

Oracle® Communications ASAP

Security Guide



Release 7.4

F40780-01

April 2022

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Copyright © 2012, 2022, Oracle and/or its affiliates.

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

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware 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 that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle, Java, and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

Audience	v
Documentation Accessibility	v
Diversity and Inclusion	v

1 ASAP Security Overview

Basic Security Considerations	1-1
Understanding the ASAP Environment	1-1
Overview of ASAP Security	1-2
Recommended Deployment Topologies	1-3
Single-Computer Installation Topology	1-3
Tiered Deployment	1-3
ASAP Port Requirements	1-4
Operating System Security	1-5
Oracle Database Security	1-5
WebLogic Server Security	1-5
LDAP Security	1-5
Oracle Security Documentation	1-5

2 Performing a Secure ASAP Installation

Pre-Installation Configuration	2-1
Installing ASAP Securely	2-1
Securely Integrating Oracle Analytics Server with ASAP	2-2

3 Implementing ASAP Security

Configuring WebLogic Server Security	3-1
Configuring Authentication Providers for ASAP	3-1
Managing ASAP WebLogic Server User Security	3-1
Configuring ASAP Server and Database Credential Security	3-1

Configuring Security for Network Elements Communication 3-2

4 Performing a Secure Order Balancer Installation

Pre-Installation Configuration	4-1
Installing Order Balancer Securely	4-1
Adding ASAP Instances	4-2
Configuring Authentication Providers for Order Balancer	4-2
Managing ASAP WebLogic Server User Security	4-2

5 Security Considerations for Developers

Securing OSS/J Over JMS Connections	5-1
Securing Web Services Connections	5-1
Cartridge Development	5-2

A ASAP Secure Deployment Checklist

Secure Deployment Checklist	A-1
-----------------------------	-----

Preface

This guide provides guidelines and recommendations for setting up Oracle Communications ASAP in a secure configuration.

Audience

This document is intended for system administrators, system integrators, database administrators, and other individuals who are responsible for managing ASAP and ensuring that the software is operating in a secure manner. This guide assumes that you have a working knowledge of ASAP, the relevant operating system, Oracle Database, Oracle WebLogic Server, and Java J2EE software.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

1

ASAP Security Overview

This chapter provides an overview of Oracle Communications ASAP security.

Basic Security Considerations

The following principles are fundamental to using any application securely:

- **Keep software up to date.** This includes the latest product release and any patches that apply to it.
- **Limit privileges as much as possible.** Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- **Monitor system activity.** Establish who should access which system components, how often they should be accessed, and who should monitor those components.
- **Install software securely.** For example, use firewalls, secure protocols (such as TLS), and secure passwords. See "[Performing a Secure ASAP Installation](#)" for more information.
- **Learn about and use ASAP security features.** See "[Implementing ASAP Security](#)" for more information.
- **Use secure development practices.** For example, take advantage of existing database security functionality instead of creating your own application security. See "[Security Considerations for Developers](#)" for more information.
- **Keep up to date on security information.** Oracle regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible. See "Critical Patch Updates and Security Alerts" on the Oracle website:

<http://www.oracle.com/technetwork/topics/security/alerts-086861.html>

Understanding the ASAP Environment

When planning your ASAP implementation, consider the following:

- **Which resources must be protected?** For example:
 - You must protect customer data.
 - You must protect internal data, such as proprietary source code.
 - You must protect system components from being disabled by external attacks or intentional system overloads.
- **Who are you protecting data from?**

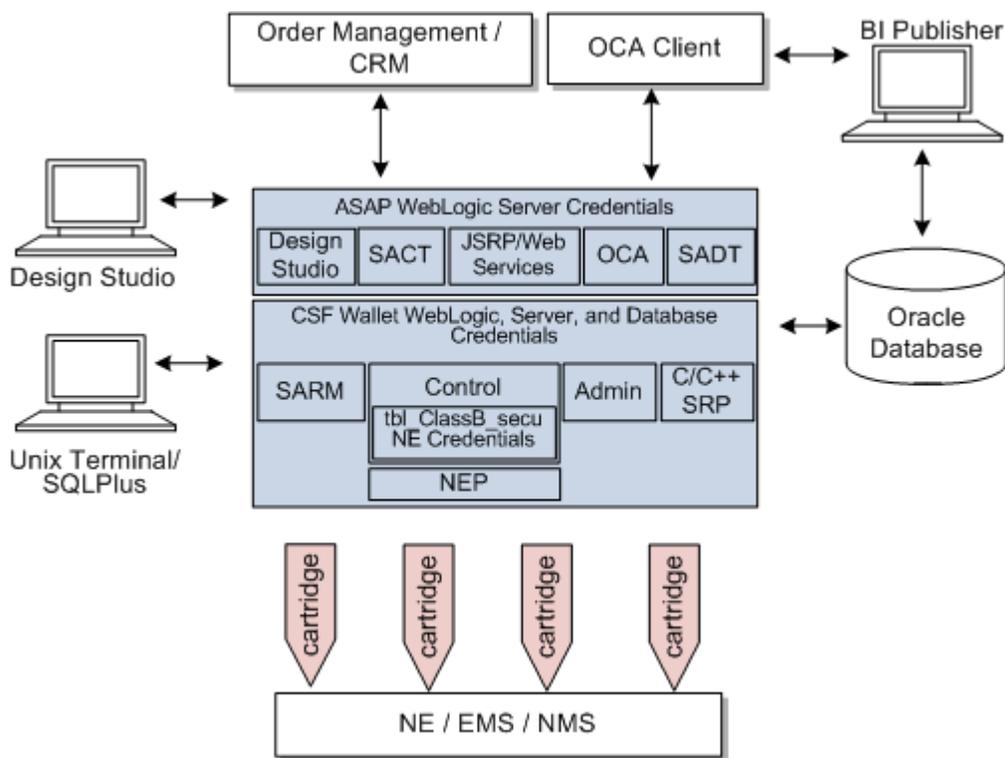
For example, if your business has service subscribers, you must protect their data from other subscribers, but someone in your organization might have to access that data to manage it. You can analyze your workflows to determine who needs access to the data; for example, a system administrator could manage your system components without needing to access the system data.

- **What happens if protections on strategic resources fail?**
In some cases, a fault in your security scheme is nothing more than an inconvenience. In other cases, a fault might cause great damage to you or your customers. Understanding the security ramifications of each resource helps you protect it properly

Overview of ASAP Security

Figure 1-1 shows all the various components that can comprise ASAP, including the components to which it connects.

Figure 1-1 ASAP Components



ASAP security is designed for three essential functions: managing ASAP WebLogic-based users, securing data, and protecting diagnostics files. ASAP provides these security functions in the following locations:

- **ASAP WebLogic server security:** An ASAP WebLogic server instance contains default users, groups, and roles that support the various WebLogic-based ASAP functionality, like the order control application (OCA) client, the Service activation configuration tool (SACT), the service activation deployment tool (SADT) and the Java service request processor (JSRP).
- **ASAP server and database credential security:** The ASAP environment contains a credential store factory (CSF) wallet that stores the ASAP schema user names and passwords, and the ASAP WebLogic server user name and password. These credentials are called class A secure data. Each ASAP server can use this

wallet to obtain these credentials. The CSF wallet provides both secure storage and encryption for these credentials.

- **Network Element (NE) credential security for Network Element Processor (NEP) to NE communication:** The ASAP Control database stores credentials required for NEPs to access NEs. These credentials are called class B secure data. You can use the ASAP security tool to add, change, or delete credential information, and also to enable encryption.
- **ASAP system configuration parameters:** Some ASAP system configuration parameters can have a significant impact on security. Parameters settings, such as diagnostic levels and server security attributes should be configured to ensure data security.

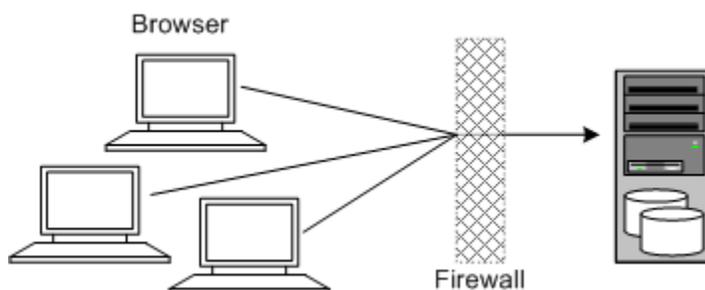
Recommended Deployment Topologies

This section describes recommended deployment topologies for ASAP.

Single-Computer Installation Topology

Figure 1-2 shows a single-computer installation topology.

Figure 1-2 Single-Computer Deployment



In this topology, all the application components and data are kept on a single system, protected from external attacks by a firewall. The firewall can be configured to block known illegal traffic types. There are fewer resources to secure because all the components are on a single system and all the communication is local. Fewer ports have to be opened through the firewall.

Conversely, there are fewer points of attack, and if security is compromised, an attacker would have access to the entire system and data.

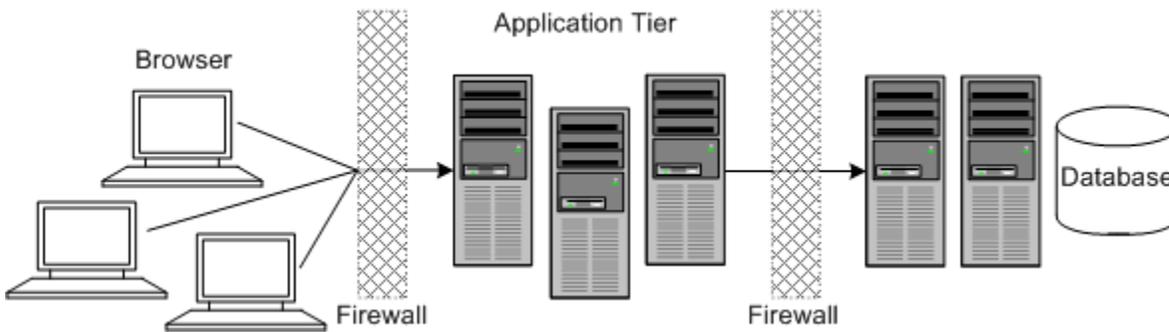
A single-computer installation topology is best suited for test and lab environments:

A single-computer deployment is cost effective for small organizations but does not provide high availability because all components are stored on a single system.

Tiered Deployment

Figure 1-3 shows a tiered installation deployment: a scalable ASAP deployment offering greater security and high availability.

Figure 1-3 Tiered Deployment



In this topology, the application tier is isolated by firewalls from both the Internet and the intranet. The database and servers are protected from potential attacks by two layers of firewall. Both firewalls can be configured to block known illegal traffic types. The two layers of firewall provide intrusion containment. Although there are a greater number of components to secure, and more ports have to be opened to allow secure communication between the tiers, the attack surface is spread out.

ASAP Port Requirements

Table 1-1 lists and describes ASAP ports.

Table 1-1 ASAP Ports

Port	Description
SARM server	The SARM server port for sending and receiving.
Control server	The Control server port for sending and receiving.
NEP server	The NEP server port for sending and receiving.
JNEP listener	The JNEP listener port for sending and receiving.
Admin server	The Admin server port for sending and receiving.
Daemon server	The Daemon server port for sending and receiving.
OCA server	The OCA server port for sending and receiving.
JSRP sending WO	The JSRP port for sending work orders.
JSRP receiving WO	The JSRP port for receiving work orders.
Database connection	The port in the Oracle database connection string. There may be multiple ports if an Oracle Real Application Clusters (RAC) database is used.
WebLogic connection	The port for the ASAP WebLogic server and optional managed server. In addition, if the ASAP WebLogic server is installed on a different machine, you must also open the ports to the Oracle database from there.
Telnet for remote servers	If ASAP is deployed on multiple servers in a distributed configuration, the telnet port for rsh connectivity must be open.

Operating System Security

See the following documents:

- *Guide to the Secure Configuration of Red Hat Enterprise Linux 6*
- *Hardening Tips for the Red Hat Enterprise Linux 6*

Oracle Database Security

For more information about securing an Oracle Database, see *Oracle Database Security Guide* and *Oracle Database Advanced Security Administrator's Guide*.

WebLogic Server Security

For information about securing an ASAP WebLogic server, see *Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server*.

LDAP Security

Oracle recommends that you use Oracle Internet Directory for identity management (for example, users, roles, certificates). You can also use an external LDAP, which you must integrate with ASAP through the ASAP WebLogic server.

For information about setting up Oracle Internet Directory, see *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

For information about setting up an external LDAP, see the LDAP application documentation. For information about security realms and setting up ASAP with an external LDAP, see *ASAP System Administrator's Guide*.

Oracle Security Documentation

ASAP uses other Oracle products, such as Oracle Database and Oracle WebLogic Server. See the following documents, as they apply to ASAP:

- *Oracle Database Security Guide*
- *Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server*
- *Oracle Fusion Middleware Securing Resources Using Roles and Policies for Oracle WebLogic Server*
- *Oracle Application Server Security Guide*
- *Oracle Application Server Administrator's Guide*

2

Performing a Secure ASAP Installation

This chapter presents planning information for your Oracle Communications ASAP system and describes recommended deployment topologies that enhance security.

For more information about installing ASAP, see *ASAP Installation Guide*.

Pre-Installation Configuration

This section explains the pre-requisites to install ASAP with security:

- You must have at least one dedicated UNIX group and one dedicated user account within that group for ASAP.
 - Create a group for ASAP that includes the ASAP user account and the **root** user.
- When creating the ASAP WebLogic Server domain:
 - Make sure that the administration server and the optional managed server SSL ports are used.
 - After you have created the WebLogic Server domain for ASAP, start the WebLogic administration server. Then, use `t3s` to start the managed server:

```
startManagedWebLogic.sh ManagedServer t3s://host_name:SSL_Port
```

Where *ManagedServer* is the name of the WebLogic managed server, *host_name* and *SSL_Port* are the host name and the secure port number of the WebLogic administration server.

- Using the WebLogic Server Administration Console, configure certificate identity and trust store to use TLS protocol. Do not use the default, demonstration certificate that comes with WebLogic Server. See the WebLogic Server documentation for more information.



Note:

Oracle recommends that you configure WebLogic Server SSL ports so that only the TLS protocol is enabled. The SSL v3.0 protocol should be disabled.

Installing ASAP Securely

You can perform a custom installation or a typical installation. Perform a custom installation to avoid installing options you do not need. Unused options and sample files can contain security vulnerabilities if deployed in a production environment.

To deploy and configure ASAP resources securely in the ASAP WebLogic Server domain, do the following:

1. Follow the steps to install ASAP as described in the *ASAP Installation Guide*, selecting the following:

- a. In the WebLogic Configuration screen, enter the secure port of WebLogic administration server.
- b. Select the option **Use SSL**.
The **Enter Keystore File** field is enabled.
- c. In the **Enter Keystore File** field, enter the KeyStore file.

Securely Integrating Oracle Analytics Server with ASAP

Oracle Analytics Server is installed into a WebLogic Server domain. When installing Oracle Analytics Server, configure it to communicate with the SARM and Admin server over an TLS-enabled channel, and disable all unused ports, especially unsecured ports. For information on installing and configuring Oracle Analytics Server, see:

<https://docs.oracle.com/en/middleware/bi/analytics-server/install-config-oas/index.html>

3

Implementing ASAP Security

This chapter explains the security features of Oracle Communications ASAP. See *ASAP System Administrator's Guide* for more information on the ASAP security functionality.

Configuring WebLogic Server Security

ASAP uses the LDAP server included with the WebLogic Server software to manage default ASAP users, groups, roles, and methods. For more information about this embedded LDAP server, see the WebLogic Server documentation.

Configuring Authentication Providers for ASAP

During the ASAP installation process, the ASAP installer creates default ASAP users, groups, roles, and methods in the embedded LDAP authentication provider included with the ASAP WebLogic Server. You can use this authentication provider to configure the default ASAP users, groups, roles, and methods, or add, delete, or modify your own users, groups, roles, and methods.

ASAP also supports external LDAP providers, such as the Oracle Internet Directory.

Managing ASAP WebLogic Server User Security

ASAP supports only the default WebLogic Server **myrealm** security realm. Using security realms other than **myrealm**, disables all ASAP WebLogic-based features.

ASAP administrators can configure user password policies through the WebLogic Administration Console and the password policy utility page. For more information, see *ASAP System Administrator's Guide*.

Configuring ASAP Server and Database Credential Security

Secure data must be stored in a secure location and distributed to authorized users. The ASAP security system governs how secure data is managed and ASAP diagnostics files are secured. This security system includes:

- **Secure Data Storage:** The ASAP security administrator pre-defines the nature and accessibility of secure data for each ASAP server. Class A secure data is stored in the CSF wallet during the initial ASAP installation procedures. For more information, see *ASAP Installation Guide*.
- **Secure Data Encryption:** The CSF wallet encrypts all data contained in it and obtained from it. In addition, the CSF wallet file (**cwallet.sso**) has restricted access permissions. Many ASAP utilities and scripts use the passwords contained in the CSF wallet.

Configuring Security for Network Elements Communication

NE credentials (also called custom secure class B data) used primarily by NEPs to establish network connections to NEs must be stored in a secure location and distributed to authorized users. An ASAP administrator can store NE credentials using ASAP APIs or the command line ASAP security tool (**asap_security_tool**).

The ASAP security tool supports the following features to protect NE credentials:

- **Secure Data Storage:** An administrator can use the ASAP security tool to create NE credentials and store these credentials in a central repository on the Control server. The Control server distributes these credentials to NEPs and Java-enabled NEPs (JNEPs).

ASAP stores NE credentials in the Control server in the **tbl_classB_secu** database table.

- **Secure Data Encryption:** The Control server uses a symmetric secret key encryption method to achieve data confidentiality for custom secure data.
- **Key Distribution:** The Control server acts as a key distribution server, and distributes custom secure data to every ASAP server during provisioning. To acquire custom secure data, ASAP servers use a pre-defined key distribution protocol.

4

Performing a Secure Order Balancer Installation

This chapter presents planning information for securely installing Order Balancer and describes recommended deployment topologies that enhance security.

Pre-Installation Configuration

This section lists the pre-requisites for installing Order Balancer with security:

- You must have at least one dedicated UNIX group and one dedicated user account within that group for Order Balancer. Create a group for Order Balancer that includes the Order Balancer user account and the **root** user.
- When creating the Order Balancer WebLogic server domain:
 - Make sure that the administration server and the optional managed server SSL ports are used.
 - After you have created the WebLogic Server domain for Order Balancer, start the WebLogic administration server.
- Using the WebLogic administration console, configure certificate identity and trust store to use TLS protocol.
- Import trust certificates into the Order Balancer trust store for each ASAP member instance that will be added to Order Balancer. This enables Order Balancer to connect to the ASAP servers securely.
- Do not use the default, demonstration certificate that comes with the WebLogic server. See the WebLogic documentation for more information.
- Disable SSL v3.0 protocol.

Note:

Oracle recommends that you configure WebLogic SSL ports so that only the TLS protocol is enabled.

Installing Order Balancer Securely

To deploy and configure Order Balancer securely in the Order Balancer WebLogic server domain, see "Installing Order Balancer" in the *ASAP System Administrator's Guide*.

[Table 4-1](#) lists the parameters you need to set in the installer input configuration properties file (**sampleConfig.properties**) to securely install Order Balancer.

Table 4-1 Configuration Properties

Parameter	Parameter Value
WLS_PROTOCOL	Set the value to <i>t3s</i> .
WLS_PORT	Set the value to the SSL Server port of Order Balancer WebLogic server.
WLS_SSL_ENABLED	Set the value to <i>true</i> .
WLS_IGNORE_HOSTNAME_VERIFICATION	Set the value to <i>true</i> or <i>false</i> in accordance with the trust certificate configuration in Order Balancer WebLogic server.
WLS_TRUST_KEYSTORE	Set the value to <i>CustomTrust</i> (default demo certificates should not be used).
WLS_CUSTOM_TRUST_KEYSTORE_TYPE	Set the value in accordance with the trust store configuration in Order Balancer WebLogic server.
WLS_CUSTOM_TRUST_KEYSTORE_FILE	Set the value to the path of the Order Balancer trust store file as configured in Order Balancer WebLogic server.

Adding ASAP Instances

The ASAP member instance trust certificates are expected to have already been added to the Order Balancer trust store that is configured for Order Balancer to use for SSL communication. To securely add ASAP member instances to Order Balancer, specify the following parameter when running the **addASAPServer** script:

asapSrvURL: Provide the t3s URL with the SSL port of the ASAP WebLogic server.

Configuring Authentication Providers for Order Balancer

During the Order Balancer installation process, the Order Balancer installer creates default Order Balancer users, groups, roles, and methods in the embedded LDAP authentication provider included with the Order Balancer WebLogic server. You can use this authentication provider to configure the default Order Balancer users, groups, roles, and methods, and add, delete, or modify your own users, groups, roles, and methods.

Managing ASAP WebLogic Server User Security

Order Balancer supports only the default WebLogic server **myrealm** security realm. Order Balancer administrators can configure user password policies through the WebLogic Administration Console. For more information, see "Installing Order Balancer" in the *ASAP System Administrator's Guide*.

5

Security Considerations for Developers

This chapter provides information for developers about how to secure Oracle Communications ASAP work order messages from order management systems to and from the Java service request processor (JSRP) or the ASAP web service implementation, and provides information about developing secure ASAP cartridges.

Securing OSS/J Over JMS Connections

You can secure OSS/J messages over Java messaging service (JMS) connections using WebLogic Server security policies. These policies can be created to secure JMS destinations. These policies enable only authorized ASAP WebLogic Server users to send, receive, and browse JMS messages to and from a destination. For more information about configuring WebLogic Server JMS connection security, see the *Oracle Fusion Middleware Securing Resources Using Roles and Policies for Oracle WebLogic Server*.

Note:

Web service messages can also be sent over JMS.

Securing Web Services Connections

Web services connections can be established over JMS, HTTP, and HTTPS. Oracle recommends using JMS or HTTPS to ensure secure web service work order communication between and order management system and ASAP.

ASAP web service access control security determines the functionality that each user can access. ASAP uses policies and roles configured within the ASAP WebLogic server to secure web service work order messages. Clients that send web service work orders must provide an ASAP WebLogic user ID that is a member of the ASAP WebLogic group **ASAP_WS_USERS_GROUP**. The **web.xml** file defines the security role **ASAP_WS_USERS** and **weblogic.xml** file defines the security principal name as **ASAP_WS_USERS_GROUP**.

Here is a sample security header in a SOAP request:

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">
<env:Header>
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-secext-1.0.xsd" env:mustUnderstand="1">
        <wsse:UsernameToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/
oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="unt_AF6po7ocfkMUDzde">
            <wsse:Username>username</wsse:Username>
            <wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/
oasis-200401-wss-username-token-profile-1.0#PasswordText">password</wsse:Password>
        </wsse:UsernameToken>
    </wsse:Security>
```

```
</env:Header>
<env:Body>
  <m:order_type xmlns:m="http://xmlns.oracle.com/communications/activation/
asap/webservices">
    OSS/J_work_order

    </m:order_type>
  </env:Body>
</env:Envelope>
```

Where:

- *username*: is the user name for the web service user-defined in the ASAP WebLogic Server instance.
- *password*: is the password for the web service user-defined in the ASAP WebLogic Server instance.
- *order_type*: is the type of work order sent.
- *OSS/J_work_order*: is the OSS/J work order information. When you add the work order information, do not include the XML header information (**<?xml version="1.0" encoding="UTF-8"?>**) since this has already been provided in the sample. Also, ensure that there are no namespace conflicts.

Cartridge Development

When developing an ASAP cartridge, store NE credentials in the Control server secure class B table. You must configure ASAP Java methods to access these credentials from the Control server when you establish connections from the NEP or JNEP to each NE. For more information, see *ASAP Cartridge Development Guide*.

A

ASAP Secure Deployment Checklist

The following security checklist lists guidelines to help you secure Oracle Communications ASAP and its components.

Secure Deployment Checklist

- Install only the components you require.
- Lock and expire default user accounts.
- Enforce strong password management.
- Restrict, control, and revisit user privileges:
 - Grant only the necessary privileges to each user.
 - Revoke unnecessary privileges from the PUBLIC user group.
 - Restrict permissions on run-time facilities
- Enforce the use of access controls.
- Require clients to authenticate.
- Restrict network access by doing the following:
 - Use firewalls.
 - Never leave an unnecessary hole in a firewall.
 - Password-protect the Oracle listener against remote access.
 - Monitor listener activity.
 - Monitor who accesses your systems.
 - Restrict system access by IP addresses.
 - Encrypt network traffic.
 - Harden the operating system by installing it in a secure location where it would be difficult for a hacker to access, by ensuring that all null passwords have been changed, and by disabling remote root login.
- Apply all security patches and workarounds.
- Encrypt sensitive information.
- Contact Oracle Security Products if you discover a vulnerability in any Oracle product.