Oracle® Fusion Middleware

Understanding Domain Configuration for Oracle WebLogic Server



26 (26.1.0.0.0)
G56921-01
November 2026



Oracle Fusion Middleware Understanding Domain Configuration for Oracle WebLogic Server, 26 (26.1.0.0.0)

G56921-01

Copyright © 2007, 2026, Oracle and/or its affiliates.

Primary Author: Oracle Corporation

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, software documentation, data (as defined in the Federal Acquisition Regulation), 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," "commercial computer software documentation," or "limited rights data" 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, MySQL, and NetSuite 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.

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.

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Contents

Preface

Audience i
Documentation Accessibility i
Diversity and Inclusion i
Related Documentation i
Conventions ii

1 Understanding Oracle WebLogic Server Domains

What Is a Domain? 1
Organizing Domains 1
Contents of a Domain 3
- Administration Server 3
- What Happens if the Administration Server Fails? 4
- Managed Servers and Managed Server Clusters 4
- Resources and Services 4

Domain Configuration Restrictions 5
Domain and Server Name Restrictions 6
Development, Production, and Secured Production Modes 6

2 Domain Configuration Files

Overview of Domain Configuration Files 1
- Editing Configuration Documents 2
- Security Credentials in Configuration Files 2
- Configuration File Archiving 3

Domain Directory Contents 3
- WSM-00001 to WSM-09029 3
- autodeploy 214
- bin 214
- config 214
- config/configCache 214
- config/diagnostics 215
- config/jdbc 215

Copyright © 2007, 2026, Oracle and/or its affiliates.

config/jms 215
config/nosql 215
config/lib 215
config/nodemanager 215
config/security 215
configArchive 216
init-info 216
lib 216
pending 216
security 216
servers 216
servers/server-name 217
servers/server-name/cache 217
servers/server-name/cache/EJBCompilerCache 217
servers/server-name/data 217
servers/server-name/data/ldap 217
servers/server-name/data/store 217
servers/server-name/logs 217
servers/server-name/logs/diagnostic_images 217
servers/server-name/logs/jmsServers 218
servers/server-name/security 218
servers/server-name/tmp 218
tmp 218
A Server's Root Directory 218
Specifying a Server Root Directory 219
Server Root Directory for an Administration Server 219
Server Root Directory for a Managed Server Started with Node Manager 219
Server Root Directory for a Managed Server Not Started with Node Manager 220

3 Managing Configuration Changes

Overview of Change Management 1
Changes Requiring Server Restart 2
Configuration Change Tools 2
Configuration Auditing 3
Change Management in the Remote Console 3
Configuration Change Management Process 3
Configuration Locks 6
Resolving Change Conflicts 7
Configuration Management State Diagram 7
Restricting Configuration Changes 8
Configuration Overriding 8

Copyright © 2007, 2026, Oracle and/or its affiliates.

About Situational Configuration Files, Names and Locations 9
Overriding the Default File Location 11
File Format 12
File Expiration 16
Loading Situational Configurations 17
Processing Multiple Fragments 18
Using Wildcards 18
Monitoring Situational Configuration Changes 20
Using Named Concurrent Edit Sessions 20

4 Server Templates

What are Server Templates? 1
Why Do You Use Server Templates? 1
Using Server Templates 2
Overriding Attributes 2
Using Macros 4
Server Templates Example 4

Copyright © 2007, 2026, Oracle and/or its affiliates.

Preface

This documentation describes the Oracle WebLogic Server domains and how the domains are configured.

Audience

This document is written mainly for Jakarta EE system architects, application developers, and system administrators who are developing or deploying Web-based applications on one or more Oracle WebLogic Server domains.

It is assumed that the reader is familiar with Jakarta EE, basic concepts of XML, and general networking and application management concepts.

The topics in this document are relevant during the design and development phases of a software project. This document does not address production phase administration, monitoring, or performance tuning topics.

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.

Related Documentation

For information about system administration tasks and the various tools you can use to perform them, see:

- System Administration in *Understanding Oracle WebLogic Server*

Copyright © 2007, 2026, Oracle and/or its affiliates.

- Developing Jakarta Management Applications for Oracle WebLogic Server
- Oracle WebLogic Server MBean Reference
- Monitoring Oracle WebLogic Server with SNMP

For more information about tools you can use to create and configure Oracle WebLogic Server domains, see:

- Creating WebLogic Domains Using the Configuration Wizard
- Understanding the WebLogic Scripting Tool
- Developing Custom Management Utilities Using JMX for Oracle WebLogic Server
- Command Reference for Oracle WebLogic Server
- Oracle WebLogic Remote Console Online Help

Samples and Tutorials

Oracle provides a variety of code examples and tutorials that show WebLogic Server configuration and API use, and provide practical instructions on how to perform key development tasks. For more information, see Sample Applications and Code Examples in *Understanding Oracle WebLogic Server*.

New and Changed WebLogic Server Features

For a comprehensive listing of the new Oracle WebLogic Server features introduced in this release, see *What's New in Oracle WebLogic Server*.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Copyright © 2007, 2026, Oracle and/or its affiliates.

1

Understanding Oracle WebLogic Server Domains

Learn about Oracle WebLogic Server domains and their contents, which include an Administration Server and usually one or more Managed Servers.

The following topics provide an overview of WebLogic Server domain, its contents, and certain restrictions associated to the domain configuration:

What Is a Domain?

An Oracle WebLogic Server administration **domain** is a logically related group of Oracle WebLogic Server resources.

Domains include a special Oracle WebLogic Server instance called the **Administration Server**, which is the central point from which you configure and manage all resources in the domain. Usually, you configure a domain to include additional Oracle WebLogic Server instances called **Managed Servers**. You deploy Web applications, EJBs, Web services, and other resources onto the Managed Servers and use the Administration Server for configuration and management purposes only.

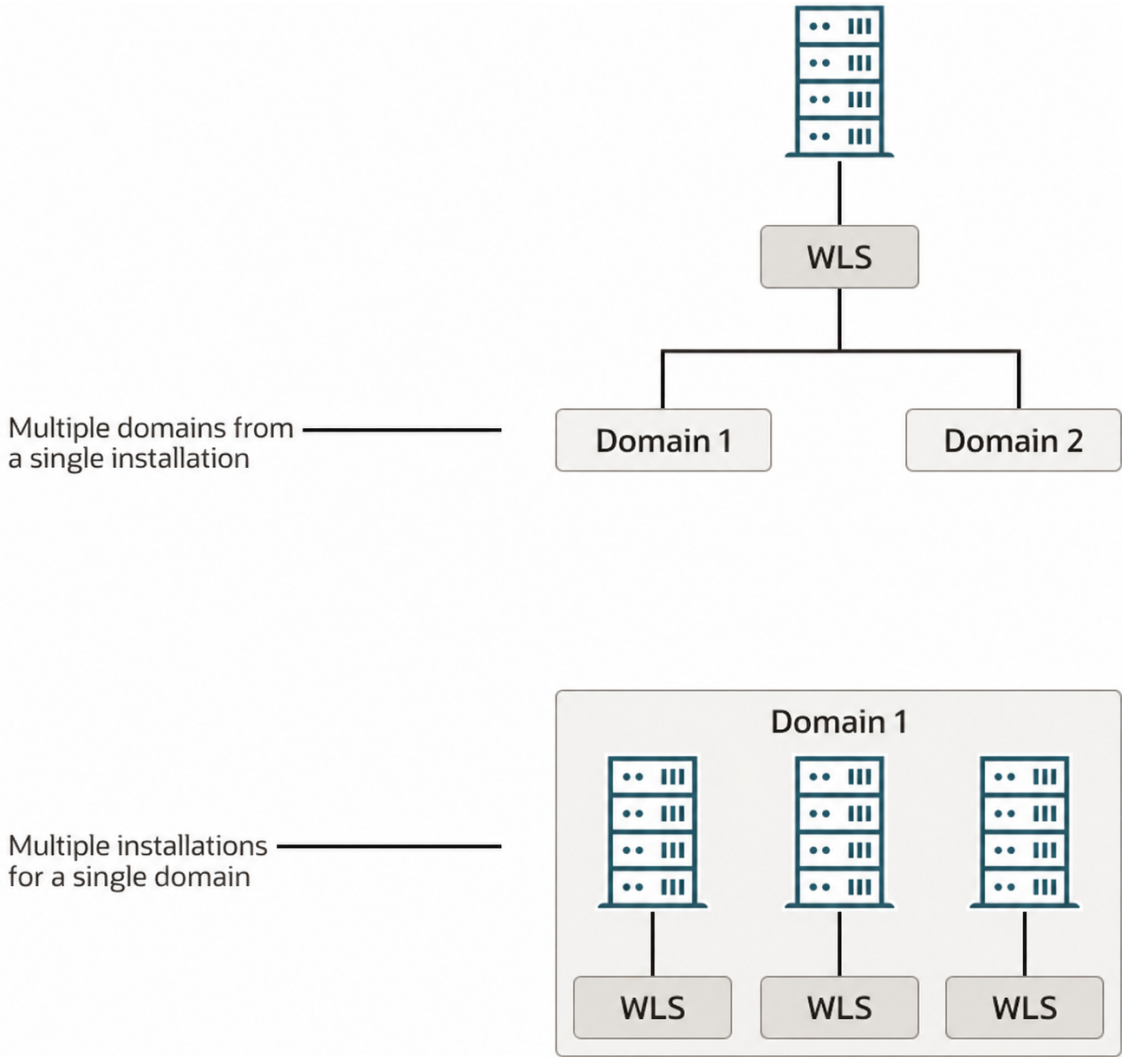
Organizing Domains

You can use a single Oracle WebLogic Server installation to create and run multiple domains, or you can use multiple installations to run a single domain.

Figure 1-1 shows multiple domains from a single installation and multiple installations for a single domain.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Figure 1-1 Oracle WebLogic Server Installations and Domains



How you organize your Oracle WebLogic Server installations into domains depends on your business needs. You can define multiple domains based on different system administrators' responsibilities, application boundaries, or geographical locations of the machines on which servers run. Conversely, you might decide to use a single domain to centralize all Oracle WebLogic Server administration activities.

Depending on your particular business needs and system administration practices, you might decide to organize your domains based on criteria such as:

- Logical divisions of applications. For example, you might have one domain devoted to end-user functions such as shopping carts and another domain devoted to back-end accounting applications.
- Physical location. You might establish separate domains for different locations or branches of your business. Each physical location requires its own Oracle WebLogic Server installation. A domain can be made up from multiple domain directories spanning multiple physical hosts. They all just need to be configured for the same domain.
- Size. You might find that domains organized in small units can be managed more efficiently, perhaps by different system administrators. Contrarily, you might find that

Copyright © 2007, 2026, Oracle and/or its affiliates.

maintaining a single domain or a small number of domains makes it easier to maintain a consistent configuration.

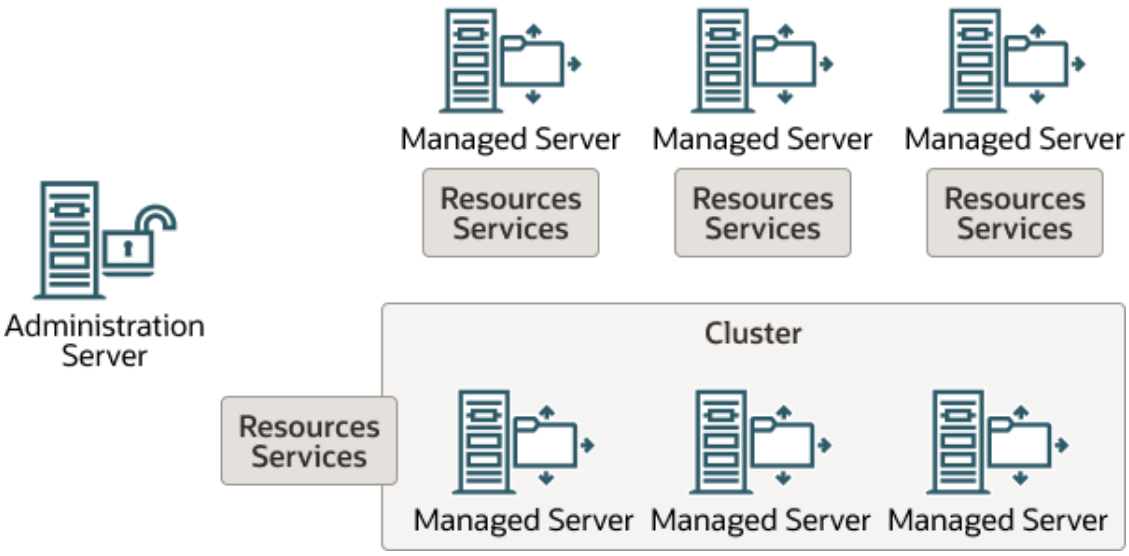
You can create a simple domain that consists of a single server instance. This single instance acts as an Administration Server and hosts the applications that you are developing. The wl_server domain that you can install with Oracle WebLogic Server is an example of this type of domain.

Contents of a Domain

An Oracle WebLogic Server domain might consist of an Administration Server, Managed Servers, and the resources and services that Managed Servers and deployed applications require.

Figure 1-2 shows a production environment that contains an Administration Server, three stand-alone Managed Servers, and a cluster of three Managed Servers.

Figure 1-2 Content of a Domain



Although the scope and purpose of a domain can vary significantly, most Oracle WebLogic Server domains contain the components described in this section.

Administration Server

The Administration Server operates as the central control entity for the configuration of the entire domain. It maintains the domain's configuration documents and distributes changes in the configuration documents to Managed Servers. You can also use the Administration Server as a central location from which to monitor all resources in a domain.

To interact with the Administration Server, you can use any of the administration tools listed in Summary of System Administration Tools and APIs in *Understanding Oracle WebLogic Server*. See System Administration in *Understanding Oracle WebLogic Server* for information about modifying the domain's configuration.

Each Oracle WebLogic Server domain must have one server instance that acts as the Administration Server.

Copyright © 2007, 2026, Oracle and/or its affiliates.

For more information about the Administration Server and its role in the Oracle WebLogic Server JMX management system, see System Administration in *Understanding Oracle WebLogic Server*.

What Happens if the Administration Server Fails?

The failure of an Administration Server does not affect the operation of Managed Servers in the domain but it does prevent you from changing the domain's configuration. If an Administration Server fails because of a hardware or software failure on its host machine, other server instances on the same machine may be similarly affected. However, the failure of an Administration Server itself does not interrupt the operation of Managed Servers in the domain.

If an Administration Server for a domain becomes unavailable while the server instances it manages—clustered or otherwise—are up and running, those Managed Servers continue to run. Periodically, the Managed Servers attempt to reconnect to the Administration Server. If the domain contains clustered server instances, the load balancing and failover capabilities supported by the domain configuration remain available, even if the Administration Server fails.

You can start a Managed Server even if the Administration Server is not running. In this case, the Managed Server uses a local copy of the domain's configuration files for its starting configuration and then periodically attempts to connect with the Administration Server. When it does connect, it synchronizes its configuration state with that of the Administration Server.

For information on starting a Managed Server without a running Administration Server, see Managed Server Independence Mode in *Administering Server Startup and Shutdown for Oracle WebLogic Server*. For information about re-starting an Administration Server, see Avoiding and Recovering From Server Failure in *Administering Server Startup and Shutdown for Oracle WebLogic Server*.

Managed Servers and Managed Server Clusters

Managed Servers host business applications, application components, Web services, and their associated resources. To optimize performance, Managed Servers maintain a read-only copy of the domain's configuration document. When a Managed Server starts up, it connects to the domain's Administration Server to synchronize its configuration document with the document that the Administration Server maintains.

For production environments that require increased application performance, throughput, or high availability, you can configure two or more Managed Servers to operate as a **cluster**. A cluster is a collection of multiple Oracle WebLogic Server instances running simultaneously and working together to provide increased scalability and reliability. In a cluster, most resources and services are deployed identically to each Managed Server (as opposed to a single Managed Server), enabling failover and load balancing. A single domain can contain multiple Oracle WebLogic Server clusters, as well as multiple Managed Servers that are not configured as clusters. The key difference between clustered and non-clustered Managed Servers is support for failover and load balancing. These features are available only in a cluster of Managed Servers. For more information about the benefits and capabilities of an Oracle WebLogic Server cluster, see Understanding WebLogic Server Clustering in *Administering Clusters for Oracle WebLogic Server*.

Resources and Services

In addition to the Administration Server and Managed Servers, a domain also contains the resources and services that Managed Servers and deployed applications require.

Managed Servers can use the following resources:

Copyright © 2007, 2026, Oracle and/or its affiliates.

- Machine definitions that identify a particular, physical piece of hardware. A machine definition is used to associate a computer with the Managed Servers it hosts. This information is used by Node Manager in restarting a failed Managed Server, and by a clustered Managed Server in selecting the best location for storing replicated session data. For more information about Node Manager, see Node Manager Overview in the *Administering Node Manager for Oracle WebLogic Server*.
- Network channels that define default ports, protocols, and protocol settings that a Managed Server uses to communicate with clients. After creating a network channel, you can assign it to any number of Managed Servers and clusters in the domain. See Configuring Network Resources in *Administering Server Environments for Oracle WebLogic Server*.
- Virtual hosting, which defines a set of host names to which Oracle WebLogic Server instances (servers) or clusters respond. When you use virtual hosting, you use DNS to specify one or more host names that map to the IP address of a server or cluster. You also specify which Web applications are served by each virtual host.

Applications can use the following resources and services:

- Security providers, which are modular components that handle specific aspects of security, such as authentication and authorization.
- Resource adapters, which are system libraries specific to Enterprise Information Systems (EIS) and provide connectivity to an EIS.
- Diagnostics and monitoring services.
- JDBC data sources, which enable applications to connect to databases.
- Mail sessions.
- XML entity caches and registry of XML parsers and transformer factories.
- Messaging services such as JMS servers and store-and-forward services.
- Persistent store, which is a physical repository for storing data, such as persistent JMS messages. It can be either a JDBC-accessible database or a disk-based file.
- Startup classes, which are Java programs that you create to provide custom, system-wide services for your applications.
- Work Managers, which determine how an application prioritizes the execution of its work based on rules you define and by monitoring actual run-time performance. You can create Work Mangers for entire Oracle WebLogic Server domains or for specific application components.
- Work Contexts, which enable applications to pass properties to a remote context without including the properties in a remote call.

Domain Configuration Restrictions

In designing your domain configuration, note the restrictions mentioned.

- Each domain requires its own Administration Server for performing management activities. When you use the WebLogic Remote Console to perform management and monitoring tasks, you can switch back and forth between domains, but in doing so, you are connecting to different Administration Servers.
- All Managed Servers in a cluster must reside in the same domain. You cannot split a cluster over multiple domains. See Relationship Between Clusters and Domains.

Copyright © 2007, 2026, Oracle and/or its affiliates.

- All Managed Servers in a domain must run the same WebLogic Server release. During a supported rolling patching operation, Managed Servers can temporarily run at different patch levels while individual instances are patched and restarted. Complete the operation promptly and restore a consistent patch level; do not retain mixed patch levels as a steady-state configuration. Follow the patch README for applicability and restart requirements. The Administration Server may run either the same version as the Managed Servers in the domain, or a later patch set.

  Configuration changes that require a server restart can temporarily leave servers using different effective runtime settings during a rolling restart. A server continues using the applicable previous settings until it is restarted. These temporary patch or configuration differences do not authorize rolling upgrades between distinct WebLogic Server releases. For example, the patching allowance does not permit a rolling upgrade from WebLogic Server 12.2.1.4, 14.1.1, or 14.1.2 to WebLogic Server 26.1 across the `javax` and `jakarta` API boundary.
- Server instances cannot have the same name as the domain.

You cannot share a configured resource or subsystem between domains. For example, if you create a JDBC data source in one domain, you cannot use it with a Managed Server or cluster in another domain. Instead, you must create a similar data source in the second domain. Furthermore, two or more system resources cannot have the same name.

Domain and Server Name Restrictions

When naming a domain or a server instance, note the restrictions and considerations mentioned.

- Use alphanumeric names for domain and server instances.
- Apart from the alphanumeric characters, a valid domain or server name can include only the following characters:
  - Underscore (_)
  - Hyphen (-)
  - Period (.)
- Use a unique name for each server instance. Within a domain, all configuration objects, including server instances, machines, clusters, JDBC connection pools, virtual hosts, and other resource types, must have unique names and must not use the same name as the domain.
- Server names are for identification purposes only. Server names are not used as part of the URL for applications deployed on the server instance. The server name displays in the Remote Console. If using WebLogic Server command-line utilities, you use the server name to identify the server instance.
- Once you have created a server instance, you cannot change its name. To use a new name, clone the server instance and provide a new name for the clone.

Development, Production, and Secured Production Modes

You can configure a WebLogic domain to run in one of three modes: development mode, production mode, or secured production mode.

The domain mode determines default settings regarding security and logging. In development mode, the security configuration is more relaxed. You can start the Administration Server using a boot identity file or deploy an application using the `autodeploy` directory. In production mode,

Copyright © 2007, 2026, Oracle and/or its affiliates.

the security configuration is more stringent, such as requiring a user name and password to deploy applications and start the Administration Server. In secured production mode, the default authorization and role mapping policies are more restrictive, and the security configurations are set to more secure default values.

As of WebLogic Server 14.1.2.0.0, when you enable production mode, it automatically enables the stricter settings of secured production mode. If you truly want to implement the more moderate default settings of production mode, you must explicitly disable secured production mode.

There are also several differences between the default settings in development mode, production mode, and secured production mode, including:

- The number of threads in an execute queue
- Log settings, including the maximum number of files saved during log rotation, the minimum size of the log file that triggers log rotation, and whether logs are rotated at startup
- The default for server lifecycle operations timeout
- SNMP security level
- Servlet reload check periods

For details about how the domain mode you select determines the default security configuration for your domain, see How Domain Mode Affects the Default Security Configuration in *Securing a Production Environment for Oracle WebLogic Server*. This topic explains how the default settings for SSL, the administrative and listen ports, auditing, logging, deployment of internal applications, the domain configuration lock, and other configuration settings differ depending on the domain mode that is enabled.

> **Note**
>
> Oracle recommends that you do not enable the Web Services Test Client in production mode. See Using the Web Services Test Client in *Administering Web Services*.

Modifying Domain Modes

You can configure the domain mode at the time you create the domain, or you can also change the domain mode any time later.

However, you cannot configure domains created prior to 12.2.1.3 to run in secured production mode; only domains running in 12.2.1.3 and later can be configured for secured production mode.

Use one of the following tools to set the domain mode:

- WebLogic Remote Console - see Change the Domain Mode in the *Oracle WebLogic Remote Console Online Help*
- WLST Offline - see the setOption WLST offline command in *WLST Command Reference for Oracle WebLogic Server*
- WLST Online - see Using WLST Online to Update an Existing WebLogic Domain in *Understanding the WebLogic Scripting Tool*
- Configuration Wizard - see Creating a WebLogic Domain in *Creating WebLogic Domains Using the Configuration Wizard*

Copyright © 2007, 2026, Oracle and/or its affiliates.

- Pack/Unpack - see the `server_start_mode` parameter in The Pack Command in *Creating Templates and Domains Using the Pack and Unpack Commands*

When you change a domain from development mode to production mode:

- The domain start scripts (and the value of the `-Xverify` flag) do not change.
- The `boot.properties` file remains in use.

To enhance the security of your existing production domains, do the following:

1. To change the value of the `-Xverify` flag from `none` to `all`, modify the domain start scripts. This change enables bytecode verification. For more information about bytecode verification, see *Java Language Security and Bytecode Verification* in the *Java Security Overview* at https://docs.oracle.com/en/java/javase/17/security/java-security-overview1.html#GUID-2EF91196-D468-4D0F-8FDC-DA2BEA165D10.
2. Restart the Administration Server and each Managed Server in your domain. In the command to restart each server instance, include the `-Dweblogic.system.RemoveBootIdentity=true` argument, which removes the boot identity file. The boot identity file only must be removed on the first restart after changing the configuration to production mode. You can use either of the following methods:
   - Open a separate command shell and include this argument in the `weblogic.Server` startup command for each server instance.
   - Define the `JAVA_OPTIONS` variable to include `-Dweblogic.system.RemoveBootIdentity=true` and then invoke the start script of the server.

Copyright © 2007, 2026, Oracle and/or its affiliates.

2

Domain Configuration Files

The domain configuration files are XML documents that Oracle WebLogic Server uses to persist the configuration of a domain.
This chapter includes the following sections:

Overview of Domain Configuration Files

Each domain describes its configuration in an XML document that is located in the configuration directory of the domain. At run time, each Oracle WebLogic Server instance in a given domain creates an in-memory representation of the configuration described in this document.

> **Note**
>
> The domain directory must have both Write and Read privileges, for the domain to function properly, even if no changes are made to the configuration after it is created. These privileges are required because WebLogic Server performs its own internal deployments, and configuration files may be rewritten when the server is restarted.
>
> Do not add non-configuration files in the `config` directory or subdirectories. Non-configuration files include log (.log) and lock (.lck) files. Administration Server replicates the `config` directory in all Managed Server instances. Storing non-configuration files in the `config` directory can cause performance issues in the domain.

The central configuration file for a domain is *`DOMAIN_NAME`*`/config/config.xml`. This file specifies the name of the domain and the configuration of each server instance, cluster, resource, and service in the domain. The file includes references to additional XML files that are stored in subdirectories of the *`DOMAIN_NAME`*`/config` directory. These included files are used to describe major subsystems of Oracle WebLogic Server.

A NoSQL resource has two domain-configuration components: the `NoSQLSystemResourceMBean` entry in `config.xml`, which identifies the resource, its external descriptor, and its targets; and the external NoSQL descriptor under `DOMAIN_HOME/config/nosql`, which contains the provider, database type, JNDI name, default-selection flag, and provider properties. Application deployment descriptors contain local resource-reference declarations and WebLogic JNDI mappings; they do not define the global system resource. Copying an external NoSQL descriptor into the domain does not by itself register or target a resource. Global NoSQL system-resource definitions cannot be packaged as application archive content.

As a performance optimization, Oracle WebLogic Server does not store most of its default values in the domain's configuration files. Sometimes, this optimization prevents XML elements from being written to the configuration files. For example, if you never modify the default logging severity level for a domain while the domain is active, the `config.xml` file does not contain an XML element for the domain's logging configuration.

Copyright © 2007, 2026, Oracle and/or its affiliates.

As an additional performance optimization, each Managed Server maintains a copy of the domain's configuration files. This copy is read-only and can be updated only as part of a change management process (see Managing Configuration Changes).

Editing Configuration Documents

In most circumstances, you should not use a text editor or other non-Oracle tools to modify a domain's configuration document. Instead, use the WebLogic Remote Console, WebLogic Scripting Tool (WLST), or one of the other tools described in System Administration in *Understanding Oracle WebLogic Server*.

However, because the Oracle WebLogic Server configuration document is an XML file that conforms to a schema, it is possible to modify them using XSLT or an XML parser application such as Apache Xerces or JDOM. Be sure to test any scripts that you create thoroughly and always make a backup copy of each configuration file before you make any changes to it.

The schemas that define a domain's configuration document are in the following locations:

- `http://xmlns.oracle.com/weblogic/domain/1.0/domain.xsd`
- `http://xmlns.oracle.com/weblogic/security/1.0/security.xsd`
- `http://xmlns.oracle.com/weblogic/weblogic-diagnostics/2.0/weblogic-diagnostics.xsd`
- In JAR files under *`WL_HOME`*`/server/lib/schema`, where *`WL_HOME`* is the directory in which you install Oracle WebLogic Server. Within this directory:
- The `domain.xsd` document is represented in the `weblogic-domain-binding.jar` under the pathname `META-INF/schemas/schema-0.xsd`.
- The `security.xsd` document is represented in the `weblogic-domain-binding.jar` under the pathname `META-INF/schemas/schema-1.xsd`.
- The `weblogic-diagnostics.xsd` document is represented in the `diagnostics-binding.jar` under the pathname `META-INF/schemas/schema-0.xsd`.

> ⚠ **Caution**
>
> Do not edit configuration files for a domain that is currently running. Because Oracle WebLogic Server rewrites the files periodically, your changes will be lost. Depending on your platform, you also could cause Oracle WebLogic Server failures.

Security Credentials in Configuration Files

Security credentials for domain security and the embedded LDAP server are stored in the `config.xml` file in encrypted form. If you create your `config.xml` file with a text editor or other non-Oracle tool, you need to locate these credentials, encrypt them, and copy the encrypted credential into your `config.xml` file.

For information about Oracle WebLogic Server's encryption utility, see encrypt in the *Command Reference for Oracle WebLogic Server*. After you encrypt the credentials, include the encrypted values in your `config.xml` file in elements as shown in Example 2-1:

Copyright © 2007, 2026, Oracle and/or its affiliates.

Example 2-1 Configuring Encrypted Credentials

```
<security-configuration>
   <credential-encrypted>{AES256}encypted-value-here</credential-encrypted>
</security-configuration>
<embedded-ldap>
   <credential-encrypted>{AES256}encypted-value-here</credential-encrypted>
</embedded-ldap>
```

Configuration File Archiving

You can configure Oracle WebLogic Server to make backup copies of the configuration files. This facilitates recovery in cases where configuration changes need to be reversed or the unlikely case that configuration files become corrupted. When the Administration Server starts up, it saves a JAR file named `config-booted.jar` that contains the configuration files. When you make changes to the configuration files, the old files are saved in the `configArchive` directory under the domain directory, in a JAR file with a sequentially-numbered name like `config-1.jar`.

To configure configuration backups using WLST, set the `DomainMBean.ConfigBackupEnabled` attribute to `true` and set `ArchiveConfigurationCount` to the number of configuration archive files to retain, as shown in Example 2-2.

Example 2-2 Configuring Archive Files

```
connect()
edit()
startEdit()
cmo.setArchiveConfigurationCount(5)
cmo.setConfigBackupEnabled(true)
activate()
```

Domain Directory Contents

By default, Oracle WebLogic Server creates domain directories under Oracle Middleware *ORACLE_HOME*`/user_projects/domains` directory. As a best practice, Oracle recommends that you create your domain directories elsewhere.

Individual applications in a domain might create additional files and directories in the domain directory.

The following section describes the contents of the domain directory and its subfolders. Here *domain-name*, *deployment-name*, and *server-name* represent names that you define when you create a domain.

WSM-00001 to WSM-09029

WSM-00001
A JAXB context for path "{0}" cannot be created due to underlying error "{1}".

Category:
Other

Cause:
The error could have been caused by creating the JAXB2.0 marshaller/unmarshaller.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Contact Oracle Support Services.

WSM-00002
A class of type {0} cannot be marshaled due to underlying error "{1}".

Category:
Other

Cause:
Error occurred in JAXB marshalling (1.e converting java object to xml.)

Action:
Contact Oracle Support Services or refer to http://java.net/jaxb.

WSM-00003
An element of type {0} cannot be unmarshalled due to underlying error "{1}".

Category:
Other

Cause:
Error occurred while doing JAXB unmarshall i.e converting XML to Java.

Action:
Contact Oracle Support Services.

WSM-00004
WS-Security Exception : {0}

Category:
Security

Cause:
The system encountered a generic failure in security.

Action:
Contact Oracle Support Services.

WSM-00005
Error in sending the request.

Category:
Security

Cause:
Failure occurred while trying to send the request message, possibly due to a failure in security code.

Action:
Retry the operation for a maximum of 3 times. If the problem persists, contact Oracle Support Services.

WSM-00006
Error in receiving the request: {0}.

Category:
Security

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
Failure occurred while processing the request message, possibly due to a failure in security checks.

Action:
Refer to the policy for the expected nature of the request message and retry the operation.

WSM-00007
JPS exception

Category:
Security

Cause:
The error was most likely due to an invalid JPS configuration.

Action:
Correct the JPS configuration and retry the operation.

WSM-00008
Login Exception: {0}.

Category:
Security

Cause:
Login Exception at OPSS.

Action:
Resend valid credentials.

WSM-00009
The password policy does not match. Expected: {0}, Received:{1}.

Category:
Security

Cause:
The expected and actual password types did not match.

Action:
Refer to the policy to determine the allowed password type value.

WSM-00010
Message rejected as the nonce element in the WS-Security header is missing.

Category:
Security

Cause:
Nonce was required according to policy requirements, but was not found.

Action:
Resend the request with valid value of nonce.

WSM-00011
The wsu:Created element is required.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Security

Cause:
The Created element was required, but was not found.

Action:
Resend the request with valid value of the Created element with the UTC timestamp of the instance in which the request was created.

WSM-00012
The password is ignored, as it is not required by the policy.

Category:
Security

Cause:
The password was sent in the <UsernameToken>, when it was not required.

Action:
The password type prescribed by the policy is None, so password should not be sent.

WSM-00015
The user name is missing.

Category:
Security

Cause:
Username was expected but was not found.

Action:
Either the username element or the username inside the username element is missing. Resend the request with a valid username.

WSM-00016
The username/password credentials or certificates {0} are missing.

Category:
Security

Cause:
It is possible that username/password or certificate is missing.

Action:
Resend valid credentials.

WSM-00017
The <bindings> element for {0}:{1} is missing.

Category:
Configuration

Cause:
It is likely that the bindings element is missing inside policy.

Action:
Re-create the policy with valid bindings.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-00018
There is more than one security header with the same role {0}.

Category:
Security

Cause:
More than one security header was found with the same role associated.

Action:
Refer to the WS-Security 1.0 or 1.1 specifications. Do not send more than one security header having the same role.

WSM-00019
The version of SOAP used is not supported: {0}.

Category:
Requests/Responses

Cause:
An envelope was obtained that conforms to an unsupported version of SOAP.

Action:
Use a supported version. SOAP 1.1 and 1.2 are supported.

WSM-00020
Error sending the response.

Category:
Other

Cause:
A failure occurred while building the response.

Action:
Retry a maximum of three times. If the retry attempts fail, contact Oracle Support Services.

WSM-00021
Error receiving the response.

Category:
Security

Cause:
A failure occurred while processing the response, most likely due to a failure in the security check.

Action:
Retry sending the response to the client.

WSM-00022
Error sending a fault.

Category:
Other

Cause:
A failure occurred while sending the fault.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Retry for a maximum of three times. If the retry attempts fail, contact Oracle Support Services.

WSM-00023
Error receiving a fault.

Category:
Security

Cause:
A failure occurred while processing the fault, most likely due to a failure in the security check.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

WSM-00024
The SAML token is missing from the security header. Ensure that there is a SAML token policy attached on the client side. Tokens found in the security header are :- {0}.

Category:
Security

Cause:
The SAML assertion that was expected inside the security header was not found.

Action:
Insert valid SAML assertions and resend the request.

WSM-00025
SAML token verification failure.

Category:
Security

Cause:
SAML token verification failed.

Action:
Check the validity period of the SAML assertion using Conditions, or determine whether the assertion must be signed. Ensure that the SAML token conforms to the requirements of the SAML 1.0 specification.

WSM-00026
The SAML token cannot be added to the security header.

Category:
Other

Cause:
A failure occurred while adding the SAML token to the security header.

Action:
Check the log file for a possible cause.

WSM-00027
The configuration parameter {0} contains an invalid value [{1}].

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Configuration

Cause:
The configuration settings were invalid.

Action:
Check the configuration and retry the operation.

WSM-00028
Failure in getting user credentials from client.

Category:
Configuration

Cause:
Failure occurred while extracting user credentials from the client side.

Action:
Check Keystore/Username and the Password/CSF configuration.

WSM-00029
The algorithms used to encrypt the data do not match those specified in the policy. : Expected : {0}, Actual : {1}.

Category:
Security

Cause:
The expected and actual data encryption algorithms did not match.

Action:
Check the policy to determine the permitted values for the data encryption algorithm.

WSM-00030
The encryption method key wrap algorithms do not match : Expected : {0}, Actual : {1}.

Category:
Security

Cause:
The expected and actual key wrap encryption algorithms did not match.

Action:
Check the policy to determine the permitted values for the key wrap encryption algorithm. In addition, refer to WS-Security Policy 1.1 for a list of allowed values.

WSM-00031
The digest algorithms do not match.

Category:
Security

Cause:
The actual digest algorithms for the signature did not match the expected algorithms.

Action:
Check the policy to determine the permitted values for the signature digest algorithms.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-00033
The encrypted message elements or parts do not comply with the policy. The following headers/elements (<name space: local name>) or attachments (<attachment ID: attachment type>) must be encrypted:- {0}

Category:
Security

Cause:
Parts or elements to be encrypted according to policy were different from those in the SOAP message.

Action:
Refer to the policy and WS-Security specifications to ensure that all encryption requirements mandated by the policy and the specifications are met.

WSM-00034
Error in Encryption reference mechanism compliance : Expected : {0} , Actual : {1}. Ensure that a compatible policy is attached at the client side.

Category:
Security

Cause:
The expected and actual encryption reference mechanisms did not match.

Action:
Check the policy to determine the permitted values for the encryption reference mechanism.

WSM-00035
Error in Signature reference mechanism compliance : Expected : {0} , Actual : {1}. Ensure that a compatible policy is attached at the client side.

Category:
Security

Cause:
The expected and actual signature reference mechanisms did not match.

Action:
Check the policy to determine the allowed value of the signature reference mechanism.

WSM-00036
The signed message elements or parts do not comply with the policy. The following headers/elements (<name space: local name>) or attachments (<attachment ID: attachment type>) must be signed:- {0}

Category:
Security

Cause:
Parts or elements to be signed according to policy were different from those in the soap message.

Action:
Refer to the policy and WS-Security specifications to make sure that all the signature requirements mandated by the policy and the specifications are met.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-00037
Error in signature confirmation compliance.

Category:
Security

Cause:
The error could have occurred because the response signature confirmation element was not signed.

Action:
Check that all the signature confirmations in the response are signed and referenced in the response signature.

WSM-00039
Message is not compliant with timestamp requirement of the policy. Timestamp element is required by policy but it is not present in the message.

Category:
Security

Cause:
Policy compliance failed due to timestamp. Timestamp element is required by policy but it is not present in the message.

Action:
Check the message and make sure message is compliant with timestamp requirement of the service policy.

WSM-00042
The request must be made over SSL.

Category:
Requests/Responses

Cause:
The request was expected to be sent over SSL, but it was not.

Action:
Check the SSL port and send the request over SSL.

WSM-00043
No peer certificates are present from the HTTP request.

Category:
Security

Cause:
A certificate in the trust chain is missing.

Action:
Ensure that the complete certificate chain is propagated in the request, if certificates signed by CA are used.

WSM-00044
The HTTP authorization header is missing.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Security

Cause:
The authorization Header was not found.

Action:
Ensure that the request HTTP headers contain an authorization header.

WSM-00045
HTTP authentication/authorization failure.

Category:
Security

Cause:
Failure occurred in basic authentication.

Action:
Use the appropriate Base64 encoded combination of a valid username and password.

WSM-00046
Error in advertisement of WS-Policy.

Category:
Other

Cause:
An error occurred while advertising ORAWSDL to WS-Policy.

Action:
Contact Oracle Support Services.

WSM-00047
Invalid key referencing mechanism: {0}.

Category:
Configuration

Cause:
The sign or encryption key reference mechanism used was invalid.

Action:
Valid supported values are direct, issuerserial, SKI, or thumbprint.

WSM-00048
The signature confirmation value is invalid. Expected : {0}, Actual : {1}.

Category:
Security

Cause:
Signature confirmation sent in the response was invalid.

Action:
See the WS-Security 1.1 specification for the correct @Value of SignatureConfirmation.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-00049
The expected {0} signature is missing in the request message.

Category:
Security

Cause:
No signature (message, or endorsing) was found in the request to confirm.

Action:
Resend the request with at least one <Signature>.

WSM-00050
Cannot obtain security token reference.

Category:
Other

Cause:
The message was not signed or encrypted properly.

Action:
Check the <ds:Reference> section of the message.

WSM-00051
The encrypted data or key cannot be obtained.

Category:
Other

Cause:
The referenced encrypted object could not be found. The referenced encrypted object could not be found.

Action:
Ensure that the reference points to valid <EncryptedData> element. Ensure that the reference points to valid <EncryptedKey> element.

WSM-00052
There is an invalid or nonexistent configuration for the Login Module class [{1}] in the Java Platform Security (JPS) context [{0}].

Category:
Configuration

Cause:
An invalid or nonexistent configuration for Login Module could have been used.

Action:
Change the configuration and retry the operation.

WSM-00053
The propagated subject is either null or empty.

Category:
Security

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
No Subject was found.

Action:
Send a valid nonempty Subject.

WSM-00054
The password credentials cannot be obtained from the Credential Store Framework (CSF). Unable to retrieve the csfKey "{0}". The csf map "{1}" found in the credential store is being used and the following keys are found in this map <CsfKeyName: UserName>:- {2}

Category:
Configuration

Cause:
Failure occurred while doing query for credentials from Credential Store Framework (CSF).

Action:
Check CSF configuration.

WSM-00055
The keystore located at {0} cannot be loaded due to {1}. Ensure that valid keystore type and password are configured.

Category:
Configuration

Cause:
The following keystore-related configuration properties may not be valid:keystore.type, keystore.pass. Also, the keystore could be corrupt or could have been tampered with.

Action:
Verify the configuration properties mentioned above and retry the operation. In a rare situation, replace or regenerate the keystore.

WSM-00056
The key, {0}, is not retrieved. Ensure that the above key exists in the credential store. The location of the key store being used is "{1}" and its type is "{2}". The following aliases are found in the keystore:- {3}

Category:
Configuration

Cause:
Error occurred while obtaining key from store.

Action:
Make sure the key exists in the keystore. Check JPS configuration settings for correct key alias, key password and keystore password. Also, check the values of the key keystore-csf-key and its password in the oracle.wsm.security map, through EM or WLST. In a rare situation, this error can also happen if the actual keystore type is ORACLE_WALLET and the keystore type specified in JPS configuration file is PKCS12.

WSM-00057
The certificate, {0}, is not retrieved.{4}The location of the key store being used is "{1}" and its type is "{2}". The following aliases are found in the keystore:- {3}

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Configuration

Cause:
Failure occurred while retrieving certificate from store.

Action:
Verify keystore location configuration property as well as make sure that the requested certificate is present.

WSM-00058
The key type {0} is not supported.

Category:
Configuration

Cause:
The private key algorithm that was used is unsupported.

Action:
Ensure that the private key follows the RSA algorithm.

WSM-00059
Signature method algorithms are mismatched. Expected : {0}, Actual : {1}.

Category:
Security

Cause:
Expected and actual values of signature method algorithms did not match.

Action:
Check the policy and WS-Security Policy 1.1 specification for valid values.

WSM-00060
Error validating timestamp.

Category:
Security

Cause:
Timestamp is expired.

Action:
Check the timestamp. Check the allowed clockskew and message expiration time.

WSM-00061
Signature digest verification failure. The system property xml.debug.verify should be enabled for the details about the digest calculations during verification phase (note xml.debug.verify slows down the signature verification for very large messages). Caused by:-{0}

Category:
Security

Cause:
Digest verification failed possibly due to corrupted digest, or a message that was tampered with.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Recompute the digest and send the message again.

WSM-00062
The path to the certificate used for the signature is invalid.

Category:
Security

Cause:
The intermediate and root certificates of the signing certificate were not present in the keystore at the verifying end.

Action:
Make sure that the entire certificate chain is available in the keystore for verification.

WSM-00063
The version of SAML is incorrect. Expected : {0}, Actual : {1}.

Category:
Security

Cause:
SAML version in the SAML assertion did not match the expected version.

Action:
Check to see that the major version and minor version of the assertion are according to policy.

WSM-00064
SAML subject confirmation mismatch. Expected : {0}, Actual : {1}.

Category:
Security

Cause:
Subject confirmation method in SAML assertion did not match the policy requirements.

Action:
Check to see that the confirmation method for all the SAML assertions is sender-vouches.

WSM-00065
Error sending request over SSL.

Category:
Other

Cause:
Failure in creating SSL request possibly due to invalid configuration of Credential Store FrameWork (CSF).

Action:
Check the JPS configuration for CSF.

WSM-00066
The matching certificate for the given Subject Key Identifier (SKI) cannot be found.

Category:
Security

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
None

Action:
None

WSM-00067
None SOAP message parts can be encrypted.

Category:
Security

Cause:
The elements to be encrypted in the policy were selected to be either of soap Envelope/Body/Header.

Action:
The core soap nodes cannot be encrypted according to WS-Security 1.0 specification.

WSM-00068
The security token is missing.

Category:
Security

Cause:
Security token was expected but was not found.

Action:
Security token is missing. Resend request with valid Security token.

WSM-00069
The security header is missing in request. Ensure that there is a valid security policy attached at the client side, and the policy is enabled.

Category:
Security

Cause:
Security header was expected but was not found.

Action:
Security header is missing. It could be that client side policy has not been applied. Resend request with appropriate Security header.

WSM-00070
The nonce cannot be validated.

Category:
Security

Cause:
Failure occurred while performing nonce Validation.

Action:
This may be due to a repeated value of nonce. Resend the request with a valid nonce.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-00071
Error validating the wsu:Created attribute.

Category:
Security

Cause:
Failure occurred while doing Created(Timestamp) validation.

Action:
Resend the request with a valid timestamp, and or within the expiration limits.

WSM-00072
An encryption algorithm suite policy compliance failure occurred, expected algorithm: {0}, actual algorithm: {1}

Category:
Security

Cause:
Failure occurred in encryption algorithms policy compliance check, expected algorithm: {0}, actual algorithm: {1}

Action:
Check the encryption algorithm requirements of the policy and resend the message with appropriate value of algorithm suite.

WSM-00073
The mechanism {0} used in the authentication header is not supported.

Category:
Configuration

Cause:
The value of mechanism attribute used was not supported.

Action:
Change the policy to point to valid value of mechanism(basic), and retry the operation.

WSM-00074
The authorization header {0} is not correctly encoded using the Base64 encoding.

Category:
Security

Cause:
The authorization header was not encoded according to Base64 requirements.

Action:
Encode the header with Base64(username:realm:password) format and resend the request.

WSM-00075
The realm property is not configured in the policy.

Category:
Configuration

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
The realm property was not configured in the policy.

Action:
Configure appropriate value of realm inside the policy.

WSM-00076
The user name is missing from the encoded authorization header.

Category:
Security

Cause:
The Authorization header did not contain a properly encoded username, or username was null.

Action:
Encode the header with Base64(username:realm:password) format and resend the request.

WSM-00077
The password is missing from the encoded authorization header.

Category:
Security

Cause:
The Authorization header did not contain password encoded properly, or password was null.

Action:
Encode the header with Base64(username:realm:password) format and resend the request.

WSM-00078
The configuration of the credentials in the policy is incorrect.

Category:
Configuration

Cause:
Credential configuration in the policy was incorrect.

Action:
Configure policy with valid Credential Store Framework (CSF) key, or username/password properties.

WSM-00079
The <BinarySecurityToken> element is missing.

Category:
Security

Cause:
<BinarySecurityToken> was not found.

Action:
For reference mechanisms that are configured with value direct, send the certificate inside <BinarySecurityToken> element.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-00080
STR Dereferencing Transform not found

Category:
Security

Cause:
STR Dereferencing Transform was not found.

Action:
For reference mechanisms that are configured with value SKI, the Transforms section should contain the STR Dereferencing Transform.

WSM-00081
The X.509 certificate is not signed.

Category:
Security

Cause:
The X509 token used was not signed according to requirements of certificate authentication scenario.

Action:
Sign the X509 token (depending upon the reference mechanism used) for certificate authentication.

WSM-00082
The roles and/or attributes of the user profile cannot be retrieved.

Category:
Security

Cause:
No information could be obtained regarding the user roles or attributes.

Action:
Try resending the request for another user.

WSM-00083
Error computing the digest for this reference.

Category:
Security

Cause:
Digest computation for the <Reference> failed.

Action:
Check log file for possible cause.

WSM-00084
Error computing <SignatureValue> for this signature block.

Category:
Security

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
Signature value computation for the signature block failed.

Action:
Check log file for possible cause.

WSM-00085
The certificates cannot be retrieved from the keystore.

Category:
Security

Cause:
Failure occurred while trying to retrieve certificate from keystore.

Action:
Use a valid alias for the certificate and retry the operation.

WSM-00086
Error initializing nonce cache.

Category:
Security

Cause:
Failure occurred while initializing iAS Cache.

Action:
Check log file for possible cause.

WSM-00087
Either {0} property or the oracle.j2ee.home system property is not set.

Category:
Security

Cause:
The cache configuration file for iAS cache was not found.

Action:
Set the system property oracle.j2ee.home or javacache.config.home system property to the path of the configuration file javacache.xml.

WSM-00088
The ObSSOCookie is missing.

Category:
Security

Cause:
The OAM security token was not found.

Action:
Resend the request by embedding the ObSSOCookie token inside a <BinarySecurityToken> element.

WSM-00089
The attachments security transform is incorrect. Expected : {0}, Actual : {1}.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Security

Cause:
The attachment security transform used was incorrect.

Action:
Refer to the recipient's policy for information about which SwA Security Transform is to be used.

WSM-00090
The signature for the attachment is non-compliant.

Category:
Security

Cause:
The attachment signature was not compliant.

Action:
Refer to the recipient's policy for information about which SwA Security Transform is to be used.

WSM-00091
The encryption of the attachment is non-compliant.

Category:
Security

Cause:
The attachment encryption was not compliant.

Action:
Refer to the recipient's policy for information about which SwA Security Transform is to be used.

WSM-00092
The <EncryptedKey> element is missing in the request. Ensure that there is a message protection policy attached at the client side.

Category:
Security

Cause:
No <EncryptedKey> elements were found in the request.

Action:
Refer to the WS-Security 1.0 and 1.0 specifications for the semantics.

WSM-00093
The <saml:Assertion> element is missing in the security header. Ensure that there is a SAML token policy attached at the client side. Tokens found in the security header are:- {0}.

Category:
Security

Cause:
No SAML assertions were found inside the security Header.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Resend the message with at least one SAML assertion in the header.

WSM-00094
The negotiated cipher suite does not meet policy requirements. Expected : {0}, Actual : {1}.

Category:
Security

Cause:
The negotiated cipher suite did not meet policy requirements.

Action:
Check the recipient's policy for the permitted values of the cipher suite.

WSM-00095
There is more than one assertion assigned to the same category {0} in the security policy.

Category:
Configuration

Cause:
Two or more assertions assigned to the same category were used.

Action:
Ensure that assertions inside a security policy belong to different categories.

WSM-00096
The order of the assertions is incorrect.

Category:
Configuration

Cause:
Assertion order does not match the requirements of policy.

Action:
Use the following order for client side policy : authentication -> msgprotection or authentication -> authorization and following for server side security policy msg-protection -> authentication or msg-protection -> authentication -> authorization.

WSM-00097
HTTP basic authentication header is missing.

Category:
Security

Cause:
HTTP basic authentication header was missing.

Action:
Client must provide the HTTP basic authentication header.

WSM-00098
User realm {0} is either null or is a mismatch with service realm {1}.

Category:
Security

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
User realm was either null or was a mismatch with service realm.

Action:
Make sure user realm sent from client matches with the service realm.

WSM-00099
Username, password, or both are missing from the HTTP authentication header.

Category:
Security

Cause:
Username, password, or both were missing from HTTP authentication header.

Action:
Make sure the HTTP request header contains the username/password token.

WSM-00100
Found more than one keystore files {0} in application classpath. By default the first keystore is used. Make sure the desired keystore is being used by clearing others from the classpath.

Category:
Security

Cause:
Found more than one keystore file in application classpath. By default, the first keystore is used.

Action:
To ensure the desired keystore is being used, remove other keystores from the classpath, if possible.

WSM-00101
The specified keystore file {0} cannot be found; it either does not exist or its path is not included in the application classpath.

Category:
Security

Cause:
Keystore file did not exist or its path was either incorrect or not included in the application classpath.

Action:
Verify the keystore file does exist and its path is included in the application classpath.

WSM-00102
The specified user/subject does not belong to any role in system ID store.

Category:
Security

Cause:
The subject/user did not belong to any defined role in system ID store.

Action:
Verify and make sure that the specified user belongs to one or more roles.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-00103
The policy is configured incorrectly without specifying roles, or denyAll or permitAll elements.

Category:
Security

Cause:
The policy was incorrectly configured with no roles and no denyAll/permitAll elements.

Action:
Correct the policy by configuring it with a denyAll element, a permitAll element, or at least one role.

WSM-00104
The specified JPS context {0} cannot be found in system-level JPS configuration file.

Category:
Security

Cause:
The JPS context could not be found in system level JPS configuration.

Action:
Verify system level JPS configuration file to ensure that it contains the context.

WSM-00105
Credential Store service instance is missing. Either the Oracle WSM JPS context being used for the keystore does not contain a reference to the Credential Store service instance, or the reference is not valid. The Credential Store service instance needs to be declared at the same level (system or application) as the keystore service instance. Therefore, if an application-level keystore is being used, a Credential Store Framework (CSF) store must also be declared at the application level.

Category:
Security

Cause:
No Credential Store (CSF) was found at the level where keystore was used.

Action:
Verify that the WSM JPS context is configured correctly. The error indicates that either the WSM JPS context which is being used for keystore does not contain reference to the Credential Store service instance, or the reference is not valid. The Credential Store service instance needs to be declared at the same level (system or application) as the keystore service instance. Therefore, if an application level keystore is being used, a CSF store must also be declared at the the application level.

WSM-00106
Assertion assigned to a non-security category {0} cannot be added to policy assigned to a security category.

Category:
Security

Cause:
Assertion belonging to non-security categories could not be added to policies belonging to security category.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Ensure that assertions in security policy also belongs to security category.

WSM-00107
Assertion belonging to {0} category is not valid for generic policy. Only assertion of type security/logging can be added to a generic policy (policy applicable to clients and servers). Check the assertions added to the generic policy.

Category:
Security

Cause:
Invalid assertions were found in generic policy.

Action:
Only assertion of type security/logging can be added to a generic policy (policy applicable to clients and servers). Recheck the assertions added to the generic policy.

WSM-00108
If password type is set to digest, addNonce and addCreated should be true.

Category:
Security

Cause:
UserNameToken Assertion had Passwordtype as digest but addNonce or addCreated was false.

Action:
In case of passwordtype as digest, addNonce and addCreated both should be true. Recheck the assertion.

WSM-00109
Algorithm suite is not supported, only TripleDes is supported for Kerberos assertion.

Category:
Security

Cause:
Kerberos Assertion had algorithm-suite other than TripleDES.

Action:
Only TripleDES algorithm is supported in case of Kerberos, so set algorithm-suite as TripleDes.

WSM-00110
Basic192 and *RSA15 algorithm-suites are not supported for SSL. Change the algorithm suite to one that is supported.

Category:
Security

Cause:
Basic192 or RSA algorithm-suite was used for SSL.

Action:
Use other supported Algorithm-suite for SSL except Basic192 and RSA algorithms.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-00111
Keystore is not properly configured. Check your keystore configurations.

Category:
Security

Cause:
Keystore was not properly configured.

Action:
Check the keystore configuration, and try again.

WSM-00112
Missing keystore service instance reference in Oracle WSM JPS context.

Category:
Security

Cause:
Keystore Service instance reference was not found in WSM JPS Context.

Action:
Add the keystore service instance reference to WSM JPS Context, and try again.

WSM-00113
Unsupported configuration value for Client Credential Configuration location.

Category:
Security

Cause:
An unsupported configuration value of Client Credential location configuration was provided.

Action:
Refer to the documentation for valid values and add the proper configuration value for Client Credential Configuration Location, and try again.

WSM-00114
No matching SSL cipher suite is found for algorithm suite value, specified in the Policy.

Category:
Security

Cause:
No matching SSL cipher suite was found for algorithm suite value, specified in WS Policy.

Action:
Set algorithm suite of Web Service policy to a value that has matching SSL cipher suite.

WSM-00115
JSSE System Property for SSL cipher suite is either not set or does not match algorithm suite value specified in WS Policy.

Category:
Security

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
JSSE System Property for SSL cipher suite was either not set or did not match algorithm suite value specified in WS Policy.

Action:
Set JSSE System Property (https.cipherSuites) to a value that matches algorithm suite as specified in WS Policy.

WSM-00116
Error retrieving SOAP body from SOAP message.

Category:
Security

Cause:
An error ocurred while retrieving SOAPBody from SOAPMessage. Either the SOAPMessage was not proper or had been tampered with.

Action:
Check whether the SOAPMessage is according to the Specifications and try again.

WSM-00117
Error occurred while transforming the security header.

Category:
Security

Cause:
TransformerException occurred while transforming the WssHeader to String. The SOAPMessage might not have been proper or it did not conform to the specifications.

Action:
Check the SOAPMessage and try again.

WSM-00118
OAM token can be inserted only on hosted clients where authenticated subject has been established.

Category:
Security

Cause:
Insertion of an OAM token tried from a non-hosted client where Authenticated Subject is not established.

Action:
Try to add OAM token from a hosted client as only the hosted clients can insert the OAM token extracting it from Authenticated Subject

WSM-00119
Either authorization header or requireTLS must be present.

Category:
Security

Cause:
The security policy attached did not have either auth Header or requireTLS set to true.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Change the policy to have either auth Header or requireTLS to be true.

WSM-00120
Cannot compute endorsing signature as no message signature is present.

Category:
Security

Cause:
The security policy did not sign anything from the message, so no signature was there. Endorsing Signature could not be computed as the signature which it was trying to endorse was not present.

Action:
Change the policy to Sign at least something in the message.

WSM-00121
Only the attachments are to be signed/encrypted and they are not present.

Category:
Security

Cause:
Only the attachments were to be signed/encrypted and they were not present.

Action:
Retry after putting attachments in the SOAP Message.

WSM-00122
Valid timestamp is not present in the message. It is missing the Created time.

Category:
Security

Cause:
Valid timestamp was not present in the message. It was missing the Created time.

Action:
Ensure the timestamp element conforms to the specifications.

WSM-00123
Timestamp of the message is in future.

Category:
Security

Cause:
The message had Created timestamp of a time in future so it failed Future message validation.

Action:
Ensure freshness of the message and check WSM configuration system for the configured value of clock skew.

WSM-00124
Timestamp of the message is in past.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Security

Cause:
The message was older than the permissible time limit so it failed Past message validation.

Action:
Ensure freshness of the Message and check the WSM configuration system for the configured values of clock skew and expire time.

WSM-00125
Password digest validation failed.

Category:
Security

Cause:
The password digest in the message was not correct so it failed the digest validation.

Action:
Retry after ensuring password digest is proper.

WSM-00126
Subject does not contain JPS user.

Category:
Security

Cause:
The subject mentioned did not have the JPS User.

Action:
Retry after ensuring JPS user in the subject.

WSM-00127
User not in identity store.

Category:
Security

Cause:
The user mentioned was not present in the identity store.

Action:
Retry after ensuring that user is present in the identity Store.

WSM-00128
Keystore instance is null.

Category:
Security

Cause:
Could not obtain keystore instance. Either the keystore instance type was wrong or the keystore configuration was wrong.

Action:
Check JPS configuration settings. Use correct keystore instance type.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-00129
Unsupported SAML token provided : {0}.

Category:
Security

Cause:
An unsupported SAML token confirmation method was provided.

Action:
Provide a supported SAML token confirmation method and retry the operation.

WSM-00130
SAML assertion subject is missing.

Category:
Security

Cause:
The SAML assertion subject name was not specified.

Action:
Provide the SAML assertion subject and retry the operation.

WSM-00131
Unsupported data encryption algorithm: {0}.

Category:
Security

Cause:
An unsupported data encryption algorithm was provided.

Action:
Consult the documentation for the supported encryption algorithms and retry the operation.

WSM-00132
Invalid JPS configuration.

Category:
Security

Cause:
An invalid JPS configuration was provided.

Action:
Make sure that the JPS configuration is valid.

WSM-00133
Unsupported MessageContext type {0}.

Category:
Configuration

Cause:
Unsupported MessageContext type was provided.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Correct the MessageContext type and retry the operation.

WSM-00134
The signature key, {0}, is not retrieved due to exception {1}.

Category:
Security

Cause:
Error occurred while obtaining the signature key from store.

Action:
Check JPS configuration settings. Make sure that the key password , keystore password, and key alias are valid.

WSM-00135
The encryption key, {0}, is not retrieved due to exception {1}.

Category:
Security

Cause:
Error occurred while obtaining encryption key from store.

Action:
Check JPS configuration settings. Use correct key password, keystore password, and key alias.

WSM-00136
The signature certificate, {0}, is not retrieved due to exception {1}.

Category:
Security

Cause:
Failure occurred while retrieving the signature certificate from store.

Action:
Check JPS configuration settings for keystore location and make sure that the requested certificate is present.

WSM-00137
The encryption certificate, {0}, is not retrieved due to exception {1}.

Category:
Security

Cause:
Failure occurred while retrieving the encryption certificate from store.

Action:
Check JPS configuration settings for keystore location and make sure that the requested certificate is present.

WSM-00138
The path to the certificate is invalid. Validation failed for the certificate {0}

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Security

Cause:
The intermediate and root certificates of the certificate were not present in the keystore during verification.

Action:
Make sure that the entire certificate chain is available in the keystore for verification.

WSM-00139
The scenario category {0} is not supported.

Category:
Security

Cause:
The scenario category is not supported.

Action:
Consult the Oracle documentation for supported categories.

WSM-00140
Invalid execution stage {0} resulting in system internal error.

Category:
Security

Cause:
System encountered an invalid execution stage.

Action:
Retry the operation, If problem persists contact Oracle Support Services.

WSM-00141
Error retrieving SOAP header from SOAP message.

Category:
Security

Cause:
An error occurred while retrieving the header from the SOAP Message. The SOAP message was invalid or was tampered with.

Action:
Make sure that the SOAP message is valid according to the specifications and retry the operation.

WSM-00142
Assertion belonging to {0} category is not valid for Component policy

Category:
Security

Cause:
Assertion belonging to authentication or message protection category was found in Component policy and it is invalid.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Modify the policy to correct the problem and retry the operation.

WSM-00143
Failure creating Java Keystore instance for type {0}.

Category:
Configuration

Cause:
Either the keystore type provided is not supported or there is no implementation provider for Java keystore.

Action:
Consult the Oracle documentation for supported Keystore types and make sure the implementation provider for Java Keystore is available.

WSM-00144
Failure retrieving Keystore aliases.

Category:
Configuration

Cause:
Keystore may have not been initialized.

Action:
Check the log file for possible causes and retry the operation.

WSM-00145
Keystore location or path can not be null or empty; it must be configured through the domain level configuration or policy configuration override.

Category:
Configuration

Cause:
Keystore location/path was either missing, set to be null, or empty.

Action:
Make sure that Keystore location is configured properly in the domain level configuration or through policy configuration override.

WSM-00146
Keystore type {0} defined using keystore.type property in the domain level configuration or through policy configuration override is not supported.

Category:
Configuration

Cause:
Invalid or unsupported keystore.type property value was found.

Action:
Consult the oracle documentation to ensure that a valid keystore.type is configured either through the domain level configuration or using policy configuration override.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-00147
JPS context property is no longer supported in policy configuration

Category:
Configuration

Cause:
Unsupported JPS context property value was found.

Action:
Remove JPS context property from the configuration file.

WSM-00148
Security policy cannot be applied to streamed attachments. Streaming should be turned off if there are any security policies for attachments.

Category:
Configuration

Cause:
Security policy cannot be applied to streamed attachments.

Action:
Make sure streaming is off if security policies are being used for attachments.

WSM-00149
SAML assertion is missing.

Category:
Security

Cause:
Failed to locate SAML assertion with ID {0}.

Action:
Make sure that a valid SAML asssertion exists.

WSM-00150
Processed header list fetched from InterceptorContext is null, agentFunction:{0}, listType:{1}.

Category:
Security

Cause:
Processed header list fetched from InterceptorContext is null.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

WSM-00151
Role class {0} specified in the policy is either invalid or is not available in the classpath. Exception thrown : {1}.

Category:
Configuration

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
Class name required for retrieving principal/role from subject is either invalid or class not present in the classpath

Action:
Specify a valid class name in the policy and ensure that the instances of the class specified are associated with the subject created.

WSM-00152
Callback {0} is not supported by Oracle WSM callback handler.

Category:
Security

Cause:
Callback specified is not supported by Oracle WSM callback handler.

Action:
Specify a valid callback class that Oracle WSM callback handler can support.

WSM-00153
Error retrieving Weblogic Server subject from JPS subject using SubjectSecurityUtil API

Category:
Security

Cause:
A failure occurred while converting JPS subject to Weblogic Server subject.

Action:
Check log file for possible cause.

WSM-00154
The empty or all-spaces value set explicitly for property {0} is detected and it is not valid value.

Category:
Security

Cause:
The property value was probably set unintentionally to empty or all-spaces through policy configuration override or JPS configuration.

Action:
Make sure that the value provided either through policy configuration override, policy binding, or JPS configuration is not empty or all spaces.

WSM-00155
Error retrieving Oracle WSM security policies.

Category:
Security

Cause:
A failure occurred while retrieving Oracle WSM security policies.

Action:
Check log file for possible cause.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-00156
Invalid binary security token.

Category:
Security

Cause:
Binary security token in the header and the certificate used for endorsing signature did not match.

Action:
Make sure a valid binary security token is being passed.

WSM-00157
Recipient key alias not configured and signer certificate was not available because no part of the request was signed.

Category:
Security

Cause:
Recipient key alias not configured and signer's certificate was not available because no part of request was signed.

Action:
Set recipient key alias in service policy or sign part of the request.

WSM-00158
KerberosLoginModule class is not available in the classpath

Category:
Security

Cause:
The class for the Kerberos login module was not available in the classpath.

Action:
Make sure that the KerberosLoginModule class is included in the classpath, and configure the class name properly in WSM configuration system.

WSM-00159
TextCallbackHandler class is not available in the classpath

Category:
Security

Cause:
The class for the Text callback handler was not available in the classpath.

Action:
Make sure that the TextCallbackHandler class is included in the classpath, and configure the class name properly in WSM configuration system.

WSM-00160
The SSL policy must contain a requireTLS element.

Category:
Security

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
The security policy attached did not have requireTLS set to true.

Action:
Change the policy to have requireTLS as true.

WSM-00161
Client encryption public certificate is not configured for Async web service client

Category:
Security

Cause:
Client encryption public certificate is not configured for async web service client with message protection.

Action:
Make sure that client public certificate is configured in client keystore, or provided through client config override for Async web service client that uses message protection

WSM-00162
Invalid recipient cert type: {0} may have been provided through override; It should be either a X509Certificate object or Base64 encoded value in String format.

Category:
Configuration

Cause:
Invalid recipient cert type may have been provided through override; It should be either a X509Certificate object or Base64 encoded value in String format.

Action:
Verify that only X509Certificate object, or Base64 encoded String value are provided in Policy, descriptor file or through program.

WSM-00163
Failure in getting recipient certificate using recipient key alias {0}

Category:
Configuration

Cause:
The recipient key alias might not be valid

Action:
Check to see if there is such certificate in keystore corresponding to the recipient key alias provided.

WSM-00164
Cannot obtain a valid recipient cert for client message sending

Category:
Configuration

Cause:
Encountered error while obtaining recipient certificate for sending request.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Must provide valid recipient certificate, or recipient alias for client to send request with message protection.

WSM-00165
Creating recipient certificate from base64 encoded string: {0} failed.

Category:
Configuration

Cause:
Encountered error while creating recipient certificate from base64 encoded string.

Action:
Must provide valid certificate in valid base64 encoded string.

WSM-00166
Extract certificate from saved ReplyTo header failed.

Category:
Configuration

Cause:
X509Certificate within ReplyTo header element might be invalid.

Action:
Ensure that cert. insertion, ReplyTo header serialization/deserializaton to JMS queue are all working properly.

WSM-00167
Actual Hostname {0} and Hostname retrieved from Certificate {1} do not match

Category:
Security

Cause:
HostName verification of certificate retrieved from WSDL failed

Action:
Either ensure that the Subject Dn matches the Hostname of the Service or disable the HostName Verification check

WSM-00168
Unable to extract X509Certificate from WSDL Definition Object as WSDL definition Object is unavailable

Category:
Security

Cause:
WSDL definition required for extraction of X509Certificate not available

Action:
Ensure that WSDL Definition Object is available from the MessageContext

WSM-00169
Error decrypting the request message.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Security

Cause:
The request message could not be decrypted using the key specified for decryption.

Action:
Ensure that the key used for decryption is same as the one used for encryption.

WSM-00170
There are no assertions available under the ExactlyOne policy operator.

Category:
Security

Cause:
There are no assertions under ExactlyOne policy operator.

Action:
Ensure that one or more security assertions are kept under ExactlyOne policy operator.

WSM-00171
A client policy contains an ExactlyOne policy operator.

Category:
Security

Cause:
A client policy contained an ExactlyOne policy operator.

Action:
Remove the ExactlyOne policy operator or switch to a service binding.

WSM-00172
A generic policy contains an ExactlyOne policy operator.

Category:
Security

Cause:
A generic policy contained an ExactlyOne policy operator.

Action:
Remove the ExactlyOne policy operator or switch to a service binding.

WSM-00173
A policy contains more than one ExactlyOne policy operator.

Category:
Security

Cause:
A policy contained more than one ExactlyOne policy operator.

Action:
Remove the additional ExactlyOne policy operators.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-00174
A policy contains a nested ExactlyOne policy operator.

Category:
Security

Cause:
A policy contained a nested ExactlyOne policy operator.

Action:
Remove the nested ExactlyOne policy operators.

WSM-00175
Recipient Certificate for async callback client is not found under the ReplyTo element in async callback client message context

Category:
Configuration

Cause:
Recipient cert. for async callback client is not available from message context.

Action:
Ensure that original async client has public encryption certificate configured and is inserted into the ReplyTo header or the original async request. Also ensure that the original ReplyTo header along with client encryption certification is preserved and restored to the callback client message context.

WSM-00176
The mapped long name(s) for property {0} is null, the property might not be available for client programmatic override. Make sure it is indeed the intention, otherwise, add a mapping to map ConfigOverrideMapping.

Category:
Configuration

Cause:
The config override property does not have a corresponding long name mapping

Action:
Make sure this is indeed intended, otherwise, add a mapping to the ConfigOverrideMapping.

WSM-00177
The CSF key provided by the user is not present in the credential store. So using the default key is being used.

Category:
Security

Cause:
The CSF key provided by the user is not present in the credential store

Action:
Provide a valid key. Till then the default key will be used.

WSM-00178
Public key not found for SAML signature verification.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Configuration

Cause:
Public key not found for SAML signature verification

Action:
Ensure that public key is present in Security header which is reqruied For SAML signature verification

WSM-00179
SAML assertion issuer name is invalid.

Category:
Security

Cause:
SAML assertion issuer name is invalid.

Action:
Check to see that the overridden SAML trused issuers has SAML assertion issuer name.

WSM-00180
The trust version {0} is not supported for policy advertisement, hence ignored. The default trust version {1} is advertised.

Category:
Configuration

Cause:
The trust version specified in the policy is not supported.

Action:
Modify the policy with a supported trust version.

WSM-00181
A policy issued-token attributes require-internal-reference and require-external-reference both are false, one of them has to be true.

Category:
Configuration

Cause:
A policy issued-token attribute require-internal-reference and require-external-reference can not both be false.

Action:
At least one of the attribute require-internal-reference and require-external-reference must be set to true

WSM-00182
A policy request-security-token-template element attribute token-type has an unsupported value: {0}

Category:
Configuration

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
A policy request-security-token-template element contains a token-type that is not supported.

Action:
Check documentation for supported token-type

WSM-00183
A policy request-security-token-template element attribute algorithm-suite has a value: {0} which does not match to that of msg-security: {1}, change it to match {1}.

Category:
Configuration

Cause:
A policy request-security-token-template element contains an algorithm-suite value that does not match to that of msg-security.

Action:
Change the algorithm-suite attribute value to match exactly the one in msg-security

WSM-00184
An attribute trust-version has an unsupported version: {0}

Category:
Configuration

Cause:
A policy contains an unsupported WS-TRUST version.

Action:
Check documentation for supported WS-TRUST version

WSM-00185
Attribute require-client-entropy and require-server-entropy can not both be set to false, at lease one of them must be set to true.

Category:
Configuration

Cause:
A policy can not have both require-client-entropy and require-server-entropy attributes set to false.

Action:
At lease set one of them to true

WSM-00186
A policy request-security-token-template key-type attribute is expected to be: {0}, but got: {1}

Category:
Configuration

Cause:
A policy request-security-token-template key-type attribute value is not set to the expected Bearer.

Action:
Set the attribute value to the expected

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-00187
A policy request-security-token-template key-type attribute is expected to be: {0}, but got: {1}

Category:
Configuration

Cause:
A Bearer policy request-security-token-template key-type attribute value is not set to the expected Symmetric or Public.

Action:
Set the attribute value to one of the expeted value Symmetric or Public

WSM-00188
STS Trust Config policy attribute port-uri has invalid value "{0}", it must be not null, not empty and in the format of http(s)://host:port/sts-service

Category:
Configuration

Cause:
STS trust config attribute port-uri is either null, empty or not in the format of "http(s)://host:port/sts-service-name".

Action:
Provide valid attribute value which is in the format of "http(s)://host:port/sts-service"

WSM-00189
STS Trust Config policy attribute port-endpoint has invalid value "{0}", it must be not empty and in the format of target-namespace#wsdl.endpoint(service-name/port-name)

Category:
Configuration

Cause:
STS trust config attribute port-endpoint is either empty or not in the format of "target-namespace#wsdl.endpoint(service-name/port-name)".

Action:
Provide valid attribute value which is in the format of "target-namespace#wsdl.endpoint(service-name/port-name)"

WSM-00190
STS Trust Config policy attribute policy-reference-uri can not have empty value.

Category:
Configuration

Cause:
The value of STS trust config attribute policy-reference-uri is empty or not in the URI format

Action:
Specify value for attribute policy-reference-uri

WSM-00191
STS Trust Config policy attribute sts-keystore-recipient-alias can not have null or empty value.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Configuration

Cause:
The value of STS trust config attribute sts-keystore-recipient-alias is null or empty

Action:
Specify a non null or empty value for attribute sts-keystore-recipient-alias

WSM-00192
Kerberos name identifier format is not supported for SAML 1.1 token.

Category:
Security

Cause:
Kerberos name identifier format is not supported for SAML 1.1 token.

Action:
Kerberos name identifier format is only for SAML 2.0 token, use other name identifier formats.

WSM-00193
Security policy contains NULL or empty value for signed-element local name or namespace.

Category:
Security

Cause:
Security policy contains NULL or empty value for signed-element local name or namespace.

Action:
Signed-element local name or namespace must not be null or empty.

WSM-00194
Security policy contains NULL or empty value for signed-part header namespace.

Category:
Security

Cause:
Security policy contains NULL or empty value for signed-part header namespace.

Action:
Signed-part header namespace must not be null or empty.

WSM-00195
Security context for derived key unknown (cannot determine the base symmetric key).

Category:
Security

Cause:
Security context for derived key unknown (cannot determine the base symmetric key).

Action:
DerivedKeyToken should include SecurityReferenceToken (can only be empty in responses where the message context includes the base key).

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-00196
Unable to resolve base key referenced in DerivedKeyToken.

Category:
Security

Cause:
Unable to resolve base key referenced in DerivedKeyToken.

Action:
Ensure the SecurityTokenReference in the DerivedKeyToken specifies a valid base key within the security context.

WSM-00197
Unsupported SecurityTokenReference type for DerivedKeyToken : {0}.

Category:
Security

Cause:
Unsupported SecurityTokenReference type for DerivedKeyToken.

Action:
Ensure the SecurityTokenReference in the DerivedKeyToken is one of the supported types.

WSM-00198
Unable to resolve EncryptedKey that matches EncryptedKeySHA1 in KeyInfo.

Category:
Security

Cause:
Unable to resolve EncryptedKey that matches EncryptedKeySHA1 in KeyInfo.

Action:
The value of the EncryptedKeySHA1 should match an encrypted key in the security context.

WSM-00199
Unsupported key identifier type "{0}" in security token reference.

Category:
Security

Cause:
Unsupported key identifier type in security token reference.

Action:
Use only of the supported key idetifier types in the security token.

WSM-00200
Exception encountered while checking compliance; returning false.

Category:
Security

Cause:
Exception encountered while checking compliance; returning false.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Check log for exception details.

WSM-00201
There are no <EncryptedKey> elements in the request.

Category:
Security

Cause:
There are no <EncryptedKey> elements in the request.

Action:
The request should have an <EncryptedKey> element.

WSM-00202
Proof key type is invalid, valid values are null, public, symmetric.

Category:
Configuration

Cause:
The value of ketype is invalid for SAML Issued Token Policy , valid values are null (no proof key), public, symmetric

Action:
Specify valid value for keytype based on the policy

WSM-00203
Invalid OPSS Trust Service

Category:
Configuration

Cause:
OPSS TrustService is empty or null

Action:
Configure Trust Service in OPSS

WSM-00204
Invalid issued token from trust token exchange

Category:
Requests/Responses

Cause:
Issued token is null

Action:
Check Logs and correct any errors during issuance

WSM-00205
Proof key type is invalid, valid value is bearer

Category:
Configuration

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
The value of ketype is invalid for SAML Bearer Issued Token Policy , valid value is bearer

Action:
Specify bearer as the key type for this policy

WSM-00206
Requester credentials for authenticating to STS are invalid

Category:
Configuration

Cause:
Requester Credentials required for autenticating to STS are missing

Action:
Configure sts.auth.user.csf.key or sts.auth.x509.csf.key in issued token policy

WSM-00207
Asymmetric proof key is invalid

Category:
Configuration

Cause:
Assymetric proof key is invalid

Action:
Configure sts.auth.x509.csf.key in issued token policy

WSM-00208
STS On behalf of user is invalid

Category:
Configuration

Cause:
STS On behalf of user is invalid

Action:
Configure sts.auth.on.behalf.of.csf.key in issued token policy

WSM-00209
Permission{0} required to switch the identity not granted to the resource. {1}

Category:
Security

Cause:
Permission required to switch the identity not granted

Action:
Grant Permission for identity switching to the codesource.

WSM-00210
Client is unable to find actual webservice endpoint to set in appliesTo

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Configuration

Cause:
Client requires appliesTo and unable to find the actual webservice endpoint URL

Action:
Chenck if agent binding ws port ID , service name and port name in log file

WSM-00211
Trust token provider tried creating RequestSecurityToken message and it failed because algorithm use to generate asymmetric key pair was invalid

Category:
Requests/Responses

Cause:
Trust token provider tried creating RequestSecurityToken message and it failed because algoirthm use to generate asymmetric key pair was invalid

Action:
Check the asymmetric key algorithm

WSM-00212
Trust token provider tried creating RequestSecurityToken message and it failed because asymmetric proof key was invalid

Category:
Requests/Responses

Cause:
Trust token provider tried creating RequestSecurityToken message and it failed because assymetic proofk key was invalid

Action:
Check if sts.auth.x509.csf.key is configured correctly in issued token client policy

WSM-00213
Unable to parse SOAP message sent by STS

Category:
Requests/Responses

Cause:
Unable to parse SOAP message sent by STS

Action:
Check if message sent by STS is valid

WSM-00214
Unable to parse RequestSecurityTokenRespnseCollection

Category:
Requests/Responses

Cause:
Unable to parse RequestSecurityTokenResponseCollection

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Check if RequestSecurityTokenResponseCollection message sent by STS is valid

WSM-00215
Unable to parse STSTrustConfig

Category:
Requests/Responses

Cause:
Unable to parse STSTrustConfig

Action:
Check if STSTrustConfig is valid

WSM-00216
Unable to create SOAP RequestSecurityToken message

Category:
Requests/Responses

Cause:
Unable to create SOAP RequestSecurityToken message

Action:
Failure in creating SOAP RequestSecurityToken message, check log files

WSM-00217
STS endpoint URL or WSDL URL (if configured) is invalid

Category:
Requests/Responses

Cause:
STS endpoit URL is invalid

Action:
Check if STS endpoint URL is valid

WSM-00218
Security token returned by STS is null

Category:
Requests/Responses

Cause:
Security token returned by STS is null

Action:
Check if RSTR message sent by STS is valid

WSM-00219
Proof token returned by STS is null

Category:
Requests/Responses

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
Proof token returned by STS is null

Action:
Check if RSTR message sent by STS is valid

WSM-00220
Invalid proof token type, valid values are computedKey and BinarySecret

Category:
Requests/Responses

Cause:
Invalid proof token type, valid values are computedKey and BinarySecret

Action:
Check the proof token type, valid values are computedKey and BinarySecret

WSM-00221
Computed key in RSTR message sent by STS is invalid

Category:
Requests/Responses

Cause:
Computed key in RSTR message sent by STS is invalid

Action:
Check the computed key in RSTR message sent by STS

WSM-00222
Computed key algorithm in RSTR message sent by STS is invalid}

Category:
Requests/Responses

Cause:
Computed key algorithm in RSTR message sent by STS is invalid, valid value is http://docs.oasis-open.org/ws-sx/ws-trust/200512/CK/PSHA1

Action:
Check the computed key in RSTR message sent by STS, valid value is http://docs.oasis-open.org/ws-sx/ws-trust/200512/CK/PSHA1

WSM-00223
Request type is invalid, valid value is issue

Category:
Requests/Responses

Cause:
Request type invalid, valid value is issue

Action:
Check request type in response sent by STS

WSM-00224
User credentials of the user on behalf of whom the token is to be issued is missing

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Requests/Responses

Cause:
User credentials of the user on behalf of whom the token is to be issued is missing

Action:
Check on.behalf.of property in issued token policy. If its set to true then either subject or sts.auth.on.behalf.of.csf-key property needs to be present

WSM-00225
STS On behalf of user password is invalid

Category:
Configuration

Cause:
STS On behalf of user password is invalid

Action:
Configure sts.auth.on.behalf.of.csf.key in issued token policy

WSM-00226
Security policy contains NULL or empty value for encrypted-element local name or namespace.

Category:
Security

Cause:
Security policy contains NULL or empty value for encrypted-element local name or namespace.

Action:
Encrypted-element local name or namespace must not be null or empty.

WSM-00227
Could not resolve key to use for decryption.

Category:
Security

Cause:
Could not resolve key to use for decryption.

Action:
Ensure request contains all the information necessary to succesfully resolve decryption key.

WSM-00228
Oracle system user is missing in identity store

Category:
Configuration

Cause:
Could not find oracle system user .

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Check if OracleSystemUser exists in identity store

WSM-00229
jndi.lookup.csf.key missing in policy-accessor-config

Category:
Configuration

Cause:
Could not find valid jndi.lookup.csf.key in wsm configuration system .

Action:
Check jndi.lookup.csf.key is configured correclty in policy-accessor-config.xml

WSM-00230
Cannot find service information from WSDL {0}

Category:
Requests/Responses

Cause:
Cannot find service information from WSDL

Action:
Check the service information in the WSDL

WSM-00231
Cannot find client compatible policy for STS {0}, port name {1}

Category:
Requests/Responses

Cause:
Cannot find compatible client policy for STS invocation

Action:
Check if policy store has compatible client policy

WSM-00232
Failed to create dynamic STS policy

Category:
Requests/Responses

Cause:
Failed to create dynamic STS policy

Action:
Check exception stack trace for details

WSM-00233
STS WSDL URI {0} is invalid

Category:
Configuration

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
STS trust config attribute wsdl-uri is not in the format of "http(s)://host:port/sts-service?wsdl".

Action:
Provide valid attribute value which is in the format of "http(s)://host:port/sts-service?wsdl

WSM-00234
The <saml:Assertion> element of version {0} is missing in the security header.

Category:
Requests/Responses

Cause:
Saml assertion with specific version e.g. 1.1, or 2.0 etc. is missing. in the received message

Action:
Check exception stack trace for details

WSM-00235
Failed to initialize dispatcher

Category:
Requests/Responses

Cause:
Failed to initialize dispatcher for client to STS communication

Action:
Check exception stack trace for details

WSM-00236
Keystore name property value was not set through the domain level configuration

Category:
Security

Cause:
Keystore name property value was not set through the domain level configuration.

Action:
Make sure that the value is provided for keystore name through the domain level configuration.

WSM-00237
KSS keystore with URI {0} can not be loaded due to {1}.

Category:
Configuration

Cause:
The following KSS keystore-related configuration properties may not be valid:keystore.type, location. Also, check permissions on the keystore.

Action:
Verify the configuration properties mentioned above and retry the operation.

WSM-00238
Unable to read KSS keystore. Grant necessary permission to read KSS keystore with URI {0}

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Configuration

Cause:
KKS keystore may have not been initialized or necessary permissions are not granted.

Action:
Ensure that necessary permission to read KSS keystore is granted.

WSM-00239
KSS trust store can not be loaded, ensure that necessary permissions are granted.

Category:
Configuration

Cause:
KSS trust store can not be loaded, probably necessary permissions are not granted.

Action:
Ensure that necessary permission to read KSS trust store is granted.

WSM-00240
KSS trust store is NULL, ensure that KSS system trust store exist.

Category:
Configuration

Cause:
KSS trust store is NULL, may be it doesn't exists or probably necessary permissions are not granted.

Action:
Ensure that KSS trust store exists in system stripe and permissions are granted.

WSM-00241
Failure retrieving KSS trust store aliases.

Category:
Configuration

Cause:
KSS trust store may have not been initialized.

Action:
Check the log file for possible causes and retry the operation.

WSM-00242
The certificates cannot be retrieved from the trust store.

Category:
Security

Cause:
Failure occurred while trying to retrieve certificate from trust store.

Action:
Use a valid alias for the certificate and retry the operation.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-00243
Unable to read key from KSS keystore. Grant necessary permission to read alias {1} from KSS keystore with URI {0}

Category:
Configuration

Cause:
Unable to read key from KSS keystore. KSS keystore may have not been initialized or necessary permissions are not granted.

Action:
Ensure that alias exists in keystore and necessary permission to read key alias is granted.

WSM-00244
Unable to read certificate from KSS keystore. Grant necessary permission to read certificate alias {1} from KSS keystore with URI {0}

Category:
Configuration

Cause:
Unable to read certificate from KSS keystore. KSS keystore may have not been initialized or necessary permissions are not granted.

Action:
Ensure that alias exists in keystore and necessary permission to read certificate alias is granted.

WSM-00245
Failure retrieving KSS key store aliases.

Category:
Configuration

Cause:
Unable to list alias from KSS key store.

Action:
Check the log file for possible causes and retry the operation.

WSM-00246
Failure retrieving IssuedTokenAssertion from advertised policy.

Category:
Data

Cause:
Possibilly there is a failure in parsing the advertised policy

Action:
Check the log file for possible causes and retry the operation.

WSM-00247
Failed to sign with RSA Key Pair

Category:
Security

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
Failed to sign with RSA Key Pair

Action:
Check exception stack trace for details

WSM-00248
Attesting entity attribute {0} is unsupported.

Category:
Security

Cause:
Unsupported attesting entity attribute is used

Action:
Attesting entity attribute must be DN.

WSM-00249
SAML token DN validation failed for SAML assertion signer DN {0}.

Category:
Security

Cause:
SAML token DN list validation failed.

Action:
Assertion signer DN is not present in trusted DN list, if DN is valid then add it to trusted DNs list.

WSM-00250
Unable to find an implementation class for {0}.

Category:
Security

Cause:
Unable to find an implementation class for 'javax.el.ExpressionFactory'.

Action:
Make sure that the implementation class for 'javax.el.ExpressionFactory' is available in the classpath.

WSM-00251
Failed to create an instance of {0}.

Category:
Security

Cause:
Failed to create an instance of the javax.el.ExpressionFactory implementation class.

Action:
Make sure that the javax.el.ExpressionFactory implementation class can be instantiated.

WSM-00252
Failed to evaluate the constraint expression "{0}" due to the exception: {1}

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Security

Cause:
Failed to evaluate the constraint expression.

Action:
Make sure that the constraint expression is valid. Check exception stack trace for details.

WSM-00253
The constraint expression "{0}" is not valid. The constraint expression should evaluate to the boolean values.

Category:
Security

Cause:
The constraint expression is not valid.

Action:
Make sure that the constraint expression evaluates to the boolean values.

WSM-00254
The message is expired. Check the timestamp element in the message. The current server time is "{0}", incoming message creation time is "{6}", configured agent expiry is {5} seconds, incoming message expiry is {7} seconds, effective message expiry (minimum of agent expiry and incoming message expiry) is {4} seconds, configured clock skew is {3} seconds. The acceptable time range is "{1}" to "{2}". The incoming message is outside the valid range as allowed by clock skew and expiry times.

Category:
Security

Cause:
The incoming message is outside the valid range as allowed by clock skew and expiry times.

Action:
Adjust times on servers/clients. Check the allowed clockskew and message expiration time and configure them as required.

WSM-00256
The property "{0}" is not set. The csf maps that are used to retrieve property are:- "{1}". The properties found in the JPS config are <PropertyName: Value>:- {2}

Category:
Security

Cause:
The property value is null.

Action:
Make sure that the value provided either through policy configuration override, policy binding, or domain level configuration is not null.

WSM-00257
Callback class name "{0}" set for SAML certificate validation not found

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Security

Cause:
Callback class set for SAML certificate validation not found.

Action:
Make sure that callback class name is correct and added in classpath.

WSM-00258
Callback class name "{0}" set for SAML certificate validation is invalid.

Category:
Security

Cause:
Callback class set for SAML certificate validation is not valid.

Action:
Make sure that callback class correctly extends required class.

WSM-00259
SAML certificate validation callback failed. {0}.

Category:
Security

Cause:
Callback class set for SAML certificate validation failed.

Action:
Check the error message for details.

WSM-00260
SAML over SSL certificate validation failed because certificate returned from callback and actual certificate differ. Actual certificate DN={0} and callback cert DN={1}

Category:
Security

Cause:
SAML over SSL certificate validation failed because certificate returned from callback and actual certificate differ.

Action:
Make sure that client certificate sent over SSL and certificate returned from callback are same.

WSM-00261
SAML certificate validation callback failed because certificate returned from callback is NULL.

Category:
Security

Cause:
Callback class set for SAML certificate validation failed because certificate returned from callback is NULL.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Check callback implementation class for the reason of null certificate.

WSM-00262
SAML assertion with confirmation method {0} is missing inside signature.

Category:
Security

Cause:
SAML assertion is missing inside signature.

Action:
Ensure that SAML assertion has required inside signature.

WSM-00263
Failed to create SAML token as 'anonymous' user principal found in Subject.

Category:
Security

Cause:
Failed to create SAML token as 'anonymous' user principal found in Subject.

Action:
Make sure that the subject is created from a valid user.

WSM-00264
Must Understand check failed for headers: "{0}" in the SOAP message.

Category:
Security

Cause:
Unprocessed 'mustUnderstand' header element in SOAP message.

Action:
Make sure that you have attached security policy at service side.

WSM-00265
The Username token is missing in the security header. Ensure that there is a Username token policy attached on the client side. Tokens found in the security header are :- {0}.

Category:
Security

Cause:
Username token was expected in the security header but was not found.

Action:
Username token is missing. Resend request with valid username token.

WSM-00266
The Kerberos token is missing in the security header.

Category:
Security

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
Kerberos token was expected in the security header but was not found.

Action:
Resend request with valid kerberos token.

WSM-00267
Authentication token specified in the policy for re-authenticate in secure conversation is not supported. Only SAML token is supported currently.

Category:
Configuration

Cause:
Authentication token specified in the policy for re-authenticate in secure conversation is not supported.

Action:
Only SAML token is supported as of now.

WSM-00268
The certificate to be validated is NULL.

Category:
Security

Cause:
The certficate to be validated is null.

Action:
Make sure that the certificate to be validated is not null.

WSM-00269
There is no trusted certificate found in the trust store.

Category:
Security

Cause:
Trust store does not have any trusted certificate.

Action:
Make sure that the required trusted certificates are present in the trust store.

WSM-00270
The issuer "{0}" is not found in the trust store.

Category:
Security

Cause:
The issuer certificate is not present in the trust store.

Action:
Make sure that the issuer certificate is present in the trust store.

WSM-00271
Basic constraints check failed due to the certificate "{0}" is not a CA certificate.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Security

Cause:
The certificate is not a CA certificate.

Action:
Make sure that the issuer certificate is a CA certificate.

WSM-00272
Basic Constraints check failed for the certificate "{0}", since only an end-entity certificate may follow this certificate in the certification path chain.

Category:
Security

Cause:
Basic Constraints check failed for the issuer certificate.

Action:
Make sure that the issuer certificate is a valid.

WSM-00273
Failed to verify the issuer "{0}".

Category:
Security

Cause:
The issuer certificate verification failed.

Action:
Check error logs for more details.

WSM-00274
The certification path for the certificate "{0}" is NULL.

Category:
Security

Cause:
The certification path is found to be null.

Action:
Check error logs for more details.

WSM-00275
The Identity type "{0}" is not supported.

Category:
Security

Cause:
The Identity type published in the WSDL certificate is not supported.

Action:
Make sure that the identity type published in the WSDL certificate is either X509Certificate or supported one.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-00276
Validation failed for the identity published in the WSDL endpoint "{1}". Caused By: {0}

Category:
Security

Cause:
Validation failed for the Identity published in the WSDL certificate.

Action:
Check error logs for more details.

WSM-00277
Endorsing signature is not found in the message. Ensure that a compatible policy is attached at the client side. The security policy "{1}" is attached to the service. Tokens found in the security header are :- {0}.

Category:
Security

Cause:
Endorsing signature is expected in the message but not found.

Action:
Make sure that the endorsing signature is included in the message.

WSM-00278
Failed to decrypt the encrypted key due to {1}. Ensure that the client is properly configured with the server certificate. Client should be using this certificate:- {0}.

Category:
Security

Cause:
An error occurred while decrypting the encrypted key.

Action:
Ensure that the client is properly configured with the server's certificate.

WSM-00279
The following Fault Message is received at the client side from the service:- {0}. The client side policy is:- {4}. The service endpoint url is:- {3}. Keystore properties:- {1}. Properties found in the message context (Partial list):- {7}. PolicyReference OverrideProperty: {6} Policy configuration properties (some of these may be overridden by the properties passed in the PolicyReference or message context, for details about the order of precedence of properties consult documentation):- {5}. Other related information:- {2}.

Category:
Security

Cause:
Fault Message received at the client side from the service

Action:
Check the log file for possible causes.

WSM-00280
Caching of STS client executor failed which is required for secure conversation.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Security

Cause:
Caching of STS client executor failed which is required for se cure conversation.

Action:
Check error logs for more details.

WSM-00281
Failed to calculate session id for user {0}, due to {1}

Category:
Security

Cause:
Failed to calculate session id for user.

Action:
Check error logs for more details.

WSM-00282
Failed to calculate session id for user {0} because required credential "{1}" is NULL.

Category:
Security

Cause:
Failed to calculate session id because required credential is NULL.

Action:
Make sure that all required credentials are set.

WSM-00283
Failed to create token context required for secure conversation due to {0}

Category:
Security

Cause:
Failed to create token context which is required for secure conversation.

Action:
Check logs for finding out exact reason of failure.

WSM-00284
Failed to send secure conversation bootstrap request.

Category:
Security

Cause:
Failure occurred while trying to send secure conversation bootstrap request message, possibly due to a failure in security code.

Action:
Check logs for finding out exact reason of failure.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-00285
Failed to issue secure conversation token due to : {0}.

Category:
Security

Cause:
Failed to issue secure conversation token.

Action:
Check logs for finding out exact reason of failure.

WSM-00286
Failed to renew secure conversation token.

Category:
Security

Cause:
Failed to renew secure conversation token.

Action:
Check logs for finding out exact reason of failure.

WSM-00287
Failed to cancel secure conversation token.

Category:
Security

Cause:
Failed to cancel secure conversation token.

Action:
Check logs for finding out exact reason of failure.

WSM-00288
SecurityContextToken required for secure conversation not found. You might have not enabled secure conversation on other side.

Category:
Security

Cause:
SecurityContextToken required for secure conversation not found.

Action:
Make sure that valid SCT is used for signing and encryption of message. You might have not enabled secure conversation on other side.

WSM-00289
SecurityContextToken version used for secure conversation is not matching with expected version. Expected : {0} but found namespace: {1}

Category:
Security

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
SecurityContextToken version used for secure conversation is not matching with expected version.

Action:
Check documentation for supported WS Secure conversation version.

WSM-00290
SecurityContextToken version "{0}" used for secure conversation is not supported.

Category:
Security

Cause:
SecurityContextToken version used for secure conversation is not supported.

Action:
Check documentation for supported WS Secure conversation version.

WSM-00291
Failed to add addressing header to the secure conversation bootstrap message.

Category:
Security

Cause:
Failed to add addressing headers when creating secure conversation bootstrap message.

Action:
Check logs for finding out exact reason of failure.

WSM-00292
sc.lifetime property value given in secure conversation policy is not valid.

Category:
Security

Cause:
sc.lifetime property value "{0}" given in secure conversation policy is not valid.

Action:
sc.lifetime should have valid integer value.

WSM-00293
sc.lifetime property value given in domain configuration is not valid.

Category:
Security

Cause:
sc.lifetime property value "{0}" given in domain configuration is not valid.

Action:
sc.lifetime should have valid integer value.

WSM-00294
Secure Conversation token inclusion mechanism is not supported: {0}

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Security

Cause:
Secure Conversation token inclusion mechanism is not supported.

Action:
Make sure to use supported token inclusion mechanism.

WSM-00295
Secure Conversation session has expired for SCT ID: {0}

Category:
Security

Cause:
Secure Conversation session has expired for SCT ID.

Action:
Renew session.

WSM-00296
Secure Conversation session not found in session manager for SCT ID: {0}

Category:
Security

Cause:
Secure Conversation session not found in session manager for SCT ID.

Action:
Check logs for the exact reason.

WSM-00297
Security Context Token in RSTR is null

Category:
Security

Cause:
Security Context Token in RSTR is null.

Action:
Check logs for the exact reason.

WSM-00298
Policy Reference URI(s) passed to dispatcher is empty.

Category:
Security

Cause:
Policy Reference URI(s) passed to dispatcher is empty.

Action:
Check logs for the exact reason.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-00299
Exception is thrown by the Session Manager

Category:
Security

Cause:
Exception is thrown by the Session Manager.

Action:
Check logs for the exact reason.

WSM-00300
Invalid input to the Session Manager on {0}.

Category:
Security

Cause:
Invalid input to Session Manager.

Action:
Check logs for the exact reason.

WSM-00301
Error in creating session id since the reference resource pattern is null

Category:
Security

Cause:
Error in creating session id since the reference resource pattern is null

Action:
Check logs for the exact reason.

WSM-00302
Error in creating session id since the service URL in message context is null

Category:
Security

Cause:
Error in creating session id since the service URL in the message context is null

Action:
Check logs for the exact reason.

WSM-00303
Secure conversation is unsupported for the assertion {0}. The policy file should be checked to not have secure conversation "on" for this assertion.

Category:
Security

Cause:
Secure conversation is unsupported for this assertion.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Check your policy

WSM-00304
Message does not contain client entropy which is required by service policy.

Category:
Security

Cause:
Message does not contain client entropy while server policy requires it.

Action:
Check your client policy and make sure require-client-entropy is enabled on it.

WSM-00305
Session ID "{0}" removed from session manager because BadContextToken received. This happens because SecurityContextToken sent from client is not accepted by service which can be due to the time difference between client and service being more than configured clock skew and it can also happen if service is not using session persistence while client is.

Category:
Security

Cause:
BadContextToken fault received which is due to invalid or expired SecurityContextToken (SCT). This happens because SCT sent from client is not accepted by service which can be due to the time difference between client and service being more than configured clock skew and it can also happen if service is not using session persistence while client is.

Action:
Replay message again which will go through fine because dead session has been cleaned. Make sure that client and server clocks are synchronized properly or set correct clock skew. Also make sure that server and client are both configured with compatible session manager providers.

WSM-00306
The derived keys security token could not be obtained from the message.

Category:
Security

Cause:
The Derived keys could not be located

Action:
Either turn off the use-derived-keys flag or provide the derived keys in the message.

WSM-00307
Client Credential did not get delegated to the Service.

Category:
Security

Cause:
Client Credential did not get delegated to the Service.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Make sure the Kerberos configuration file on the client supports credential delegation.

WSM-00308
Conflicting client credential available from Config-Override and Credential Delegation.

Category:
Security

Cause:
Conflicting client credential available from Config-Override and Credential Delegation.

Action:
Either remove the client side config-overrides for Caller Principal Name and Keytab location or disable credential delegation.

WSM-00309
HTTP SPNEGO Authorization Header is missing in the request.

Category:
Security

Cause:
HTTP SPNEGO Authorization Header is missing in the request.

Action:
Client must provide a valid Authorization header for SPNEGO.

WSM-00310
Client Credential not available.

Category:
Security

Cause:
Client Credential not available.

Action:
Either provide caller principal name and keytab location or enable credential delegation if appropriate.

WSM-00311
SAML over HTTP authentication failure.

Category:
Security

Cause:
Failure occurred in SAML over HTTP authentication.

Action:
Use the appropriate GZIP and Base64 encoded combination of a valid SAML.

WSM-00312
Keystore reloading failed due to {0}

Category:
Security

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
Reloading of the keystore failed.

Action:
Restart the server to load the latest keystore.

WSM-00313
Could not obtain the certificate for the corresponding thumbprint

Category:
Security

Cause:
The certificate for the corresponding SKI could not be obtained

Action:
Add the certificate to the Keystore.

WSM-00314
The Xpath transformation of the type "{0}" is not allowed. Only Xpath transformations of the type "{1}" are allowed. To allow all the Xpath transformations, set the property "{2}" to true.

Category:
Security

Cause:
The Xpath transformation present in the incoming SOAP message is not supported.

Action:
Make sure that incoming SOAP message contains only supported Xpath expressions, see the exception stack trace for details.

WSM-00315
The details of the keystore {0} removed from the system.

Category:
Security

Cause:
Removing the keystore details as keystore was replaced with a wrong one.

Action:
Replace the keystore with a valid one. After keystore has been replaced, it will be reloaded on next invocation.

WSM-00316
The CSF key "{0}" is reserved and can not be used for username credentials. Ensure that the reserved CSF key {1} is not used.

Category:
Security

Cause:
The CSF key being used is reserved and can not be used for username credentials.

Action:
Ensure that the reserved CSF keys are not used. Check error logs for more details.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-00317
Required OES resource string is incomplete: application: {0}, resource_type: {1}, resource_name: {2}

Category:
Security

Cause:
Required OES resource string is incomplete.

Action:
Ensure that all components of resource string is available either dynamially or using config overrides.

WSM-00318
Required OES resource string is null because required resource pattern is null.

Category:
Security

Cause:
Required OES resource string is null because resource patterns is null.

Action:
Ensure that resource pattern is available which is passed from web service stack.

WSM-00319
Error while populating attributes for OES authorization. Actual error message is: {0}

Category:
Security

Cause:
Error occured while populating attributes for OES authorization.

Action:
Check logs for actual cause of error.

WSM-00320
PEPException has occurred while making authorization call to PDP using PEP API.

Category:
Security

Cause:
Error occured while invoking OES's authorization engine using PEP API.

Action:
Check logs for actual cause of PEP APIs failure.

WSM-00321
XPath attributes configured for fine-grained authorization will be ignored because no valid XML message found in current payload.

Category:
Security

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
XPath attributes are being ignored because no SOAP message or XML msg found in current payload.

Action:
SOAP message should have valid envelope or if its SOA then XML request message should be available.

WSM-00322
Error occurred while evaluating XPath query. XPath query will be ignored. Specific error is: {0}

Category:
Security

Cause:
Error while evaluating XPath query. Query is being ignored.

Action:
Check logs if there is any error or XPath query may not be valid for current XML payload.

WSM-00323
STS {0} obtained from WSDL is {1}. Local STS configuration is also not available.

Category:
Security

Cause:
STS (issuer) uri is not available in the WSDL or client side STS configuration.

Action:
Ensure that STS trust config policy is attached to either the client or the service.

WSM-00324
Automatic (Client) Policy Configuration failed to determine a compatible client side policy to communicate with the STS at {0}.

Category:
Security

Cause:
Automatic (Client) Policy Configuration failed to determine compatible client side policy to communicate with STS.

Action:
Ensure that STS trust config service policy is attached and is configured with the correct issuer uri.

WSM-00325
The protocol "{0}" set in the token configuration for the token to be cached is not recognized. If the problem persists, contact Oracle Support Services.

Category:
Security

Cause:
The protocol set in the token configuration for the token to be cached is not recognized.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
If the problem persists, contact Oracle Support Services.

WSM-00326
The client clock skew value should not be negative

Category:
Security

Cause:
Invalid client clock skew value.

Action:
Change client clock skew to a positive value.

WSM-00327
Incoming request did not have a valid authentication token. Service will send a 401 Challenge in response to the client with WWW-Authenticate header.

Category:
Security

Cause:
Incoming request did not have a valid authentication token.

Action:
Service will send a 401 Challenge in response to the client. Client should understand the authentication scheme and re-send the request with required token.

WSM-00328
The XPath expression {0} is not valid.

Category:
Security

Cause:
The XPATH expression could not be evaluated for the SOAP/XML Message. It could be because the xpath is not following xpath syntax.

Action:
THe XPATH expression is not valid, correct the XPATH and try again.

WSM-00329
The PII for the xpath {0} to be encrypted is already encrypted.

Category:
Security

Cause:
The PII Node to be encrypted is already encrypted. It could be because the same XPATH is being used twice or the message already had PII encrypted

Action:
Check if the same XPATH is being used again. There is some place where the PII policy should have been attached but was not attached properly.

WSM-00330
The XPATH {0} used to configure the PII does not result in TEXT_NODE.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Security

Cause:
The PII Xpath did not return a TEXT_NODE. If the Xpath does not return a TEXT_NODE then it is not a Supported XPATH

Action:
Rectify the XPATH configured for the PII so that it returns a TEXT_NODE.

WSM-00331
The key used to encrypt/decrypt PII could not derived.

Category:
Security

Cause:
The Secret Key for PII could not be derived. The policy is not configured properly

Action:
Rectify the PII configuration so that the secret key can be generated.

WSM-00332
The resource pattern is not configured properly.

Category:
Security

Cause:
The Resource Pattern is null.

Action:
The ResourcePattern should be properly configured.

WSM-00333
The PII policy is not supported on the SubjectType: {0}

Category:
Security

Cause:
PII Policy not supported on this SubjectType.

Action:
Dettach the PII policy from this subject as it is not supported here.

WSM-00334
The PII denoted by xpath {0} was encrypted in {1}, but was being decrypted in {2}, which is not allowed.

Category:
Security

Cause:
PII encrypted in one entity and decrypted in a different entity.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Attach the decrypt policy in the earlier entity, so that PII gets decrypted in the same entity where it was encrypted.

WSM-00335
Anonymous user found in the SAML assertion so anonymous subject has been created. Trusted issuers validation, DN list validation and other validations related to SAML token will be skipped. Subject: {0}

Category:
Security

Cause:
Anonymous user found in the SAML assertion so anonymous subject has been created. Trusted issuers validation, DN list validation and other validations related to SAML token will be skipped.

Action:
If anonymous user was not expected in token then check client's configuration.

WSM-00336
Anonymous user is being propagated as subject is {0}.

Category:
Security

Cause:
Anonymous user is being propagated as subject is either NULL or anonymous.

Action:
Check client's configuration if anonymous user should not be propagated.

WSM-00338
Error creating OPSS subject from username and policy context.

Category:
Security

Cause:
A failure occurred while creating OPSS subject from username and policy context.

Action:
Check log file for possible cause.

WSM-00339
Error creating anonymous subject.

Category:
Security

Cause:
A failure occurred while creating anonymous subject.

Action:
Check log file for possible cause.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-00340
The key for the alias {0} not found in the KSS Keystore {1}. The following aliases are found in the Keystore: {2}

Category:
Configuration

Cause:
Key does not exist in the KSS keystore.

Action:
Ensure that alias exists in keystore and necessary permission to read key alias is granted.

WSM-00341
SAML assertion signature digest verification failed

Category:
Security

Cause:
SAML assertion signature verification failed.

Action:
Ensure that SAML assertion signature is valid.

WSM-00342
Certificate/Key with subject DN "{0}" has expired.

Category:
Security

Cause:
Certificate/Key has expired.

Action:
Get a new certificate/key.

WSM-00343
Could not get new Kerberos TGT and current TGT has expired.

Category:
Security

Cause:
Could not get new Kerberos TGT and current TGT has expired.

Action:
Check logs for the reason of failure. Principal and password (for example using keytab) must be available for login.

WSM-00344
Failed to authorize user request for {0}. {1}

Category:
Security

Cause:
Failed to authorize user request.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Check logs for the reason of failure and also check if required premission is granted.

WSM-00345
Failed to decrypt the encrypted key at client side due to {0}. Ensure that the client is configured with sign key as crypt key.

Category:
Security

Cause:
An error occurred while decrypting the encrypted key at client side.

Action:
Ensure that the client is configured with the sign key as crypt key.

WSM-00346
There is no matching assertion found in the service side policy which can process the incoming message. Ensure that there is a compatible policy attached at the client side. Tokens found in the security header are:- {0}. Authentication mechanism found in the HTTP header:- {1}. The assertions found in the service side policy are:- {2}.

Category:
Security

Cause:
No matching assertion found in the service side policy which can process the incoming message.

Action:
Ensure that a compatible client policy is attached and enabled at the client side.

WSM-00347
The request message contains the Derived Keys but service side policy is not configured to use Derived Keys for message decryption. Ensure that the service side policy is configured to use Derived Keys.

Category:
Security

Cause:
The request message contains the Derived Keys but service side policy is not configured to use Derived Keys for message decryption.

Action:
Ensure that the service side policy is configured to use Derived Keys.

WSM-00348
EncrytpedData element found inside the ReferenceParameters element. This might result in security vulnerabilities, so removing its data reference "{0}" from the reference list to avoid decryption of any EncrytpedData element inside the ReferenceParameters element. Ensure that the entire ReferenceParameters element is either encrypted or without any EncrytpedData element.

Category:
Security

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
EncrytpedData element found inside the ReferenceParameters element. This might result in security vulnerabilities.

Action:
Ensure that the entire ReferenceParameters element is either encrypted or without any EncrytpedData element.

WSM-00349
The HTTP header is missing in the incoming client request message. Service will send back a 401 Challenge to the client with response header {0}: {1}.

Category:
Security

Cause:
Incoming request did not have any authentication token in the HTTP header.

Action:
Service will send back a 401 Challenge to the client. Client should understand one of the authentication schemes and re-send the request with one of the supported authentication token.

WSM-00350
The name attribute for the token issuer trust document is not found.

Category:
Security

Cause:
The name attribute for the token issuer trust document is not found.

Action:
Make sure the name is provided when creating a token issuer trust document.

WSM-00351
The tokentype attribute "{0}" for the Issuer in token issuer trust document is not supported.

Category:
Security

Cause:
The tokentype attribute for the Issuer in the token issuer trust document is not supported.

Action:
Change it to a supported token type when creating the Issuer in token issuer trust document.

WSM-00352
The keytype attribute "{0}" for a trusted key for an Issuer in the token issuer trust document is not supported.

Category:
Security

Cause:
The keytype attribute for a trusted key for an Issuer in the token issuer trust document is not supported.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Change it to a supported key type when creating the trusted key for the Issuer in token issuer trust document.

WSM-00353
The valuetype attribute "{0}" for a trusted key for an Issuer in the token issuer trust document is not supported.

Category:
Security

Cause:
The valuetype attribute for a trusted key for an Issuer in the token issuer trust document is not supported.

Action:
Change it to a supported key valuetype when creating the trusted key for the Issuer in token issuer trust document.

WSM-00354
The attribute "{0}" for which the filter is configured in a token attribute rule is not supported.

Category:
Security

Cause:
The attribute for which the filter is configured in a token attribute rule is not supported.

Action:
Set the filter only for supported attributes in a token attribute rule.

WSM-00355
Name Id "{0}" in the token is not allowed by the token attribute rule for the DN "{1}".

Category:
Security

Cause:
Token Name ID validation for the DN failed.

Action:
Name ID value is not allowed for the DN of token signing certificate. Make sure a valid user is sent.

WSM-00356
Failed to enforce token attribute rule "{0}" configured for the DN "{1}" of the signing certificate.

Category:
Security

Cause:
Token attribute rule configured for the DN of the signing certificate failed.

Action:
Check logs for the details. Either rule is not configured properly or token does not has required details to enforce it.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-00357
Token attribute rule identifier "{0}" is not associated with any trusted key of a trusted token issuer.

Category:
Security

Cause:
Token attribute rule identifier "{0}" is not assocoated with any trusted key of a trusted token issuer.

Action:
Check the identifier to make sure it matches the key identifier value of a trusted key for an trusted issuer configured.

WSM-00358
SAML assertion signature reference is pointing to invalid URI

Category:
Security

Cause:
SAML assertion signature reference is pointing to invalid URI .

Action:
Ensure that SAML assertion signature is valid

WSM-00359
Instance tenancy is not available but used as property value: "{0}"

Category:
Security

Cause:
Instance tenancy is not available.

Action:
Make sure that instance tenancy is available or don't use that property if not required.

WSM-00360
Tenant name set in configuration property "{0}" does not match with tenancy: "{1}" of current subject.

Category:
Security

Cause:
Tenant name set in configuration property does not match with current subject's tenancy.

Action:
Make sure that tenant name set as configuration property matches with current subject's tenant name.

WSM-00361
The SAML HOK token found in the incoming message does not contain the KeyInfo element. Make sure that the incoming message contains a valid SAML HOK assertion and contains the KeyInfo element.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Security

Cause:
The SAML HOK assertion found in the incoming message does not contain the KeyInfo element.

Action:
Insert valid SAML HOK assertion containing the KeyInfo element and resend the request.

WSM-00362
The SAML HOK token found in the incoming message does not contain the KeyValue element. Make sure that the incoming message contains a valid SAML HOK assertion and contains the KeyValue element.

Category:
Security

Cause:
The SAML HOK token found in the incoming message does not contain the KeyValue element.

Action:
Insert valid SAML HOK token containing the KeyValue element and resend the request.

WSM-00363
The SAML token found in the incoming message is not valid. Both AttributeStatement and AuthenticationStatement elements are missing from the SAML assertion.

Category:
Security

Cause:
The SAML token found in the incoming message is not valid. Both AttributeStatement and AuthenticationStatement elements are missing from the SAML assertion.

Action:
Insert valid SAML token and resend the request.

WSM-00364
JWT token has expired

Category:
Security

Cause:
JWT token received after the token has expired.

Action:
Fix the expiry claim and retry the operation.

WSM-00365
JWT token issuer - "{0}" is not trusted. Configured trusted issuers are "{1}"

Category:
Security

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
JWT token issuer is not trusted.

Action:
Fix the issuer claim and retry the operation.

WSM-00366
JWT symmetric key "{0}" is not trusted

Category:
Security

Cause:
JWT key id is not trusted.

Action:
Fix the symmetric key and retry the operation.

WSM-00367
JWT certificate DN "{0}" is not trusted

Category:
Security

Cause:
JWT certificate DN is not trusted.

Action:
Fix the JWT certificate and retry the operation.

WSM-00368
JWT x5t claim is invalid

Category:
Security

Cause:
Cannot find certificate matching the JWT x5t claim.

Action:
Fix the JWT x5t claim and retry the operation.

WSM-00369
JWT signature csf key is not configured

Category:
Configuration

Cause:
Cannot find JWT signature csf key.

Action:
Fix the JWT signature csf key and retry the operation.

WSM-00370
JWT token is not signed

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Security

Cause:
JWT token is not signed.

Action:
Sign the JWT token and retry the operation.

WSM-00371
JWT signature algorithm mismatch, expecting "{0}", found "{1}"

Category:
Security

Cause:
JWT signature algorithm does not match policy.

Action:
Fix the JWT signature algorithm and retry the operation.

WSM-00372
Unsupported signature algorithm specified

Category:
Security

Cause:
An unsupported signature algorithm was provided.

Action:
Consult the documentation for the supported signature algorithms and retry the operation.

WSM-00373
JWT audience claim - "{0}" is invalid. Audience conditions are not satisfied. "{1}"

Category:
Security

Cause:
JWT audience claim is invalid

Action:
Fix the audience claim to match the resource and retry the operation.

WSM-00374
JWT issued time claim is invalid

Category:
Security

Cause:
JWT token received before the issued time.

Action:
Fix the issued time claim and retry the operation.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-00375
Unable to determine user tenant name in multi-tenant environment

Category:
Security

Cause:
Unable to determine user tenant name in multi-tenant environment.

Action:
Ensure that the user tenant name is set.

WSM-00376
SAML token authentication failed for issuer "{0}"

Category:
Security

Cause:
SAML token based authentication failed.

Action:
SAML token based authentication failed. Check logs for more details.

WSM-00377
{0}. This error is most likely due to secure conversation not enabled at the service side policy

Category:
Security

Cause:
Secure conversation is not enabled at the service side policy.

Action:
Disable secure conversation at the client side policy and try again.

WSM-00378
Incoming Kerberos token has an invalid/unsupported Value Type: {0} : {1}

Category:
Security

Cause:
The value type of the incoming Kerberos token did not match the expected type at service side.

Action:
Make sure client sends the Kerberos token of value type as expected by service policy.

WSM-00379
There are no Xpath transformations allowed inside CipherReference in EncryptedKey. To allow all the Xpath transformations, set the property {0} to true.

Category:
Security

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
No Xpath transformations are supported inside CipherReference in EncryptedKey which are present in the incoming SOAP message.

Action:
Do not include any XPATH transformations inside CipherReference

WSM-00380
An Exception was thrown while retreiving the keystore password from the credential store.

Category:
Security

Cause:
The Keystore password was not retrieved

Action:
Check if the keystore password is configured correctly.

WSM-00381
Alias "{0}" is not valid for the keystore entry.

Category:
Security

Cause:
Alias doesn't point to any trusted certificate or a private key entry.

Action:
Ensure that alias either points to any trusted certificate or a private key entry and retry the operation.

WSM-00382
An Exception was thrown while loading the keystore, only JKS type keystores are supported by the oracle.wsm.security.store.jks.mgmt.KeystoreMBean.

Category:
Configuration

Cause:
Keystore MBean only support JKS type keystore.

Action:
Consult the oracle documentation to ensure that keystore.type that is configured is of type JKS for the oracle.wsm.security.store.jks.mgmt.KeystoreMBean.

WSM-00383
Failed to initialize JKS Mbean auditor.

Category:
Security

Cause:
An internal error occurred; failed to initialize the auditor.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-00384
Alias "{0}" points to a certificate which is not a trusted certificate.

Category:
Security

Cause:
Alias already exists but does not identify an entry containing a trusted certificate.

Action:
Check that a trusted certificate already exists for the given alias and retry the operation.

WSM-00385
Alias "{0}" does not point to a valid private key entry in the keystore.

Category:
Security

Cause:
Alias doesn't point to a private key entry.

Action:
Ensure that alias points to a private key entry in the keystore.

WSM-00386
Invalid type argument "{0}". Valid values are "Certificate" and "PKCS7".

Category:
Security

Cause:
Invalid type argument. Valid values are "Certificate" for single certificate and "PKCS7" for certificate chain.

Action:
Ensure that either "Certificate" or "PKCS7" is passed as type argument.

WSM-00387
No trusted certificate identified by alias "{0}".

Category:
Security

Cause:
No trusted certificate entry identified by the alias.

Action:
Ensure that alias points to a trusted certificate and retry the operation.

WSM-00388
Certificate deletion failed for "{0}" alias(es).

Category:
Security

Cause:
An error occurred while deleting the alias.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

WSM-00389
Public key entry of the certificate to be imported does not match the existing public key entry in the keystore for alias "{0}".

Category:
Security

Cause:
The public key in the certificate does not match the one in the keystore.

Action:
Ensure that the certificate is imported into the alias used for generating certificate request.

WSM-00390
Failed to retrieve Private key entry for alias "{0}" due to invalid password.

Category:
Security

Cause:
Failed to retrieve private key entry due to invalid password.

Action:
Ensure that correct password is used to import/set the certificate.

WSM-00391
Creating certificate from base64 encoded string failed for alias "{0}".

Category:
Configuration

Cause:
Encountered error while creating certificate from base64 encoded string.

Action:
Must provide valid certificate in valid base64 encoded string.

WSM-00392
Failed to store keystore to the file system.

Category:
Configuration

Cause:
Encountered error while storing the keystore to the file system.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

WSM-00393
Permission "{0}" required to access the application specific CSF map "{1}" is not granted to the resource "{2}". Underlying exception message : "{3}"

Category:
Security

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
Permission required to access application specific credential map is not granted.

Action:
Grant permission for accessing application specific credential map to the codesource and retry the operation.

WSM-00394
The given name "{0}" for permission "{1}" with action "{2}" is not supported target format. If action is "assert", supported target format is resource={RESOURCENAME}. If action is "getKey", supported target format is resource={RESOURCENAME},mapName={CSF_MAP_NAME}.

Category:
Security

Cause:
The target format of the specified WSIdentityPermission is not supported.

Action:
Correct the supported target terms for WSIdentityPermission and retry the operation.

WSM-00395
The action "{0}" is not supported for permission "{1}".

Category:
Security

Cause:
The action of the specified WSIdentityPermission is not supported.

Action:
Correct the supported actions for WSIdentityPermission and retry the operation.

WSM-00396
JKS "{0}" audit operation failed.

Category:
Configuration

Cause:
Encountered error while auditing JKS operation.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

WSM-00397
JKS Mbean registration failed.

Category:
Security

Cause:
JKS Mbean registration failed.

Action:
Check logs for actual cause of Mbean registration failure.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-00398
The OAuth2 policy configuration property token-uri has an invalid value of "{0}". The value must point to a valid Oauth token endpoint and should be specified in the form "http(s)://host:port/tokens"; it should not be a null or empty string.

Category:
Configuration

Cause:
OAuth2 config attribute token-uri is either null, empty or not in the format of "http(s)://host:port/tokens".

Action:
Provide valid attribute value for Oauth token endpoint which is in the format of "http(s)://host:port/tokens".

WSM-00399
OAuth2 request sent to OAuth2 server failed with Message : "{0}". Please check OAuth2 server logs for more details.

Category:
Security

Cause:
OAuth2 token request failed

Action:
Check the OAuth2 Server logs and exception stack trace to determine why the request failed.

WSM-00400
OAuth2 server responded with status : "{0} {1}", error : "{2}". Please check OAuth2 server logs for more details. Additional info: Token URI - "{3}", Client ID - "{4}", Scope - "{5}".

Category:
Security

Cause:
OAuth2 server responded with error message and bad request

Action:
Check the error message returned by OAuth2 server to determine why the request was rejected.

WSM-00401
JWT signature verification failed.

Category:
Security

Cause:
JWT Signature verification failed

Action:
Fix the JWT token or import the right trusted issuer certificate and retry the operation.

WSM-00402
JWT kid "{0}" claim is not valid. Certificate mathcing the kid claim does not exist in OWSM trust store.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Security

Cause:
Cannot find certificate matching the JWT kid claim.

Action:
Fix the JWT kid claim or import the certificate in OWSM trust store and retry the operation.

WSM-00403
oauth2_config_client_policy is not found. Attach it using GPA or LPA.

Category:
Configuration

Cause:
The oauth2_config_client_policy is not attached.

Action:
Check the configuration and attach oauth2_config_client_policy using GPA or LPA.

WSM-00404
Provide valid value for oauth2.client.csf.key config override.

Category:
Configuration

Cause:
oauth2.client.csf.key config override is missing.

Action:
Provide valid value for oauth2.client.csf.key after adding entry in CSF.

WSM-00405
Add a CSF entry with client id

Category:
Configuration

Cause:
oauth2.client.csf.key config override does not point to a valid entry

Action:
Add an entry in CSF corresponding to oauth2.client.csf.key.

WSM-00406
Configured redirect.uri = "{0}" is invalid .Configure a valid redirect.uri value for 3-legged OAuth

Category:
Configuration

Cause:
redirect.uri config override does not point to a valid value

Action:
Configure redirect.uri in the config override

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-00407
Invalid policy alternatives found inside XOR policy operator. It contains two or more message protection assertions ({0}, {1}) which have same authentication token type.

Category:
Configuration

Cause:
Invalid policy alternatives found inside XOR policy operator. It contains two or more message protection assertions which have same authentication token type.

Action:
Ensure that you have only one message protection assertion with same authentication token type in the XOR policy

WSM-00408
Invalid policy alternatives found inside XOR policy operator. It contains two or more non message protection or SSL assertions ({0}, {1}) which have same authentication token type.

Category:
Configuration

Cause:
Invalid policy alternatives found inside XOR policy operator. It contains two or more non message protection or SSL assertions which have same authentication token type.

Action:
Ensure that you have only one non message protection assertion with same authentication token type in the XOR policy

WSM-00409
Invalid policy alternatives found inside XOR policy operator. It contains more than one of x509, anonymous or custom authentication token type ({0}, {1}).

Category:
Configuration

Cause:
Invalid policy alternatives found inside XOR policy operator. It contains more than one of x509, anonymous or custom authentication token type.

Action:
Ensure that you have only one of either x509, anonymous or custom authentication token types in the XOR policy

WSM-00410
Invalid policy alternatives found inside XOR policy operator. It contains two or more secure conversation enabled message protection assertions ({0}, {1}) which have same authentication token type.

Category:
Configuration

Cause:
Invalid policy alternatives found inside XOR policy operator. It contains two or more secure conversation enabled message protection assertions which have same authentication token type.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Ensure that you have only one secure conversation enabled message protection assertion with same authentication token type in the XOR policy

WSM-00411
Invalid policy alternatives found inside XOR policy operator. It contains two or more secure conversation enabled SSL assertions ({0}, {1}) which have same authentication token type.

Category:
Configuration

Cause:
Invalid policy alternatives found inside XOR policy operator. It contains two or more secure conversation enabled SSL assertions which have same authentication token type.

Action:
Ensure that you have only one secure conversation enabled SSL assertion with same authentication token type in the XOR policy

WSM-00412
Invalid policy alternatives found inside XOR policy operator. It contains more than one secure conversation enabled assertion with either x509, anonymous or custom authentication token types ({0}, {1}).

Category:
Configuration

Cause:
Invalid policy alternatives found inside XOR policy operator. It contains more than one secure conversation enabled assertion with x509, anonymous or custom authentication token type.

Action:
Ensure that you have only one secure conversation enabled assertion with either x509, anonymous or custom authentication token types in the XOR policy

WSM-00413
Invalid policy alternatives found inside XOR policy operator. It contains two or more message protection assertions which have different values for keystore.enc.csf.key ({0}, {1}).

Category:
Configuration

Cause:
Invalid policy alternatives found inside XOR policy operator. It contains two or more message protection assertions which have different values for keystore.enc.csf.key property.

Action:
Ensure that you have same value for keystore.enc.csf.key for all message protetcion assertions

WSM-00414
DMS string not available in ClientConfig properties. Setting dummy value for OWSM agent initialization. Monitoring will not work for subject identified by {0}

Category:
Security

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
DMS string not available in ClientConfig properties.

Action:
Set the WSMExecutionConstants.AGENT_TOPOLOGYNODE_PATH proeprty with a String value in the ClientConfig object of the Jersey Client.

WSM-00415
The value of algorithm suite,"{0}" used in the JWT assertion is not valid. The only valid value to be used is "{1}".

Category:
Security

Cause:
The algorithm suite specified in the policy is not supported by JWT policies. Only Asymmetric key signature is supported at this time.

Action:
Make sure that a valid value of algorithm-suite is provided in the JWT assertion.

WSM-00416
The current server time is "{0}", incoming message creation time is "{1}", incoming message expiry time is "{2}" , configured clock skew is "{3}" seconds. The acceptable time range is "{4}" to "{5}". The incoming token is outside the valid range as allowed by clock skew and expiry times.

Category:
Security

Cause:
The incoming message is outside the valid range as allowed by clock skew and expiry times.

Action:
Make sure the token is not expired. Check the allowed clock skew and configure them as required.

WSM-00417
Alias "{0}" already exists in the Keystore.

Category:
Security

Cause:
Alias already points to trusted certificate or a private key entry.

Action:
Ensure that alias do not already exist in the Keystore and retry the operation.

WSM-00418
Subject Name Identifier is missing in the SAML token. Check if the user identifier is properly set up to be included in the SAML assertion.

Category:
Security

Cause:
Subject Name Identifier is missing in the SAML token.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Check if the user identifier is properly set up to be included in the SAML assertion.

WSM-00419
Keystore properties updation failed due to {0}

Category:
Security

Cause:
Check nested error for failure

Action:
Check nested error for fixing the issue

WSM-00420
The key, {0}, is not retrieved due to exception "{4}". The location of the key store being used is "{1}" and its type is "{2}". The following aliases are found in the keystore:- {3}

Category:
Configuration

Cause:
Error occurred while obtaining key from store.

Action:
Make sure the key exists in the keystore. Check JPS configuration settings for correct key alias, key password and keystore password. Also, check the values of the key keystore-csf-key and its password in the oracle.wsm.security map, through EM or WLST. In a rare situation, this error can also happen if the actual keystore type is ORACLE_WALLET and the keystore type specified in JPS configuration file is PKCS12.

WSM-00421
The claim "{0}" contains null or empty value in the JWT token "{1}".

Category:
Security

Cause:
The claim contains empty or null value in the incoming JWT token.

Action:
Make sure that the claim is present in the incoming JWT token.

WSM-00422
Message is not compliant with timestamp requirement of the policy. Policy indicates that the timestamp element should not be present, but it is found in the message.

Category:
Security

Cause:
Timestamp policy compliance failed. Policy indicates that the timestamp element should not be present, but it is found in the message.

Action:
Check the message and make sure message is compliant with timestamp requirement of the service policy.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-00423
Web service authentication failed.

Category:
Security

Cause:
Web Service Authentication failed at the server end.

Action:
Resend valid credentials.

WSM-00424
The init-param named servlet-name not found in the deployment descriptor. Skipping SecurityFilter initialization. OWSM SecurityFilter will not be enforced.

Category:
Security

Cause:
servlet-name init param for the OWSM security filter definition was missing from the application's web.xml.

Action:
User must provide a value for the servlet-name init param of the filter definition in the web.xml for the OWSM Security Filter to be initialized.

WSM-00425
The security header is missing in request. Ensure that there is a valid security policy attached at the client side, and the policy is enabled. And make sure timestamp is present in the security header.

Category:
Security

Cause:
Security header was expected but was not found.

Action:
Security header is missing in request. It could be that client side policy has not been applied. Resend request with appropriate Security header. And make sure timestamp is present in the security header.

WSM-00426
The security header is missing in response. Ensure that response message is compliant with security requirement of the client policy. And make sure timestamp is present in the security header.

Category:
Security

Cause:
Security header was expected but was not found.

Action:
Security header is missing in response. The response message is not compliant with security requirement of the client policy. Check the response message sent by service. And make sure timestamp is present in the security header.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-00427
Security Exception : {0}

Category:
Security

Cause:
The system encountered a failure while enforcing security.

Action:
Check diagnostic log file to get more details.

WSM-00428
The certificate for the alias {0} not found in the KSS Keystore {1}. The following aliases are found in the Keystore: {2}

Category:
Configuration

Cause:
Certificate does not exist in the KSS keystore.

Action:
Ensure that certificate exists in keystore

WSM-00429
The value of the name id attribute {0} present in the token is not of type string.

Category:
Configuration

Cause:
name id attribute value present in the token is not of string type.

Action:
Ensure that name id attribute value is of type string in the token.

WSM-00430
Signature not present in the SAML Assertion.

Category:
Security

Cause:
Signature not present in the SAML Assertion.

Action:
Check to see that the SAML Assertion is signed or turn off saml.enveloped.signature.required.

WSM-00431
Provide valid value for oauth1.client.csf.key config override.

Category:
Configuration

Cause:
oauth1.client.csf.key config override is missing.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Provide valid value for oauth1.client.csf.key after adding entry in CSF.

WSM-00432
The property "{0}" is not found in the incoming message context.

Category:
Configuration

Cause:
The message contains empty or null value for the property in the incoming message context.

Action:
Make sure that the property is present in the incoming message context.

WSM-00433
HTTP Request type "{0}" is invalid. Valid values are GET and POST.

Category:
Configuration

Cause:
The HTTP Request type was invalid.

Action:
Valid supported values are GET and POST

WSM-00434
Entity type "{0}" is invalid. Only type Form corresponding to Content-Type application/x-www-form-urlencoded is supported.

Category:
Configuration

Cause:
Entity type is invalid. Only type Form corresponding to Content-Type application/x-www-form-urlencoded is supported.

Action:
Use Content-Type application/x-www-form-urlencoded and corresponding class object

WSM-00435
Message type "{0}" is invalid. Only REST is supported for oauth1 client policy.

Category:
Configuration

Cause:
Message type is invalid. Only REST is supported.

Action:
Use REST for using oauth1 policy

WSM-00436
Provide valid value for csf-key config override.

Category:
Configuration

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
csf-key config override is missing.

Action:
Provide valid value for csf-key after adding entry in CSF.

WSM-00437
Virtual user is being propagated as subject is {0}.

Category:
Security

Cause:
Subject based on virtual user is being propagated.

Action:
Check client's configuration if virtual user should not be propagated.

WSM-00438
Failure occurred while performing signature caching validation.

Category:
Security

Cause:
Failure occurred while performing signature caching validation.

Action:
This may be due to same message being replayed. SignatureValue entry is found in the Signature Replay Cache. Resend the request with a valid signature.

WSM-00439
Algorithm Suite mismatch, expecting "{1}", found "{0}".

Category:
Security

Cause:
UsernameToken with Password Derived Keys Assertion had algorithm-suite other than Basic128.

Action:
UsernameToken with Password Derived Keys supports only BASIC128 algorithm suite.Set algorithm-suite as Basic128.

WSM-00440
Both Signed and Encrypted parts not allowed when using password derived keys support .

Category:
Security

Cause:
Both Signing and Encryption not supported for UsernameToken with Password Derived Keys Policy.

Action:
Make sure policy does not have both signed and encrypted parts.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-00441
The iterations value provided by the user: "{0}" is not valid. The default value of 1000 is being used .

Category:
Security

Cause:
The Iteration value provided by the user is not valid

Action:
Provide a valid value. Till then the default value 1000 will be used.

WSM-00442
The {0} token found in the request, Encoded token: [{1}] Decoded token: [{2}] is invalid and token authentication failed

Category:
Security

Cause:
Improper security token/assertion in the request found during authentication.

Action:
Check the security token/assertion in the request.

WSM-00443
The HTTP USER header from OAM is missing.

Category:
Security

Cause:
The User Header was not found.

Action:
Ensure that the request HTTP headers contain an User header from OAM.

WSM-00444
Public keys using open id connect discovery document could not be trusted for issuer {0}.

Category:
Security

Cause:
Cannot configure jwk trust with the issuer.

Action:
Check the logs and retry the operation.

WSM-00445
The key type of the public key is not supported. Only RSA is supported.

Category:
Security

Cause:
JWK key type of the key is not trusted. Only RSA is supported.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Check the kty param of JWK document and retry the operation.

WSM-00447
Kid {0} is not a valid a trusted kid for issuer {1}.

Category:
Security

Cause:
JWK key id is not trusted.

Action:
Import the JWK through CLI or REST API.

WSM-00448
Public key required for signature verification could not be retrieved for kid {0} from both local JWK as well as remotely configured JWK.

Category:
Security

Cause:
kid is not present in the JWT token.

Action:
Check kid present in the JWT.

WSM-00449
kid attribute is missing in the JWT token.

Category:
Security

Cause:
The kid attribute is missing in the JWT Token.

Action:
Check the JWK token and try again.

WSM-00450
The JWK url is not configured.

Category:
Security

Cause:
The JWK URL is not configured.

Action:
Configure the JWK trust using REST or CLI command.

WSM-00451
JWK or Certificate based trust is not configured.

Category:
Security

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
JWK or Certificate based trust is not configured

Action:
Configure the JWK or Certificate based trust using REST or CLI command.

WSM-00452
Failure in looking up requested Runtime MBean Server of the Weblogic Server where this application is running because the JNDI name used, "{0}", is wrong.

Category:
Security

Cause:
Failure occurred in looking up or connecting to the requested Runtime MBean server on the Weblogic server.

Action:
Make sure that the right JNDI name for the Runtime MBean server is passed for the lookup and retry the operation.

WSM-00453
Failure in identifying the correct object name of the Runtime Service MBean for this Weblogic server because the String provided, "{0}", does not correspond to a valid object-name representing the WLS Runtime Service MBean.

Category:
Security

Cause:
Failure occurred in identifying the correct object name of the Runtime Service MBean for this Weblogic server.

Action:
Make sure that the String representing the object-name of the Runtime Service MBean is correct.

WSM-00454
JWT audience claim - "{0}" is invalid. The value of resource tenancy "{1}" is not same as tenant claim "{2}"

Category:
Security

Cause:
JWT audience claim is invalid

Action:
Fix the audience claim to match the resource tenancy with tenant claim and retry the operation.

WSM-00455
JWT audience claim - "{0}" is invalid. Necessary Audience condition is not satisfied. "{1}"

Category:
Security

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
JWT necessary audience claim is not satisfied

Action:
Fix the audience claim to match the resource and retry the operation.

WSM-00456
Failure occurred while looking for a specific MBean or attribute in the Runtime Service MBean, "{0}", for this Weblogic server. See the exception for more details.

Category:
Security

Cause:
Failure occurred while looking for a specific MBean or attribute in the Runtime Service MBean for this Weblogic server.

Action:
Make sure that the MBean name or attribute name being looked for is correct.

WSM-00457
Credential could not be found for csf key "{0}" under csf map "{1}".

Category:
Other

Cause:
Credentials are not found in the credential store..

Action:
Check for credentials in the credential store..

WSM-00458
Could not connect to "{0}". Server returned HTTP Code: {1}.

Category:
Other

Cause:
Incorrect response code is recieved.

Action:
Check if URL endpoint is correct and is serving content.

WSM-00459
Failure occurred while trying to authenticate an incoming Basic Auth header on behalf of Weblogic server. See the exception for more details.

Category:
Security

Cause:
Failure occurred while trying to authenticate incoming Basic Auth header on behalf of Weblogic server.

Action:
Make sure that valid credentials are being used to generate the request.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-00460
JWT token verification failed.

Category:
Security

Cause:
JWT Token verification failed

Action:
Fix the JWT token and retry the operation.

WSM-00461
Global configuration for IDCS issuer is invalid with incorrect baseURL={0} or idcsClientCsfKey={1}. It might not have been configured

Category:
Security

Cause:
Global configuration for IDCS issuer is invalid. It might not have been correctly configured

Action:
check the global configuration and retry the operation.

WSM-00462
Global configuration for IDCS issuer is not present. Hence unable to retrieve baseURL and idcsClientCsfKey

Category:
Security

Cause:
Global configuration for IDCS issuer is not present.

Action:
create the global configuration and retry the operation.

WSM-00463
Service instance app name is not present in HTTP header. This is required for retrieving TAGS configuration from IDCS.

Category:
Security

Cause:
Service instance app name is not present in HTTP header. This is required for retrieving TAGS configuration from IDCS.

Action:
configure the client to send service instance app name and retry the operation.

WSM-00464
Resource tenancy is not present in HTTP header. This is required for retrieving TAGS configuration from IDCS.

Category:
Security

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
Resource Tenancy is not present in HTTP header. This is required for retrieving TAGS configuration from IDCS.

Action:
configure the client to send resource tenancy and retry the operation.

WSM-00465
Failure occurred while trying to retieve tags from IDCS due to {0}

Category:
Security

Cause:
Failure occurred while trying to retrieve tags from IDCS.

Action:
Make sure that IDCS is up and has tags configured.

WSM-00466
Error parsing refresh interval {0}, using default value...

Category:
Security

Cause:
Error parsing refresh interval.

Action:
Make sure that refreshInterval is a valid integer value.

WSM-00467
Failed retrieving IDCS Discovery Metadata for {0} info from {1}.

Category:
Security

Cause:
Failed retrieving IDCS Discovery Metadata.

Action:
Make sure that IDCS is up and running.

WSM-00468
Error locating service with HK2: {0}

Category:
Security

Cause:
Failure in locating service.

Action:
Make sure that services are properly configured with HK2.

WSM-00469
Failure occurred while trying to get access token from IDCS due to {0}

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Security

Cause:
Failure occurred while trying to retrieve access token from IDCS.

Action:
Make sure that IDCS is up and credentials are correct.

WSM-00470
Error processing tags with TAG data used: {0}

Category:
Security

Cause:
Failed processing tags.

Action:
Analyze the data.

WSM-00471
JWT audience claim - "{0}" is invalid. Custom necessary audience condition returns NULL result on evaluation

Category:
Security

Cause:
JWT necessary audience claim is not satisfied as the implementation of custom condition not correct

Action:
Fix the custom audience condition implementation and retry the operation.

WSM-00472
Required policy configuration scope is missing for OAuth2 three-legged policy. Configure a valid scope value

Category:
Security

Cause:
Required policy configuration scope is missing for OAuth2 three-legged policy.

Action:
Configure policy with a valid scope config override.

WSM-00473
State is not present in the response received from OAuth2 server for the request for authorization code for 3-legged flow. Hence rejecting the response.

Category:
Security

Cause:
State is not present in the response received from OAuth2 server for the request for authorization code for 3-legged flow.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Resend the request.

WSM-00474
State is not valid in the response received from OAuth2 server for the request for authorization code for 3-legged flow. Hence rejecting the response.

Category:
Security

Cause:
State is not valid in the response received from OAuth2 server for the request for authorization code for 3-legged flow.

Action:
Resend the request.

WSM-00475
Error initializing servlet filter for 3-legged flow.

Category:
Security

Cause:
There was error in initializing servlet filter for 3-legged flow.

Action:
Check the server for application deployment logs.

WSM-00476
Error in redirecting incoming request to original address for 3-legged flow.

Category:
Security

Cause:
There was error in redirecting incoming request to original address for 3-legged flow.

Action:
Check the server for application deployment logs.

WSM-00477
Servlet Filter Exception while enforcing 3-legged OAuth security

Category:
Security

Cause:
The system encountered a failure while enforcing security in the servlet filter for 3-legged flow.

Action:
Check diagnostic log file to get more details.

WSM-00478
Error in enforcing security for OAuth2 3-legged flow. Please check the logs for more details.

Category:
Security

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
The system encountered a failure while enforcing security in the servlet filter for 3-legged flow.

Action:
Check diagnostic log file to get more details.

WSM-00479
There is no incoming authorization code found but the policy is configured for 3-legged flow.

Category:
Security

Cause:
There is no incoming authorization code found but the policy is configured for 3-legged flow.

Action:
Configure the required filters to obtain authorization code.

WSM-00481
Configured authorization.uri = "{0}" is invalid .Configure a valid authorization.uri value for 3-legged OAuth

Category:
Configuration

Cause:
authorization.uri config override does not point to a valid value

Action:
Configure authorization.uri in the config override

WSM-01501
failure in parsing the policy attachment

Category:
Data

Cause:
The XML was not well formed, or the XML did not follow the policy attachment schema.

Action:
Ensure that the XML is well formed, and the XML follows the policy attachment schema.

WSM-01502
failure in parsing the assertion template

Category:
Data

Cause:
The XML was not well formed, or the XML did not follow the assertion template schema.

Action:
Ensure that the XML is well formed, and the XML follows the assertion template schema.

WSM-01503
failure in parsing the assertion

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Data

Cause:
The XML was not well formed, or the XML did not follow the assertion schema.

Action:
Ensure that the XML is well formed, and the XML follows the assertion schema.

WSM-01504
failure in parsing the property set configuration

Category:
Data

Cause:
The XML was not well formed, or the XML did not follow the property set Config schema.

Action:
Ensure that the XML is well formed, and the XML follows the property set Config schema.

WSM-01505
failure in creating a copy of the policy {0}

Category:
Data

Cause:
Copying of the policy failed.

Action:
Ensure that the policy to be copied is valid. If the problem persists, contact Oracle Support Services.

WSM-01506
failure in creating a copy of the assertion template {0}

Category:
Data

Cause:
Copying of the assertion template failed.

Action:
Ensure that the assertion template to be copied is valid. If the problem persists, contact Oracle Support Services.

WSM-01507
failure in creating a copy of the assertion {0}

Category:
Data

Cause:
Copying of the assertion failed.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Ensure that the assertion to be copied is valid. If the problem persists, contact Oracle Support Services.

WSM-01508
failure in transforming policy {0} to XML

Category:
Data

Cause:
The policy could not be serialized to XML.

Action:
Ensure that the policy Java object can be serialized to XML format.

WSM-01509
failure in transforming policy set {0} to XML

Category:
Data

Cause:
The policy set could not be serialized to XML.

Action:
Ensure that the policy set Java object can be serialized to XML format.

WSM-01510
failure in transforming policy attachment {0} to XML

Category:
Data

Cause:
The policy attachment could not be serialized to XML.

Action:
Ensure that the policy attachment Java object can be serialized to XML format.

WSM-01511
failure in transforming assertion template {0} to XML

Category:
Data

Cause:
The assertion template could not be serialized to XML.

Action:
Ensure that the assertion template Java object can be serialized to XML format.

WSM-01512
failure in transforming assertion {0} to XML

Category:
Data

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
The assertion could not be serialized to XML.

Action:
Ensure that the assertion Java object can be serialized to XML format.

WSM-01513
failure in transforming configuration {0} to XML

Category:
Data

Cause:
The configuration could not be serialized to XML.

Action:
Ensure that the configuration Java object can be serialized to XML format.

WSM-01514
failure in transforming policy reference {0} to XML

Category:
Data

Cause:
System could not serialize policy reference to XML.

Action:
Ensure passed policy reference Java object doesn't have issues that causes the serialization to XML to fail.

WSM-01515
failure in transforming policy subject {0} to XML

Category:
Data

Cause:
System could not serialize policy subject to XML.

Action:
Ensure passed policy subject Java object doesn't have issues that cause the serialization to XML to fail.

WSM-01524
failure in serialization of WSDL

Category:
Data

Cause:
WSDL Serialization failed.

Action:
Ensure WSDL Extensions are available and configured. Consult diagnostic log for details or contact Oracle Support Services.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-01526
WSDL Definition object is null

Category:
Data

Cause:
WSDL Definition Object is not available

Action:
Ensure that a valid WSDL Definition object is sent to OWSM for advertisement of wsdl.

WSM-01527
Failed to advertise policy for tenant context {0} due to underlying exception "{1}".

Category:
Configuration

Cause:
The policy advertisement failed due to invalid tenant context.

Action:
Ensure that a valid tenant context is set in the header for the policy advertisement.

WSM-01600
error in creating or initializing the assertion, key={0}, qname={1}, wspqname={2}, constructorName={3}

Category:
Programmatic

Cause:
An assertion object could not be created.

Action:
Verify that the assertion follows the interface requirements defined in the Oracle documentation.

WSM-01601
failure in loading the resource

Category:
Configuration

Cause:
The requested resource could not be loaded.

Action:
Ensure that the requested resource is present in the class path.

WSM-01602
error in loading class {0}

Category:
Programmatic

Cause:
The requested class could not be loaded.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Ensure that the requested class is present in the class path.

WSM-01603
failure in parsing the policy due to {0}.

Category:
Data

Cause:
Parsing of the policy failed.

Action:
Ensure that the policy XML follows the policy schema, or a valid policy file exists.

WSM-01604
XML Parser Configuration error

Category:
Configuration

Cause:
The XML Parser was not configured properly.

Action:
Consult Oracle documentation or Java documentation on how to configure the XML Parser.

WSM-01605
XML parser exception

Category:
Data

Cause:
Parsing of the XML failed.

Action:
Ensure that the XML is well formed.

WSM-01606
system I/O error

Category:
Files

Cause:
The system could not open the Input/Output streams.

Action:
Consult the Java documentation.

WSM-01607
XPath expression evaluation error

Category:
Data

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
Evaluation of the XPATH expression failed.

Action:
Ensure that the XPATH expression is valid, and the XML follows the schema.

WSM-01608
The class cannot be found.

Category:
Configuration

Cause:
The requested class was not found in the class path.

Action:
Ensure that the class name is correct in the configuration files and is in the class path.

WSM-01610
cannot initialize standard serializers/deserializers

Category:
Configuration

Cause:
The standard serializer and deserializer objects could not be loaded.

Action:
Ensure that the product configuration is correct. If the problem persists, contact Oracle Support Services.

WSM-01611
The class cannot be loaded because of Java security restrictions.

Category:
Configuration

Cause:
The requested classes could not be loaded due to class loading security restrictions.

Action:
Contact the site administrator or consult the Java documentation to ensure that the classes have the necessary Java security permissions.

WSM-01612
An instance of the requested class cannot be created.

Category:
Configuration

Cause:
The system could not create an instance of the requested class.

Action:
Consult the Java documentation or contact Oracle Support Services.

WSM-01613
The XML parser cannot be configured.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Configuration

Cause:
The XML parser could not be configured.

Action:
Consult the Java documentation on how to configure the XML parser.

WSM-01614
The assertion XML Java Document cannot be serialized to a String.

Category:
Data

Cause:
The assertion XML Java Document could not be serialized to a String.

Action:
Check the assertion for any errors and retry the operation.

WSM-01615
The assertion XML String cannot be converted to a Java object.

Category:
Data

Cause:
The assertion XML String could not converted to a Java Document.

Action:
Ensure that the String being converted to XML is a well-formed XML.

WSM-01616
Policy {0} cannot be inserted into the WSDL.

Category:
Data

Cause:
The WSDL extensions for the policy could not be found or were incorrectly configured.

Action:
Ensure that the WSDL extensions for the policy being injected are available and configured. Consult Oracle documentation for more information.

WSM-01617
error in parsing the policies embedded in the WSDL

Category:
Data

Cause:
The WSDL extensions for the policy could not be found or were incorrectly configured.

Action:
Ensure that the WSDL extensions for policy are available and configured. Consult Oracle documentation for more information.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-01618
error in parsing the policy references embedded in the WSDL

Category:
Data

Cause:
The XML for the policy references in the WSDL could not be parsed.

Action:
Ensure that the WSDL extensions for the policy reference are available and configured. Consult Oracle documentation for more information.

WSM-01619
This assertion type is not recognized.

Category:
Data

Cause:
The assertion type was not recognized.

Action:
Consult Oracle documentation for the supported assertion types.

WSM-01620
cannot convert XML Java Document to String

Category:
Data

Cause:
The XML Java Document being converted was not well formed.

Action:
Ensure that the assertions can be serialized to a String.

WSM-01621
Policy intersection algorithm is not defined for assertion type :

Category:
Data

Cause:
The policy intersection algorithm was not found for the assertion.

Action:
Ensure that the intersection algorithm for the assertion used is configured.

WSM-01622
Policy merge algorithm is not defined for assertion type :

Category:
Data

Cause:
The policy merge algorithm was not found for the assertion.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Ensure that the merge algorithm for the assertion used is configured.

WSM-01623
Policy reference cannot be resolved :

Category:
Data

Cause:
The policy reference was invalid.

Action:
Ensure that the policy reference is valid.

WSM-01624
The policy does not exist in the policy store :

Category:
Data

Cause:
The policy reference was invalid, or the referenced policy could not be retrieved.

Action:
Ensure that the policy reference is valid, and the policy exists in the policy store.

WSM-01625
The Name attribute of the property is missing.

Category:
Data

Cause:
The Name attribute for a property was missing.

Action:
Provide a value for the Name attribute.

WSM-01626
The Type attribute of the property is missing.

Category:
Data

Cause:
The Type attribute for a property was missing.

Action:
Provide a value for the Type attribute.

WSM-01627
The assertion contains too many bindings.

Category:
Data

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
The assertion contained more than one binding.

Action:
Ensure that the assertion contains a single binding.

WSM-01628
The policy normalization algorithm is not defined for this assertion type

Category:
Data

Cause:
The policy normalization algorithm was not found for the assertion.

Action:
Ensure that the normalization algorithm for the assertion used is configured.

WSM-01629
The assertion template contains too many assertions.

Category:
Data

Cause:
The assertion template contained more than one assertion.

Action:
Ensure that assertion template contains only one assertion.

WSM-01630
Element {0} is not a known policy element.

Category:
Data

Cause:
XML parsing failed; the system encountered unsupported XML elements.

Action:
Ensure that the XML follows the schema, and the XML contains only those elements that are supported.

WSM-01631
The assertion {0} contains multiple bindings.

Category:
Data

Cause:
The assertion contained more than one binding.

Action:
Ensure that the assertion contains only one binding.

WSM-01632
The assertion {0} contains multiple policies as child elements.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Data

Cause:
The assertion contained more than one policy child element.

Action:
Ensure that the assertion contains only one policy child element.

WSM-01633
Assertion type {0} does not match the corresponding Java Object type created.

Category:
Configuration

Cause:
The assertion type was incorrectly defined for the assertion.

Action:
Ensure that the correct assertion type is set for the assertion.

WSM-01635
Passed Java Object {0} does not extend the Assertion class

Category:
Data

Cause:
The Assertion class did not extend the correct classes.

Action:
Consult Oracle Documentation for creating assertion implementations.

WSM-01636
The assertion type {0} is not supported.

Category:
Data

Cause:
The assertion type does not match any of the predefined assertion types.

Action:
Ensure that the assertion type is supported.

WSM-01637
The policy attachment cannot be parsed.

Category:
Data

Cause:
The policy attachment XML was invalid.

Action:
Ensure that policy attachment XML follows the policy attachment XML schema.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-01638
The policy attachment is not valid because the domain is not specified.

Category:
Data

Cause:
The policy attachment did not contain domain expressions.

Action:
Ensure that policy attachment XML follows the policy attachment XML schema.

WSM-01640
The policy reference {0} is not valid.

Category:
Data

Cause:
The policy reference could not be resolved.

Action:
Ensure that the referenced policy exists in the policy store.

WSM-01641
The policy advertisement level is not specified for the policy.

Category:
Configuration

Cause:
The policy advertisement level was not specified.

Action:
Ensure that a valid value is set for the policy advertisement level.

WSM-01642
Policy advertisement is not supported for unsupported WSDL elements.

Category:
Data

Cause:
Policy advertisement was not supported for the WSDL object.

Action:
Consult Oracle documentation for supported WSDL objects.

WSM-01643
What the XML system expects is different from what is encountered.

Category:
Data

Cause:
Usage of system was invalid or the feature was unsupported.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Consult Documentation on usage and supported features.

WSM-01644
The WSDL object {0} is not supported.

Category:
Data

Cause:
The WSDL object was not supported.

Action:
Consult Oracle documentation for the supported WSDL objects.

WSM-01645
The resource pattern {0} does not match the corresponding WSDL object.

Category:
Data

Cause:
WSDL Objects did not match.

Action:
Ensure that the WSDL Objects match.

WSM-01646
The value for the attachTo attribute of the policy is not valid.

Category:
Data

Cause:
The attachTo attribute of the policy did not match any of the predefined attachTo values.

Action:
Consult Oracle documentation for the valid values for the attachTo attribute.

WSM-01647
There are no policies that match the specified category {0} and resource pattern {1}.

Category:
Data

Cause:
No policies matched the specified search criteria.

Action:
Ensure that the policies that match the search categories exist in the policy store.

WSM-01650
cannot construct policy object

Category:
Programmatic

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
Construction of the policy Java object failed.

Action:
Consult the diagnostic log for details.

WSM-01651
cannot advertise requested policies

Category:
Programmatic

Cause:
Advertisement of the policies failed.

Action:
Consult the diagnostic log for details, or contact Oracle Support Services.

WSM-01652
error in parsing the time stamp in the policy set document

Category:
Data

Cause:
The Timestamp attribute in the XML representation of a policy set document is not a valid number.

Action:
Correct or remove the invalid attribute value.

WSM-01653
The assertion contains more than one Guard element.

Category:
Data

Cause:
The assertion contained more than one guard.

Action:
Ensure that the assertion contains a single guard.

WSM-01654
failure in serialization of security scenario assertion

Category:
Data

Cause:
The SecurityScenario in OraPolicy could not be serialized or was incorrectly configured.

Action:
Ensure that the OraPolicy is correct. Consult Oracle documentation for more information.

WSM-01655
There are no policies that match the specified category {0}.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Data

Cause:
No policies matched the specified category.

Action:
Ensure that the policies that match the search category exist in the policy store.

WSM-01656
generic Oracle WSM Policy Manager error

Category:
Data

Cause:
An internal error occurred during the Policy related operation.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

WSM-01657
Oracle WSM Advertisement Engine must be initialized with valid properties. Following properties [{0}] are either empty or null

Category:
Configuration

Cause:
WSM Advertisement Engine initialized with invalid parameters.

Action:
Ensure that valid parameters are set during WSM Advertisement Engine configuration

WSM-01658
X509 Certificate will not be advertised as {0} not found

Category:
Other

Cause:
Implementation class for advertising X509 Certificate in WSDL is not available

Action:
Ensure that implementation class required for advertising X509 Certificate in WSDL is not available. Consult diagnostic log for details or contact Oracle Support Services.

WSM-01659
A JAXBContext cannot be created due to underlying exception "{0}".

Category:
Data

Cause:
One or more expected classes could not be located.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-01660
A JAXB unmarshaller cannot be created due to underlying exception "{0}".

Category:
Data

Cause:
An error occurred while creating an unmarshaller.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

WSM-01661
A string cannot be unmarshalled into an object due to underlying exception "{0}".

Category:
Data

Cause:
The string is not suitable for unmarshalling to the requested type.

Action:
Provide a string that is suitable for unmarshalling to the requested type.

WSM-01662
The QName "{0}" does not match the expected QName "{1}" for the unmarshalled object.

Category:
Data

Cause:
The string is not suitable for unmarshalling to the requested type.

Action:
Provide a string that is suitable for unmarshalling to the requested type.

WSM-01663
A null or empty string cannot be unmarshalled into an Intent object.

Category:
Data

Cause:
An attempt was made to unmarshall an Intent from a null or empty String.

Action:
Provide a String that contains a marshalled Intent.

WSM-01664
A null or empty string cannot be unmarshalled into a PolicySet object.

Category:
Data

Cause:
An attempt was made to unmarshall a PolicySet from a null or empty String.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Provide a String that contains a marshalled PolicySet.

WSM-01665
A JAXB marshaller cannot be created due to underlying exception "{0}".

Category:
Data

Cause:
An error occurred while creating a marshaller.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

WSM-01666
An object cannot be marshalled to a string due to underlying exception "{0}".

Category:
Data

Cause:
Marshalling the supplied type of the object is not supported.

Action:
Provide an object of a supported type.

WSM-01667
An object cannot be marshalled to a DOM object due to underlying exception "{0}".

Category:
Data

Cause:
Marshalling the supplied type of the object is not supported.

Action:
Provide an object of a supported type.

WSM-01668
A null Intent object cannot be marshalled.

Category:
Data

Cause:
An attempt was made to marshall a null Intent object.

Action:
Provide a non-null Intent object.

WSM-01669
A null PolicySet object cannot be marshalled.

Category:
Data

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
An attempt was made to marshall a null PolicySet object.

Action:
Provide a non-null PolicySet object.

WSM-01670
An object cannot be marshalled into a null DOM object.

Category:
Data

Cause:
An attempt was made to marshall an object into a null Document object.

Action:
Provide a non-null Document object.

WSM-01671
The DOM element cannot be null for policy subject identified by the resource pattern: "{0}".

Category:
Compliance

Cause:
The null DOM element was passed.

Action:
Pass a valid non-null DOM element.

WSM-01672
The policy reference URI: "{1}" for policy subject identified by the resource pattern: "{0}" cannot be empty.

Category:
Compliance

Cause:
Empty policy references were found in the DOM element node.

Action:
Verify the DOM element node and make sure the policy references specify a valid value and the referenced policies exist in the repository.

WSM-01673
Duplicate policy references: "{1}" are found for policy subject identified by resource pattern "{0}".

Category:
Compliance

Cause:
Duplicate policy references were found in the same DOM element node.

Action:
Remove the duplicate policy references from the DOM element node.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-01674
The DOM element: "{1}" for policy subject identified by resource pattern "{0}" is unsupported element.

Category:
Compliance

Cause:
Policies cannot be retrieved for unsupported DOM element node.

Action:
Verify that a supported DOM element node is provided for retrieving the policy.

WSM-01675
The policy references cannot be null.

Category:
Compliance

Cause:
A null policy reference was passed.

Action:
Pass the valid non-null policy reference object.

WSM-01676
The resource pattern cannot be null.

Category:
Compliance

Cause:
A null resource pattern was passed.

Action:
Pass a valid non-null resource pattern.

WSM-01677
The domain expression cannot be null.

Category:
Compliance

Cause:
A null domain expression was passed.

Action:
Pass a valid non-null domain expression.

WSM-01678
Element {0} is not a valid child element for Policy object.

Category:
Data

Cause:
Invalid child element found for Policy object.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Check the policy string being parsed and make sure only valid child elements are present for the Policy.

WSM-01679
A DOM node cannot be unmarshalled into an object due to underlying exception "{0}".

Category:
Data

Cause:
The string is not suitable for unmarshalling to the requested type.

Action:
Provide a string that is suitable for unmarshalling to the requested type.

WSM-01680
A null node cannot be unmarshalled into a RepositoryInfo object.

Category:
Data

Cause:
An attempt was made to unmarshall a RepositoryInfo from a null node.

Action:
Provide a node that contains a marshalled RepositoryInfo.

WSM-01681
A null or empty string cannot be unmarshalled into a RepositoryInfo object.

Category:
Data

Cause:
An attempt was made to unmarshall a RepositoryInfo from a null or empty String.

Action:
Provide a String that contains a marshalled RepositoryInfo.

WSM-01682
A null RepositoryInfo object cannot be marshalled.

Category:
Data

Cause:
An attempt was made to marshall a null RepositoryInfo object.

Action:
Provide a non-null RepositoryInfo object.

WSM-01683
The passed String "{0}" could not be parsed using UTF encoding.

Category:
Data

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
Underlying JVM does not support UTF-8 encoding.

Action:
Check the JVM configuration to make sure it supports UTF-8 encoding format.

WSM-01684
A null or empty string cannot be unmarshalled into a Policy object.

Category:
Data

Cause:
An attempt was made to unmarshall a Policy from a null or empty String.

Action:
Provide a String that contains a marshalled Policy.

WSM-01685
Issuer Uri is not available. Either sts_trust_config_service_policy is not attached to service or the Issuer Uri is missing from the policy. Ignore this warning if sts_trust_config_client_policy is attached to client.

Category:
Configuration

Cause:
Issuer Uri is not available. Either sts_trust_config_service_policy is not attached to service or the Issuer Uri is missing from the policy. Ignore this warning if sts_trust_config_client_policy is attached to client.

Action:
Attach sts_trust_config_service_policy if not attached yet, or specify issuer uri value in the policy if not specified. Ignore if using sts_trust_config_client_policy.

WSM-01686
Advertisement failed due to an unexpected assertion type: {0}.

Category:
Configuration

Cause:
The assertion type is not recognized.

Action:
Internal error. Provide

WSM-01687
The constant property "{0}" cannot be overridden.

Category:
Configuration

Cause:
There is an attempt to override a property value which is defined as a constant in the policy.

Action:
Ensure that there is no attempt to override a constant property.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-01688
X509 Certificate will not be advertised due to underlying exception "{0}".

Category:
Configuration

Cause:
Either the keystore was not available or the keystore configuration was incorrect.

Action:
Ensure the keystore exists and that the keystore password and aliases are correct.

WSM-01689
Advertisement failed due to an incorrect ws-policy/ws-securitypolicy specification version {0}/{1}.

Category:
Configuration

Cause:
Invalid ws-policy/ws-securitypolicy specification version used to advertise policy.

Action:
Ensure the ws-policy/ws-securitypolicy specification versions are correct.

WSM-01690
Assertion {0} located by QName {1} is not an instanceof type {2}.

Category:
Data

Cause:
An internal error, probably policy was not deserialized into the correct assertion instance.

Action:
Consult diagnostic log for details or contact Oracle Support Services.

WSM-01691
Cannot construct or access policy object for policy "{0}" due to underlying exception "{1}".

Category:
Programmatic

Cause:
Construction of the policy Java object failed for the given policy name.

Action:
Consult the diagnostic log for details.

WSM-01692
Advertisement failed due to multiple ws-policy specification version specified.

Category:
Configuration

Cause:
Multiple ws-policy specification version used to advertise policy.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Remove the duplicate ws-policy specification versions and try again.

WSM-01693
Advertisement failed due to multiple wssecurity-policy specification version specified.

Category:
Configuration

Cause:
Multiple ws-securitypolicy specification version used to advertise policy.

Action:
Remove the duplicate ws-securitypolicy specification versions and try again.

WSM-01694
Policy compatibility check failed due to invalid policy set. {0}.

Category:
Other

Cause:
Policy compatibility check failed due to invalid policy set.

Action:
Ensure that the policy set attached to the client is a valid policy set. Consult diagnostic log for details or contact Oracle Support Services.

WSM-01695
Encountered internal error while attempting to reorder PolicyReferences "{0}" in a PolicySet "{1}".

Category:
Other

Cause:
Encountered unexpected Policy model exception during reordering PolicyReferences in a PolicySet

Action:
Consult diagnostic log for details or contact Oracle Support Services.

WSM-01696
While validating the input PolicySet array to be merged, one or more PolicySets resource pattern are not same as that of the base, baseResourcePattern={0}, invalid input PolicySets= {1}

Category:
Other

Cause:
While validating the input PolicySet array to be merged, found policyset resourcepattern that is different than that of the base.

Action:
Make sure ResourcePattern of all PolicySet in the array either all null, or for non-null ones they must all have the same ResourcePattern.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-01697
The ResourcePattern of the base runtime PolicySet for merging is null, basePolicySet={0}, input PolicySet array={1}. All PolicySet in the array should be either null, or has the same resource pattern as that of the base policy set and all callback policy sets should have the same resource pattern.

Category:
Other

Cause:
The ResourcePattern of the base runtime Policy Set for merging is null, possibly the base runtime Policy Set is constructed using empty Policyset() constructor.

Action:
Make sure runtime PolicySet is created with not-null ResourcePattern.

WSM-01698
Runtime PolicySet is locked and it can not be modified with operation "{0}" and argument "{1}".

Category:
Other

Cause:
Runtime PolicySet is locked and read only; it cannot be modified

Action:
Donot modify PolicySet

WSM-01699
Runtime PolicySet "{0}" operation got an invalid argument "{1}" with value "{2}".

Category:
Other

Cause:
Runtime PolicySet add method passed in a null or invalid argment(s).

Action:
Check the arguments and correct them.

WSM-01700
The current Runtime PolicySet "{0}" merge method got an invalid PolicySet "{1}" in the List of PolicySet passed in; it is not an instance of PolicySet, very likely it is a CallbackPolicySet

Category:
Other

Cause:
Runtime PolicySet merge method passed invalid argument.

Action:
Check the arguments and correct them.

WSM-01701
Cannot perform changes to the DOM document provided to the storage provider since its a read-only document.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Other

Cause:
WSM Assembly document could not be fetched for write operation.

Action:
The WSM Assembly document provided to the storage provider does not support update. Provide a writeable DOM document and retry the operation.

WSM-01702
A null WSM Assembly object cannot be marshalled.

Category:
Other

Cause:
An attempt was made to marshall a null WsmAssembly object.

Action:
Provide a non-null WsmAssembly object.

WSM-01703
Failed to retrieve descriptor identified by "{0}" in storage provider due to an exception

Category:
Other

Cause:
WSM descriptor document could not be fetched due to IOException.

Action:
Check with logging for detail, and retry, if problem persists, contact Oracle Support.

WSM-01704
While advertising policies under subject "{0}", the specified web service with QName "{1}" does not exist in the wsdl; it may not be valid, make sure that namespace and local name of the service are correct.

Category:
Other

Cause:
The QName of the web service specified does not exist in the wsdl

Action:
Verify the namespace and local name and make sure there are valid

WSM-01705
While advertising policies under subject "{0}", the specified port name "{1}" does not exist under the service "{2}" in wsdl.

Category:
Other

Cause:
The port name specified does not exist in the servie of wsdl

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Verify the port name and make sure it is valid

WSM-01706
A null node cannot be unmarshalled into an Intent object.

Category:
Data

Cause:
An attempt was made to unmarshall an intent from a null node.

Action:
Provide a node that contains a marshalled intent.

WSM-01707
A null node cannot be unmarshalled into an assertion metadata object.

Category:
Data

Cause:
An attempt was made to unmarshall assertion metadata from a null node.

Action:
Provide a node that contains a marshalled assertion metadata.

WSM-01708
Advertisement expression "{0}" for portable expression "{1}" is not valid.

Category:
Data

Cause:
The advertisment expression probably is not set correctly.

Action:
Check the log and verify it is not null and confirm to the format.

WSM-01709
The Runtime PolicySet cannot be advertised due to validation errors. PolicySet "{0}" validation errors: "{1}" .

Category:
Other

Cause:
Runtime PolicySet cannot be advertised due to validation errors.

Action:
Check the logs and correct errors in the PolicySet.

WSM-01710
The Policy "{0}" has following validation errors= "{1}".

Category:
Other

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
Policy has validation errors.

Action:
Check the logs and correct errors in the Policy.

WSM-01711
One or more Callback PolicySets ResourcePattern are not the same. baseResourcePattern={0}, callbackPolicySetsHaveDifferentResourcePatterns= {1}. All PolicySet in the array should be either null, or has the same resource pattern as that of the base policy set and all callback policy sets should have the same resource pattern.

Category:
Other

Cause:
Found invalid PolicySet in the input PolicySet array to be merged.

Action:
Make sure all PolicySet resource pattern in the array should be either null, or has the same resource pattern as that of the base policy set and all callback policy sets should have the same resource pattern.

WSM-01712
While validating the input PolicySet array to be merged, input resource pattern subject type={0} is incompatible with that of base={1}, input policySet={2}.

Category:
Other

Cause:
While validating the input PolicySet array to be merged, input callback subject type is not compatible with that of the base.

Action:
Input resource pattern should be either null, same as base, or a compatible callback type

WSM-01713
A null node cannot be unmarshalled into a TimestampInfo object.

Category:
Data

Cause:
An attempt was made to unmarshall a TimestampInfo from a null node.

Action:
Check the log and retry the operation.

WSM-01714
A null TimestampInfo object cannot be marshalled.

Category:
Data

Cause:
An attempt was made to marshall a null TimestampInfo object.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Check the log and retry the operation.

WSM-01715
The current thread context class loaders "{0}" are unable to locate the OWSM seed policy JAR "{1}". URLs that have the searched resource "{2}" are "{3}".

Category:
Configuration

Cause:
The current thread classpath does not include the path to the wsm-seed-policies.jar.

Action:
Check the log for detail info.

WSM-01716
The current thread context class loader is unable to locate the OWSM seed policy JAR "{0}" by searching resource "{1}".

Category:
Configuration

Cause:
The current thread classpath does not include the path to the wsm-seed-policies.jar.

Action:
Check the log and retry the operation.

WSM-01717
A null node cannot be unmarshalled into an PolicyReference object.

Category:
Data

Cause:
An attempt was made to unmarshal PolicyReference from a null node.

Action:
Provide a node that contains a valid policy reference.

WSM-01718
A null PolicyReference object cannot be marshalled.

Category:
Data

Cause:
An attempt was made to marshal a null PolicyReference object.

Action:
Provide a non-null PolicyReference object.

WSM-01719
Error while getting input stream for entry "{0}" from seed jar located at "{1}".

Category:
Data

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
Error in reading jar entry from seed jar.

Action:
Check the jar file and retry the operation.

WSM-01720
Error while parsing entry "{0}" from seed jar located at "{1}".

Category:
Data

Cause:
Error in parsing file in seed jar.

Action:
Remove the invalid file and retry the operation.

WSM-01751
The name of an assertion property is empty.

Category:
Data

Cause:
The name of an assertion property was empty.

Action:
Make sure that you specify a name for all assertion properties.

WSM-01752
The data type of the value does not match the data type of property {0}. The expected data type is "string".

Category:
Data

Cause:
The datatype of the property value entered was not of type "string".

Action:
Make sure that the data type for the property value is of type "string".

WSM-01753
The data type of the value does not match the data type of property {0}. The expected data type is "boolean".

Category:
Data

Cause:
The data type of the property value entered was not of type "boolean".

Action:
Make sure that the data type for the property value is of type "boolean".

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-01754
The data type of the value does not match the data type of property {0}. The expected data type is "integer".

Category:
Data

Cause:
The data type of the property value entered was not of type "integer".

Action:
Make sure that the data type for the property value is of type "integer".

WSM-01755
An empty value is specified for property {0}.

Category:
Data

Cause:
An empty value was specified for a property that has a data type of type "password".

Action:
Specify a value for all properties that have a data type of type "password".

WSM-01756
The Property Set name field of context: {0} is empty

Category:
Data

Cause:
The Property Set Name field in one of the assertions was empty.

Action:
Make sure that you specify a name for all assertion property sets.

WSM-01757
The name attribute for the "Config" element is empty.

Category:
Data

Cause:
The name for the Config element was empty.

Action:
Make sure that a name is specified for the Config element.

WSM-01758
The assertion name is empty.

Category:
Data

Cause:
The assertion name was empty.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Make sure that the assertion name is specified.

WSM-01759
The policy ID is empty.

Category:
Data

Cause:
The policy ID was empty.

Action:
Make sure that the policy ID is specified.

WSM-01760
The policy name is empty.

Category:
Data

Cause:
The policy name was empty.

Action:
Make sure that the policy name is specified.

WSM-01761
Specifying a policy ID for a child policy is not permitted : {0}.

Category:
Data

Cause:
Policy ID must not be specified for child policies.

Action:
Remove the policy ID of the child policy.

WSM-01762
Specifying a policy name for a child policy is not permitted : {0}.

Category:
Data

Cause:
Policy name must not be specified for child policies.

Action:
Remove the policy name of the child policy.

WSM-01763
The value specified for the policy attachTo attribute {0}, does not match any of the supported values.

Category:
Data

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
The value specified for the policy attachTo attribute did not match any of the supported values.

Action:
Specify a valid value for the attachTo attribute. Consult the Oracle documentation for the supported values.

WSM-01764
The value specified for the policy category {0} does not match any of the supported values.

Category:
Data

Cause:
The value specified for policy category attribute did not match any of the supported values.

Action:
Specify a valid value for the category attribute. Consult the Oracle documentation for the supported values.

WSM-01765
The data type of the value specified for property {0} is not supported.

Category:
Data

Cause:
The data type specified for the property did not match any of the supported data types.

Action:
Specify a valid data type for the property. Consult the Oracle documentation for the supported data types.

WSM-01766
The assertion template ID cannot be empty.

Category:
Data

Cause:
The assertion template ID was empty.

Action:
Specify a value for assertion template ID.

WSM-01767
The assertion template name cannot be empty.

Category:
Data

Cause:
The assertion template name was empty.

Action:
Specify a value for the assertion template name.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-01768
The value specified for the assertion template attachTo attribute {0} does not match any of the supported values.

Category:
Data

Cause:
The value specified for the assertion template attachTo attribute did not match any of the supported values.

Action:
Specify a valid value for the attachTo attribute. Consult the Oracle documentation for the supported values.

WSM-01769
The value specified for the assertion template category {0} does not match any of the supported values.

Category:
Data

Cause:
The value specified for the assertion template category attribute did not match any of the supported values.

Action:
Specify a valid value for the category attribute. Consult the Oracle documentation for the supported values.

WSM-01770
A value or default value is not specified for property {0}.

Category:
Data

Cause:
No value or default value was specified for the property.

Action:
Specify a value or a default value for the property.

WSM-01771
Attaching multiple reliable messaging policies is not supported. Only one reliable messaging policy can be attached to a policy subject

Category:
Data

Cause:
More than one reliable messaging policy was attached to a policy subject.

Action:
Make sure that only one reliable messaging policy is attached to a policy subject.

WSM-01772
Attaching multiple make connection(WSMC) policies is not supported. Only one WSMC policy can be attached to a policy subject.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Data

Cause:
More than one MTOM policy was attached to a policy subject.

Action:
Make sure that only one reliable MTOM is attached to a policy subject.

WSM-01773
Attaching multiple WS-Addressing policies is not supported. Only one WS-Addressing policy can be attached to a policy subject.

Category:
Data

Cause:
The user attached more than one WS-Addressing policy.

Action:
Make sure that only one reliable WS-Addressing is attached to a policy subject.

WSM-01774
The policy "{0}" cannot be attached to policy subject "{1}" having unsupported subject type "{2}".

Category:
Data

Cause:
A policy was attached to an unsupported policy subject.

Action:
Make sure that the policy subject supports policy attachment. Consult the Oracle documentation for the supported values.

WSM-01775
The policy "{0}" cannot be attached to ResourcePattern "{1}" SubjectType "{2}" of attachTo "{3}" since it may only be used with "{4}".

Category:
Data

Cause:
An incompatible policy was attached to the policy subject.

Action:
Make sure that the attached policy is compatible with the policy subject.

WSM-01776
The policy reference "{0}" is invalid.

Category:
Data

Cause:
The policy reference was invalid because the policy did not exist.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Make sure that the referenced policy exists in the policy store.

WSM-01777
Attaching multiple authorization security policies is not supported. Only one authorization security policy can be attached to a policy subject.

Category:
Data

Cause:
More than one authorization security policy was attached to a policy subject.

Action:
Make sure that only one authorization security policy is attached to a policy subject.

WSM-01778
Attaching multiple authentication security policies is not supported. Only one authentication security policy can be attached to a policy subject.

Category:
Data

Cause:
More than one authentication security policy was attached to a policy subject.

Action:
Make sure that only one authentication security policy is attached to a policy subject.

WSM-01779
Attaching multiple message protection security policies is not supported. Only one message protection security policy can be attached to a policy subject.

Category:
Data

Cause:
More than one message protection security policy was attached to a policy subject.

Action:
Make sure that only one message protection security policy is attached to a policy subject.

WSM-01780
The policy reference category and the policy category do not match.

Category:
Data

Cause:
There was a mismatch between the policy reference category and the policy category.

Action:
Ensure that the policy reference category matches the policy category.

WSM-01781
Validation failure due to generic error.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Data

Cause:
A generic internal error occurred.

Action:
Consult the diagnostic logs for details.

WSM-01782
Policy contains no assertions. A policy must contain at least one assertion.

Category:
Data

Cause:
The policy did not contain any assertions.

Action:
Make sure that the policy contains at least one assertion.

WSM-01783
Guard does not contain any of the three elements of resource-match, action-match and constraint-match.

Category:
Data

Cause:
Guard does not contain any of the three elments of resource-match, action-match and constraint-match.

Action:
Make sure that at least one of three elements of resource-match, action-match and constraint-match is specified with its corresponding value in the Guard element.

WSM-01784
Validation is not supported for "{0}" type of Documents. Only a Policy, AssertionTemplate or PolicySet can be validated.

Category:
Data

Cause:
Validation is not supported for the type of Documents.

Action:
Ensure that the document is either a Policy or a PolicySet or AssertionTemplate.

WSM-01785
Signing or encryption of the soap fault is not supported.

Category:
Data

Cause:
The soap fault is to be signed or encrypted.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Make sure that the soap fault is not to be signed or encrypted.

WSM-01786
Attaching multiple STS-Config policies is not supported. Only one STS-Config policy can be attached to a policy subject.

Category:
Data

Cause:
More than one sts-config policy was attached to a policy subject.

Action:
Make sure that only one sts-config policy is attached to a policy subject.

WSM-01787
The policy name {0} contains invalid characters.

Category:
Data

Cause:
The policy name contains invalid characters.

Action:
Make sure that policy name contains valid characters.

WSM-01788
The assertion template name {0} contains invalid characters.

Category:
Data

Cause:
The assertion template name contains invalid characters.

Action:
Specify a valid value for the assertion template name.

WSM-01789
Attaching multiple web service transaction(WSTX) policies is not supported. Only one WSTX policy can be attached to a policy subject.

Category:
Data

Cause:
More than one WSMC policy was attached to a policy subject.

Action:
Make sure that only one make connection policy is attached to a policy subject.

WSM-01790
Attaching multiple Message Transmission Optimization Mechanism (MTOM) policies is not supported. Only one MTOM policy can be attached to a policy subject.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Data

Cause:
More than one WSTX policy was attached to a policy subject.

Action:
Make sure that only one reliable WSTX is attached to a policy subject.

WSM-01791
Combination of a sts-config policy and a non sts authentication/message protection policy is not valid.

Category:
Data

Cause:
sts-config policy and non sts policy was attached to a policy subject.

Action:
Make sure that a sts-config policy and a non sts config policy are not attached together to a policy subject.

WSM-01792
Attachment of a sts-config policy without any sts policy is invalid. Attach a valid sts policy together with a sts-config policy.

Category:
Data

Cause:
Sts policy was attached without sts-config policy to a policy subject.

Action:
Make sure that a sts config policy is attached together with a sts policy to a policy subject.

WSM-01793
The OR group contains no assertions. Edit the OR group to include one or more assertions.

Category:
Data

Cause:
The OR group contains no assertions.

Action:
Edit the OR group to include one or more assertions.

WSM-01794
Combination of an oauth2-config policy and a non oauth2 client policy is not valid.

Category:
Data

Cause:
oauth2-config policy and non oauth2 policy was attached to a policy subject.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Make sure that an oauth2-config policy and a non oauth2 config policy are not attached together to a policy subject.

WSM-01795
Attachment of an oauth2 config policy without any oauth2 client policy is invalid. Ensure you attach a valid oauth2 policy either via Direct Policy Attachment or via Global Policy Attachment along with an oauth2 config policy.

Category:
Data

Cause:
Oauth2 config policy was attached without oauth2 client policy to a policy subject.

Action:
Make sure that an oauth2 config policy is attached together with a oauth2 policy to a policy subject.

WSM-01796
Attaching multiple Oauth2-Config policies is not supported. Only one Oauth2-Config policy can be attached to a policy subject.

Category:
Data

Cause:
More than one oauth2-config policy was attached to a policy subject.

Action:
Make sure that only one oauth2-config policy is attached to a policy subject.

WSM-01797
Attachment of an oauth2 client policy without oauth2 config policy is invalid. Ensure you attach a valid oauth2 config policy either via Direct Policy Attachment or via Global Policy Attachment along with an oauth2 client policy.

Category:
Data

Cause:
Oauth2 client policy was attached without oauth2-config policy to a policy subject.

Action:
Make sure that a oauth2 config policy is attached together with a oauth2 policy to a policy subject.

WSM-01801
The type of resources expression is empty or missing.

Category:
Data

Cause:
The value specified for the appliesTo attribute was empty.

Action:
Specify a valid non-empty value for the appliesTo attribute.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-01802
The type of resources expression "{0}" is not supported.

Category:
Data

Cause:
The value specified for the appliesTo attribute was invalid.

Action:
Specify a valid value for the appliesTo attribute.

WSM-01811
The attachment expression is empty or missing; a non-empty expression with a function is expected.

Category:
Data

Cause:
The value specified for the attachTo attribute was empty.

Action:
Specify a valid, non-empty value for the attachTo attribute.

WSM-01812
The function "{2}" at index {1} in attachment expression "{0}" is empty or malformed. A function requires a non-empty, quoted value.

Category:
Data

Cause:
The argument for a function was missing, empty, or malformed.

Action:
Specify a valid, non-empty value for the function argument.

WSM-01813
The function "{2}" at index {1} in attachment expression "{0}" duplicates a previous function. A function may only appear once in an expression.

Category:
Data

Cause:
A function appeared more than once in an attachment expression.

Action:
Remove the duplicated function from the expression.

WSM-01814
The function "{2}" is not expected at index {1} in attachment expression "{0}". An operator is expected at this point.

Category:
Data

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
A function was found in an attachment expression where an operator was expected.

Action:
Specify the "and" operator between each function.

WSM-01815
A function is expected at index {1} in attachment expression "{0}".

Category:
Data

Cause:
The attachment expression ended with an operator.

Action:
Remove the dangling operator or add the missing function.

WSM-01816
The operator "{2}" at index {1} in attachment expression "{0}" is not supported. "and" is the only supported operator.

Category:
Data

Cause:
An unrecognized operator was found in an attachment expression.

Action:
Specify the "and" operator between each function.

WSM-01817
The text "{2}" at index {1} in attachment expression "{0}" is not expected. A function is expected at this point.

Category:
Data

Cause:
An unrecognized block of text was found in an attachment expression where a function was expected.

Action:
Specify a valid function in the expression.

WSM-01818
The text "{2}" at index {1} in attachment expression "{0}" is unrecognized. The operator "and" is expected at this point.

Category:
Data

Cause:
An unrecognized block of text was found in an attachment expression where an operator was expected.

Action:
Specify the "and" operator between each function.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-01821
The function "{0}" in attachment expression "{1}" is incompatible with "{2}" type of resources.

Category:
Data

Cause:
A function was found in an attachment expression that is not usable with the type of resource.

Action:
Specify a function that is compatible with the associated type of resource.

WSM-01822
The function "{0}" in attachment expression "{1}" is not supported for attachment.

Category:
Data

Cause:
A function was found in an attachment expression that is not usable for attachment.

Action:
Specify a function that is compatible with the associated type of resource.

WSM-01823
The policy set name is empty.

Category:
Data

Cause:
The policy set name was empty.

Action:
Make sure that the policy set name is specified.

WSM-01824
The policy set name {0} contains invalid characters.

Category:
Data

Cause:
The policy set name contains invalid characters.

Action:
Make sure that policy set name contains valid characters.

WSM-01825
Secure conversation is enabled in assertion to which it does not currently apply.

Category:
Data

Cause:
Secure conversation is enabled in assertion to which it does not currently apply.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Make sure that secure conversation is enabled only in supported assertions.

WSM-01826
Secure conversation re-authenticate feature is not supported in this assertion.

Category:
Data

Cause:
Secure conversation re-authenticate feature is not supported in this assertion.

Action:
Make sure that secure conversation re-authenticate feature is enabled only in supported assertions.

WSM-01827
Attaching multiple policies of category "{0}" is not supported. Policies in list ["{1}"] already have the category, current policy "{2}" also has that category.

Category:
Data

Cause:
More than one policy with the same category was attached to a policy subject.

Action:
Make sure that only one such policy is attached to a policy subject.

WSM-01828
Invalid category : {0} for policy : {1}. Only policies assigned to the security category are supported.

Category:
Compliance

Cause:
The Policy category provided was not valid.

Action:
Verify that the Policy category is correct.

WSM-01829
Policy: {0} contains unsupported assertions.

Category:
Security

Cause:
Policy contains unsupported assertions. Assertions of type http-security are not supported for WLS JAXWS web services.

Action:
Check the assertion type.

WSM-01830
The policy binding value "{0}" is not valid.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Security

Cause:
The policy binding value provided for the PolicySubject is invalid.

Action:
Verify that the SubjectType arguemt is correct.

WSM-01831
PII assertions cannot be combined with other assertions in a policy. This policy includes PII and non PII assertions which is not valid.

Category:
Configuration

Cause:
The policy contains PII assertion as well as other assertions. PII Assertion cannot be combined with other assertions in a policy.

Action:
Remove other assertions from this policy or remove the PII assertion.

WSM-01832
PII Policy {0} is not supported on the Resource {1} , as the PII policy is not supported on SubjectType : {2}

Category:
Configuration

Cause:
The PII Policy is not applicable on this SubjectType.

Action:
Detach the PII policy from the Subject.

WSM-01833
PII Policy {0} has local optimization turned ON, it should always be turned OFF.

Category:
Security

Cause:
Local optimization cannot be ON for PII Policy.

Action:
Turn local optimization off in PII policy.

WSM-01834
Policy: {0} contains assertion(s) that are not supported for the REST endpoint with Resource Pattern: {1}

Category:
Security

Cause:
Policy Set validation failed because the attached policy contains assertions that are not supported for REST endpoints.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Make sure the assertion(s) included in the policy are supported for REST endpoints.

WSM-01835
Policy: {0} contains assertion(s) that are not supported for the virtual endpoint with Resource Pattern: {1}, Subject type: {2}. If SubjectType is VS_SERVICE, policy must have VS_SERVICE intent and policy references must have SOAP_HTTP intent. If SubjectType is VS_REST_RESOURCE, policy must have VS_REST_RESOURCE intent and policy references must have REST_HTTP intent. If SubjectType is VS_URL_RESOURCE, policy must have VS_URL_RESOURCE intent and policy references must have URL intent.

Category:
Security

Cause:
Policy Set validation failed because the attached policy contains assertions that are not supported for virtual endpoints.

Action:
Make sure the assertion(s) included in the policy are supported for virtual endpoints. Check log for more details.

WSM-01844
The data type of the value does not match the data type of property {0}. The expected data type is "long".

Category:
Data

Cause:
The data type of the property value entered was not of type "long".

Action:
Make sure that the data type for the property value is of type "long".

WSM-01845
The value specified for the policy attachTo attribute {0}, is invalid for the assertion category: {1}.

Category:
Data

Cause:
The value specified for the policy attachTo attribute is invalid for the category.

Action:
Specify a valid value for the attachTo attribute. Consult the Oracle documentation for the supported values.

WSM-01846
The policy "{0}" having category "{1}" is not valid for resource pattern "{2}" of subject type "{3}".

Category:
Security

Cause:
Policy of this category is not applicable to the subject type.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Detach the policy from the subject.

WSM-01847
The type of policy set "{0}" is not specified or empty.

Category:
Data

Cause:
The policy set type is not specified or empty.

Action:
Make sure that the policy set type is specified.

WSM-01848
The type "{0}" of PolicySet "{1}" is invalid

Category:
Data

Cause:
The value specified for the policy set type is invalid.

Action:
Specify a valid value for policy set type. Refer documentation for the list of valid values.

WSM-01849
The type "{0}" of PolicySet "{1}" does not support external attachments.

Category:
Data

Cause:
The external attachment is not spoorted by the specified subject type.

Action:
Specify subject type which supports external attachment.

WSM-01850
WARNING: Non-Security policies do not apply to {0}

Category:
Data

Cause:
Non-Security policies do not apply to resource type.

Action:
Make correction according to the documentation and retry.

WSM-01851
The policy "{0}" is not supported for SOAP/JMS endpoint.

Category:
Data

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
Specified policy is not supported for SOAP JMS.

Action:
Make correction according to the documentation and retry.

WSM-01852
The field "{0}" of policyset "{1}" is not updatable; attampted to change {2} to "{3}".

Category:
Data

Cause:
Policyset field is not updatable.

Action:
Do not change the value of the field.

WSM-01853
The status field of object "{0}" has invalid value "{1}".

Category:
Data

Cause:
The value specified for status is invalid.

Action:
Specify a valid value for status. Refer documentation for the list of valid values.

WSM-01854
The constraint value "{0}" of PolicySet "{1}" is invalid and caused ParseException.

Category:
Data

Cause:
Parsing of constraint set in the global PolicySet caused ParseException

Action:
Correct the value of constraint in global PolicySet and retry.

WSM-01860
The configuration property name "{0}" is unknown.

Category:
Data

Cause:
The configuration property name is unknown.

Action:
Check the documentation and provide a valid name.

WSM-01861
The configuration property category "{0}" unknown.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Data

Cause:
The configuration property category is invalid.

Action:
Check the documentation and provide a valid category.

WSM-01862
The combination of property name "{0}" and category "{1}" is invalid.

Category:
Data

Cause:
The combination of property name and category is invalid.

Action:
Check the documentation and provide a valid combination of property name and category.

WSM-01863
Property "{0}" within category "{1}" is readonly and cannot be modified.

Category:
Data

Cause:
Read-only property cannot be modified.

Action:
Specify a modifiable property.

WSM-01864
Multiple values are not allowed for property "{0}" within category "{1}"

Category:
Data

Cause:
Multiple values are not allowed for the property.

Action:
Specify a single value.

WSM-01865
The format for value(s) "{0}" does not match the allowed format "{1}".

Category:
Data

Cause:
Format of the value does not match the allowed format.

Action:
Check the documentation and provide a valid format.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-01866
The provided configuration platform type "{0}" contains invalid character.

Category:
Data

Cause:
The configuration platform type contains invalid character.

Action:
Please check the documentation and provide a valid platform type.

WSM-01867
The provided configuration domain name "{0}" contains invalid character.

Category:
Data

Cause:
The configuration domain name contains invalid character.

Action:
Please check the documentation and provide a valid domain name.

WSM-01868
Seed token issuer trust document "{0}" can not be modified or deleted. It is a read-only document.

Category:
Data

Cause:
The Seed Token Issuer Trust Document is read-only and can not be modified or deleted.

Action:
Create a new document that can be customized to your needs.

WSM-01869
A token issuer trust document name must be provided for this operation.

Category:
Data

Cause:
A token issuer trust document name is required for this operation.

Action:
Specify a name to proceed with this operation.

WSM-01870
The field "{0}" of Token Issuer Trust "{1}" is not updatable; attampted to change "{2}" to "{3}".

Category:
Data

Cause:
Trust field is not updatable.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Do not change the value of the field.

WSM-01871
The TokenIssuerTrust document name cannot be null or empty.

Category:
Security

Cause:
The TokenIssuerTrust document name cannot be null or empty.

Action:
Make sure the name is provided when creating an Issuer.

WSM-01872
The tokentype attribute "{0}" for the Issuer "{1}" is not supported.

Category:
Security

Cause:
The tokentype attribute for the Issuer is not supported.

Action:
Change it to a supported token type when creating the Issuer in token issuer trust document.

WSM-01873
The field "{0}" of an Issuer cannot be missing.

Category:
Security

Cause:
The issuer name cannot be null or empty.

Action:
Make sure the name is provided when creating an Issuer.

WSM-01874
The field "{0}" of Issuer is not updatable.

Category:
Data

Cause:
Trust field is not updatable.

Action:
Do not change the value of the field.

WSM-01875
The value of field "{0}" of Issuer is not valid, it must be a boolean value.

Category:
Security

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
The enabled field should be a boolean value.

Action:
Make sure to use "true" or "false" boolean value.

WSM-01876
RelyingParty is only valid for Issuers that of JWT token type. Current Issuer token type is . "{0}".

Category:
Security

Cause:
The replying party is only valid for Issuers that are of JWT token type.

Action:
Change it to a supported tokentype vs relying party type pair when creating replying party under an Issuer.

WSM-01877
The value of field "{0}" in TokenIssuerTrust is not supported.

Category:
Security

Cause:
The field value in TokenIssuerTrust is not supported.

Action:
Change it to a supported key value type when creating the trusted key under an Issuer.

WSM-01878
KeyIdentifiers that are of publickey type are not accepted through user input but are resolved from metadata url "{0}".

Category:
Security

Cause:
The public key is not accepted through user input

Action:
Remove public KeyIdentifiers from user input data.

WSM-01879
The value of field "{0}" of the TrustedKey is not valid, it must be a boolean value.

Category:
Security

Cause:
The enabled field should be a boolean value.

Action:
Make sure to use "true" or "false" boolean value.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-01880
The combination of value of field "{0}" and field "{1}" of TrustedKey is not supported.

Category:
Security

Cause:
The key and key value type combination is not valid

Action:
Change it to a supported key and key value type pair when creating the trusted key under an Issuer.

WSM-01881
The value of field "{0}" of TrustedKey is not valid for value of field "{1}" in Issuer.

Category:
Security

Cause:
The key type and its beloning Issuer's token type combination is not valid

Action:
Change it to a supported key type when creating the trusted key under an Issuer.

WSM-01882
The metadata URL "{0}" for fetching public key is not valid URL.

Category:
Security

Cause:
The TrustedKey MDRUL is not valid URL.

Action:
Provide a valid URL.

WSM-01883
Field "{0}" must be set.

Category:
Security

Cause:
The TrustedKey MDRUL should not be null.

Action:
Provide a valid URL value.

WSM-01884
Refresh interval "{0}" of TrustedKey is not valid; it should be an integer.

Category:
Security

Cause:
The TrustedKey refreshinterval is not an integer.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Provide an integer value.

WSM-01885
The field "{0}" in TrustedKey is applicable only and must be set for Issuers that are of JWT token type, current issuer token type is "{1}".

Category:
Security

Cause:
The TrustedKey MDRUL is applicable for issers of JWT token type.

Action:
Choose Issuer that is of JWT token type.

WSM-01886
The field "{0}" and "{1}" of a TokenAttributeRule cannot be empty, missing or NONE at the same time.

Category:
Security

Cause:
The TokenAttributeRule field cannot be null or empty at the same time.

Action:
Make sure the fields are provided when creating a TokenAttributeRule.

WSM-01887
The field "{0}" of TokenAttributeRule is not updatable.

Category:
Data

Cause:
TokenAttributeRule field is not updatable.

Action:
Do not change the value of the field.

WSM-01888
The field "{0}" of an Attribute is not updatable.

Category:
Data

Cause:
Attribute field is not updatable.

Action:
Do not change the value of the field.

WSM-01889
The field "{0}" of an Attribute cannot be missing.

Category:
Security

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
The Attribute field cannot be null or empty.

Action:
Make sure the field is provided when creating an Attribute.

WSM-01890
The field "{0}" of the VirtualUser is not updatable.

Category:
Data

Cause:
VirtualUser field is not updatable.

Action:
Do not change the value of the field.

WSM-01891
The value of field "{0}" of the VirtualUser is not valid, it must be a boolean value.

Category:
Security

Cause:
The enabled field of VirtualUser should be a boolean value.

Action:
Make sure to use "true" or "false" boolean value.

WSM-01892
One or more values of field "{0}" in the VirtualUser is not valid.

Category:
Security

Cause:
One or more values in the a filed of a VritualUser is not valid.

Action:
Make a correction and try again.

WSM-01893
The value of field "{0}" of a TokenRoleMapping should not be null or empty

Category:
Security

Cause:
The field of a TokenRoleMapping should not have null or empty value.

Action:
Provid a non empty generic name.

WSM-01894
The value of field "{0}" of TokenRoleMapping should be an non empty list.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Security

Cause:
The field of TokenRoleMapping should not have null or empty list.

Action:
Provid a list of values.

WSM-01895
The value of field "{0}" of an Attribute or NameId should not be null or empty

Category:
Security

Cause:
The field of an Attribute or NameId should not have null or empty value.

Action:
Provid a non empty generic name.

WSM-01896
The value of field "{0}" of Mapping should not be null or empty

Category:
Security

Cause:
The field of an Mapping should not have null or empty value.

Action:
Provid a non empty generic name.

WSM-01897
ConfigOverride field "{0}" is either missing or has null or empty value

Category:
Security

Cause:
The field of ConfigOverride have either null or empty value.

Action:
Provid a generic name or value.

WSM-01898
The value of "{0}" contains invalid NCName character

Category:
Data

Cause:
Name contains invalid character.

Action:
Please check the documentation and provide valid name.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-01899
The value of fields "{0}" of DiscoveryInfo must be set.

Category:
Data

Cause:
Required fields are null.

Action:
Provide valid value.

WSM-01900
Field "{0}" value of "{1}" is not a valid URL

Category:
Data

Cause:
Field value is not a valid URI.

Action:
Provide valid value.

WSM-01901
Field "{0}" value of "{1}" is not a valid PATH

Category:
Data

Cause:
Field value is not a valid URI.

Action:
Provide valid value.

WSM-01902
The value of one or more required fields "{0}" of Proxy are either empty or missing.

Category:
Data

Cause:
Required fields are missing.

Action:
Provide valid value.

WSM-01903
The proxyport value "{0}" of the Proxy is not an integer.

Category:
Data

Cause:
Port is not an integer.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Provide integer value.

WSM-01904
The field "{0}" of Proxy cannot be set to null

Category:
Data

Cause:
Field cannot be set to null.

Action:
Provide a valid value.

WSM-01905
The field "{0}" has invalid value, must be one of the predefinded values: {1}

Category:
Security

Cause:
The TrustedKey trust type is not one of the valid predefined values.

Action:
Provide a valid trust type.

WSM-03001
Oracle WSM Monitor internal error {0}

Category:
Configuration

Cause:
An unexpected error occurred while monitoring Oracle WSM Agent.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

WSM-03002
Failure initializing Oracle WSM Monitor, {0} is null.

Category:
Configuration

Cause:
Creation of one or more DMS Event sensors failed while initializing Oracle WSM Monitor.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

WSM-03003
The topology node value {0} is not valid.

Category:
Configuration

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
The topology node value passed from the security interceptor to Oracle WSM Agent was invalid.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

WSM-03004
The parameter {0} is not valid.

Category:
Configuration

Cause:
The parameter was either null or invalid.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

WSM-04501
generic error in accessing the data store

Category:
Data

Cause:
An internal error occurred while accessing the MDS data store.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

WSM-04502
The name of the resource is empty.

Category:
Programmatic

Cause:
The name of the resource to be updated or retrieved was empty.

Action:
Assign a name to the resource being processed.

WSM-04503
resource {0} does not exist in the data store

Category:
Data

Cause:
The requested resource was not found in the data store.

Action:
Check the search criteria and try again.

WSM-04504
resource {0} cannot be updated

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Data

Cause:
The resource could not be updated.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

WSM-04505
resource {0} cannot be created

Category:
Data

Cause:
The specified name has already been assigned to another resource.

Action:
Specify a unique name, and retry the operation.

WSM-04506
cannot create resource {0}

Category:
Data

Cause:
The resource could not be saved to the data store.

Action:
Retry the operation.

WSM-04507
cannot delete resource {0}

Category:
Data

Cause:
The resource could not be deleted from the data store.

Action:
Retry the operation.

WSM-04508
cannot update resource {0}

Category:
Data

Cause:
The resource could not be updated to the data store.

Action:
Retry the operation.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-04509
cannot initialize the connection to the data store

Category:
Data

Cause:
Connecting to the data store failed.

Action:
Check the data store credentials, and retry the operation. Ensure that WSM-PM is installed, deployed correctly and running at http://<host:port>/wsm-pm/ and by clicking the Validator link. Also, ensure that the database to which WSM-PM connects is up and the mds-owsm data source is configured properly and targeted to the right server.

WSM-04510
The version {0} for resource {1} cannot be found.

Category:
Data

Cause:
The requested version for the specified resource was not found.

Action:
Check the search criteria, and retry the operation.

WSM-04511
cannot perform simultaneous deletes

Category:
Data

Cause:
Deleting multiple resources simultaneously from the data store failed.

Action:
Check supplied data, and retry the operation.

WSM-04512
internal data store error

Category:
Data

Cause:
A generic data store exception occurred.

Action:
Check the data store credentials that were provided and retry the operation. If the problem persists, contact Oracle Support Services.

WSM-04513
cannot commit changes to the repository

Category:
Data

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
A failure occurred while finalizing changes to the data store.

Action:
Retry the operation.

WSM-04514
The version {0} for resource {1} cannot be deleted.

Category:
Data

Cause:
Deleting the specified version(s) of the resource failed.

Action:
Check the supplied values, and retry the operation.

WSM-04515
Auditing is disabled for MDS operations.

Category:
Data

Cause:
An internal error occurred; failed to initialize the auditor.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

WSM-04516
The version of the passed resource is invalid.

Category:
Programmatic

Cause:
The requested version of the resource was invalid.

Action:
The version number must be a positive integer.

WSM-04517
cannot update resource {0}

Category:
Programmatic

Cause:
The resource to be updated was concurrently being updated by another process.

Action:
Make sure no other process is attempting to change the resource being updated, and retry the operation.

WSM-04518
document name is invalid

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Programmatic

Cause:
The document name was invalid.

Action:
Specify a name for the document that follows the document naming conventions. Refer to Oracle documentation for the naming rules.

WSM-04519
Unable to create document.

Category:
Programmatic

Cause:
The repository permissions were read-only. Creation of a new document requires write permissions.

Action:
Reconfigure the repository to have write permissions.

WSM-04520
The repository timestamp is invalid.

Category:
Programmatic

Cause:
The repository timestamp was invalid or missing.

Action:
Retry the operation. If the problem persists, consult the diagnostic logs.

WSM-04521
Resource to be deleted does not exist in datastore.

Category:
Data

Cause:
The resource could not be deleted since it does not exist in the data store.

Action:
You don't need to take any action, the resource is not present in the datastore.

WSM-04601
A JDBC URL is required to connect to a database-based MDS repository.

Category:
Programmatic

Cause:
A null or empty JDBC URL was provided when attempting to create an MDS instance for a database-based repository.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Provide a valid JDBC URL and try again.

WSM-04602
A password is required to connect to a database-based MDS repository.

Category:
Programmatic

Cause:
A null or empty password was provided when attempting to create an MDS instance for a database-based repository.

Action:
Provide a valid password and try again.

WSM-04603
A username is required to connect to a database-based MDS repository.

Category:
Programmatic

Cause:
A null or empty username was provided when attempting to create an MDS instance for a database-based repository.

Action:
Provide a valid username and try again.

WSM-04606
One or more directories are required to connect to a file-based MDS repository.

Category:
Programmatic

Cause:
A path was not provided when attempting to create an MDS instance for a file-based repository.

Action:
Provide a valid directory and try again.

WSM-04611
An MDS session cannot be created due to underlying error "{0}".

Category:
Data

Cause:
MDS encountered an unexpected condition.

Action:
Follow the recommendations for the underlying exception.

WSM-04641
The operation "{0}" for document "{1}" cannot be performed on a closed session.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Programmatic

Cause:
A operation was requested on a session that has already been closed.

Action:
Create a new repository session and perform the operation again.

WSM-04642
The operation "{0}" for document "{1}" cannot be performed on a read-only session.

Category:
Configuration

Cause:
A write operation was requested on a read-only session. See error message.

Action:
Provide the name of a creator to associate with write operations. Create a new session on a writable repository and try again.

WSM-04643
The operation "{0}" cannot be performed on virtual document "{1}".

Category:
Configuration

Cause:
A write operation was requested on a virtual document.

Action:
Choose a different document name and try again.

WSM-04651
The search criterion "{0}" does not identify a specific document to be created.

Category:
Programmatic

Cause:
The supplied criterion does not have the correct type.

Action:
Supply a NAME search criterion.

WSM-04652
The document "{0}" already exists in the repository.

Category:
Data

Cause:
The document already exists in the repository.

Action:
Choose a different name for the document to create or perform an update instead.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-04653
The document "{0}" cannot be created in a read-only repository.

Category:
Configuration

Cause:
The repository is read-only.

Action:
Reconfigure the repository to support writes and try again.

WSM-04654
The name "{0}" is invalid for creating a document due to underlying reason "{2}".

Category:
Data

Cause:
The document name is invalid for the repository.

Action:
Choose a valid name and try again.

WSM-04655
Repository information cannot be marshalled due to underlying parser error "{2}"

Category:
Other

Cause:
The system does not support the required DOM document builder configuration.

Action:
Correct underlying error or contact Oracle Support Services for assistance.

WSM-04656
Repository information cannot be marshalled due to underlying marshalling error "{2}"

Category:
Data

Cause:
The repository information object could not be marshalled into a DOM document.

Action:
Correct underlying error or contact Oracle Support Services for assistance.

WSM-04657
The document "{0}" cannot be created in a session spanning multiple stores due to underlying error "{2}".

Category:
Configuration

Cause:
The document to be created belongs in a store that is different from other write operations in the session.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Create the document in a different session.

WSM-04661
The document "{0}" cannot be deleted in a read-only repository.

Category:
Data

Cause:
The repository is read-only.

Action:
Reconfigure the repository to support writes and try again.

WSM-04662
The name "{0}" is invalid for deleting a document due to underlying reason "{2}".

Category:
Data

Cause:
The document name is invalid for the repository.

Action:
Choose a valid name and try again.

WSM-04663
The document "{0}" cannot be deleted in a session spanning multiple stores due to underlying error "{2}".

Category:
Data

Cause:
The document to be created belongs in a store that is different from other write operations in the session.

Action:
Delete the document in a different session.

WSM-04664
Version {1} to {3} of document "{0}" cannot be deleted.

Category:
Data

Cause:
The repository does not support deletion of individual versions of a document.

Action:
Ignore the document version or delete the entire document.

WSM-04671
A concurrent write prevented the document "{0}" from being written due to underlying error "{2}".

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Data

Cause:
Two or more incompatible operations were performed on the same document. A document in this session was modified by another session.

Action:
Perform the incompatible operations in different sessions. Retry the operation.

WSM-04672
The document "{0}" cannot be written to repository due to underlying error "{2}".

Category:
Data

Cause:
An I/O error occurred while writing to repository.

Action:
Correct the underlying problem and retry.

WSM-04673
The session cannot be committed due to underlying error "{2}".

Category:
Data

Cause:
The resource could not be deleted since it does not exist in the data store.

Action:
You don't need to take any action, the resource is not present in the datastore.

WSM-04674
The document "{0}" cannot be validated due to underlying error "{2}".

Category:
Data

Cause:
Validation failed for a metadata object written in the session.

Action:
Correct the underlying problem and retry.

WSM-04681
The document "{0}" to be modified was not found in the repository due to underlying error "{2}".

Category:
Data

Cause:
The document was not found in the repository.

Action:
Create the document instead of modifying it.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-04682
The document "{0}" cannot be modified in a session spanning multiple stores due to underlying error "{2}".

Category:
Data

Cause:
The document to be modified belongs in a store that is different from other write operations in the session.

Action:
Modify the document in a different session.

WSM-04691
The document "{0}" cannot be found in repository due to underlying error "{2}".

Category:
Data

Cause:
The document was not found in the repository.

Action:
Create the document and try again.

WSM-04692
The name "{0}" is invalid for retrieving a document due to the error "{2}".

Category:
Data

Cause:
The document name is invalid for the repository.

Action:
Choose a valid name and try again.

WSM-04693
Version information is not available for document "{0}".

Category:
Data

Cause:
The document does not exist The repository does not support versioning.

Action:
Create the document first. Configure the repository to support versioning.

WSM-04694
An invalid directory was provided to connect to a file-base MDS repository.

Category:
Programmatic

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
An invalid directory was provided when attempting to create an MDS instance for a file-based repository.

Action:
Provide a valid directory and try again.

WSM-04695
The retrieved version of document "{0}" is no longer available.

Category:
Data

Cause:
A new version of the document was created after it was initially retrieved.

Action:
Retry the operation to get the latest version of the document.

WSM-04696
The operation "{0}" cannot be performed on a closed session.

Category:
Programmatic

Cause:
A operation was requested on a session that has already been closed.

Action:
Create a new repository session and perform the operation again.

WSM-04697
The operation "{0}" cannot be performed on a read-only session.

Category:
Configuration

Cause:
A write operation was requested on a read-only session. See error message.

Action:
Provide the name of a creator to associate with write operations. Create a new session on a writable repository and try again.

WSM-04698
Versions {1} to {3} of document "{0}" cannot be deleted due to underlying error "{2}".

Category:
Data

Cause:
An I/O error occurred while trying to delete versions of a document from repository.

Action:
Correct the underlying problem and retry.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-04699
A write lock is not available to delete versions {1} to {3} of document "{0}" due to underlying error "{2}".

Category:
Data

Cause:
A write lock could not be obtained to delete versions of a document.

Action:
Retry the operation.

WSM-04700
cannot delete read-only resources {0}

Category:
Programmatic

Cause:
The document is read-only and cannot be deleted.

Action:
Choose document(s) that are not read-only for modification.

WSM-04701
A connection provider is required to connect to a database-based MDS repository.

Category:
Programmatic

Cause:
A null connection provider was provided when attempting to create an MDS instance for a database-based repository.

Action:
Provide a valid connection provider and try again.

WSM-04702
Timestamp information cannot be marshalled due to underlying parser error "{2}"

Category:
Data

Cause:
The timestamp information object could not be marshalled into a DOM document.

Action:
Retry the operation and if problem persists, contact Oracle Support Services for assistance.

WSM-04703
Repository timestamp information cannot be marshalled due to underlying parser error "{2}"

Category:
Other

Cause:
The system does not support the required DOM document builder configuration.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Correct underlying error or contact Oracle Support Services for assistance.

WSM-06001
Error obtaining Policy Set.

Category:
Configuration

Cause:
Failed to get PolicySet.

Action:
Check log file for possible causes.

WSM-06017
Error converting to the canonical path for the File Policy Resolver.

Category:
Files

Cause:
An invalid canonical path was passed for the File Policy Resolver.

Action:
Verify the canonical path passed for the File Policy Resolver and retry the operation.

WSM-06036
The class cannot be instantiated.

Category:
Configuration

Cause:
The system could not instantiate a class.

Action:
Consult the Java documentation or Oracle Support Services.

WSM-06101
The policy set cannot be created for null Service Component Architecture (SCA) node.

Category:
Compliance

Cause:
The PolicySet could not be generated for the null Service Component Architecture (SCA) node.

Action:
Pass a valid SCA node object.

WSM-06102
The policy reference URI "{0}" is not valid.

Category:
Compliance

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
The Policy Reference URI provided was not valid.

Action:
Verify that the Policy Reference URI in the SCA node is correct and the policy exists in the repository.

WSM-06103
No configuration has been specified for the Policy Accessor.

Category:
Configuration

Cause:
The Policy Accessor object could not be initialized because it is not correctly configured.

Action:
Call the init method to initialize the Policy Accessor object before invoking this method.

WSM-06104
The protocol specified for Policy Accessor is not supported.

Category:
Compliance

Cause:
A policy access protocol was specified that was invalid for this environment.

Action:
Change protocol to one that is supported by the environment. For J2EE environments, the supported protocols are "local" and "remote"; for J2SE environments, the supported protocols are "classpath", "local", and "remote".

WSM-06105
The duplicate policy references are found in the same Service Component Architecture (SCA) binding node.

Category:
Compliance

Cause:
The same policy has been attached multiple times and so duplicate policy references were found in the same Service Component Architecture (SCA) binding node.

Action:
Remove the duplicate policy references from the SCA binding node by attaching each policy only once.

WSM-06106
The policy reference URI cannot be empty.

Category:
Compliance

Cause:
Empty policy references were found in the Service Component Architecture (SCA) node.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Verify the Service Component Architecture (SCA) node and make sure the policy references specify a valid value and the referenced policies exist in the repository.

WSM-06107
The node that is expected is <binding.ws> or <component>. The node {0} passed is not a supported node.

Category:
Compliance

Cause:
An unsupported Service Component Architecture (SCA) node was found.

Action:
Specify a supported SCA node. Consult Oracle documentation for further details

WSM-06108
Error initializing the Oracle WSM Policy Resolver because incorrect configuration is passed

Category:
Configuration

Cause:
The Policy Resolver did not get created. This could be due to the wrong configuration being passed.

Action:
Verify the configuration passed for creating the Policy Resolver. Verify that the correct Policy Accessor protocol is passed.

WSM-06109
Cannot retrieve policies.

Category:
Data

Cause:
The policies were not retrieved. This may be due to incorrect policy references in the Service Component Architecture (SCA) node.

Action:
Verify that the policy references are referring to policies that exist in the repository. Also, ensure that the data store is seeded with policies.

WSM-06110
The MetaData Store (MDS) home cannot be null.

Category:
Configuration

Cause:
The Policy Repository was not valid because MDS Home is set to null.

Action:
Check the mds.home.module property for the correct value for MDS Home.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-06111
The policy name cannot be null.

Category:
Compliance

Cause:
The policy name passed was null or empty.

Action:
Verify that the policy name is not an empty string, and verify that a null policy name is not being passed.

WSM-06112
Policies are not supported for a node of type:{0}.

Category:
Compliance

Cause:
Policies cannot be retrieved for unsupported Service Component Architecture (SCA) nodes.

Action:
Verify that a supported SCA node is provided for retrieving the policy.

WSM-06113
The configuration name cannot be null or empty.

Category:
Configuration

Cause:
The configuration file was either empty or did not exist.

Action:
Verify that the configuration file exists and contains policy references to retrieve policies from the Policy Repository.

WSM-06114
The home directory for the File Policy Resolver cannot be null.

Category:
Files

Cause:
The home directory for File Policy Resolver was null.

Action:
Verify that a valid home directory is passed for the File Policy Resolver.

WSM-06115
The path for the File Policy Resolver does not exist.

Category:
Files

Cause:
The path for File Policy Resolver did not exist.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Ensure that a valid path is passed for File Policy Resolver.

WSM-06116
The path for the File Policy Resolver is not a directory.

Category:
Files

Cause:
An invalid directory name was passed for the File Policy Resolver.

Action:
Verify that a valid directory name is passed for the File Policy Resolver.

WSM-06118
The resource name for the File Policy Resolver cannot be null.

Category:
Files

Cause:
The resource name for the File Policy Resolver is null.

Action:
Verify that a valid resource name is passed for the File Policy Resolver.

WSM-06119
The file {0} for the File Policy Resolver does not exist under {1}.

Category:
Files

Cause:
The file did not exist.

Action:
Verify that the file exists at the specified location.

WSM-06120
The resource name for the File Policy Resolver cannot be null.

Category:
Files

Cause:
The resource name for the File Policy Resolver was null.

Action:
Ensure that a non-null resource name is passed for the File Policy Resolver.

WSM-06121
No policy is found for the policy reference: {0}.

Category:
Data

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
No policy was found for the specified policy reference.

Action:
Verify that the policy exists in the repository for the given policy reference, and that the correct policy reference is passed.

WSM-06122
Error retrieving policies.

Category:
Data

Cause:
An unexpected error occurred while retrieving the policies from the Policy Manager.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

WSM-06123
Error initializing internally the File Policy Resolver: {0} {1}

Category:
Security

Cause:
An unexpected error occurred while initializing the File Policy Resolver.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

WSM-06124
Error initializing the Oracle WSM Policy Manager Policy Resolver : {0} {1}.

Category:
Configuration

Cause:
An unexpected error occurred while initializing the Policy Manager Policy Resolver. The Policy Manager Policy Resolver was not able to find the property named mds.config

Action:
Verify that the property mds.config exists and is referencing a valid property file.

WSM-06125
Error in the XPath expression {0}.

Category:
Compliance

Cause:
The XPath Expression for the policy reference for the given Service Component Architecture (SCA) node was invalid.

Action:
Verify the XPath for the policy reference within the SCA node.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-06128
Error accessing the PolicySet : {0} : {1}.

Category:
Configuration

Cause:
An unexpected error occurred while accessing the PolicySet.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

WSM-06129
Error parsing the PolicySet : {0} : {1}.

Category:
Configuration

Cause:
An unexpected error occurred while parsing the PolicySet.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

WSM-06130
Error creating the policy parser.

Category:
Configuration

Cause:
The Policy Parser did not get created.

Action:
Check the configuration for the Policy Parser.

WSM-06132
Error creating a connection to Oracle WSM Policy Manager.

Category:
Configuration

Cause:
A failure occurred while connecting to the Policy Manager.

Action:
Ensure that the Policy Manager is up and running. Ensure that WSM-PM is installed, deployed correctly and running at http://<host:port>/wsm-pm/ and by clicking the Validator link. Also, ensure that the database to which WSM-PM connects is up and the mds-owsm data source is configured properly and targeted to the right server.

WSM-06133
Error connecting to Oracle WSM Policy Manager.

Category:
Configuration

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
A failure occurred while connecting to Policy Manager J2EE Application.

Action:
Before connecting to a Policy Manager, ensure that the Policy Manager is up and running.

WSM-06134
The class cannot be found.

Category:
Configuration

Cause:
The class could not be found in the classpath.

Action:
Verify that the class name is correct in the configuration files and ensure that the class is specified in the classpath variable.

WSM-06135
The class cannot be loaded due to Java 2 security restrictions.

Category:
Configuration

Cause:
Some classes were not loaded due to class loading security restrictions.

Action:
Contact the site administrator or Java documentation to ensure that the classes have the necessary Java2 security permissions.

WSM-06137
The "mds" policy access protocol is deprecated - use "local" instead.

Category:
Configuration

Cause:
A deprecated Policy Accessor Protocol was specified.

Action:
Update the configuration to use the standard protocol name.

WSM-06138
The "owsm" policy access protocol is deprecated - use "remote" instead.

Category:
Configuration

Cause:
A deprecated Policy Accessor protocol was specified.

Action:
Update the configuration to use the standard protocol name.

WSM-06139
Error closing a stream

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Configuration

Cause:
Failure occurred in closing the stream while parsing the configuration file or the policy in the FILE protocol.

Action:
Verify that the correct configuration file or policy name is provided.

WSM-06140
Failure finding policy {0} in the classpath roots path {1}.

Category:
Configuration

Cause:
The policy did not exist in any of the configured roots. The configured roots are invalid.

Action:
Correct the reference to point to a policy that exists. Correct the classpath roots to point to the correct locations.

WSM-06141
Error initializing Policy Resolver.

Category:
Configuration

Cause:
The Policy Resolver was not initialized.

Action:
Invoke the init method to initialize the Policy Resolver before executing this method.

WSM-06142
Unable to retrieve policy store timestamp.

Category:
Configuration

Cause:
The Policy Resolver could not connect to Policy Manager to retrieve the policy store timestamp.

Action:
Check the MDS configuration file.

WSM-06143
The validation check in the policy "{0}" failed.

Category:
Configuration

Cause:
An error occurred while validating the policy.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Ensure that the policy is valid.

WSM-06144
Null policy subject value is not allowed from JEE application.

Category:
Compliance

Cause:
The null policy subject value was passed from JEE application.

Action:
Ensure that a valid policy subject is passed from the JEE application.

WSM-06145
Internal system error, cannot look up credential

Category:
Configuration

Cause:
Failure occurred while looking up credentials.

Action:
Internal system configuration error. Contact Oracle Support Services.

WSM-06146
Error deleting the attachment entries.

Category:
Configuration

Cause:
Failure occurred while deleting the attachment entries.

Action:
Ensure that a valid list of policy subjects for deactivated lifecycle type is passed

WSM-06147
There is mismatch in Policy reference category "{0}" and Policy category "{1}". Policy reference category should match with Policy category.

Category:
Data

Cause:
Mismatch in expected policy category and fetched policy category.

Action:
Confirm that the Policy Reference category is correct and that it matches the Policy category.

WSM-06148
Unable to apply property overrides to Policy

Category:
Data

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
Unable to apply property overrides to Policy.

Action:
Make sure the policy model conforms to the Oracle Web service policy model.

WSM-06149
The policy reference URI is not valid : {0}

Category:
Compliance

Cause:
The Policy Reference URI provided was not valid.

Action:
Verify that the Policy Reference URI is correct.

WSM-06150
Invalid category : {0} for policy : {1}. Only policies assigned to the security category are supported.

Category:
Compliance

Cause:
The Policy category provided was not valid.

Action:
Verify that the Policy category is correct.

WSM-06152
The Policy Cache is not available.

Category:
Compliance

Cause:
The Policy Cache is not available.

Action:
You may need to restart the server.

WSM-06153
Could not access the Policy Cache.

Category:
Compliance

Cause:
Cannot access the Policy Cache.

Action:
You may need to restart the server.

WSM-06154
Could not initialize Policy Java Object Cache.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Compliance

Cause:
Cannot initialize the Policy Cache.

Action:
You may need to restart the server.

WSM-06155
Could not re-create Policy Java Object Cache.

Category:
Compliance

Cause:
Could not re-create the Policy Cache.

Action:
You may need to restart the server.

WSM-06156
The policy referenced by URI "{0}" could not be retrieved since the URI is invalid.

Category:
Compliance

Cause:
The policy URI is missing, empty or contains invalid characters.

Action:
Provide a valid URI for a policy in the repository or remove the reference.

WSM-06157
The policy referenced by URI "{0}" could not be retrieved due to incorrect repository configuration.

Category:
Compliance

Cause:
The repository database is not configured correctly or not running.

Action:
Verify that the repository database is configured correctly according to the user documentation and is running.

WSM-06158
The policy referenced by URI "{0}" does not exist in the repository.

Category:
Data

Cause:
The referenced policy does not exist in the repository.

Action:
Provide the URI for a policy in the repository or load the desired policy into the repository.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-06159
The policy referenced by URI "{0}" could not be retrieved due to invalid credential "{1}" being used to connect to the Policy Manager.

Category:
Compliance

Cause:
Cannot connect to the policy manager due to credential issue.

Action:
Verify that credentials are correctly specified, if not using the default principal, and that the principal is authorized to access the policy manager application.

WSM-06160
The policy referenced by URI "{0}" could not be retrieved since Policy Manager is either not deployed or not in active state.

Category:
Compliance

Cause:
The policy manager application has not been deployed or is not running.

Action:
Verify that the policy manager application is deployed and configured correctly and in an active state.

WSM-06161
The policy referenced by URI "{0}" could not be retrieved since Policy Manager is not deployed.

Category:
Compliance

Cause:
The policy manager application has not been deployed.

Action:
Verify that the policy manager application is deployed.

WSM-06162
The policy referenced by URI "{0}" could not be retrieved as connection to Policy Manager cannot be established at "{1}" due to invalid configuration or inactive state.

Category:
Compliance

Cause:
The policy manager application is not running or is not configured correctly.

Action:
Verify that the policy manager application is configured correctly and is in an active state. Provide correct configuration for URL of policy manager, setting its listen address if using auto-discovery, and ensure that any required SSL certificate is valid.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-06163
The policy referenced by URI "{0}" could not be retrieved as connection to Policy Manager cannot be established due to invalid certificate configuration.

Category:
Compliance

Cause:
Cannot connect to the policy manager due to certificate issue.

Action:
Verify that credential store and trust store location are correctly specified, and ensure that the certificate entry is valid.

WSM-06201
The {0} repository accessor class cannot be accessed due to underlying error "{1}".

Category:
Configuration

Cause:
The nullary constructor for the specified accessor is not accessible to the configuration framework.

Action:
Specify a valid accessor.

WSM-06202
The {0} repository accessor class cannot be initialized due to underlying error "{1}".

Category:
Configuration

Cause:
A exception was encountered during evaluation of a static initializer for the specified accessor class.

Action:
Specify a valid accessor.

WSM-06203
The {0} repository accessor class cannot be used as a repository accessor because it does not implement the {1} interface.

Category:
Configuration

Cause:
The specified accessor does not implement the IRepositoryAccessor interface.

Action:
Specify a valid accessor.

WSM-06204
The {0} repository accessor class cannot be linked due to underlying error "{1}".

Category:
Configuration

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
The specified accessor depends on a class whose signature has changed since the accessor was compiled.

Action:
Update the accessor class or revert to an older version of the dependent class.

WSM-06205
The repository accessor "{0}" cannot be found due to underlying error "{1}".

Category:
Configuration

Cause:
The specified accessor was not found.

Action:
Specify a valid accessor.

WSM-06206
The {0} repository accessor class cannot be instantiated due to underlying error "{1}".

Category:
Configuration

Cause:
The specified accessor is an abstract class, an interface, an array class, a primitive type, or void, or the class does not have a nullary constructor.

Action:
Specify a valid accessor.

WSM-06207
A task scheduler was not available for configuring the {0} repository accessor for context "{1}".

Category:
Configuration

Cause:
A task scheduler was not supplied to the configuration framework.

Action:
Provide a task scheduler to the configuration framework.

WSM-06208
Access to the {0} repository accessor class is denied due to underlying error "{1}".

Category:
Configuration

Cause:
The configuration framework does not have permission to instantiate the specified accessor.

Action:
Ensure the necessary permissions are granted to the WSM code base.

WSM-06214
A task scheduler was provided for configuring the {0} repository accessor for context "{1}".

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Configuration

Cause:
A task scheduler was supplied to the configuration framework.

Action:
None.

WSM-06219
A task scheduler was not available for configuring the {0} repository accessor for the default context.

Category:
Configuration

Cause:
A task scheduler was not supplied to the configuration framework.

Action:
Provide a task scheduler to the configuration framework.

WSM-06220
A task scheduler was provided for configuring the {0} repository accessor for the default context.

Category:
Configuration

Cause:
A task scheduler was supplied to the configuration framework.

Action:
None.

WSM-06221
The password credentials cannot be obtained from the Credential Store.

Category:
Configuration

Cause:
Failure occurred while querying for credentials from CSF.

Action:
Check CSF configuration.

WSM-06222
The credentials passed to the credentials store are expired.

Category:
Configuration

Cause:
The Credentials have expired.

Action:
Ensure valid credentials are passed

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-06223
The access to the store or credentials is denied.

Category:
Configuration

Cause:
The requested access Credentials or Store is denied.

Action:
Ensure Store is properly initialized and valid credentials are passed

WSM-06224
Unexpected exception "{0}" caught when privileged method is called.

Category:
Configuration

Cause:
Unexpected exception caught on calling a privileged code.

Action:
Check the underlying signature of method called in privileged code

WSM-06225
Unable to retrieve credentials for the specified CSF key {0}.

Category:
Configuration

Cause:
Credential configuration in the policy accessor configuration file was incorrect.

Action:
Configure policy with valid CSF key.

WSM-06226
An instance of the {0} bean was obtained for accessing the local repository at path "{1}".

Category:
Configuration

Cause:
A bean instance was obtained by the configuration framework.

Action:
None.

WSM-06227
An instance of the {0} bean was obtained for accessing the remote repository.

Category:
Configuration

Cause:
A bean instance was obtained by the configuration framework.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
None.

WSM-06228
Unable to retrieve "ENTERPRISE" model via classpath accessor during configuration initialization.

Category:
Configuration

Cause:
The seed ENTERPRISE model cannot be retrieved via ClasspathAccessor during configuration manager startup.

Action:
Verify the availability of seed documents jar witin the classpath.

WSM-06229
Unable to retrieve "default" resource via classpath accessor during configuration initialization.

Category:
Configuration

Cause:
The seed default resource cannot be retrieved via ClasspathAccessor during configuration manager startup.

Action:
Verify the availability of seed documents jar witin the classpath.

WSM-06301
Subject Metadata is required when registering a listener.

Category:
Programmatic

Cause:
A null value was provided for the subject metadata.

Action:
Provide a valid metadata.

WSM-06302
A listener is required for asynchronous notification.

Category:
Programmatic

Cause:
A null value was provided for asynchronous listener registration.

Action:
Provide a valid listener.

WSM-06303
The method "{0}" was not called with required permission "{1}"

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Security

Cause:
The method was not called with required permission

Action:
Ensure necessary permissions are granted to the caller before calling the required methods.

WSM-06401
The assembly referenced by "{0}" is not registered with the application.

Category:
Programmatic

Cause:
The assembly is not registered with the application.

Action:
Retry the operation after registering the assembly with the application.

WSM-06402
The resource pattern identifying the metadata model is not provided.

Category:
Programmatic

Cause:
The resource pattern identifying the metadata is not provided.

Action:
Ensure that a valid resource pattern is passed for identifying the metadata.

WSM-06403
Valid instance of StorageProvider must be provided for accessing the assembly file.

Category:
Programmatic

Cause:
A storage provider is required for extracting metadata information from assembly file.

Action:
Retry the operation with valid instance of storage provider.

WSM-06404
The resource pattern "{0}" identify the subject is invalid or incomplete .

Category:
Programmatic

Cause:
The resource pattern identifying the subject is invalid.

Action:
Retry the operation with valid value for subject resource pattern.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-06405
The subject referenced by "{0}" is not registered with the assembly.

Category:
Programmatic

Cause:
The subject is not registered with the assembly.

Action:
Retry the operation after registering the subject with the assembly.

WSM-06406
Valid PolicySubjectDefinition must be provided for retrieving the effective policy set.

Category:
Programmatic

Cause:
The subject definition is not provided for creating policy set.

Action:
Provide valid value for subject definition for creating policy set.

WSM-06407
Attempted to register the listener "{0}" to a policy subject "{1}" which was already previously registered with listener "{2}".

Category:
Programmatic

Cause:
Attempt to reregistering a listener for a policy subject.

Action:
Make sure that a policy subject registers a listener only once.

WSM-06408
The local policy attachment data for policy subject "{0}" is not available due to underlying IO exception "{1}".

Category:
Data

Cause:
The policy assembly containing the policy subject's metadata cannot be accessed.

Action:
Correct the underlying condition and retry the operation.

WSM-06409
The local policy attachment data for policy subject "{0}" is not available due to underlying JAXB exception "{1}".

Category:
Data

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
The policy assembly containing the policy subject's metadata is corrupt.

Action:
Correct the underlying condition and retry the operation.

WSM-06410
JMX APIs are not available in this environment, verify environment configuration for JMX.

Category:
Data

Cause:
JMX api's are not available in this environment, so not initializing PolicyApplicationMBean

Action:
Verify environment configuration for JMX.

WSM-06411
A task scheduler was not available for configuring the repository accessor due to undelying error "{0}".

Category:
Configuration

Cause:
OWSM Configuration Manager not able to set the task scheduler.

Action:
Provide a task scheduler to the configuration framework.

WSM-06412
The partition aware scheduler fetch failed due to underlying Naming exception "{0}".

Category:
Data

Cause:
The partition aware scheduler cannot be fetched.

Action:
Correct the underlying condition and retry the operation.

WSM-06413
The value of term "{0}" from resource pattern terms "{1}" is not provided and cannot be resolved by platform support API either, hence will be set to default "{2}", please verify the cause.

Category:
Data

Cause:
PlatformSupport API returned unexpected null value in J2EE environment.

Action:
Check the log for more info and possible cause.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-07501
Failure in Oracle WSM Agent processRequest, category={0}, function={1}, application={2}, composite={3}, modelObj={4}, policy={5}, policyVersion={6}, assertionName={7}.

Category:
Configuration

Cause:
Processing request failed in the security interceptor while enforcing policy.

Action:
Check the log file for possible causes.

WSM-07502
Failure in Oracle WSM Agent processResponse, category= {0}, function={1}, application={2}, composite={3}, modelObj={4}, policy={5}, policyVersion={6}, assertionName={7}.

Category:
Configuration

Cause:
Processing response failed in the security interceptor while enforcing policy.

Action:
Check the log file for possible causes.

WSM-07503
Failure in Oracle WSM Agent processFault, category= {0}, function={1}, application={2}, composite={3}, modelObj={4}, policy={5}, policyVersion={6}, assertionName={7}.

Category:
Configuration

Cause:
Processing fault failed in the security interceptor while enforcing policy.

Action:
Check the log file for possible causes.

WSM-07504
Failure in Oracle WSM Agent processEvent, category= {0}, function={1}, application={2}, composite={3}, modelObj={4}.

Category:
Configuration

Cause:
Processing Fabric Lifecycle event failed in security interceptor.

Action:
Check the log file for possible causes

WSM-07505
Failure in Oracle WSM Agent initialization, category= {0}, function={1}.

Category:
Configuration

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
Agent initialization failed in the security interceptor.

Action:
Check the log file for possible causes.

WSM-07506
Failure in Oracle WSM Agent processFinish, category= {0}, function={1}, application={2}, composite={3}, modelObj={4}.

Category:
Configuration

Cause:
Agent finish failed in the security interceptor.

Action:
Check the log file for possible causes.

WSM-07507
Failure in Oracle WSM Agent, category= {0}, function={1}, stage={2} due to RuntimeException.

Category:
Data

Cause:
An unexpected RuntimeException was encountered while trying to access security interceptor.

Action:
Check the log file for possible causes and retry the operation.

WSM-07508
Oracle WSM Agent initialization failed due to PolicySet validation errors: {0}, with PolicySet={1}

Category:
Configuration

Cause:
Agent not initialized due to PolicySet validation errors

Action:
Check the log for detail

WSM-07509
Oracle WSM Agent must be initialized with valid properties. Following parameters [{0}] are either Empty or null

Category:
Configuration

Cause:
Agent not initialized with valid parameters.

Action:
Initialize the Agent with required parameters

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-07510
JAX-RS Filter is already initialized for policy subject with Resource Pattern "{0}". It can not be passed another PolicySubjectDefintion with Resource Patter "{1}". {2}

Category:
Data

Cause:
The JAX-RS Filter was already initialized with a PolicySubjectDefinition. It can not be passed any more PolicySubjectDefinition objects.

Action:
Do not Initialize the JAX-RS Filter multiple times.

WSM-07511
Failed to initialize JAX-RS Filter. The PolicySubjectDefinition array is either null, empty or has length > 1

Category:
Data

Cause:
JAX-RS Filter not initialized with an array of PolicySubjectDefinition objects whose length is exactly 1. The filter supports a single PolicySubjectDefinition at any time.

Action:
Create a PolicySubjectDefinition array with a single object and retry the operation.

WSM-07512
PolicySubjectDefinition could not be created for the JAX-RS resource. The JAX-RS resource object passed to create PolicySubjectDefinition was null.

Category:
Programmatic

Cause:
PolicySubjectDefinition could not be created for the JAX-RS resource. The JAX-RS resource object passed to create PolicySubjectDefinition was null.

Action:
Pass a valid, non-null resource class object.

WSM-07513
A resource filter could not be created for the JAX-RS resource. Either the HttpServletRequest [{0}] or the HttpServletResponse [{1}] passed to the constructor was null.

Category:
Programmatic

Cause:
RESTResourceFilter could not be instantiated. Either of the servlet request or response objects passed by the RESTResourceFilterFactory was null.

Action:
Make sure the HttpServletRequest/Response objects were injected in the filter factory.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-07514
OWSM Security Filter failed to initialize. The param-value of "oracle.wsm.metadata.policySet" init-param can not be parsed.

Category:
Configuration

Cause:
The XML value configured as CDATA for "oracle.wsm.metadata.policySet" init-param in the application's web.xml was not parsed successfully.

Action:
Make sure that the value of "oracle.wsm.metadata.policySet" init-param is well-formed XML enclosed as CDATA.

WSM-07515
OWSM Security Filter failed to initialize. The filter was unable to create a valid ResourcePattern object for this servlet: {0}.

Category:
Configuration

Cause:
The servlet may be under the default (root) context path.

Action:
Make sure that the servlet to be protected is not under the default (root) context path.

WSM-07516
OWSM Authorization Code Client Filter failed to initialize. The param-value of "oracle.wsm.metadata.policySet" init-param can not be parsed.

Category:
Configuration

Cause:
The XML value configured as CDATA for "oracle.wsm.metadata.policySet" init-param in the application's web.xml was not parsed successfully.

Action:
Make sure that the value of "oracle.wsm.metadata.policySet" init-param is well-formed XML enclosed as CDATA.

WSM-07600
Error while copying the message.

Category:
Security

Cause:
An unexpected error occurred while cloning SOAP or normalized message context.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

WSM-07601
Failure initializing the WSPolicyExecutor class {0}.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Configuration

Cause:
An unexpected error occurred while initializing the policy engine.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

WSM-07602
Failure in WS-Policy Execution due to exception.

Category:
Security

Cause:
Due to an unexpected error, policy execution failed at runtime.

Action:
Check the log file for possible causes.

WSM-07603
Failure in log assertion execution caused by exception.

Category:
Files

Cause:
File I/O problem or SOAP message access problem occurred.

Action:
Verify file access permission and the SOAP message.

WSM-07604
Internal error during policy enforcement.

Category:
Security

Cause:
An unexpected error occurred while enforcing the policy.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

WSM-07605
The binding.ws port ID {0} is invalid.

Category:
Configuration

Cause:
An unexpected error occurred in the Oracle WSM processEvent API.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-07606
Policy {0} execution failure.

Category:
Security

Cause:
Due to an unexpected error, policy execution failed at runtime.

Action:
Check the log file for possible causes.

WSM-07607
Failure in execution of assertion {0} executor class {1}.

Category:
Security

Cause:
The policy engine failed to execute an assertion.

Action:
Check the log file for possible causes.

WSM-07608
The assertion type is not valid.

Category:
Security

Cause:
Policy execution failed due to an invalid assertion.

Action:
Check the assertion type.

WSM-07609
Policy with attachto value of {0} cannot be applied to subject of type {1}.

Category:
Security

Cause:
The attached policy was incompatible with the subject.

Action:
Verify that the subject type and the policy's Attachto value are compatible.

WSM-07610
Internal error in policy status audit. One or more of the argument passed is null, result:{0}, agentFunction:{1}, policy:{2}, msgCtx:{3}

Category:
Configuration

Cause:
An internal error occurred; the enforcement auditor encountered one or more null arguments.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

WSM-07611
Failure initializing of enforcement auditor: category={0}, function= {1}, topologyNode={2}.

Category:
Configuration

Cause:
An internal error occurred; the enforcement auditor initialization failed.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

WSM-07612
Failure shutting down enforcement auditor.

Category:
Configuration

Cause:
An internal error occurred; the enforcement auditor shutdown failed.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

WSM-07613
Failure enforcing auditing policy.

Category:
Configuration

Cause:
An internal error occurred while auditing security or management policy enforcement.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

WSM-07614
Failure in Agent initialization due to invalid topology node path. Topology node path cannot be null or empty for non-JSE client. category={0}, function={1}, topologyNode={2}, isRunningInJEE={3}

Category:
Configuration

Cause:
Oracle WSM Agent initialization failed due to problem creating and initializing DMS instrumentation. An invalid, null, or empty topology node path was encountered for non-JSE client.

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

WSM-07616
Resource name not retrievable from MessageContext. Guard evaluation requires resource name to be present in MessageContext

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Security

Cause:
Resource name not retrievable from MessageContext. Guard evaluation requires resource name to be present in MessageContext

Action:
Retry the operation. If the problem persists, contact Oracle Support Services.

WSM-07617
Policy: {0} contains unsupported assertions.

Category:
Security

Cause:
Policy contains unsupported assertions. Assertions of type http-security are not supported for WLS JAXWS web services.

Action:
Check the assertion type.

WSM-07618
Failed to execute the assertion "{0}" in the conditional policy. {1}

Category:
Security

Cause:
Failed to execute the assertion

Action:
Check exception stack trace for details

WSM-07619
Failed to retrieve the Weblogic Server subject.

Category:
Security

Cause:
An error occurred while retrieving Weblogic Server subject.

Action:
Check log file for possible cause.

WSM-07620
Agent cannot enforce policies due to either failure in retrieving polices or error in validations, detail= "{0}".

Category:
Security

Cause:
Either policies can not be retrieved or Policy/PolicySet have validation errors.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Correct the validation errors and retry again.

WSM-07621
Oracle WSM Advertisement Engine failed with valid PolicySet, validation errors: [{0}], and PolicySet: [{1}]

Category:
Other

Cause:
Advertisment failed due to runtime PolicySet validation error in WSMEngineInvoker

Action:
Check log for detail to correct Runtime PolicySet

WSM-07622
The agent instance for enforcement cannot be null for scope "{0}". Check logs for details.

Category:
Data

Cause:
The agent instance for enforcement is null.

Action:
Check server logs for more details.

WSM-09001
The audit event definitions cannot be found.

Category:
Configuration

Cause:
Component audit event definitions were missing.

Action:
Check the installation for any missing or corrupted JAR files.

WSM-09002
The audit event definitions file cannot be opened.

Category:
Configuration

Cause:
Component audit event definitions could not be opened.

Action:
Check the installation for any corrupted JAR files, or free up system resources.

WSM-09003
The audit event definitions file cannot be read.

Category:
Configuration

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
Component's audit event definitions were not readable.

Action:
Check the installation for any corrupted JAR files.

WSM-09004
Component auditing cannot be initialized.

Category:
Logging

Cause:
The audit framework encountered an error.

Action:
Check the logs for the possible causes.

WSM-09005
It is not possible to verify that the event is enabled.

Category:
Logging

Cause:
The audit framework encountered an error.

Action:
Check the logs for the possible causes.

WSM-09006
The event cannot be audited. Another attempt will be made to audit the event.

Category:
Logging

Cause:

Action:

WSM-09007
The event cannot be audited.

Category:
Logging

Cause:
The audit framework encountered an error.

Action:
Check the logs for the possible causes.

WSM-09008
A URL cannot be created for {0}.

Category:
Logging

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
XML utility encountered an error.

Action:
Check the logs for the possible causes.

WSM-09009
Failure parsing the XML file

Category:
Logging

Cause:
XML utility encountered an error.

Action:
Check the logs for the possible causes.

WSM-09010
Error opening and/or closing the stream

Category:
Logging

Cause:
XML utility encountered an error.

Action:
Check the logs for the possible causes.

WSM-09011
Error writing the XML file

Category:
Logging

Cause:
XML utility encountered an error.

Action:
Check the logs for the possible causes.

WSM-09012
Key, {0}, is not found in the resource bundle {1}.

Category:
Configuration

Cause:
No key was found in the provided resource bundle.

Action:
Add the key to the resource bundle and retry the operation.

WSM-09013
Failure shutting down auditing.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Category:
Logging

Cause:
An exception was caught when attempting to shut down the audit framework.

Action:
Examine the stack trace for any underlying errors.

WSM-09014
Streaming SOAP message attachment is not being logged.

Category:
Logging

Cause:
SOAP message attachment was not logged because it was a streaming attachment.

Action:
Check the logs for the possible causes.

WSM-09015
Interrupted while checking out object from pool.

Category:
Other

Cause:
Received interrupt while checking out from pool.

Action:
Check the logs for the possible causes.

WSM-09016
Failure creating transformer using factory {0}.

Category:
Other

Cause:
Transformer factory failed to create new transformer instance.

Action:
Check the logs for the possible causes.

WSM-09017
Failure checking out a transformer instance.

Category:
Other

Cause:
Failure checking out a transformer instance.

Action:
Check the logs for the possible causes.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WSM-09018
A ScheduledExecutorService is required when creating a scheduler wrapper.

Category:
Other

Cause:
A ScheduledExecutorService was not provided when constructing a wrapper.

Action:
Provide a valid ScheduledExecutorService instance.

WSM-09019
An executor requires a task for scheduling.

Category:
Other

Cause:
A task was not provided when scheduling a task.

Action:
Provide a valid task.

WSM-09020
An executor rejected a task due to error "{0}".

Category:
Other

Cause:
The ScheduledExecutorService refused to schedule a task.

Action:
Check the logs for the possible causes.

WSM-09021
A TimerManager is required when creating a scheduler wrapper.

Category:
Other

Cause:
A TimerManager was not provided when constructing a wrapper.

Action:
Provide a valid TimerManager instance.

WSM-09022
A timer cannot schedule a task due to illegal argument error "{0}".

Category:
Other

Cause:
A task was not provided when scheduling a task. The scheduling parameters were negative.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Action:
Provide a valid task. Provide non-negative values.

WSM-09023
A timer cannot schedule a task due to illegal state error "{0}".

Category:
Other

Cause:
A task could not be scheduled because the underlying TimerManager was stopped.

Action:
Schedule the task using a running TimerManager.

WSM-09024
Failure parsing the XML URL when: {0}, from: {1}

Category:
Logging

Cause:
XML utility parseXMLDocument from URL encountered an error.

Action:
Check the logs for the possible causes.

WSM-09025
Unable to initialize WSM Coherence cache service, Defaulting to local Coherence cache. {0}

Category:
Logging

Cause:
Unable to initialize Coherence cache service.

Action:
Make sure that the Coherence is properly configured for the cluster environment.

WSM-09027
Resource bundle {0} is missing.

Category:
Configuration

Cause:
Resource bundle is missing.

Action:
Add the resource bundle and retry the operation.

WSM-09028
Failed to get server log directory due to error {0}.

Category:
Other

Copyright © 2007, 2026, Oracle and/or its affiliates.

Cause:
Failed to get server Log directory.

Action:
See logs for details.

WSM-09029
Diagnostic logging handler creation failed due to error {0}.

Category:
Other

Cause:
Failed to create handler for diagnosis logs.

Action:
See logs for details.

autodeploy

This directory provides a quick way to deploy applications in a development server. When the Oracle WebLogic Server instance is running in development mode, it automatically deploys any applications or modules that you place in this directory.

The files you place in this directory can be Jakarta EE applications, such as:

- An EAR file
- A WAR, EJB JAR, RAR, or CAR archived module
- An exploded archive directory for either an application or a module

bin

This directory contains scripts that are used in the process of starting and stopping the Administration Server and the Managed Servers in the domain. These scripts are provided as `.sh` files for UNIX and `.cmd` files for Windows. The `bin` directory can optionally contain other scripts of domain-wide interest, such as scripts to start and stop database management systems, full-text search engine processes, and such. See Administering Server Startup and Shutdown for Oracle WebLogic Server.

config

This directory contains the current configuration and deployment state of the domain. The central domain configuration file, `config.xml`, resides in this directory.

config/configCache

Contains data that is used to optimize performance when validating changes in the domain's configuration documents. This data is internal to Oracle WebLogic Server and does not need to be backed up.

Copyright © 2007, 2026, Oracle and/or its affiliates.

config/diagnostics

This directory contains system modules for instrumentation in the WebLogic Diagnostic Framework. See Configuring and Using the Diagnostics Framework for Oracle WebLogic Server.

config/jdbc

This directory contains system modules for JDBC: global JDBC modules that can be configured directly from JMX (as opposed to JSR-88). See Database Connectivity for Oracle WebLogic Server.

config/jms

This directory contains system modules for JMS: global JMS modules that can be configured directly from JMX (as opposed to JSR-88). See Messaging for Oracle WebLogic Server.

config/nosql

This directory contains external descriptors for NoSQL system resources. The default location is `DOMAIN_HOME/config/nosql/<mapped-name>-nosql.xml`; the filename is derived from the resource name using the platform filename mapping. `NoSQLSystemResourceMBean.DescriptorFileName` is relative to the domain's `config` directory and is established when the resource is created; it is read-only afterward. When supplying an explicit filename at creation, use a single filename ending in `-nosql.xml`, optionally prefixed by `nosql/`. Absolute paths, traversal, alternate directories, null explicit filenames, and malformed filenames are rejected. Use the one-argument creator to derive the filename automatically.

Use supported management tools to maintain the domain entry and external descriptor together. Include both components in configuration backup and restore procedures, together with the platform security material required to use protected configuration values. A domain without configured NoSQL resources need not contain this directory.

The NoSQL descriptor namespace is `http://xmlns.oracle.com/weblogic/nosql-resource`; its schema location is `http://xmlns.oracle.com/weblogic/nosql-resource/1.0/weblogic-nosql.xsd`. For the detailed namespace, schema, and file contract, see Resource Configuration and Files in Administering NoSQL Resources for Oracle WebLogic Server.

config/lib

This directory is not used in the current release of Oracle WebLogic Server.

config/nodemanager

This directory holds information for connection to the Node Manager. See Node Manager Configuration and Log Files in *Administering Node Manager for Oracle WebLogic Server*.

config/security

This directory contains system modules for the security framework. It contains one security provider configuration extension for each kind of security provider in the current realm of the domain. See *Understanding Security for Oracle WebLogic Server*.

Copyright © 2007, 2026, Oracle and/or its affiliates.

configArchive

This directory contains a set of JAR files that save the domain's configuration state. Just before pending changes to the configuration are activated, the domain's existing configuration state, consisting of the `config.xml` file and the other related configuration files, is saved in a versioned JAR file with a name like `config-1.jar`, `config-2.jar`, and so on.

The maximum number of versioned JAR files to be kept is specified by the `archiveConfigurationCount` attribute of `DomainMBean`. Once this maximum number is reached, the oldest configuration archive is deleted before a new one is created.

init-info

This directory contains files used for WebLogic domain provisioning. You should not modify any files in this directory.

lib

JAR files you put in this directory are made available (within a separate system level classloader) to all Jakarta EE applications running on WebLogic Server instances in the domain. See Adding JARs to the Domain `/lib` Directory in *Developing Applications for Oracle WebLogic Server*.

pending

This directory contains domain configuration files representing configuration changes that have been requested, but not yet activated. Once the configuration changes have been activated, the configuration files are deleted from this directory. See Managing Configuration Changes.

security

This directory holds those security-related files that are the same for every Oracle WebLogic Server instance in the domain:

- `SerializedSystemIni.dat`

This directory also holds security-related files that are only needed by the domain's Administration Server:

- `DefaultAuthorizerInit.ldift`
- `DefaultAuthenticatorInit.ldift`
- `DefaultRoleMapperInit.ldift`
- XACMLRoleMapperInit.ldift

See *Understanding Security for Oracle WebLogic Server*.

servers

This directory contains one subdirectory for each Oracle WebLogic Server instance in the domain. The sub-directories contain data that is specific to each server instance.

For more information about server naming convention, see Domain and Server Name Restrictions.

Copyright © 2007, 2026, Oracle and/or its affiliates.

servers/*server-name*

This directory is the server directory for the Oracle WebLogic Server instance with the same name as the directory. The name must conform to the guidance in Domain and Server Name Restrictions.

servers/*server-name*/cache

This directory holds directories and files that contain cached data. By "cached" we mean that the data is a copy, possibly in a processed form (compiled, translated, or reformatted), of other data.

servers/*server-name*/cache/EJBCompilerCache

This directory is a cache for compiled EJBs.

servers/*server-name*/data

This directory holds files that maintain persistent per-server state used to run the Oracle WebLogic Server instance, other than security state, as opposed to temporary, cached or historical information. Files in this directory are important data that must be retained as the Oracle WebLogic Server instance is brought up, is brought down, crashes, restarts, or is upgraded to a new version.

servers/*server-name*/data/ldap

This directory holds the embedded LDAP database. The run-time security state for the Oracle WebLogic Server instance is persisted in this directory.

servers/*server-name*/data/store

This directory holds WebLogic persistent stores. For each persistent store, there is a subdirectory that holds the files that represent the persistent store. The name of the subdirectory is the name of the persistent store. By convention there is one store named `default`.

servers/*server-name*/logs

This directory holds logs and diagnostic information. This information is historical in nature. It is not crucial to the operation of the server, and can be deleted (while the Oracle WebLogic Server instance is down, at least) without affecting proper operation. However, the information can be quite useful for debugging or auditing purposes and should not be deleted without good reason.

servers/*server-name*/logs/diagnostic_images

This directory holds information created by the Server Image Capture component of the WebLogic Diagnostic Framework. See *Configuring and Using the Diagnostics Framework for Oracle WebLogic Server*.

Copyright © 2007, 2026, Oracle and/or its affiliates.

servers/*server-name*/logs/jmsServers

This directory contains one subdirectory for each JMS server in the Oracle WebLogic Server instance. Each such subdirectory contains the logs for that JMS server. The name of the subdirectory is the name of the JMS server.

servers/*server-name*/security

This directory holds security-related files that can be or must be different for each Oracle WebLogic Server instance. The file `boot.properties` is an example of a file that resides here because it can differ from one server to the next. This directory also maintains files related to SSL keys.

servers/*server-name*/tmp

This directory holds temporary directories and files that are created while a server instance is running. For example, a JMS paging directory is automatically created here unless another location is specified. Files in this directory must be left alone while the server is running, but may be freely deleted when the server instance is shut down.

tmp

This directory stores temporary files used in the change management process. You should not modify any files in this directory.

A Server's Root Directory

All instances of Oracle WebLogic Server use a root directory to store their working copy of the domain's configuration files, to store run-time data, and to provide the context for any relative path names in the server's configuration.

An Administration Server always uses the domain directory as its root directory. A Managed Server can use the domain directory but can also use any other directory that you define.

For example, if you start a Managed Server on a computer that does not share a file system with the computer that hosts the Administration Server, the Managed Server creates its own root directory. The server copies data from the domain directory to this root directory and writes run-time data in this directory.

> **Note**
>
> To create a Managed Server instance in a directory that is outside the domain directory, Oracle recommends using the `pack` command with the `-managed=true` option, or the Configuration Wizard. However, if you create a Managed Server manually by starting it in an empty directory outside the domain directory, you must first copy the `security` directory, and its contents, from the Administration Server directory to your Managed Server directory.

You can specify the path and name of the server root directory for each server instance. You can specify a common server root directory for multiple server instances hosted on a single

Copyright © 2007, 2026, Oracle and/or its affiliates.

computer or you can specify a different server root directory for each server. A domain has one or more server root directories.

Specifying a Server Root Directory

You can specify the path for the server root directory by one of the following means:

- Use the `-Dweblogic.RootDirectory=path` option when starting a Oracle WebLogic Server instance from command line. For example, the following command starts a Oracle WebLogic Server instance and uses `c:\MyServerRootDirectory` as the server root directory:

  ```
  java -Dweblogic.RootDirectory=c:\MyServerRootDirectory weblogic.Server
  ```

- If you use Node Manager to start an Oracle WebLogic Server instance, you can specify a server root directory with the *Root Directory* attribute in the WebLogic Remote Console on the **Environment**: **Servers**: *myServer*: **Advanced**: **Node Manager** page. For more information, see Configure Startup Arguments for a Managed Server in the *Oracle WebLogic Remote Console Online Help*.

If you do not use one of the above means to specify a server root directory, the path and name of the server root directory depend on whether a server instance is a Managed Server or the Administration Server and whether or not you use Node Manager to start the server instance. These variations are discussed in the next sections.

Server Root Directory for an Administration Server

An Administration Server uses its server root directory as a repository for the domain's configuration data (such as `config.xml`) and security resources (such as the default, embedded LDAP server).

To determine the root directory for an Administration Server, Oracle WebLogic Server does the following:

- If the server's startup command includes the `-Dweblogic.RootDirectory=path` option, then the value of *path* is the server root directory.
- If `-Dweblogic.RootDirectory=path` is not specified, then the working directory is the server root directory.

If Oracle WebLogic Server cannot find a `config.xml` file, then it offers to create one. You can use this method to create a new domain. See Using the weblogic.Server Command Line to Create a Domain in the *Command Reference for Oracle WebLogic Server*.

Server Root Directory for a Managed Server Started with Node Manager

If you use the Node Manager to start a Managed Server, the root directory is located on the computer that hosts the Node Manager process. To determine the location of the server's root directory, Oracle WebLogic Server does the following:

- If you specified a root directory in the WebLogic Remote Console on the **Environment**: **Servers**: *myServer*: **Advanced**: **Node Manager** page, then the directory you specified is the server root directory.
- If you did not specify a root directory in the WebLogic Remote Console, then the server root directory is:

  ORACLE_HOME`\user_projects\domains\domain-name\servers\managed-server-name`

Copyright © 2007, 2026, Oracle and/or its affiliates.

where *ORACLE_HOME* is the directory in which you installed Oracle WebLogic Server on the Node Manager's host computer.

Server Root Directory for a Managed Server Not Started with Node Manager

If you do not use the Node Manager to start a Managed Server (and therefore use the `java weblogic.Server` command or a script that calls that command), Oracle WebLogic Server does the following to determine the root directory:

- If the server's startup command includes the `-Dweblogic.RootDirectory=`*path* option, then the value of *path* is the server's root directory.
- If `-Dweblogic.RootDirectory=`*path* is not specified, then the working (current) directory is the root directory. For example, if you run the `weblogic.Server` command from `c:\config\MyManagedServer`, then `c:\config\MyManagedServer` is the root directory.

To make it easier to maintain your domain configurations and applications across upgrades of Oracle WebLogic Server software, it is recommended that the server root directory not be the same as the installation directory for the Oracle WebLogic Server software.

Copyright © 2007, 2026, Oracle and/or its affiliates.

3

Managing Configuration Changes

The change management process in Oracle WebLogic Server provides a secure and predictable means for distributing configuration changes in domains. In this process, in-memory changes can be made using editable Configuration MBeans.

This chapter includes the following sections:

Overview of Change Management

To provide a secure, predictable means for distributing configuration changes in a domain, WebLogic Server imposes a change management process that loosely resembles a database transaction.

Each domain describes its configuration in an XML document that is located in the domain's configuration directory. At run time, each Oracle WebLogic Server instance in a given domain creates an in-memory representation of the configuration described in this document. The in-memory representation of a domain's configuration is a collection of read-only managed beans (MBeans) called Configuration MBeans.

In addition to the read-only Configuration MBeans, the Administration Server maintains another collection of Configuration MBeans that you can edit (see Figure 3-1). To edit these Configuration MBeans, you obtain a lock using any of the administration tools listed in Summary of System Administration Tools and APIs in *Understanding Oracle WebLogic Server*.

While you have the lock on the editable Configuration MBeans, you can save your in-memory changes, which cause the Administration Server to write the changes to a set of pending configuration documents in the domain directory. Oracle WebLogic Server instances do not consume the changes until you activate the changes.

When you activate changes, each server in the domain determines whether it can accept the change. If all servers are able to accept the change, they update their copy of the domain's configuration document. Then they update their working copy of Configuration MBeans and the change is completed (see Figure 3-2).

Configure NoSQL resources offline only while the domain is inactive. For an existing domain, use `readDomain`, make the configuration changes, call `updateDomain`, and finish with `closeDomain`. For a new domain, follow the template-based `writeDomain` procedure. Persist the resource registration, external descriptor, properties, protected values, and target references as one complete configuration. After starting the domain, confirm that the resource and its intended targets load correctly and that the bound application can be deployed without repairing the configuration online. Verify database access separately through an authorized application operation.

For the offline procedure and startup checks, see Configure a Resource using Offline Tools in Administering NoSQL Resources for Oracle WebLogic Server.

Oracle WebLogic Server's change management process applies to changes in domain and server configuration data, not to security or application data.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Changes Requiring Server Restart

Some configuration changes can take effect on the fly, while others require the affected servers to be restarted before they take effect. Configuration changes that can take effect without a server restart are sometimes referred to as *dynamic* changes; configuration changes that require a server restart are sometimes referred to as *non-dynamic* changes. In the WebLogic Remote Console, an attribute that requires a server restart for changes to take effect is marked with this icon:



Edits to dynamic configuration attributes become available once they are activated, without restarting the affected server or system resource. Edits to non-dynamic configuration attributes require that the affected servers or system resources be restarted before they become effective.

If an edit is made to a non-dynamic configuration setting, no edits to dynamic configuration settings 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.

NoSQL Configuration Changes

NoSQL system-resource creation, descriptor changes, targeting changes, and removal are dynamic. A valid, compatible provider-property-only update drains and replaces provider runtimes while preserving stable application manager and repository handles and the selected global resource identity. Applications must reacquire generation-bound capabilities retained from the former configuration generation.

An accepted change affecting resource selection or provider compatibility, resource removal, untargeting, or resource unavailability that terminally invalidates a deployment requires full application redeployment after the intended configuration is restored. Stopping and starting an application, changing its administration mode, or making a later compatible edit does not clear that invalidation. Rejected proposals, rollback of a prepared update, and an unchanged activation preserve the active generation.

For update classification and application recovery procedures, see Update a Resource and Recover Applications in Administering NoSQL Resources for Oracle WebLogic Server.

Configuration Change Tools

As described in Summary of System Administration Tools and APIs in *Understanding Oracle WebLogic Server*, you can use a variety of different Oracle WebLogic Server tools to make configuration changes:

- WebLogic Remote Console
- WebLogic Scripting Tool
- RESTful management APIs
- JMX APIs

Whichever tool you use to make configuration changes, Oracle WebLogic Server handles the change process in basically the same way.

Copyright © 2007, 2026, Oracle and/or its affiliates.

For more information about how configuration changes are carried out through JMX and Configuration MBeans, see Understanding WebLogic Server MBeans in *Developing Custom Management Utilities Using JMX for Oracle WebLogic Server*. For more information about making configuration changes with WLST, see Configuring Existing Domains in *Understanding the WebLogic Scripting Tool*.

Configuration Auditing

Using the WebLogic Auditing provider or another auditing security provider, you can record audit information about changes made to your Oracle WebLogic Server configuration. See Enabling Configuration Auditing in *Administering Security for Oracle WebLogic Server*.

Change Management in the Remote Console

After you connect an Administration Server to the WebLogic Remote Console, you are ready to make configuration changes to your domain.

In the WebLogic Remote Console, it is generally two-step process to apply configuration changes to your domain. For detailed change management information, see Configuring a WebLogic Server Domain in the *Oracle WebLogic Remote Console Online Help*.

Configuration Change Management Process

Configuration changes happen in basically the same way, regardless of the method you choose to use (the WebLogic Remote Console, WLST, JMX or REST APIs).

The following steps describe the process in detail, starting from when you first boot the domain's Administration Server:

> **Note**
>
> Do not add non-configuration files in the `config` directory or subdirectories. Non-configuration files include log (.log) and lock (.lck) files. Administration Server replicates the `config` directory in all Managed Server instances. Storing non-configuration files in the `config` directory can cause performance issues in the domain.

1. When the Administration Server starts, it reads the domain's configuration files, including the `config.xml` file and any subsidiary configuration files referred to by the `config.xml` file and uses the data to instantiate the following MBean trees in memory:
   - A read-only tree of Configuration MBeans that contains the current configuration of resources that are on the Administration Server.
   - An editable tree of all Configuration MBeans for all servers in the domain.

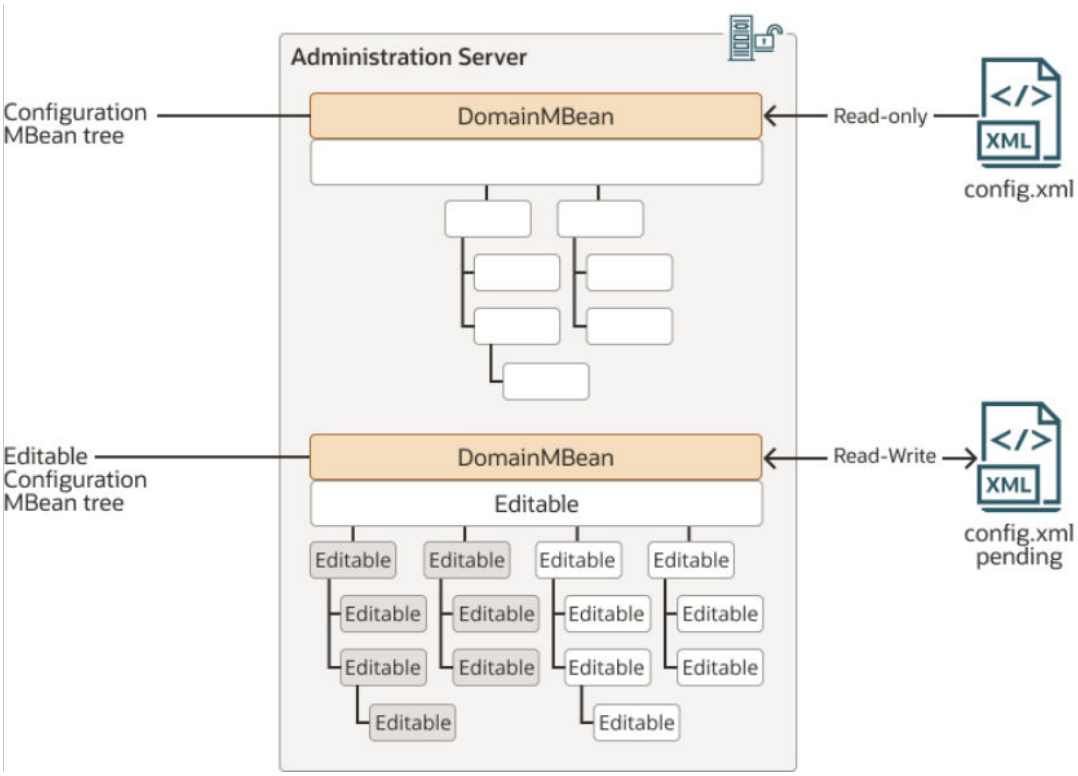
   > **Note**
   >
   > The Administration Server also instantiates a Runtime MBean tree and a DomainRuntime MBean tree, but these are not used for configuration management.

Copyright © 2007, 2026, Oracle and/or its affiliates.

2. To initiate a configuration change, you do the following:
   a. Obtain a lock on the current configuration.
   b. Make any changes you desire, using the tool of your choice (the WebLogic Remote Console, WLST, the JMX APIs, and such).
   c. Save your changes to a pending version of the `config.xml` file, using the **Save** button in the WebLogic Remote Console; using the WLST `save` command; or using the `save` operation on the `ConfigurationManagerMBean`.
3. The Configuration Manager service saves all data from the edit MBean tree to a separate set of configuration files in a directory named `pending`. See Figure 3-1.

   The `pending` directory is immediately below the domain's root directory. For example, if your domain is named `mydomain`, then the default pathname of the pending `config.xml` file is `mydomain/pending/config.xml`.

Figure 3-1 The Administration Server's Pending config.xml File



4. Make additional changes or undo changes that you have already made.
5. When you are ready, activate your changes in the domain, in the Remote Console, open the Shopping Cart and then click **Commit Changes**; using the WLST `activate` command; or using the `activate` operation on the `ConfigurationManagerMBean`.

   When you activate changes (see Figure 3-2):
   a. For each server instance in the domain, the Configuration Manager service copies the pending configuration files to a `config` directory in the server's root directory.

      If a Managed Server shares its root directory with the Administration Server, `ConfigurationManagerMBean` does not copy the pending configuration files; the Managed Server uses the Administration Server's `config` directory.

Copyright © 2007, 2026, Oracle and/or its affiliates.

b. Each server instance compares its current configuration with the pending configuration.

c. Subsystems within each server vote on whether they can consume the new configuration.

   If any subsystem indicates that it cannot consume the changes, the entire activation process is rolled back and the `ConfigurationManagerMBean` emits an exception. You can modify your changes and retry the change activation, or you can abandon your lock, in which case the edit Configuration MBean tree and the pending configuration files are reverted to the configuration in the read-only Configuration MBean tree and configuration files.

d. If all subsystems on all servers can consume the change, the Configuration Manager service replaces the read-only configuration files on each server instance in the domain with the pending configuration files.

e. Each server instance updates its beans and its read-only Configuration MBean tree according to the changes in the new configuration files. In cases that include one or more changes that require the server to be restarted, this occurs the next time the server is restarted.

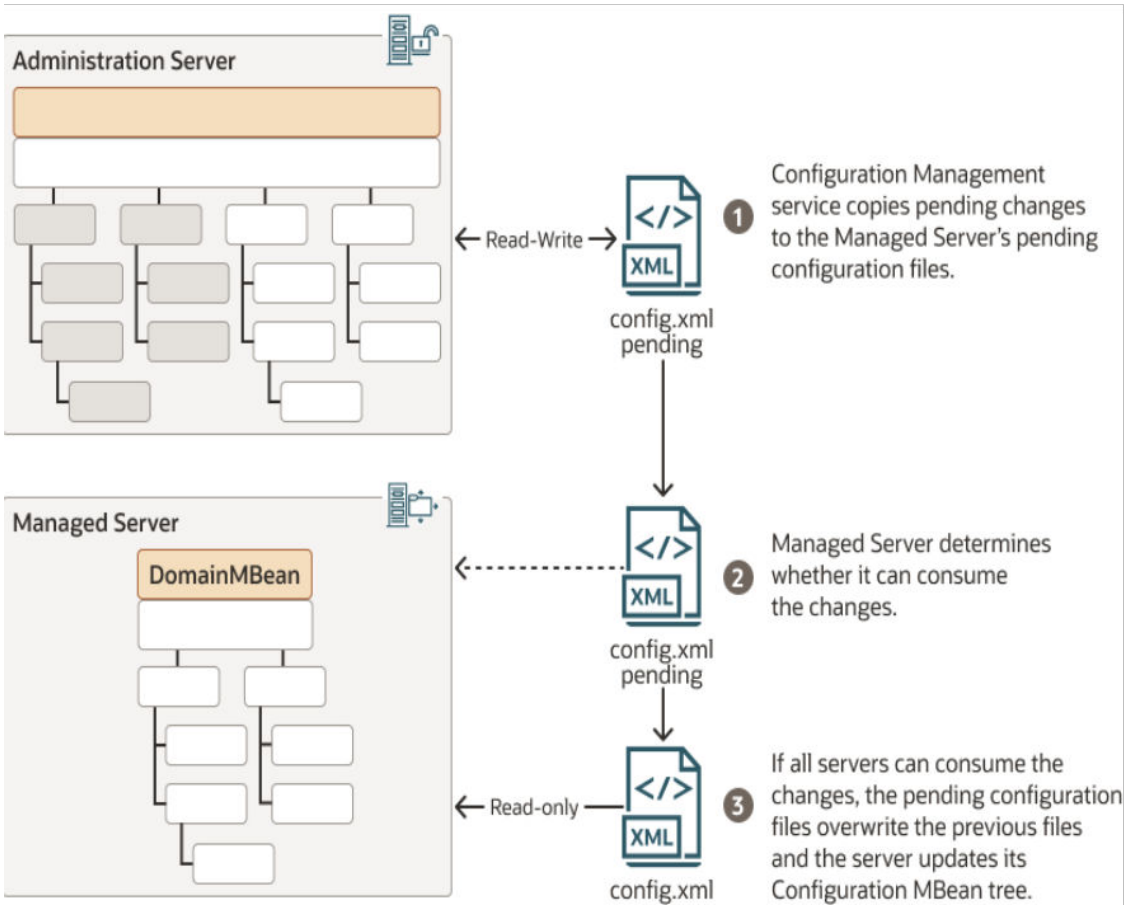
f. The pending configuration files are then deleted from the `pending` directory.

> **Note**
>
> If the Administration Server crashes before completing activation of your changes (step 5.f), upon restart, the Administration Server will recover the pending configuration files saved in step 5.a. In the log file, this process is referred to as `config recovery`.

6. You can retain your lock to make additional changes or release it so that others can update the configuration. You can configure a time-out period that causes the Configuration Manager service to abandon a lock.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Figure 3-2 Activating Changes in Managed Servers



Configuration Locks

When you start an edit session, whether you use the WebLogic Remote Console, WLST, or the Management APIs, you obtain a lock on the Configuration MBean edit tree.

The configuration change lock does not by itself prevent you from making conflicting configuration edits using the same administrator user account. For example, if you obtain a configuration change lock using the WebLogic Remote Console, and then use the WebLogic Scripting Tool with the same user account, you will access the same edit session that you opened in the WebLogic Remote Console and you will not be locked out of making changes with the Scripting Tool. You can reduce the risk that such a situation might occur by maintaining separate administrator user accounts for each person with an administrative role. Similar problems can still occur, however, if you have multiple instances of the same script using the same user account.

To reduce further the risk of this situation, you can obtain an *exclusive* configuration change lock. When you have an exclusive configuration lock, a subsequent attempt to start an edit session by the same owner will wait until the edit session lock is released. To obtain an exclusive configuration lock using WLST, use `true` for the exclusive argument in the `startEdit` command:

```
wls:/mydomain/edit> startEdit(60000, 120000, true)
```


Copyright © 2007, 2026, Oracle and/or its affiliates.

To obtain an exclusive configuration edit lock using the Management API, pass `true` as the third argument to `ConfigurationManagerMBean.startEdit`:

```
DomainMBean editableDomain = configurationManager.startEdit(60000, 120000, true);
```

Here, `configurationManager` is the `ConfigurationManagerMBean` for the selected edit session.

You cannot modify the domain configuration using the compatibility MBean server when either of the following is true:

- there is an existing editing session, or
- there are pending changes saved, but not yet activated from a previous edit session.

Resolving Change Conflicts

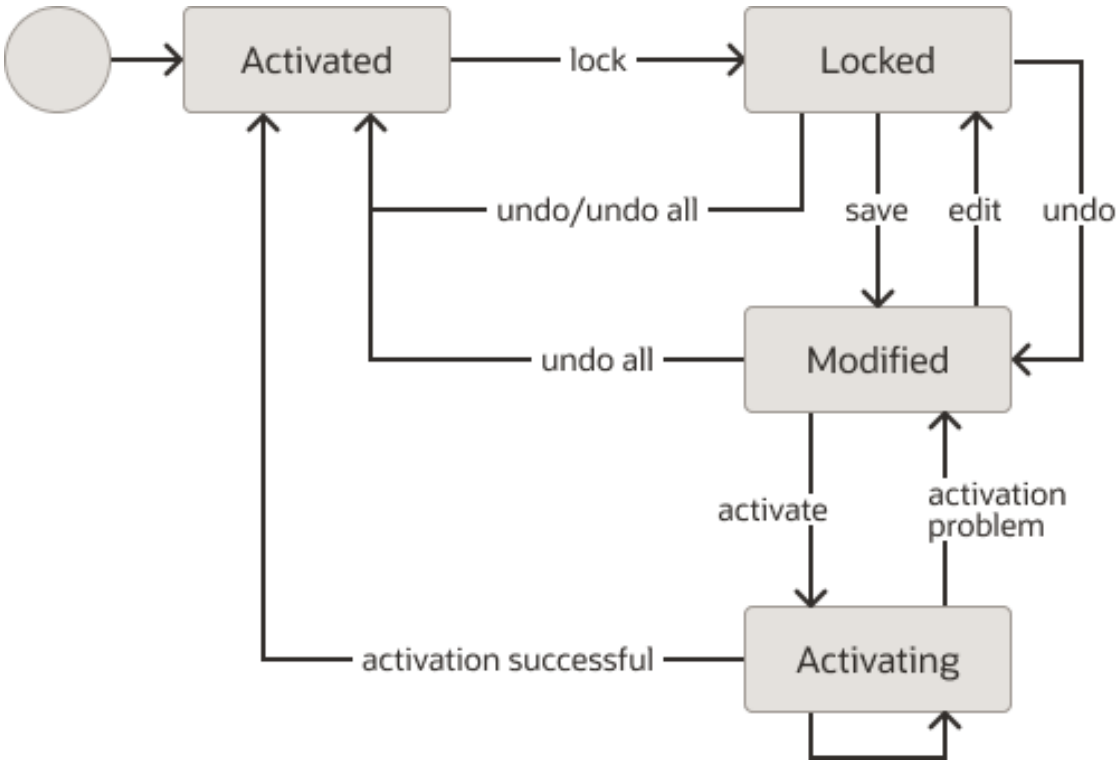
In the event that you have saved more than one change set without activating them and one change would invalidate a prior change, the Change Management service requires you to manually resolve the invalidation before it will save your changes.

Configuration Management State Diagram

The Configuration Management service follows a series of states.

These states are described in Figure 3-3.

Figure 3-3 Configuration Management State Diagram



Copyright © 2007, 2026, Oracle and/or its affiliates.

Restricting Configuration Changes

You can block configuration changes by setting a domain to be read-only. Do this by setting the `EditMBeanServerEnabled` attribute of the `JMXMBean` configuration MBean to false, using either WLST or the Management APIs.

Once you have set your domain to be read-only, you can no longer edit its configuration using the WebLogic Remote Console, WLST online, or the Management APIs. To make the domain editable again, you must either edit the `config.xml` file directly in a text editor, or use WLST offline, and then restart the affected servers.

You must establish appropriate access controls to the domain's configuration, limiting access to users with the proper security roles. In addition, using the WebLogic Auditing provider or another auditing security provider, you can record audit information about changes made to your Oracle WebLogic Server configuration. See Enabling Configuration Auditing in *Administering Security for Oracle WebLogic Server*.

Configuration Overriding

Configuration overriding lets administrators place configuration information, contained in an XML file, in a known location where running servers identify and load it, overriding aspects of the existing configuration.

In large clusters or complex distributed environments, such as in cloud platforms, setting and removing configuration properties can be challenging due to network, software, and scaling issues. Situations arise where you might want or need to run your servers in Managed Server Independence Mode (MSI) mode. You can use configuration overriding (also called *situational configuration*) to change settings such as server debugging flags, timeout values, or diagnostics settings, without running the Administration Server. The configuration overrides are targeted to Managed Servers but can also be applied to the Administration Server. When using configuration overriding, there is no synchronization between the Administration Server and Managed Servers. Configuration overriding bypasses the Administration Server as the primary means of distributing configuration information to Managed Servers.

Situational configuration lets you place a file containing configuration changes (overrides) that need to be added to a running WebLogic Server instance. The overrides may have an expiration time to ensure that the configuration changes do not remain in effect longer than necessary or they can be permanent; no expiration time is specified. In an earlier release of WebLogic Server, an overridden domain configuration required an expiration time and was therefore always temporary. However, this limitation is now removed. For more information, see “Temporary Configuration Overriding” in *Understanding Domain Configuration for Oracle WebLogic Server*.

Consider this scenario. In certain environments, you might want to allow for different size clusters. You could have a base configuration for all environments, combined with configuration overrides that provide the appropriate configurations for small, medium, or large clusters. This allows the common, shared configuration to be separate from the cluster-size specific configurations. For example, certain servers are needed only in the large cluster environment. In the small cluster environment, the administrator does not want these servers to be present. The administrator creates a situational configuration file that deletes the servers. At runtime, the situational configuration file is loaded and the unwanted servers are removed from the configuration.

Situational configuration:

Copyright © 2007, 2026, Oracle and/or its affiliates.

- Applies a configuration change to a running system; it does not impact the stored configuration.
- Employs an XML fragment, in a file, which contains values to be changed and context information. The file is used to update configuration information coming from the `config.xml` file or system resource files that exist in the `jdbc`, `jms`, and `diagnostics` subdirectories of the domain `config` directory.
- Can replace configuration element values, add new configuration elements, or delete existing configuration elements.
- Can update dynamic and non-dynamic attributes. However, when changes include non-dynamic modifications that were applied after the server was started, the server will not update a situational configuration change until the next server start.
- May contain an expiration time for the configuration override, but it is not required. Overrides are reverted when the XML file is removed, renamed, or expired.
- Contains an option to *require* that situational configuration files be present, and if not found, then the server startup fails.
- Does not require involvement by the Administration Server and the Managed Servers do not synchronize their values in any way.

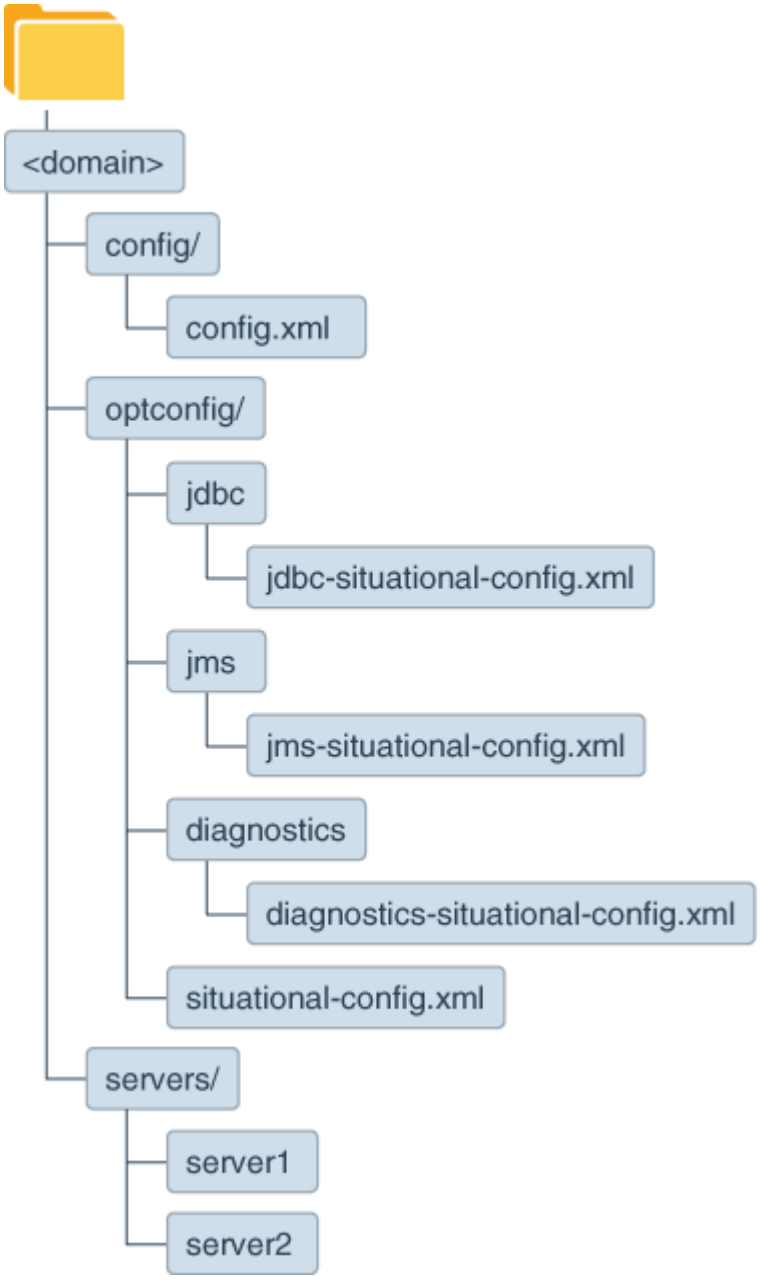
If a value which is currently overridden by a situational configuration is changed in an edit session, that change will *not* take effect until the situational configuration overrides are removed. Situational configuration will log a message in the server's log when it is applied and expired or removed.

About Situational Configuration Files, Names and Locations

Situational configuration files end with the suffix "`situational-config.xml`" and are domain configuration files, which, by default, reside in an `optconfig` directory. In the case of JDBC, JMS, and diagnostic system resources, they reside in `jdbc`, `jms`, and `diagnostics` subdirectories of `optconfig`.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Figure 3-4 Domain Configuration File Directories Layout



Administrators create, update, and delete `situational-config.xml` files. If the domains are located on separate systems, the situational configuration XML files must be copied into each `optconfig` directory.

For JDBC, JMS, and diagnostic system resource files, the situational configuration file name *must* match the system resource file name, then add the `situational-config.xml` suffix. For example, a JMS system resource named *myqueues-jms.xml*, can be overridden only by a file with the name *myqueues-jms-situational-config.xml*.

Copyright © 2007, 2026, Oracle and/or its affiliates.

Overriding the Default File Location

Using the system property, `weblogic.SituationalConfigPath`, you can override the default `optconfig` directory location for `situational-config.xml` files.

To set the value, choose an absolute directory path and retain any previously configured Java options: `export JAVA_OPTIONS="${JAVA_OPTIONS:+$JAVA_OPTIONS }-Dweblogic.SituationalConfigPath=/absolute/path/to/optconfig"` Then start the server.

For example:

```
export JAVA_OPTIONS="${JAVA_OPTIONS:+$JAVA_OPTIONS }"
JAVA_OPTIONS+='-Dweblogic.SituationalConfigPath=$optconfig:$domainroot/mydir:/scratch/
myoptconfig'
export JAVA_OPTIONS
```

This example is for Bash/Zsh. The single quotes preserve the literal `$optconfig` and `$domainroot` tokens for WebLogic Server to replace.

The following substitutions are supported:

- `$domainroot` - the domain root directory
- `$optconfig` - the default location for `optconfig`, for example, `$domainroot/optconfig`

You can locate `situational-config.xml` files in server-specific directories under a defined `optconfig` directory. For example, the Administration Server will look for situational configuration files in `$domainroot/optconfig` and `$domainroot/optconfig/<administration-server-name>`. On a Managed Server, `ms1`, the server will look for situational configuration files in `$domainroot/optconfig` and `$domainroot/optconfig/ms1`.

For each configured search path, WebLogic Server watches the path itself, its `<server-name>` subdirectory, and its direct `jdbc`, `jms`, and `diagnostics` subdirectories. Place system-resource fragments in those direct system-resource subdirectories; do not rely on nested `<server-name>/jdbc`, `<server-name>/jms`, or `<server-name>/diagnostics` directories.

The system property can be a colon-separated list of paths, for example: `$optconfig:$domainroot/mydir:/scratch/myoptconfig`. Given this example path, the server will look for (process) situational configuration files in the following order:

```
<domain root>/optconfig
<domain root>/optconfig/<servername>
<domain root>/optconfig/jms
<domain root>/optconfig/jdbc
<domain root>/optconfig/diagnostics

<domain root>/mydir/
<domain root>/mydir/<servername>
<domain root>/mydir/jms
<domain root>/mydir/jdbc
<domain root>/mydir/diagnostics

/scratch/myoptconfig
/scratch/myoptconfig/<servername>
/scratch/myoptconfig/jms
/scratch/myoptconfig/jdbc
/scratch/myoptconfig/diagnostics
```


Copyright © 2007, 2026, Oracle and/or its affiliates.

File Format

A situational configuration file contains an XML fragment that references the structure of the configuration it is modifying. For example, to modify this server's debug configuration in `config.xml`:

```
<domain .... >
  <name>sitconfigDomain</name>
  <server>
    <name>admin</name>
    <server-debug>
    </server-debug>
  </server>
...
```

The situational configuration XML fragment would look like this:

These examples omit an expiration element, so the override remains in effect until the file is removed or renamed. To use a temporary override, add an expiration time later than the current time; see File Expiration.

```
<?xml version='1.0' encoding='UTF-8'?>
<dom:domain
 xmlns:dom="http://xmlns.oracle.com/weblogic/domain"
 xmlns:f="http://xmlns.oracle.com/weblogic/domain-fragment"
 xmlns:s="http://xmlns.oracle.com/weblogic/situational-config" >
  <dom:name>sitconfigDomain</dom:name>
  <dom:server>
    <dom:name>admin</dom:name>
    <dom:server-debug>
      <dom:debug-jmx-core f:combine-mode="replace">true</dom:debug-jmx-core>
    </dom:server-debug>
  </dom:server>
  </dom:domain>
```

In the following example, `debug-jmx-core`, is *not* replaced (overridden) because part of the path (`<server-debug>`) is missing.

```
<f:domain  xmlns=.... >
   <dom:server>
     <dom:name>admin</dom:name>
      <dom:debug-jmx-core f:combine-mode="replace">true</dom:debug-jmx-core>
   </dom:server>
</f:domain>
```

Schemas

Situational configuration XML fragments include entries from multiple schemas. The `situational-config` schema provides information on how the situational configuration will be applied; for example, its expiration time. The rest of the fragment contains information on how to modify the in-memory contents of `config.xml` or system resource file.

The `situational-config.xsd` contains these lines:

```
    <?xml version="1.0" encoding="UTF-8" ?>
    <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
         <!-- expiration time for this file -->
        <xs:element name="expiration" type="xs:string"/>
    </xs:schema>
```


Copyright © 2007, 2026, Oracle and/or its affiliates.

Declare `http://xmlns.oracle.com/weblogic/domain-fragment` for the `f` prefix and use `f:combine-mode` to specify each modification. Use the following example:

```
<?xml version="1.0" encoding="UTF-8"?>
<dom:domain xmlns:dom="http://xmlns.oracle.com/weblogic/domain" xmlns:f="http://
xmlns.oracle.com/weblogic/domain-fragment" xmlns:s="http://xmlns.oracle.com/weblogic/
situational-config">
 <dom:name>sitconfigDomain</dom:name>
 <dom:server><dom:name>admin</dom:name><dom:server-debug><dom:debug-jmx-core f:combine-
mode="replace">true</dom:debug-jmx-core></dom:server-debug></dom:server>
</dom:domain>
```

Situational configuration fragments for system resources are similar to the situational configuration files for `config.xml` overrides. For JDBC, JMS, and diagnostic system resource files, the XML situational configuration and namespaces are specific to the system resource type (JMS, JDBC, or WLDF). The rest of the fragment contains information on how to modify the in-memory contents of the system resource. Consider the following example situational configuration files for JMS, JDBC, and WLDF system resources.

- A JMS situational configuration file that overrides the shared configuration element and the expiration policy:

  ```
  <?xml version='1.0' encoding='UTF-8'?>
  <jms:weblogic-jms
   xmlns:jms="http://xmlns.oracle.com/weblogic/weblogic-jms"
   xmlns:f="http://xmlns.oracle.com/weblogic/weblogic-jms-fragment"
   xmlns:s="http://xmlns.oracle.com/weblogic/situational-config" >
   <jms:quota jms:name="MyTemplate.Quota">
      <jms:shared f:combine-mode="replace">true</jms:shared>
   </jms:quota>
    <jms:template jms:name="MyTemplate">
      <jms:delivery-failure-params>
        <jms:expiration-policy f:combine-mode="replace">Discard</jms:expiration-policy>
      </jms:delivery-failure-params>
    </jms:template>
  </jms:weblogic-jms>
  ```

- A JDBC file that adds a user name and password property:

  ```
  <?xml version="1.0" encoding="UTF-8"?>
  <jdbc:jdbc-data-source
   xmlns:jdbc="http://xmlns.oracle.com/weblogic/jdbc-data-source"
   xmlns:f="http://xmlns.oracle.com/weblogic/jdbc-data-source-fragment">
   <jdbc:name>jdbcDataSource</jdbc:name>
   <jdbc:jdbc-driver-params>
    <jdbc:properties>
     <jdbc:property f:combine-mode="replace">
      <jdbc:name>user</jdbc:name>
      <jdbc:value>Jones</jdbc:value>
     </jdbc:property>
     <jdbc:property f:combine-mode="replace">
      <jdbc:name>password</jdbc:name>
      <jdbc:value>REPLACE_WITH_TEST_PASSWORD</jdbc:value>
     </jdbc:property>
    </jdbc:properties>
   </jdbc:jdbc-driver-params>
  </jdbc:jdbc-data-source>
  ```

  The password value is a placeholder for an isolated example. Protect configuration files containing credentials; do not publish or commit real passwords.

- A diagnostics file that enables instrumentation:

Copyright © 2007, 2026, Oracle and/or its affiliates.

```
<?xml version="1.0" encoding="UTF-8"?>
<wldf:wldf-resource
 xmlns:wldf="http://xmlns.oracle.com/weblogic/weblogic-diagnostics"
 xmlns:f="http://xmlns.oracle.com/weblogic/weblogic-diagnostics-fragment">
 <wldf:instrumentation>
  <wldf:enabled f:combine-mode="replace">true</wldf:enabled>
 </wldf:instrumentation>
</wldf:wldf-resource>
```

To add or delete configuration elements, use the syntax, `f:combine-mode="add"` or `f:combine-mode="delete"`, as shown in the following examples.

- The following configuration file fragments demonstrate adding both basic datatypes (String, int, Boolean) and arrays of nested elements. Elements are added at both the domain and nested server layer:

```
<?xml version='1.0' encoding='UTF-8'?>
<dom:domain
 xmlns:dom="http://xmlns.oracle.com/weblogic/domain"
 xmlns:f="http://xmlns.oracle.com/weblogic/domain-fragment"
 xmlns:s="http://xmlns.oracle.com/weblogic/situational-config" >
  <dom:name>sitconfigDomain</dom:name>
  <dom:notes f:combine-mode="add">Situational Config Domain</dom:notes>
  <dom:archive-configuration-count f:combine-mode="add">2</dom:archive-configuration-
count>
  <dom:startup-class f:combine-mode="add">
    <dom:deployment-order>33</dom:deployment-order>
    <dom:name>AddedStartupClassOne</dom:name>
  </dom:startup-class>
  <dom:startup-class f:combine-mode="add">
    <dom:deployment-order>44</dom:deployment-order>
    <dom:name>AddedStartupClassTwo</dom:name>
  </dom:startup-class>
  <dom:server>
    <dom:name>admin</dom:name>
    <dom:notes f:combine-mode="add">admin server</dom:notes>
    <dom:server-debug>
      <dom:debug-jmx-core f:combine-mode="add">true</dom:debug-jmx-core>
    </dom:server-debug>
    <dom:max-message-size f:combine-mode="add">78787878</dom:max-message-size>
  </dom:server>
</dom:domain>
```

- The following configuration file fragments demonstrate adding a new server to the domain:

```
<?xml version='1.0' encoding='UTF-8'?>
<dom:domain
  xmlns:dom="http://xmlns.oracle.com/weblogic/domain"
 xmlns:f="http://xmlns.oracle.com/weblogic/domain-fragment"
 xmlns:s="http://xmlns.oracle.com/weblogic/situational-config" >
  <dom:name>sitconfigDomain</dom:name>
  <dom:server f:combine-mode="add">
    <dom:name>addedServer</dom:name>
    <dom:notes>addedServer notes</dom:notes>
    <dom:listen-port>7401</dom:listen-port>
    <dom:tgiop-enabled>false</dom:tgiop-enabled>
    <dom:network-access-point>
      <dom:name>AddedNetworkAccessPointOne</dom:name>
      <dom:listen-port>7501</dom:listen-port>
    </dom:network-access-point>
    <dom:network-access-point>
      <dom:name>AddedNetworkAccessPointTwo</dom:name>
      <dom:listen-port>7601</dom:listen-port>
```


Copyright © 2007, 2026, Oracle and/or its affiliates.

```
    </dom:network-access-point>
  </dom:server>
</dom:domain>
```

- The following configuration file fragments demonstrate deleting both basic datatypes (String, int, Boolean). Elements are deleted at both the domain and nested server layer:

```
<?xml version='1.0' encoding='UTF-8'?>
<dom:domain
  xmlns:dom="http://xmlns.oracle.com/weblogic/domain"
 xmlns:f="http://xmlns.oracle.com/weblogic/domain-fragment"
 xmlns:s="http://xmlns.oracle.com/weblogic/situational-config" >
  <dom:name>sitconfigDomain</dom:name>
  <dom:configuration-version f:combine-mode="delete"></dom:configuration-version>
  <dom:server>
    <dom:name>MyServerOne</dom:name>
    <dom:listen-port f:combine-mode="delete"></dom:listen-port>
    <dom:network-access-point f:combine-mode="delete"></dom:network-access-point>
   </dom:server>
  <dom:server>
    <dom:name>MyServerTwo</dom:name>
    <dom:listen-port f:combine-mode="delete"></dom:listen-port>
  </dom:server>
  <dom:server>
    <dom:name>ms1</dom:name>
    <dom:accept-backlog f:combine-mode="delete"></dom:accept-backlog>
    <dom:ignore-sessions-during-shutdown f:combine-mode="delete"></dom:ignore-
sessions-during-shutdown>
  </dom:server>
</dom:domain>
```

XML Namespaces

The following table summarizes the XML namespaces used by situational configuration files.

xmlns Type	Example	Description
Domain	`xmlns:dom="http://xmlns.oracle.com/weblogic/domain"`	Used for domain situational `config.xml` overrides to identify domain elements, for example, `<dom:domain>`.
Domain Fragment	`xmlns:f="http://xmlns.oracle.com/weblogic/domain-fragment"`	Used for domain `config.xml` overrides to identify domain fragment elements, for example, `f:combine-mode="replace"` inside a domain element.
Situational Configuration	`xmlns:s="http://xmlns.oracle.com/weblogic/situational-config"`	Used for domain config.xml and system resource overrides to identify situational configuration elements, for example, `<s:expiration>`.
JMS	`xmlns:jms="http://xmlns.oracle.com/weblogic/weblogic-jms"`	Used to identify JMS system resource elements, for example, `<jms:template name="JMSTemplate1">`.
JDBC	`xmlns:jdbc="http://xmlns.oracle.com/weblogic/jdbc-data-source"`	Used to identify JDBC system resource elements, for example, `<jdbc:jdbc-driver-params>`.
Diagnostics	`xmlns:wldf="http://xmlns.oracle.com/weblogic/weblogic-diagnostics"`	Used to identify WLDF system resource elements, for example, `<wldf:watch-notification>`.

Copyright © 2007, 2026, Oracle and/or its affiliates.

xmlns Type	Example	Description
JMS System Resource Fragment	`xmlns:f="http://xmlns.oracle.com/weblogic/weblogic-jms-fragment"`	Used for JMS system resource overrides to identify JMS system resource fragment elements, for example, `f:combine-mode="replace"` inside a JMS system resource element.
JDBC System Resource Fragment	`xmlns:f="http://xmlns.oracle.com/weblogic/jdbc-data-source-fragment"`	Used for JDBC system resource overrides to identify JDBC system resource fragment elements, for example, `f:combine-mode="replace"` inside a JDBC system resource element.
WLDF System Resource Fragment	`xmlns:f="http://xmlns.oracle.com/weblogic/weblogic-diagnostics-fragment"`	Used for WLDF system resource overrides to identify WLDF system resource fragment elements, for example, `f:combine-mode="replace"` inside a WLDF system resource element.

File Expiration

If desired, you can set an explicit expiration time in the XML fragment file by referencing the `situational-config.xsd` schema and then setting the expiration time element. The expiration time is either a long (system time) or a W3C-compliant string.

The following historical timestamps illustrate the syntax; replace them with a future time before testing an expiring override.

For example:

```
<s:expiration> 2020-11-29T10:24-08:00 </s:expiration>
     11/29/2020 @ 10:24 am (UTC−08:00)

<s:expiration> 2020-11-29T10:24 </s:expiration>
     11/29/2020 @ 10:24 am (local timezone)

<s:expiration> 2020-11-29T10:24:15 </s:expiration>
     11/29/2020 @ 10:24:15 am (local timezone)
```

The situational configuration values will be in place until either the file is removed or the system time exceeds the expiration time. After that happens, the file and its values will be unloaded and the settings will return to their previous values. If the situational configuration file has a timeout value which is earlier than the current time (the file has expired), the contents of the file will be ignored.

To enable a *permanent* situational configuration file with no expiration, specify either no expiration element or an expiration element value of minus one (`-1`).

- An example permanent situational configuration file with no expiration element:

```
<?xml version="1.0" encoding="UTF-8"?>
<dom:domain xmlns:dom="http://xmlns.oracle.com/weblogic/domain" xmlns:f="http://
xmlns.oracle.com/weblogic/domain-fragment" xmlns:s="http://xmlns.oracle.com/weblogic/
situational-config">
 <dom:name>sitconfigDomain</dom:name>
 <dom:server><dom:name>admin</dom:name><dom:server-debug><dom:debug-jmx-core
f:combine-mode="replace">true</dom:debug-jmx-core></dom:server-debug></dom:server>
</dom:domain>
```

- An example permanent situational configuration file with an expiration of -1:

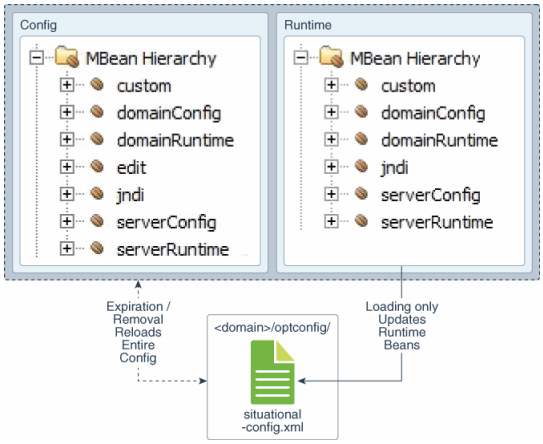
Copyright © 2007, 2026, Oracle and/or its affiliates.

```
<?xml version='1.0' encoding='UTF-8'?>
<dom:domain
  xmlns:dom="http://xmlns.oracle.com/weblogic/domain"
 xmlns:f="http://xmlns.oracle.com/weblogic/domain-fragment"
 xmlns:s="http://xmlns.oracle.com/weblogic/situational-config" >
  <s:expiration>-1</s:expiration>
  <dom:name>sitconfigDomain</dom:name>
    <dom:server>
      <dom:name>admin</dom:name>
      <dom:server-debug>
        <dom:debug-jmx-core f:combine-mode="replace">true</dom:debug-jmx-core>
      </dom:server-debug>
    </dom:server>
  </dom:domain>
```

Loading Situational Configurations

The situational configuration file exists when a server is started. Situational configurations are loaded into the runtime hierarchy, not the edit configuration hierarchy. Administrators can see the effective configuration (base configuration + situational configuration overrides) by looking at the runtime tree. The configuration edit tree shows only the base values before the situational configuration was applied or after the situational configuration is removed.

Figure 3-5 Loading and Removal of Situational Configuration Files



Accessing the Edit and Runtime Configuration Using WLST

Given:

- A `config.xml` with a domain `Notes` attribute, "My Domain"
- A situational configuration file that overrides the domain `Notes` attribute with the value, "My New Domain"

Using WLST, you can access the values in the runtime and edit configurations as follows:

```
# runtime configuration
serverConfig()
wls:/mydomain/serverConfig/> print cmo.getNotes()
My New Domain
# edit configuration
wls:/mydomain/serverConfig/> edit()
wls:/mydomain/edit/> print cmo.getNotes()
My Domain
```


Copyright © 2007, 2026, Oracle and/or its affiliates.

Processing Multiple Fragments

Each situational configuration XML fragment is stored in its own `situational-config.xml` file; only one fragment per file is allowed. If multiple fragments are available, there will be multiple situational configuration files, each named uniquely. For example:

```
wildcard-situational-config.xml
example1-situational-config.xml
foobar-situational-config.xml
```

Situational configuration files are loaded based on their modification date, such that the oldest file is loaded first, then subsequent files are processed (loaded).

Using Wildcards

In XML fragments, you can use wildcards to make them more flexible, such as, to process the same set of configuration settings on multiple resources.

For example, to override identical debug settings on all servers in a cluster:

```
<f:domain
  xmlns=.... >
    <dom:server>
     <dom:name>'*'</dom:name>
     <dom:max-message-size f:combine-mode="replace">30000000</dom:max-message-size>
      <dom:server-debug>
               <dom:debug-jmx-core f:combine-mode="replace">true</dom:debug-jmx-core>
      </dom:server-debug>
   </dom:server>
</f:domain>
```

Only one wildcard is supported, `'*'` (an asterisk, escaped within single quotation marks). It matches everything.

Follow these rules when using wildcards:

- Use wildcards in elements only.
  - Wildcards let you replace a specific element with an asterisk (*) and have it match any element within the same set of tags.
  - The wildcard can match any element. For example, if you change the server name, `admin`, to *, any settings in the fragment which were targeted for `admin` would now be applied to all servers. For example: `<name>'*'</name>`
- Tags cannot contain wildcards. The following is not supported: `<'*'>admin</'*'>`
- Elements which are to be modified (overridden) cannot have wildcards. The following are not supported:

```
<dom:debug-jmx-core f:combine-mode='*'>'*'</dom:debug-jmx-core>
<dom:debug-jmx-core f:combine-mode="replace">'*'</dom:debug-jmx-core>
```

- A wildcard replaces a whole word (all or nothing); there are no partial matches. For example, if the string is LKS, * will match; L* or LK* will *not* match and generate an error.
- You can use wildcards to add or delete elements. However, because only asterisk ('*') is supported, the add or delete applies to all MBeans. For example, if used with a Server MBean, this action would delete all the servers in the domain. Consider the following examples.

Copyright © 2007, 2026, Oracle and/or its affiliates.

- The following configuration file fragments demonstrate the use of a wildcard to add basic datatype and container elements to all servers in the domain.

```
<?xml version='1.0' encoding='UTF-8'?>
<dom:domain
  xmlns:dom="http://xmlns.oracle.com/weblogic/domain"
 xmlns:f="http://xmlns.oracle.com/weblogic/domain-fragment"
 xmlns:s="http://xmlns.oracle.com/weblogic/situational-config" >
  <s:expiration> 2020-11-30T19:20+01:00 </s:expiration>
  <dom:name>sitconfigDomain</dom:name>
  <dom:server>
    <dom:name>'*'</dom:name>
    <dom:notes f:combine-mode="add">wildcard notes</dom:notes>
    <dom:server-debug>
      <dom:debug-jmx-core f:combine-mode="add">true</dom:debug-jmx-core>
    </dom:server-debug>
    <dom:cluster-weight f:combine-mode="add">49</dom:cluster-weight>
      <dom:network-access-point f:combine-mode="add">
        <dom:name>AddedNetworkAccessPoint</dom:name>
        <dom:enabled>false</dom:enabled>
        <dom:listen-port>7501</dom:listen-port>
      </dom:network-access-point>
   </dom:server>
</dom:domain>
```

- The following configuration file fragments demonstrate the use of a wildcard to delete basic datatypes from all servers in the domain.

```
<?xml version='1.0' encoding='UTF-8'?>
<dom:domain
  xmlns:dom="http://xmlns.oracle.com/weblogic/domain"
 xmlns:f="http://xmlns.oracle.com/weblogic/domain-fragment"
 xmlns:s="http://xmlns.oracle.com/weblogic/situational-config" >
  <s:expiration> 2020-11-30T19:20+01:00 </s:expiration>
  <dom:name>sitconfigDomain</dom:name>
  <dom:server>
    <dom:name>'*'</dom:name>
    <dom:accept-backlog f:combine-mode="delete"></dom:accept-backlog>
    <dom:server-debug>
      <dom:debug-jms-back-end f:combine-mode="delete"></dom:debug-jms-back-end>
    </dom:server-debug>
  </dom:server>
</dom:domain>
```

Wildcard Overrides

If a file has both wildcard and non-wildcard entries for a value, the first one which matches prevails.

For example:

```
<dom:server>
   <dom:name>server2</dom:name>
    <dom:max-message-size f:combine-mode="replace">666666</dom:max-message-size>
</dom:server>
 <dom:server>
    <dom:name>'*'</dom:name>
     <dom:max-message-size f:combine-mode="replace">30000000</dom:max-message-size>
 </dom:server>
 <dom:server>
    <dom:name>server1</dom:name>
     <dom:max-message-size f:combine-mode="replace">9999999</dom:max-message-size>
 </dom:server>
```


Copyright © 2007, 2026, Oracle and/or its affiliates.

In this example, `server2` has a `max-message-size` of `666666` but `server1` has a value of `30000000` (because the * is above `server1` in the file).

Monitoring Situational Configuration Changes

Use the `ServerRuntimeMBean.isInSitConfigState()` method to check if a situational configuration is currently in place. For example:

```
ServerRuntimeMBean runtimeMBean = runtimeService.getServerRuntime();
    boolean setting = runtimeMBean.isInSitConfigState();
```

To control how frequently the server polls for situational configuration changes (new, removed, or changed `situational-config.xml` files), use `ServerMBean.setSitConfigPollingInterval(int)` to configure the polling period (in seconds).

For example, to set the polling rate:

```
    DomainMBean domainMBean = domainService.getDomainConfiguration();
    ServerMBean serverMBean = domainMBean.lookupServer(adminServerName);
    serverMBean.setSitConfigPollingInterval(value);
```

Require Situational Configuration

By default, applying a configuration override is optional. Under certain conditions, you might want to *require* a configuration override, for example, to prevent booting with the default large cluster configuration on a small pod. The `SitConfigRequired` attribute on the Server MBean controls whether a situational configuration is required or not. This configuration attribute causes the server to *not* start if no override files are applied. The default is to start the server and not fail.

```
/**
 * Sets whether situational config files are required. If required, then WebLogic Server
will
 * fail to boot if no situational config files are present. The default is to not
require situational config files.
 * @param isRequired - true if situational config files are required, false otherwise.
 * @default false
 * @dynamic
 * @include-api for-public-api
 */
void setSitConfigRequired(boolean isRequired);

/**
 * Returns whether situational config files are required and WebLogic Server should fail
to boot if situational config files are not present.
 * @return  true if situational config files are required, false otherwise.
 * @dynamic
 * @include-api for-public-api
 */
boolean isSitConfigRequired();
```

Using Named Concurrent Edit Sessions

In prior releases, WebLogic Server supported only one active configuration edit session at a time. The system administrator got a global edit lock, made changes, and then activated them. Other administrators could not make changes at the same time without first taking the configuration lock from another administrator, then editing the same active edit session. However, now WebLogic Server enables multiple, named concurrent edit sessions, which

Copyright © 2007, 2026, Oracle and/or its affiliates.

allows more than one administrator to make configuration changes in separate edit sessions at the same time.

The concurrent edit sessions are typically useful when multiple administrators work in different parts of the system. Also, when configuring a system takes a long time because of the serial execution of configuration commands, a single administrator can open multiple named edit sessions. This saves time by running the configuration edit sessions in parallel.

Copyright © 2007, 2026, Oracle and/or its affiliates.

4

Server Templates

Use server templates to easily manage configuration for a group of server instances in one centralized location. Learn how to create, configure, and use server templates in WebLogic Server.

This chapter includes the following sections:

What are Server Templates?

A server template contains common, non-default settings and attributes that you can apply to a set of server instances, which then inherit the template configuration. You can define server-specific values for server instances that require unique attributes by overriding the server template in the server instance definition.

At runtime, the domain merges the attributes configured in the server template with any server-specific overrides so that all attributes are defined for all server instances.

Example 4-1 shows an example `config.xml` file that uses a server template. In this example, common configuration is defined in the `<server-template>` element. The individual server definitions set server-specific attributes (`name`, `listen-port`) and specify the server template upon which to base additional configuration (`my-cluster-server-template`).

Example 4-1 Example config.xml File Using a Server Template

```
<server>
    <name>my-server-1</name>
    <listen-port>7010</listen-port>
    <server-template>my-cluster-server-template</server-template>
</server>

<server>
    <name>my-server-2</name>
    <listen-port>7020</listen-port>
    <server-template>my-cluster-server-template</server-template>
</server>

<server-template>
    <name>my-cluster-server-template</name>
    <accept-backlog>2000</accept-backlog>
    <cluster>my-cluster</cluster>
    <restart-max>10</restart-max>
    <reverse-dns-allowed>true</reverse-dns-allowed>
    <startup-timeout>600</startup-timeout>
</server-template>
```

Why Do You Use Server Templates?

Server templates enable you to easily manage configuration for a group of server instances in one centralized location. You can define common configuration attributes in a server template and then apply the template to other server instances without having to manually configure each one.

Copyright © 2007, 2026, Oracle and/or its affiliates.

You can use server templates in one of the following two ways:

- As the basis for any configured managed server
- As the basis for dynamic servers in a dynamic cluster

Use Server Templates as the Basis for Any Configured Managed Server

A server template serves as a way to simplify server configuration. The managed server inherits the configuration attributes from the server template it references except for attributes that are manually configured in the server configuration. You can override any configuration attribute in this case.

If you need to define any server-specific attributes, you can easily override the server template at the individual server level.

If you need to update an attribute across all server instances, you can simply change the value in the server template and the new value takes effect in all the server instances that use that server template. You do not need to write a WLST script to update all the servers in the domain.

Server templates also help with performance and startup time. Defining common attributes once in the server template, instead of setting the same attribute in each server instance definition, reduces the size of the `config.xml` file.

Use Server Templates as the Basis for Dynamic Servers in a Dynamic Cluster

You also use server templates to create dynamic clusters. You can define a specific server template to use as the basis for all dynamic servers in a dynamic cluster.

A dynamic cluster contains multiple dynamic servers that are based on a single-server template. This server template is the basis for all the servers in the cluster so that you do not need to manually configure each server when expanding the cluster. When you use a server template to create a dynamic cluster and specify the number of server instances you want, WebLogic Server inherits and calculates necessary values from the server template and then uses these calculated values for the attributes. You cannot change individual server configuration for dynamic servers except for system properties that you would specify when starting the server. To know more about how to create, configure, and use dynamic clusters in WebLogic Server, see Dynamic Clusters in *Administering Clusters for Oracle WebLogic Server*.

Using Server Templates

You create server templates using WebLogic Scripting Tool (WLST) or the WebLogic Remote Console.

To create server templates using WLST, see Example 4-2. To create server templates using the WebLogic Remote Console, see Create a Server Template in the *Oracle WebLogic Remote Console Online Help*.

To configure server templates, you can use any of the administration tools listed in Summary of System Administration Tools and APIs in *Understanding Oracle WebLogic Server*.

Overriding Attributes

A server template contains different types of attributes, including primitive datatypes, singleton elements, and arrays of configuration elements. To override a server template value, you define the attribute in the individual server definition.

Copyright © 2007, 2026, Oracle and/or its affiliates.

WebLogic Server determines which attribute value to use based on the following override hierarchy:

- If you do not define an attribute in the individual server configuration or in the server template, then the default value is used.
- If you define an attribute in the server template, then the server template overrides the default value. The server template value is used.
- If you define an attribute in the individual server configuration, then the server configuration overrides the server template value and the default value. The individual server configuration value is used.

> **Note**
>
> Once you override a value in the individual server configuration, this value always takes precedence over the value in the server template. To remove the overridden value and use the value in the server template, use the `unSet` attribute command.

At runtime, the domain merges the attributes defined in the server template and individual server definitions to return the desired configuration.

A server instance can override attributes from a server template, but the overrides for each type of attribute differ. For primitive datatypes, the server configuration value overrides the value in the server template. For example, if the server template defines the listen port to be `7101`, but you set an explicit listen port value in the server configuration, the server instance value overrides the server template listen port value.

A server instance also overrides values for attributes contained within a child singleton element. For example, if the server template defines a common root directory value in the `<server-start>` child element, but you set an explicit root directory value in the `<server-start>` element in the server configuration, the server instance overrides the server template root directory value.

Named child configuration beans, such as `NetworkAccessPoints`, are inherited by name. Adding a differently named child to a server does not remove the other inherited children. A server-specific child with the same name can override attributes of the inherited child.

The following example demonstrates overriding `NetworkAccessPoints` in a server instance by using WLST, and includes inline comments.

```
#
#A server template named Cluster Template defines a NetworkAccessPoint named
#AccessPoint-1. The server instance s1 references Cluster Template as its
#template. A ls() command on s1 shows the following:
#

wls:/mydomain/edit/Servers/s1/NetworkAccessPoints !> ls

drw- AccessPoint-1

#
#Server instance s1 then defines a NetworkAccessPoint at the server instance
#level.
#

wls:/mydomain/edit/Servers/s1 !>
cmo.createNetworkAccessPoint("AccessPoint-2")
```


Copyright © 2007, 2026, Oracle and/or its affiliates.

```
#
#The server retains inherited AccessPoint-1 and adds its own AccessPoint-2.
#

wls:/mydomain/edit/Servers/s1/NetworkAccessPoints !> ls

drw- AccessPoint-1
drw- AccessPoint-2
```

Using Macros

Server templates contain common attributes and provide the same values for each server instance that inherits configuration from the template. In some cases, you may want to define a standard value for an attribute, but the value must be slightly different for each server instance. You can define the server-specific attribute value in each server instance, but if the attribute follows a pattern, you may be able to use a macro.

You can define a macro for any string attribute in a server template. Macros are case sensitive and cannot be used for integers or references to other configuration elements. The valid macros available for use in server templates are:

- `${id}`: Instance ID of the dynamically created server; this ID starts at `1`.
- `${serverName}`: The name of the server to which this element belongs.
- `${clusterName}`: The name of the cluster to which this element belongs. If this element does not belong to a cluster, then an empty string is substituted.
- `${domainName}`: The name of the domain to which this element belongs.
- `${system-property-name}`: If this is not one of the predefined macro names listed previously, then it is evaluated as a system property, and the value is returned. If the system property does not exist, then an empty string is substituted.

Server Templates Example

Examine an example that demonstrates using WLST to create two server instances that use the same server template.

Example 4-2 includes inline comments and describes how to:

1. Create a server template and name it `my-cluster-server-template`.
2. Set all of the common attributes in `my-cluster-server-template`.
3. Create server instances `my-server1` and `my-server2`, and assign the `my-cluster-server-template` to each one.
4. Set server-specific attributes.

Example 4-2 Using Server Templates with WLST

```
#
# This example demonstrates the WLST commands needed to create a server template
# (my-cluster-server-template) and server instances (my-server-1, my-server-2)
# that use the server template. The creation of the cluster (my-cluster) and
# machines (PrimaryMachine, SecondaryMachine) are not included in this example;
# they must be created before running this script. To keep this example
# simple, error handling was omitted.
#
connect()
```


Copyright © 2007, 2026, Oracle and/or its affiliates.

```
edit()
startEdit()
#
# Create the server template and set the common attributes that are used in all
# servers. Attributes such as Accept Backlog, Auto Restart, etc. are the same
# across all cluster members.
#
serverTemplate=cmo.createServerTemplate("my-cluster-server-template")
serverTemplate.setAcceptBacklog(2000)
serverTemplate.setAutoRestart(true)
serverTemplate.setRestartMax(10)
serverTemplate.setReverseDNSAllowed(true)
serverTemplate.setStagingMode("external_stage")
serverTemplate.setStartupTimeout(600)
myCluster=cmo.lookupCluster("my-cluster")
serverTemplate.setCluster(myCluster)
#
# Create the individual server instances, set the server specific attributes, and
# set the template so the server uses the common attributes from the template.
# Attributes such as cluster weight, listen port, and machine are server-specific
# so they are not included in the server template.
#
server1=cmo.createServer("my-server-1")
server1.setClusterWeight(70)
server1.setListenPort(7010)
primary=cmo.lookupMachine("PrimaryMachine")
server1.setMachine(primary)
server1.setServerTemplate(serverTemplate)
#
server2=cmo.createServer("my-server-2")
server2.setClusterWeight(90)
server2.setListenPort(7020)
secondary=cmo.lookupMachine("SecondaryMachine")
server2.setMachine(secondary)
server2.setServerTemplate(serverTemplate)
#
# activate the changes
#
activate()
```

The resulting `config.xml` file is:

```
<server>
    <name>my-server-1</name>
     <cluster-weight>70</cluster-weight>
     <listen-port>7010</listen-port>
     <machine>PrimaryMachine</machine>
     <server-template>my-cluster-server-template</server-template>
</server>

<server>
     <name>my-server-2</name>
     <cluster-weight>90</cluster-weight>
     <listen-port>7020</listen-port>
     <machine>SecondaryMachine</machine>
     <server-template>my-cluster-server-template</server-template>
</server>

<server-template>
     <name>my-cluster-server-template</name>
     <accept-backlog>2000</accept-backlog>
     <auto-restart>true</auto-restart>
```


Copyright © 2007, 2026, Oracle and/or its affiliates.

```
        <cluster>my-cluster</cluster>
        <restart-max>10</restart-max>
        <reverse-dns-allowed>true</reverse-dns-allowed>
        <staging-mode>external_stage</staging-mode>
        <startup-timeout>600</startup-timeout>
    </server-template>
```


Copyright © 2007, 2026, Oracle and/or its affiliates.