending the Administration Console](#).

You can use either the WebLogic-supplied security providers or a custom security provider in a security realm. To configure a custom security provider, see [Configure a custom security provider](#) in the *Administration Console Online Help*.

Reordering Security Providers

You can configure more than one security provider of a given type in a security realm. For example, you might use two or more different Role Mapping providers or Authorization providers. If you have more than one security provider of the same type in a security realm, the order in which these providers are called can affect the overall outcome of the security processes. By default, security providers are called in the order that they were added to the realm. You can use the Administration Console to change the order of the providers. See [Re-order security providers](#) in the *Administration Console Online Help*.

Configuring an Authorization Provider

Authorization is the process whereby the interactions between users and resources are limited to ensure integrity, confidentiality, and availability. In other words, authorization is responsible for controlling access to resources based on user identity or other information. You should only need to configure an Authorization provider when you create a new security realm.

By default, security realms in newly created domains include the XACML Authorization provider. The XACML Authorization provider uses XACML, the eXtensible Access Control Markup Language. For information about using the XACML Authorization provider, see [Using XACML Documents to Secure WebLogic Resources](#) in *Securing WebLogic Resources Using Roles and Policies*. WebLogic Server also includes the WebLogic Authorization provider, which uses a proprietary policy language. This provider is named DefaultAuthorizer, but is no longer the default authorization provider.

See [Configure Authorization providers](#) in the *Administration Console Online Help*.

Note: The WebLogic Authorization provider improves performance by caching the roles, predicates, and resource data that it looks up. For information on configuring these caches, see [Best Practices: Configure Entitlements Caching When Using WebLogic Providers](#) in *Securing WebLogic Resources Using Roles and Policies*. The XACML Authorization uses its own cache, but this cache is not configurable.

Configuring the WebLogic Adjudication Provider

When multiple Authorization providers are configured in a security realm, each may return a different answer to the “is access allowed” question for a given resource. This answer may be `PERMIT`, `DENY`, or `ABSTAIN`. Determining what to do if multiple Authorization providers do not agree on the answer is the primary function of the Adjudication provider. Adjudication providers resolve authorization conflicts by weighting each Authorization provider’s answer and returning a final decision.

Each security realm requires an Adjudication provider, and can have no more than one active Adjudication provider. By default, a WebLogic security realm is configured with the WebLogic Adjudication provider. You can use either the WebLogic Adjudication provider or a custom Adjudication provider in a security realm.

Note: In the Administration Console, the WebLogic Adjudication provider is referred to as the Default Adjudicator.

By default, most configuration options for the WebLogic Adjudication provider are defined. However, you can set the Require Unanimous Permit option to determine how the WebLogic Adjudication provider handles a combination of `PERMIT` and `ABSTAIN` votes from the configured Authorization providers.

- If the option is enabled (the default), all Authorization providers must vote `PERMIT` in order for the Adjudication provider to vote `true`.
- If the option is disabled, `ABSTAIN` votes are counted as `PERMIT` votes.

Configuring a Role Mapping Provider

Role Mapping providers compute the set of roles granted to a subject for a given resource. Role Mapping providers supply Authorization providers with this role information so that the Authorization provider can answer the “is access allowed?” question for WebLogic resources. By default, a WebLogic security realm is configured with the XACML Role Mapping provider. The XACML Role Mapping provider uses XACML, the eXtensible Access Control Markup Language. For information about using the XACML Role Mapping provider, see [Using XACML Documents to Secure WebLogic Resources](#) in *Securing WebLogic Resources Using Roles and Policies*.

WebLogic Server also includes the WebLogic Role Mapping provider, which uses a proprietary policy language. This provider is named `DefaultRoleMapper`, but is no longer the default role

mapping provider in newly-created security realms. You can also use a custom Role Mapping provider in your security realm.

By default, most configuration options for the XACML Role Mapping provider are already defined. However, you can set Role Mapping Deployment Enabled, which specifies whether or not this Role Mapping provider imports information from deployment descriptors for Web applications and EJBs into the security realm. This setting is enabled by default.

In order to support Role Mapping Deployment Enabled, a Role Mapping provider must implement the `DeployableRoleProvider` SSPI. Roles are stored by the XACML Role Mapping provider in the embedded LDAP server.

For information about using, developing, and configuring Role Mapping providers, see:

- [Users, Groups, And Security Roles](#) in *Securing WebLogic Resources Using Roles and Policies*
- [Role Mapping Providers](#) in *Developing Security Providers for WebLogic Server*
- [Configure Role Mapping providers](#) in the *Administration Console Online Help*

Note: The WebLogic Role Mapping provider improves performance by caching the roles, predicates, and resource data that it looks up. For information on configuring these caches, see [Best Practices: Configure Entitlements Caching When Using WebLogic Providers](#) in *Securing WebLogic Resources Using Roles and Policies*. The XACML Role Mapping provider uses its own cache, but this cache is not configurable.

Configuring the WebLogic Auditing Provider

Auditing is the process whereby information about operating requests and the outcome of those requests are collected, stored, and distributed for the purposes of non-repudiation. In other words, Auditing providers produce an electronic trail of computer activity.

Configuring an Auditing provider is optional. The default security realm (`myrealm`) does not have an Auditing provider configured. WebLogic Server includes a provider named the WebLogic Auditing provider (referred to as `DefaultAuditor` in the Administration Console). You can also develop custom Auditing providers, as described in [Auditing Providers](#) in *Developing Security Providers for WebLogic Server*.

The WebLogic Auditing provider can log the events described in [Table 4-1](#). In addition, if you enable configuration auditing (as described in [“Configuration Auditing” on page 4-10](#)), the WebLogic Auditing provider can log the events described in [Table 4-5](#).

Table 4-1 WebLogic Auditing Provider Events

Audit Event	Indicates...
AUTHENTICATE	Simple authentication (username and password) occurred.
ASSERTIDENTITY	Perimeter authentication (based on tokens) occurred.
USERLOCKED	A user account is locked because of invalid login attempts.
USERUNLOCKED	The lock on a user account is cleared.
USERLOCKOUTEXPIRED	The lock on a user account expired.
ISAUTHORIZED	An authorization attempt occurred.
ROLEEVENT	A <code>getRoles</code> event occurred.
ROLEDEPLOY	A <code>deployRole</code> event occurred.
ROLEUNDEPLOY	An <code>undeployRole</code> event occurred.
POLICYDEPLOY	A <code>deployPolicy</code> event occurred.
POLICYUNDEPLOY	An <code>undeployPolicy</code> event occurred.
START_AUDIT	An Auditing provider has been started.
STOP_AUDIT	An Auditing provider has been stopped.

By default, most configuration options for the WebLogic Auditing provider are already defined and, once it is added to the active security realm, the WebLogic Auditing provider will begin to record audit events. However, you need to define the following settings, which you can do in the Administration Console on the Configuration → Provider Specific page for the provider. You can also use WebLogic Scripting tool or the Java Management Extensions (JMX) APIs to configure the Auditing provider:

- **Rotation Minutes**—Specifies how many minutes to wait before creating a new `DefaultAuditRecorder.log` file. At the specified time, the audit file is closed and a new one is created. A backup file named `DefaultAuditRecorder.YYYYMMDDHHMM.log` (for example, `DefaultAuditRecorder.200405130110.log`) is created in the same directory.

- **Severity**—Severity level appropriate for your WebLogic Server deployment. The WebLogic Auditing provider audits security events of the specified severity, as well as all events with a higher numeric severity rank. For example, if you set the severity level to `ERROR`, the WebLogic Auditing provider audits security events of severity level `ERROR`, `SUCCESS`, and `FAILURE`. You can also set the severity level to `CUSTOM`, and then enable the specific severity levels you want to audit, such as `ERROR` and `FAILURE` events only. Audit events include both the severity name and numeric rank; therefore, a custom Auditing provider can filter events by either the name or the numeric rank. Auditing can be initiated when the following levels of security events occur.

Table 4-2 Audit Severity Levels

Event Severity	Rank
INFORMATION	1
WARNING	2
ERROR	3
SUCCESS	4
FAILURE	5

All auditing information recorded by the WebLogic Auditing provider is saved in `WL_HOME\yourdomain\yourserver\logs\DefaultAuditRecorder.log` by default. Although an Auditing provider is configured per security realm, each server writes auditing data to its own log file in the server directory. You can specify a new directory location for the `DefaultAuditRecorder.log` file on the command line with the following Java startup option:

```
-Dweblogic.security.audit.auditLogDir=c:\foo
```

The new file location will be `c:\foo\yourserver\logs\DefaultAuditRecorder.log`.

For more information, see *Security* in the [WebLogic Server Command Reference](#).

WARNING: Using an Auditing provider affects the performance of WebLogic Server even if only a few events are logged.

For more information, see [Configure Auditing providers](#) in the *Administration Console Online Help*.

Auditing ContextHandler Elements

An Audit Event includes a `ContextHandler` that can hold a variety of information or objects. Set the WebLogic Auditing provider's `Active ContextHandler Entries` attribute to specify which `ContextElement` entries in the `ContextHandler` are recorded by the Auditing provider. By default, none of the `ContextElements` are audited. Objects in the `ContextHandler` are in most cases logged using the `toString` method. [Table 4-3](#) lists the available `ContextHandler` entries.

Table 4-3 Context Handler Entries for Auditing.

Context Element Name	Description and Type
<code>com.bea.contextelement.servlet.HttpServletRequest</code>	A servlet access request or SOAP message via HTTP <code>javax.http.servlet.HttpServletRequest</code>
<code>com.bea.contextelement.servlet.HttpServletResponse</code>	A servlet access response or SOAP message via HTTP <code>javax.http.servlet.HttpServletResponse</code>
<code>com.bea.contextelement.wli.Message</code>	A WebLogic Integration message. The message is streamed to the audit log. <code>java.io.InputStream</code>
<code>com.bea.contextelement.channel.Port</code>	Internal listen port of the network channel accepting or processing the request <code>java.lang.Integer</code>
<code>com.bea.contextelement.channel.PublicPort</code>	External listen port of the network channel accepting or processing the request <code>java.lang.Integer</code>
<code>com.bea.contextelement.channel.RemotePort</code>	Port of the remote end of the TCP/IP connection of the network channel accepting or processing the request <code>java.lang.Integer</code>
<code>com.bea.contextelement.channel.Protocol</code>	Protocol used to make the request of the network channel accepting or processing the request <code>java.lang.String</code>
<code>com.bea.contextelement.channel.Address</code>	The internal listen address of the network channel accepting or processing the request <code>java.lang.String</code>

Context Element Name	Description and Type
com.bea.contextelement. channel.PublicAddress	The external listen address of the network channel accepting or processing the request <code>java.lang.String</code>
com.bea.contextelement. channel.RemoteAddress	Remote address of the TCP/IP connection of the network channel accepting or processing the request <code>java.lang.String</code>
com.bea.contextelement. channel.ChannelName	Name of the network channel accepting or processing the request <code>java.lang.String</code>
com.bea.contextelement. channel.Secure	Whether the network channel is accepting or processing the request using SSL <code>java.lang.Boolean</code>
com.bea.contextelement. ejb20.Parameter[1-N]	Object based on parameter
com.bea.contextelement. wsee.SOAPMessage	<code>javax.xml.rpc.handler.MessageContext</code>
com.bea.contextelement. entitlement.EAuxiliaryID	Used by a WebLogic Server internal process. <code>weblogic.entitlement.expression.EAuxiliary</code>
com.bea.contextelement. security.ChainPrevalidatedBySSL	SSL framework has validated the certificate chain, meaning that the certificates in the chain have signed each other properly; the chain terminates in a certificate that is one of the server's trusted CAs; the chain honors the basic constraints rules; and the certificates in the chain have not expired. <code>java.lang.Boolean</code>
com.bea.contextelement. xml.SecurityToken	Not used in this release of WebLogic Server. <code>weblogic.xml.crypto.wss.provider.SecurityToken</code>
com.bea.contextelement. xml.SecurityTokenAssertion	Not used in this release of WebLogic Server. <code>java.util.Map</code>

Context Element Name	Description and Type
com.bea.contextelement. webservice.Integrity{id:XXXXX}	<code>javax.security.auth.Subject</code>
com.bea.contextelement. saml.SSLClientCertificateChain	SSL client certificate chain obtained from the SSL connection over which a sender-vouches SAML assertion was received. <code>java.security.cert.X509Certificate[]</code>
com.bea.contextelement. saml.MessageSignerCertificate	Certificate used to sign a Web Services message. <code>java.security.cert.X509Certificate</code>
com.bea.contextelement. saml.subject.ConfirmationMethod	Type of SAML assertion: bearer, artifact, sender-vouches, or holder-of-key. <code>java.lang.String</code>
com.bea.contextelement. saml.subject.dom.KeyInfo	<code><ds:KeyInfo></code> element to be used for subject confirmation with holder-of-key SAML assertions. <code>org.w3c.dom.Element</code>

Configuration Auditing

You can configure the Administration Server to emit log messages and generate audit events when a user changes the configuration of any resource within a domain or invokes management operations on any resource within a domain. For example, if a user disables SSL on a Managed Server in a domain, the Administration Server emits log messages. If you have enabled the WebLogic Auditing provider, it writes the audit events to an additional security log. These messages and audit events provide an audit trail of changes within a domain's configuration (configuration auditing).

The Administration Server writes configuration auditing messages to its local log file. They are not written to the domain-wide message log by default.

Note that configuration audit information is contained in Authorization Events. As a result, another approach to configuration auditing is to consume Authorization Events. Note, however, that the information in an Authorization Event tells you whether access was allowed to perform a configuration change; it does not tell you whether the configuration change actually succeeded (for instance, it might have failed because it was invalid).

Enabling Configuration Auditing

Enable configuration auditing by one of these methods:

- Use the Administration Console. On the Configuration → General page for your domain, set the Configuration Audit Type. See [Enabling Configuration Auditing](#) in the *Administration Console Online Help*.
- When you start the Administration Server, include one of the following Java options in the `weblogic.Server` command:
 - `-Dweblogic.domain.ConfigurationAuditType="audit"`
Causes the domain to emit Audit Events only.
 - `-Dweblogic.domain.ConfigurationAuditType="log"`
Causes the domain to write configuration auditing messages to the Administration Server log file only.
 - `-Dweblogic.domain.ConfigurationAuditType="logaudit"`
Causes the domain to emit Audit Events and write configuration auditing messages to the Administration Server log file.

See [weblogic.Server Command-Line Reference](#).
- Use the WebLogic Scripting Tool to change the value of the `ConfigurationAuditType` attribute of the `DomainMBean`. See [WebLogic Scripting Tool](#).

Configuration Auditing Messages

Configuration auditing messages are of the following severities:

Table 4-4 Configuration Auditing Message Severities

Severity	Description
SUCCESS	A successful configuration change occurred.
FAILURE	An attempt to modify the configuration failed due to insufficient user credentials.
ERROR	An attempt to modify the configuration failed due to an internal error.

Configuration auditing messages are identified by message IDs that fall within the range of 159900-159910.

The messages use MBean object names to identify resources. Object names for WebLogic Server MBeans reflect the location of the MBean within the hierarchical data model. To reflect the location, object names contain name/value pairs from the parent MBean. For example, the object name for a server's LogMBean is:

`mydomain:Name=myserverlog,Type=Log,Server=myserver`. See [WebLogic Server MBean Data Model](#) in *Developing Custom Management Utilities with JMX*.

[Table 4-5](#) summarizes the messages.

Table 4-5 Summary of Configuration Auditing Messages

When This Event Occurs...	WebLogic Server Generates a Message With This ID...	And This Message Text...
Authorized user creates a resource.	159900	USER <i>username</i> CREATED <i>MBean-name</i> where <i>username</i> identifies the WebLogic Server user who logged in and created a resource.
Unauthorized user attempts to create a resource.	159901	USER <i>username</i> CREATED <i>MBean-name</i> FAILED <code>weblogic.management.NoAccessRuntimeException: exception-text stack-trace</code> where <i>username</i> identifies the unauthorized WebLogic Server user.
Authorized user deletes a resource.	159902	USER <i>username</i> REMOVED <i>MBean-name</i> where <i>username</i> identifies the WebLogic Server user who logged in and deleted a resource.
Unauthorized user attempts to delete a resource.	159903	USER <i>username</i> REMOVE <i>MBean-name</i> FAILED <code>weblogic.management.NoAccessRuntimeException: exception-text stack-trace</code> where <i>username</i> identifies the unauthorized WebLogic Server user.

Table 4-5 Summary of Configuration Auditing Messages (Continued)

When This Event Occurs...	WebLogic Server Generates a Message With This ID...	And This Message Text...
Authorized user changes a resource's configuration.	159904	<p>USER <i>username</i> MODIFIED <i>MBean-name</i> ATTRIBUTE <i>attribute-name</i> FROM <i>old-value</i> TO <i>new-value</i></p> <p>where <i>username</i> identifies the WebLogic Server user who logged in and changed the resource's configuration.</p>
Unauthorized user attempts to change a resource's configuration.	159905	<p>USER <i>username</i> MODIFY <i>MBean-name</i> ATTRIBUTE <i>attribute-name</i> FROM <i>old-value</i> TO <i>new-value</i> FAILED weblogic.management. NoAccessRuntimeException: <i>exception-text stack-trace</i></p> <p>where <i>username</i> identifies the unauthorized WebLogic Server user.</p>
<p>Authorized user invokes an operation on a resource.</p> <p>For example, a user deploys an application or starts a server instance.</p>	159907	<p>USER <i>username</i> INVOKED ON <i>MBean-name</i> METHOD <i>operation-name</i> PARAMS <i>specified-parameters</i></p> <p>where <i>username</i> identifies the WebLogic Server user who logged in and invoked a resource operation.</p>
Unauthorized user attempts to invoke an operation on a resource.	159908	<p>USER <i>username</i> INVOKED ON <i>MBean-name</i> METHOD <i>operation-name</i> PARAMS <i>specified-parameters</i> FAILED weblogic.management. NoAccessRuntimeException: <i>exception-text stack-trace</i></p> <p>where <i>username</i> identifies the unauthorized WebLogic Server user.</p>

Table 4-5 Summary of Configuration Auditing Messages (Continued)

When This Event Occurs...	WebLogic Server Generates a Message With This ID...	And This Message Text...
Authorized user enables configuration auditing.	159909	USER <i>username</i> , Configuration Auditing is enabled where <i>username</i> identifies the WebLogic Server user who enabled configuration auditing.
Authorized user disables configuration auditing.	159910	USER <i>username</i> , Configuration Auditing is disabled where <i>username</i> identifies the WebLogic Server user who disabled configuration auditing.

Note: Each time an authorized user adds, modifies, or deletes a resource, the Management subsystem also generates an `Info` message with the ID 140009 regardless of whether configuration auditing is enabled. For example:

```
<Sep 15, 2005 11:54:47 AM EDT> <Info> <Management> <140009>
<Configuration changes for domain saved to the repository.>
```

While the message informs you that the domain’s configuration has changed, it does not provide the detailed information that configuration auditing messages provide. Nor does the Management subsystem generate this message when you invoke operations on resources.

[Table 4-6](#) lists additional message attributes for configuration auditing messages. All configuration auditing messages specify the same values for these attributes.

Table 4-6 Common Message Attributes and Values

Message Attribute	Attribute Value
Severity	Info
Subsystem	Configuration Audit
User ID	kernel identity This value is always <code>kernel identity</code> , regardless of which user modified the resource or invoked the resource operation.

Table 4-6 Common Message Attributes and Values

Message Attribute	Attribute Value
Server Name	<i>AdminServerName</i> Because the Administration Server maintains the configuration data for all resources in a domain, this value is always the name of the Administration Server.
Machine Name	<i>AdminServerHostName</i> Because the Administration Server maintains the configuration data for all resources in a domain, this value is always the name of the Administration Server's host machine.
Thread ID	<i>execute-thread</i> The value depends on the number of execute threads that are currently running on the Administration Server.
Timestamp	<i>timeStamp</i> at which the message is generated.

Audit Events and Auditing Providers

An audit event is an object that Auditing providers can read and process in specific ways. An Auditing provider is a pluggable component that the security realm uses to collect, store, and distribute information about operating requests and the outcome of those requests for the purposes of non-repudiation.

If you enable a domain to emit Audit Events, the domain emits the events described in [Table 4-7](#). All Auditing providers that are configured for the domain can handle these events.

All of the events are of severity level `SUCCESS` and describe the security principal who initiated the action, whether permission was granted, and the object (MBean or MBean attribute) of the requested action.

Table 4-7 Summary of Audit Events for Configuration Auditing

When This Event Occurs...	WebLogic Server Generates This Audit Event Object...
A request to create a new configuration artifact has been allowed or prevented.	<code>weblogic.security.spi.AuditCreateConfigurationEvent</code> See Javadoc .
A request to delete an existing configuration artifact has been allowed or prevented.	<code>weblogic.security.spi.AuditDeleteConfigurationEvent</code> See Javadoc .
A request to modify an existing configuration artifact has been allowed or prevented.	<code>weblogic.security.spi.AuditInvokeConfigurationEvent</code> See Javadoc .
A invoke an operation on an existing configuration artifact has been allowed or prevented.	<code>weblogic.security.spi.AuditSetAttributeConfigurationEvent</code> See Javadoc .

If you enable the default WebLogic Server Auditing provider, it writes all Audit Events as log messages in its own log file.

Other Auditing providers that you create or purchase can filter these events and write them to output repositories such as an LDAP server, database, or a simple file. In addition, other types of security providers can request audit services from an Auditing provider. See [Auditing Providers](#) in *Developing Security Providers for WebLogic Server*.

Configuring a WebLogic Credential Mapping Provider

Credential mapping is the process whereby the authentication and authorization mechanisms of a remote system (for example, a legacy system or application) obtain an appropriate set of credentials to authenticate remote users to a target WebLogic resource. The WebLogic Credential Mapping provider maps WebLogic Server subjects to the username/password pairs to be used when accessing such resources.

By default, most configuration options for the WebLogic Credential Mapping provider are defined. However, you have the option of setting Credential Mapping Deployment Enabled, which specifies whether or not this Credential Mapping provider imports credential maps from a

resource adapter's deployment descriptor (`weblogic-ra.xml` file) into the security realm. This setting is enabled by default.

In order to support Credential Mapping Deployment Enabled, a Credential Mapping provider must implement the `DeployableCredentialProvider` SSPI. The credential mapping information is stored in the embedded LDAP server.

For more information:

- See [Credential Mapping Providers](#) in *Developing Security Providers for WebLogic Server*
- See [Configure Credential Mapping providers](#) and [Create Credential Mappings](#) in the *Administration Console Online Help*.
- For information about using credential maps, see *Programming WebLogic Resource Adapters*.
- You can also use the WebLogic Scripting Tool or Java Management Extensions (JMX) APIs to create a new security configuration.
- For information about other credential mapping providers, see “[Configuring a PKI Credential Mapping Provider](#)” on page 4-17 and “[Configuring a SAML Credential Mapping Provider for SAML 1.1](#)” on page 4-19.

Configuring a PKI Credential Mapping Provider

The PKI (Public Key Infrastructure) Credential Mapping provider included in WebLogic Server maps (a) a WebLogic Server subject (the initiator) and target resource (and an optional credential action) to (b) a key pair or public certificate that can be used by applications when accessing the targeted resource. The PKI Credential Mapping provider uses the subject and resource name to retrieve the corresponding credential from the keystore.

To use the PKI Credential Mapping provider, you need to:

1. Configure keystores with appropriate keys and distribute the keystores on all machines in a WebLogic Server cluster. Setting up keystores is not a WebLogic Server function. For information about setting up keystores, see the [help for the Java keytool utility](http://java.sun.com/j2se/1.4.2/docs/tooldocs/solaris/keytool.html) at <http://java.sun.com/j2se/1.4.2/docs/tooldocs/solaris/keytool.html>. See also [Chapter 11, “Configuring Identity and Trust,”](#) for information about keystores and keys in WebLogic Server.
2. Configure a PKI Credential Mapping provider. A PKI Credential Mapping provider is not already configured in the default security realm (`myrealm`). See “[PKI Credential Mapper](#)”

[Attributes](#)” on page 4-18 and [Configure Credential Mapping providers](#) in the *Administration Console Online Help*.

3. Create credential mappings. See [Create PKI Credential Mappings](#) in the *Administration Console Online Help*.

PKI Credential Mapper Attributes

To configure the PKI Credential Mapping provider, set values for these attributes. See [Configure Credential Mapping providers](#) in the *Administration Console Online Help*.

- **Keystore Provider**—A keystore provider for the Java Security API. If no value is specified, the default provider class is used.
- **Keystore Type**— JKS (the default) or PKCS12.
- **Keystore Pass Phrase**—Password used to access the keystore
- **Keystore File Name**—Location of the keystore relative to the directory where the server was started.

In addition, two optional attributes determine how the PKI Credential Mapping provider locates credential mappings in cases where the exact resource or subject may not be available:

- **Use Resource Hierarchy**—A credential is located by traversing up the resource hierarchy for each type of resource. The search for all possible PKI credentials will start from the specific resource and will walk up the resource hierarchy to find all possible matches. This attribute is enabled by default.
- **Use Initiator Group Names**—When a subject is passed to the PKI Credential Mapper provider, a credential is located by examining the groups of which the initiator is a member. This is enabled by default.

Credential Actions

Optionally, you can label a credential mapping with a credential action. You can do this in the Administration Console when you create the credential mapping. The credential action is an arbitrary string that distinguishes credential mappings used in different circumstances. For example, one credential mapping could decrypt a message from a remote resource and another credential mapping could sign messages to be sent to the same resource. The subject initiator and the target resource are not sufficient to distinguish these two credential mappings. You can use the credential action to label one of these credential mappings something like `decrypt` and the

other one `sign`. Then, the application calling the PKI Credential Mapping provider can provide the desired credential action value in the `ContextHandler` that is passed to the provider.

For information about adding credential actions to PKI credential mappings, see [Create PKI Credential Mappings](#) in the *Administration Console Online Help*.

Configuring a SAML Credential Mapping Provider for SAML 1.1

This release of WebLogic Server includes two SAML Credential Mapping providers. SAML Credential Mapping Provider Version 2 provides greatly enhanced configuration options and is recommended for new deployments. SAML Credential Mapping Provider Version 1 is deprecated in WebLogic Server 9.1. A security realm can have not more than one SAML Credential Mapping provider, and if the security realm has both a SAML Credential Mapping provider and a SAML Identity Assertion provider, both must be of the same version. Do not use a Version 1 SAML provider in the same security realm as a Version 2 SAML provider. For information about configuring the SAML Credential Mapping Provider Version 1, see [Configuring a SAML Credential Mapping Provider](#) in the WebLogic Server 9.0 documentation.

For general information about WebLogic Server's support for SAML, see [Security Assertion Markup Language \(SAML\)](#) and [Single Sign-On with the WebLogic Security Framework](#) in *Understanding WebLogic Security*. For information about how to use the SAML Credential Mapping provider in a SAML single sign-on configuration, see [Chapter 7, "Configuring Single Sign-On with Web Browsers and HTTP Clients."](#)

Configuring Assertion Lifetime

A SAML Assertion's validity is typically time-limited. The default time-to-live for assertions generated by the SAML Credential Mapping provider is specified by the `DefaultTimeToLive` attribute. You can override the default time-to-live for assertions generated for different SAML Relying Parties.

Normally, an assertion is valid from the `NotBefore` time, which defaults to (roughly) the time the assertion was generated, until the `NotOnOrAfter` time, which is calculated as (`NotBefore` + `TimeToLive`). To allow the Credential Mapper to compensate for clock differences between the source and destination sites, you can configure the SAML Credential Mapping provider's `DefaultTimeToLiveDelta` attribute. This time-to-live offset value is a positive or negative integer indicating how many seconds before or after "now" the assertion's `NotBefore` value should be set to. If you set a value for `DefaultTimeToLiveDelta`, then the assertion lifetime is

still calculated as (NotBefore + TimeToLive), but the NotBefore value is set to (now + TimeToLiveDelta). For example, given the following settings:

```
DefaultTimeToLive = 120
```

```
DefaultTimeToLiveDelta = -30
```

an assertion when generated would have a lifetime of two minutes (120 seconds), starting 30 seconds before it is generated.

Relying Party Registry

When you configure WebLogic Server to act as a source of SAML security assertions, you need to register the parties that may request SAML assertions to be generated. For each SAML Relying Party, you can specify the SAML profile used, details about the Relying Party, and the attributes expected in assertions for the Relying Party. For information, see:

- [“Configure Relying Parties” on page 7-4.](#)
- [Configure a SAML Relying Party](#) in the *Administration Console Online Help*.

Configuring a SAML 2.0 Credential Mapping Provider for SAML 2.0

The SAML 2.0 Credential Mapping provider included with WebLogic Server generates SAML 2.0 assertions that can be used to assert identity in the following use cases:

- SAML 2.0 Web SSO Profile
- WS-Security SAML Token Profile version 1.1

The SAML 2.0 Credential Mapping provider generates the assertion types listed and described in [Table 4-8](#).

Table 4-8 Assertion Types Supported by the SAML 2.0 Credential Mapping Provider

Assertion Type	Description
bearer	The subject of the assertion is the bearer of the assertion, subject to optional constraints on confirmation using attributes that may be included in the <SubjectConfirmationData> element of the assertion. Used for all assertions generated for the SAML 2.0 Web Browser SSO Profile and with the Web Service Security SAML Token Profile 1.1.
sender-vouches	The Identity Provider (different from the subject) vouches for the verification of the subject. The receiver must have a trust relationship with the Identity Provider. Used with the Web Service Security SAML Token Profile 1.1 only.
holder-of-key	The subject represented in the assertion uses an X.509 certificate that may not be trusted by the receiver to protect the integrity of the request messages. Used with the Web Service Security SAML Token Profile 1.1 only.

For general information about WebLogic Server’s support for SAML 2.0, see [Security Assertion Markup Language \(SAML\)](#) and [Single Sign-On with the WebLogic Security Framework](#) in *Understanding WebLogic Security*. For information about how to use the SAML 2.0 Credential Mapping provider in a SAML 2.0 single sign-on configuration, see [Chapter 7, “Configuring Single Sign-On with Web Browsers and HTTP Clients.”](#) For information about specifying the confirmation method for assertions generated for web service Service provider partners, see [“Using Security Assertion Markup Language \(SAML\) Tokens For Identity”](#) in *Securing WebLogic Web Services*.

SAML 2.0 Credential Mapping Provider Attributes

Configuration of the SAML 2.0 Credential Mapping provider is controlled by setting attributes on the `SAML2CredentialMapperMBean`. You can access the `SAML2CredentialMapperMBean` using the WebLogic Scripting Tool (WLST), or through the Administration Console by using the Security Realms → *RealmName* → Providers → Credential Mapping page and creating or selecting `SAML2CredentialMapper`. The `SAML2CredentialMapperMBean` is described at the following location:

http://e-docs.bea.com/wls/docs103/saml2_javadocs/com/bean/security/saml2/providers/SAML2CredentialMapperMBean.html

To configure the SAML 2.0 Credential Mapping provider, set the following attributes:

- Issuer URI

Name of this security provider. The value that you specify should match the Entity ID specified in the SAML 2.0 General page that configures the per-server SAML 2.0 properties.

- Name Qualifier

Used by the Name Mapper class as the security or administrative domain that qualifies the name of the subject. This provides a means to federate names from disparate user stores while avoiding the possibility of subject name collision.

- Assertion life time

Values that limit the life time of generated assertions during which they may be used. Expired assertions cannot be made available for use.

- Web service assertion signing key alias and passphrase

Used for signing generated assertions.

- Custom name mapper class

The custom Java class that overrides the default SAML 2.0 Credential Mapping provider name mapper class, which maps Subjects to identity information contained in the assertion.

- Generate attributes

Specifies whether group membership information associated with the authenticated Subject is included in generated assertions.

Service Provider Partners

When you configure WebLogic Server to act as an Identity Provider, you need to create and configure the Service Provider partners for whom SAML 2.0 assertions are generated. When an Identity Provider site needs to generate an assertion, the SAML 2.0 Credential Mapping provider determines the Service Provider partner for whom the assertion must be generated, and generates it according to the configuration of that Service Provider partner.

The way in which you configure a Service Provider partner, and the specific information you configure for that partner, depends upon whether the partner is used for web single sign-on or web services. Configuring a web single sign-on Service Provider partner consists of importing that partner's metadata file and establishing additional basic information about that partner, such as the following:

- Determining whether SAML documents, such as authentication responses, SAML artifacts, and artifact requests, must be signed
- Certificates used for validating signed documents received from this partner
- The binding to be used for sending SAML artifacts to this partner
- The client user name and password used by this partner when connecting to the local site's binding

For details about configuring a Service Provider partner for web single sign-on, see:

- [“Create and Configure Web Single Sign-On Service Provider Partners” on page 7-15](#)
- [Create a SAML 2.0 Web Single Sign-on Service Provider partner](#) in the *Administration Console Online Help*

Configuring a web service Service Provider partner does not use a metadata file, but does consist of establishing the following information about that partner:

- Audience URIs, which specify an audience restriction to be included in assertions generated for this partner

In WebLogic Server, the Audience URI attribute is overloaded to also include the partner lookup string, which is required by the web service run time to discover the partner. See [“Partner Lookup Strings Required for Web Service Partners” on page 4-23](#).

- Custom name mapper class that overrides the default name mapper and that is to be used specifically with this partner
- Values that specify the life span attributes of assertions generated for this partner
- Confirmation method for assertions received from this partner

For more information about configuring web service Service Provider partners, see [Create a SAML 2.0 Web Service Service Provider partner](#) in the *Administration Console Online Help*.

Partner Lookup Strings Required for Web Service Partners

For web service Service Provider partners, you also configure Audience URIs. In WebLogic Server, the Audience URI attribute is overloaded to perform two distinct functions:

- Specify an audience restriction that consists of the target service URL, per the OASIS SAML 2.0 specification.

- Contain a partner lookup string, which is required at run time by WebLogic Server to discover the Service Provider partner for which a SAML 2.0 assertion needs to be generated.

The partner lookup string specifies an endpoint URL, which is used for partner lookup and can optionally also serve as an Audience URI restriction that is included in the generated assertion. The ability to specify a partner lookup string that is also an Audience URI eliminates the need to specify a given target URL twice: once for lookup, and again for audience restriction.

Note: You must configure a partner lookup string for a Service Provider partner so that partner can be discovered at run time by the web service run time.

Lookup String Syntax

The partner lookup string has the following syntax:

```
[target:char:]<endpoint-url>
```

In this syntax, `target:char:` is a prefix that designates the partner lookup string, where `char` represents one of three special characters: a hyphen, plus sign, or asterisk (-, +, or *). This prefix determines how partner lookup is performed, as described in [Table 4-9](#).

Table 4-9 Service Provider Partner Lookup String Syntax

Lookup String	Description
<code>target::-<endpoint-url></code>	<p>Specifies that partner lookup is conducted for an exact match of the URL, <code><endpoint-url></code>. For example, <code>target::-http://www.avitek.com:7001/myserver/myservicecontext/my-service-endpoint</code> specifies the endpoint that can be matched to this Service Provider, for which an assertion should be generated.</p> <p>This form of partner lookup string excludes the endpoint URL from being added as an Audience URI in the generated assertion.</p>

Table 4-9 Service Provider Partner Lookup String Syntax (Continued)

Lookup String	Description
<code>target::<endpoint-url></code>	<p>Specifies that partner lookup is conducted for an exact match of the URL, <code><endpoint-url></code>.</p> <p>Using the plus sign (+) in the lookup string results in the endpoint URL being added as an Audience URI in the assertion generated for this Service Provider partner.</p>
<code>target::*:<endpoint-url></code>	<p>Specifies that partner lookup is conducted for an initial-string pattern match of the URL, <code><endpoint-url></code>. For example, <code>target::*:http://www.avitek.com:7001/myserver</code> specifies that any endpoint URL beginning with <code>http://www.avitek.com:7001/myserver</code> can be matched to this Service Provider, such as:</p> <p><code>http://www.avitek.com:7001/myserver/contextA/endpointA</code> and <code>http://www.avitek.com:7001/myserver/contextB/endpointB</code>.</p> <p>If more than one Service Provider partner is discovered that is a match for the initial string, the partner with the longest initial string match is selected.</p> <p>This form of partner lookup string excludes the endpoint URL from being added as an Audience URI in the generated assertion.</p>

Notes: Configuring one or more partner lookup strings for a Service Provider partner is required in order for that partner to be discovered at run time. If this partner cannot be discovered, no assertions for this partner can be generated.

If you configure an endpoint URL without using the target lookup prefix, it will be handled as a conventional Audience URI that must be contained in assertions generated for this Service Provider partner. (This also enables backwards-compatibility with existing Audience URIs that may be configured for this partner.)

Specifying Default Partners

To support the need for a default Service Provider partner entry, one or more of the default partner's Audience URI entries may contain a wildcard match that works for all targets. The actual wildcard URI may depend on the specific format used by the web service run time. For example:

- `target::*:http://`

- `target:*:https://`

Management of Partner Certificates

The SAML 2.0 Credential Mapping provider manages a set of trusted certificates for each partner configured for web single sign-on. Whenever a signed authentication or artifact request is received during a message exchange with a partner, the trusted certificate is used to verify the partner's signature. Partner certificates are used for the following purposes:

- To validate trust when the SAML 2.0 Credential Mapping provider receives a signed authentication request or artifact request.
- To validate trust in a Service Provider partner that is retrieving a SAML artifact from the Artifact Resolution Service (ARS) via an SSL connection.

From the Administration Console, you can view a web single sign-on Service Provider partner's signing certificate and transport layer client certificate in the partner management pages of the configured SAML 2.0 Credential Mapping provider.

Java Interface for Configuring Service Provider Partner Attributes

Operations on web service partners are available in the [com.bea.security.saml2.providers.registry.Partner](#) Java interface.

Configuring the Certificate Lookup and Validation Framework

WebLogic Server may receive digital certificates as part of Web Services requests, two-way SSL, or other secure interactions. To validate these certificates, WebLogic Server includes a Certificate Lookup and Validation (CLV) framework, whose function is to look up and validate X.509 certificate chains. The key elements of the CLV framework are the `CertPathBuilder` and the `CertPathValidators`. The CLV framework requires one and only active `CertPathBuilder` which, given a reference to a certificate chain, finds the chain and validates it, and zero or more `CertPathValidators` which, given a certificate chain, validates it.

When WebLogic Server receives a certificate, the CLV framework uses the security provider configured as the `CertPathBuilder` to look up and validate the certificate chain. If the certificate chain is found and valid, the framework then calls each configured `CertPathValidator`, in the order the administrator configured them, to perform extra validation on the chain. The chain is only valid if the builder and all the validators successfully validate it.

A chain is valid only if all of the following are true:

- The certificates in the chain have signed each other properly.
- The chain terminates in a certificate that is one of the server's trusted CAs.
- The chain honors the basic constraints rules (for example, no certificate in the chain has been issued by a certificate that is not allowed to issue certificates).
- The certificates in the chain have not expired.

WebLogic Server includes two CLV security providers: the WebLogic CertPath provider (which acts as both a CertPathBuilder and a CertPathValidator), described in [“CertPath Provider” on page 4-27](#), and the Certificate Registry, described in [“Certificate Registry” on page 4-27](#). Use just the WebLogic CertPath provider if you want to use trusted CA-based validation of the full certificate chain. Use just the Certificate Registry if you want only to validate that certificates are registered. Use both, designating the Certificate Registry as the current builder, if you want to use both types of validation.

For more information about certificate lookup and validation, see [Chapter 11, “Configuring Identity and Trust.”](#)

CertPath Provider

The default security realm in WebLogic Server is configured with the WebLogic CertPath provider. The CertPath provider serves two functions: CertPathBuilder and CertPathValidator. The CertPath provider receives an end certificate or a certificate chain. It uses the server's list of trusted CAs to complete the certificate chain, if necessary. After building the chain, the CertPath provider validates the chain, checking the signatures in the chain, ensuring that the chain has not expired, checking the chain's basic constraints, and verifying that the chain terminates in a certificate issued by one of the server's trusted CAs.

The WebLogic CertPath provider requires no configuration, other than its Current Builder attribute, which indicates whether the CertPath provider should be used as the active certificate chain builder.

Certificate Registry

The Certificate Registry is a security provider that allows you to explicitly register the list of trusted certificates that are allowed to access WebLogic Server. If you configure a Certificate Registry as part of your security realm, then only certificates that are registered in the Certificate Registry will be considered valid. The Certificate Registry provides an inexpensive mechanism

for performing revocation checking. By removing a certificate from the Certificate Registry, you can invalidate a certificate immediately. The registry is stored in the embedded LDAP server.

The Certificate Registry is both a CertPath Builder and a CertPath Validator. In either case, the Certificate Registry ensures that the chain's end certificate is stored in the registry, but does no other validation. If you use the Certificate Registry as your security realm's CertPath Builder and you also want to use the WebLogic CertPath provider or another security provider to perform full chain validation, make sure that you register the intermediate and root CAs in each server's trust keystore, and the end certificates in the Certificate Registry.

The default security realm in WebLogic Server does not include a Certificate Registry. Once you configure a Certificate Registry, you can use the WebLogic Administration Console to add, remove, and view certificates in the registry. You can export a certificate from a keystore to a file, using the Java `keytool` utility. You can import a certificate that is a PEM or DER file in the file system into the Certificate Registry using the console. You can also use the Console to view the contents of a certificate, including its subject DN, issuer DN, serial number, valid dates, fingerprints, etc.

See [Configure Certification Path providers](#) in the *Administration Console Online Help*.

Configuring a WebLogic Keystore Provider

Note: The WebLogic Keystore provider is deprecated. It is only supported for backward compatibility. Use Java KeyStores (JKS) instead. All of the functionality that was supported by the WebLogic Keystore provider is available through use of Java KeyStores.

For information about configuring the WebLogic Keystore provider, see [Configure keystores](#) in the *Administration Console Online Help*.

Configuring Authentication Providers

WebLogic Server includes numerous Authentication security providers. Most of them work in similar fashion: given a username and password credential pair, the provider attempts to find a corresponding user in the provider's data store. These Authentication providers differ primarily in what they use as a data store: one of many available LDAP servers, a SQL database, or other data store. In addition to these username/password based security providers, WebLogic Server includes identity assertion Authentication providers, which use certificates or security tokens, rather than username/password pairs, as credentials.

The following sections describe how to configure the Authentication security providers supplied by WebLogic Server.

- [“Choosing an Authentication Provider” on page 5-2](#)
- [“Using More Than One Authentication Provider” on page 5-3](#)
- [“Configuring the WebLogic Authentication Provider” on page 5-4](#)
- [“Configuring LDAP Authentication Providers” on page 5-5](#)
- [“Configuring RDBMS Authentication Providers” on page 5-13](#)
- [“Configuring a Windows NT Authentication Provider” on page 5-16](#)
- [“Configuring the SAML Authentication Provider” on page 5-18](#)
- [“Configuring the Password Validation Provider” on page 5-19](#)
- [“Configuring Identity Assertion Providers” on page 5-25](#)

- [“How an LDAP X509 Identity Assertion Provider Works” on page 5-27](#)
- [“Ordering of Identity Assertion for Servlets” on page 5-37](#)

Choosing an Authentication Provider

Authentication is the process whereby the identity of users and system processes are proved or verified. Authentication also involves remembering, transporting, and making identity information available to various components of a system when that information is needed.

The WebLogic Server security architecture supports: certificate-based authentication directly with WebLogic Server; HTTP certificate-based authentication proxied through an external Web server; perimeter-based authentication (Web server, firewall, VPN); and authentication based on multiple security token types and protocols.

WebLogic Server offers the following types of Authentication providers:

- *The WebLogic Authentication provider* accesses user and group information in WebLogic Server’s embedded LDAP server.
- *LDAP Authentication providers* access external LDAP stores. You can use an LDAP Authentication provider to access any LDAP server. WebLogic Server provides LDAP Authentication providers already configured for Open LDAP, Sun iPlanet, Microsoft Active Directory and Novell NDS LDAP servers.
- *RDBMS Authentication providers* access external relational databases. WebLogic Server provides three RDBMS Authentication providers: SQL Authenticator, Read-only SQL Authenticator, and Custom RDBMS Authenticator.
- *The WebLogic Identity Assertion provider* validates X.509 and IIOP-CSIV2 tokens and optionally can use a user name mapper to map that token to a user in a WebLogic Server security realm.
- *The SAML Authentication provider*, which authenticates users based on Security Assertion Markup Language 1.1 (SAML) assertions.
- *The Negotiate Identity Assertion provider*, which uses Simple and Protected Negotiate (SPNEGO) tokens to obtain Kerberos tokens, validates the Kerberos tokens, and maps Kerberos tokens to WebLogic users.
- *The SAML Identity Assertion provider*, which acts as a consumer of SAML security assertions. This enables WebLogic Server to act as a SAML destination site and supports using SAML for single sign-on.

In addition, you can use:

- Custom (non-WebLogic) Authentication providers, which offer different types of authentication technologies.
- Custom (non-WebLogic) Identity Assertion providers, which support different types of tokens.

Using More Than One Authentication Provider

Each security realm must have one at least one Authentication provider configured. The WebLogic Security Framework is supports multiple Authentication providers (and thus multiple LoginModules) for multipart authentication. Therefore, you can use multiple Authentication providers as well as multiple types of Authentication providers in a security realm. For example, if you want to use both a retina-scan and a username/password-based form of authentication to access a system, you configure two Authentication providers.

How you configure multiple Authentication providers can affect the overall outcome of the authentication process. Configure the JAAS Control Flag for each Authentication provider to set up login dependencies between Authentication providers and allow single-sign on between providers. See [“Setting the JAAS Control Flag Option” on page 5-3](#).

Authentication providers are called in the order in which they were configured in the security realm. Therefore, use caution when configuring Authentication providers. You can use the WebLogic Administration Console to re-order the configured Authentication providers, thus changing the order in which they are called. See [“Changing the Order of Authentication Providers” on page 5-4](#).

Setting the JAAS Control Flag Option

When you configure multiple Authentication providers, use the JAAS Control Flag for each provider to control how the Authentication providers are used in the login sequence. You can set the JAAS Control Flag in the WebLogic Administration Console. See [Set the JAAS control flag](#) in the *Administration Console Online Help*. You can also use the WebLogic Scripting Tool or Java Management Extensions (JMX) APIs to set the JAAS Control Flag for an Authentication provider.

JAAS Control Flag values are:

- **REQUIRED**—The Authentication provider is always called, and the user must always pass its authentication test. If authentication succeeds or fails, authentication still continues down the list of providers.
- **REQUISITE**—The user is required to pass the authentication test of the Authentication provider. If the user passes the authentication test of this Authentication provider, subsequent providers are executed but can fail (except for Authentication providers with the JAAS Control Flag set to **REQUIRED**).
- **SUFFICIENT**—The user is not required to pass the authentication test of the Authentication provider. If authentication succeeds, no subsequent Authentication providers are executed. If authentication fails, authentication continues down the list of providers.
- **OPTIONAL**—The user is allowed to pass or fail the authentication test of this Authentication provider. However, if all Authentication providers configured in a security realm have the JAAS Control Flag set to **OPTIONAL**, the user must pass the authentication test of one of the configured providers.

When additional Authentication providers are added to an existing security realm, by default the Control Flag is set to **OPTIONAL**. If necessary, change the setting of the Control Flag and the order of Authentication providers so that each Authentication provider works properly in the authentication sequence.

Changing the Order of Authentication Providers

The order in which WebLogic Server calls multiple Authentication providers can affect the overall outcome of the authentication process. The Authentication Providers table lists the authentication providers in the order in which they will be called. By default, Authentication providers are called in the order in which they were configured. You can use the Administration Console to change the order of Authentication providers. Use the Reorder button on the Security Realms → Providers → Authentication page in the Administration Console to change the order in which Authentication providers are called by WebLogic Server and listed in the console.

See [Re-order Authentication Providers](#) in the *Administration Console Online Help*.

Configuring the WebLogic Authentication Provider

The WebLogic Authentication provider uses WebLogic Server's embedded LDAP server to store user and group membership information. This provider allows you to edit, list, and manage users and group membership. By default, most configuration options for the WebLogic Authentication

provider are already defined. You should need to configure a WebLogic Authentication provider only when creating a new security realm. However, note the following:

- The WebLogic Authentication provider is configured in the default security realm with the name `DefaultAuthenticator`.
- User and group names in the WebLogic Authentication provider are case insensitive.
- Ensure that all user names are unique.
- Use the Minimum Password Length option on the Configuration → Provider Specific page to specify the length of passwords defined for users that are stored in the embedded LDAP server.
- If you are using multiple Authentication providers, set the JAAS Control Flag to determine how the WebLogic Authentication provider is used in the authentication process. See [“Using More Than One Authentication Provider”](#) on page 5-3.

Configuring LDAP Authentication Providers

WebLogic Server includes the following LDAP Authentication providers:

- iPlanet Authentication provider
- Active Directory Authentication provider
- Open LDAP Authentication provider
- Novell Authentication provider
- generic LDAP Authentication provider

Each LDAP Authentication provider stores user and group information in an external LDAP server. They differ primarily in how they are configured by default to match typical directory schemas for their corresponding LDAP server.

WebLogic Server does not support or certify any particular LDAP servers. Any LDAP v2 or v3 compliant LDAP server should work with WebLogic Server. The following LDAP directory servers have been tested:

- Sun iPlanet version 4.1.3
- Active Directory shipped as part of Windows 2000
- Open LDAP version 2.0.7

- Novell NDS version 8.5.1

An LDAP Authentication provider can also be used to access other LDAP servers. However, you must either use the LDAP Authentication provider (`LDAPAuthenticator`) or choose a pre-defined LDAP provider and customize it. See [“Accessing Other LDAP Servers”](#) on page 5-7.

Requirements for Using an LDAP Authentication Provider

If an LDAP Authentication provider is the only configured Authentication provider for a security realm, you must have the `Admin` role to boot WebLogic Server and use a user or group in the LDAP directory. Do one of the following in the LDAP directory:

- By default in WebLogic Server, the `Admin` role includes the `Administrators` group. Create an `Administrators` group in the LDAP directory, if one does not already exist. Make sure the LDAP user who will boot WebLogic Server is included in the group.

The Active Directory LDAP directory has a default group called `Administrators`. Add the user who will be booting WebLogic Server to the `Administrators` group and define Group Base Distinguished Name (DN) so that the `Administrators` group is found.

- If you do not want to create an `Administrators` group in the LDAP directory (for example, because the LDAP directory uses the `Administrators` group for a different purpose), create a new group (or use an existing group) in the LDAP directory and include the user from which you want to boot WebLogic Server in that group. In the WebLogic Administration Console, assign that group the `Admin` role.

Configuring an LDAP Authentication Provider: Main Steps

To configure an LDAP Authentication provider:

1. Choose an LDAP Authentication provider that matches your LDAP server and create an instance of the provider in your security realm. See [Configure Authentication and Identity Assertion providers](#) in the *Administration Console Online Help*.
2. Configure the provider-specific attributes of the LDAP Authentication provider, which you can do through the Administration Console. For each LDAP Authentication provider, there are attributes that:
 - a. Enable communication between the LDAP server and the LDAP Authentication provider. For a more secure deployment, Oracle recommends using the SSL protocol to protect communications between the LDAP server and WebLogic Server. Enable SSL with the `SSLEnabled` attribute.

- b. Configure options that control how the LDAP Authentication provider searches the LDAP directory.
 - c. Specify where in the LDAP directory structure users are located.
 - d. Specify where in the LDAP directory structure groups are located.
 - e. Define how members of a group are located.
3. Configure performance options that control the cache for the LDAP server. Use the Configuration → Provider Specific and Performance pages for the provider in the Administration Console to configure the cache. See [“Improving the Performance of WebLogic and LDAP Authentication Providers”](#) on page 5-9.

For more information, see:

- [“Accessing Other LDAP Servers”](#) on page 5-7
- [“Accessing Other LDAP Servers”](#) on page 5-7
- [“Configuring Failover for LDAP Authentication Providers”](#) on page 5-8
- [“Improving the Performance of WebLogic and LDAP Authentication Providers”](#) on page 5-9

Accessing Other LDAP Servers

The LDAP Authentication providers in this release of WebLogic Server are configured to work readily with the SunONE (iPlanet), Active Directory, Open LDAP, and Novell NDS LDAP servers. You can use an LDAP Authentication provider to access other types of LDAP servers. Choose either the LDAP Authentication provider (`LDAPAuthenticator`) or the existing LDAP provider that most closely matches the new LDAP server and customize the existing configuration to match the directory schema and other attributes for your LDAP server.

Dynamic Groups and WebLogic Server

Many LDAP servers have a concept of dynamic groups or virtual groups. These are groups that, rather than consisting of a list of users and groups, contain some policy statements, queries, or code that define the set of users that belong to the group. Even if a group is marked dynamic, users must log out and log back in before any changes in their group memberships take effect. The term dynamic describes the means of defining the group and not any runtime semantics of the group within WebLogic Server.

Configuring Failover for LDAP Authentication Providers

You can configure an LDAP provider to work with multiple LDAP servers and enable failover if one LDAP server is not available. Use the Host attribute (found in the Administration Console on the Configuration → Provider Specific page for the LDAP Authentication provider) to specify the names of the additional LDAP servers. Each host name may include a trailing comma and a port number. In addition, set the Parallel Connect Delay and Connection Timeout attributes for the LDAP Authentication provider:

- **Parallel Connect Delay**—Specifies the number of seconds to delay when making concurrent attempts to connect to multiple servers. An attempt is made to connect to the first server in the list. The next entry in the list is tried only if the attempt to connect to the current host fails. This setting might cause your application to block for an unacceptably long time if a host is down. If the value is greater than 0, another connection setup thread is started after the specified number of delay seconds has passed. If the value is 0, connection attempts are serialized.
- **Connection Timeout**—Specifies the maximum number of seconds to wait for the connection to the LDAP server to be established. If the set to 0, there is no maximum time limit and WebLogic Server waits until the TCP/IP layer times out to return a connection failure. Set to a value over 60 seconds depending upon the configuration of TCP/IP.

The following examples present scenarios that occur when an LDAP Authentication provider is configured for LDAP failover.

LDAP Failover Example 1

In the following scenario, an LDAP Authentication provider is configured with three servers in its Host attribute: `directory.knowledge.com:1050`, `people.catalog.com`, and `199.254.1.2`. The status of the LDAP servers is as follows:

- `directory.knowledge.com:1050` is down
- `people.catalog.com` is up
- `199.254.1.2` is up

WebLogic Server attempts to connect to `directory.knowledge.com`. After 10 seconds, the connect attempt times out and WebLogic Server attempts to connect to the next specified host (`people.catalog.com`). WebLogic Server then uses `people.catalog.com` as the LDAP Server for this connection.

Table 5-1 LDAP Configuration Example 1

LDAP Option	Value
Host	directory.knowledge.com:1050 people.catalog.com 199.254.1.2
Parallel Connect Delay	0
Connect Timeout	10

LDAP Failover Example 2

In the following scenario, WebLogic Server attempts to connect to `directory.knowledge.com`. After 1 second (specified by the `Parallel Connect Delay` attribute), the connect attempt times out and WebLogic Server tries to connect to the next specified host (`people.catalog.com`) and `directory.knowledge.com` at the same time. If the connection to `people.catalog.com` succeeds, WebLogic Server uses `people.catalog.com` as the LDAP Server for this connection. WebLogic Server cancels the connection to `directory.knowledge.com` after the connection to `people.catalog.com` succeeds.

Table 5-2 LDAP Configuration Example 2

LDAP Option	Value
Host	directory.knowledge.com:1050 people.catalog.com 199.254.1.2
Parallel Connect Delay	1
Connect Timeout	10

Improving the Performance of WebLogic and LDAP Authentication Providers

To improve the performance of WebLogic and LDAP Authentication providers:

- Optimize the group membership caches used by the WebLogic and LDAP Authentication providers. See [“Optimizing the Group Membership Caches”](#) on page 5-10.

- Expose the Principal Validator cache for the security realm and increase its thresholds. See [“Optimizing the Principal Validator Cache” on page 5-12](#).
- If you are using the Active Directory Authentication provider, configure it to perform group membership lookups using the `tokenGroups` option. The `tokenGroups` option holds the entire flattened group membership for a user as an array of system ID (SID) values. The SID values are specially indexed in the Active Directory and yield extremely fast lookup response. See [“Configuring the Active Directory Authentication Provider to Improve Performance” on page 5-12](#).

Optimizing the Group Membership Caches

To optimize the group membership caches for WebLogic and LDAP Authentication providers, set the following attributes (found in the Administration Console on the LDAP Authentication provider’s Configuration → Provider Specific and Performance pages):

- **Group Membership Searching**—Controls whether group searches are limited or unlimited in depth. This option controls how deeply to search into nested groups. For configurations that use only the first level of nested group hierarchy, this option allows improved performance during user searches by limiting the search to the first level of the group.
 - If a limited search is defined, `Max Group Membership Search Level` must be defined.
 - If an unlimited search is defined, `Max Group Membership Search Level` is ignored.
- **Max Group Membership Search Level**—Controls the depth of a group membership search if `Group Membership Searching` is defined. Possible values are:
 - 0—Indicates only direct groups will be found. That is, when searching for membership in Group A, only direct members of Group A will be found. If Group B is a member of Group A, the members will not be found by this search.
 - Any positive number—Indicates the number of levels to search. For example, if this option is set to 1, a search for membership in Group A will return direct members of Group A. If Group B is a member of Group A, the members of Group B will also be found by this search. However, if Group C is a member of Group B, the members of Group C will not be found by this search.
- **Enable Group Membership Lookup Hierarchy Caching**—Indicates whether group membership hierarchies found during recursive membership lookup are cached. Each subtree found will be cached. The cache holds the groups to which a group is a member. This setting only applies if `Group Membership` is enabled. By default, it is disabled.

- **Max Group Hierarchies in Cache**—The maximum size of the Least Recently Used (LRU) cache that holds group membership hierarchies. This setting only applies if Enable Group Membership Lookup Hierarchy Caching is enabled.
- **Group Hierarchy Cache TTL**—The number of seconds cached entries stay in the cache. The default is 60 seconds.

In planning your cache settings, bear in mind the following considerations:

- Enabling a cache involves a trade-off of performance and accuracy. Using a cache means that data is retrieved faster, but runs the risk that the data may not be the latest available.
- The time-to-live (TTL) setting how long you are willing to accept potentially stale data. This depends a lot on your particular business needs. If you frequently changes group memberships for users, then a long TTL could mean that group related changes won't show up for a while, and you may want a short TTL. If group memberships almost never change after a user is added, a longer TTL may be fine.
- The cache size is related to the amount of memory you have available, as well as the cache TTL. Consider the number of entries that might be loaded in the span of the TTL, and size the cache in relation to that number. A longer TTL will tend to require a larger cache size.

Configuring Dynamic Groups in the iPlanet Authentication Provider to Improve Performance

Dynamic groups do not list the names of their members. Instead, the membership of the dynamic group is constructed by matching user attributes. Because group membership needs to be computed dynamically for dynamic groups, there is a risk of performance problems for large groups. Configuring the iPlanet Authentication provider appropriately can improve performance where dynamic groups are involved.

In the iPlanet Authentication provider, the User Dynamic Group DN Attribute attribute specifies the attribute of an LDAP user object that specifies the distinguished names (DNs) of dynamic groups to which this user belongs. If such an attribute does not exist, WebLogic Server determines if a user is a member of a group by evaluating the URLs on the dynamic group. By default, User Dynamic Group DN Attribute is null. If you set User Dynamic Group DN Attribute to some other value, to improve performance set the following attributes for the iPlanet Authentication provider:

```
UserDynamicGroupDNAttribute="wlsMemberOf "
```

```
DynamicGroupNameAttribute="cn"
```

```
DynamicGroupObjectClass=" "
```

```
DynamicMemberURLAttribute=" "
```

To set these attributes in the Administration Console:

1. Expand Security Realms-->*realm name*-->Providers-->Authentication.
2. On the Provider Specific tab for your iPlanet Authentication provider, set User Dynamic Group DN Attribute. Set Dynamic Group Object Class and Dynamic Member URL Attribute to null (delete anything in the fields) and leave Dynamic Group Name Attribute set to `cn`.

Optimizing the Principal Validator Cache

To improve the performance of a WebLogic or LDAP Authentication provider, the settings of the cache used by the WebLogic Principal Validation provider can be increased as appropriate. The Principal Validator cache used by the WebLogic Principal Validation provider caches signed `WLSAbstractPrincipals`. To optimize the performance of the Principal Validator cache, set these attributes for your security realm (found in the Administration Console on the Configuration → Performance page for the security realm):

- **Enable WebLogic Principal Validator Cache**—Indicates whether the WebLogic Principal Validation provider uses a cache. This setting only applies if Authentication providers in the security realm use the WebLogic Principal Validation provider and `WLSAbstractPrincipals`. By default, it is enabled.
- **Max WebLogic Principals In Cache**—The maximum size of the Last Recently Used (LRU) cache used for validated `WLSAbstractPrincipals`. The default setting is 500. This setting only applies if Enable WebLogic Principal Validator Cache is enabled.

Configuring the Active Directory Authentication Provider to Improve Performance

To configure an Active Directory Authentication provider to use the `tokenGroups` option, set the following attributes (found in the Administration Console on the Active Directory Authentication provider's Configuration → Provider Specific page):

- **Use Token Groups for Group Membership Lookup**—Indicates whether to use the Active Directory `tokenGroups` lookup algorithm instead of the standard recursive group membership lookup algorithm. By default, this option is not enabled.

Note: Access to the `tokenGroups` option is required (meaning, the user accessing the LDAP directory must have privileges to read the `tokenGroups` option and the `tokenGroups` option must be in the schema for user objects).

- **Enable SID to Group Lookup Caching**—Indicates whether or not SID-to-group name lookup results are cached. This setting only applies if the Use Token Groups for Group Membership Lookup option is enabled.
- **Max SID To Group Lookups In Cache**—The maximum size of the Least Recently Used (LRU) cache for holding SID to group lookups. This setting applies only if both the Use Token Groups for Group Membership Lookup and Enable SID to Group Lookup Caching options are enabled.

Configuring RDBMS Authentication Providers

In WebLogic Server, an RDBMS Authentication provider is a username/password based Authentication provider that uses a relational database (rather than an LDAP directory) as its data store for user, password, and group information. WebLogic Server includes these RDBMS Authentication providers:

- **SQL Authenticator**—Uses a SQL database and allows both read and write access to the database. This Authentication provider is configured by default with a typical SQL database schema, which you can configure to match your database's schema. See [“Configuring the SQL Authentication Provider” on page 5-14](#).
- **Read-only SQL Authenticator**—Uses a SQL database and allows only read access to the database. For write access, you use the SQL database's own interface, not the WebLogic security provider. See [“Configuring the Read-Only SQL Authenticator” on page 5-15](#).
- **Custom RDBMS Authenticator**—Requires you to write a plug-in class. This may be a better choice if you want to use a relational database for your authentication data store, but the SQL Authenticator's schema configuration is not a good match for your existing database schema. See [“Configuring the Custom DBMS Authenticator” on page 5-15](#).

For information about adding an RDBMS Authentication provider to your security realm, see [Configure Authentication and Identity Assertion providers](#) in the *Administration Console Online Help*. Once you have created an instance of the RDBMS Authentication provider, configure it on the RDBMS Authentication provider's Configuration → Provider Specific page in the Administration Console.

Common RDBMS Authentication Provider Attributes

All three RDBMS Authentication providers include these configuration options.

Data Source Attribute

The Data Source Name specifies the WebLogic Server data source to use to connect to the database.

Group Searching Attributes

The Group Membership Searching and Max Group Membership Search Level attributes specify whether recursive group membership searching is unlimited or limited, and if limited, how many levels of group membership can be searched. For example, if you specify that Group Membership Searching is LIMITED, and the Max Group Membership Search Level is 0, then the RDBMS Authentication providers will find only groups that the user is a direct member of. Specifying a maximum group membership search level can greatly increase authentication performance in certain scenarios, since it may reduce the number of DBMS queries executed during authentication. However, you should only limit group membership search if you can be certain that the group memberships you require are within the search level limits you specify.

Group Caching Attributes

You can improve the performance of RDBMS Authentication providers by caching the results of group hierarchy lookups. Use of this cache can reduce the frequency with which the RDBMS Authentication provider needs to access the database. In the Administration Console, you can use the Performance page for your Authentication provider to configure the use, size, and duration of this cache. See [Security Realms: Security Providers: SQL Authenticator: Performance](#) in the *Administration Console Online Help*.

Configuring the SQL Authentication Provider

For detailed information about configuring a SQL Authentication provider, see [Security Realms: Security Providers: SQL Authenticator: Provider Specific](#) in the *Administration Console Online Help*. In addition to the attributes described in “[Common RDBMS Authentication Provider Attributes](#)” on page 5-13, the SQL Authentication provider has the following configurable attributes.

Password Attributes

The following attributes govern how the RDBMS Authentication provider and its underlying database handle user passwords:

- Plaintext Passwords Enabled

- Password Style Retained
- Password Style
- Password Algorithm

SQL Statement Attributes

SQL statement attributes specify the SQL statements used by the provider to access and edit the username, password, and group information in the database. With the default values in the SQL statement attributes, it is assumed that the database schema includes the following tables:

- users (username, password, [description])
- groupmembers (group name, group member)
- groups (group name, group description)

Note: The tables referenced by the SQL statements must exist in the database; the provider will not create them. You can modify these attributes as needed to match the schema of your database. However, if your database schema is radically different from this default schema, you may need to use a Custom DBMS Authentication provider instead.

Configuring the Read-Only SQL Authenticator

For detailed information about configuring a Read-Only SQL Authentication provider, see [Security Realms: Security Providers: Read-Only SQL Authenticator: Provider Specific](#) in the *Administration Console Online Help*. In addition to the attributes described in “[Common RDBMS Authentication Provider Attributes](#)” on page 5-13, the Read-Only SQL Authentication provider’s configurable attributes include attributes that specify the SQL statements used by the provider to list the username, password, and group information in the database. You can modify these attributes as needed to match the schema of your database.

Configuring the Custom DBMS Authenticator

The Custom DBMS Authentication provider, like the other RDBMS Authentication providers, uses a relational database as its data store for user, password, and group information. Use this provider if your database schema does not map well to the SQL schema expected by the SQL Authenticator. In addition to the attributes described in “[Common RDBMS Authentication Provider Attributes](#)” on page 5-13, the Custom DBMS Authentication provider’s configurable attributes include the following.

Plug-In Class Attributes

A Custom DBMS Authentication provider requires that you write a plug-in class that implements the

`webllogic.security.providers.authentication.CustomDBMSAuthenticatorPlugin` interface. The class must exist in the CLASSPATH and must be specified in the Plug-in Class Name attribute for the Custom DBMS Authentication provider. Optionally, you can use the Plugin Properties attribute to specify values for properties defined by your plug-in class.

Configuring a Windows NT Authentication Provider

The Windows NT Authentication provider uses account information defined for a Windows NT domain to authenticate users and groups and to permit Windows NT users and groups to be listed in the WebLogic Server Administration Console.

To use the Windows NT Authentication provider, create the provider in the Administration Console. In most cases, you should not need to do anything more to configure this Authentication provider. Depending on how your Windows NT domains are configured, you may want to set the Domain Controllers and Domain Controller List attributes, which control how the Windows NT Authentication provider interacts with the Windows NT domain.

Note: The Windows NT Authentication provider is deprecated as of WebLogic Server 10.0. Use one or more other supported authentication providers instead.

Domain Controller Settings

Username in a Windows NT domain can take several different forms. You may need to configure the Windows NT Authentication provider to match the form of usernames you expect your users to sign on with. A simple username is one that gives no indication of the domain, such as `smith`. Compound usernames combine a username with a domain name and may take a form like `domain\smith` or `smith@domain`.

If the local machine is not part of a Microsoft domain, then no changes to the Domain Controllers and Domain Controller List attributes are needed. On a stand-alone machine, the users and groups to be authenticated are defined only on that machine.

If the local machine is part of a Microsoft domain and is the domain controller for the local domain, then no changes are needed to the Domain Controller List attribute. Users defined on the local machine and the domain are the same in this case, so you can use the default Domain Controllers setting.

If the local machine is part of a Microsoft domain, but is not the domain controller for the local domain, then a simple username might be found on either the local machine or in the domain. In this case, consider the following:

- Do you want to prevent the users and groups from the local machine from being displayed in the Console when the local machine is part of a Microsoft domain?
- Do you want users from the local machine to be found and authenticated when a simple username is entered?

If the answer to either question is yes, then set the Domain Controller attribute to `DOMAIN`.

If you have multiple trusted domains, you may need to set the Domain Controller attribute to `LIST` and specify a Domain Controller List. Do this if:

- You require the users and groups for other trusted domains to be visible in the Console, or
- You expect that your users will be entering simple usernames and expect them to be located in the trusted domains (that is, users will sign on with a simple username like enter `smith`, not `smith@domain` or `domain\Smith`).

If either of these situations is the case, then set the Domain Controllers attribute to `LIST` and specify the names of the domain controllers in the Domain Controller List attribute for the trusted domains that you want to be used. Consider also whether to use explicit names for the local machine and local domain controller or if you want to use placeholders in the list for those. You can use the following placeholders in the Domain Controller List attribute:

- `[Local]`
- `[LocalAndDomain]`
- `[Domain]`

LogonType Setting

The proper value of the `LogonType` attribute in the Windows NT Authentication provider depends on the Windows NT logon rights of the users that you want to be able to authenticate:

- If users have the “logon locally” right assigned to them on the machines that will run WebLogic Server, then use the default value, `interactive`.
- If users have the “Access this computer from the Network” right assigned to them, then change the `LogonType` attribute to `network`.

You must assign one of these rights to users in the Windows NT domain or else the Windows NT Authentication provider will not be able to authenticate any users.

UPN Names Settings

UPN style usernames can take the form `user@domain`. You can configure how the Windows NT Authentication provider handles usernames that include the `@` character, but which may not be UPN names, by setting the `mapUPNNames` attribute in the Windows NT Authentication provider.

If none of your Windows NT domains or local machines have usernames that contain the `@` character other than UPN usernames, then you can use the default value of the `mapUPNNames` attribute, `FIRST`. However, you may want to consider changing the setting to `ALWAYS` in order to reduce the amount of time it takes to detect authentication failures. This is especially true if you have specified a long domain controller list.

If your Windows NT domains do permit non-UPN usernames with the `@` character in them, then:

- if a username with the `@` character is more likely to be a UPN username than a simple username, set the `mapUPNNames` attribute to `FIRST`.
- if a username with the `@` character is more likely to be a simple username than a UPN username, set the `mapUPNNames` attribute to `LAST`.
- if a username is never in UPN format, set the `mapUPNNames` attribute to `NEVER`.

Configuring the SAML Authentication Provider

The SAML Authentication provider may be used in conjunction with the SAML 1.1 or SAML 2.0 Identity Assertion provider to do the following:

- Allow virtual users to log in via SAML
If true, the SAML Identity Asserter will create user/group principals, with the possible result that the user is logged in as a virtual user — a user that does not correspond to any locally-known user.
- If the SAML Authentication provider is configured to run before other authentication providers, and has a JAAS Control Flag set to `SUFFICIENT`, this provider creates an authenticated subject using the user name and groups retrieved from a SAML assertion by the SAML Identity Assertion provider V2 or the SAML 2.0 Identity Assertion provider.

If the SAML Authentication provider is not configured, or if another authentication provider (e.g., the default LDAP Authentication provider) is configured before it and its JAAS Control

Flag set is set to SUFFICIENT, then the user name returned by the SAML Identity Assertion provider is validated by the other authentication provider. In the case of the default LDAP Authentication provider, authentication fails if the user does not exist in the identity directory.

If you want groups from a SAML assertion, you must configure the SAML Authentication provider even if you want the LDAP Authentication provider to verify the user's existence. Otherwise, the groups with which the user is associated is derived from the LDAP directory and not with the groups in the assertion.

The SAML Authentication provider creates a subject only for users whose identities are asserted by either the SAML Identity Assertion provider V2 or SAML 2.0 Identity Assertion provider. The SAML Authentication provider ignores all other authentication or identity assertion requests

Configuring the Password Validation Provider

WebLogic Server includes a Password Validation provider, which manages and enforces a set of configurable password composition rules. When configured in a security realm, the Password Validation provider is automatically invoked by a supported authentication provider whenever a password is created or updated for a user in that realm. The Password Validation provider then performs a check to determine whether the password meets the criteria established by the composition rules, and the password is accepted or rejected as appropriate.

The following authentication providers can be used with the Password Validation provider:

- WebLogic Authentication provider
- SQL Authenticator provider
- LDAP Authentication provider
- Active Directory Authentication provider
- iPlanet Authentication provider
- Novell Authentication provider
- Open LDAP Authentication provider

The Password Validation provider may be configured only via the WebLogic Scripting Tool (WLST). This provider cannot be configured via the WebLogic Administration Console. The following sections describe the composition rules that may be configured and explain how to create and configure an instance of the Password Validation provider in a security realm:

- [“Password Composition Rules for the Password Validation Provider”](#) on page 5-20
- [“Using the Password Validation Provider with the WebLogic Authentication Provider”](#) on page 5-23
- [“Using WLST to Create and Configure the Password Validation Provider”](#) on page 5-24

Password Composition Rules for the Password Validation Provider

The password composition rules you can configure for the Password Validation provider include the following:

- Whether the password may contain the user’s name, or the reverse of that name
- A minimum or maximum password length (composition rules may specify both a minimum and maximum length)
- Whether and how many of the following characters must be in the password:
 - Numeric characters
 - Lowercase alphabetic characters
 - Uppercase alphabetic characters
 - Non-alphanumeric characters (e.g., parentheses or asterisks)

[Table 5-3](#) describes each of the password composition rules you can configure, identifies the default values of those rules, and recommends settings you can use to create strong passwords that cannot be easily determined.

Note: Setting password composition rules is only one component of hardening the WebLogic Server environment against brute-force password attacks. To protect user accounts, you should also configure user lockout. User lockout specifies the number of incorrect passwords that may be entered within a given interval of time before the user is locked out of his or her account. For more information, see [“Protecting User Accounts”](#) on page 13-9.

Table 5-3 Password Composition Rules and Default Values

The following rule name . . .	Specifies the following composition rule . . .	Default Value
<code>RejectEqualOrContainUsername</code>	Whether the password may contain the username. Validation is not case sensitive. If the value is set to <code>true</code> , the password may not consist of, nor contain, the username. Recommendation: <code>true</code>	<code>false</code>
<code>RejectEqualOrContainReverseUsername</code>	Whether the password may contain a reverse of the username (e.g., Ramgad instead of Dagmar). If the value is set to <code>true</code> , the password may not consist of, nor contain, a reverse of the username. Recommendation: <code>true</code>	<code>false</code>
<code>MaxPasswordLength</code>	The maximum number of characters that the password may contain. In order to be accepted, the password may not contain a greater number of characters than the value specified. Specifying 0 results in no restriction on password length. Recommendation: 12	0 (zero)
<code>MinPasswordLength</code>	The minimum number of characters that the password must contain. In order to be accepted, the password must contain at least as many characters as the value specified. Recommendation: 6 Note: If the WebLogic Authentication provider is configured in the realm, make sure that this number is consistent with the one configured for that provider. See “Using the Password Validation Provider with the WebLogic Authentication Provider” on page 5-23.	0 (zero)
<code>MaxInstancesOfAnyCharacter</code>	The maximum instances that any one character may appear in the password. For example, if this value is set to 2, the password <code>alabaster</code> is rejected. Specifying 0 results in no restriction. Recommendation: 4	0 (zero)

Table 5-3 Password Composition Rules and Default Values (Continued)

The following rule name . . .	Specifies the following composition rule . . .	Default Value
MaxConsecutiveCharacters	<p>The maximum number of characters that may appear consecutively in the password. Specifying 0 results in no restriction.</p> <p>Recommendation: 3</p>	0 (zero)
MinAlphabeticCharacters	<p>The minimum number of alphabetic characters that must appear in the password. A valid value for this rule must be greater than or equal to 0 (zero).</p> <p>Recommendation: 1</p>	0 (zero)
MinNumericCharacters	<p>The minimum number of numeric characters that must appear in the password. A valid value for this rule must be greater than or equal to 0 (zero).</p> <p>Recommendation: 1</p>	0 (zero)
MinLowercaseCharacters	<p>The minimum number of lowercase alphabetic characters that must appear in the password. A valid value for this rule must be greater than or equal to 0 (zero).</p> <p>Recommendation: 1</p>	0 (zero)
MinUppercaseCharacters	<p>The minimum number of uppercase alphabetic characters that must appear in the password. A valid value for this rule must be greater than or equal to 0 (zero).</p> <p>Recommendation: 1</p>	0 (zero)
MinNonAlphanumericCharacters	<p>The minimum number of non-alphanumeric characters (also known as special characters, such as %, *, #, or }) that must appear in the password. A valid value for this rule must be greater than or equal to 0 (zero).</p> <p>Recommendation: 1</p>	0 (zero)

For information about setting these composition rules, see [“Using WLST to Create and Configure the Password Validation Provider” on page 5-24.](#)

Using the Password Validation Provider with the WebLogic Authentication Provider

By default, the WebLogic Authentication provider requires a minimum password length of 8 characters. However, the minimum password length enforced by this provider can be customized. If the WebLogic Authentication provider and Password Validation provider are both configured in the security realm, and you attempt to create a password that does not meet the minimum length enforced by the WebLogic Authentication provider, an error is generated. For example, the following message is displayed in the Administration Console:

```
Error [Security:090285]password must be at least 8 characters long
Error Errors must be corrected before proceeding.
```

If the WebLogic Authentication provider rejects a password because it does not meet the minimum length requirement, the Password Validation provider is not called. To ensure that the Password Validator is always used in conjunction with the WebLogic Authentication provider, make sure that the minimum password length is the same for both providers.

Using the Administration Console, you can set the minimum password length for WebLogic Authentication provider by completing the following steps:

1. If you have not already done so, in the Change Center of the Administration Console, click **Lock & Edit**.
2. In the left pane, select **Security Realms** and click the name of the realm you are configuring (for example, *myrealm*).
3. Select **Providers** → **Authentication** and click **DefaultAuthenticator**.
4. Selected **Configuration** → **Provider Specific** and enter the minimum password length in the field labeled Minimum Password Length.
5. Click **Save** to save your changes.
6. To activate these changes, in the Change Center, click **Activate Changes**.

For information about how to set the minimum password length in the Password Validation provider, see [“Using WLST to Create and Configure the Password Validation Provider”](#) on page 5-24.

Using WLST to Create and Configure the Password Validation Provider

The Password Validation provider can be administered in the security realm only via WLST. You may create and configure the Password Validation provider from a single WLST script, or you may have separate scripts that perform these functions separately. The following topics explain how to do this, providing sample WLST code snippets:

- [“Creating an Instance of the Password Validation Provider” on page 5-24](#)
- [“Specifying the Password Composition Rules” on page 5-25](#)

Creating an Instance of the Password Validation Provider

[Listing 5-1](#) shows an example of WLST code that creates an instance of the Password Validation provider in the security realm. This code does the following:

1. Gets the current realm and Password Validation provider.
2. Determines whether an instance of the Password Validator provider has been created:
 - If the provider has been created, the script displays a message confirming its presence.
 - If the provider has not been created, the script creates it in the security realm and displays a message indicating that it has been created.

Listing 5-1 Creating the System Password Validator

```
edit()
startEdit()

realm = cmo.getSecurityConfiguration().getDefaultRealm()
pwdvalidator = realm.lookupPasswordValidator('systemPasswordValidator')

if pwdvalidator:
    print 'Password Validator provider is already created'

else:
    # Create SystemPasswordValidator
    syspwdValidator = realm.createPasswordValidator('systemPasswordValidator',
        'com.bea.security.providers.authentication.passwordvalidator.SystemPasswordValidator')
    print "--- Creation of system Password Validator succeeded!"

save()
activate()
```


Specifying the Password Composition Rules

[Listing 5-2](#) shows an example of WLST code that sets the composition rules for the Password Validation provider. For information about the rules attributes set in this script, see [Table 5-3](#).

Listing 5-2 Configuring the Password Composition Rules

```
edit()
startEdit()

# Configure SystemPasswordValidator
try:
    pwdvalidator.setMinPasswordLength(8)
    pwdvalidator.setMaxPasswordLength(12)
    pwdvalidator.setMaxConsecutiveCharacters(3)
    pwdvalidator.setMaxInstancesOfAnyCharacter(4)
    pwdvalidator.setMinAlphabeticCharacters(1)
    pwdvalidator.setMinNumericCharacters(1)
    pwdvalidator.setMinLowercaseCharacters(1)
    pwdvalidator.setMinUppercaseCharacters(1)
    pwdvalidator.setMinNonAlphanumericCharacters(1)
    pwdvalidator.setRejectEqualOrContainUsername(true)
    pwdvalidator.setRejectEqualOrContainReverseUsername(true)
    print " --- Configuration of SystemPasswordValidator complete ---"
except Exception,e:
    print e

save()
activate()
```

Configuring Identity Assertion Providers

If you are using perimeter authentication, you need to use an Identity Assertion provider. In perimeter authentication, a system outside of WebLogic Server establishes trust through tokens (as opposed to simple authentication, where WebLogic Server establishes trust through usernames and passwords). An Identity Assertion provider verifies the tokens and performs whatever actions are necessary to establish validity and trust in the token. Each Identity Assertion provider is designed to support one or more token formats.

WebLogic Server includes the following Identity Assertion providers:

- WebLogic Identity Asserter
- LDAP X.509 Identity Asserter
- Negotiate Identity Asserter
- SAML Identity Asserter (for SAML 1.1)
- SAML 2.0 Identity Asserter

Multiple Identity Assertion providers can be configured in a security realm, but none are required. Identity Assertion providers can support more than one token type, but only one token type per Identity Assertion provider can be active at a given time. In the Active Type field on the Provider Specific configuration page in the Administration Console, define the active token type. The WebLogic Identity Assertion provider supports identity assertion with X.509 certificates and CORBA Common Secure Interoperability version 2 (CSI v2). If you are using CSI v2 identity assertion, define the list of client principals in the Trusted Principals field.

If multiple Identity Assertion providers are configured in a security realm, they can all support the same token type. However, the token can be active for only one provider at a time.

With the WebLogic Identity Assertion provider, you can use a user name mapper to map the tokens authenticated by the Identity Assertion provider to a user in the security realm. For more information about configuring a user name mapper, see [“Configuring a WebLogic Credential Mapping Provider” on page 4-16](#).

If the authentication type in a Web application is set to `CLIENT-CERT`, the Web Application container in WebLogic Server performs identity assertion on values from request headers and cookies. If the header name or cookie name matches the active token type for the configured Identity Assertion provider, the value is passed to the provider.

The Base64 Decoding Required value on the Provider Specific page determines whether the request header value or cookie value must be Base64 Decoded before sending it to the Identity Assertion provider. The setting is enabled by default for purposes of backward compatibility; however, most Identity Assertion providers will disable this option.

For more information see [Configure Authentication and Identity Assertion providers](#) in the *Administration Console Online Help*. In addition, see the following sections:

- [“How an LDAP X509 Identity Assertion Provider Works” on page 5-27](#)
- [“Configuring an LDAP X509 Identity Assertion Provider: Main Steps” on page 5-28](#)

- [“Configuring a Negotiate Identity Assertion Provider” on page 5-29](#)
- [“Configuring a SAML Identity Assertion Provider for SAML 1.1” on page 5-30](#)
- [“Configuring a SAML 2.0 Identity Assertion Provider for SAML 2.0” on page 5-31](#)
- [“Ordering of Identity Assertion for Servlets” on page 5-37](#)
- [“Configuring Identity Assertion Performance in the Server Cache” on page 5-38](#)
- [“Configuring a User Name Mapper” on page 5-39](#)
- [“Configuring a Custom User Name Mapper” on page 5-40](#)

How an LDAP X509 Identity Assertion Provider Works

The LDAP X509 Identity Assertion provider receives an X509 certificate, looks up the LDAP object for the user associated with that certificate, ensures that the certificate in the LDAP object matches the presented certificate, and then retrieves the name of the user from the LDAP object.

The LDAP X509 Identity Assertion provider works in the following manner:

1. An application is set up to use perimeter authentication (in other words, users or system process use tokens to assert their identity).
2. As part of the SSL handshake, the application presents its certificate. The Subject DN in the certificate can be used to locate the object that represents the user in the LDAP server. The object contains the user's certificate and name.
3. The LDAP X509 Identity Assertion provider uses the certificate in the Subject DN to construct an LDAP search to find the LDAP object for the user in the LDAP server. It gets the certificate from that object, ensures it matches the certificate it holds, and retrieves the name of the user.
4. The username is passed to the authentication providers configured in the security realm. The authentication providers ensure the user exists and locate the groups to which the user belongs.

Configuring an LDAP X509 Identity Assertion Provider: Main Steps

Typically, if you use the LDAP X509 Identity Assertion provider, you also need to configure an LDAP Authentication provider that uses an LDAP server. The authentication provider ensures the user exists and locates the groups to which the user belongs. You should ensure both providers are properly configured to communicate with the same LDAP server.

To use an LDAP X509 Identity Assertion provider:

1. Obtain certificates for users and put them in an LDAP Server. See [Chapter 11, “Configuring Identity and Trust.”](#)

A correlation must exist between the Subject DN in the certificate and the location of the object for that user in the LDAP server. The LDAP object for the user must also include configuration information for the certificate and the username that will be used in the Subject.

2. In your security realm, configure an LDAP X509 Identity Assertion provider. See [Configure Authentication and Identity Assertion providers](#) in the *Administration Console Online Help*.
3. In the WebLogic Server Administration Console, configure the LDAP X509 Identity Assertion provider to find the LDAP object for the user in the LDAP directory given the certificate’s Subject DN.
4. Configure the LDAP X509 Identity Assertion provider to search the LDAP server to locate the LDAP object for the user. This requires the following pieces of data.
 - A base LDAP DN from which to start searching. The Certificate Mapping option for the LDAP X509 Identity Assertion provider tells the identity assertion provider how to construct the base LDAP DN from the certificate’s Subject DN. The LDAP object must contain an attribute that holds the certificate.
 - A search filter that only returns LDAP objects that match a defined set of options. The filter narrows the LDAP search. Configure User Filter Search to construct a search filter from the certificate’s Subject DN.
 - Where in the LDAP directory to search for the base LDAP DN. The LDAP X509 Identity Assertion provider searches recursively (one level down). This value must match the values in the certificate’s Subject DN.
5. Configure the Certificate Attribute attribute of the LDAP X509 Identity Assertion provider to specify how the LDAP object for the user holds the certificate. The LDAP object must contain an attribute the holds the certificate.

6. Configure the User Name Attribute attribute of the LDAP X509 Identity Assertion provider to specify which of the LDAP object's attributes holds the username that should appear in the Subject DN.
7. Configure the LDAP server connection for the LDAP X509 Identity Assertion provider. The LDAP server information should be the same as the information defined for the LDAP Authentication provider configured in this security realm.
8. Configure an LDAP Authentication provider for use with the LDAP X509 Identity Assertion provider. The LDAP server information should be the same the information defined for the LDAP X509 Identity Assertion provider configured in Step 7. See [“Configuring LDAP Authentication Providers” on page 5-5.](#)

Configuring a Negotiate Identity Assertion Provider

The Negotiate Identity Assertion provider enables single sign-on (SSO) with Microsoft clients. The identity assertion provider decodes Simple and Protected Negotiate (SPNEGO) tokens to obtain Kerberos tokens, validates the Kerberos tokens, and maps Kerberos tokens to WebLogic users. The Negotiate Identity Assertion provider utilizes the Java Generic Security Service (GSS) Application Programming Interface (API) to accept the GSS security context via Kerberos.

The Negotiate Identity Assertion provider is an implementation of the Security Service Provider Interface (SSPI) as defined by the WebLogic Security Framework and provides the necessary logic to authenticate a client based on the client's SPNEGO token.

For information about adding a Negotiate Identity Assertion provider to a security realm, see [Configure Authentication and Identity Assertion providers](#) in the *Administration Console Online Help*. For information about using the Negotiate Identity Assertion provider with Microsoft client SSO, see [Chapter 6, “Configuring Single Sign-On with Microsoft Clients.”](#)

Table 5-4 Negotiate Identity Asserter Attributes

Attribute	Description
Form Based Negotiation Enabled	Indicates whether the Negotiate Identity Assertion provider and servlet filter should negotiate when a Web application is configured for FORM authentication.

Table 5-4 Negotiate Identity Asserter Attributes

Attribute	Description
Active Types	<p>The token type this Negotiate Identity Assertion provider uses for authentication. Available token types are <code>Authorization.Negotiate</code> and <code>WWW-Authenticate.Negotiate</code>.</p> <p>Ensure no other identity assertion provider configured in the same security realm has this attribute set to <code>X509</code>.</p>

Configuring a SAML Identity Assertion Provider for SAML 1.1

The SAML Identity Assertion provider acts as a consumer of SAML 1.1 security assertions, allowing WebLogic Server to act as a destination site for using SAML 1.1 for single sign-on. The SAML Identity Assertion provider validates SAML 1.1 assertions by checking the signature and validating the certificate for trust in the certificate registry maintained by the provider. If so, identity is asserted based on the `AuthenticationStatement` contained in the assertion. The SAML Identity Assertion provider can also ensure that the assertion has not been previously used. The SAML Identity Assertion provider must be configured if you want to deploy a SAML Assertion Consumer Service on a server instance.

This release of WebLogic Server includes two SAML Identity Assertion providers for SAML 1.1. SAML Identity Asserter Version 2 provides greatly enhanced configuration options and is recommended for new deployments. SAML Identity Asserter Version 1 has been deprecated in WebLogic Server 9.1. A security realm can have not more than one SAML Identity Assertion provider, and if the security realm has both a SAML Identity Assertion provider and a SAML Credential Mapping provider, both must be of the same version. Do not use a Version 1 SAML provider in the same security realm as a Version 2 SAML provider. For information about configuring the SAML Identity Assertion provider Version 1, see [Configuring a SAML Identity Assertion Provider](#) in the WebLogic Server 9.0 documentation.

For information about how to use the SAML Identity Assertion provider in a SAML single sign-on configuration, see [Chapter 7, “Configuring Single Sign-On with Web Browsers and HTTP Clients.”](#) For general information about SAML support in WebLogic Server, see [Security Assertion Markup Language \(SAML\)](#) in *Understanding WebLogic Security*.

Asserting Party Registry

When you configure WebLogic Server to act as a consumer of SAML security assertions, you need to register the parties whose SAML assertions will be accepted. For each SAML Asserting Party, you can specify the SAML profile used, details about the Asserting Party, and the attributes expected in assertions received from the Asserting Party. For information, see:

- [“Configuring Asserting Parties” on page 7-7 in Chapter 7, “Configuring Single Sign-On with Web Browsers and HTTP Clients”](#) in this guide.
- [Configure a SAML Asserting Party](#) in the *Administration Console Online Help*.

Certificate Registry

The SAML Identity Assertion provider maintains a registry of trusted certificates. Whenever a certificate is received, it is checked against the certificates in the registry for validity. For each Asserting Party, the following certificates from that partner are contained in this registry:

- The certificate used for validating the signature of assertions received from this Asserting Party.
- The certificate used for verifying signatures on SAML protocol elements from this Asserting Party. This certificate must be set for the Browser/POST profile.
- The TLS/SSL certificate used for verifying trust in the Asserting Party when that partner is retrieving an artifact from the Assertion Retrieval Service (ARS) via an SSL connection.

You can add trusted certificates to the certificate registry through the Administration Console:

1. In the Console, navigate to the Security Realms → *your realm* → Providers → Authentication page.
2. Click the name of the SAML Identity Assertion provider and open the Management → Certificates page

On the Management → Certificates page, you can add, view, or delete certificates from the registry.

Configuring a SAML 2.0 Identity Assertion Provider for SAML 2.0

The SAML 2.0 Identity Assertion provider acts as a consumer of SAML 2.0 security assertions, allowing WebLogic Server to act as a Service Provider for the following:

- Web single sign-on
- WebLogic Web Services Security: accepting SAML tokens for identity through the use of the appropriate WS-SecurityPolicy assertions

The SAML 2.0 Identity Assertion provider does the following:

- Validates SAML 2.0 assertions by checking the signature and validating the certificate for trust based on data configured for the partner. The SAML 2.0 Identity Assertion provider then extracts the identity information contained in the assertion, and maps it to a local subject in the security realm.
- Optionally, extracts attribute information contained in an assertion that the SAML Authentication provider, if configured in the security realm, can use to determine the local groups in which the mapped subject belongs. (For more information, see “[Configuring the SAML Authentication Provider](#)” on page 5-18.)
- Optionally, verifies that an assertion’s specified lifespan and re-use settings are properly valid, rejecting the assertion if it is expired or is not available for reuse.

Configuration of the SAML 2.0 Identity Assertion provider is controlled by setting attributes on the `SAML2IdentityAsserterMBean`. You can access the `SAML2IdentityAsserterMBean` using the WebLogic Scripting Tool (WLST), or through the Administration Console by using the Security Realms → *RealmName* → Providers → Authentication page and creating or selecting `SAML2IdentityAsserter`. The `SAML2IdentityAsserterMBean` is described at the following location:

http://e-docs.bea.com/wls/docs103/saml2_javadocs/com/bea/security/saml2/providers/SAML2IdentityAsserterMBean.html

For information about how to use the SAML 2.0 Identity Assertion provider in a SAML single sign-on configuration, see [Chapter 7, “Configuring Single Sign-On with Web Browsers and HTTP Clients.”](#) For general information about SAML support in WebLogic Server, see [Security Assertion Markup Language \(SAML\)](#) in *Understanding WebLogic Security*. For information about using the SAML 2.0 Identity Assertion provider in Web Service Security, see “[Using Security Assertion Markup Language \(SAML\) Tokens For Identity](#)” in *Securing WebLogic Web Services*.

Identity Provider Partners

When you configure WebLogic Server to act as a Service Provider, you create and configure the Identity Provider partners from whom SAML 2.0 assertions are received and validated.

Configuring an Identity Provider partner consists of establishing basic information about that partner, such as the following:

- Partner name and general description
- Name mapper class to be used with this partner
- Whether to consume attribute statements included in assertions received from this partner
- Whether the identities contained in assertions received from this partner should be mapped to virtual users
- Certificates used for validating signed assertions received from this partner

The specific information you establish depends upon whether you are configuring the partner for web single sign-on or web services. Configuring a web single sign-on Identity Provider partner also involves importing that partner's metadata file and establishing additional basic information about that partner, such as the following:

- Redirect URIs, which are URLs that, when invoked by an unauthenticated user, cause the user request to be redirected to that Identity Provider partner for authentication
- Whether SAML artifact requests received from this partner must be signed
- How SAML artifacts should be delivered to this partner

For details about configuring web single sign-on Identity Provider partners, see:

- [“Create and Configure Web Single Sign-On Identity Provider Partners” on page 7-20](#)
- [Create a SAML 2.0 Web Single Sign-on Identity Provider partner](#) in the *Administration Console Online Help*

Configuring a web service Identity Provider partner does not use a metadata file, but does consist of establishing the following information about that partner:

- Issuer URI, which is a string that uniquely identifies this Identity Provider partner, distinguishing it from other partners in your SAML federation
- Audience URIs, which specify an audience restriction to be included in assertions received from this partner

In WebLogic Server, the Audience URI attribute is overloaded to also include the partner lookup string, which is required by the web service run time to discover the partner. See [“Partner Lookup Strings Required for Web Service Partners” on page 5-34](#).

- Custom name mapper class that overrides the default name mapper and that is to be used specifically with this partner

For more information about configuring web service Service Provider partners, see [Create a SAML 2.0 Web Service Identity Provider partner](#) in the *Administration Console Online Help*.

Partner Lookup Strings Required for Web Service Partners

For web service Identity Provider partners, you also configure Audience URIs. In WebLogic Server, the Audience URI attribute is overloaded to perform two distinct functions:

- Specify an audience restriction consisting of a target URL, per the OASIS SAML 2.0 specification.
- Contain a partner lookup string, which is required at run time by WebLogic Server to discover the Identity Provider partner for which a SAML 2.0 assertion needs to be validated.

The partner lookup string specifies an endpoint URL, which is used for partner lookup and can optionally also serve as an Audience URI restriction that must be included in the assertion received from this Identity Provider partner.

Note: You must configure a partner lookup string for an Identity Provider partner so that partner can be discovered at run time by the web service run time.

Lookup String Syntax

The partner lookup string has the following syntax:

```
[target:char:]<endpoint-url>
```

In this syntax, `target:char:` is a prefix that designates the partner lookup string, where `char` represents one of three special characters: a hyphen, plus sign, or asterisk (-, +, or *). This prefix determines how partner lookup is performed, as described in [Table 5-5](#).

Note: A WebLogic Server instance that is configured in the role of Service Provider always strips off the transport, host, and port portions of an endpoint URL that is passed in to the SAML 2.0 Identity Assertion provider. Therefore, the endpoint URLs you configure in any lookup string for an Identity Provider partner should contain only the portion of the URL that follows the host and port. For example, `target:*:/myserver/xxx`.

When you configure a Service Provider site, this behavior enables you to configure a single Identity Provider partner that can be used to validate all assertions for the same web service, regardless of the variations in the transport protocol (i.e., HTTP vs. HTTPS), host name, IP address, and port information across all the machines in a domain that host that web service.

Table 5-5 Service Provider Partner Lookup String Syntax

Lookup String	Description
<code>target::-<endpoint-url></code>	<p>Specifies that partner lookup is conducted for an exact match of the URL, <code><endpoint-url></code>. For example, <code>target::-/myserver/myservicecontext/my-endpoint</code> specifies the endpoint that can be matched to this Identity Provider partner, for which an assertion should be validated.</p> <p>This form of partner lookup string excludes the endpoint URL from being added as an Audience URI for this Identity Provider partner.</p>
<code>target::+<endpoint-url></code>	<p>Specifies that partner lookup is conducted for an exact match of the URL, <code><endpoint-url></code>.</p> <p>Note: Using the plus sign (+) in the lookup string results in the endpoint URL being added as an Audience URI in the assertion received from this Identity Provider partner. Because this form of lookup string is unlikely to produce a match for an Identity Provider partner, it should be avoided.</p>
<code>target::*<endpoint-url></code>	<p>Specifies that partner lookup is conducted for an initial-string pattern match of the URL, <code><endpoint-url></code>. For example, <code>target::*:/myserver</code> specifies that any endpoint URL beginning with <code>/myserver</code> can be matched to this Identity Provider, such as: <code>/myserver/contextA/endpointA</code> and <code>/myserver/contextB/endpointB</code>.</p> <p>If more than one Identity Provider partner is discovered that is a match for the initial string, the partner with the longest initial string match is selected.</p> <p>This form of partner lookup string excludes the endpoint URL from being added as an Audience URI for this Identity Provider partner.</p>

Notes: Configuring one or more partner lookup strings for an Identity Provider partner is required in order for that partner to be discovered at run time. If this partner cannot be discovered, no assertions for this partner can be validated.

If you configure an endpoint URL without using the target lookup prefix, it will be handled as a conventional Audience URI that must be contained in assertions received from this Identity Provider partner. (This also enables backwards-compatibility with existing Audience URIs that may be configured for this partner.)

Specifying Default Partners

To support the need for a default Identity Provider partner entry, one or more of the default partner's Audience URI entries may contain a wildcard match that works for all targets. For example, `target:*:/*`.

Management of Partner Certificates

The SAML 2.0 Identity Assertion provider manages the trusted certificates for configured partners. Whenever a certificate is received during an exchange of partner messages, the certificate is checked against the certificates maintained for the partner. Partner certificates are used for the following purposes:

- To validate trust when the Service Provider site receives a signed assertion or a signed SAML artifact request.
- To validate trust in an Identity Provider partner that is retrieving a SAML artifact from the Artifact Resolution Service (ARS) via an SSL connection.

The following certificates, which are obtained from each configured Identity Provider partner, are required:

- The certificate used to verify signed SAML documents received from the partner, such as assertions and artifact requests

The certificate used to verify signed SAML documents in web single sign-on is included in the metadata file received from the Identity Provider partner. When configuring web service Identity Provider partners, you obtain this certificate from your partner and import it into this partner's configuration via the Assertion Signing Certificate tab of the partner management page in the Administration Console.

- The Transport Layer Security (TLS) client certificate that is used to verify the connection made by the partner to the local site's SSL binding for retrieving SAML artifacts (used in web single sign-on only)

When configuring a web single sign-on Identity Provider partner, you must obtain the TLS client certificate directly from the partner. It is not automatically included in the metadata file. You can import this certificate into the configuration data for this partner via the Transport Layer Client Certificate tab of the partner management page in the Administration Console.

Java Interface for Configuring Identity Provider Partner Attributes

Operations on web service partners are available in the [com.bea.security.saml2.providers.registry.Partner](#) Java interface.

Ordering of Identity Assertion for Servlets

When an HTTP request is sent, there may be multiple matches that can be used for identity assertion. However, identity assertion providers can only consume one active token type at a time. As a result there is no way to provide a set of tokens that can be consumed with one call. Therefore, the servlet contained in WebLogic Server is forced to choose between multiple tokens to perform identity assertion. The following ordering is used:

1. An X.509 digital certificate (signifies two-way SSL to client or proxy plug-in with two-way SSL between the client and the Web server) if X.509 is one of the active token types configured for the Identity Assertion provider in the default security realm.
2. Headers with a name in the form `WL-Proxy-Client-<TOKEN>` where `<TOKEN>` is one of the active token types configured for the Identity Assertion provider in the default security realm.

Note: This method is deprecated and should only be used for the purpose of backward compatibility.
3. Headers with a name in the form `<TOKEN>` where `<TOKEN>` is one of the active tokens types configured for the Identity Assertion provider in the default security realm.
4. Cookies with a name in the form `<TOKEN>` where `<TOKEN>` is one of the active tokens types configured for the Identity Assertion provider in the default security realm.

For example, if an Identity Assertion provider in the default security realm is configured to have the `FOO` and `BAR` tokens as active token types (for the following example, assume the HTTP request contains nothing relevant to identity assertion except active token types), identity assertion is performed as follows:

- If a request comes in with a `FOO` header over a two-way SSL connection, X.509 is used for identity assertion.
- If a request comes in with a `FOO` header and a `WL-Proxy-Client-BAR` header, the `BAR` token is used for identity assertion.
- If a request comes in with a `FOO` header and a `BAR` cookie, the `FOO` token will be used for identity assertion.

The ordering between multiple tokens at the same level is undefined, therefore:

- If a request comes in with a FOO header and a BAR header, then either the FOO or BAR token is used for identity assertion, however, which one is used is unspecified.
- If a request comes in with a FOO cookie and a BAR cookie, then either the FOO or BAR token is used for identity assertion, however, which one is used is unspecified.

Configuring Identity Assertion Performance in the Server Cache

When you use an Identity Assertion provider, either for an X.509 certificate or some other type of token, subjects are cached within the server. (A subject is a grouping of related information for a single entity (such as a person), including an identity and its security-related configuration options.) Caching subjects within the server greatly enhances performance for servlets and EJB methods with `<run-as>` tags as well as in other situations where identity assertion is used but not cached in the `HTTPSession`, for example, in signing and encrypting XML documents).

Note: Caching can violate the desired semantics.

You can change the lifetime of items in this cache by setting the maximum number of seconds a subject can live in the cache via the `-Dweblogic.security.identityAssertionTTL` command-line argument. The default for this command-line argument is 300 seconds (that is, 5 minutes). Possible values for the command-line argument are:

- Less than 0—Disables the cache.
- 0—Caching is enabled and the identities in the cache never time out so long as the server is running. Any changes in the user database of cached entities requires a server reboot in order for the server to pick them up.
- Greater than 0—Caching is enabled and the cache is reset at the specified number of seconds.

To improve the performance of identity assertion, specify a higher value for this command-line argument.

Note: As identity assertion performance improves, the Identity Assertion provider is less responsive to changes in the configured Authentication provider. For example, a change in the user's group will not be reflected until the subject is flushed from the cache and recreated. Setting a lower value for the command-line argument makes authentication changes more responsive at a cost for performance.

Configuring a User Name Mapper

WebLogic Server verifies the digital certificate of the Web browser or Java client when establishing a two-way SSL connection. However, the digital certificate does not identify the Web browser or Java client as a user in the WebLogic Server security realm. If the Web browser or Java client requests a WebLogic Server resource protected by a security policy, WebLogic Server requires the Web browser or Java client to have an identity. The WebLogic Identity Assertion provider allows you to enable a user name mapper that maps the digital certificate of a Web browser or Java client to a user in a WebLogic Server security realm.

The user name mapper must be an implementation of the `weblogic.security.providers.authentication.UserNameMapper` interface. This interface maps a token to a WebLogic Server user name according to whatever scheme is appropriate for your needs. By default, WebLogic Server provides a default implementation of the `weblogic.security.providers.authentication.UserNameMapper` interface. You can also write your own implementation.

The WebLogic Identity Assertion provider calls the user name mapper for the following types of identity assertion token types:

- X.509 digital certificates passed via the SSL handshake
- X.509 digital certificates passed via CSIV2
- X.501 distinguished names passed via CSIV2

The default user name mapper uses the subject DN of the digital certificate or the distinguished name to map to the appropriate user in the WebLogic Server security realm. For example, the user name mapper can be configured to map a user from the Email attribute of the subject DN (`smith@example.com`) to a user in the WebLogic Server security realm (`smith`). Use Default User Name Mapper Attribute Type and Default Username Mapper Attribute Delimiter attributes of the WebLogic Identity Assertion provider to define this information:

- Default User Name Mapper Attribute Type—The subject distinguished name (DN) in a digital certificate used to calculate a username. Valid values are: C, CN, E, L, O, OU, S and STREET.
- Default User Name Mapper Attribute Delimiter—Ends the username. The user name mapper uses everything to the left of the value to calculate a username. The default delimiter is @.

For more information, see [Configure a user name mapper](#) in the *Administration Console Online Help*.

Configuring a Custom User Name Mapper

You can also write a custom user name mapper to map a token to a WebLogic Server user name according to whatever scheme is appropriate for your needs. The custom user name mapper must be an implementation of the

`weblogic.security.providers.authentication.UserNameMapper` interface. You then configure the custom user name mapper in the active security realm, using the User Name Mapper Class Name attribute of the WebLogic Identity Assertion provider.

For more information, see [Configure custom user name mappers](#) in the *Administration Console Online Help*.

Configuring Single Sign-On with Microsoft Clients

The following sections explain how to set up single sign-on (SSO) with Microsoft clients, using Windows authentication based on the Simple and Protected Negotiate (SPNEGO) mechanism and the Kerberos protocol, together with the WebLogic Negotiate Identity Assertion provider.

- [“Overview of Single Sign-On with Microsoft Clients” on page 6-1](#)
- [“System Requirements for SSO with Microsoft Clients” on page 6-2](#)
- [“Single Sign-On with Microsoft Clients: Main Steps” on page 6-3](#)
- [“Creating a Kerberos Identification for WebLogic Server” on page 6-5](#)
- [“Configuring Microsoft Clients to Use Windows Integrated Authentication” on page 6-7](#)
- [“Creating a JAAS Login File” on page 6-9](#)
- [“Configuring the Identity Assertion Provider” on page 6-11](#)
- [“Using Startup Arguments for Kerberos Authentication with WebLogic Server” on page 6-11](#)
- [“Verifying Configuration of SSO with Microsoft Clients” on page 6-11](#)

Overview of Single Sign-On with Microsoft Clients

Single sign-on (SSO) with Microsoft clients allows cross-platform authentication between Web applications or Web Services running in a WebLogic Server domain and .NET Web Service clients or browser clients (for example, Internet Explorer) in a Microsoft domain. The Microsoft

clients must use Windows authentication based on the Simple and Protected Negotiate (SPNEGO) mechanism.

Cross-platform authentication is achieved by emulating the negotiate behavior of native Windows-to-Windows authentication services that use the Kerberos protocol. In order for cross-platform authentication to work, non-Windows servers (in this case, WebLogic Server) need to parse SPNEGO tokens in order to extract Kerberos tokens which are then used for authentication.

For more information about Windows and Kerberos, see

<http://www.microsoft.com/technet/prodtechnol/windows2000serv/deploy/confeat/kerberos.mspx>.

System Requirements for SSO with Microsoft Clients

To use SSO with Microsoft clients you need:

A host computer with:

- Windows 2000 or later installed
- Fully-configured Active Directory authentication service. Specific Active Directory requirements include:
 - User accounts for mapping Kerberos services
 - Service Principal Names (SPNs) for those accounts
 - Key tab files created and copied to the start-up directory in the WebLogic Server domain
- WebLogic Server installed and configured properly to authenticate through Kerberos, as described in this chapter

Client systems with:

- Windows 2000 Professional SP2 or later installed
- One of the following types of clients:
 - A properly configured Internet Explorer browser. Internet Explorer 6.01 or later is supported.
 - .NET Framework 1.1 and a properly configured Web Service client.

Clients must be logged on to a Windows 2000 domain and have Kerberos credentials acquired from the Active Directory server in the domain. Local logons will not work.

Single Sign-On with Microsoft Clients: Main Steps

Configuring SSO with Microsoft clients requires set-up procedures in the Microsoft Active Directory, the client, and the WebLogic Server domain. (These procedures are detailed in the sections that follow.)

- Define a principal in Active Directory to represent the WebLogic Server. The Kerberos protocol uses the Active Directory server in the Microsoft domain to store the necessary security information.
- Any Microsoft client you want to access in the Microsoft domain must be set up to use Windows Integrated authentication, sending a Kerberos ticket when available.
- In the security realm of the WebLogic Server domain, configure a Negotiate Identity Assertion provider. The Web application or Web Service used in SSO needs to have authentication set in a specific manner. A JAAS login file that defines the location of the Kerberos identification for WebLogic Server must be created.

To configure SSO with Microsoft clients:

1. Configure your network domain to use Kerberos. See [“Configuring Your Network Domain to Use Kerberos”](#) on page 6-4.
2. Create a Kerberos identification for WebLogic Server.
 - a. Create a user account in the Active Directory for the host on which WebLogic Server is running.
 - b. Create a Service Principal Name for this account.
 - c. Create a user mapping and keytab file for this account.See [“Creating a Kerberos Identification for WebLogic Server”](#) on page 6-5.
3. Choose a Microsoft client (either a Web Service or a browser) and configure it to use Windows Integrated authentication. See [“Configuring Microsoft Clients to Use Windows Integrated Authentication”](#) on page 6-7.
4. Set up the WebLogic Server domain to use Kerberos authentication.
 - a. Create a JAAS login file that points to the Active Directory server in the Microsoft domain and the keytab file created in Step 1. See [“Creating a JAAS Login File”](#) on page 6-9.

- b. Configure a Negotiate Identity Assertion provider in the WebLogic Server security realm. See [“Configuring a Negotiate Identity Assertion Provider”](#) on page 5-29.
5. Start WebLogic Server using specific start-up arguments. See [“Using Startup Arguments for Kerberos Authentication with WebLogic Server”](#) on page 6-11.

The following sections describe these steps in detail.

Configuring Your Network Domain to Use Kerberos

A Windows domain controller can serve as the Kerberos Key Distribution Center (KDC), using the Active Directory and the Kerberos services. On any domain controller, the Active Directory and the Kerberos services are running automatically.

Java GSS requires a Kerberos configuration file. The default name and location of the Kerberos configuration file depends on the operating system being used. Java GSS uses the following order to search for the default configuration file:

1. The file referenced by the Java property `java.security.krb5.conf`.
2. `${java.home}/lib/security/krb5.conf`.
3. `%windir%\krb5.ini` on Microsoft Windows platforms.
4. `/etc/krb5/krb5.conf` on Solaris platforms.
5. `/etc/krb5.conf` on other Unix platforms.

To configure Kerberos in your Windows domain controller, you need to configure each machine that will access the KDC to locate the Kerberos realm and available KDC servers. For example:

Listing 6-1 Sample `krb5.ini` File

```
[libdefaults]
default_realm = MYDOM.COM (Identifies the default realm. Set its value to
your Kerberos realm)
default_tkt_enctypes = des-cbc-crc
default_tgs_enctypes = des-cbc-crc
ticket_lifetime = 600

[realms]
```

```

MYDOM.COM = {
kdc = <IP address for MachineA> (host running the KDC)
(For Unix systems, you need to specify port 88, as in <IP-address>:88)
admin_server = MachineA
default_domain = MYDOM.COM
}

[domain_realm]
.mydom.com = MYDOM.COM

[appdefaults]
autologin = true
forward = true
forwardable = true
encrypt = true

```

Creating a Kerberos Identification for WebLogic Server

Active Directory provides support for service principal names (SPN), which are a key component in Kerberos authentication. SPNs are unique identifiers for services running on servers. Every service that uses Kerberos authentication needs to have an SPN set for it so that clients can identify the service on the network. An SPN usually looks something like `name@YOUR.REALM`. You need to define an SPN to represent your WebLogic Server in the Kerberos realm. If an SPN is not set for a service, clients have no way of locating that service. Without correctly set SPNs, Kerberos authentication is not possible. Keytab files are the mechanism for storing the SPNs. Keytab files are copied to the WebLogic Server domain and are used in the login process. This configuration step describes how to create an SPN, user mapping, and keytab file for WebLogic Server.

This configuration step requires the use of the following Active Directory utilities:

- `setspn`—Windows 2000 Resource Kit
- `ktpass`—Windows 2000 distribution CD in `Program Files\Support Tools`

Note: The `setspn` and `ktpass` Active Directory utilities are products of Microsoft. Therefore, Oracle does not provide complete documentation for this utilities. For more information, see the appropriate Microsoft documentation.

To create a Kerberos identification for WebLogic Server:

1. In the Active Directory server, create a user account for the host computer on which WebLogic Server runs. (Select New → User, not New → Machine.)

When creating the user account, use the simple name of the computer. For example, if the host is named `myhost.example.com`, create a user in Active Directory called `myhost`.

Note the password you defined when creating the user account. You will need it in step 3. Do not select the `User must change password at next logon` option, or any other password options.

2. Configure the new user account to comply with the Kerberos protocol. The user account's encryption type must be DES and the account must require Kerberos pre-authentication.
 - a. Right-click the name of the user account in the Users tree in the left pane and select Properties.
 - b. Select the Account tab and check the box "Use DES encryption types for this account." Make sure no other boxes are checked, particularly the box "Do not require Kerberos pre-authentication."
 - c. Setting the encryption type may corrupt the password. Therefore, reset the user password by right-clicking the name of the user account, selecting Reset Password, and re-entering the same password specified earlier.
3. Use the `setspn` utility to create the Service Principal Names (SPNs) for the user account created in step 1. Enter the following commands:

```
setspn -a host/myhost.example.com myhost
setspn -a HTTP/myhost.example.com myhost
```

4. Check which SPNs are associated with your user account, using the following command:

```
setspn -L account name
```

This is an important step. If the same service is linked to a different account in the Active Directory server, the client will not send a Kerberos ticket to the server.

5. Create a user mapping using the `ktpass` utility:

Windows

```
ktpass -princ host/myhost@Example.CORP -pass password -mapuser myhost
-out c:\temp\myhost.host.keytab
```

6. Create a keytab file. On Windows, the `ktab` utility manages principal name and key pairs in the key table and allows you to list, add, update, or delete principal names and key pairs. On UNIX, it is preferable to use the `ktpass` utility.

Windows

- a. Run the `ktab` utility on the host on which WebLogic Server is running to create the keytab file:

```
ktab -k keytab-filename -a myhost@Example.CORP
```

- b. Copy the keytab file to the startup directory in the WebLogic Server domain.

UNIX

- a. Create a user mapping using the `ktpass` utility, using a command like this, where *password* is the password for the user account created in step 1:

```
ktpass -princ HTTP/myhost@Example.CORP -pass password -mapuser myhost  
-out c:\temp\myhost.HTTP.keytab
```

- b. Copy the keytab file created in Step a to the startup directory in the WebLogic Server domain.

- c. Login as root and then merge them into a single keytab using the `ktutil` utility as follows:

```
ktutil: "rkt myhost.host.keytab"  
ktutil: "rkt myhost.HTTP.keytab"  
ktutil: "wkt mykeytab"  
ktutil: "q"
```

7. Run the `kinit` utility to verify Kerberos authentication is working properly.

```
kinit -k -t keytab-file account-name
```

The output should be something similar to:

```
New ticket is stored in cache file C:\Documents and  
Settings\Username\krb5cc_MachineB
```

Configuring Microsoft Clients to Use Windows Integrated Authentication

Ensure the Microsoft client you want to use for single sign-on is configured to use Windows Integrated authentication. The following sections describe how to configure a .NET Web server and an Internet Explorer browser client to use Windows Integrated authentication.

Configuring a .NET Web Service

To configure a .NET Web Service to use Windows authentication:

1. In the `web.config` file for the Web Service, set the authentication mode to Windows for IIS and ASP.NET as follows:

```
<authentication mode="Windows" />
```

This setting is usually the default.

2. Add the statement needed for the Web Services client to pass to the proxy Web Service object so that the credentials are sent through SOAP.

For example, if you have a Web Service client for a Web Service that is represented by the proxy object `conv`, the syntax is as follows:

```
/*  
* Explicitly pass credentials to the Web Service  
*/  
conv.Credentials =  
System.Net.CredentialCache.DefaultCredentials;
```

Configuring an Internet Explorer Browser

To configure an Internet Explorer browser to use Windows authentication, follow these procedures in Internet Explorer.

Configure Local Intranet Domains

1. In Internet Explorer, select Tools → Internet Options.
2. Select the Security tab.
3. Select Local intranet and click Sites.
4. In the Local intranet popup, ensure that the “Include all sites that bypass the proxy server” and “Include all local (intranet) sites not listed in other zones” options are checked.
5. Click Advanced.
6. In the Local intranet (Advanced) dialog box, add all relative domain names that will be used for WebLogic Server instances participating in the SSO configuration (for example, `myhost.example.com`) and click OK.

Configure Intranet Authentication

1. Select Tools → Internet Options.
2. Select the Security tab.

3. Select Local intranet and click Custom Level....
4. In the Security Settings dialog box, scroll to the User Authentication section.
5. Select Automatic logon only in Intranet zone. This option prevents users from having to re-enter logon credentials, which is a key piece to this solution.
6. Click OK.

Verify the Proxy Settings

If you have a proxy server enabled:

1. Select Tools → Internet Options.
2. Select the Connections tab and click LAN Settings.
3. Verify that the proxy server address and port number are correct.
4. Click Advanced.
5. In the Proxy Settings dialog box, ensure that all desired domain names are entered in the Exceptions field.
6. Click OK to close the Proxy Settings dialog box.

Set Integrated Authentication for Internet Explorer 6.0

In addition to the settings already described, one additional setting is required if you are running Internet Explorer 6.0.

1. In Internet Explorer, select Tools → Internet Options.
2. Select the Advanced tab.
3. Scroll to the Security section.
4. Make sure that Enable Integrated Windows Authentication option is checked and click OK.
5. If this option was not checked, restart the computer.

Creating a JAAS Login File

If you are running WebLogic Server on either the Windows or UNIX platforms, you need a JAAS login file. The JAAS login file tells the WebLogic Security Framework to use Kerberos authentication and defines the location of the keytab file which contains Kerberos identification

information for WebLogic Server. You specify the location of this file in the `java.security.auth.login.config` startup argument for WebLogic Server, as described in [“Using Startup Arguments for Kerberos Authentication with WebLogic Server”](#) on page 6-11.

Note: For JDK 1.5 and JDK 1.4, the JAAS Login Entry name is `com.sun.security.jgss.accept`.

For JDK 1.6, the JAAS Login Entry name was changed to `com.sun.security.jgss.krb5.accept`.

[Listing 6-2](#) contains a sample JAAS login file for Kerberos authentication. Significant sections are shown in bold.

Listing 6-2 Sample JAAS Login File for Kerberos Authentication

```
com.sun.security.jgss.initiate {  
  
    com.sun.security.auth.module.Krb5LoginModule required  
    principal="myhost@Example.CORP" useKeyTab=true  
    keyTab=mykeytab storeKey=true;  
};  
  
com.sun.security.jgss.accept {  
  
    com.sun.security.auth.module.Krb5LoginModule required  
    principal="myhost@Example.CORP" useKeyTab=true  
    keyTab=mykeytab storeKey=true;  
  
};
```

For the `principal` option, specify the value of the `userPrincipalName` attribute of the account under which the service is running. (Incorrectly specifying the user principal name results in an error such as “Unable to obtain password from user.”)

The `keytab` file specified in the `keytab` option must be accessible by the WebLogic Server process. Ensure that the appropriate permissions are set. If you are unsure of the search path WebLogic Server is using, provide the absolute path to the file.

Configuring the Identity Assertion Provider

WebLogic Server includes a security provider, the Negotiate Identity Assertion provider, to support single sign-on (SSO) with Microsoft clients. This identity assertion provider decodes Simple and Protected Negotiate (SPNEGO) tokens to obtain Kerberos tokens, validates the Kerberos tokens, and maps Kerberos tokens to WebLogic users. You need to configure a Negotiate Identity Assertion provider in your WebLogic security realm in order to enable SSO with Microsoft clients. See [“Configuring a Negotiate Identity Assertion Provider” on page 5-29](#) and [Configure Authentication and Identity Assertion providers](#) in the *Administration Console Online Help*.

Using Startup Arguments for Kerberos Authentication with WebLogic Server

To use Kerberos authentication with WebLogic Server, use the following start-up arguments when you start WebLogic Server:

```
-Djava.security.krb5.realm=Example.CORP  
-Djava.security.krb5.kdc=ADhostname  
-Djavax.security.auth.useSubjectCredsOnly=false
```

where

- `java.security.krb5.realm` defines the Microsoft domain in which the Active Directory server runs.
- `java.security.krb5.kdc` defines the host name on which the Active Directory server runs.
- `javax.security.auth.useSubjectCredsOnly` specifies that it is permissible to use an authentication mechanism other than Subject credentials.
- Java GSS messages are often very useful during troubleshooting, so you might want to add `-Dsun.security.krb5.debug=true` as part of the initial setup.

Verifying Configuration of SSO with Microsoft Clients

To verify that SSO with Microsoft clients is configured properly, point a browser (that you have configured as described in [“Configuring an Internet Explorer Browser” on page 6-8](#)) to the Microsoft Web application or Web Service you want to use. If you are logged on to a Windows domain and have Kerberos credentials acquired from the Active Directory server in the domain,

Configuring Single Sign-On with Microsoft Clients

you should be able to access the Web application or Web Service without providing a username or password.

Configuring Single Sign-On with Web Browsers and HTTP Clients

The Security Assertion Markup Language (SAML) enables cross-platform authentication between Web applications or Web Services running in a WebLogic Server domain and Web browsers or other HTTP clients. WebLogic Server supports single sign-on (SSO) based on SAML. When users are authenticated at one site that participates in a single sign-on (SSO) configuration, they are automatically authenticated at other sites in the SSO configuration and do not need to log in separately.

The following sections describe how to set up single sign-on (SSO) with Web browsers or other HTTP clients by using authentication based on the Security Assertion Markup Language (SAML) versions 1.1 and 2.0.

- [“Configuring SAML 1.1 Services” on page 7-2](#)
- [“Configuring SAML 2.0 Services” on page 7-9](#)

Note: A WebLogic Server instance that is configured for SAML 2.0 SSO is not interoperable with one that is configured for SAML 1.1

For an overview of SAML-based single sign on, see the following topics in *Understanding WebLogic Security*:

- [Security Assertion Markup Language \(SAML\)](#)
- [Web Browsers and HTTP Clients via SAML](#)
- [Single Sign-On with the WebLogic Security Framework](#)

Configuring SAML 1.1 Services

This topic includes the following sections:

- [“Enabling Single Sign-on with SAML 1.1: Main Steps”](#) on page 7-2
- [“Configuring a SAML 1.1 Source Site for Single Sign-On”](#) on page 7-3
- [“Configuring a SAML 1.1 Destination Site for Single Sign-On”](#) on page 7-5
- [“Configuring Relying and Asserting Parties with WLST”](#) on page 7-7

Enabling Single Sign-on with SAML 1.1: Main Steps

To enable single sign-on with SAML, configure WebLogic Server as either a source site or destination site as described in the sections that follow.

Configuring a Source Site: Main Steps

To configure a WebLogic Server instance in the role of a source site, complete the following main steps:

1. Create and configure a SAML Credential Mapping provider V2 in your security realm.
2. Configure the federation services for the server instance in the realm that will serve as a source site.
3. Create and configure the relying parties for which SAML assertions will be produced.
4. If you want to require relying parties to use SSL certificates to connect to the source site, add any such certificates to the SAML credential mapping provider’s Certificate Registry.

Configuring a Destination Site: Main Steps

To configure a WebLogic Server instance in the role of a destination site, complete the following main steps:

1. Create and configure a SAML Identity Assertion provider V2 in your security realm.
2. Configure the federation services for the server instance realm that will serve as a destination site.
3. Create and configure the asserting parties from which SAML assertions will be consumed.

4. Establish trust by registering the asserting parties' SSL certificates in the certificate registry maintained by the SAML Identity Assertion provider.

Configuring a SAML 1.1 Source Site for Single Sign-On

The following topics explain how to configure a WebLogic Server instance as a SAML 1.1 source site:

- [“Configure the SAML 1.1 Credential Mapping Provider” on page 7-3](#)
- [“Configure the Source Site Federation Services” on page 7-3](#)
- [“Configure Relying Parties” on page 7-4](#)
- [“Replacing the Default Assertion Store” on page 7-5](#)

Configure the SAML 1.1 Credential Mapping Provider

In your security realm, create a SAML Credential Mapping Provider V2 instance. The SAML Credential Mapping provider is not part of the default security realm. See [“Configuring a SAML Credential Mapping Provider for SAML 1.1” on page 4-19](#).

Configure the SAML Credential Mapping provider as a SAML authority, using the Issuer URI, Name Qualifier, and other attributes.

Configure the Source Site Federation Services

Configuration of a WebLogic Server instance as a SAML 1.1 source site is controlled by the `FederationServicesMBean`. Access the `FederationServicesMBean` with the WebLogic Scripting Tool or through the Administration Console, on the Environment → Servers → *ServerName* → Configuration → Federation Services → SAML 1.1 Source Site page. See [Configure SAML source services](#) in the *Administration Console Online Help*.

Configure SAML source site attributes as follows:

- **Enable the SAML Source Site.** Allow the WebLogic server instance to serve as a SAML source site by setting Source Site Enabled to true.
- **Set Source Site URL and Service URIs.** Set the URL for the SAML source site. This is the URL that hosts the Intersite Transfer Service and Assertion Retrieval Service. The source site URL is encoded as a source ID in hex and Base64. When you configure a SAML Asserting Party for Browser/Artifact profile, you specify the encoded source ID.

Also specify the URIs for the Intersite Transfer Service and (to support Browser/Artifact profile) the Assertion Retrieval Service. These URIs are also specified in the configuration of an Asserting Party.

- **Add signing certificate.** The SAML source site requires a trusted certificate with which to sign assertions. Add this certificate to the keystore and enter the credentials (alias and passphrase) to be used to access the certificate. The server's SSL identity key/certificates will be used by default if a signing alias and passphrase are not supplied.
- **Configure SSL for the Assertion Retrieval Service.** You can require all access to the Assertion Retrieval Service to use SSL by setting `FederationServicesMBean.arsRequiresSSL` to true. You can require two-way SSL authentication for the Assertion Retrieval Service by setting both `arsRequiresSSL` and `ARSRequiresTwoWaySSL` to true.

Configure Relying Parties

A SAML Relying Party is an entity that relies on the information in a SAML assertion produced by the SAML source site. You can configure how WebLogic Server produces SAML assertions separately for each Relying Party or use the defaults established by the Federation Services source site configuration for producing assertion.

You configure a Relying Party in the Administration Console, on the Security Realms → *RealmName* → Providers → Credential Mapper → *SAMLCredentialMapperName* → Management → Relying Parties page. See [Create a SAML Relying Party](#) and [Configure a SAML Relying Party](#) in the *Administration Console Online Help*.

You can also configure a Relying Party with the WebLogic Scripting Tool. See “[Configuring Relying and Asserting Parties with WLST](#)” on page 7-7.

Configure Supported Profiles

When you configure a SAML Relying Party, you can specify support for Artifact profile or POST profile, for the purposes of SAML SSO. As an alternative configure a Relying Party to support WSS/Holder-of-Key or WSS/Sender-Vouches profiles for Web Services Security purposes. Be sure to configure support for the profiles that the SAML destination sites support.

If you support the POST profile, optionally create a form to use in POST profile assertions for the Relying Party and set the pathname of that form in the POST Form attribute.

Assertion Consumer Parameters

For each SAML Relying Party, you can configure one or more optional query parameters (such as a partner ID) that will be added to the ACS URL when redirecting to the destination site. In the case of POST profile, these parameters will be included as form variables when using the default POST form. If a custom POST form is in use, the parameters will be made available as a Map of names and values, but the form may or may not be constructed to include the parameters in the POSTed data.

Replacing the Default Assertion Store

WebLogic Server uses a simple assertion store to maintain persistence for produced assertions. You can replace this assertion store with a custom assertion store class that implements `weblogic.security.providers.saml.AssertionStoreV2`. Configure WebLogic Server to use your custom assertion store class, rather than the default class, using the `FederationServicesMBean.AssertionStoreClassName` attribute. You can configure properties to be passed to the `initStore()` method of your custom assertion store class by using the `FederationServicesMBean.AssertionStoreProperties` attribute. Configure these attributes in the Administration Console on the Environment: Servers → *ServerName* → Configuration → Federation Services → SAML 1.1 Source Site page.

Configuring a SAML 1.1 Destination Site for Single Sign-On

The following topics describe how to configure WebLogic Server as a SAML destination site:

- [“Configure SAML Identity Assertion Provider” on page 7-5](#)
- [“Configure Destination Site Federation Services” on page 7-5](#)
- [“Configuring Asserting Parties” on page 7-7](#)

Configure SAML Identity Assertion Provider

In your security realm, create and configure a SAML Identity Assertion Provider V2 instance. The SAML Identity Assertion provider is not part of the default security realm. See [“Configuring a SAML Identity Assertion Provider for SAML 1.1” on page 5-30](#).

Configure Destination Site Federation Services

Before you configure WebLogic as a SAML destination site, you must first create a SAML Identity Assertion Provider V2 instance in your security realm. Configuration of a WebLogic Server instance as a SAML destination site is controlled by the `FederationServicesMBean`.

You can access the `FederationServicesMBean` using the WebLogic Scripting Tool or through the Administration Console, using the Environment: Servers → *ServerName* → Configuration → Federation Services → SAML 1.1 Destination Site page.

Configure the SAML destination site attributes as follows.

Enable the SAML Destination Site

Allow the WebLogic Server instance to serve as a SAML destination site by setting Destination Site Enabled to true.

Set Assertion Consumer URIs

Set the URIs for the SAML Assertion Consumer Service. This is the URL that receives assertions from source sites, so that the destination site can use the assertions to authenticate users. The Assertion Consumer URI is also specified in the configuration of a Relying Party.

Configure SSL for the Assertion Consumer Service

You can require all access to the Assertion Consumer Service to use SSL by setting `FederationServicesMBean.acsRequiresSSL` to true.

Add SSL Client Identity Certificate

The SAML destination site uses a trusted certificate with which to sign POST profile responses. Add this certificate to the keystore and enter the credentials (alias and passphrase) to be used to access the certificate.

Configure Single-Use Policy and the Used Assertion Cache or Custom Assertion Cache

Optionally, you can require that each POST profile assertion be used no more than once. WebLogic Server maintains a cache of used assertions so that it can support a single-use policy for assertions. You can replace this assertion cache with a custom assertion cache class that implements `weblogic.security.providers.saml.SAMLUsedAssertionCache`. Configure WebLogic Server to use your custom assertion cache class, rather than the default class, using the `FederationServicesMBean.SAMLUsedAssertionCache` attribute. You can configure properties to be passed to the `initCache()` method of your custom assertion cache class using the `FederationServicesMBean.UsedAssertionCacheProperties` attribute. You can configure these attributes in the Administration Console on the Environment → Servers → *ServerName* → Configuration → Federation Services → SAML 1.1 Destination Site page.

Configure Recipient Check for POST Profile

Optionally, you can require that the recipient of the SAML Response must match the URL in the HTTP Request. Do this by setting the POST Recipient Check Enabled attribute.

Configuring Asserting Parties

A SAML Asserting Party is a trusted SAML Authority (an entity that can authoritatively assert security information in the form of SAML Assertions). Configure an Asserting Party in the Administration Console, using the Security Realms → *RealmName* → Providers → Credential Mapper → *SAMLCredentialMapperName* → Management: Asserting Parties page. See [Create a SAML Asserting Party](#) and [Configure a SAML Asserting Party](#) in the *Administration Console Online Help*.

You can also configure an Asserting Party with the WebLogic Scripting Tool. See “[Configuring Relying and Asserting Parties with WLST](#)” on page 7-7.

Configure Supported Profiles

When you configure a SAML Asserting Party, you can specify support for Artifact profile or POST profile, for the purposes of SAML SSO. Alternatively, configure an Asserting Party to support WSS/Holder-of-Key or WSS/Sender-Vouches profiles for Web Services Security purposes.

Configure Source Site ITS Parameters

For each SAML Asserting Party, configure zero or more optional query parameters (such as a partner ID) that will be added to the ITS URL when redirecting to the source site.

Configuring Relying and Asserting Parties with WLST

SAML partners (Relying Parties and Asserting Parties) are maintained in a registry. You can configure SAML partners using the WebLogic Administration Console or using WebLogic Scripting Tool. The following example shows how you might configure two Relying Parties using WLST in online mode.

Listing 7-1 Creating Relying Parties with WLST

```
connect('weblogic','weblogic','t3://localhost:7001')
rlm=cmo.getSecurityConfiguration().getDefaultRealm()
```

Configuring Single Sign-On with Web Browsers and HTTP Clients

```
cm=rlm.lookupCredentialMapper('samlv2cm')

rp=cm.newRelyingParty()
rp.setDescription('test post profile')
rp.setProfile('Browser/POST')
rp.setAssertionConsumerURL('http://domain.example.com:7001/saml_destinatio
n/acs')
rp.setAssertionConsumerParams(array(['APID=ap_00001'],String))
rp.setSignedAssertions(true)
rp.setEnabled(true)
cm.addRelyingParty(rp)

rp=cm.newRelyingParty()
rp.setDescription('test artifact profile')
rp.setProfile('Browser/Artifact')
rp.setAssertionConsumerURL('http://domain.example.com:7001/saml_destinatio
n/acs')
rp.setAssertionConsumerParams(array(['APID=ap_00002'],String))
rp.setARSUsername('foo')
rp.setARSPassword('bar')
rp.setSSLClientCertAlias('demoidentity')
rp.setEnabled(true)
cm.addRelyingParty(rp)

disconnect()

exit()
```

The following example shows how you might edit an existing Asserting Party. The example gets the Asserting Party, using its Asserting Party ID, and sets the Assertion Retrieval URL.

Listing 7-2 Editing an Asserting Party with WLST

```

connect('weblogic','weblogic','t3://localhost:7001')
rlm=cmo.getSecurityConfiguration().getDefaultRealm()
ia=rlm.lookupAuthenticationProvider('samlv2ia')
ap=ia.getAssertingParty('ap_00002')
ap.setAssertionRetrievalURL('https://hostname:7002/samlars/ars')
ia.updateAssertingParty(ap)
disconnect()
exit()

```

Configuring SAML 2.0 Services

This topic includes the following sections:

- [“Configuring SAML 2.0 Services: Main Steps”](#) on page 7-9
- [“Configuring SAML 2.0 General Services”](#) on page 7-11
- [“Configuring an Identity Provider Site for SAML 2.0 Single Sign-On”](#) on page 7-14
- [“Configuring a Service Provider Site for SAML 2.0 Single Sign-On”](#) on page 7-18
- [“Web Application Deployment Considerations for SAML 2.0”](#) on page 7-24

Configuring SAML 2.0 Services: Main Steps

A summary of the main steps you take to configure SAML 2.0 services are as follows:

1. Determine whether you plan to have SAML 2.0 services running in more than one WebLogic Server instance in the domain. If so, do the following:
 - a. Create a domain in which the RDBMS security store is configured.

The RDBMS security store is required by the SAML 2.0 security providers so that the data they manage can be synchronized across all the WebLogic Server instances that share that data.

Note that Oracle does not recommend upgrading an existing domain in place to use the RDBMS security store. If you want to use the RDBMS security store, you should

configure the RDBMS security store at the time of domain creation. If you have an existing domain with which you want to use the RDBMS security store, create the new domain and migrate your existing security realm to it.

For information, see [Chapter 10, “Managing the RDBMS Security Store.”](#)

- b. Ensure that all SAML 2.0 services are configured identically in each WebLogic Server instance. If you are configuring SAML 2.0 services in a cluster, each Managed Server in that cluster must be configured individually.
 - c. Note the considerations described in [“Web Application Deployment Considerations for SAML 2.0”](#) on page 7-24.
2. If you are configuring a SAML 2.0 Identity Provider site:
- a. Create and configure an instance of the SAML 2.0 Credential Mapping provider in the security realm.
 - b. Configure the SAML 2.0 general services identically and individually in each WebLogic Server instance in the domain that will run SAML 2.0 services.
 - c. Configure the SAML 2.0 Identity Provider services identically and individually in each WebLogic Server instance in the domain that will run SAML 2.0 services.
 - d. Publish the metadata file describing your site, and manually distribute it to your Service Provider partners.
 - e. Create and configure your Service Provider partners.
3. If you are configuring a SAML 2.0 Service Provider site:
- a. Create and configure an instance of the SAML 2.0 Identity Assertion provider in the security realm.

Optionally, you may also need to create and configure an instance of the SAML Authentication provider.
 - b. Configure the SAML 2.0 general services identically and individually in each WebLogic Server instance in the domain that will run SAML 2.0 services.
 - c. Configure the SAML 2.0 Service Provider services identically and individually in each WebLogic Server instance in the domain that will run SAML 2.0 services.
 - d. Publish the metadata file describing your site, and manually distribute it to your Identity Provider partners.

- e. Create and configure your Identity Provider partners.

The sections that follow provide details about each set of main steps.

Configuring SAML 2.0 General Services

Regardless of the SAML 2.0 role in which you wish to configure a WebLogic Server instance — that is, as either a Service Provider or Identity Provider — you need to configure the server’s general SAML 2.0 services. Configuration of the SAML 2.0 general services for a WebLogic Server instance is controlled by the `SingleSignOnServicesMBean`. You can access the `SingleSignOnServicesMBean` with the WebLogic Scripting Tool or through the Administration Console, on the Environment → Servers → *ServerName* → Configuration → Federation Services → SAML 2.0 General page.

Note: You cannot configure SAML 2.0 general services in a WebLogic Server instance until you have first configured either the SAML 2.0 Identity Assertion or SAML 2.0 Credential Mapping provider and restarted the server instance.

The following sections describe SAML 2.0 general services:

- [“About SAML 2.0 General Services” on page 7-11](#)
- [“Publishing and Distributing the Metadata File” on page 7-13](#)

About SAML 2.0 General Services

The general SAML 2.0 services you configure include the following:

- Whether you wish to enable the replicated cache

Enabling the replicated cache is required if you are configuring SAML 2.0 services on two or more WebLogic Server instances in a domain, such as in a cluster. The replicated cache enables server instances to share and be synchronized with the data that is managed by the SAML 2.0 security providers; that is, either or both the SAML 2.0 Identity Assertion provider and the SAML 2.0 Credential Mapping provider.

Note that the RDBMS security store is strongly recommended if you enable the replicated cache. Therefore prior to configuring SAML 2.0 services, the preferred approach is first to create a domain that is configured to use the RDBMS security store. For more information, see [Chapter 10, “Managing the RDBMS Security Store.”](#)

- Information about the local site

The site information you enter is primarily for the benefit of the business partners in the SAML federation with whom you share it. Site information includes details about the local

contact person who is your partners' point of contact, your organization name, and your organization's URL.

- Published site URL

This URL specifies the base URL that is used to construct endpoint URLs for the various SAML 2.0 services. The published site URL should specify the host name and port at which the server is visible externally, which might not be the same at which the server is accessed locally. For example, if SAML 2.0 services are configured in a cluster, the host name and port may correspond to the load balancer or proxy server that distributes client requests to the Managed Servers in that cluster.

The published site URL should be appended with `/saml2`. For example:

```
https://www.avitek.com:7001/avitek-domain/aviserver/saml2
```

- Entity ID

The entity ID is a human-readable string that uniquely distinguishes your site from the other partner sites in your federation. When your partners need to generate or consume an assertion, the SAML 2.0 services use the entity ID as part of the process of identifying the partner that corresponds with that assertion.

- Whether recipient check is enabled

If enabled, the recipient of the authentication request or response must match the URL in the HTTP Request.

- Whether TLS/SSL client authentication is required for invocations on the Artifact Resolution Service. If enabled, SAML artifacts are encrypted when transmitted to partners.

- Transport Layer Security keystore alias and passphrase, used for retrieving the server's keys that are used for securing outgoing communications with partners.

- Whether Basic authentication client authentication is required when your partners invoke the HTTPS bindings of the local site.

If you enable this setting, you also specify the client username and password to be used. These credentials are then included in the published metadata file that you share with your federated partners.

- Whether requests for SAML artifacts received from your partners must be signed.

- Configuration settings for the SAML artifact cache.

- Keystore alias and passphrase for the key to be used when signing documents sent to your federated partners, such as authentication requests or responses.

For information about the steps for configuring SAML 2.0 general services, see [Configure SAML 2.0 general services](#) in the *Administration Console Online Help*.

Publishing and Distributing the Metadata File

The local site information that is needed by your federated partners — such as the local site contact information, entity ID, published site URL, whether TLS/SSL client authentication is required, and so on — is published to a metadata file by clicking **Publish Meta Data** in the SAML 2.0 General console page.

When you publish the metadata file, you specify an existing directory on the local machine in which the file can be created. The process of distributing the metadata file to your federated partners is a detail that is not implemented by WebLogic Server. However, you may send this file via a number of commonly used mechanisms suitable for securely transferring electronic documents, such as encrypted email or secure FTP.

Keep the following in mind regarding the metadata file:

- Before you publish the metadata file, you should configure the Identity Provider and/or Service Provider services for the SAML 2.0 roles in which the WebLogic Server instances in your domain are enabled to function.

The configuration data for the SAML 2.0 services your site offers that is needed by your federated partners is included in this metadata file, greatly simplifying the tasks your partners perform to import your signing certificates, identify your site's SAML 2.0 service endpoints, and use the correct binding types for connecting to your site's services, and so on.

- You should have only a single version of the metadata file that you share with your federated partners, even if your site functions in the role of Service Provider with some partners and Identity Provider with others. By having only a single version of the metadata file, you reduce the likelihood that your configuration settings might become incompatible with those of a partner.
- If you change the local site's SAML 2.0 configuration, you should update your metadata file. Because the metadata file is shared with your partners, it will be convenient to minimize the frequency with which you update your SAML 2.0 configuration so that your partners can minimize the need to make concomitant updates to their own partner registries.
- When you receive a metadata file from a federated partner, place it in a location that can be accessed by all the nodes in your domain in which SAML 2.0 services are configured. At

the time you create a partner, you bring the contents the partner's metadata file into the partner registry.

Operations on the metadata file are available via the `com.bea.security.saml2.providers.registry.Partner` Java interface.

Configuring an Identity Provider Site for SAML 2.0 Single Sign-On

This section presents the following topics:

- “Configure the SAML 2.0 Credential Mapping Provider” on page 7-14
- “Configure SAML 2.0 Identity Provider Services” on page 7-14
- “Create and Configure Web Single Sign-On Service Provider Partners” on page 7-15

Configure the SAML 2.0 Credential Mapping Provider

In your security realm, create a SAML 2.0 Credential Mapping provider instance. The SAML 2.0 Credential Mapping provider is not part of the default security realm. See “Configure a SAML 2.0 Credential Mapping Provider for SAML 2.0” on page 4-20.

Configure the SAML 2.0 Credential Mapping provider as a SAML authority. Attributes you specify include the following:

- Issuer URI
- Name Qualifier
- Life span attributes for generated SAML 2.0 assertions
- Name mapper class name
- Whether generated assertions should include attribute information, which specify the groups to which the identity contained in the assertion belongs

After you configure the SAML 2.0 Credential Mapping provider, configure SAML 2.0 general services, as described in “Configure SAML 2.0 General Services” on page 7-11.

Configure SAML 2.0 Identity Provider Services

Configuration of a WebLogic Server instance as a SAML 2.0 Identity Provider site is controlled by the `SingleSignOnServicesMBean`. You can access the `SingleSignOnServicesMBean` using the WebLogic Scripting Tool (WLST), or through the Administration Console by using the

Environment → Servers → *ServerName* → Configuration → Federation Services → SAML 2.0 Identity Provider page.

The sections that follow summarize the configuration tasks. For more information about performing these tasks, see [Configure SAML 2.0 Identity Provider services](#) in the *Administration Console Online Help*.

Enable the SAML 2.0 Identity Provider Site

From the SAML 2.0 Identity Provider page in the console, allow the WebLogic Server instance to serve as an Identity Provider site by setting the Enabled attribute to true.

Specify a Custom Login Web Application

Optionally, you may use a custom login web application to authenticate users into the Identity Provider site. To configure a custom login web application, enable the Login Customized attribute and specify the URL of the web application.

Enable Binding Types

Oracle recommends enabling all the available binding types for the endpoints of the Identity Provider services; namely, POST, Redirect, and Artifact. Optionally you may select a preferred binding type.

Publish Your Site's Metadata File

After you have configured the SAML 2.0 general services and Identity Provider services, publish your site's metadata file and distribute it to your federated partners, as described in [“Publishing and Distributing the Metadata File”](#) on page 7-13.

Create and Configure Web Single Sign-On Service Provider Partners

A SAML 2.0 Service Provider partner is an entity that consumes the SAML 2.0 assertions generated by the Identity Provider site. The configuration of Service Provider partners is available from the Administration Console, using the Security Realms → *RealmName* → Providers → Credential Mapper → *SAML2CredentialMapperName* → Management page.

The attributes that can be set on this console page can also be accessed programmatically via a set of Java interfaces, which are identified in the sections that follow.

See [Create a SAML 2.0 Web Single Sign-on Service Provider partner](#) in the *Administration Console Online Help* for complete details about the specific steps for configuring a Service Provider partner. For a summary of the site information, signing certificates, and service endpoint

information available when you configure a web single sign-on partner, see [“Viewing Partner Site, Certificate, and Service Endpoint Information”](#) on page 7-23.

Obtain Your Service Provider Partner’s Metadata File

Before you configure a Service Provider partner for web single sign-on, you need to obtain the partner’s SAML 2.0 metadata file via a trusted and secure mechanism, such as encrypted email or an SSL-enabled FTP site. Your partner’s metadata file describes the partner site and binding support, includes the partner’s certificates and keys, contains your partner’s SAML 2.0 service endpoints, and more. Copy the partner’s metadata file into a location that can be accessed by each node in your domain configured for SAML 2.0.

The SAML 2.0 metadata file is described in [“Publishing and Distributing the Metadata File”](#) on page 7-13.

Create Partner and Enable Interactions

To create and enable a Service Provider partner for web single sign-on:

1. From the Management tab of the SAML 2.0 Credential Mapping provider page, specify the partner’s name and metadata file.
2. From the General tab of the partner configuration page, enable interactions between the partner and the WebLogic Server instance

WebLogic Server provides the `com.bea.security.saml2.providers.registry.Partner` Java interface for configuring these attributes.

Configure How Assertions are Generated

Optionally from the General tab of the partner configuration page in the console, you can configure the following attributes of the SAML 2.0 assertions generated specifically for this Service Provider partner:

- The Service Provider Name Mapper Class name

This is the Java class that overrides the default username mapper class with which the SAML 2.0 Credential Mapping provider is configured in this security realm.

- Time to Live attributes

The Time to Live attributes specify the interval of time during which the assertions generated for this partner are valid. These attributes prevent expired assertions from being used.

- Whether to generate attribute information that is included in assertions
If enabled, the SAML 2.0 Credential Mapping provider adds, as attributes in the assertion, the groups to which the corresponding user belongs.
- Whether the assertions sent to this partner must be disposed of immediately after use
- Whether this server's signing certificate is included in assertions generated for this partner

WebLogic Server provides the

`com.bea.security.saml2.providers.registry.SPPartner` Java interface for configuring these attributes.

Configure How Documents Are Signed

You can use the General tab of the Service Provider partner configuration page to determine how the following documents exchanged with this partner must be signed:

- Assertions
Operations on this attribute are available in the `com.bea.security.saml2.providers.registry.SPPartner` interface
- Authentication requests
Operations on this attribute are available in the `com.bea.security.saml2.providers.registry.WebSSOSPPartner` interface
- Artifact requests
Operations on this attribute are available in the `com.bea.security.saml2.providers.registry.WebSSOPartner` interface

The attributes for specifying whether this partner accepts only signed assertions, or whether authentication requests must be signed, are read-only: they are derived from the partner's metadata file.

Configure Artifact Binding and Transport Settings

Optionally, you also use the General tab of the Service Provider partner configuration page to configure the following:

- Whether SAML artifacts are delivered to this partner via the HTTP POST binding. If so, you may also specify the URI of a custom web application that generates the HTTP POST form for sending the SAML artifact.

- The URI of a custom web application that generate the HTTP POST form for sending request or response messages via the POST binding.

Operations on these attributes are available via the

[com.bea.security.saml2.providers.registry.WebSSOPartner](#) Java interface.

For added security in the exchange of documents with this partner, you can also specify a client user name and password to be used by the Service Provider partner when connecting to the local site's binding using Basic authentication. This attribute is available via the

[com.bea.security.saml2.providers.registry.BindingClientPartner](#) Java interface.

Configuring a Service Provider Site for SAML 2.0 Single Sign-On

This section presents the following topics:

- [“Configure the SAML 2.0 Identity Assertion Provider” on page 7-18](#)
- [“Configure the SAML Authentication Provider” on page 7-19](#)
- [“Configure SAML 2.0 Service Provider Services” on page 7-19](#)
- [“Create and Configure Web Single Sign-On Identity Provider Partners” on page 7-20](#)

Configure the SAML 2.0 Identity Assertion Provider

In your security realm, create an instance of the SAML 2.0 Identity Assertion provider. The SAML 2.0 Identity Assertion provider is not part of the default security realm. The attributes you specify for the SAML 2.0 Identity Assertion provider include the following:

- Whether the replicated cache is enabled
 - If you are configuring SAML 2.0 Identity Provider services in two or more server instances in the domain, this attribute must be enabled.
- A custom name mapper class that overrides the default SAML 2.0 assertion name mapper class

For more information about this security provider, see [“Configuring a SAML 2.0 Identity Assertion Provider for SAML 2.0” on page 5-31](#).

Configure the SAML Authentication Provider

If you plan to enable virtual users, or consume attribute statements contained in assertions that you receive from your Identity Provider partners, you need to create and configure an instance of the SAML Authentication provider. For more information, see [“Configuring the SAML Authentication Provider” on page 5-18](#).

Configure SAML 2.0 General Services

After configuring the SAML 2.0 Identity Assertion provider, and optionally the SAML Authentication provider, configure the SAML 2.0 general services, as described in [“Configuring SAML 2.0 General Services” on page 7-11](#).

Configure SAML 2.0 Service Provider Services

Configuration of a WebLogic Server instance as a SAML 2.0 Service Provider site is controlled by the `SingleSignOnServicesMBean`. You can access the `SingleSignOnServicesMBean` using the WebLogic Scripting Tool (WLST), or through the Administration Console using the Environment → Servers → *ServerName* → Configuration → Federation Services → SAML 2.0 Service Provider page.

You configure the SAML 2.0 Service Provider site attributes as summarized in the sections that follow. For more information about these configuration tasks, see [Configure SAML 2.0 Service Provider services](#) in the *Administration Console Online Help*.

Enable the SAML 2.0 Service Provider Site

From the Federation Services: SAML 2.0 Identity Provider page in the console, allow the WebLogic Server instance to serve as a Service Provider site by setting the Enabled attribute to true.

Specify How Documents Must Be Signed

Optionally you may enable the attributes that set the following document signing requirements:

- Whether authentication requests sent to Identity Provider partners are signed
- Whether assertions received from Identity Provider partners are signed

Specify How Authentication Requests Are Managed

Optionally you may enable the following attributes of the authentication request cache:

- Maximum cache size

- Time-out value for authentication requests, which establishes the time interval beyond which stored authentication requests are expired

Enable Binding Types

Oracle recommends enabling all the available binding types for the endpoints of the Service Provider services; namely, POST, Redirect, and Artifact. Optionally you may specify a preferred binding type.

Set Default URL

Optionally, you may specify the URL to which unsolicited authentication responses are sent if they do not contain an accompanying target URL.

Create and Configure Web Single Sign-On Identity Provider Partners

A SAML 2.0 Identity Provider partner is an entity that generates SAML 2.0 assertions consumed by the Service Provider site. The configuration of Identity Provider partners is available from the Administration Console, using the Security Realms → *RealmName* → Providers → Authentication → *SAML2IdentityAsserterName* → Management page.

The attributes that can be set on this console page can also be accessed programmatically via a set of Java interfaces, which are identified in the sections that follow.

See [Create a SAML 2.0 Web Single Sign-on Identity Provider partner](#) in the *Administration Console Online Help* for complete details about the specific steps for configuring a Service Provider partner.

For a summary of the site information, signing certificates, and service endpoint information available when you configure a web single sign-on partner, see [“Viewing Partner Site, Certificate, and Service Endpoint Information”](#) on page 7-23.

The following sections summarize tasks for configuring an Identity Provider partner.

Obtain Your Identity Provider Partner’s Metadata File

Before you configure an Identity Provider partner for web single sign-on, you need to obtain the partner’s SAML 2.0 metadata file via a trusted and secure mechanism, such as encrypted email or an SSL-enabled FTP site. Your partner’s metadata file describes that partner site and binding support, includes the partner’s certificates and keys, and so on. Copy the partner’s metadata file into a location that can be accessed by each node in your domain configured for SAML 2.0.

The SAML 2.0 metadata file is described in [“Publishing and Distributing the Metadata File”](#) on page 7-13.

Create Partner and Enable Interactions

To create an Identity Provider partner and enable interactions for web single sign-on:

- From the Management tab of the SAML 2.0 Identity Assertion configuration page, specify the partner's name and metadata file.
- From the General tab of the partner configuration page, enable interactions between the partner and the WebLogic Server instance.

WebLogic Server provides the `com.bea.security.saml2.providers.registry.Partner` Java interface for configuring these attributes.

Configure Authentication Requests and Assertions

Optionally, you can configure the following attributes of the authentication requests generated for, and assertions received from, this Identity Provider partner:

- The Identity Provider Name Mapper Class name

This is the custom Java class that overrides the default username mapper class with which the SAML 2.0 Identity Assertion provider is configured in this security realm. The custom class you specify is used only for identities contained in assertions received from this particular partner.

Operations on this attribute are available in the `com.bea.security.saml2.providers.registry.IdPPartner` Java interface.

- Whether the identities contained in assertions received from this partner are mapped to virtual users in the security realm

Note: To use this attribute, you must have a SAML Authentication provider configured in the realm.

Operations on this attribute are available in the `com.bea.security.saml2.providers.registry.IdPPartner` Java interface.

- Whether to consume attribute information contained in assertions received from this partner

If enabled, the SAML 2.0 Identity Assertion provider extracts attribute information from the assertion, which it uses in conjunction with the SAML Authentication provider (which must be configured in the security realm) to determine the groups in the security realm to which the corresponding user belongs.

Operations on this attribute are available in the `com.bea.security.saml2.providers.registry.IdPPartner` Java interface.

- Whether authentication requests sent to this Identity Provider partner must be signed. This is a read-only attribute that is derived from the partner's metadata file.

Operations on this attribute are available in the [com.bea.security.saml2.providers.registry.WebSSOIDPPartner](#) Java interface.

- Whether SAML artifact requests received from this Identity Provider partner must be signed.

Operations on this attribute are available in the [com.bea.security.saml2.providers.registry.WebSSOPartner](#) Java interface.

Configure Redirect URIs

You can configure a set of URIs that, if invoked by an unauthenticated user, cause the user request to be redirected to the Identity Provider partner where the user can be authenticated.

WebLogic Server provides the

[com.bea.security.saml2.providers.registry.WebSSOIDPPartner](#) Java interface for configuring this attribute.

Configure Binding and Transport Settings

Optionally, you also use the General tab of the Service Provider partner configuration page to configure the following:

- Whether SAML artifacts are delivered to this partner via the HTTP POST method. If so, you may also specify the URI of a custom web application that generates the HTTP POST form for sending the SAML artifact.
- The URL of the custom web application that generates the POST form for carrying the SAML response for POST bindings to this Identity Provider partner.
- The URL of the custom web application that generates the POST form for carrying the SAML response for Artifact bindings to this Identity Provider partner.

Operations on these attributes are available via the

[com.bea.security.saml2.providers.registry.WebSSOPartner](#) Java interface.

For added security in the exchange of documents with this partner, you can also specify a client user name and password to be used by this Identity Provider partner when connecting to the local site's binding using Basic authentication. This attribute is available via the

[com.bea.security.saml2.providers.registry.BindingClientPartner](#) Java interface.

Viewing Partner Site, Certificate, and Service Endpoint Information

When you configure SAML 2.0 partners, the partner configuration pages displayed by the Administration Console include tabs for viewing and configuring the following additional information about the partner:

- The Site tab displays information about the Service Provider partner, which is derived from the partner's metadata file. The data in this tab is read-only.

WebLogic Server provides the

[com.bea.security.saml2.providers.registry.MetadataPartner](#) Java interface for partner site information.

- The Single Sign-On Signing Certificate tab displays details about the partner's signing certificate, which are also derived from the partner's metadata file. The data in this tab is read-only.

Operations on these attributes are available from the

[com.bea.security.saml2.providers.registry.WebSSOPartner](#) Java interface.

- The Transport Layer Client Certificate tab displays partner's transport layer client certificate. You can optionally import this certificate by clicking **Import Certificate from File**.

Operations on this attribute is available from the

[com.bea.security.saml2.providers.registry.BindingClientPartner](#) Java interface.

- When configuring Service Provider partners, the Assertion Consumer Service Endpoints tab is available, which displays the Service Provider partner's ACS endpoints. This data is also available from the [com.bea.security.saml2.providers.registry.WebSSOSPPartner](#) Java interface.
- When configuring Identity Provider partners, the Single Sign-On Service Endpoints tab is available, which displays the Identity Provider partner's single sign-on service endpoints. This data is also available from the [com.bea.security.saml2.providers.registry.WebSSOIdPPartner](#) Java interface.
- The Artifact Resolution Service Endpoints tab displays the partner's ARS endpoints. This data is also available from the [com.bea.security.saml2.providers.registry.WebSSOPartner](#) Java interface

Web Application Deployment Considerations for SAML 2.0

When deploying web applications for SAML-based SSO in a clustered environment, note the following considerations to prevent SAML-based single sign-on from failing:

- [“Deployment Descriptor Recommendations” on page 7-24](#)
- [“Login Application Considerations for Clustered Environments” on page 7-25](#)

Deployment Descriptor Recommendations

Note the following recommendations regarding the use of the following elements in deployment descriptor files:

- `relogin-enabled`
- `cookie-name`

Use of `relogin-enabled` with CLIENT-CERT Authentication

If a user logs in to a web application and tries to access a resource for which that user is not authorized, an HTTP FORBIDDEN (403) response is generated. This is standard web application behavior. However, for backwards compatibility with earlier releases, WebLogic Server permits web applications to use the `relogin-enabled` element in the `weblogic.xml` deployment descriptor file, so that the response to an access failure results in a request to authenticate. In certain circumstances, it can cause SAML 2.0 based web single sign-on to fail.

Normally, the SAML 2.0 Assertion Consumer Service (ACS) logs the user into the application and redirects the user request to the target web application. However, if that web application is enabled for SAML 2.0 single sign-on, is protected by CLIENT-CERT authentication, and has the `relogin-enabled` deployment descriptor element set to `true`, an infinite loop can occur in which a request to authenticate a user is issued repeatedly. This loop can occur when a user is logged in to the web application and attempts to access a resource for which the user is not permitted: instead of generating a FORBIDDEN message, a new authentication request is generated that triggers another SAML 2.0 based web single sign-on attempt.

To prevent this situation from occurring in a web application that is protected by CLIENT-CERT authentication, either remove the `relogin-enabled` deployment descriptor element for the web application, or set the element to `false`. This enables standard web application authentication behavior.

Use of Non-default Cookie Name

When the Assertion Consumer Service logs in the Subject contained in an assertion, an HTTP servlet session is created using the default cookie name `JSESSIONID`. After successfully processing the assertion, the ACS redirects the user's request to the target web application. If the target web application uses a cookie name other than `JSESSIONID`, the Subject's identity is not propagated to the target web application. As a result, the servlet container treats the user as if unauthenticated, and consequently issues an authentication request.

To avoid this situation, do not change the default cookie name when deploying web applications in a domain that are intended to be accessed by SAML 2.0 based single sign-on.

Login Application Considerations for Clustered Environments

Note the following two login limitations that are rare in clustered environments, but if they occur, they may prevent a single sign-on session from succeeding.

- When an Identity Provider's single sign-on service receives an authentication request, it redirects that request to the login application to authenticate the user. The login application must execute on the same cluster node as that single sign-on service. If not, the Identity Provider is unable to produce a SAML 2.0 assertion even if the authentication succeeds.

Under normal circumstances, the login application executes on the same node as the single sign-on service, so likelihood of the authentication request being redirected to a login application executing on a different node in the domain is very small. However, it may happen if an authentication request is redirected by a cluster node different than the one hosting the login application. You can almost always prevent this situation from occurring if you configure the Identity Provider to use the default login URI with Basic authentication.

- When the SAML 2.0 Assertion Consumer Service (ACS) successfully consumes an assertion, it logs in the Subject represented by the assertion. The ACS then redirects the user request to the target application. Normally, the target application executes on the same node as the ACS. However, in rare circumstances, the target application to which is the user request is redirected executes on a cluster node other than the one hosting the ACS on which the login occurred. When this circumstance occurs, the identity represented by the assertion is not propagated to the target application node. The result is either another attempt at the single sign-on process, or denied access.

Because the target application executes on the same node as the ACS, this situation is expected to occur very rarely.

Configuring Single Sign-On with Web Browsers and HTTP Clients

Migrating Security Data

You can export security data from one security realm or security provider and import the data into another realm or provider. The following sections provide information about exporting and importing security data.

- [“Overview of Security Data Migration”](#) on page 8-1
- [“Migration Concepts”](#) on page 8-2
- [“Formats and Constraints Supported by WebLogic Security Providers”](#) on page 8-3
- [“Migrating Data with WLST”](#) on page 8-6

Overview of Security Data Migration

WebLogic security realms persist different kinds of security data — for example, users and groups (for the WebLogic Authentication provider), security policies (for the XACML Authorization provider), security roles (for the XACML Role Mapping provider), and credential maps (for the WebLogic Credential Mapping provider). When you configure a new security realm or a new security provider, you may prefer to use the security data from your existing realm or provider, rather than recreate all the users, groups, policies, roles, and credential maps. Several WebLogic security providers support security data migration. This means you can export security data from one security realm, and import it into a new security realm. You can migrate security data for each security provider individually, or migrate security data for all the WebLogic security providers at once (that is, security data for an entire security realm). Note that you can only migrate security data from one provider to another if the providers use the same data format. See [“Formats and Constraints Supported by WebLogic Security Providers”](#) on page 8-3. You

migrate security data through the WebLogic Administration Console or by using the WebLogic Scripting Tool (WLST).

Migrating security data may be helpful when you:

- Transition from development to production mode.
- Copy production mode security configurations to security realms in new WebLogic Server domains.
- Move data from one security realm to a new security realm in the same WebLogic Server domain, where one or more of the default WebLogic security providers will be replaced with new security providers.

The remainder of this section describes security migration concepts, the formats and constraints supported by the WebLogic security providers, and steps for migrating security data with WLST.

To migrate security data with the WebLogic Administration Console, see the following topics in the *Administration Console Online Help*:

- [Export data from security realms](#)
- [Import data into security realms](#)
- [Export data from security providers](#)
- [Import data into security providers](#)

Migration Concepts

A **format** is a data format that specifies how security data should be exported or imported.

Supported formats are the list of data formats that a given security provider understands how to process.

Constraints are key/value pairs that specify options to the export or import process. Use constraints to control which security data is exported to or imported from the security provider's database (in the case of the WebLogic Server security providers, the embedded LDAP server). For example, you may want to export only users (not groups) from an Authentication provider's database. **Supported constraints** are the list of constraints you can specify during the migration process for a particular security provider. For example, you can specify that an Authentication provider's database be used to import users and groups, but not security policies.

Export files are the files to which security data is written (in the specified format) during the export portion of the migration process. **Import files** are files from which security data is read

(also in the specified format) during the import portion of the migration process. Both export and import files are simply temporary storage locations for security data as it is migrated from one security provider’s data store to another security provider’s data store.

Formats and Constraints Supported by WebLogic Security Providers

In order for security data to be exported and imported between security providers, both security providers must process the same format. Some data formats used for the WebLogic Server security providers are unpublished; therefore, you cannot currently migrate security data from a WebLogic security provider to a custom security provider, or vice versa, using the unpublished formats.

WebLogic security providers support the following import and export formats.

Table 8-1 Import and Export Formats Supported by the WebLogic Security Providers

WebLogic Provider	Supported Format
WebLogic Authentication Provider	DefaultAtn—unpublished format
XACML Authorization Provider	XACML—standard XACML 2.0 format DefaultAtz—unpublished format
WebLogic Authorization Provider	DefaultAtz—unpublished format
XACML Role Mapping Provider	XACML—standard XACML 2.0 format DefaultRoles—unpublished format
WebLogic Role Mapping Provider	DefaultRoles—unpublished format
WebLogic Credential Mapping Provider	DefaultCreds—unpublished format
SAML Identity Asserter V2 SAML Credential Mapping Provider V2	XML Partner Registry—An XML format defined by the SAML partner registry schema JKS Key Store—A key store file format for importing and exporting partner certificates only LDIF Template—LDIF format

WebLogic security providers support the following import and export constraints.

Table 8-2 Constraints Supported by the WebLogic Security Providers

WebLogic Security Provider	Supported Constraints	Description
WebLogic Authentication	users groups	Export all users or all groups
XACML Authorization	None	
WebLogic Authorization	None	
XACML Role Mapping	None	
WebLogic Role Mapping	None	
WebLogic Credential Mapping	passwords	With the constraint passwords=cleartext, passwords will be exported in clear text. Otherwise, they will be exported in encrypted form.
SAML Identity Asserter V2 SAML Credential Mapping V2	partners	Which partners to import or export. The constraint value can be one of: <ul style="list-style-type: none"> all—all partners none—no partners list—only listed partners enabled—only enabled partners disabled—only disabled partners

Table 8-2 Constraints Supported by the WebLogic Security Providers

SAML Identity Asserter V2 SAML Credential Mapping V2	certificates	Which certificates to import or export. The constraint value can be one of the following: all—all certificates none—no certificates list—only listed certificates referenced—only certificates referenced by a partner
SAML Identity Asserter V2 SAML Credential Mapping V2	passwords	With the constraint <code>passwords=cleartext</code> , passwords will be exported in clear text. Otherwise, they will be exported in encrypted form.
SAML Identity Asserter V2 SAML Credential Mapping V2	importMode	Specifies how to resolve name conflicts between the imported data and existing data in the SAML registry. The constraint value can be one of the following: fail—the import operation will fail if conflicts are detected (default) rename—rename the imported entry that conflicts replace—replace the existing entry with the conflicting imported entry

When exporting from the WebLogic Credential Mapping provider, SAML Credential Mapping provider, or SAML Identity Asserter, you need to specify whether or not the passwords for the credentials are exported in clear text. The constraint `passwords=cleartext` specifies that passwords will be exported in clear text. Otherwise, they will be exported in encrypted form. The mechanism used to encrypt passwords in each WebLogic Server domain is different; therefore, you want to export passwords in clear text if you plan to use them in a different WebLogic Server

domain. After the credential maps are imported into the new WebLogic Server domain, the passwords are encrypted. Carefully protect the directory and file in which you export credential maps in clear text as secure data is available on your system during the migration process.

Migrating Data with WLST

You can use the WebLogic Scripting Tool (WLST) to export and import data from a security provider. Access the Runtime MBean for the security provider and use its `importData` or `exportData` operation. For example, you might use WLST to import data using commands like these:

```
domainRuntime()  
cd('DomainServices/DomainRuntimeService/DomainConfiguration/mydomain/SecurityConfiguration/mydomain/DefaultRealm/myrealm/path-to-MBean/mbeanname')  
cmo.importData(format, filename, constraints)
```

where

mbeanname—Name of the security provider MBean.

format—A format that is valid for the particular security provider. See [Table 8-1, “Import and Export Formats Supported by the WebLogic Security Providers,”](#) on page 8-3.

filename—The directory location and filename in which to export or import the security data. Remember that, regardless of whether you are using a UNIX or Windows operating system, you need to use a forward slash, not a back slash, as a path separator for pathname arguments in WLST commands.

constraints—The constraints that limit the data to be exported or imported

For more information, see [WebLogic Scripting Tool](#).

Migrating Data Using `weblogic.admin`

Note: The `weblogic.Admin` utility is deprecated. Use WLST instead.

You can also use the `weblogic.Admin` utility to export and import security data between security realms and security providers. The format of the command is:

```
java weblogic.Admin -username username -password password \  
INVOKE -mbean mbeanname \  
-method methodname dataformat filename constraints
```

where

username—Name of the Admin user

password—Password of the Admin user

mbeanname—Name of the security provider MBean.

methodname—`exportData` or `importData`

dataFormat—`DefaultAtn`, `DefaultAtz`, `DefaultRoles`, or `DefaultCreds`

filename—The directory location and filename in which to export or import the security data

constraints—The constraints that limit the data to be exported or imported

Note: The directory and file into which you export the security data should be carefully protected with operating system security as they contain secure information about your deployment.

For example:

```
java weblogic.Admin -username system -password weblogic INVOKE -mbean
Security:Name=myrealmDefaultAuthenticator -method importData DefaultAtn
d:\temp\security.info ""
```

Migrating Security Data

Managing the Embedded LDAP Server

WebLogic Server includes an embedded LDAP server that acts as the default security provider data store for the WebLogic Authentication, Authorization, Credential Mapping, and Role Mapping providers. The following sections explain how to manage the embedded LDAP server:

- [“Configuring the Embedded LDAP Server” on page 9-1](#)
- [“Embedded LDAP Server Replication” on page 9-2](#)
- [“Viewing the Contents of the Embedded LDAP Server from an LDAP Browser” on page 9-3](#)
- [“Exporting and Importing Information in the Embedded LDAP Server” on page 9-4](#)
- [“LDAP Access Control Syntax” on page 9-6](#)

Configuring the Embedded LDAP Server

The embedded LDAP server contains user, group, group membership, security role, security policy, and credential map information. By default, each WebLogic Server domain has an embedded LDAP server configured with the default values set for each type of information. The WebLogic Authentication, Authorization, Credential Mapping, and Role Mapping providers use the embedded LDAP server as their data store. If you use any of these providers in a new security realm, you may want to change the default values for the embedded LDAP server to optimize its use in your environment.

Note: The performance of the embedded LDAP server is best with fewer than 10,000 users. If you have more users, consider using a different LDAP server and Authentication provider.

See [Configure the embedded LDAP server](#) in the *Administration Console Online Help*.

The data file and change log file used by the embedded LDAP server can potentially grow quite large. You can configure maximum sizes for these files with the following `weblogic.Server` command line arguments:

- `-Dweblogic.security.ldap.maxSize=<max bytes>`, which limits the size of the data file used by the embedded LDAP server. When the data file exceeds the specified size, WebLogic Server eliminates from the data file space occupied by deleted entries.
- `-Dweblogic.security.ldap.changeLogThreshold=<number of entries>`, which limits the size of the change log file used by the embedded LDAP server. When the change log file exceeds the specified number of entries, WebLogic Server truncates the change log by removing all entries that have been sent to all managed servers.

Embedded LDAP Server Replication

The WebLogic Server embedded LDAP server for a domain consists of a master LDAP server, maintained in the domain's Administration Server, and a replicated LDAP server maintained in each Managed Server in the domain. When changes are made using a Managed Server, updates are sent to the embedded LDAP server on the Administration Server. The embedded LDAP server on the Administration Server maintains a log of all changes. The embedded LDAP server on the Administration Server also maintains a list of Managed Servers and the current change status for each one. The embedded LDAP server on the Administration Server sends appropriate changes to each Managed Server and updates the change status for each server. This process occurs when an update is made to the embedded LDAP server on the Administration Server. However, depending on the number of updates, it may take several seconds or more for the change to be replicated to the Managed Server.

You can configure the behavior of the embedded LDAP server on the Administration Server and the Managed Servers in a domain using the Administration Console. On the Domain → Security → Embedded LDAP Server page in the Administration Console, you can set these attributes:

- **Refresh Replica At Startup**—Specifies whether the embedded LDAP server in a Managed Server should refresh all replicated data at boot time. This setting is useful if you have made many changes when the Managed Server was not active, and you want to download the entire replica instead of having the Administration Server push each change to the Managed Server.

- Master First—Specifies whether a Managed Server should always connect to the embedded LDAP server on the Administration Server, instead of connecting to the local replicated LDAP server.

See [Configure the embedded LDAP server](#) in the *Administration Console Online Help*.

Note: Deleting and modifying the configured security providers through the WebLogic Administration Console may require manual clean up of the embedded LDAP server. Use an external LDAP browser to delete unnecessary information.

Viewing the Contents of the Embedded LDAP Server from an LDAP Browser

To view the contents of the embedded LDAP server through an LDAP browser:

1. Download and install an external LDAP browser. You can find one LDAP browser at the following location:

<http://www-unix.mcs.anl.gov/~gawor/ldap/>

In this procedure it is assumed that you are using this LDAP browser; other LDAP browsers may differ in detail.

2. In the WebLogic Server Administration Console, change the credential for the embedded LDAP server:
 - a. Expand Domain → Security → Embedded LDAP.
 - b. In the Credential field, enter the new credential.
 - c. In the Confirm Credential field, enter the new credential again.
 - d. Click Save.
 - e. Reboot WebLogic Server.

Caution: Changing the credential can affect the operation of the domain. Do not perform this step on a production server.

3. Start the LDAP browser. To start the LDAP Browser/Editor mentioned in step 1, use this command:

```
lbe.sh
```

4. In the LDAP browser, configure a new connection in the LDAP browser:

- a. Select the QuickConnect tab.
 - a. Set the host field to `localhost`.
 - b. Set the port field to `7001` (`7002` if SSL is being used).
 - c. Set the Base DN field to `dc=mydomain` where `mydomain` is the name of the WebLogic Server domain you are using.
 - d. Uncheck the Anonymous Bind option.
 - e. Set the User DN field to `cn=Admin`.
 - f. Set the Password field to the credential you specified in Step 2.
5. Click the new connection.

Use the LDAP browser to navigate the hierarchy of the embedded LDAP server.

Note: You can also view the contents of the embedded LDAP server by exporting its data and reviewing the exported file. See [“Exporting and Importing Information in the Embedded LDAP Server”](#) on page 9-4.

Exporting and Importing Information in the Embedded LDAP Server

You can export and import data from the embedded LDAP server using either the WebLogic Server Administration Console or an LDAP browser. To export and import data with the Console, use the Migration page of each security provider. See [Export data from a security provider](#) and [Import data into a security provider](#) in the *Administration Console Online Help*.

WARNING: When you use the Administration Console Migration tab to export security data, the export process deletes any existing files in the target directory with the `.dat` extension. Always export security data to an empty directory.

This section describes how to use an LDAP browser to export and import data stored in the embedded LDAP server. [Table 9-1](#) summarizes where data is stored in the hierarchy of the embedded LDAP server.

Table 9-1 Location of Security Data in the Embedded LDAP Server

Security Data	Embedded LDAP Server DN
Users	<i>ou=people,ou=myrealm,dc=mydomain</i>
Groups	<i>ou=groups,ou=myrealm,dc=mydomain</i>
Security roles	<i>ou=ERole,ou=myrealm,dc=mydomain</i>
Security policies	<i>ou=EResource,ou=myrealm,dc=mydomain</i>

To export security data from the embedded LDAP server using the LDAP Browser/Editor:

1. Enter the following command at a command prompt to start the LDAP Browser/Editor:
`lbe.sh`
2. Specify the data to be exported (for example, to export users specify *ou=people,ou=myrealm,dc=mydomain*).
3. Select the LDIF → Export option.
4. Select Export all children.
5. Specify the name of the file into which the data will be exported.

To import security data into the embedded LDAP server using the LDAP Browser/Editor:

1. Enter the following command at a command prompt to start the LDAP browser:
`lbe.sh`
2. Specify the data to be imported (for example, to import users, specify *ou=people,ou=myrealm,dc=mydomain*).
3. In the LDAP Browser/Editor, select the LDIF → Import option.
4. Select Update/Add.
5. Specify the name of the file from which the data will be imported.

LDAP Access Control Syntax

The embedded LDAP server supports the IETF LDAP Access Control Model for LDAPv3. This section describes how that access control is implemented within the embedded LDAP server. You can apply these rules directly to entries within the directory as intended by the standard or you can configure and maintain them by editing the access control file (`acls.prop`).

Note: The default behavior of the embedded LDAP server is to allow access only from the Admin account in WebLogic Server. The WebLogic security providers use only the Admin account to access the embedded LDAP server. If you are not planning to access the embedded LDAP server from an external LDAP browser or if you are planning only to use the Admin account, you do not need to edit the `acls.prop` file and can ignore the information in this section.

The Access Control File

The access control file (`acls.prop`) maintained by the embedded LDAP server contains the complete list of access control lists (ACLs) for an entire LDAP directory. Each line in the access control file contains a single access control rule. An access control rule is made up of the following components:

- Location in the LDAP directory where the rule applies. See [“Access Control Location” on page 9-7](#).
- Scope within that location to which the rule applies. See [“Access Control Scope” on page 9-7](#).
- Access rights (either grant or deny). See [“Access Rights” on page 9-7](#).
- Permissions (either grant or deny). See [“Attribute Permissions” on page 9-8](#) and [“Entry Permissions” on page 9-9](#).
- Attributes to which the rule applies. See [“Attributes Types” on page 9-11](#).
- Subject being granted or denied access. See [“Subject Types” on page 9-11](#).

[Listing 9-1](#) shows a sample access control file.

Listing 9-1 Sample `acl.props` File

```
[root]|entry#grant:r,b,t#[all]#public
```

```

ou=Employees,dc=octetstring,dc=com|subtree#grant:r,c#[all]#public:
ou=Employees,dc=octetstring,dc=com|subtree#grant:b,t#[entry]#public:
ou=Employees,dc=octetstring,dc=com|subtree#deny:r,c#userpassword#public:
ou=Employees,dc=octetstring,dc=com|subtree#grant:r#userpassword#this:
ou=Employees,dc=octetstring,dc=com|subtree#grant:w,o#userpassword,title,
description,
postaladdress,telephonenumber#this:
cn=schema|entry#grant:r#[all]#public:

```

Access Control Location

Each access control rule is applied to a given location in the LDAP directory. The location is normally a distinguished name (DN) but the special location `[root]` can be specified in the `acls.prop` file if the access control rule applies to the entire directory.

If an entry being accessed or modified on the LDAP server does not equal or reside below the location of the access control rule, the given access control rule is not evaluated further.

Access Control Scope

The following access control scopes are defined:

- **Entry**—An ACL with a scope of Entry is only evaluated if the entry in the LDAP directory shares the same DN as the location of the access control rule. Such rules are useful when a single entry contains more sensitive information than parallel or subentries entries.
- **Subtree**—A scope of Subtree is evaluated if the entry in the LDAP directory equals or ends with the location of this access control. This scope protects means the location entry and all subentries.

If an entry in the directory is covered by conflicting access control rules (for example, where one rule is an Entry rule and the other is a Subtree rule), the Entry rule takes precedence over rules that apply because of the Subtree rule.

Access Rights

Access rights apply to an entire object or to attributes of the object. Access can be granted or denied. Either of the actions `grant` or `deny` may be used when you create or update the access control rule.

Each LDAP access right is discrete. One right does not imply another right. The rights specify the type of LDAP operations that can be performed.

Attribute Permissions

The following permissions apply to actions involving attributes.

Table 9-2 Attribute Permissions

Permission	Description
r Read	Read attributes. If granted, permits attributes and values to be returned in a Read or Search operation.
w Write	Modify or add attributes. If granted, permits attributes and values to be added in a Modify operation.
o Obliterate	Modify and delete attributes. If granted, permits attributes and values to be deleted in a Modify operation.
s Search	Search entries with specified attributes. If granted, permits attributes and values to be included in a Search operation.
c Compare	Compare attribute values. If granted, permits attributes and values to be included in a Compare operation.
m Make	Make attributes on a new LDAP entry below this entry.

The **m** permission is required for all attributes placed on an object when it is created. Just as the **w** and **o** permissions are used in the Modify operation, the **m** permission is used in the Add operation. The **w** and **o** permissions have no bearing on the Add operation and **m** has no bearing on the Modify operation. Since a new object does not yet exist, the **a** and **m** permissions needed to create it must be granted to the parent of the new object. This requirement differs from **w** and **o** permissions which must be granted on the object being modified. The **m** permission is distinct and separate from the **w** and **o** permissions so that there is no conflict between the permissions needed to add new children to an entry and the permissions needed to modify existing children of the same entry. In order to replace values with the Modify operation, a user must have both the **w** and **o** permissions.

Entry Permissions

The following permissions apply to entire LDAP entries.

Table 9-3 Entry Permissions

Permission	Description
a Add	Add an entry below this LDAP entry. If granted, permits creation of an entry in the DIT subject to control on all attributes and values placed on the new entry at the time of creation. In order to add an entry, permission must also be granted to add at least the mandatory attributes.
d Delete	Delete this entry. If granted, permits the entry to be removed from the DIT regardless of controls on attributes within the entry.
e Export	<p>Export entry and all subentries to new location.</p> <p>If granted, permits an entry and its subentries (if any) to be exported; that is, removed from the current location and placed in a new location subject to the granting of suitable permission at the destination.</p> <p>If the last RDN is changed, Rename permission is also required at the current location.</p> <p>In order to export an entry or its subentries, there are no prerequisite permissions to the contained attributes, including the RDN attribute. This is true even when the operation causes new attribute values to be added or removed as the result of the changes to the RDN.</p>

Table 9-3 Entry Permissions

Permission	Description
i Import	<p>Import entry and subentries from specified location.</p> <p>If granted, permits an entry and its subentries (if any) to be imported; that is, removed from one location and placed at the specified location (if suitable permissions for the new location are granted).</p> <p>When you import an entry or its subentries, the contained attributes, including the RDN attributes, have no prerequisite permissions. This is true even when the operation causes new attribute values to be added or removed as the result of the changes to RDN.</p>
n RenameDN	<p>Change the DN of an LDAP entry. Granting the Rename permission is necessary for an entry to be renamed with a new RDN, taking into account consequential changes to the DN of subentries. If the name of the superior entry is unchanged, the grant is sufficient.</p> <p>When you rename an entry, there are no prerequisite permissions for the contained attributes, including the RDN attributes. This is true even when the operation causes new attribute values to be added or removed as the result of the changes of RDN.</p>
b BrowseDN	<p>Browse the DN of an entry. If granted, this permission permits entries to be accessed using directory operations that do not explicitly provide the name of the entry.</p>
t ReturnDN	<p>Allows DN of entry to be disclosed in an operation result. If granted, this permission allows the distinguished name of the entry to be disclosed in the operation result.</p>

Attributes Types

The attribute types to which an access control rule applies should be listed in the ACL where necessary. The following keywords are available:

- `[entry]` indicates the permissions apply to the entire object. This could mean actions such as delete the object, or add a child object.
- `[all]` indicates the permissions apply to all attributes of the entry.

If the keyword `[all]` and another attribute are both specified within an ACL, the more specific permission for the attribute overrides the less specific permission specified by the `[all]` keyword.

Subject Types

Access control rules can be associated with a number of subject types. The subject of an access control rule determines whether the access control rule applies to the currently connected session.

The following subject types are defined:

- `authzID`—Applies to a single user that can be specified as part of the subject definition. The identity of that user in the LDAP directory is typically defined as a DN.
- `Group`—Applies to a group of users specified by one of the following object classes:
 - `groupOfUniqueNames`
 - `groupOfNames`
 - `groupOfUniqueURLs`

The first two types of groups contain lists of users, and the third type allows users to be included in the group automatically based on defined criteria.

- `Subtree`—Applies to the DN specified as part of the subject and all subentries in the LDAP directory tree.
- `IP Address`—Applies to a particular Internet address. This subject type is useful when all access must come through a proxy or other server. Applies only to a particular host, not to a range or subnet.
- `Public`—Applies to anyone connected to the directory, whether they are authenticated or not.
- `This`—Applies to the user whose DN matches that of the entry being accessed.

Grant/Deny Evaluation Rules

The decision whether to grant or deny a client access to the information in an entry is based on many factors related to the access control rules and the entry being protected. Throughout the decision making process, these guiding principles apply:

- More specific rules override less specific ones (for example, individual user entries in an ACL take precedence over a group entry).
- If a conflict still exists in spite of the specificity of the rule, the subject of the rule determines which rule will be applied. Rules based on an `IP Address` subject are given the highest precedence, followed by rules that are applied to a specific `AuthzID` or `This` subject. Next in priority are rules that apply to `Group` subjects. Last priority is given to rules that apply to `Subtree` and `Public` subjects.
- When there are conflicting ACL values, Deny takes precedence over Grant.
- Deny is the default when there is no access control information. Additionally, an entry scope takes precedence over a subtree scope.

Managing the RDBMS Security Store

WebLogic Server provides the option of using an external RDBMS as a datastore that is used by authorization, role mapping, credential mapping, and certificate registry providers. This datastore, called the RDBMS security store, is strongly recommended for the use of SAML 2.0 services in two or more WebLogic Server instances in that domain, such as in a cluster.

Note: In order to use the RDBMS security store, the preferred approach is first to create a domain in which the external RDBMS server is configured. Prior to booting the domain, you create the tables in the datastore that are required by the RDBMS security store. The WebLogic Server installation directory contains a set of SQL scripts that create these tables for each supported database.

The following sections explain how to configure and manage the RDBMS security store:

- [“Security Providers that Use the RDBMS Security Store”](#) on page 10-2
- [“Configuring the RDBMS Security Store”](#) on page 10-3
- [“Upgrading a Domain to Use the RDBMS Security Store”](#) on page 10-11

For the most up-to-date details about the specific database systems that are supported by WebLogic Server to function as the RDBMS security store, see [Supported Configurations](#).

Security Providers that Use the RDBMS Security Store

The following security providers use the RDBMS security store if that store is configured in a domain:

- XACML Authorization provider
- XACML Role Mapping provider
- The following providers for SAML 1.1:
 - SAML Identity Assertion provider V2
 - SAML Credential Mapping provider V2
- The following providers for SAML 2.0:
 - SAML 2.0 Identity Assertion provider
 - SAML 2.0 Credential Mapping provider
- WebLogic Credential Mapping provider
- PKI Credential Mapping provider
- Certificate Registry

When the RDBMS security store is configured in a domain, an instance of any of the preceding security providers that has been created in the security realm automatically uses only the RDBMS security store as a datastore, and not the embedded LDAP server. WebLogic security providers configured in the domain that are not among those in the preceding list continue to use their respective default stores; for example, the WebLogic Authentication provider continues to use the embedded LDAP server.

Oracle recommends that you configure the RDBMS security store at the time of domain creation. The Configuration Wizard has been enhanced to simplify this process. This utility includes an option for testing the RDBMS connection to help ensure that when the domain is booted, the security policies required to access the domain can be retrieved.

In addition to the Configuration Wizard, WebLogic Server also contains the `RDBMSSecurityStore` MBean, which is the interface for configuring the RDBMS security store via the WebLogic Scripting Tool (WLST).

Configuring the RDBMS Security Store

To create and configuring the RDBMS security store in a domain, complete the tasks described in the following sections:

- [“Create a Domain with the RDBMS Security Store”](#) on page 10-3
- [“Create RDBMS Tables in the Security Datastore”](#) on page 10-7
- [“Configure a JMS Topic for the RDBMS Security Store”](#) on page 10-8

Create a Domain with the RDBMS Security Store

To use the RDBMS security store in a domain, Oracle recommends that you configure the RDBMS security store at the time you create that domain. Modifying an existing domain in place to use the RDBMS security store is possible; however, it is not recommended because if the database connection is not configured correctly, the policies necessary for granting access to the domain could become unavailable, resulting in a domain that cannot be used.

WebLogic Server provides two ways to create a domain in which the RDBMS security store may be configured:

- By using the Configuration Wizard, which includes an option to configure the RDBMS security store. This option is available from the Customize Environment and Services Settings page.

If you choose this option, the Configuration Wizard displays subsequent windows in which you can:

- a. Select the specific database system you wish to use as the RDBMS security store
 - b. Configure the database connection settings
 - c. Test the database connection
- By using the WebLogic Scripting Tool (WLST) Offline. Operations for creating and configuring the RDBMS security store are available via the RDBMSSecurityStore MBean.

Regardless of the method you choose to create the domain, be sure to configure the connection properties for the database that serves as the RDBMS security store as explained in the following sections.

Specifying Database Connection Properties

When configuring the RDBMS security store in either the Configuration Wizard or WLST, you need to specify or configure the following:

- RDBMS type

The following RDBMS systems are supported for containing the RDBMS security store:

- Oracle 9i, 10g, and 11g
- MS-SQL 2000 and 2005
- DB2 9.2 and 9.5
- PointBase RDBMS 5.1 included with WebLogic Server

Note: When you use the Configuration Wizard to configure the RDBMS security store, the Configuration Wizard provides a drop-down list for selecting the database you want to use. The databases appearing in this drop-down list are not exclusive to only those supported for the RDBMS security store. Make sure you choose a database that is supported for this purpose. (See [Supported Configurations](#) for the most up-to-date list.)

- JDBC driver and class name for connecting to the RDBMS
- RDBMS name, host, port, and URL
- Username and password of the domain user who can access the RDBMS system
- Optionally, any properties that need to be passed to the RDBMS system

The parameters that you specify in the JDBC driver connection properties attribute must be a comma-separated list. The following examples show the use of WLST to configure the database connection properties for Oracle, MS-SQL, and DB2.

Oracle Example

[Listing 10-1](#) shows an example of configuring Oracle for the RDBMS security store.

Listing 10-1 Configuring Oracle for the RDBMS Security Store

```
create('base_domain', 'SecurityConfiguration')
cd('/SecurityConfiguration/base_domain')
a=get('DefaultRealm')
```

```

cd('Realm/myrealm')
rdbms = create("myRDBMSSecurityStore", "RDBMSSecurityStore")
rdbms.setUsername('ortiz')
rdbms.setPasswordEncrypted('weblogic')
rdbms.setConnectionURL('jdbc:bea:oracle://avitek21:1521')
rdbms.setDriverName('weblogic.jdbc.oracle.OracleDriver')
rdbms.setConnectionProperties('user=ortiz,portNumber=1521,SID=pint101a,serverName=avitek21')

```

MS-SQL Example

[Listing 10-2](#) shows an example of configuring MS-SQL for the RDBMS security store.

Listing 10-2 Configuring MS-SQL for the RDBMS Security Store

```

create('base_domain','SecurityConfiguration')
cd('/SecurityConfiguration/base_domain')
a=get('DefaultRealm')
cd('Realm/myrealm')
rdbms = create("myRDBMSSecurityStore", "RDBMSSecurityStore")
rdbms.setUsername('garnett')
rdbms.setPasswordEncrypted('weblogic')
rdbms.setConnectionURL('jdbc:bea:sqlserver://avitek6:1433')
rdbms.setDriverName('weblogic.jdbc.sqlserver.SQLServerDriver')
rdbms.setConnectionProperties('user=garnett,portNumber=1433,databaseName=wl3,serverName=avitek6')

```

DB2 Example

[Listing 10-3](#) shows an example of configuring DB2 for the RDBMS security store.

Note: If you choose DB2, you have the option of selecting the WebLogic Type 4 JDBC driver for DB2 that is provided in WebLogic Server. However, if you use this JDBC driver, you must also specify the additional property `BatchPerformanceWorkaround` and set it to `true`. If you do not set the `BatchPerformanceWorkaround` to `true` in this configuration, WebLogic Server may fail to boot, generating a `SecurityServiceException` message.

Listing 10-3 Configuring DB2 for the RDBMS Security Store

```
create('base_domain','SecurityConfiguration')
cd('/SecurityConfiguration/base_domain')
a=get('DefaultRealm')
cd('Realm/myrealm')
rdbms = create("myRDBMSSecurityStore", "RDBMSSecurityStore")
rdbms.setUsername('brady')
rdbms.setPasswordEncrypted('weblogic')
rdbms.setConnectionURL('jdbc:bea:db2://avitek3:50000')
rdbms.setDriverName('weblogic.jdbc.db2.DB2Driver')
rdbms.setConnectionProperties('user=brady,portNumber=50000,databaseName=wl
s,serverName=avitek3,batchPerformanceWorkaround=true')
```

For more information about specifying connection properties for the WebLogic Type 4 JDBC driver for DB2, see “[The DB2 Driver](#)” in *Type 4 JDBC Drivers*.

For More Information About Default Connection Properties

Internally, the RDBMS security store uses Oracle Kodo to connect to and interoperate with the database using the WebLogic Type 4 JDBC driver for DB2. The attributes set on the RDBMSSecurityStore MBean are converted into attributes set on the properties of Kodo’s `javax.sql.DataSource` implementation.

For more information about these attributes, see the following topics:

- For more information about the attributes you can set on the RDBMSSecurityStore MBean, see [RDBMSSecurityStoreMBean](#) in the *WebLogic Server MBean Reference*.
- For information about the default database connection properties in the Kodo DataSource, see “Using the Kodo DataSource” in the JDBC chapter of the *Kodo JPA/JDO Reference Guide*, available at the following URL:

http://e-docs.bea.com/kodo/docs41/full/html/ref_guide_dbsetup.html#ref_guide_dbsetup_builtin

Testing the Database Connection

During the process of configuring the RDBMS security store via the Configuration Wizard, you are presented with the option of testing the database connection. Oracle strongly recommends using this option because it can verify that the connection is set up properly. If there were a problem with the database connection, you might not be able subsequently to boot the domain if

the security providers that control access to that domain are unable to obtain the necessary security policies.

For information about configuring the RDBMS security store via the Configuration Wizard, see [“Customizing the Environment”](#) in *Creating WebLogic Domains Using the Configuration Wizard*.

Create RDBMS Tables in the Security Datastore

Prior to booting the domain, the database administrator needs to run the SQL script that creates the RDBMS tables in the datastore used by the RDBMS security store. A set of SQL scripts for creating these tables for, and also removing them from, each supported RDBMS system is available in the following WebLogic Server installation directory:

`WL_HOME/server/lib`

When running the appropriate SQL script for the database serving as the RDBMS security store, be sure to specify the same connection properties, including the credentials of the user who has access, the database URL, etc., as specified for that RDBMS during domain creation.

[Table 10-1](#) identifies the name of each of these SQL scripts.

Table 10-1 SQL Scripts for Creating and Removing RDBMS Datastore Tables

RDBMS System	SQL Script in <code>WL_HOME/server/lib</code>	
	For Creating Datastore Tables	For Removing Datastore Tables
Oracle 9i, 10g, 11g	<code>rdbms_security_store_oracle.sql</code>	<code>rdbms_security_store_oracle_remove.sql</code>
MS-SQL 2000, 2005	<code>rdbms_security_store_sqlserver.sql</code>	<code>rdbms_security_store_sqlserver_remove.sql</code>
DB2 9.2, 9.5	<code>rdbms_security_store_db2.sql</code>	<code>rdbms_security_store_db2_remove.sql</code>
PointBase 5.1	<code>rdbms_security_store_pointbase.sql</code>	<code>rdbms_security_store_pointbase_remove.sql</code>

Configure a JMS Topic for the RDBMS Security Store

If the RDBMS security store is configured in a domain that includes two or more WebLogic Server instances, or a cluster, Oracle strongly recommends that you also perform the following tasks:

1. Enable JMS notifications for that domain.
2. Configure a JMS topic that can be used by the RDBMS security store.

JMS notifications enable the security data that is contained in the RDBMS security store, and that is managed by security providers in the realm, to be synchronized among all server instances in the domain.

Caution: If you do not configure a JMS topic that can be used by the RDBMS security store when configured in a multi-server or clustered domain, care should be taken when making security policy or security configuration updates. If no JMS topic is configured, it may be necessary to reboot the domain to ensure that all server instances function consistently with regards to those security updates.

You can enable JMS notifications by booting the domain in which the RDBMS security store has been configured, and configuring attributes on the RDBMSSecurityStore MBean via either of the following mechanisms:

- WebLogic Scripting Tool
- The Security Realms → *RealmName* → RDBMS Security Store page in the Administration Console

The attributes of the RDBMSSecurityStore MBean that must be set to enable JMS notifications are listed and described in [Table 10-2](#).

Table 10-2 RDBMSecurityStore MBean Attributes for Configuring a JMS Topic

Attribute Name	Description
JMSTopic	The JMS topic to which the Kodo remote commit provider should publish notifications and subscribe for notifications sent from other JVMs. The target JMS topic needs to be pre-deployed.
JMSTopicConnectionFactory	<p>The JNDI name of a <code>javax.jms.TopicConnectionFactory</code> instance to use for finding JMS topics.</p> <p>The topic “Connection Factory Configuration” in <i>Configuring and Managing WebLogic JMS</i> describes the WebLogic JMS connection factory, <code>weblogic.jms.ConnectionFactory</code>, which is a <code>javax.jms.TopicConnectionFactory</code> instance. Refer to this topic for information about configuring a connection factory.</p>
NotificationProperties	<p>A comma-delimited list of key-value properties to pass to the JNDI <code>InitialContext</code> on construction, in the form of <code>xxKey=xxValue, xxKey=xxValue</code>. The following properties must be specified:</p> <ul style="list-style-type: none"> • <code>java.naming.provider.url</code> — Property for specifying configuration information for the service provider to use. The value of the property should contain a URL string. For example: <code>iiops://localhost:7002</code> • <code>java.naming.factory.initial</code> — Property for specifying the initial context factory to use. The value of the property should be the fully-qualified class name of the factory class that will create an initial context. For example: <code>weblogic.jndi.WLInitialContextFactory</code>
JNDIUserName	The identity of any valid user in the security realm who has access to JNDI.

Table 10-2 RDBMSSecurityStore MBean Attributes for Configuring a JMS Topic

Attribute Name	Description
JNDIPassword	The password of the user specified in the JNDIUserName attribute.
JMSExceptionReconnectAttempts	The number of reconnect attempts to be made if the JMS system notifies Kodo of a serious connection error. The default is 0, which causes an error to be logged, but does not result in a reconnect attempt.

For more information, see the following topics:

- [Configure topics](#) in the *Administration Console Online Help*
- “[Configuring Basic JMS System Resources](#)” in *Configuring and Managing WebLogic JMS*
- [Configure the RDBMS security store](#) in the *Administration Console Online Help*
- [RDBMSSecurityStoreMBean](#) in the *WebLogic Server MBean Reference*

Configuring JMS Connection Recovery in the Event of Failure

Normally, the WebLogic Security Service contained in each WebLogic Server instance in a multi-node domain connects at startup to the JMS server. If a security provider that uses the RDBMS security store makes a change to its security data, all WebLogic Server instances are notified via JMS, and the local caches used by the WebLogic Security Service in each server instance are synchronized to that change.

If the JMS connection fails in a WebLogic Server instance that has been successfully started, the WebLogic Security Service associated with that server instance starts the JMS connection recovery process. The recovery process sleeps one second between reconnect attempts. The recovery process is stopped if the JMS connection failure persists after the number of reconnect attempts with which the `JMSExceptionReconnectAttempts` property has been configured is reached. No further reconnect attempts are made: If a change is made to the security data in one WebLogic Server instance, the local caches managed by the WebLogic Security Service in other WebLogic Server instances are not synchronized to that change. However, if the JMS connection is successfully recovered by other means (such as a server reboot), those caches become synchronized.

If the JMS connection is not successfully started at the time a WebLogic Server instance is booted, a timer task that makes reconnect attempts is automatically started. The timer task is

cancelled once the connection is successfully made. Two system properties may be configured for this timer task:

- `com.bea.common.security.jms.initialConnectionRecoverInterval`

Specifies the delay, in milliseconds, before the connection recovery task is executed. The default value is 1000, which causes the connection recovery process to be executed after a delay of one second.

- `com.bea.common.security.jms.initialConnectionRecoverAttempts`

Specifies the maximum number of reconnect attempts that can be made prior to cancelling the timer task. The default value is 3600, which causes the timer task to be cancelled once 3600 reconnect attempts have been made. No further reconnect attempts are made.

You can calculate the maximum connection polling duration by multiplying the values specified by each of the preceding system properties. For example, multiplying the default values of these two properties yields a maximum polling duration of one hour (1000 millisecond delay multiplied by 3600 reconnect attempts).

Upgrading a Domain to Use the RDBMS Security Store

To upgrade a domain to use the RDBMS security store, Oracle recommends creating a new domain in which the RDBMS security store is configured. After you create the new domain, you should export the security data from the security realm of the old domain, and import it into a security realm of the new domain. When you import security data into a security realm in a domain that uses the RDBMS security store, the data for the security providers that use the RDBMS security store is automatically loaded into that datastore. Data for security providers that do not use the RDBMS security store is automatically imported into the stores that those providers normally use by default.

It is possible to selectively migrate security providers individually from one security realm to another. However, when migrating security data to a domain that uses the RDBMS security store, Oracle recommends migrating the security realm's data in a single operation.

For information about migrating security realms, see the following topics:

- [Chapter 8, “Migrating Security Data”](#)
- [Export data from security realms](#) and [Import data into security realms](#) in the *Administration Console Online Help*

Managing the RDBMS Security Store

Configuring Identity and Trust

The following sections describe how to configure identity and trust for WebLogic Server:

- “Private Keys, Digital Certificates, and Trusted Certificate Authorities” on page 11-1
- “Configuring Identity and Trust: Main Steps” on page 11-2
- “Supported Formats for Identity and Trust” on page 11-3
- “Obtaining Private Keys, Digital Certificates, and Trusted Certificate Authorities” on page 11-4
- “Storing Private Keys, Digital Certificates, and Trusted Certificate Authorities” on page 11-11
- “How WebLogic Server Locates Trust” on page 11-13
- “Configuring Keystores for Production” on page 11-13

Before performing the steps in this chapter, review the [Identity and Trust](#) section in *Understanding WebLogic Security*.

Private Keys, Digital Certificates, and Trusted Certificate Authorities

Private keys, digital certificates, and trusted certificate authorities establish and verify server identity and trust.

SSL uses public key encryption technology for authentication. With public key encryption, a public key and a *private key* are generated for a server. Data encrypted with the public key can only be decrypted using the corresponding private key and data encrypted with the private key can only be decrypted using the corresponding public key. The private key is carefully protected so that only the owner can decrypt messages that were encrypted using the public key.

The public key is embedded in a *digital certificate* with additional information describing the owner of the public key, such as name, street address, and e-mail address. A private key and digital certificate provide *identity* for the server.

The data embedded in a digital certificate is verified by a certificate authority and digitally signed with the certificate authority's digital certificate. Well-known certificate authorities include Verisign and Entrust.net. The trusted certificate authority (CA) certificate establishes *trust* for a certificate.

An application participating in an SSL connection is authenticated when the other party evaluates and accepts the application's digital certificate. Web browsers, servers, and other SSL-enabled applications generally accept as genuine any digital certificate that is signed by a trusted certificate authority and is otherwise valid. For example, a digital certificate can be invalidated because it has expired or the digital certificate of the certificate authority used to sign it expired. A server certificate can be invalidated if the host name in the digital certificate of the server does not match the URL specified by the client.

Configuring Identity and Trust: Main Steps

To create identity and trust for a server:

1. Obtain digital certificates, private keys, and trusted CA certificates from the CertGen utility, Sun Microsystem's `keytool` utility, or a reputable vendor such as Entrust or Verisign. You can also use the digital certificates, private keys, and trusted CA certificates provided by the WebLogic Server kit. The demonstration digital certificates, private keys, and trusted CA certificates should be used in a development environment only.
2. Store the private keys, digital certificates, and trusted CA certificates. Private keys and trusted CA certificates are stored in a keystore.

Note: The preferred keystore format is JKS (Java KeyStore). WebLogic Server supports private keys and trusted CA certificates stored in files or in the WebLogic Keystore provider for the purpose of backward compatibility only.

3. Configure the identity and trust keystores for WebLogic Server in the WebLogic Server Administration Console. See [Configure Keystores](#) in the *Administration Console Online Help*.

The remaining sections describe these steps.

Supported Formats for Identity and Trust

The PEM (Privacy Enhanced Mail) format is the preferred format for private keys, digital certificates, and trusted certificate authorities (CAs). The preferred keystore format is the JKS (Java KeyStore) format.

A `.pem` format file begins with this line:

```
-----BEGIN CERTIFICATE-----
```

and ends with this line:

```
-----END CERTIFICATE-----
```

A `.pem` format file supports multiple digital certificates (for example, a certificate chain can be included). The order of certificates within the file is important. The server's digital certificate should be the first digital certificate in the file, followed by the issuer certificate, and so on. Each certificate in the chain is followed by its issuer certificate. If the last certificate in the chain is the self-signed (self-issued) root certificate of the chain, the chain is considered complete. Note that the chain does not have to be complete.

When using the deprecated file-based private keys, digital certificates, and trusted CAs, WebLogic Server can use digital certificates in either PEM or distinguished encoding rules (DER) format.

A `.der` format file contains binary data for a single certificate. Thus, a `.der` file can be used only for a single certificate, while a `.pem` file can be used for multiple certificates.

Microsoft is often used as a certificate authority. Microsoft issues trusted CA certificates in p7b format, which must be converted to PEM before they can be used with WebLogic Server. For more information, see [“Converting a Microsoft p7b Format to PEM Format”](#) on page 11-8.

Private key files (meaning private keys not stored in a keystore) must be in PKCS#5/PKCS#8 PEM format.

You can still use private keys and digital certificates used with other versions of WebLogic Server with this version of WebLogic Server. Convert the private key and digital certificate from distinguished encoding rules (DER) format to privacy-enhanced mail (PEM) format. For more

information, see the description of the [der2pem](#) utility in *Using the WebLogic Server Java Utilities* in *WebLogic Server Command Reference*.

After converting the files, ensure the digital certificate file has the

-----BEGIN CERTIFICATE----- header and the -----END CERTIFICATE----- footer.

Otherwise, the digital certificate will not work.

Note: OpenSSL can add a header to the PEM certificate it generates. In order to use such certificates with WebLogic Server, everything in front of "-----BEGIN CERTIFICATE-----" should be removed from the certificate, which you can do with a text editor.

Obtaining Private Keys, Digital Certificates, and Trusted Certificate Authorities

Servers need a private key, a digital certificate containing the matching public key, and a certificate for at least one trusted certificate authority. WebLogic Server supports private keys, digital certificates, and trusted CA certificates from the following sources:

- The demonstration digital certificates, private keys, and trusted CA certificates in the `WL_HOME\server\lib` directory and the `JAVA_HOME\jre\lib\security` directory.

The demonstration digital certificates, private keys, and trusted CA certificates should be used in a development environment only.

- Sun Microsystem's `keytool` utility can also be used to generate a private key, a self-signed digital certificate for WebLogic Server, and a Certificate Signing Request (CSR).
 - Submit the CSR to a certificate authority to obtain a digital certificate for WebLogic Server.
 - Use the `keytool` utility to update the self-signed digital certificate with a new digital certificate.
 - Use the `keytool` utility to obtain trust and identity when using WebLogic Server in a production environment.

For more information about Sun's `keytool` utility, see the `keytool-Key and Certificate Management Tool` description at

<http://java.sun.com/j2se/1.5.0/docs/tooldocs/windows/keytool.html>.

Note: When you use the `keytool` utility, the default key pair generation algorithm is Digital Signature Algorithm (DSA). WebLogic Server does not support DSA. Specify another key pair generation and signature algorithm when using WebLogic Server.

- The CertGen utility generates digital certificates and private keys that should be used only for demonstration or testing purposes in a development environment, and not in a production environment. Use the CertGen utility if you want to set an expiration date in the digital certificate or specify a correct host name in the digital certificate so that you can use host name verification. (The demonstration digital certificate provided by WebLogic Server uses the machine's default host name as the host name.) For more information about using the CertGen utility to obtain private keys and digital certificates, see “Using the CertGen Utility” on page 11-6.

Note: The Certificate Request Generator servlet is deprecated. Use the `keytool` utility from Sun Microsystems in place of the Certificate Request Generator servlet. For more information about `keytool`, see “Common Keytool Commands” on page 11-5.

Common Keytool Commands

Table 11-1 lists `keytool` commands you use when creating and using JKS keystores with WebLogic Server.

Note: The `keytool` utility is a product of Sun Microsystems. Therefore, Oracle does not provide complete documentation on the utility. For more information, see the `keytool`-Key and Certificate Management Tool description at <http://java.sun.com/j2se/1.5.0/docs/tooldocs/windows/keytool.html>.

Table 11-1 Commonly Used keytool Commands

Command	Description
<code>keytool -genkey -keystore keystorename -storepass keystorepassword</code>	Generates a new private key entry and self-signed digital certificate in a keystore. If the keystore does not exist, it is created.
<code>keytool -import -alias aliasforprivatekey -file privatekeyfilename.pem -keypass privatekeypassword -keystore keystorename -storepass keystorepassword</code>	Updates the self-signed digital certificate with one signed by a trusted CA.

Table 11-1 Commonly Used keytool Commands (Continued)

Command	Description
<pre>keytool -import -alias rootCA -trustcacerts -file RootCA.pem -keystore trust.jks -storepass keystorepassword keytool -import -alias intermediate -trustcacerts -file Intermediate.pem -keystore keystorename -storepass keystorepassword</pre>	<p>Creates a custom keystore to be used for holding an intermediate CA certificate.</p> <ul style="list-style-type: none"> The first keytool command creates the keystore, <code>trust.jks</code>, which holds the root CA certificate. The second keytool command imports the intermediate CA certificate into <code>trust.jks</code>. <p>This enables WebLogic Server's SSL implementation to transmit the intermediate certificate with the server's public certificate to the client during the SSL handshake.</p>
<pre>keytool -import -alias aliasfortrustedca -trustcacerts -file trustedcafilename.pem -keystore keystorename -storepass keystorepassword</pre>	<p>Loads a trusted CA certificate into a keystore. If the keystore does not exist, it is created.</p>
<pre>keytool -certreq -alias alias -sigalg sigalg -file certreq_file -keypass privatekeypassword -storetype keystoretype -keystore keystorename -storepass keystorepassword</pre>	<p>Generates a Certificate Signing Request (CSR), using the PKCS#10 format, and a self-signed certificate with a private key.</p> <p>Stores the CSR in the specified <code>certreq_file</code>, and the certificate/private key pair as a key entry in the specified keystore under the specified alias.</p>
<pre>keytool -list -keystore keystorename</pre>	<p>Displays what is in the keystore.</p>
<pre>keytool -delete -keystore keystorename -storepass keystorepassword -alias privatekeyalias</pre>	<p>Deletes the entry identified by the specified alias from the keystore.</p>
<pre>keytool -help</pre>	<p>Provides online help for keytool.</p>

Using the CertGen Utility

Note: The CertGen utility generates digital certificates and private keys that should only be used for demonstration or testing purposes, not in a production environment.

The CertGen utility provides command line options to specify a CA certificate and key to be used for issuing generated certificates. The digital certificates generated by the CertGen utility have the host name of the machine on which they were generated as the value for its common name field (`cn`) by default only. Command line options let you specify values for the `cn` and other Subject domain name (DN) fields, such as `orgunit`, `organization`, `locality`, `state`, and `countrycode`.

The CertGen utility generates public certificate and private key files in PEM and DER formats. On Windows, double-click `.der` files to view the details of the generated digital certificate. The `.pem` files can be used when you boot WebLogic Server or use the digital certificates with a client.

By default, the CertGen utility uses the following demonstration digital certificate and private-key files: `CertGenCA.der` and `CertGenCAKey.der`. CertGen looks for these files in the current directory, or in the `WL_HOME/server/lib` directory, as specified in the `weblogic.home` system property or the `CLASSPATH`. If you want to use these files, you need not specify CA files on the command line. Alternatively, you can specify CA files on the command line.

For information about the CertGen utility's syntax and arguments, see [CertGen](#) in the *WebLogic Server Command Reference*.

For an example that generates a certificate and private key using the CertGen utility, and then creates a keystore and stores a private key using the `ImportPrivateKey` utility, see [ImportPrivateKey](#) in the *WebLogic Server Command Reference*.

Note: If you do not explicitly specify a hostname with the `-cn` option, CertGen uses the `JDK InetAddress.getHostname()` method to get the hostname that it puts in the Subject common name. The `getHostName()` method works differently on different platforms. It returns a fully qualified domain name (FQDN) on some platforms (for example, Solaris) and a short host name on other platforms (for example, Windows NT). On Solaris, the result of `InetAddress.getHostname()` depends on how the hosts entry is configured in the `/etc/nsswitch.conf` file.

If WebLogic Server is acting as a client (and by default host name verification is enabled), you need to ensure that the host name specified in the URL matches the Subject common name in the server certificate. Otherwise, connections will fail because the host names do not match.

Using Your Own Certificate Authority

Many companies act as their own certificate authority. To use those trusted CA certificates with WebLogic Server:

1. Ensure the trusted CA certificates are in PEM format.
 - If the trusted CA certificate is in DER format, use the `der2pem` utility to convert them.
 - If the trusted CA certificate was issued by Microsoft, see “[Converting a Microsoft p7b Format to PEM Format](#)” on page 11-8.
 - If the trusted CA certificate has a custom file type, use the steps in “[Converting a Microsoft p7b Format to PEM Format](#)” on page 11-8 to convert the trusted CA certificate to PEM format.
2. Create a trust keystore. For more information, see “[How WebLogic Server Locates Trust](#)” on page 11-13.
3. Store the trusted CA certificate in the trust keystore. For more information, see “[How WebLogic Server Locates Trust](#)” on page 11-13.
4. Configure WebLogic Server to use the trust keystore. For more information, see “[Configuring Keystores for Production](#)” on page 11-13.

Converting a Microsoft p7b Format to PEM Format

Digital certificates issued by Microsoft are in a format (p7b) that cannot be used by WebLogic Server. The following example converts a digital certificate in p7b (PKCS#7) format to PEM format on Windows XP:

1. In Windows Explorer, select the file (`filename.p7b`) you want to convert. Double-click on the file to display a Certificates window.
2. In the left pane of the Certificates window, expand the file.
3. Expand the Certificates folder to display a list of certificates.
4. Select a certificate to convert to PEM format. Right-click on the certificate, then choose All Tasks → Export to display the Certificate Export Wizard.
5. In the wizard, click Next
6. Select the Base-64 encoded X.509 (.CER) option. Then click Next. (Base-64 encoded is the PEM format.)
7. In the File name: field, enter a name for the converted digital certificate; then click Next.

Note: The wizard appends a .cer extension to the output file. The .cer extension is a generic extension which is appended to both base-64 encoded certificates and DER certificates. You can change the extension to .pem after you exit the wizard.

8. Verify that the settings are correct. If the settings are correct, click Finish; if they are not correct, click Back and make any necessary modifications.

Note: For p7b certificate files that contain certificate chains, you need to concatenate the issuer PEM digital certificates to the certificate file. The resulting certificate file can be used by WebLogic Server.

Obtaining a Digital Certificate for a Web Browser

Low-security browser certificates are easy to acquire and can be done from within the Web browser, usually by selecting the Security menu item in Options or Preferences. Go to the Personal Certificates item and ask to obtain a new digital certificate. You will be asked for some information about yourself.

The digital certificate you receive contains public information, including your name and public key, and additional information you would like authenticated by a third party, such as your E-mail address. Later you will present the digital certificate when authentication is requested.

As part of the process of acquiring a digital certificate, the Web browser generates a public-private key pair. The private key should remain secret. It is stored on the local file system and should never leave the Web browser's machine, to ensure that the process of acquiring a digital certificate is itself safe. With some browsers, the private key can be encrypted using a password, which is not stored. When you encrypt your private key, you will be asked by the Web browser for your password at least once per session.

Note: Digital certificates obtained from Web browsers do not work with other types of Web browsers or on different versions of the same Web browser.

Using Certificate Chains (Deprecated)

Note: The use of file-based certificate chains is deprecated. Now the whole certificate chain is imported into a keystore. The steps in this section are provided for the purpose of backward compatibility only.

To use certificate chains with WebLogic Server:

1. Ensure that all the digital certificates are in PEM format. If they are in DER format, you can convert them using the [der2pem](#) utility. If you are using a digital certificate issued by Microsoft, see [“Converting a Microsoft p7b Format to PEM Format” on page 11-8](#). You can use the steps in the section to convert other types of digital certificates. Save the digital certificate in Base 64 format.

2. Open a text editor and include all the digital certificate files into a single file. The order is important. The server digital certificate should be the first digital certificate in the file. The issuer of that digital certificate should be the next in the file and so on until you get to the self-signed root certificate authority certificate. This digital certificate should be the last certificate in the file.

You cannot have blank lines between digital certificates.

3. Specify the file in the Server Certificate File Name field on the **Configuration** → **SSL** page in the WebLogic Server Administration Console.

Listing 11-1 shows a sample certificate chain.

Listing 11-1 Sample File with Certificate Chain

```

-----BEGIN CERTIFICATE-----
MIICyzCCAjSgAwIBAgIBLDANBgkqhkiG9w0BAQQFADCBtjELMAkGA1UEBhMCVVMxeZARBgNVBA
gTCKNhbG1mb3JuaWEeXFjAUBgNVBAcTDVNHbiBGcmFuY2IzY28xFTATBgNVBAoTDEJFQSBSXZWJM
b2dpYzERMA8GA1UECXMUIU2VjdXJpdHkxLzAtBgNVBAMTJkRlbW8gQ2VydG1maWNhdGUGQXV0aG
9yaXR5IENvbnN0cmFpbmRzMR8wHQYJKoZIhvcNAQkBFhBzZWN1cm10eUBiZWUyY29tMB4XDTAY
MTEwMTIwMDIxM1oXDTA2MTAxNTIwMDIxM1owgZ8xCzAJBgNVBAYTALVTMRMwEQYDVQQLIEwpcDYW
xpZm9ybmlhMRYwFAYDVQQHEw1TYW4gRnJhbmNpc2NvMRUwEwYDVQQKEwxCRUeGv2ViTG9naWMx
ETAPBgNVBAsTCFNlY3VyaXR5MRkwFwYDVQQDEXB3ZWJsb2dpYy5iZWUyY29tMR4wHAYJKoZIhvc
NAQkBFg9zdXBw3J0QGU1YS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMJX8nKU
gsFej8pEu/1IVcHUKwY0c2JbBzOryu3sce4QjX+rGxiCjoPm2MY=yts2BvonuJ6CztdZf8B/LB
EWCz+qRrtDfn9mKSZGWvrAkmMPz2RhXEOTthpoRo5kZz2FQ9XF/PxIJXTYCM7yooRBwXoKYjqUR
wiZntUiU9kyi6Z3prAgMBAAEwDQYJKoZIhvcNAQEEBQADgYEAh2eqQxGEMUnNTwEUD
0tBq+7YuAkjecEocGXvi2G4YSOWVLgnVzJoJuds3c35KE6sxBe1luJQuQkE9SzaLG/61DIJ5ct
PsHFmZzZxY7scLl6hWj5ON8oN2YTh5Jo/ryqjvnZvqiniWe/gqr2GLIkaJc0mz4un1LiYORPig
3fBMH0=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIC+jCCAMogAwIBAgIBADANBgkqhkiG9w0BAQQFADCBtjELMAkGA1UEBhMCVVMxeZARBgNVBA
gTCKNhbG1mb3JuaWEeXFjAUBgNVBAcTDVNHbiBGcmFuY2IzY28xFTATBgNVBAoTDEJFQSBSXZWJM
b2dpYzERMA8GA1UECXMUIU2VjdXJpdHkxLzAtBgNVBAMTJkRlbW8gQ2VydG1maWNhdGUGQXV0aG
9yaXR5IENvbnN0cmFpbmRzMR8wHQYJKoZIhvcNAQkBFhBzZWN1cm10eUBiZWUyY29tMB4XDTAY
MTEwMTIwMDIxMVoXDTA2MTAxNjIwMDIxMVowgZ8wDQYJKoZIhvcNAQEBBQADgYEAh2eqQxGEMUnNTwEUD
xpZm9ybmlhMRYwFAYDVQQHEw1TYW4gRnJhbmNpc2NvMRUwEwYDVQQKEwxCRUeGv2ViTG9naWMx
ETAPBgNVBAsTCFNlY3VyaXR5MS8wLQYDVQQDEYzEZW1vIENlcnRpb2l1YXN1eF1dGhvcml0eS
BDb25zdHJhaW50czEfmB0GCSqGSIb3DQEJARYQc2VjdXJpdHlAYmVhLmNvbTcBznANBgkqhkiG
9w0BAQEFAAOBjQAwGyKCGYEA3ynD815JfLob4g6d94dNtIOEep6QN19bblmswnrjiYz1BVjjrj
NVal9fRs+8jvm85kIwlerKzIMJginsj50W1XzNX6orszggSsW15pqV0aYE9Re9K
CNNnORlsLjmrhuVxg9rJfEtjHmjrSYr2IDFhcdwPgIt0meWEVnKNObSFYcCAwEAAAMWMBQwEgY
DVR0TAQH/BagwBgEB/wIBATANBgkqhkiG9w0BAQQFAAOBgQBS+0oqWxGyqbZ0028zf9tQT2Rko

```



```
jfuwywrDoGW96Un5IqpFnBHlIu5atliJo3OUpiH18KkwLN8DVP/3t3K3O3kXdIuLbqAL0i5xyB1  
Ahr7gE5eVhIyeMg7ETBPLyGO2BF13Y24LlsO+MX9jW7fxMraPN608QeJXkZw0E0cGwrw2AQ==  
-----END CERTIFICATE-----
```

Storing Private Keys, Digital Certificates, and Trusted Certificate Authorities

Once you have obtained private keys, digital certificates, and trusted CA certificates, you need to store them so that WebLogic Server can use them to find and verify identity. Private keys, their associated digital certificates, and trusted CA certificates are stored in keystores. The keystores can be configured through the WebLogic Server Administration Console or specified on the command line. Use the **Configuration** → **Keystore** page in the WebLogic Server Administration Console to configure identity and trust keystores for WebLogic Server. See [Configuring Keystores](#) in the *Administration Console Online Help*.

For the purpose of backward compatibility, private keys and trusted CA certificates can be stored in a file or in a JKS keystore accessed via the WebLogic Keystore provider. In addition, trusted CA certificates can be stored in a JKS keystore. Use the **Configuration** → **SSL** page of the WebLogic Server Administration Console to specify identity and trust options when using a file or a JKS keystore accessed via the WebLogic Keystore provider.

Guidelines for Using Keystores

When you configure SSL, you have to decide how identity and trust will be stored. Although one keystore can be used for both identity and trust, Oracle recommends using separate keystores for both identity and trust because the identity keystore (private key/digital certificate pairs) and the trust keystore (trusted CA certificates) may have different security requirements. For example:

- For trust, you only have to put the certificates (non-sensitive data) in the keystore while for identity, you have to put the certificate and private key (sensitive data) in the keystore.
- The identity keystore may be prohibited by company policy from ever being put in the network while the trust keystore can be distributed over the network.
- The identity keystore may be protected by the operating system for both reading and writing by non-authorized users while the trust keystore only needs to be write protected.
- The identity keystore password is generally known to fewer people than the password for the trust keystore.

In general, systems within a domain have the same trust rules (use the same set of trusted CAs), while they tend to have per-server identity. Identity requires a private key, and private keys should not be copied from one system to another. Therefore, you should maintain separate identity keystores for each system, each keystore containing only the server identity needed for that system. However, trust keystores can be copied from system to system; thus making it easier to standardize trust rules.

Identity is more likely to be stored in hardware keystores such as nCipher. Trust can be stored in a file-based JDK keystore without having security issues because a trust store contains only certificates, not private keys.

Creating a Keystore and Loading Private Keys and Trusted Certificate Authorities into the Keystore

A keystore is for the secure storage and management of private keys/digital certificate pairs and trusted CA certificates. Use the following mechanisms to create a keystore and load private keys and trusted CA certificates into the keystore:

- The WebLogic `ImportPrivateKey` utility. The `ImportPrivateKey` utility allows you to take private key and digital certificate files and load them into a keystore. For more information, see [ImportPrivateKey](#) in the *WebLogic Server Command Reference*.
- Sun Microsystem's `keytool` utility. Use the `keytool` utility to generate a private key/digital certificate pair and then import the signed private key into the keystore. For more information, see [“How WebLogic Server Locates Trust” on page 11-13](#). While you can use the `keytool` utility to generate new private keys and digital certificates and add them to a keystore, the utility does not allow you to take an existing private key from a file and import it into the keystore. Instead, use the WebLogic `ImportPrivateKey` utility.

Note: The `keytool` utility does allow you to import trusted CA certificates from a file into a keystore.

- Custom utilities. WebLogic Server can use keystores created with custom tools or utilities. How to create and use these utilities is outside the scope of this document.

All private key entries in a keystore are accessed by WebLogic Server via unique aliases. You specify the alias when loading the private key into the keystore. Aliases are case-insensitive; the aliases `HUGO` and `hugo` would refer to the same keystore entry. Aliases for private keys are specified in the Private Key Alias field on the **Configuration** → **SSL** page in the WebLogic Server Administration Console. Although WebLogic Server does not use the alias to access trusted CA certificates, the keystore does require an alias when loading a trusted CA certificate into the keystore.

All certificate authorities in a keystore identified as trusted by WebLogic Server are trusted.

Configuring Demo Certificates for Clients

To use SSL in development mode between a client such as Eclipse and WebLogic Server, configure the demo certificates in the JVM for both the client and the server:

1. Copy `BEA_HOME/wlserver_10.3/server/lib/cacerts` to the `jre/lib/security` directory of the client's JVM. For example, if you are using Eclipse with its default JDK, copy `cacerts` to `BEA_HOME/jdk160_03/jre/lib/security`.
2. Copy `BEA_HOME/wlserver_10.3/server/lib/cacerts` to the `jre/lib/security` directory of the WebLogic Server's JVM. For a domain using JRockit, copy `cacerts` to `BEA_HOME/jrockit90_160_02/jre/lib/security`.
3. Restart both WebLogic Server and the client.

As an alternative, you can import the certificates, rather than copying the `cacerts` files.

How WebLogic Server Locates Trust

WebLogic Server uses the following algorithm when it loads its trusted CA certificates:

1. If the keystore is specified by the `-Dweblogic.security.SSL.trustedCAkeystore` command-line argument, load the trusted CA certificates from that keystore.
2. Else if the keystore is specified in the configuration file (`config.xml`), load trusted CA certificates from the specified keystore. If the server is configured with DemoTrust, trusted CA certificates will be loaded from the `WL_HOME\server\lib\DemoTrust.jks` and the JDK `cacerts` keystores.
3. Else if the trusted CA file is specified in the configuration file (`config.xml`), load trusted CA certificates from that file (this is only for compatibility with 6.x SSL configurations).
4. Else load trusted CA certificates from `WL_HOME\server\lib\cacerts` keystore.

Configuring Keystores for Production

By default, WebLogic Server is configured with two keystores:

- `DemoIdentity.jks`—Contains a demonstration private key for WebLogic Server. This keystore contains the identity for WebLogic Server.

- `DemoTrust.jks`—Contains the trusted certificate authorities from the `WL_HOME\server\lib\DemoTrust.jks` and the JDK `cacerts` keystores. This keystore establishes trust for WebLogic Server.

These keystores are located in the `WL_HOME\server\lib` directory. For testing and development purposes, the keystore configuration is complete. However, do not use the demonstration keystores in a production environment. Because the digital certificates and trusted CA certificates in the demonstration keystores are signed by a WebLogic Server demonstration certificate authority, a WebLogic Server installation using the demonstration keystores will trust **any** WebLogic Server installation that also uses the demonstration keystores. You want to create a secure environment where only your installations trust each other.

To configure keystores for use in a production environment:

1. Obtain private keys and digital certificates from a reputable certificate authority such as Verisign, Inc. or Entrust.net. See [“Obtaining Private Keys, Digital Certificates, and Trusted Certificate Authorities”](#) on page 11-4.
2. Create identity and trust keystores. See [“Creating a Keystore and Loading Private Keys and Trusted Certificate Authorities into the Keystore”](#) on page 11-12.
3. Load the private keys and trusted CAs into the identity and trust keystores. See [“Creating a Keystore and Loading Private Keys and Trusted Certificate Authorities into the Keystore”](#) on page 11-12.
4. Use the WebLogic Server Administration Console to configure the identity and trust keystores. See [Configure Keystores](#) in the *Administration Console Online Help*.

You can also use the WebLogic Scripting Tool or Java Management Extensions (JMX) APIs to create a new security configuration. For more information see the [WebLogic Scripting Tool](#) and [Developing Custom Management Utilities with JMX](#) manuals.

Configuring SSL

Configuring SSL is an optional step; however, Oracle recommends SSL for production environments. The following sections describe how to configure SSL for WebLogic Server.

Notes: The following sections apply to WebLogic Server deployments that use the security features in this release of WebLogic Server as well as deployments that use Compatibility Security.

All machines must be kept up to date with the current set of recommended patches from the operating system vendors.

- [“SSL: An Introduction” on page 12-2](#)
- [“One-Way and Two-Way SSL” on page 12-2](#)
- [“Setting Up SSL: Main Steps” on page 12-2](#)
- [“Using Host Name Verification” on page 12-3](#)
- [“Enabling SSL Debugging” on page 12-4](#)
- [“SSL Session Behavior” on page 12-5](#)
- [“SSL Certificate Validation” on page 12-7](#)
- [“Using the nCipher JCE Provider with WebLogic Server” on page 12-12](#)
- [“Specifying the Version of the SSL Protocol” on page 12-14](#)

SSL: An Introduction

Secure Sockets Layer (SSL) provides secure connections by allowing two applications connecting over a network to authenticate each other's identity and by encrypting the data exchanged between the applications. Authentication allows a server and optionally a client to verify the identity of the application on the other end of a network connection. Encryption makes data transmitted over the network intelligible only to the intended recipient.

SSL in WebLogic Server is an implementation of the SSL 3.0 and Transport Layer Security (TLS) 1.0 specifications.

WebLogic Server supports SSL on a dedicated listen port which defaults to 7002. To establish an SSL connection, a Web browser connects to WebLogic Server by supplying the SSL listen port and the HTTPs protocol in the connection URL, for example, `https://myserver:7002`.

Using SSL is computationally intensive and adds overhead to a connection. Avoid using SSL in development environments when it is not necessary. However, always use SSL in a production environment.

One-Way and Two-Way SSL

SSL can be configured one-way or two-way:

- With one-way SSL, the server is must present a certificate to the client, but the client is not required to present a certificate to the server. The client must authenticate the server, but the server accepts a connection from any client. One-way SSL is common on the Internet where customers want to create secure connections before they share personal data. Often, clients will also use SSL to log on in order that the server can authenticate them.
- With two-way SSL (SSL with client authentication), the server presents a certificate to the client and the client presents a certificate to the server. WebLogic Server can be configured to require clients to submit valid and trusted certificates before completing the SSL connection.

Setting Up SSL: Main Steps

To set up SSL:

1. Obtain an identity (private key and digital certificates) and trust (certificates of trusted certificate authorities) for WebLogic Server. Use the digital certificates, private keys, and trusted CA certificates provided by the WebLogic Server kit, the CertGen utility, Sun

Microsystem's `keytool` utility, or a reputable vendor such as Entrust or Verisign to perform this step.

2. Store the identity and trust. Private keys and trusted CA certificates which specify identity and trust are stored in a keystore.

Note: This release of WebLogic Server supports private keys and trusted CA certificates stored in files, or in the WebLogic Keystore provider for the purpose of backward compatibility only.

3. Configure the identity and trust keystores for WebLogic Server in the WebLogic Server Administration Console. See [Configure Keystores](#) in the *Administration Console Online Help*.
4. Set SSL configuration options for the private key alias and password in the WebLogic Server Administration Console. Optionally, set configuration options that require the presentation of client certificates (for two-way SSL). See [Configure SSL](#) and [Configure two-way SSL](#) in the *Administration Console Online Help*.

Note: To enable a WebLogic Server instance to use a FIPS-compliant (FIPS 140-2) crypto module in the server's SSL implementation, make sure that the server start script (for example, `startWebLogic.cmd/sh`) contains the following:

- `jsafeFIPS.jar` is added to the `PRE_CLASSPATH` variable.
- The command line argument `-Dweblogic.security.SSL.nojce=true` is specified.

FIPS 140-2 is a standard that describes U.S. Federal government requirements for sensitive, but unclassified use.

For information on configuring identity and trust for WebLogic Server, see [“Obtaining Private Keys, Digital Certificates, and Trusted Certificate Authorities”](#) on page 11-4 and [“Storing Private Keys, Digital Certificates, and Trusted Certificate Authorities”](#) on page 11-11.

Using Host Name Verification

A host name verifier ensures the host name in the URL to which the client connects matches the host name in the digital certificate that the server sends back as part of the SSL connection. A host name verifier is useful when an SSL client (or a WebLogic Server acting as an SSL client) connects to an application server on a remote host. It helps to prevent man-in-the-middle attacks.

By default, WebLogic Server has host name verification enabled. As a function of the SSL handshake, WebLogic Server compares the common name in the SubjectDN in the SSL server's

digital certificate with the host name of the SSL server used to initiate the SSL connection. If these names do not match, the SSL connection is dropped. The SSL client is the actual party that drops the SSL connection if the names do not match.

If anything other than the default behavior is desired, either turn off host name verification or configure a custom host name verifier. Turning off host name verification leaves WebLogic Server vulnerable to man-in-the-middle attacks. Oracle recommends leaving host name verification on in production environments.

In this release of WebLogic Server, the host name verification feature is updated so that if the host name in the certificate matches the local machine's host name, host name verification passes if the URL specifies `localhost`, `127.0.0.1`, or the default IP address of the local machine.

For more information, see the following topics in the *Administration Console Online Help*:

- [Verify Host Name Verification is enabled](#)
- [Disable Host Name Verification](#)
- [Configure a Custom Host Name Verifier](#)
- [Configuring SSL](#)

Enabling SSL Debugging

SSL debugging provides more detailed information about the SSL events that occurred during an SSL handshake. The SSL debug trace displays information about:

- Trusted certificate authorities
- SSL server configuration information
- Server identity (private key and digital certificate)
- The encryption strength that is allowed
- Enabled ciphers
- SSL records that were passed during the SSL handshake
- SSL failures detected by WebLogic Server (for example, trust and validity checks and the default host name verifier)
- I/O related information

Use the following command-line properties to enable SSL debugging:


```
-Dssl.debug=true -Dweblogic.StdoutDebugEnabled=true
```

You can include SSL debugging properties in the start script of the SSL server, the SSL client, and the Node Manager. For a Managed Server started by the Node Manager, specify this command-line argument on the Remote Start page for the Managed Server.

SSL debugging dumps a stack trace whenever an ALERT is created in the SSL process. The types and severity of the ALERTS are defined by the Transport Layer Security (TLS) specification.

The stack trace dumps information into the log file where the ALERT originated. Therefore, when tracking an SSL problem, you may need to enable debugging on both sides of the SSL connection (on both the SSL client or the SSL server). The log file contains detailed information about where the failure occurred. To determine where the ALERT occurred, confirm whether there is a trace message after the ALERT. An ALERT received after the trace message indicates the failure occurred on the peer. To determine the problem, you need to enable SSL debugging on the peer in the SSL connection.

When tracking an SSL problem, review the information in the log file to ensure:

- The correct `config.xml` file was loaded
- The setting for domestic, or export, is correct
- The trusted certificate authority was valid and correct for this server.
- The host name check was successful
- The certificate validation was successful

Note: Sev 1 type 0 is a normal close ALERT, not a problem.

SSL Session Behavior

WebLogic Server allows SSL sessions to be cached. Those sessions live for the life of the server.

Clients that use SSL sockets directly can control the SSL session cache behavior. The SSL session cache is specific to each SSL context. All SSL sockets created by SSL socket factory instances returned by a particular SSL context can share the SSL sessions.

Clients default to resuming sessions at the same IP address and port. Multiple SSL sockets that use the same host and port share SSL sessions by default, assuming the SSL sockets are using the same underlying SSL context.

Clients that are not configured to use SSL sessions must call `setEnabledSessionCreation(false)` on the SSL socket to ensure that no SSL sessions are

cached. This setting only controls whether an SSL session is added to the cache; it does not stop an SSL socket from finding an SSL session that was already cached. For example, SSL socket 1 caches the session, SSL socket 2 sets `setEnabledSessionCreation` to `false` but it can still reuse the SSL session from SSL socket 1 because that session was put in the cache.

SSL sessions exist for the lifetime of the SSL context; they are not controlled by the lifetime of the SSL socket. Therefore, creating a new SSL socket and connecting to the same host and port used by a previous session can resume a previous session as long as you create the SSL socket using an SSL socket factory from the SSL context that has the SSL session in its cache.

By default, clients that use HTTPS URLs get a new SSL session for each URL because each URL uses a different SSL context and therefore SSL sessions can not be shared or reused. You can retrieve the SSL session by using the `weblogic.net.http.HttpsClient` class or the `weblogic.net.http.HttpsURLConnection` class. Clients can also resume URLs by sharing a `SSLSocketFactory` between them.

Session caching is maintained by the SSL context, which can be shared by threads. A single thread has access to the entire session cache, not just one SSL session, so multiple SSL sessions can be used and shared in a single (or multiple) thread.

The following command-line arguments are ignored:

- `weblogic.security.SSL.sessionCache.size`
- `weblogic.security.SSL.sessionCache.ttl`

Configuring RMI over IIOP with SSL

Use SSL to protect Internet Interop-Orb-Protocol (IIOP) connections to Remote Method Invocation (RMI) remote objects. SSL secures connections through authentication and encrypts the data exchanged between objects.

To use SSL to protect RMI over IIOP connections:

1. Configure WebLogic Server to use SSL.
2. Configure the client Object Request Broker (ORB) to use SSL. Refer to the product documentation for your client ORB for information about configuring SSL.
3. Use the `host2ior` utility to print the WebLogic Server IOR to the console. The `host2ior` utility prints two versions of the interoperable object reference (IOR), one for SSL connections and one for non-SSL connections. The header of the IOR specifies whether or not the IOR can be used for SSL connections.

4. Use the SSL IOR when obtaining the initial reference to the CosNaming service that accesses the WebLogic Server JNDI tree.

For more information about using RMI over IIOP, see [Programming WebLogic RMI](#).

SSL Certificate Validation

WebLogic Server ensures that each certificate in a certificate chain was issued by a certificate authority. All X509 V3 CA certificates used with WebLogic Server must have the Basic Constraint extension defined as CA, thus ensuring that all certificates in a certificate chain were issued by a certificate authority. By default, any certificates for certificate authorities not meeting this criteria are rejected. This section describes the command-line argument that controls the level of certificate validation.

Note: If WebLogic Server is booted with a certificate chain that will not pass the certificate validation, an information message is logged noting that clients could reject it.

Controlling the Level of Certificate Validation

By default WebLogic Server rejects any certificates in a certificate chain that do not have the Basic Constraint extension defined as CA. However, you may be using certificates that do not meet this requirement or you may want to increase the level of security to conform to the IETF RFC 2459 standard. Use the following command-line argument to control the level of certificate validation performed by WebLogic Server:

```
-Dweblogic.security.SSL.enforceConstraints=option
```

[Table 12-1](#) describes the options for the command-line argument.

Table 12-1 Options for `-Dweblogic.security.SSL.enforceConstraints`

Option	Description
<code>strong</code> or <code>true</code>	<p>Use this option to ensure that the Basic Constraints extension on the CA certificate is defined as CA.</p> <p>For example:</p> <pre data-bbox="374 545 1056 644">-Dweblogic.security.SSL.enforceConstraints=strong or -Dweblogic.security.SSL.enforceConstraints=true</pre> <p>By default, WebLogic Server performs this level of certificate validation.</p>
<code>strict</code>	<p>Use this option to ensure the Basic Constraints extension on the CA certificate is defined as CA and set to critical. This option enforces the IETF RFC 2459 standard.</p> <p>For example:</p> <pre data-bbox="374 878 1056 900">-Dweblogic.security.SSL.enforceConstraints=strict</pre> <p>This option is not the default because a number of commercially available CA certificates do not conform to the IETF RFC 2459 standard.</p>
<code>off</code>	<p>Use this option to turn off checking for the Basic Constraints extension. The rest of the certificate is still validated.</p> <p>For example:</p> <pre data-bbox="374 1138 1009 1161">-Dweblogic.security.SSL.enforceConstraints=off</pre> <p>Oracle does not recommend using this option in a production environment. Instead, purchase new CA certificates that comply with the IETF RFC 2459 standard. CA certificates from most commercial certificate authorities should work with the default <code>strong</code> option.</p>

Accepting Certificate Policies in Certificates

WebLogic Server offers limited support for Certificate Policy Extensions in X.509 certificates. Use the `weblogic.security.SSL.allowedcertificatepolicyids` argument to provide a comma separated list of Certificate Policy IDs. When WebLogic Server receives a certificate with a critical Certificate Policies Extension, it verifies whether any Certificate Policy is on the list of allowed certificate policies and whether there are any unsupported policy qualifiers. This release

of WebLogic Server supports Certification Practice Statement (CPS) Policy qualifiers and does not support User Notice qualifiers. A certificate is also accepted if it contains a special policy `anyPolicy` with the ID 2.5.29.32.0, which indicates that the CA does not wish to limit the set of policies for this certificate.

To enable acceptance of Certificate Policies, start WebLogic Server with the following argument:

```
-Dweblogic.security.SSL.allowedcertificatepolicyids
<identifier1>,<identifier2>,...
```

This argument should contain a comma-separated list of Certificate Policy identifiers for all the certificates with critical extensions that might be present in the certificate chain, back to the root certificate, in order for WebLogic Server to accept such a certificate chain.

Checking Certificate Chains

Use the WebLogic Server `validateCertChain` command-line utility to confirm whether an existing certificate chain will be rejected by WebLogic Server. The utility validates certificate chains from PEM files, PKCS-12 files, PKCS-12 keystores, and JKS keystores. A complete certificate chain must be used with the utility. The following is the syntax for the `ValidateCertChain` command-line utility:

```
java utils.ValidateCertChain -file pemcertificatefilename
java utils.ValidateCertChain -pem pemcertificatefilename
java utils.ValidateCertChain -pkcs12store pkcs12storefilename
java utils.ValidateCertChain -pkcs12file pkcs12filename password
java utils.ValidateCertChain -jks alias storefilename [storePass]
```

Example of valid certificate chain:

```
java utils.ValidateCertChain -pem zippychain.pem
```

```
Cert[0]: CN=zippy,OU=FOR TESTING
ONLY,O=MyOrganization,L=MyTown,ST=MyState,C=US
```

```
Cert[1]: CN=CertGenCAB,OU=FOR TESTING
ONLY,O=MyOrganization,L=MyTown,ST=MyState,C=US
```

```
Certificate chain appears valid
```

Example of invalid certificate chain:

```
java utils.ValidateCertChain -jks mykey mykeystore
```

```
Cert[0]: CN=corbal,OU=FOR TESTING ONLY,  
O=MyOrganization,L=MyTown,ST=MyState,C=US  
  
CA cert not marked with critical BasicConstraint indicating it is a CA  
Cert[1]: CN=CACERT,OU=FOR TESTING ONLY,  
O=MyOrganization,L=MyTown,ST=MyState,C=US  
  
Certificate chain is invalid
```

Using Certificate Lookup and Validation Providers

WebLogic Server SSL has built-in certificate validation. Given a set of trusted CAs, this validation:

- Verifies that the last certificate in the chain is either a trusted CA or is issued by a trusted CA.
- Completes the certificate chain with trusted CAs.
- Verifies the signatures in the chain.
- Ensures that the chain has not expired.

You can use certificate lookup and validation (CLV) providers to perform additional validation on the certificate chain. In this release, WebLogic Server has added two CLV providers:

- **WebLogic CertPath Provider**—Completes certificate paths and validates certificates using the trusted CA configured for a particular server instance, providing the same functionality as the built-in SSL certificate validation. This is configured by default.
- **Certificate Registry**—The system administrator makes a list of trusted CA certificates that are allowed access to the server; a certificate is valid if the end certificate is in the registry. The administrator revokes a certificate by removing it from the certificate registry, which is an inexpensive mechanism for performing revocation checking. This is not configured by default.

Alternatively, you can write a custom CertPathValidator to provide additional validation on the certificate chain. See [CertPath Providers](#) in *Developing Security Providers for WebLogic Server*.

How SSL Certificate Validation Works in WebLogic Server

Outbound SSL and two-way inbound SSL in a WebLogic Server instance receive certificate chains during the SSL handshake that must be validated. An example of two-way inbound SSL

is a browser connecting to a Web application over HTTPS where the browser sends the client's certificate chain to the Web application. The inbound certificate validation setting is used for all two-way client certificate validation in the server.

Examples of WebLogic Server using outbound SSL (that is, acting as an SSL client) include:

- Connecting to the Node Manager
- Connecting to another WebLogic Server instance over the Administration port
- Connecting to an external LDAP server, such as the LDAPAuthenticator

Using the Administration Console or WLST, you can independently configure inbound and outbound SSL certificate validation using these `SSLMBean` attributes:

`InboundCertificateValidation` and `OutboundCertificateValidation`.

Legal values for both attributes are:

- `BUILTIN_SSL_VALIDATION`: Use the built-in SSL certificate validation code to complete and validate the certificate chain. That is, configure SSL to work as it has in previous releases. This is the default behavior.
- `BUILTIN_SSL_VALIDATION_AND_CERT_PATH_VALIDATORS`: Use the built-in trusted CA-based validation and the configured `CertPathValidator` providers to perform additional validation. That is, configure SSL to work as it has in previous releases and to do extra validation.

See:

- [SSLMBean](#) in the *WebLogic Server MBean Reference*
- [Set Up SSL](#) in the *Administration Console Online Help*

Troubleshooting Problems with Certificate Validation

If SSL communications that worked properly in a previous release of WebLogic Server start failing unexpectedly, the likely problem is that the certificate chain is failing the validation.

Determine where the certificate chain is being rejected, and decide whether to update the certificate chain with one that will be accepted, or change the setting of the `-Dweblogic.security.SSL.enforceConstraints` command-line argument.

To troubleshoot problems with certificates, use one of the following methods:

- If you know where the certificate chains for the processes using SSL communication are located, use the `ValidateCertChain` command-line utility to check whether the certificate chains will be accepted.
- Turn on SSL debug tracing on the processes using SSL communication. The syntax for SSL debug tracing is:

```
-Dssl.debug=true -Dweblogic.StdoutDebugEnabled=true
```

The following message indicates the SSL failure results from problems in the certificate chain:

```
<CA certificate rejected. The basic constraints for a CA certificate were not marked for being a CA, or were not marked as critical>
```

When you use one-way SSL, look for this error in the client log. With two-way SSL, look for this error in the client and server logs.

Using the nCipher JCE Provider with WebLogic Server

Note: Java Cryptography Extension (JCE) providers are written using the application programming interfaces (APIs) in the JCE available in JDK 5.0. This type of provider is different from the providers written using the WebLogic Security Service Provider Interfaces (SSPIs). WebLogic Server does not provide a JCE provider by default.

SSL is a key component in the protection of resources available in Web servers. However, heavy SSL traffic can cause bottlenecks that affect the performance of Web servers. JCE providers like nCipher that use a hardware card for encryption offload SSL processing from Web servers, which frees the servers to process more transactions. They also provide strong encryption and cryptographic processes to preserve the integrity and secrecy of keys.

WebLogic Server supports the use of the following JCE providers:

- The JDK JCE provider (`SunJCE`) in the JDK 5.0. For more information about the features in the JDK JCE provider, see <http://java.sun.com/products/jce>.

By default, the JCE provider in the JDK 5.0 has export strength jurisdiction policy files. After filling out the appropriate forms, the domestic strength jurisdiction policy files are downloadable from Sun Microsystems at <http://java.sun.com/products/jce/javase.html#UnlimitedDownload>.

WebLogic Server will continue to control the strength of the cryptography used by the WebLogic Server Application Programming Interfaces (APIs). Client code without the appropriate domestic strength cryptography setting will only be able to use the J2SE export

strength default cryptography. On the server, WebLogic Server will enable either export or domestic strength cryptography.

- The nCipher JCE provider. See <http://www.ncipher.com>.

To install the nCipher JCE provider:

1. Install and configure the hardware for the nCipher JCE provider according to the product's documentation.
2. Install the files for the nCipher JCE provider. The following files are required:
 - Jurisdiction policy files—The JDK installs these files by default but they are of limited export strength.
 - Certificate that signed the JAR file

Note: This step may have been performed as part of installing the hardware for nCipher JCE provider. In that case, verify that the files are correctly installed.

- The JCE provider JAR files

Choose an installation method for the files:

- Install files as an extension. Copy the files to one of the following locations:

```
JAVA_HOME/jre/lib/ext
```

For example:

```
BEA_HOME/jdk150_03/jre/lib/ext
```

- Install files in the CLASSPATH of the server.

3. Edit the Java security properties file (`java.security`) to add the nCipher JCE provider to the list of approved JCE providers for WebLogic Server. The Java security properties file is located in:

```
JAVA_HOME/jre/lib/security/java.security
```

Specify the nCipher JCE provider as:

```
security.provider.n=com.ncipher.provider.km.mCipherKM
```

where

n specifies the preference order that determines the order in which providers are searched for requested algorithms when no specific provider is requested. The order is 1-based; 1 is the most preferred, followed by 2, and so on.

The nCipher JCE provider must follow the RSA JCA provider in the security properties file. For example:

```
security.provider.1=sun.security.provider.Sun
security.provider.2=com.sun.rsa.jca.Provider
security.provider.3=com.ncipher.provider.km.mCipherKM
```

4. Boot WebLogic Server.
5. To ensure the nCipher JCE provider is working properly, enable debugging according to the nCipher product documentation.

Specifying the Version of the SSL Protocol

WebLogic Server supports both the SSL V3.0 and TLS V1.0 protocols. When WebLogic Server is acting as an SSL server, the protocol that the client specifies as preferred in its client hello message. When WebLogic Server is acting as an SSL client, it specifies TLS1.0 as the preferred protocol in its SSL V2.0 client hello message, but can use SSL V3.0 as well, if that is the highest version that the SSL server on the other end supports. The peer must respond with an SSL V3.0 or TLS V1.0 message or the SSL connection is dropped.

While in most cases the SSL V3.0 protocol is acceptable some circumstances (compatibility, SSL performance, and environments with maximum security requirements) make the TLS V1.0 protocol more desirable. The `weblogic.security.SSL.protocolVersion` command-line argument lets you specify which protocol is used for SSL connections.

Note: The SSL V3.0 and TLS V1.0 protocols can not be interchanged. Only use the TLS V1.0 protocol if you are certain all desired SSL clients are capable of using the protocol.

The following command-line argument can be specified so that WebLogic Server supports only SSL V3.0 or TLS V1.0 connections:

- `-Dweblogic.security.SSL.protocolVersion=SSL3`—Only SSL V3.0 messages are sent and accepted.
- `-Dweblogic.security.SSL.protocolVersion=TLS1`—Only TLS V1.0 messages are sent and accepted.
- `-Dweblogic.security.SSL.protocolVersion=ALL`—This is the default behavior.

Configuring Security for a WebLogic Domain

The following sections describe how to set security configuration options for a WebLogic domain:

- [“Important Information Regarding Cross-Domain Security Support”](#) on page 13-1
- [“Enabling Trust Between WebLogic Server Domains”](#) on page 13-2
- [“Using Connection Filters”](#) on page 13-6
- [“Using the Java Authorization Contract for Containers”](#) on page 13-8
- [“Viewing MBean Attributes”](#) on page 13-8
- [“How Passwords Are Protected in WebLogic Server”](#) on page 13-8
- [“Protecting User Accounts”](#) on page 13-9

Note: These sections apply to WebLogic Server deployments using the security features in this release of WebLogic Server as well as deployments using Compatibility Security.

Important Information Regarding Cross-Domain Security Support

This section describes important information regarding support for the cross-domain security solution.

As described in [“Enabling Trust Between WebLogic Server Domains”](#) on page 13-2, cross-domain security establishes trust between domains such that principals in a subject from

one WebLogic Server domain can make calls in another domain. WebLogic Server establishes a security role for cross-domain users, and uses the WebLogic Credential Mapping security provider in each domain to store the credentials to be used by the cross-domain users.

In this release of WebLogic Server, subsystems such as JMS, JTA, MDB, and WAN replication implement cross-domain security. These subsystems can authenticate and send the required credentials across domains.

However, the EJB container does not implement the solution for cross-domain security. As a result, the WLS cross-domain security feature does not work in the following situations:

- WLI domain
- With ALSB, when ALSB is configured to use the SB and DSP transports.
- ALDSP domain

For these domain types, the alternative is to use the global trust feature, in which global trust is established between two domains by using the same domain credential in each domain. For information about the global trust approach in WLS, see [“Enabling Global Trust” on page 13-5](#).

Enabling Trust Between WebLogic Server Domains

Trust between domains is established so that principals in a Subject from one WebLogic Server domain can make calls in another domain. In previous releases of WebLogic Server, there was only one type of domain trust which is now referred to as Global Trust. WebLogic Server now supports a type of domain trust that is referred to as Cross Domain Security.

- [“Enabling Cross Domain Security Between WebLogic Server Domains” on page 13-2](#)
- [“Enabling Global Trust” on page 13-5](#)

Enabling Cross Domain Security Between WebLogic Server Domains

Note: Please see [“Important Information Regarding Cross-Domain Security Support” on page 13-1](#) before enabling cross domain security.

Cross Domain Security establishes trust between two WebLogic Server domain pairs by using a credential mapper to configure communication between these WebLogic Server domains. Configuration and use of cross-domain security is described in the following sections:

- [“Configuring Cross-Domain Security” on page 13-3](#)

- [“Configuring a Cross-Domain User” on page 13-3](#)
- [“Configure a Credential Mapping for Cross-Domain Security” on page 13-4](#)

In addition to the approach that uses a Credential Mapping security provider for cross-domain security, WebLogic Server also enables a different approach, under which global trust is established between two or more domains by using the same domain credential in each domain. If you enable global trust between two or more domains, the trust relationship is transitive and symmetric. In other words, if Domain A trusts Domain B and Domain B trusts Domain C, then Domain A will also trust Domain C and Domain B and Domain C will both trust Domain A. In most cases, the Cross Domain Security approach is preferable to the global trust approach, because its use of a specific user group and role for cross-domain actions allows for finer grained security. For information about the global trust approach in WebLogic Server, see [“Enabling Global Trust” on page 13-5](#).

Configuring Cross-Domain Security

To configure cross-domain security in a WebLogic Server domain, set the `SecurityConfigurationMBean.CrossDomainSecurityEnabled` attribute to true. To do this in the WebLogic Server Administration Console:

1. Click the name of the domain in the Domain Configuration panel.
2. Open the Security: General tab in the console.
3. Check Cross Domain Security Enabled.

If you maintain any WebLogic Server domains that have not enabled cross-domain security, you need to add their domain names to the list of excluded domains, in the `SecurityConfigurationMBean.ExcludedDomainNames` attributes. To do this in the WebLogic Server Administration Console:

1. Click the name of the domain in the Domain Configuration panel.
2. Open the Security: General tab in the console.
3. In the Excluded Domain Names field, enter the names of any domains that do not have cross-domain security enabled. Enter the names of these domains separated either by semicolons or line breaks.

Configuring a Cross-Domain User

Cross-domain security in WebLogic Server uses a global security role named `CrossDomainConnector` with resource type remote and a group named

`CrossDomainConnectors`, which is assigned the `CrossDomainConnector` role. Invocation requests from remote domains are expected to be from users with the `CrossDomainConnector` role. By default, the `CrossDomainConnectors` has no users as members. You need to create one or more users and add them to the group `CrossDomainConnectors`. Typically, such a user will be a virtual system user and preferably should have no privileges other than those granted by the `CrossDomainConnector` security role.

Configure a Credential Mapping for Cross-Domain Security

Note: The Credential Mapper identifies domains by their names. Therefore, it is important that the domains involved have unique names.

In each WebLogic Server domain, you need to specify a credential to be used by each user on each remote domain that needs to be trusted. Do this by configuring credential mappings for each domain in the connection. Each credential mapping needs to specify:

- The resource protocol, which is named `cross-domain-protocol`
- The name of the remote domain that needs to interact with the local domain
- The name of the user in the remote domain that will be authorized to interact with the local domain
- The password of the user in the remote domain that will be authorized to interact with the local domain

To configure a cross-domain security credential mapping in the WebLogic Server Administration Console, click Security Realms in the left panel.

1. Click the name of your security realm (default is `myrealm`).
2. On the Credential Mappings → Default tab, click New.
3. On the Creating the Remote Resource for the Security Credential Mapping:
 - Select Use cross-domain protocol.
 - In the Remote Domain field, enter the name of the remote domain that needs to interact with the local domain.
4. Click Next.
5. On the Create a New Security Credential Map Entry page, enter the following:

Local User: `cross-domain`

Remote User: User configured in the Remote Domain that is authorized to interact with the Local Domain.

Password: The password for the Remote User.

6. Click Finish.

See [Create a Cross-Domain Security Credential Mapping](#) in the *Administration Console Online Help*.

Enabling Global Trust

Note: Enabling Global Trust between WebLogic Server domains has the potential to open the servers up to man-in-the-middle attacks. Great care should be taken when enabling trust in a production environment. Oracle recommends having strong network security such as a dedicated communication channel or protection by a strong firewall.

WebLogic Server enables you to establish global trust between two or more domains. You do this by specifying the same Domain Credential for each of the domains. By default, the Domain Credential is randomly generated and therefore, no two domains will have the same Domain Credential. If you want two WebLogic Server domains to interoperate, you need to replace the generated credential with a credential you select, and set the same credential in each of the domains. For configuration information, see [Enable global trust between domains](#) in the *Administration Console Online Help*.

If you enable global trust between two domains, the trust relationship is transitive and symmetric. In other words, if Domain A trusts Domain B and Domain B trusts Domain C, then Domain A will also trust Domain C and Domain B and Domain C will both trust Domain A. In most cases, the credential mapper approach, described in [“Enabling Cross Domain Security Between WebLogic Server Domains” on page 13-2](#), is preferable to the global trust approach, because it provides closer control over access.

Global trust between domains is established so that principals in a Subject from one WebLogic Server domain are accepted as principals in another domain. When this feature is enabled, identity is passed between WebLogic Server domains over an RMI connection without requiring authentication in the second domain (for example: log in to Domain 1 as Joe, make an RMI call to Domain 2 and Joe is still authenticated). WebLogic Server signs Principals with the Domain Credential as Principals are created. When a Subject is received from a remote source, its Principals are validated (the signature is recreated and if it matches, the remote domain has the same Domain Credential). If validation fails, an error is generated. If validation succeeds, the Principals are trusted as if they were created locally.

Note: Any credentials in clear text are encrypted the next time the `config.xml` file is persisted to disk.

If you are enabling global trust between domains in a Managed Server environment, you must stop the Administration Server and all the Managed Servers in both domains and then restart them. If this step is not performed, servers that were not rebooted will not trust the servers that were rebooted.

Keep the following points in mind when enabling global trust between WebLogic Server domains:

- Because a domain will trust remote Principals without requiring authentication, it is possible to have authenticated users in a domain that are not defined in the domain's authentication database. This situation can cause authorization problems.
- Any authenticated user in a domain can access any other domain that has trust enabled with the original domain without re-authenticating. There is no auditing of this login and group membership is not validated. Therefore, if Joe is a member of the Administrators group in the original domain where he authenticated, he is automatically a member of the Administrators group for all trusted domains to which he makes RMI calls.
- If Domain 2 trusts both Domain 1 and Domain 3, Domain 1 and Domain 3 now implicitly trust each other. Therefore, members of the Administrators Group in Domain 1 are members of the Administrators group in Domain 3. This may not be a desired trust relationship.
- If you extended the `WLSUser` and `WLSGroup` Principal classes, the custom Principal classes must be installed in the server's classpath in all domains that share trust.

To avoid these issues, Oracle recommends that rather than enabling global trust between two domains, you should instead configure users with the `CrossDomainConnector` role and use the credential mapping approach described in [“Enabling Cross Domain Security Between WebLogic Server Domains”](#) on page 13-2.

Using Connection Filters

Connection filters allow you to deny access at the network level. They can be used to protect server resources on individual servers, server clusters, or an entire internal network or intranet. For example, you can deny any non-SSL connections originating outside of your corporate network. Network connection filters are a type of firewall in that they can be configured to filter on protocols, IP addresses, and DNS node names.

Connection filters are particularly useful when using the Administration port. Depending on your network firewall configuration, you may be able to use a connection filter to further restrict administration access. A typical use might be to restrict access to the Administration port to only the servers and machines in the domain. An attacker who gets access to a machine inside the firewall, still cannot perform administration operations unless the attacker is on one of the permitted machines.

WebLogic Server provides a default connection filter called `weblogic.security.net.ConnectionFilterImpl`. This connection filter accepts all incoming connections and also provides static factory methods that allow the server to obtain the current connection filter. To configure this connection filter to deny access, simply enter the connection filters rules in the WebLogic Administration Console.

You can also use a custom connection filter by implementing the classes in the `weblogic.security.net` package. For information about writing a connection filter, see [Using Network Connection Filters](#) in *Programming WebLogic Security*. Like the default connection filter, custom connection filters are configured in the WebLogic Administration Console.

To configure a connection filter:

1. Enable the logging of accepted messages. This Connection Logger Enabled option logs successful connections and connection data in the server. This information can be used to debug problems relating to server connections.
2. Choose which connection filter is to be used in the domain.
 - To configure the default connection filter, specify `weblogic.security.net.ConnectionFilterImpl` in Connection Filter.
 - To configure a custom connection filter, specify the class that implements the network connection filter in Connection Filter. This class must also be specified in the CLASSPATH for WebLogic Server.
3. Enter the syntax for the connection filter rules.

For more information:

- See [Configure connection filtering](#) in the *Administration Console Online Help*.
- For information about connection filter rules and writing a custom connection filter, see [Using Network Connection Filters](#) and [Developing Custom Connection Filters](#) in *Programming WebLogic Security*.
- You can also use the WebLogic Scripting Tool or Java Management Extensions (JMX) APIs to create a new security configuration.

Using the Java Authorization Contract for Containers

The Java Authorization Contract for Containers (JACC) Standard can replace the EJB and Servlet container deployment and authorization provided by WebLogic Server. When you configure a WebLogic Server domain to use JACC, EJB and servlet authorization decisions are made by the classes in the JACC framework. All other authorization decisions within WebLogic Server are still determined by the WebLogic Security Framework. For information about the WebLogic JACC provider, see [Using the Java Authorization Contract for Containers](#) in *Programming WebLogic Security*.

You configure WebLogic Server to use JACC with a command line start option. For more information, see the description of the `-Djava.security.manager` option in the [weblogic.Server Command-Line Reference](#).

Note that an Administration Server and all Managed Servers in a domain need to have the same JACC configuration. If you change the JACC setting on the Administration Server, you should shut down the Managed Server and reboot them with the same settings as the Administration Server to avoid creating a security vulnerability. Otherwise, it may appear that EJBs and servlets in your domain are protected by WebLogic Security Framework roles and policies, when in fact the Managed Servers are still operating under JACC.

Viewing MBean Attributes

The Anonymous Admin Lookup Enabled option specifies whether anonymous, read-only access to WebLogic Server MBeans should be allowed from the `MBean` API. With this anonymous access, you can see the value of any MBean attribute that is not explicitly marked as protected by the WebLogic Server MBean authorization process. This option is enabled by default to assure backward compatibility. For greater security, you should disable this anonymous access.

To verify the setting of the Anonymous Admin Lookup Enabled option through the WebLogic Administration Console, see the Domain → Security → General page in the Administration Console or the `SecurityConfigurationMBean.AnonymousAdminLookupEnabled` attribute.

How Passwords Are Protected in WebLogic Server

It is important to protect passwords that are used to access resources in a WebLogic Server domain. In the past, usernames and passwords were stored in clear text in a WebLogic security realm. Now all the passwords in a WebLogic Server domain are hashed. The `SerializedSystemIni.dat` file contains the hashes for the passwords. It is associated with a specific WebLogic Server domain so it cannot be moved from domain to domain.

If the `SerializedSystemIni.dat` file is destroyed or corrupted, you must reconfigure the WebLogic Server domain. Therefore, you should take the following precautions:

- Make a backup copy of the `SerializedSystemIni.dat` file and put it in a safe location.
- Set permissions on the `SerializedSystemIni.dat` file such that the system administrator of a WebLogic Server deployment has write and read privileges and no other users have any privileges.

Protecting User Accounts

WebLogic Server defines a set of configuration options to protect user accounts from intruders. In the default security configuration, these options are set for maximum protection. You can use the Administration Console to modify these options on the Configuration → User Lockout page.

As a system administrator, you have the option of turning off all the configuration options, increasing the number of login attempts before a user account is locked, increasing the time period in which invalid login attempts are made before locking the user account, and changing the amount of time a user account is locked. Remember that changing the configuration options lessens security and leaves user accounts vulnerable to security attacks. See [Set user lockout attributes](#) in the *Administration Console Online Help*.

Notes: The User Lockout options apply to the default security realm and all its security providers. The User Lockout options do not work with custom security providers in a security realm other than the default security realm. To use the User Lockout options with custom security providers, configure the custom security providers in the default security realm. Include the customer providers in the authentication process after the WebLogic Authentication provider and the WebLogic Identity Assertion provider. This ordering may cause a small performance hit.

If you are using an Authentication provider that has its own mechanism for protecting user accounts, disable Lockout Enabled.

If a user account becomes locked and you delete the user account and add another user account with the same name and password, the User Lockout configuration options will not be reset.

For information about unlocking a locked user account on the Administration Server, see [Unlock a user account](#) in the *Administration Console Online Help*. Unlocking a locked user account on a Managed Server cannot be done through the WebLogic Administration Console. The unlock information is propagated through a multicast message which is only configured in a cluster environment. Use the following command instead:

Configuring Security for a WebLogic Domain

```
java weblogic.Admin -url url -username adminuser  
-password passwordforadminuser -type  
weblogic.management.security.authentication.UserLockoutManager -method  
clearLockout lockedusername
```

You can also wait the time specified in the Lockout Duration attribute: the user account will be unlocked after the specified time.

Using Compatibility Security

Compatibility security is the capability to run security configurations developed with WebLogic Server 6.x in this release of WebLogic Server. In Compatibility security, you manage 6.x security realms, users, groups, and ACLs, protect user accounts, and configure the Realm Adapter Auditing provider and optionally the Identity Assertion provider in the Realm Adapter Authentication provider. The following sections describe how to configure Compatibility security:

- [“Running Compatibility Security: Main Steps”](#) on page 14-2
- [“Limited Visibility of Compatibility Security MBeans”](#) on page 14-2
- [“The Default Security Configuration in the CompatibilityRealm”](#) on page 14-3
- [“Configuring a Realm Adapter Authentication Provider”](#) on page 14-4
- [“Configuring the Identity Assertion Provider in the Realm Adapter Authentication Provider”](#) on page 14-5
- [“Configuring a Realm Adapter Auditing Provider”](#) on page 14-5
- [“Protecting User Accounts in Compatibility Security”](#) on page 14-5
- [“Accessing 6.x Security from Compatibility Security”](#) on page 14-6

Note: Compatibility security is deprecated in this release of WebLogic Server and will not be supported in future major releases. Oracle strongly recommends upgrading your WebLogic Server deployment to the security features in this release of WebLogic Server. You should only use Compatibility security pending such an upgrade.

Running Compatibility Security: Main Steps

To set up Compatibility security:

1. Make a backup copy of your 6.x WebLogic domain (including your `config.xml` file) before using Compatibility security.
2. Add the following to the 6.x `config.xml` file if it does not exist, replacing the values with the actual names of your domain, security realm, and `FileRealm`:

```
<Security Name="mydomain" Realm="mysecurity" />
<Realm Name="mysecurity" FileRealm="myrealm" />
<FileRealm Name="myrealm" />
```

3. Install the current version of WebLogic Server in a new directory location. Do not overwrite your existing 6.x installation directory. For more information, see [Installation Guide](#).
4. Modify the start script for your 6.x server to point to the new WebLogic Server installation. Specifically, you need to modify:
 - The classpath to point to the `weblogic.jar` file in the new WebLogic Server installation.
 - The `JAVA_HOME` variable to point to the new WebLogic Server installation.
5. Use the start script for your 6.x server to boot the new version of WebLogic Server.

To verify whether you are running Compatibility security correctly, open the new WebLogic Server Administration Console. If you are running Compatibility security, a Compatibility Security node is displayed on the left in the Domain Structure pane.

Limited Visibility of Compatibility Security MBeans

All Compatibility security MBeans are marked excluded and therefore have limited visibility in the WebLogic Scripting Tool. For example, if you use a command like this:

```
java weblogic.WLST
connect()
ls()
```

then the attributes of the `DomainMBean` will be listed, excluding Compatibility security attributes such as `FileRealmMBean`. However, if you address a Compatibility MBean directly, you can access it, as in this example:

```
java weblogic.WLST
connect()
cmo.getFileRealms()
```

The Default Security Configuration in the CompatibilityRealm

By default, the `CompatibilityRealm` is configured with a Realm Adapter Adjudication provider, a Realm Adapter Authentication provider, a WebLogic Authorization provider, a Realm Adapter Authorization provider, a WebLogic Credential Mapping provider, and a WebLogic Role Mapping provider.

- In the `CompatibilityRealm`, the Realm Adapter Authentication provider is populated with users and groups from the 6.x security realm defined in the `config.xml` file.
 - If you used the File realm in your 6.x security configuration, you can manage the users and groups in the Realm Adapter Authentication provider following the steps in [Define Users](#) and [Define Groups](#) topics of the Compatibility security section of the *Administration Console Online Help*.
 - If you are using an alternate security realm (LDAP, Windows NT, RDBMS, or custom), you must use the administration tools provided by that realm to manage users and groups.

For information about configuring a Realm Adapter Authentication provider, see [“Configuring a Realm Adapter Authentication Provider”](#) on page 14-4

You can use implementations of the `weblogic.security.acl.CertAuthenticator` class in Compatibility security by configuring the Identity Assertion provider in the Realm Adapter Authentication provider. For more information, see [“Configuring the Identity Assertion Provider in the Realm Adapter Authentication Provider”](#) on page 14-5.

- Access Control Lists (ACLs) in the 6.x security realm are used to populate the Realm Adapter Authorization provider.
- The Realm Adapter Adjudication provider enables the use of both ACLs and security roles and security policies in Compatibility security. The Realm Adapter Adjudication provider can be used only with the Realm Adapter Authentication provider and the WebLogic Authorization provider. It resolves access decision conflicts between ACLs and new security policies set through the Administration Console. The Realm Adapter Adjudication provider permits access if the one authorization provider votes PERMIT and the other authorization provider votes DENY.

- The WebLogic Credential Mapping provider allows the use of credential maps in Compatibility security. For more information, see [Programming WebLogic Resource Adapters](#).
- You can add a Realm Adapter Auditing provider to access implementations of the `weblogic.security.audit.AuditProvider` class from the `CompatibilityRealm`. For more information, see [Configure a Realm Adapter Auditing Provider](#) in the *Administration Console Online Help*.

Configuring a Realm Adapter Authentication Provider

When using Compatibility security, a Realm Adapter Authentication provider is by default configured for the `CompatibilityRealm`. For information about using the Realm Adapter Authentication provider in the `CompatibilityRealm`, see [“The Default Security Configuration in the CompatibilityRealm”](#) on page 14-3.

The Realm Adapter Authentication provider also allows use of implementations of the `weblogic.security.acl.CertAuthenticator` class with this release of WebLogic Server. The Realm Adapter Authentication provider includes an Identity Assertion provider that asserts identity based on X.509 tokens. For information about using a `CertAuthenticator` with WebLogic Server, [“Configuring the Identity Assertion Provider in the Realm Adapter Authentication Provider”](#) on page 14-5.

When you add a Realm Adapter Authentication provider to a security realm with an Authentication provider already configured, WebLogic Server sets the JAAS Control Flag on the Realm Adapter Authentication provider to `OPTIONAL` and checks for the presence of a `fileRealm.properties` file in the domain directory. WebLogic Server will not add the Realm Adapter Authentication provider to the security realm if the `fileRealm.properties` file does not exist.

Note: The subjects produced by the Realm Adapter Authentication provider do not contain principals for the groups to which a user belongs. Use the `weblogic.security.SubjectUtils.isUserInGroup()` method to determine whether a user is in a group. When you use subjects produced by the Realm Adapter Authentication provider, you cannot iterate the complete set of groups to which a user belongs.

Configuring the Identity Assertion Provider in the Realm Adapter Authentication Provider

The Realm Adapter Authentication provider includes an Identity Assertion provider. The Identity Assertion provider provides backward compatibility for implementations of the deprecated `weblogic.security.acl.CertAuthenticator` class. The identity assertion is performed on X.509 tokens. By default, the Identity Assertion provider is not enabled in the Realm Adapter Authentication provider.

For information about how to enable the Identity Assertion provider, see [Enable the Identity Assertion provider](#) in the *Administration Console Online Help*.

Configuring a Realm Adapter Auditing Provider

The Realm Adapter Auditing provider allows you to use implementations of the `weblogic.security.audit.AuditProvider` interface when using Compatibility security. In order for the Realm Adapter Auditing provider to work properly, the implementation of the `AuditProvider` interface must have been defined. You can define the `AuditProvider` class using the Administration Console, in the Audit Provider Class field on the Domain: Compatibility Security → General page.

For information, see [Configure a Realm Adapter Auditing provider](#) in the *Administration Console Online Help*.

Protecting User Accounts in Compatibility Security

Password guessing is a common type of security attack. In this type of attack, a hacker attempts to log in to a computer using various combinations of usernames and passwords. WebLogic Server provides a set of lockout configuration options to protect user accounts from this kind of attack. By default, these options are set for maximum protection. As a system administrator, you have the option of turning off all the options, increasing the number of login attempts before a user account is locked, increasing the time period in which invalid login attempts are made before locking the user account, and changing the amount of time a user account is locked. Remember that changing the configuration options lessens security and leaves user accounts vulnerable to security attacks.

There are two sets of configuration options available to protect user accounts, one set at the domain and one set at the security realm. You may notice that if you set one set of configuration options (for example, the options for the security realm) and exceed any of the values, the user

account is not locked. This happens because the user account lockout options at the domain override the user account options at the security realm. To avoid this situation, disable the user account lockout options at the security realm.

WARNING: If you disable the user lockout configuration option at the security realm, you must set the user lockout configuration options on the domain otherwise the user accounts will not be protected.

For information, see [Protect user accounts](#) and [Unlock user accounts](#) in the *Administration Console Online Help*.

Accessing 6.x Security from Compatibility Security

Using Compatibility security assumes that you have an existing `config.xml` file with a security realm that defines users and groups and ACLs that protect the resources in your WebLogic Server domain. WebLogic Server 6.x security management tasks such as configuring a security realm or defining ACLs should not be required and therefore those management tasks are not described in this section. However, if you corrupt an existing 6.x security realm and have no choice but to restore it, the following 6.x security management tasks are described in the Compatibility Security topic of the *Administration Console Online Help*:

- Configure LDAP V1 security realms
- Configure LDAP V2 security realms
- Configure RDBMS security realms
- Configure Windows NT security realms
- Configure wlauth for UNIX security realms
- Configure UNIX security realms
- Configure Custom security realms
- Configure Caching realms
- Configure the File realm
- Define ACLs
- Define groups
- Delete groups

- Define users
- Delete users
- Change user passwords
- Change the system password
- Disable the Guest user

WARNING: Compatibility security provides backward compatibility only and should not be considered a long-term security solution.

Using Compatibility Security

Security Configuration MBeans

This section describes MBeans used in configuring the WebLogic Security Framework. Each MBean attribute is marked either dynamic, meaning that the attribute value can be changed without requiring a server restart, or non-dynamic, meaning that if you change the attribute value, you need to restart the server for the change to take effect. Note also that if an edit is made to a non-dynamic attribute, no edits to dynamic attributes will take effect until after restart. This is to assure that a batch of updates having a combination of dynamic and non-dynamic attribute edits will not be partially activated.

Any security MBeans not listed are completely non-dynamic (create or destroy MBean, change any attribute).

For more information about WebLogic Security MBeans, see:

- [Managing Security Realms with JMX](#) in *Developing Custom Management Utilities with JMX*
- [Security MBeans](#) in the *WebLogic Server MBean Reference*

SSLMBean

Creating or destroying this bean is dynamic.

Dynamic attributes:

Enabled, TwoWaySSLEnabled, ClientCertificateEnforced, ListenPort

Ciphersuites, ExportKeyLifespan, SSLRejectionLoggingEnabled, LoginTimeoutMillis

ServerCertificateChainFileName, ServerKeyFileName, ServerCertificateFileName,
TrustedCAFileName

ServerPrivateKeyAlias, ServerPrivateKeyPassPhrase

IdentityAndTrustLocations

InboundCertificateValidation, OutboundCertificateValidation

All other attributes are non-dynamic.

ServerMBean

Creating or destroying this bean is dynamic.

Dynamic attributes:

KeyStores

CustomIdentityKeyStoreFileName, CustomIdentityKeyStoreType,
CustomIdentityKeyStorePassPhrase

CustomTrustKeyStoreFileName, CustomTrustKeyStoreType, CustomTrustKeyStorePassPhrase

JavaStandardTrustKeyStorePassPhrase

All other attributes are non-dynamic.

EmbeddedLDAPMBean

Dynamic attributes:

Credential

All other attributes are non-dynamic

SecurityMBean

Dynamic attributes:

ConnectionFilterRules

ConnectionLoggerEnabled

All other attributes are non-dynamic

SecurityConfigurationMBean

Dynamic attributes:

Credential

ConnectionFilterRules, ConnectionLoggerEnabled, CompatibilityConnectionFiltersEnabled

NodeManagerUsername, NodeManagerPassword

All other attributes are non-dynamic.

RealmMBean

Creating or destroying this MBean is non-dynamic.

Dynamic attributes:

DeployRoleIgnored, DeployPolicyIgnored, DeployCredentialMappingIgnored

FullyDelegateAuthorization

ValidateDDSecurityData, SecurityDDModel

CombinedRoleMappingEnabled

All other attributes are non-dynamic

WindowsNTAuthenticatorMBean

Creating or destroying this MBean is non-dynamic.

Dynamic attributes:

BadDomainControllerRetryInterval

MapUPNNames, LogonType

MapNTDomainName

All other attributes are non-dynamic.

CustomDBMSAuthenticatorMBean

Creating or destroying this MBean is non-dynamic. The ControlFlag and read-only provider attributes (such as ProviderClassName and Description) are non-dynamic. All other attributes are dynamic.

ReadOnlySQLAuthenticatorMBean

Creating or destroying this MBean is non-dynamic.

The ControlFlag and read-only provider attributes (such as ProviderClassName and Description) are non-dynamic. All other attributes are dynamic.

SQLAuthenticatorMBean

Creating or destroying this MBean is non-dynamic.

The ControlFlag and read-only provider attributes (such as ProviderClassName and Description) are non-dynamic. All other attributes are dynamic.

DefaultAuditorMBean

Creating or destroying this MBean is non-dynamic.

Dynamic attributes:

Severity

All other attributes are non-dynamic

Compatibility Security MBeans

All MBeans used for Compatibility security are completely non-dynamic (create or destroy MBean, change any attribute). These MBeans include:

RealmMBean

FileRealmMBean

BasicRealmMBean

CachingRealmMBean

PasswordPolicyMBean

CustomRealmMBean

LDAPRealmMBean

NTRealmMBean

RDBMSRealmMBean

UnixRealmMBean

UserLockoutManagerMBean

This MBean is completely non-dynamic (create or destroy MBean, change any attribute).

Other Security Provider MBeans

All other security MBeans are completely non-dynamic (create or destroy MBean, change any attribute).

Security Configuration MBeans