

**Oracle® Fusion Middleware**

Help Reference for Oracle Mobile Security Suite Consoles

11g Release 2 (11.1.2.3)

**E57093-03**

October 2016

E57093-03

Copyright © 2016 Oracle and/or its affiliates. All rights reserved.

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

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

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

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. 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 and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon 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, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

# Contents

## Part I Mobile Security Manager (MSM) Console Help

### 1 Devices Page Help

1.1	Search .....	1-1
1.2	Device Management .....	1-3
1.2.1	Device Details Tab .....	1-4
1.2.2	Device Credentials Tab .....	1-5
1.2.3	Device Policies Tab .....	1-6
1.3	Workspace Management .....	1-9
1.3.1	Workspace Details Tab .....	1-10
1.3.2	Workspace Apps Tab .....	1-11
1.3.3	Workspace Activity Tab .....	1-11
1.3.4	Workspace Credentials Tab .....	1-12
1.3.5	Workspace Policies Tab .....	1-13

### 2 Mobile App Catalog Page Help

2.1	Mobile App Catalog Page .....	2-1
2.2	Add Application Dialog .....	2-2

### 3 Mobile Security Policies Page Help

3.1	Policy Search .....	3-1
3.2	Policy Management Page (Create Policy Page) .....	3-2

### 4 Mobile Roles Page Help

4.1	Roles Page .....	4-1
-----	------------------	-----

### 5 Mobile Users Page Help

5.1	Users Page .....	5-1
-----	------------------	-----

### 6 Device Configurations Help

6.1	Device Configurations Page .....	6-1
-----	----------------------------------	-----

## 7 Mobile Security Manager Settings Help

7.1	Client Settings.....	7-1
7.2	Server Settings .....	7-2
7.3	Identity Store Settings .....	7-4
7.4	CA Settings .....	7-5
7.5	User Notification Settings.....	7-6
7.6	Exchange Server Settings.....	7-7
7.7	Device Notification Settings .....	7-8
7.8	Apple Push Notification Service (APNS) Settings .....	7-8
7.9	Google Cloud Messaging (GCM) Settings .....	7-9
7.10	Notification Templates.....	7-10
7.11	MDM Agent Settings.....	7-11
7.12	Blacklisted Apps.....	7-12

## Part II Mobile Security Access Server (MSAS) Console Help

### 8 MSAS Applications Help

8.1	MSAS Applications Page .....	8-1
8.2	MSAS Applications Detail Page .....	8-5
8.3	Proxy URLs Page.....	8-7
8.4	URLs Page .....	8-9
8.5	URL Policy Configuration Page.....	8-11
8.6	Application Roles Summary Page.....	8-15
8.7	Application Roles Page .....	8-16

### 9 Environments Help

9.1	Environments Page.....	9-1
9.2	MSAS Instances Summary Page .....	9-2
9.3	MSAS Instance Configuration Page .....	9-3

### 10 Access Policies Help

10.1	Access Policies Page .....	10-1
10.2	Policy Details Page.....	10-3
10.3	Policy Version History Page.....	10-8
10.4	Assertion Templates Page.....	10-10
10.5	Assertion Templates Details Page .....	10-12

---

---

# Preface

This guide contains the contents of the online help that is included with the Mobile Security Manager and Mobile Security Access Server consoles.

## Audience

This document is intended for Systems Administrators who use the Mobile Security Manager and Mobile Security Access Server consoles to manage Oracle Mobile Security Suite.

## 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.

## Related Documents

For more information, see the following documents in the Oracle Fusion Middleware 11g Release 2 (11.1.2.3) documentation set:

- *Oracle Fusion Middleware Identity Management Release Notes*
- *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*
- *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite*
- *Oracle Fusion Middleware High Availability Guide for Oracle Identity and Access Management*
- *Oracle Fusion Middleware Administering Oracle Mobile Security Suite*
- *Oracle Fusion Middleware Administering Mobile Security Access Server*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*

## Conventions

The following text conventions are used in this document:

<b>Convention</b>	<b>Meaning</b>
<b>boldface</b>	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	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.

# Part I

## Mobile Security Manager (MSM) Console Help

This part contains reference documentation that describes how to use the Mobile Security Manager (MSM) console to manage Oracle Mobile Security Suite (OMSS).

This part contains the following chapters:

- [Chapter 1, "Devices Page Help"](#)
- [Chapter 2, "Mobile App Catalog Page Help"](#)
- [Chapter 3, "Mobile Security Policies Page Help"](#)
- [Chapter 4, "Mobile Roles Page Help"](#)
- [Chapter 5, "Mobile Users Page Help"](#)
- [Chapter 6, "Device Configurations Help"](#)
- [Chapter 7, "Mobile Security Manager Settings Help"](#)





---

---

## Devices Page Help

Use the Mobile Devices page to search for and view details about the devices and Workspaces registered to a user, and to perform routine administrative tasks on managed devices (Lock, Wipe, De-register, Sync, Clear/Reset Passcode) and Workspaces (Lock, Unlock, Wipe, Reset Passcode).

The following topics are covered:

- [Search](#)
- [Device Management](#)
- [Workspace Management](#)

### 1.1 Search

Use this section to:

- Search for devices and Workspaces.
- View the devices and Workspaces registered to a user.
- Select a managed device or Workspace to manage.

This view is arranged in the following sections:

- [Action Bar and Search](#)
- [Table of Users, Devices, and Workspaces \(Search Results\)](#)

#### Action Bar and Search



Search for users, then use the **Status** and **Sort** menus to further refine your search. The buttons on the action bar are described in the following table.


Element	Description
Search	<p>Type a search term and press the search button. Search results are returned as follows:</p> <ul style="list-style-type: none"><li>■ Devices and Workspaces are returned if the search term matches a device/Workspace display name, the model of the device/Workspace, the device/Workspace ID that is assigned by the server, or the user ID of the user who has enrolled the device/Workspace.</li></ul> <p>You cannot use wildcards but partial matches will return results, for example: <i>mith</i> will return results for "Smith."</p>

Element	Description
Status	<p>Choose from the following menu options:</p> <ul style="list-style-type: none"> <li>■ <b>Active</b> - Show registered and locked devices and Workspaces. This is the default option.</li> <li>■ <b>All</b> - Show all Workspaces regardless of status.</li> <li>■ <b>Registered</b> - Show devices that are enrolled in the system and not in a locked state.</li> <li>■ <b>Deregistered</b> - Show devices that are no longer enrolled in the system.</li> <li>■ <b>Locked</b> - Show Workspaces that have been locked and disallowed access to the server.</li> <li>■ <b>Wiped</b> - Show Workspaces with a status of wiped, which signifies that all data has been erased.</li> </ul>
Refresh	Click <b>Refresh</b> to update the screen with any changes made on the (back-end) server.
Sort	<p>Choose from the following menu options:</p> <ul style="list-style-type: none"> <li>■ <b>Last Sync Time</b> - Sort Workspace search results chronologically using the date and time that the device was last synchronized. This is the default option.</li> <li>■ <b>Name</b> - Sort Workspace search results alphabetically by name.</li> <li>■ <b>User</b> - Sort Workspace search results alphabetically by user name.</li> <li>■ <b>State</b> - Sort managed device and Workspace search results alphabetically by registration state.</li> <li>■ <b>Identifier</b> - Sort Workspace search results alphanumerically by GUID.</li> </ul>

### Table of Users, Devices, and Workspaces (Search Results)

This section of the Devices page lists users, devices, and Workspaces that meet the search criteria. Click a device or Workspace icon to view additional details and management options.

Element	Description
User Name (UID)	The user name (UID) of the user to which the device and/or Workspace is registered. A user with multiple devices will have multiple records, one record per device and/or Workspace.
	<p>Indicates a managed device. Click to manage the device and view additional details.</p> <p>The search results table displays the name given to the device.</p>
	Indicates an unmanaged device (that is, a device that belongs to the user). You cannot perform actions on unmanaged devices.

Element	Description
	<p>Click to manage the Workspace and view additional details.</p> <p>The search results table displays the Workspace's globally unique identifier (GUID).</p>

### Related Topics

"Managing Devices and Workspaces" in *Administering Oracle Mobile Security Suite*

## 1.2 Device Management

Use this section to:

- Manage a specific managed device registered to a user. (You cannot manage an unmanaged device.)
- View detailed information about a specific mobile device registered to a user.

This view is arranged in the following sections:

- [Action Bar](#)
- [Device Information Tabs](#)
  - [Device Details Tab](#)
  - [Device Credentials Tab](#)
  - [Device Policies Tab](#)




### Action Bar

Use the buttons to secure data on the device.

Element	Description
Lock	<p>Locks the device. The user can unlock the device by entering their PIN or password. Mobile Security Manager cannot unlock the device remotely.</p> <p><b>Note:</b> The device status displays as "Registered"; it does not change to "Locked."</p>
Wipe	Resets the device to its original factory state by erasing all of the stored settings, data, and applications.
De-register	Removes the Workspace app, including certificates, restrictions, and other content that was provisioned by the Mobile Security Manager. Containerized apps no longer work, but the user must delete them manually. All pending operations are cancelled, and certificates issued to the device are revoked. Following this action the device is no longer controlled by the server. In the console the device status displays as "De-registered," unless the <b>Device/Workspace De-registration Policy</b> (located in Server Settings) is set to <b>Delete</b> , in which case the device record is deleted from the server
Sync	Forces the device to synchronize with the Mobile Security Manager, to update the app, certificates, restrictions, and other content that was provisioned.

Element	Description
Clear Passcode / Reset Passcode	<p>This action is intended for use when the device user forgets their password.</p> <ul style="list-style-type: none"> <li>For iOS devices, the Clear Passcode command removes the Passcode and grants the user access to the device.</li> <li>For Android devices, the Reset Passcode command resets the passcode to a new randomly generated passcode. If using the Self-Service Console, the new passcode is displayed on the screen. Otherwise, a Help Desk Administrator or System Administrator should communicate the new passcode to the user.</li> </ul>

### Device Information Tabs

Element	Description
	<p>Click to:</p> <ul style="list-style-type: none"> <li>View device properties</li> </ul>
Details	
	<p>Click to:</p> <ul style="list-style-type: none"> <li>View details about certificates provisioned to the device</li> </ul>
Credentials	
	<p>Click to:</p> <ul style="list-style-type: none"> <li>View policies applicable to the device and the effective policy enforced on the device</li> </ul>
Policies	

## 1.2.1 Device Details Tab

View device properties from this tab. 

### Basic Properties

Element	Description
Name	Shows the model ID for iOS devices, and the model number for Android devices.
Description	A short description of the type of device.
Identifier	A unique identifier assigned to the device by the Mobile Security Manager.
Version	Version label of the device operating system assigned by the manufacturer.
Platform	Indicates the operating system software installed on the device. Either <b>iOS</b> or <b>Android</b> .
Platform Version	The version number of the operating system software installed on the device.

Element	Description
Compliance Level	Indicates if the device is in compliance with the effective policy. One of the following: <ul style="list-style-type: none"> <li>▪ <b>Fully Compliant</b></li> <li>▪ <b>Non-Compliant</b> - Indicates that the device is out of compliance. Click the <b>i</b> icon to view the reason(s) why.</li> </ul>
State	The Mobile Security Manager registration status of this device. One of the following: <ul style="list-style-type: none"> <li>▪ Registered</li> <li>▪ De-registered</li> <li>▪ Identified</li> <li>▪ Certificate issued</li> <li>▪ Wiped</li> </ul>
User	The user ID of the user who enrolled the device with the Mobile Security Manager system.
Enrollment Time	Timestamp that indicates when the device was enrolled with the Mobile Security Manager system. The recorded time is the time at the Mobile Security Manager server, not the time where the device is located.
Last Sync Time	Timestamp that indicates when the device was last synchronized with the Mobile Security Manager system. The recorded time is the time at the Mobile Security Manager server, not the time where the device is located.

### Device Properties

Element	Description
Model	The model name of the device.
Manufacturer	The name of the device manufacturer.
Manufacturer ID	The unique identifier assigned to the device by the manufacturer.
Serial Number	The unique code assigned by the manufacturer to a specific unit of the device.
MAC	The unique MAC (Media Access Control) address of the device.
Product Type	The product classification.
Storage Capacity	The amount of data in Gigabytes (GB) that the device can store.
Available Storage	The amount of remaining storage in Gigabytes (GB) that the device can use to store apps, files, and other data.
Battery Level	The estimated amount of battery life available on the device represented as a decimal percentage where 1 means 100% (full).

### Smartphone Device Properties

Lists additional properties captured from the device. Refer to the device manufacturer's documentation for details.


## 1.2.2 Device Credentials Tab

View details about certificates provisioned to the device. Click a certificate record in the table to view details.

If no certificates are present, this tab is hidden. 

Element	Description
View	Choose from the menu to control how the search results are displayed: <ul style="list-style-type: none"> <li>▪ <b>Columns</b> - Click a column header name to quickly show or hide a single column. Click <b>Manage Columns</b> to open a dialog that lets you show, hide, and reorder multiple columns.</li> <li>▪ <b>Reorder Columns</b> - Click to open a dialog that lets you change the order of the table columns.</li> </ul>
Serial Number	The serial number that uniquely identifies the certificate.
Expires On	Date and time that the certificate will stop being valid. The certificate should be renewed or replaced prior to this date.
Created On	Date and time that the certificate was created.
Issued By	The name of the certificate authority that issued the digital certificate.
Primary	Indicates if this certificate is the primary authentication certificate for this device used for communication with the Mobile Security Manager.

### 1.2.3 Device Policies Tab

View the applicable and effective device management policies from this tab. 

#### Applicable Policies

The list of mobile security policies that are applicable for this device. Click an applicable policy name. The read-only policy details are shown in a pop-up.

#### Effective Policy

The mobile security policy that is enforced on the device. Specifically, the Effective Policy is the merge of elements across all applicable mobile security policies that apply to the device.

**Restrictions** Device restrictions as established by the Effective Policy. A check mark shows functionality that is disabled on the device due to policy restrictions.

Element	Description
General	A check mark disables options in this category. This applies to all platforms (both iOS and Android devices).
Camera	Prevents use of the camera.
iOS	A check mark disables options in this category.
App Installation	Removes the App Store icon and prevents users from installing or updating apps using the Apple App Store.
Assistant	Disables Siri.
Assistance while device locked	Disables Siri when the device is locked. This restriction is ignored if the device does not have a passcode set. (iOS 5.1 and later)
Cloud Backup	Prevents backing up the device to iCloud. (iOS 5.0 and later)
Cloud Document Sync	Prevents document syncing to iCloud. (iOS 5.0 and later)
Cloud Keychain Sync	Prevents iCloud Keychain synchronization. (iOS 7.0 and later)

Element	Description
Diagnostic Submission	Prevent diagnostic data from being reported to Apple. (iOS 6.0 and later)
Explicit Content	Block explicit music or video content purchased from the iTunes Store.
Fingerprint for Unlock	Disables the TouchID feature, which unlocks the device using fingerprints. (iOS 7.0 and later)
Lock Screen Control Center	Prevents the Control Center (accessed by swiping up from the bottom of the screen) from appearing on the lock screen. (iOS 7.0 and later)
Lock Screen Notifications View	Blocks the Notification Center from showing on the lock screen. (iOS 7.0 and later)
Lock Screen Today View	Blocks the Today View from showing on the lock screen. (iOS 7.0 and later)
Ad Tracking	Limits ad tracking.
iTunes	Removes the iTunes icon and prevents access to the iTunes music store.
iTunes Store Password Entry	Requires the user to enter a valid iTunes password before every transaction.
Untrusted TLS Prompt	Automatically rejects untrusted HTTPS certificates without prompting the user. (iOS 5.0 and later)
Shared Stream	Blocks the shared albums or shared Photo Stream feature. (iOS 6.0 and later)
Screenshot	Prevents users from saving a screen capture of the display.
Safari	Removes the Safari icon and prevents the use of the Safari Web browser. This also prevents users from opening Web clips.
Photo Stream	Disables the Photo Stream feature. (iOS 5.0 and later)
Passbook While Locked	Prevents the Passbook notifications from being shown on the lock screen. (iOS 6.0 and later)
Over-the-air PKI Updates	Prevents over-the-air PKI updates. This restriction does not disable CRL and OCSP checks. (iOS 7.0 and later)

**Authentication** Authentication settings applicable to the device as established by the Effective Policy.

Element	Description
Password Required	A check mark indicates that password authentication is required.
Password Minimum Length	The least number of characters that the system will accept when the user creates a password. A value of 0 means there is no minimum length.
Password History	The number of passwords that the system will retain to prevent a user from reusing the same passwords. A value of 0 means the system will not prevent a user from reusing the same password.
Maximum Idle Timeout for Auto Lock	The number of minutes before an inactive device is locked. A value of 0 means the Auto Lock feature is disabled.
Maximum Failed Attempts Before Device Wipe	Indicates the number of failed authentication attempts allowed before the system deletes the device and the user data that it contains. A value of 0 means that this feature is disabled.

Element	Description
Password Expiry	Indicates if the user credential should expire after a set number of days. <ul style="list-style-type: none"> <li>▪ <b>Set Days</b> - The user credential expires after the number of days defined in <b>Password Expiry Duration</b> has elapsed. The user must change the password once it expires. If the user does not change the password, the device is marked as non-compliant.</li> <li>▪ <b>Never</b> - The password does not expire.</li> </ul>
Password Expiry Duration	The number of days that the user credential will remain valid, after which the user must choose a new password.
Password Complexity	<ul style="list-style-type: none"> <li>▪ <b>Simple</b> - The system does not impose any password requirements. The user can use any combination of letters, numbers, and/or special characters.</li> <li>▪ <b>Alphanumeric</b> - The password must contain letters and numbers.</li> <li>▪ <b>Complex</b> - The password must contain at least one letter, one number, and one special character.</li> </ul>

**Apps** Apps provisioned to the device by the Effective Policy.

Element	Description
App Name	The name of the app, Web app, or shared folder app.
Description	A short description of the app set by the individual that added the app to the Mobile Security Manager.
Containerized	<b>Yes</b> indicates that the app has been secured using the Oracle Mobile Security Suite App Containerization Tool. Containerization adds enterprise security services to apps including advanced features such as multi-factor authentication and Integrated Windows Authentication (Kerberos or NTLM).
Virtual App Type	Either a Web App that displays in a web browser or a Shared Folder App that connects to a network file share.
Platform	Either Apple iOS, Google Android, or both.
Install on Homepage	If selected, makes virtual apps appear on the user's main screen or homepage.
Upgrade Alert	If selected, the user is alerted when launching an app if an upgrade is available. If the option is not selected, a badge on the catalog app indicates that an update is available, but the system does not alert the user otherwise.

**Device Configurations** The pre-configured E-mail, VPN, calendar, and/or Wi-Fi settings provisioned to the device by the Effective Policy.

Element	Description
Type	One of the following device setting types: <ul style="list-style-type: none"> <li>▪ <b>VPN</b></li> <li>▪ <b>E-mail</b></li> <li>▪ <b>Wi-Fi</b></li> <li>▪ <b>Calendar</b></li> </ul> For more information, see <a href="#">Chapter 6, "Device Configurations Help."</a>
Configuration Name	The name of the device configuration applicable for this device setting type on this device.



Element	Description
Configuration Description	A short description of the device configuration applicable for this device setting type on this device.

### Related Topics

"Managing Devices and Workspaces" in *Administering Oracle Mobile Security Suite*

## 1.3 Workspace Management

Click a Workspace icon to open Workspace management controls and view additional details. This section provides details about Workspace management controls.

Use this view to:

- Manage a specific Workspace on a specific device
- View detailed information about a specific Workspace

This view is arranged in the following sections:






- [Action Bar](#)
- [Workspace Information Tabs](#)
  - [Workspace Details Tab](#)
  - [Workspace Apps Tab](#)
  - [Workspace Activity Tab](#)
  - [Workspace Credentials Tab](#)
  - [Workspace Policies Tab](#)

### Action Bar


Use the buttons to secure data in the Workspace.

Element	Description
Lock (Unlock)	Locks or unlocks the Workspace. An administrator can unlock the account using the Mobile Security Manager console. (The end-user cannot unlock a locked Workspace account using the Self-Service console.) To lock the Workspace remotely when it is unlocked, click Lock. To unlock the Workspace remotely when it is locked, click Unlock. Once the Workspace is unlocked, the user has to log in.
Wipe	Resets the Workspace to its original system state by erasing all of the stored data. This action does not remove the Workspace app. The user can log in to the Workspace again by providing their credentials, but all previously stored data will be lost.
Reset Passcode	Resets the passcode to a new randomly generated passcode that is displayed on the screen. The user must enter the new passcode the next time they open the Workspace.  Note: The Reset Passcode button is only available if the Workspace is enrolled using certificate-based (PKINIT) authentication. This button will be available if a certificate is present, even though a PIN may not be required.

## Workspace Information Tabs


Element	Description
	<p>Click to:</p> <ul style="list-style-type: none"> <li>View read-only device and Workspace properties.</li> </ul>
Details	
	<p>Click to:</p> <ul style="list-style-type: none"> <li>Search a list of apps installed within the Workspace.</li> <li>View a list of apps installed within the Workspace.</li> </ul>
Apps	
	<p>Click to:</p> <ul style="list-style-type: none"> <li>Search the container log for events that meet the search criteria.</li> <li>View event details about activities performed on the Secure Workspace app.</li> </ul>
Activity	
	<p>Click to:</p> <ul style="list-style-type: none"> <li>View details about certificates provisioned to the Workspace. (The Credentials tab is not available if the container is registered with kinit authentication unless other certificates are present, in which case this tab is present.)</li> </ul>
Credentials	
	<p>Click to:</p> <ul style="list-style-type: none"> <li>View policies applicable to the Workspace and the effective policy enforced on the Workspace.</li> <li>View policies having to do with authentication, security, and Workspace app settings.</li> </ul>
Policies	

### 1.3.1 Workspace Details Tab

View device and Workspace properties from this tab. 

#### Basic Properties

Element	Description
Name	The package name of the Secure Workspace app.
Description	A short description of the type of device.
Identifier	A unique identifier assigned to the Workspace by the Mobile Security Manager.
Version	The version of the Workspace app.
Platform	Indicates the operating system software installed on the device. Either <b>iOS</b> or <b>Android</b> .
Platform Version	The version number of the operating system software installed on the device.

Element	Description
Compliance Level	One of the following: <ul style="list-style-type: none"> <li>■ <b>Fully Compliant</b></li> <li>■ <b>Non-Compliant</b> - Indicates that the device is out of compliance. Click the  icon to view the reason(s) why.</li> </ul>
State	The Mobile Security Manager registration status of this Workspace. One of the following: <ul style="list-style-type: none"> <li>■ Registered</li> <li>■ De-registered</li> <li>■ Locked</li> </ul>
User	The user ID of the user who enrolled the device with the Mobile Security Manager system.
Enrollment Time	Timestamp that indicates when the Workspace was enrolled with the Mobile Security Manager system. The recorded time is the time at the Mobile Security Manager server, not the time where the device is located.
Last Sync Time	Timestamp that indicates when the Workspace was last synchronized with the Mobile Security Manager system. The recorded time is the time at the Mobile Security Manager server, not the time where the device is located.

### Workspace Properties

Element	Description
Manufacturer Device ID	The unique identifier assigned to a device by the manufacturer.
Gateway URL	The configuration URL for the Workspace app hosted by the Mobile Security Access Server.
Model	The model name of the device that the Workspace is installed on, for example: iPhone 3S, SM-N900, or Nexus 5.
Workspace Name	The package name of the Secure Workspace app.
Workspace Version	The version of the Workspace app.


### 1.3.2 Workspace Apps Tab

View apps deployed in the Workspace from this tab. 

Click the app name to view the app details in a pop-up.

Element	Description
Search	Search for an app by name or leave the search box empty to display all apps installed in the Workspace.
App Icon Grid (Search Results section)	Displays applications installed in the Workspace that meet the search criteria.

### 1.3.3 Workspace Activity Tab

Search a log of Workspace activity from this tab. 

## Search Section and Page Controls

Element	Description
Search	Search for an event by typing an event key word. Search looks across fields for matching strings.
View	Choose from the menu to control how the search results are displayed: <ul style="list-style-type: none"> <li>▪ <b>Columns</b> - Click a column header name to quickly show or hide a single column. Click <b>Manage Columns</b> to open a dialog that lets you show, hide, and reorder multiple columns.</li> <li>▪ <b>Reorder Columns</b> - Click to open a dialog that lets you change the order of the table columns.</li> </ul>
Sort	Choose from the following: <ul style="list-style-type: none"> <li>▪ <b>Event</b> - Sort search results alphabetically by the name of the logged event.</li> <li>▪ <b>Event Source</b> - Sort search results alphabetically by the source of the event, for example <i>Device</i> or <i>Mobile Security Manager</i>.</li> <li>▪ <b>Initiated By</b> - Sort search results alphabetically by the user or system that initiated the operation, for example the <i>SecureWorkspace</i>, or a specific user, such as the end user or an Admin user.</li> <li>▪ <b>Date/Time</b> - Sort search results by the timestamp recorded on the device. This is the default option.</li> </ul>

## Events (Search Results) Section

Element	Description
Event	The name of the logged event.
Event Source	Indicates if the event was initiated by the <i>Device</i> , or if it was initiated by a command sent from the <i>Mobile Security Manager</i> .
Initiated By	Indicates the user or system that initiated the operation, for example the <i>SecureWorkspace</i> , or a specific user, such as the end user or an Admin user.
Location	The latitude and longitude coordinates where the event took place. If latitude and longitude are not available then this field will be empty. The coordinates will not be available if the user chooses to not allow location services for the Secure Workspace app.
Date/Time	The timestamp when the even occurred.

### 1.3.4 Workspace Credentials Tab

View details about certificates provisioned to the Workspace.

If no certificates are present, this tab is hidden. 

This tab is only shown when a Workspace is configured to authenticate using a certificate (PKINIT-based authentication).

Element	Description
View	Choose from the menu to control how the search results are displayed: <ul style="list-style-type: none"> <li>▪ <b>Columns</b> - Click a column header name to quickly show or hide a single column. Click <b>Manage Columns</b> to open a dialog that lets you show, hide, and reorder multiple columns.</li> <li>▪ <b>Reorder Columns</b> - Click to open a dialog that lets you change the order of the table columns.</li> </ul>
Serial Number	The serial number that uniquely identifies the certificate.
Expires On	Date and time that the certificate will stop being valid. The certificate should be renewed or replaced prior to this date.
Created On	Date and time that the certificate was created.
Issued By	The name of the certificate authority that issued the digital certificate.
Primary	Indicates if this certificate is the primary authentication certificate for this Workspace used for communication with the Mobile Security Manager.

### 1.3.5 Workspace Policies Tab

View the Effective Policy for the Workspace from this tab. 

#### Applicable Policies

The list of mobile security policies that are applicable for this Workspace. Click an applicable policy name. The read-only policy details are shown in a pop-up.

#### Effective Policy

The mobile security policy that is enforced on the Workspace. Specifically, the Effective Policy is the merge of elements across all applicable mobile security policies. Device policy attributes (that is, MDM policy attributes) do not apply to Workspace policies.

**Authentication** The authentication settings applicable to the Workspace as established by the Effective Policy.

Element	Description
Authentication Only	If selected, hides the Workspace home from the user if the Workspace container is being used purely as an authentication client and not for any app UI.
Authentication Frequency	Specifies how often the user sees the login screen: <ul style="list-style-type: none"> <li>▪ <b>Always</b> - The user must authenticate every time they try to access the Secure Workspace on their device.</li> <li>▪ <b>Idle Timeout</b> - Enforces authentication each time the Idle Timeout Period has been reached. The Timeout Period is the number of minutes a container is allowed to remain inactive before prompting with the login screen with a maximum of two hours. This period continues to apply while the user is outside the container.</li> <li>▪ <b>Session</b> - Allows users to exit the Mobile Security Container to use other apps and does not require them to log in upon return until the session ends. A session expires when the Oracle S-token expires (configurable with a default of 10 hours) or the device closes the app due to low memory.</li> </ul>
Idle Timeout Period	If <b>Authentication Frequency</b> is set to <b>Idle Timeout</b> , the length of time without user activity before the system requires the user to authenticate.

Element	Description
Account Lockout Threshold	The number of failed authentication attempts allowed before the <b>Account Lockout Action</b> is triggered.
Account Lockout Action	The action to take when the <b>Account Lockout Threshold</b> has been exceeded: <ul style="list-style-type: none"> <li>■ <b>Do Nothing</b> - Do not take any action.</li> <li>■ <b>Lock</b> - Disables the Secure Workspace from operating and stops user access to virtual applications or information. Only an administrator can unlock the account using the Mobile Security Manager console. Once the Workspace is unlocked, the user still has to log in.</li> <li>■ <b>Wipe</b> - Delete the Workspace and the user data that it contains. This is a severe action that cannot be undone. Wipe assures nothing remains on the device for anyone to access.</li> </ul>
PIN History	The number of previously used user credentials (PINs) that the system will retain so as to prevent a user from reusing the same PIN. For example, if PIN History is set to 3 and a user changes an initial PIN of demo1 to demo2 and wants to change it back, they cannot do so until they have changed the PIN to a different value a total of 3 times.  PIN options only apply if your environment uses certificate-based authentication.
PIN Minimum Length	The minimum number of characters that the user must enter when creating a user credential (PIN). Set this value anywhere between 4 to 14 characters.
Shared Workspace Mode	Configures how the Secure Workspace functions on a device that is shared by multiple users. Choose from the following: <ul style="list-style-type: none"> <li>■ <b>Single User</b> - The Workspace will only be used by a single user on a given device.</li> <li>■ <b>Multi-User</b> - The Workspace can be shared by multiple users on a given device. The Workspace data will be wiped every time a user logs out of the Workspace.</li> </ul>
PIN Expiry	Choose <b>Set Days</b> to force the user to choose a new user credential on a regular basis.
PIN Expiry Duration	The number of days that the user credential will remain valid, after which the user must choose a new PIN. If the user does not change the PIN, the device is marked as non-compliant.
PIN Complexity	Indicates if minimum requirements are enforced when users create user credential (PIN) values.
PIN Complexity Min Checks	A number between 1 and 4 that indicates how many of the following <b>Pin must contain...</b> requirements must be satisfied.  If the number of options selected below is greater than the <b>PIN Complexity Min Checks</b> value, users may set their PIN with any combination of options that meets the requirements. For example, if <b>PIN Complexity Min Checks</b> is 2 and all four complexity types are selected, a PIN with any combination of two or more of the requirements is acceptable.
PIN must contain lowercase	A check mark indicates that the PIN must include at least one lowercase letter.
PIN must contain uppercase	A check mark indicates that the PIN must include at least one uppercase letter.
PIN must contain special character	A check mark indicates that the PIN must include at least one non-alphanumeric character.

Element	Description
PIN must contain numeric	A check mark indicates that the PIN must include at least one numeric character.

**Workspace/ Apps** The allowed Workspace settings as established by the Effective Policy. Except for **File Sharing** and **Copy/Paste**, allowed items have a check mark.

Element	Description
Location Settings	Allows device location coordinates to be collected from the device if the user has allowed location services during installation. If disabled, the user is not asked to accept location services during installation and user location is not tracked.
Offline Access	Allows the user to access the information already in the container when the user is offline. If disabled, users cannot access the Secure Workspace unless they are online and logged in.
E-mail	Allows the user to send e-mail messages from the native OS e-mail client.
Instant Messaging	Allows the user to send instant messages from the Secure Workspace.
Video Chat	Allows the user to access video chat functionality such as FaceTime.
Social Share	Allows the user to access social sharing through integrated services such as Facebook or Twitter.
Print	Allows Workspace apps to print to a printer.
Redirects to Workspace	Allows apps outside the Secure Workspace to redirect a URL into the Workspace.
Save to Media Gallery	Allows photos, images, and videos to be saved to the local media store on the device.
Save to Local Contacts	Allows user contacts to be saved to the contacts manager on the device.
Redirects From Workspace	Allows the Secure Workspace to redirect to an app outside the Workspace with a custom URL scheme.
(Restrict) File Sharing	If checked, restricts the ability of the user to share files outside the Secure Workspace.
(Restrict) Copy/Paste	If checked, copy and paste is only allowed inside the Secure Container, containerized apps, or between containerized apps, but not to apps outside the Secure Workspace.

**Application Settings** The Workspace Apps settings as established by the Effective Policy.

Element	Description
Browser	Indicates browser settings as follows: <ul style="list-style-type: none"> <li>▪ <b>Address Bar Enabled</b> - A check mark indicates that the address bar in the Secure Browser (part of the Secure Workspace) is visible. If the box is not checked, the address bar is disabled and the Secure Browser is hidden.</li> <li>▪ <b>Download Bar Enabled</b> - A check mark indicates that downloading is allowed in the Secure Browser. If the box is not checked, downloading is disabled.</li> </ul>

Element	Description
Doc Editing	Indicates doc editing settings as follows: <ul style="list-style-type: none"> <li>■ <b>Allow</b> - A check mark indicates that the user can access the Workspace doc editor app (if installed).</li> </ul>
File Manager	Indicates file manager settings as follows: <ul style="list-style-type: none"> <li>■ <b>Allow</b> - A check mark indicates that the user has full access to the Workspace file manager utility.</li> <li>■ <b>Download Allowed</b> -A check mark indicates that the user can download files and save them locally.</li> </ul>
File Manager Server Based URL	If the File Manager function is enabled, this is the URL of the File Manager service that provides access to network file shares.
PIM	Oracle Secure Mobile Mail Manager (the personal information manager app) covers e-mail, calendar, contacts, and notes. Indicates settings as follows: <ul style="list-style-type: none"> <li>■ <b>Allow</b> - A check mark indicates that the user can access the Workspace personal information manager app.</li> </ul>
E-mail Server URL	The URL of the e-mail server that the personal information manager app will connect to.
Basic ActiveSync Authentication	Indicates if Basic authentication is enabled.
Configuration Type	One of the following: <ul style="list-style-type: none"> <li>■ <b>AUTO</b> - The user only needs to enter their e-mail ID. Server details and the password value are populated automatically.</li> <li>■ <b>BASIC</b> - The user needs to enter their e-mail ID and password. Server details are populated automatically.</li> <li>■ <b>MANUAL</b> - The user needs to enter all details: their e-mail ID, server details, and the password value.</li> </ul>

**Time Access / Geo Access** These Effective Policy settings restrict access to the Workspace by time and/or location. When these policies are violated the Workspace automatically locks, and when they are back in compliance the Workspace automatically unlocks.

Element	Description
Time-fence	Shows up to five access windows between 12:00 midnight and 11:59 pm that can be set to restrict user access to the Workspace. The time in the <b>From</b> column specifies the time that restricted access should start, and the time in the <b>To</b> column specifies the time that restricted access should end.
Geo-fence	Shows the cities, states, or countries where access to the Worksapce is allowed. If no Geo-Fence is defined the policy defaults to no geo-location restrictions.

**Apps** Apps provisioned to the Workspace by the Effective Policy. Only the apps listed can be installed in the Workspace. These apps show up in the user’s App Catalog inside their Workspace, if enabled.



Element	Description
App Name	The name of any apps, Web apps, or shared folder apps that are assigned to this Workspace policy.
Description	A brief note regarding the app created by a Mobile Security Manager administrator.
Containerized	Indicates if the iOS or Android app is containerized. Containerization adds enterprise security services to apps including advanced features such as multi-factor authentication and Integrated Windows Authentication (Kerberos or NTLM).
Virtual App Type	Indicates if the app is a <b>Web App</b> that runs on a remote server and displays in a Web browser, or a <b>Shared Folder App</b> that users can mount on the Workspace.
Platform	Either <b>iOS</b> or <b>Android</b> or both. This field applies to Apps, but not Virtual Apps.
Install on Homepage	If selected, makes virtual apps appear on the Secure Workspace's home screen.
Upgrade Alert	If selected, the user is alerted when launching an app if an upgrade is available. If the option is not selected, a badge on the catalog app indicates that an update is available, but the system does not alert the user otherwise.

### Related Topics

"Managing Devices and Workspaces" in *Administering Oracle Mobile Security Suite*



# 2

## Mobile App Catalog Page Help

System Administrators use the Mobile App Catalog to manage the lifecycle of enterprise apps for users, including installation and update. Apps can include native iOS and Android apps that are containerized or non-containerized, and "virtual apps"—either a Web app that displays in a web browser, or a Shared Folder app that connects to a network file share. Apps in the Catalog are assigned to policies so that they can be made available to users based on their role assignments.

The following topics are covered:

- [Mobile App Catalog Page](#)
- [Add Application Dialog](#)

### 2.1 Mobile App Catalog Page

Use the Mobile App Catalog page to:

- Search the catalog for apps.
- View and edit app details.
- Add and remove apps in the catalog.
- Assign a graphic icon to an app for use in the Mobile Security Manager console.

The Mobile App Catalog page is arranged in the following sections:

- [Command Bar and Search](#)
- [Table of Apps \(Search Results Section\)](#)

#### Command Bar and Search

Search for apps by name, then use the **Sort** menu to reorder the search results. The buttons on the command bar are described in the following table.

Element	Description
Search	Type a search term and press the search button. Both the app Name and the description fields are searched. You cannot use wildcards but partial matches will return results, for example: <i>cal</i> will return results for "Calculator."
Add	Click to add an app to the catalog. The Add Application dialog box opens. Only Systems Administrators can add apps to the catalog.
Refresh	Click to refresh the search results table.

Element	Description
Sort	Choose from the following: <ul style="list-style-type: none"> <li>▪ <b>Last Updated</b> - Sort search results such that the most recently updated apps are returned first.</li> <li>▪ <b>Display Name</b> - Sort search results alphabetically by app name.</li> </ul>

### Table of Apps (Search Results Section)

Apps that meet the search criteria display in the area below the command bar. Click the app record to toggle the **App Details** panel open and closed.

Element	Description
App Icon	The graphic icon that helps users identify the app.
Name	The name of the app.
Description	A brief note regarding the app created by a Mobile Security Manager administrator.
Type	One of the following: <ul style="list-style-type: none"> <li>▪ <b>App</b> - A native iOS or Android app. The app can be containerized or uncontainerized.</li> <li>▪ <b>Virtual App</b> - Either a Web app that runs on a remote server and displays in a Web browser, or a Shared Folder app that users can mount on the Workspace.</li> </ul>
Containerized	Indicates if a native iOS or Android app has been secured using the Oracle Mobile Security Suite Application Containerization Tool.
Virtual App Type	One of the following: <ul style="list-style-type: none"> <li>▪ <b>Web App</b> - An app that runs on a remote server and displays in a Web browser.</li> <li>▪ <b>Shared Folder App</b> - A desktop folder that users can mount on the Workspace.</li> </ul>
Platform	Either <b>iOS</b> or <b>Android</b> , or both <b>iOS</b> and <b>Android</b> .
Installed On	Indicates how many devices the app is installed on.
x	Click to delete the app from the catalog. Only Systems Administrators can delete the app from the catalog.

### Related Topics

"Managing Apps" in *Administering Oracle Mobile Security Suite*

## 2.2 Add Application Dialog

Complete the form to add an app to the Mobile App Catalog. If the app supports multiple platforms (iOS *and* Android), add the app once and configure the platform specific details in the Distributions section.

The Create App dialog is arranged in the following sections:

- [App Details](#)
- [Distributions](#)

## App Details

Complete this section of the form to configure general information about the app. Depending on your selections, only some of the following elements will be available.

Element	Description
App Type	Choose <b>App</b> if the app is a native iOS or Android app. Choose <b>Virtual App</b> if the app is a Web app that runs on a remote server and displays in a Web browser or it is a network file share.
Containerized	Choose <b>Yes</b> if a native iOS or Android app has been secured using the Oracle Mobile Security Suite Application Containerization Tool.
Secure Workspace App	Only select if the app is the Secure Workspace app. Typically, there should be only one such app. The Secure Workspace app is installed on users' devices as part of Workspace registration and provides the Secure Workspace functionality. For all other apps, do not select this option.
Name	Type the name of the application.
Description	A short description to help you or another administrator identify this app in the future.
Platform	Choose from the following: <ul style="list-style-type: none"> <li>■ <b>iOS</b> - The app runs on mobile devices that run the iOS mobile operating system from Apple.</li> <li>■ <b>Android</b> - The app runs on mobile devices that run the Android operating system from Google.</li> <li>■ <b>All</b> - The app runs on both iOS and Android.</li> </ul>
Vendor	Type the name of the company or developer that created the app.
Icon	Upload an app icon that will display alongside the app name in the Mobile Security Manager console. Click <b>Choose File</b> and navigate to the icon file.  The icon file should be in the PNG format. The recommended icon size in pixels is 114 x 114.
Implementation Type	Choose <b>Web App</b> if the app runs in a Web browser, or choose <b>Shared Folder App</b> to configure a desktop folder that users can mount on the Workspace.
Target URL	If configuring a Web app, type the complete URL starting with the protocol (for example, <code>http://</code> or <code>https://</code> ).
Target Folder	If configuring a Shared Folder app, type the path to the folder that users will mount on the Workspace. For example: <code>smb://sharedfolder</code>  You can also enter the <code>*Homedirectory*</code> LDAP attribute without the <code>smb</code> or <code>http</code> protocol identifier and the system will internally convert it to the correct URL.

## Distributions

Choose from the **Platform** menu to populate the Distributions section. If the app supports both iOS and Android, use the tabs to configure each separately.

Element	Description
Distribution Location	<p>To upload a Containerized app or the Secure Workspace app, click <b>Choose File</b> to upload the app binary.</p> <p>For all other apps, choose from the following to specify the distribution location:</p> <ul style="list-style-type: none"> <li>■ Specify the public app store for the platform (<b>iTunes App Store</b> or <b>Google Play Store</b>)</li> <li>■ Click <b>Choose File</b> to upload the binary directly</li> </ul> <p>If <b>Binary</b> is selected for the distribution location, the <b>Package Name</b>, <b>Version</b>, and <b>Min OS Version</b> fields are automatically populated after you extract the uploaded binary file.</p>
AppID	For an iOS app, add the App ID.
App URL	Enter the URL where users can download the app if you are not directly uploading the binary and if you are not distributing the app using the iTunes App Store or Google Play Store.
Package Name	The app's complete package name, for example: <code>com.oraclecorp.internal.WhitePages</code>
Version	The version name or number assigned to the app by the app creator.
Containerization Version	If the app is containerized, the version of the containerization tool that was used to process the app.
Min OS Version	The minimum version of the mobile operating system software needed to run the app.

### Related Topics

"About the Mobile App Catalog and Adding Apps to the Device" in *Administering Oracle Mobile Security Suite*

# 3

## Mobile Security Policies Page Help

Organizations use mobile security policies to empower users by provisioning apps to mobile devices and enabling mobile access to corporate file shares. Policies also protect sensitive data by restricting users' actions and access based on role assignments. System Administrators assign policies to roles, not directly to individual users. For each individual user, Mobile Security Manager merges the policies assigned to the user's roles (the *applicable policies*) and arrives at the *Effective Policy*, which is the merge of all policy elements across the applicable policies. The Effective Policy is the policy that is enforced on the device or Workspace. To view a user's Effective Policy, use the Mobile Devices page to search for and view details about the devices or Workspaces registered to the user. For details, see "[Devices Page Help](#)."

The following topics are covered:

- [Policy Search](#)
- [Policy Management Page \(Create Policy Page\)](#)

### 3.1 Policy Search

Use the Policy Search page to:

- Search for a policy.
- View a policy.
- Open the Policy Management View that you use to create or edit a policy.

The Policy Search View page is arranged in the following sections:

- [Command Bar and Search](#)
- [Table of Policies \(Search Results Section\)](#)

#### **Command Bar and Search**

Use the Search controls to create a query based on filter conditions. The controls are described in the following table.

Element	Description
Search	Type a search term and press the search button. You can search by role name, policy name, or policy description. Role name search is case sensitive. If you are searching by role name, enter the whole name using the exact sequence of upper and lowercase characters.  You cannot use wildcards but partial matches will return results, for example: <i>cal</i> will return results for "Calculator."
Add	Click to open the Create Policy dialog from which you can create a new policy. (Systems Administrators only.)

### Table of Policies (Search Results Section)

This section of the Mobile Security Policies page lists policies that meet the search criteria.

Element	Description
Name	The name of the mobile security policy. Click the policy record to expand it and display additional details; click again to hide the policy details. Use the expanded policy management record to edit the policy.
Description	A short description to help you or another administrator identify this policy in the future.
Roles	Lists the mobile roles to which the mobile security policy has been added.
Actions	Systems Administrators can choose from the following: <ul style="list-style-type: none"> <li>■ <b>Duplicate</b> - Opens the policy in Policy Management View so that you can create a copy of the policy with a new name.</li> <li>■ <b>Remove</b> - Deletes the policy after asking you to confirm the action.</li> </ul>

### Related Topics

"How to Perform Common Mobile Security Policy Tasks" in *Administering Oracle Mobile Security Suite*

## 3.2 Policy Management Page (Create Policy Page)

Use the Policy Management page and Create Policy page to:

- View policy details.
- Create, duplicate, or edit a policy.
- Delete a policy.
- Add a role to a policy; remove a role from a policy.

Only Systems Administrators can create, duplicate, edit, or delete a policy, associate a role with a policy, or remove a role from a policy.

---

**Note:** When policies are in conflict the system typically enforces the most restrictive policy. For details, see "Understanding How the System Enforces Policy Conflicts" in *Administering Oracle Mobile Security Suite*.

---

The Policy Management (Create Policy) page is arranged in the following sections:

- [General Information](#)



- [Roles](#)
- [Enrollment](#)
- [Device](#)
- [Workspace](#)
- [Apps and Configuration](#)

**Tip:** When editing a policy, click **Apply** to save your changes, or click **Revert** to reset the page to the last saved version.

In the Create Policy wizard, click **Next** to proceed to the next configuration page; click **Finish** to save the policy and close the wizard; click **Cancel** to close the wizard without saving.

### General Information

Enter or view the policy name and description.

Element	Description
Policy Name	The name of the mobile security policy.
Description	A short description to help you or another administrator identify this policy in the future.

### Roles

Use the Roles tab to:

- View the roles currently assigned to the policy.
- Add one or more roles to the policy.
- Remove one or more roles from the policy.
- Exclude a child role from the policy. Do this to exempt a role from a policy that applies to a parent role.

Only Systems Administrators can use the Roles tab to add or remove roles, or exclude child roles.

Element	Description
View	Click <b>View &gt; Detach</b> to open the table in a larger window.
Add	Click to add a new <b>Role Name</b> row to the table.
Remove	Click a <b>Role Name</b> row to select it (the row should be highlighted), then click <b>Remove</b> to delete the row.
Role Name	When adding a role to a policy, type the role name or click the search feature.
Description	A short description to help you or another administrator identify this role in the future.

### Excluded Child Roles

Element	Description
View	Click <b>View &gt; Detach</b> to open the table in a larger window.

Element	Description
Add	Click to add a new Excluded Child Role Name row to the table.
Remove	Click an Excluded Child Role Name row to select it (the row should be highlighted), then click <b>Remove</b> to delete the row.
Role Name	Type the name of the child role(s) to exclude. For example, if you need to exempt VPs from a policy that covers the <i>Employees</i> (parent) role, add the <i>Vice Presidents</i> (child) role as an excluded role. Note that when entering a role name, auto-complete returns all matching role names, not just the names of valid child roles.

### Enrollment

Use the Enrollment tab to view the enrollment and compliance settings assigned to the policy. Only Systems Administrators can edit enrollment/compliance settings. The Enrollment tab is arranged in the following sections:

- [Device Criteria](#)
- [Enrollment Data](#)
- [Additional Compliance Rules](#)

Element	Description
Selected Roles	The roles that this policy will affect. Click the <b>Roles</b> tab to add and remove roles.
Specify enrollment/compliance details for this policy	To specify enrollment/compliance details for this policy, select the check box. Keep in mind that when multiple policies are assigned to a role, the policies are merged. If enrollment/compliance details are specified for this policy, the values will be merged with the enrollment/compliance values from other policies.  To create a policy without specifying enrollment/compliance values, <i>clear</i> the option box.

### Device Criteria

Element	Description
Platforms	Indicates the device platforms that are eligible for enrollment under this policy. Clear an option to exclude it.
Minimum Version	Indicates the oldest version of the platform software that is eligible for enrollment under this policy. For example, for iOS, setting a value of 8.0 will block iOS 7.0.4 from enrolling.
Maximum Number of Devices Per User	Indicates the most devices that a user can enroll under this policy.
Inactivity Duration	Indicates the number of days since the device/Workspace has been in contact with the Mobile Security Manager before the device is considered to be inactive. <b>Inactivity Duration</b> can be used in combination with <b>Inactivity Duration Action</b> (in the <a href="#">Additional Compliance Rules</a> section at the bottom of the page) to trigger a security action.

**Enrollment Data**

<b>Element</b>	<b>Description</b>
Invite Template	Indicates the e-mail template that is used to invite users to enroll in the mobile security management system. Notification templates are managed on the Mobile Security Manager Settings page.
Identity Certificate	Indicates the certificate template that will be used when generating certificates in the Workspace app to identify and authenticate users. Certificate templates are managed on the Mobile Security Manager Settings page.
Additional Certificates	Indicates the certificate template that will be used when generating certificates in the Workspace app for additional purposes such as signing and encryption.
Allow Client Specific Builds	Select to choose the Workspace app builds that are allowed to register with the Mobile Security Manager. This is to ensure that Workspace app builds for other Oracle customers or from public app stores are not allowed to be registered with this Mobile Security Manager deployment.
Allow Client Builds	The set of Workspace app builds that are allowed to register with the Mobile Security Manager.

**Additional Compliance Rules** On managed devices (MDM+MAM deployments), compliance rule checks occur (1) during the enrollment process, (2) whenever the device **Sync** command is issued from the MSM server, and (3) every night at a set time when the `ComplianceCheckTrigger` scheduled job runs and flags non-compliant devices. On unmanaged devices (MAM-only deployments), compliance rule checks happen (1) during the enrollment process, (2) whenever a policy is updated, and (3) every night when the `ComplianceCheckTrigger` scheduled job runs on the device and evaluates all enrolled devices for policy compliance.

<b>Element</b>	<b>Description</b>
Device Criteria Violation	<p>Indicates the security action to take if the policy parameters specified in the Device Criteria section are violated. Note that <b>Inactivity Duration</b> is a separate security action.</p> <p>This compliance rule applies to both managed and unmanaged devices. Note that the Wipe action is different for managed and unmanaged devices.</p> <ul style="list-style-type: none"> <li>■ <b>Lock</b> - Disables the Secure Workspace from operating and stops user access to virtual applications or information.</li> <li>■ <b>Wipe</b> - On managed devices: De-registers the managed device from MSM, removes profiles, and wipes the Workspace and the user data that it contains. Following this action the device is no longer controlled by the server. <ul style="list-style-type: none"> <li>On managed devices: Resets the Workspace to its original system state by erasing all of the stored data.</li> </ul> </li> <li>■ <b>Do Nothing</b> - Do not take any action.</li> </ul>

Element	Description
Device Jailbroken	<p data-bbox="565 226 1375 281">Indicates the security action to take if the device operating system is found to be jailbroken.</p> <p data-bbox="565 296 1375 350">This compliance rule applies to both managed and unmanaged devices. Note that the Wipe action is different for managed and unmanaged devices.</p> <ul data-bbox="565 365 1375 680" style="list-style-type: none"> <li data-bbox="565 365 1375 420">■ <b>Lock</b> - Disables the Secure Workspace from operating and stops user access to virtual applications or information.</li> <li data-bbox="565 434 1375 548">■ <b>Wipe</b> - On managed devices: De-registers the managed device from MSM, removes profiles, and wipes the Workspace and the user data that it contains. Following this action the device is no longer controlled by the server.  On managed devices: Resets the Workspace to its original system state by erasing all of the stored data.</li> <li data-bbox="565 646 1375 680">■ <b>Do Nothing</b> - Do not take any action.</li> </ul>
Blacklisted Apps Installed	<p data-bbox="565 695 1375 749">Indicates the security action to take if an app marked as Blacklisted is installed. This compliance rule applies to managed devices, only.</p> <ul data-bbox="565 764 1375 980" style="list-style-type: none"> <li data-bbox="565 764 1375 819">■ <b>Lock</b> - Disables the Secure Workspace from operating and stops user access to virtual applications or information.</li> <li data-bbox="565 833 1375 926">■ <b>Wipe</b> - De-registers the managed device from MDM, removes profiles, and wipes the Workspace and the user data that it contains. Following this action the device is no longer controlled by the server.</li> <li data-bbox="565 949 1375 980">■ <b>Do Nothing</b> - Do not take any action.</li> </ul>
Inactivity Duration Action	<p data-bbox="565 995 1375 1075">Indicates the security action to take if the <b>Inactivity Duration</b> value is exceeded. This compliance rule applies to both managed and unmanaged devices.</p> <p data-bbox="565 1089 1375 1144">This compliance rule applies to both managed and unmanaged devices. Note that the Wipe action is different for managed and unmanaged devices.</p> <ul data-bbox="565 1159 1375 1470" style="list-style-type: none"> <li data-bbox="565 1159 1375 1218">■ <b>Lock</b> - Disables the Secure Workspace from operating and stops user access to virtual applications or information.</li> <li data-bbox="565 1232 1375 1346">■ <b>Wipe</b> - On managed devices: De-registers the managed device from MSM, removes profiles, and wipes the Workspace and the user data that it contains. Following this action the device is no longer controlled by the server.  On managed devices: Resets the Workspace to its original system state by erasing all of the stored data.</li> <li data-bbox="565 1444 1375 1470">■ <b>Do Nothing</b> - Do not take any action.</li> </ul>

Element	Description
Passcode Compliance Action	<p>Indicates the security action to take if the device passcode value is out of compliance with the policy. If the iOS <b>Clear Passcode</b> command is issued, the user must enter a compliant passcode within the time allotted by the Passcode Expiration setting (defined under Server Settings). The default value is 60 minutes. If a passcode is not entered in time, the device is marked as non-compliant and the system carries out the Passcode Compliance Action.</p> <p>This compliance rule applies to both managed and unmanaged devices. Note that the Wipe action is different for managed and unmanaged devices.</p> <ul style="list-style-type: none"> <li>▪ <b>Lock</b> - Disables the Secure Workspace from operating and stops user access to virtual applications or information.</li> <li>▪ <b>Wipe</b> - On managed devices: De-registers the managed device from MSM, removes profiles, and wipes the Workspace and the user data that it contains. Following this action the device is no longer controlled by the server. <ul style="list-style-type: none"> <li>On managed devices: Resets the Workspace to its original system state by erasing all of the stored data.</li> </ul> </li> <li>▪ <b>Do Nothing</b> - Do not take any action.</li> </ul>

### Device

Use the Device tab to view device-specific settings assigned to the policy. Only Systems Administrators can define an MDM policy and edit device-specific settings.

---

**Note:** Use the **Device** tab to define an MDM policy. Only specify device details if the policy is intended for managed devices. If an unmanaged device tries to run an MDM policy, it will report an error on the device.

---

The Device tab is arranged in the following sections:

- [Restrictions](#)
- [Authentication](#)
- [Android Device Encryption](#)

Element	Description
Selected Roles	The roles that this policy will affect. Click the <b>Roles</b> tab to add and remove roles.
Specify device details for this policy	<p>To specify device settings for this policy, <i>select</i> the option box. Keep in mind that when multiple policies are assigned to a role, the policies are merged. If device settings are specified for this policy, the values will be merged with the device settings from other policies. For MAM-only devices, do not specify device policy settings.</p> <p>To create a policy without specifying device settings, <i>clear</i> the option box.</p>

**Restrictions** Device restrictions applicable to the device.

Element	Description
General	Select an option in this category to disable it; clear a check box to enable it. This applies to all platforms (both iOS and Android devices).
Camera	Prevents use of the camera.
iOS	Select an iOS-specific option in this category to disable it; clear a check box in this category to enable it. Refer to the iOS documentation for details about specific functionality.
App Installation	Removes the App Store icon and prevents users from installing or updating apps using the Apple App Store.
Assistant	Disables Siri.
Assistance while device locked	Disables Siri when the device is locked. This restriction is ignored if the device does not have a passcode set. (iOS 5.1 and later)
Cloud Backup	Prevents backing up the device to iCloud. (iOS 5.0 and later)
Cloud Document Sync	Prevents document syncing to iCloud. (iOS 5.0 and later)
Cloud Keychain Sync	Prevents iCloud Keychain synchronization. (iOS 7.0 and later)
Diagnostic Submission	Prevent diagnostic data from being reported to Apple. (iOS 6.0 and later)
Explicit Content	Block explicit music or video content purchased from the iTunes Store.
Fingerprint for Unlock	Disables the TouchID feature, which unlocks the device using fingerprints. (iOS 7.0 and later)
Lock Screen Control Center	Prevents the Control Center (accessed by swiping up from the bottom of the screen) from appearing on the lock screen. (iOS 7.0 and later)
Lock Screen Notifications View	Blocks the Notification Center from showing on the lock screen. (iOS 7.0 and later)
Lock Screen Today View	Blocks the Today View from showing on the lock screen. (iOS 7.0 and later)
Ad Tracking	Limits ad tracking.
iTunes	Removes the iTunes icon and prevents access to the iTunes music store.
iTunes Store Password Entry	Requires the user to enter a valid iTunes password before every transaction.
Untrusted TLS Prompt	Automatically rejects untrusted HTTPS certificates without prompting the user. (iOS 5.0 and later)
Shared Stream	Blocks the shared albums or shared Photo Stream feature. (iOS 6.0 and later)
Screenshot	Prevents users from saving a screen capture of the display.
Safari	Removes the Safari icon and prevents the use of the Safari Web browser. This also prevents users from opening Web clips.
Photo Stream	Disables the Photo Stream feature. (iOS 5.0 and later)
Passbook While Locked	Prevents the Passbook notifications from being shown on the lock screen. (iOS 6.0 and later)
Over-the-air PKI Updates	Prevents over-the-air PKI updates. This restriction does not disable CRL and OCSP checks. (iOS 7.0 and later)

**Authentication** Authentication settings applicable to the device.

---

**Note:** If a password policy is enforced on an iOS device, iOS automatically enables the Auto Lock feature. This iOS feature cannot be overridden or disabled by the user or Mobile Security Manager.

---

Element	Description
Password Required	Select to enable password authentication and activate the form for editing.
Password Minimum Length	The least number of characters that the system will accept when the user creates a password.
Password History	The number of passwords that the system will retain to prevent a user from reusing the same passwords.
Maximum Idle Timeout for Auto Lock	The number of minutes before an inactive device is locked.
Maximum Failed Attempts Before Device Wipe	Indicates the number of failed authentication attempts allowed before the system deletes the Workspace and the user data that it contains. When the maximum number of attempts is exceeded, the system resets the device to its original factory state by erasing all of the stored settings, data, and applications.
Password Expiry	Indicates if the user credential should expire after a set number of days. <ul style="list-style-type: none"> <li>■ <b>Set Days</b> - The user credential expires after the number of days defined in <b>Password Expiry Duration</b> has elapsed. The user must change the password once it expires. If the user does not change the password, the device is marked as non-compliant.</li> <li>■ <b>Never</b> - The password does not expire.</li> </ul>
Password Expiry Duration	The number of days that the user credential will remain valid, after which the user must choose a new password.
Password Complexity	<ul style="list-style-type: none"> <li>■ <b>Simple</b> - The system does not impose any password requirements. The user can use any combination of letters, numbers, and/or special characters.</li> <li>■ <b>Alphanumeric</b> - The password must contain letters and numbers.</li> <li>■ <b>Complex</b> - The password must contain at least one letter, one number, and one special character.</li> </ul>

### Android Device Encryption

Element	Description
Turn on Device Encryption	Enables device encryption for Android devices. This option cannot be turned off again once the policy is saved. This option is not available for devices running Android 5.0 (Lollipop) or higher because Device Encryption is always turned on automatically.

### Workspace

Use the Workspace tab to view Workspace settings assigned to this policy. Only Systems Administrators can specify Workspace settings. The Workspace tab is arranged in the following sections:

- [Authentication](#)
- [Workspace/ Apps](#)
- [Application Settings](#)

- [Time Access / Geo Access](#)

Element	Description
Selected Roles	The roles that this policy will affect. Click the <b>Roles</b> tab to add and remove roles.
Specify Workspace details for this policy	To specify Workspace settings for this policy, <i>select</i> the option box. Keep in mind that when multiple policies are assigned to a role, the policies are merged. If Workspace settings are specified for this policy, the values will be merged with the Workspace settings from other policies.  To create a policy without specifying Workspace settings, <i>clear</i> the option box.

**Authentication** Note: PIN settings only apply for PKI authentication and clients configured for PKINIT authentication.

Element	Description
Authentication Only	Select to hide the contents of the Workspace from the user if the Workspace container is being used purely as an authentication client and not for any app UI.
Authentication Frequency	Specifies how often the user sees the login screen: <ul style="list-style-type: none"> <li>■ <b>Always</b> - The user must authenticate every time they try to access the Secure Workspace on their device.</li> <li>■ <b>Idle Timeout</b> - Enforces authentication each time the Idle Timeout Period has been reached. The Timeout Period is the number of minutes a container is allowed to remain inactive before prompting with the login screen with a maximum of two hours. Time that the user spends outside the container is counted against idle time.</li> <li>■ <b>Session</b> - Allows users to exit the Mobile Security Container to use other apps and does not require them to log in upon return until the session ends. A session expires when the Oracle S-token expires (configurable with a default of 10 hours) or the device closes the app due to low memory.</li> </ul>
Idle Timeout Period	The number of minutes before the Workspace is considered to be idle. To be used in combination with the <b>Authentication Frequency - Idle Timeout</b> setting.
Account Lockout Threshold	The number of failed authentication attempts allowed before the <b>Account Lockout Action</b> is triggered.
Account Lockout Action	The action to take when the <b>Account Lockout Threshold</b> has been exceeded: <ul style="list-style-type: none"> <li>■ <b>Do Nothing</b> - Do not take any action.</li> <li>■ <b>Lock</b> - Disables the Secure Workspace from operating and stops user access to virtual applications or information. Only an administrator can unlock the account using the Mobile Security Manager console. Once the Workspace is unlocked, the user still has to log in.</li> <li>■ <b>Wipe</b> - Delete the Workspace and the user data that it contains.</li> </ul>



Element	Description
Shared Workspace Mode	Configures how the Secure Workspace functions on a device that is shared by multiple users. Choose from the following: <ul style="list-style-type: none"> <li>▪ <b>Single User</b> - The Workspace will only be used by a single user on a given device.</li> <li>▪ <b>Multi-User</b> - The Workspace can be shared by multiple users on a given device. The Workspace data will be wiped every time a user logs out of the Workspace.</li> </ul>
PIN History	The number of user credentials that the system will retain to prevent a user from reusing the same PIN.
PIN Minimum Length	The least number of characters that the system will accept when the user creates a PIN.
PIN Expiry	Indicates if the user credential should expire after a set number of days. <ul style="list-style-type: none"> <li>▪ <b>Set Days</b> - The user credential expires after the number of days defined in <b>PIN Expiry Duration</b> has elapsed.</li> <li>▪ <b>Never</b> - The PIN does not expire.</li> </ul>
PIN Expiry Duration	The number of days that the user credential will remain valid, after which the user must choose a new PIN. If the user does not change the PIN, the device is marked as non-compliant.
PIN Complexity	Indicates if minimum requirements are enforced when users create PIN values.
PIN Complexity Min Checks	A number between 1 and 4 that indicates how many of the following <b>Pin must contain...</b> requirements must be satisfied. If the number of options selected below is greater than the <b>PIN Complexity Min Checks</b> value, users may set their PIN with any combination of options that meets the requirements. For example, if <b>PIN Complexity Min Checks</b> is 2 and all four complexity types are selected, a PIN with any combination of two or more of the requirements is acceptable.
PIN must contain lowercase	A check mark indicates that the PIN must include at least one lowercase letter.
PIN must contain uppercase	A check mark indicates that the PIN must include at least one uppercase letter.
PIN must contain special character	A check mark indicates that the PIN must include at least one special character.
PIN must contain numeric	A check mark indicates that the PIN must include at least one numeric character.

**Workspace/ Apps** The Workspace settings to allow or block. Except for **File Sharing** and **Copy/Paste**, allowed items have a check mark.

Element	Description
Location Settings	Allows device location coordinates to be collected from the device if the user has allowed location services during installation. If disabled, the user is not asked to accept location services during installation and user location is not tracked.

Element	Description
Offline Access	Allows the user to access the information already in the container when the user is offline. If disabled, users cannot access the Secure Workspace unless they are online and logged in.  Note that <b>Offline Access</b> only applies if the <b>Shared Workspace Mode</b> setting is set to <b>Single User</b> . If <b>Shared Workspace Mode</b> is set to <b>Multi-User</b> , the container is automatically wiped between user sessions.
E-mail	Allows the user to send e-mail messages from the native OS e-mail client.
Instant Messaging	Allows the user to send instant messages from the Secure Workspace.
Video Chat	Allows the user to access video chat functionality such as FaceTime.
Social Share	Allows the user to access social sharing through integrated services such as Facebook or Twitter.
Print	Allows Workspace apps to print to a printer.
Redirects to Workspace	Allows apps outside the Secure Workspace to redirect a URL into the Workspace.
Save to Media Gallery	Allows photos, images, and videos to be saved to the local media store on the device.
Save to Local Contacts	Allows user contacts to be saved to the contacts manager on the device.
Redirects from Workspace	Allows the Secure Workspace to redirect to an app outside the Workspace with a custom URL scheme.
(Restrict) File Sharing	If checked, restricts the ability of the user to share files outside the Secure Workspace.
(Restrict) Copy/Paste	If checked, copy and paste is only allowed inside the Secure Container, containerized apps, or between containerized apps, but not to apps outside the Secure Workspace.

### Application Settings

Element	Description
Browser	Indicates browser settings as follows: <ul style="list-style-type: none"> <li>■ <b>Address Bar Enabled</b> - Select to show the address bar in the Secure Browser (part of the Secure Workspace). Clear the check box to hide the address bar in the Secure Browser.</li> <li>■ <b>Download Bar Enabled</b> - A check mark indicates that downloading is allowed in the Secure Browser. Clear the check box to disable downloading.</li> </ul>
Doc Editing	Indicates doc editing settings as follows: <ul style="list-style-type: none"> <li>■ <b>Allow</b> - A check mark indicates that the user can access the Workspace doc editor app (if installed).</li> </ul>
File Manager	Indicates file manager settings as follows: <ul style="list-style-type: none"> <li>■ <b>Allow</b> - A check mark indicates that the user has full access to the Secure Workspace file manager app.</li> <li>■ <b>Download Allowed</b> - A check mark indicates that the user can download files and save them locally.</li> </ul>
File Manager Server-Based URL	If the File Manager function is enabled, this is the URL of the File Manager service that provides access to network file shares.

Element	Description
PIM	The PIM (personal information manager) app covers e-mail, calendar, contacts, and notes. Indicates personal information manager settings as follows: <ul style="list-style-type: none"> <li>▪ <b>Allow</b> - A check mark indicates that the user can access the Workspace personal information manager app. Note that the PIM app is licensed separately. Selecting this option does not provide the app.</li> </ul>
E-mail Server URL	Provide the e-mail server URL for the ActiveSync server as it applies to users assigned to this policy. Mobile Security Manager supports different mail servers for different user groups.
Basic ActiveSync Authentication	Select to configure basic authentication for Microsoft Exchange ActiveSync.
Configuration Type	Choose one of the following ActiveSync authentication options: <ul style="list-style-type: none"> <li>▪ <b>Auto</b> - The e-mail server URL is automatically retrieved from the policy and authentication to the e-mail server occurs automatically when it is enabled for one of the single sign-on mechanisms supported by the Secure Workspace app.</li> <li>▪ <b>Basic</b> - The e-mail server URL is automatically retrieved from the policy but basic authentication credentials must be entered by the user during configuration of their PIM client.</li> <li>▪ <b>Manual</b> - Both the e-mail server URL and basic authentication credentials must be entered by the user during configuration of their PIM client.</li> </ul>

### Time Access / Geo Access

Element	Description
Time-Fence	Restrict user access to the Workspace by time of day. Click <b>Add</b> to add a row to the table. In the <b>From</b> column set the time that restricted access should start, and in the <b>To</b> column set the time that the restricted access period should end. Choose a time zone from the <b>Time Zone</b> menu.  To remove a row, select it in the table and click <b>Remove</b> .
Set Geo-Fence by	Shows the cities, states, or countries where access to the Workspace is allowed. If no Geo-Fence is defined the policy defaults to no geo-location restrictions.  Click <b>Add</b> to add a row to the table. Start typing the location name and then select the name from the menu.  To remove a row, select it in the table and click <b>Remove</b> .

### Apps and Configuration

Use the Apps and Configuration tab to view apps and Device Settings assigned to this policy. Only Systems Administrators can edit the settings on the Apps and Configuration tab. The tab is arranged in the following sections:

- [Apps](#)
- [Device Configurations \(iOS Only\)](#)

Element	Description
Selected Roles	The roles that this policy will affect. Click the <b>Roles</b> tab to add and remove roles.

Element	Description
Specify Apps and Configuration details for this policy	To specify apps and/or Device Configuration details for this policy, <i>select</i> the option box. Keep in mind that when multiple policies are assigned to a role, the policies are merged. If catalog details are specified for this policy, the values will be merged with the catalog details from other policies.
	To create a policy without specifying catalog details, <i>clear</i> the option box.

### Apps

Element	Description
Add	Click to add a row to the Apps table, then type the name of the app from the catalog to add for this policy. Apps assigned to the policy can be installed by users whose roles include the policy.
Remove	Click to remove an app from the policy.
Search and Add Apps...	Click to open the Add App dialog and search the catalog for an app to add for this policy. Apps assigned to the policy can be installed by users whose roles include the policy. Choose from the following sort options: <ul style="list-style-type: none"> <li>■ <b>Last Updated</b> - Sort search results such that the most recently updated apps are returned first.</li> <li>■ <b>Display Name</b> - Sort search results alphabetically by app name.</li> </ul> Click <b>Refresh</b> to update the screen with any changes made on the (back-end) server. Click <b>Add</b> to add the selected app to the Apps table. Click <b>Cancel</b> to close the Add App dialog without making any changes.
App Name	The name of the app.
Description	A brief note regarding the app created by a Mobile Security Manager administrator.
Containerized	Indicates if the iOS or Android app is containerized. Containerization adds enterprise security services to apps including advanced features such as multi-factor authentication and Windows integrated Authentication (Kerberos or NTLM).
Virtual App Type	Indicates if the app is a <b>Web App</b> that runs on a remote server and displays in a Web browser, or a <b>Shared Folder App</b> that users can mount on the Workspace.
Platform	Either <b>iOS</b> or <b>Android</b> , or both. This field applies to Apps, but not Virtual Apps.
Install on Homepage	Select to automatically provision this app to the user's main screen or homepage, where they see the browser icon.
Upgrade Alert	Select to alert the user when an app is launched that an update is available. If the option is not selected, a badge on the catalog app indicates that an update is available, but the system does not alert the user otherwise.

**Device Configurations (iOS Only)** Device Configurations allow you to pre-configure e-mail, calendar, Wi-Fi, and VPN settings that you can then assign to policies so that they can be automatically provisioned to users' devices upon device enrollment.

Note: Only *managed* iOS devices support Device Configurations. Device configurations are ignored on Android devices and unmanaged iOS devices.

Element	Description
Type	One of the following device configuration types: <ul style="list-style-type: none"><li>▪ VPN</li><li>▪ E-mail</li><li>▪ Wi-Fi</li><li>▪ Calendar</li></ul> For more information, see <a href="#">Chapter 6, "Device Configurations Help."</a>
Configuration Name	Choose a saved device configuration from the menu.
Configuration Description	A short description to help you or another administrator identify this configuration in the future.

**Related Topics**

"Managing Mobile Security Policies" in *Administering Oracle Mobile Security Suite*



# 4

## Mobile Roles Page Help

System Administrators use roles to associate policies with users, and to perform bulk actions on groups of users based on their role.

### 4.1 Roles Page

Use the Mobile Roles page to:

- Search for one or more roles.
- View a role.
- Add policies to a role (or remove policies from a role).
- Invite users by role assignment to register a device in Oracle Mobile Security Suite.
- Lock, unlock, and wipe devices and Workspaces by role assignment.

#### Search and Sort Menu

Search for roles by name or description, then use the **Sort** menu to reorder the search results.

Element	Description
Search	Type your search criteria.
Sort	Choose from the following: <ul style="list-style-type: none"><li>■ <b>Name</b> - Sort search results alphabetically by role name.</li><li>■ <b>Description</b> - Sort search results alphabetically by Description.</li></ul>

#### Table of Roles

This section of the Mobile Roles page lists roles that meet the search criteria.

Element	Description
Role Name	The name of the role. Role names are managed separately on your organization's directory server. Click the role record to expand it and display additional details; click again to hide the role details.
Description	A brief description of the role.
Last Updated	Timestamp showing the last time that the role metrics were updated.

Element	Description
Actions	<p>Choose from the following:</p> <ul style="list-style-type: none"> <li>▪ <b>Lock</b> - Lock the devices/Workspaces of users assigned to this role. Users can unlock the device by entering a PIN or password. System Administrators <i>cannot</i> unlock the device remotely. Users <i>cannot</i> unlock a locked Workspace. Either a System Administrator or a Help Desk Administrator can unlock a locked Workspace remotely.</li> <li>▪ <b>Unlock</b> - Unlock the devices/Workspaces of users assigned to this role.</li> <li>▪ <b>Wipe</b> - Wipe the devices/Workspaces that belong to users assigned to this role. User data will also be deleted.</li> <li>▪ <b>Invite</b> - Invite users with this role assignment to register a device/Workspace with Oracle Mobile Security Suite.</li> </ul>

The following elements display in the expanded details view if you click a **Role Name**.

Element	Description
Role Name	The name of the role.
Description	A brief description of the role.
Users	The number of users assigned to this role.
Devices	The number of enrolled devices connected to this role.
Workspaces	The number of enrolled Workspaces connected to this role.
Policy	Lists the policies assigned to this role. Click <b>Add</b> to add a new row to the table. Select a row and click <b>Remove</b> to remove a policy from this role.

### Related Topics

"Managing Users and Mobile Roles" in *Administering Oracle Mobile Security Suite*



# 5

## Mobile Users Page Help

Users are managed using your existing directory server. From the Mobile Users page you can view basic user information from the connected directory server, and invite individual users to register a device / Workspace with Oracle Mobile Security Suite.

### 5.1 Users Page

Use the Mobile Users Search View page to:

- Search for one or more users.
- View basic user information from the connected Identity Store.
- Invite a user to register a device/Workspace with Oracle Mobile Security Suite.

#### Search and Sort Menu

Search for users by user name, display name, or e-mail address, then use the **Sort** menu to reorder the search results.

Element	Description
Search	Type your search criteria.
Sort	Choose from the following: <ul style="list-style-type: none"><li>■ <b>Name</b> - Sort search results alphabetically by user name.</li><li>■ <b>Display Name</b> - Sort search results alphabetically by display name.</li><li>■ <b>E-mail</b> - Sort search results alphabetically by e-mail address.</li></ul>

#### Table of Users (Search Results)

This section of the Mobile Users page lists users that meet the search criteria. Click **Load More Items** at the bottom of the page to view additional user records. Click a record to open and close additional user details, or click **Invite** to send an e-mail to a user that invites the user to register a device with Oracle Mobile Security Suite.

Element	Description
User Name	The name that the mobile user uses to sign into the Mobile Security Manager system. This is the unique identifier in the LDAP directory, for example the UID or UPN attribute.
Display Name	The mobile user's display name (usually the first and last name). Click the name to expand the user record and display additional user details; click again to hide the user details.
E-mail	The mobile user's e-mail address.

Element	Description
Invite	Click to open a dialog from which you can send an automated e-mail to the mobile user inviting the user to register a device with Oracle Mobile Security Suite. The <b>Invite</b> button is disabled if an e-mail address is not available for the user, or if the user account is disabled.

The following elements display in the expanded details view if you click a **User Name**.

Element	Description
Display Name	The mobile user's display name (usually the first and last name).
User Name	The name that the mobile user uses to sign into the Mobile Security Manager system. This is the unique identifier in the LDAP directory, for example the UID or UPN attribute.
Status	The status of the user in the LDAP directory.
E-mail	The mobile user's e-mail address.
Roles	A list of roles that the user is a member of.
MSM Role	Indicates whether the user is an administrator, help desk user, or end user when accessing the Mobile Security Manager.

### Related Topics

"Managing Users and Mobile Roles" in *Administering Oracle Mobile Security Suite*

---

---

## Device Configurations Help

Mobile Device Configurations allow Systems Administrators to pre-configure e-mail, calendar, Wi-Fi, and VPN settings. Systems Administrators can then assign Device Configurations to policies so that they can be made available to users based on their role assignments.

### 6.1 Device Configurations Page

Use the Device Configurations page to:

- Search for one or more device configurations.
- View device configuration information.
- Add a new E-mail, VPN, calendar, or Wi-Fi configuration, or delete an existing configuration. (Systems Administrators only.)

The following topics are covered:

- [Device Configuration Search](#)
- [Add E-mail \(Edit E-mail\) Configuration](#)
- [Add VPN \(Edit VPN\) Configuration](#)
- [Add Calendar \(Edit Calendar\) Configuration](#)
- [Add Wi-Fi \(Edit Wi-Fi\) Configuration](#)

#### Device Configuration Search

The Device Configuration Search View page is arranged in the following sections:

- [Command Bar and Search](#)
- [Table of Configurations \(Search Results\)](#)

#### Command Bar and Search





Search for configurations by name, description, or type, then use the **Sort** menu to reorder the search results.

Element	Description
Search	Type your search criteria.
Refresh	Click <b>Refresh</b> to update the screen with any changes made on the (back-end) server.

Element	Description
Sort	Choose from the following: <ul style="list-style-type: none"> <li>▪ <b>Name</b> - Sort search results alphabetically by configuration name.</li> <li>▪ <b>Last Updated</b> - Sort search results chronologically so that the most recently updated records display at the top.</li> </ul>
Add	Click <b>Add</b> to create a new E-mail, VPN, Calendar, or Wi-Fi Device Configuration.

### Table of Configurations (Search Results)

This section of the Device Configurations page lists configurations that meet the search criteria. Click a configuration record to open or close additional details.

Element	Description
	Indicates an E-mail configuration.
	Indicates a VPN configuration.
	Indicates a calendar configuration.
	Indicates a Wi-Fi configuration.
Name	The name assigned to the configuration. Click the name to expand the device configuration record and display additional details; click again to hide the details. Systems Administrators can use the expanded device configuration record to edit the policy.
Description	A short description to help you or another administrator identify this configuration in the future.
Type	One of the following configuration types: E-mail, VPN, Calendar, or Wi-Fi.

### Add E-mail (Edit E-mail) Configuration

Use this page to create a new E-mail configuration, or to edit or view an existing configuration.

#### Basic Properties

Element	Description
Name	The name of this device configuration.

Element	Description
Description	A short description to help you or another administrator identify this configuration in the future.
Account Type	Choose one of the following from the menu: <ul style="list-style-type: none"> <li>■ <b>POP</b> - Post Office Protocol server.</li> <li>■ <b>IMAP</b> - Internet Message Access Protocol server.</li> </ul>
Incoming Mail Server Settings	<p><b>Mail Server</b> - Enter the name of the mail server, for example: <code>imap.example.com</code></p> <p><b>Port</b> - Enter the port number that the incoming mail server is listening on.</p> <p><b>Use SSL</b> - Select if the configuration should use SSL/TLS to connect to the mail server.</p> <p><b>Authentication Type</b> - Choose one of the following from the menu:</p> <ul style="list-style-type: none"> <li>■ <b>Password</b> - The mail server requires a password.</li> <li>■ <b>None</b> - The mail server does not require a password.</li> </ul>
Outgoing Mail Server Settings	<p><b>Mail Server</b> - Enter the name of the mail server, for example: <code>smtp.example.com</code></p> <p><b>Port</b> - Enter the port number that the outgoing mail server is listening on.</p> <p><b>Use SSL</b> - Select if the configuration should use HTTPS (Hypertext Transfer Protocol Secure) to connect to the mail server.</p> <p><b>Authentication Type</b> - Choose one of the following from the menu:</p> <ul style="list-style-type: none"> <li>■ <b>Password</b> - The mail server requires a password.</li> <li>■ <b>None</b> - The mail server does not require a password.</li> </ul>

### Add VPN (Edit VPN) Configuration

Use this page to create a new VPN (virtual private network) configuration, or to edit or view an existing configuration.

#### Basic Properties

Element	Description
Name	The name of this device configuration that will display in the Mobile Security Manager console.
User Defined Name	The VPN configuration name that will be displayed on the end user's device.
VPN Type	Choose one of the following from the menu: <ul style="list-style-type: none"> <li>■ <b>L2TP</b> - Layer 2 Tunneling Protocol</li> <li>■ <b>PPTP</b> - Point-to-Point Tunneling Protocol</li> <li>■ <b>IPSec</b> - Internet Protocol Security</li> </ul>
Description	A short description to help you or another administrator identify this configuration in the future.
Primary Overridden	Specifies whether to send all traffic through the VPN interface. If selected, all network traffic is sent through the VPN.

### Add Calendar (Edit Calendar) Configuration

Use this page to create a new calendar configuration, or to edit or view an existing configuration. This page is arranged in the following sections:

- [Basic Properties](#)
- [Calendar Properties](#)

### Basic Properties

Element	Description
Name	The name of this device configuration.
Description	A short description to help you or another administrator identify this configuration in the future.

### Calendar Properties

Element	Description
Host	Type the calendar server host name.
Port	Enter the calendar server port number.
SSL Enabled	Select this option if the calendar server requires an SSL connection. The configuration will use SSL/TLS to connect to the calendar server.
Account Description	A brief description that will be displayed on the end user's device.

### Add Wi-Fi (Edit Wi-Fi) Configuration

Use this page to create a new Wi-Fi configuration, or to edit or view an existing configuration. This page is arranged in the following sections:

- [Basic Properties](#)
- [Proxy Settings](#)
- [Encryption Settings](#)

### Basic Properties

Element	Description
Name	Enter a unique name for this Wi-Fi configuration.
Service Set Identifier (SSID)	The identifier of the Wi-Fi network to connect to.
Encryption Type	The encryption type enabled on the Wi-Fi network to connection to.
Auto Join Enabled	Select this option if you want mobile devices to automatically connect to the Wi-Fi network without prompting users.
Description	A short description to help you or another administrator identify this Wi-Fi configuration in the future.
Hidden Network	Select if the Wi-Fi network to connect to runs in hidden mode (does not broadcast an SSID).
Protocols	The authentication protocols supported by the Wi-Fi network that this configuration will connect to.

---

## Proxy Settings

Element	Description
Proxy Type	Selects whether a proxy server should be used for the Wi-Fi network and if so whether the proxy server should be specified manually or picked up from a proxy auto-configuration (PAC) file.
Proxy Server	If required, type the name of the proxy server.
Proxy Server Port	If required, type the proxy server port number.

## Encryption Settings

Choose from the provided options to configure the Wi-Fi network's encryption settings. Refer to the manufacturer's documentation for details.

## Related Topics

"Managing Device Configurations" in *Administering Oracle Mobile Security Suite*





# 7

## Mobile Security Manager Settings Help

This section documents the Mobile Security Manager Settings page in the Oracle Access Management console. To open this page from the Oracle Access Management **Launch Pad**, click **Configuration**, then click **View** in the Settings section, then choose **Mobile Security Manager Settings** from the menu. Note that the Mobile Security Manager Settings page says **Mobile Security Settings**.

The following topics are covered:

- [Client Settings](#)
- [Server Settings](#)
- [Identity Store Settings](#)
- [CA Settings](#)
- [User Notification Settings](#)
- [Exchange Server Settings](#)
- [Device Notification Settings](#)
- [Apple Push Notification Service \(APNS\) Settings](#)
- [Google Cloud Messaging \(GCM\) Settings](#)
- [Notification Templates](#)
- [MDM Agent Settings](#)
- [Blacklisted Apps](#)

### 7.1 Client Settings

Use the Client Settings tab to change options and configuration settings that affect the Secure Workspace.

Element	Description
Refresh/Apply/Revert	Click <b>Refresh</b> to update the screen with any changes made on the (back-end) server. Click <b>Apply</b> to save your changes. Click <b>Revert</b> to erase your unsaved changes and restore the screen to its previous state.
Show Save Checkbox in login page	Select to allow users the option to enable the "remember user name" option on the login page. The "remember user name" option is only available if both of the following are true: <ul style="list-style-type: none"><li>▪ The client is configured as the KINIT or OAuth authentication type.</li><li>▪ The Show Save Checkbox in login page option is enabled.</li></ul>

Element	Description
Open URL in secure browser	Select to open protected URLs in the secure browser inside the Secure Workspace. Clear this option to open URLs in the device's default browser. A protected URL is a web app that is protected behind the Mobile Security Access Server.
Enable add App button	Select to include the Catalog app on the users home screen.
Advanced certificate expiration warning time	Enter the number of days in advance that the Secure Workspace should warn users about upcoming certificate expirations.
Poll Interval	Displays the frequency, in seconds, at which the client polls the server for new policies and commands. Values can only be reset by Oracle Professional Services.

### Related Topics

*Administering Oracle Mobile Security Suite*

## 7.2 Server Settings

Use the Server Settings tab to configure the properties that control how the Mobile Security Manager functions at the server level. This tab is organized into the following sections:

- [Server Settings](#)
- [Proxy Settings](#)
- [File Manager Settings](#)

Element	Description
Refresh/Apply/Revert	Click <b>Refresh</b> to update the screen with any changes made on the (back-end) server. Click <b>Apply</b> to save your changes. Click <b>Revert</b> to erase your unsaved changes and restore the screen to its previous state.

### Server Settings

Element	Description
Passcode Expiration	Enter the number of minutes that the Time Limited Passcode (TLP) that is used to reset forgotten PINs or provision Secure Workspace containers is valid. The default value is 60 minutes.
Default Page Size	The default number of records returned at once for a search query (for example, user search, role search, policy search, and so on).
MSAS Host	The complete name of the host that is running the Mobile Security Application Server, for example: host123.example.com
MSAS Port	The SSL port number that the Mobile Security Application Server is listening on. MSM must use an SSL port to communicate with MSAS. The default port number is 9001.

Element	Description
Device/Workspace Operation Queue Archival Policy	<p>Determines if the commands that the Mobile Security Manager sends to devices or Workspaces are deleted or archived (for auditing purposes) after they have been executed.</p> <p>Choose from the following:</p> <ul style="list-style-type: none"> <li>■ <b>Delete</b> - Permanently remove the commands.</li> <li>■ <b>Archive</b> - Save the commands to allow for auditing.</li> </ul>
Device/Workspace De-registration Policy	<p>For devices and Workspaces that have been de-registered, determines if database records are deleted or archived (for auditing purposes) after the de-registration has occurred.</p> <p>Choose from the following:</p> <ul style="list-style-type: none"> <li>■ <b>Delete</b> - Permanently remove the database records.</li> <li>■ <b>Archive</b> - Save the commands to allow for auditing.</li> </ul>

### Proxy Settings

Complete the fields in this section if your environment requires a proxy server to access external web resources.

Element	Description
Use proxy	Select if your enterprise uses a proxy server to access the Internet when sending notification messages.
Proxy Server Host	The complete name of the host that is running the proxy service, for example: <code>www-proxy.example.com</code>
Proxy Server Port	The port number that the proxy service is listening on.
Authentication	Select if authentication is required. Provide values for the <b>Proxy Username</b> and <b>Proxy Password</b> fields.
Proxy User name	The account name required to access the proxy server. Leave blank if the proxy server does not require a user name.
Proxy Password	The account password required to access the proxy server. Leave blank if the proxy server does not require a password.

### File Manager Settings

This tab controls access and security settings for the File Manager service.

Element	Description
Authentication Protocol	Select the authentication options the server should use for the File Manager service.
HTTP Basic	Select this option if the server should use HTTP Basic authentication.
Authentication Challenge	<p>Select this option if the server should offer HTTP Basic authentication to the client.</p> <ul style="list-style-type: none"> <li>■ If selected, the server will offer an HTTP Basic authentication prompt when responding to any unauthenticated requests.</li> <li>■ If this option is <i>not</i> selected, the server will accept HTTP Basic credentials only if the client proactively sends the credentials; the server will reject all other unauthenticated requests without extending an authentication offer.</li> </ul>

Element	Description
Non-SSL	<p>Select this option if the server should allow HTTP Basic authentication over a non-HTTPS connection.</p> <ul style="list-style-type: none"> <li>■ If selected, the server will allow HTTP Basic authentication over insecure connections. This sends unencrypted login information over the network, which is a SEVERE security risk. Selecting this option in a production environment is strongly discouraged.</li> <li>■ If this option is <i>not</i> selected, the server will allow Basic authentication only if the connection is secure.</li> </ul>
Kerberos / NTLM	<p>Select this option if the server should offer Kerberos/NTLM authentication to the client. Kerberos is the preferred authentication protocol for Windows 2000 and subsequent Active Directory domains. NTLM is an older Microsoft authentication protocol.</p>
Options	<p>Select the option that should be given priority. If <b>Kerberos</b> is selected, Kerberos is tried first, followed by NTLM if Kerberos is unsuccessful; If NTLM is selected, NTLM is tried first, followed by Kerberos if NTLM is unsuccessful.</p>

### Related Topics

*Administering Oracle Mobile Security Suite*

## 7.3 Identity Store Settings

Use the Identity Store Settings tab to configure the properties that control how the Mobile Security Manager interacts with the directory server.

Element	Description
Refresh/Apply/Revert	<p>Click <b>Refresh</b> to update the screen with any changes made on the (back-end) server. Click <b>Apply</b> to save your changes. Click <b>Revert</b> to erase your unsaved changes and restore the screen to its previous state.</p>
IDS Profile Name	<p>The Identity Directory Service Profile created in the Oracle Access Management console. Refer to the <i>Oracle Fusion Middleware Administrator's Guide for Oracle Access Management</i> for more details.</p>
System Admin Groups	<p>Add LDAP groups as needed to grant users System Administrator privileges to Oracle Mobile Security Suite.</p> <p>Click <b>Add</b> to create new rows in the table. Click <b>Remove</b> to remove the selected (highlighted) row from the table. Click <b>View &gt; Detach</b> to open the table in a larger window.</p>
Help Desk Groups	<p>Add LDAP groups as needed to grant users Helpdesk User privileges, including access to the Mobile Security Manager console.</p> <p>Click <b>Add</b> to create new rows in the table. Click <b>Remove</b> to remove the selected (highlighted) row from the table. Click <b>View &gt; Detach</b> to open the table in a larger window.</p>

Element	Description
User Deleted Action	<p>Choose the default action that the system should carry out when a user account is deleted in the directory server.</p> <p>Choose from the following:</p> <ul style="list-style-type: none"> <li>▪ <b>Lock</b> - Locks an enrolled device, disables the Secure Workspace container from operating, and stops user access to virtual applications and information.</li> <li>▪ <b>Wipe</b> - Delete the Workspace and the user data that it contains. In the case of an MDM-enrolled device, the device is reset to factory settings. Resetting the device to factory settings is a severe action that cannot be undone.</li> <li>▪ <b>Do Nothing</b> - Retain the user account in Oracle Mobile Security Suite. This option may be useful in test environments.</li> </ul>
User Disabled Action	<p>Choose the default action that the system should carry out when a user account is disabled in the directory of users.</p> <p>Choose from the following:</p> <ul style="list-style-type: none"> <li>▪ <b>Lock</b> - Disables the Secure Workspace container from operating and stops user access to virtual applications and information. This action is typically used in production environments.</li> <li>▪ <b>Wipe</b> - Delete the Workspace and the user data that it contains. This is a severe action that cannot be undone.</li> <li>▪ <b>Do Nothing</b> - Retain the user account in Oracle Mobile Security Suite. This option may be useful in test environments.</li> </ul>
Additional User Attributes	<p>If you are using Mobile Security File Manger and need some LDAP attributes to map a user's Home drive, add those attributes here. For example: <code>homedirectory</code>, <code>uid</code>.</p> <p>Click <b>Add</b> to create new rows in the table. Click <b>Remove</b> to remove the selected (highlighted) row from the table. Click <b>View &gt; Detach</b> to open the table in a larger window.</p>

### Related Topics

"About the Identity Store Directory Server" in *Administering Oracle Mobile Security Suite*

## 7.4 CA Settings

Use the CA Settings tab to create PKI certificate profiles and CA connections.

---

**Note:** Choose a CA provider that uses Microsoft CA servers. Only Microsoft CA servers are supported.

---

For successful processing, you must trust the NDES certificate authority and the certificates issued by the MSM server and the MSAS server. For instructions, see "Configuring NDES and the Active Directory Certificate Authority," and "Configuring CA Settings" in *Administering Oracle Mobile Security Suite*.

- To create a new certificate profile, click **Add Certificate Profile**.
- To edit a certificate profile, click the profile name.
- To delete a certificate profile, click the x to the right of the certificate profile record.

Element	Description
Refresh	Click <b>Refresh</b> to update the screen with any changes made on the (back-end) server.
Element	Description
Name	The name of the certificate profile.
Cert Authority	The name of the certification authority that issued the digital certificate.
SCEP Server URL	The URL for the SCEP (Simple Certificate Enrollment Protocol) server. For example: <code>http://abc.example.com/CertSrv/mscep</code>
Template Name	The name of the certificate template to use. The template name must be present in the CA Authority (NDES), otherwise cert provisioning will fail. Also, the template must be unique for every SCEP profile you create.
Subject Container	A subject Distinguished Name value that is descriptive of your environment, for example:  <code>CN=HOST123-SCEP, OU=Accounting, OU=XYZ, O=ACME, L=Springfield, ST=California, C=US</code>
Static Challenge Credential	The challenge password sent as part of the enrollment request. Click <b>Reveal</b> to show the password; click <b>Conceal</b> to hide it.
Key Type	Choose <b>RSA</b> or <b>DSA</b> from the menu.
Key Size	The bit length for the certificate. Choose <b>512</b> , <b>1024</b> , or <b>2048</b> from the menu.
Subject Name Expression	The name of the holder of the private key associated with the certificate.
Cert Type	Choose from the following: <ul style="list-style-type: none"> <li>■ <b>New</b> - The imported template should be a new cert.</li> <li>■ <b>Escrowed</b> - The imported template should be an escrowed cert.</li> </ul>
Escrow Duration	The number of months that the encryption key is escrowed.
Key Usage	Choose from the menu: <ul style="list-style-type: none"> <li>■ <b>32</b> - Key Encipherment</li> <li>■ <b>128</b> - Digital Signature</li> <li>■ <b>160</b> - Both</li> </ul>
Number of Retries	The number of times that a device should try and get a certificate from the SCEP server.
Retry Delay	The timeout delay in seconds between each retry.

### Related Topics

"Configuring CA Settings" in *Administering Oracle Mobile Security Suite*

"Configuring NDES and the Active Directory Certificate Authority" in *Administering Oracle Mobile Security Suite*

"Configuring Automatic Certificate Revocation with the Active Directory Certificate Authority" in *Administering Oracle Mobile Security Suite*

## 7.5 User Notification Settings

Use this tab to enter your mail server settings. Mobile Security Manager uses e-mail to send users notifications.

---



---

**Note:** Upon clicking **Apply** (save), the system uses a test connection to validate the e-mail server settings.

---



---

Element	Description
Refresh/Apply/Revert	Click <b>Refresh</b> to update the screen with any changes made on the (back-end) server. Click <b>Apply</b> to save your changes. Click <b>Revert</b> to erase your unsaved changes and restore the screen to its previous state.
SMTP Host	The complete name of the host that is running the simple mail transfer protocol service, for example: <code>smtp-host.example.com</code>
SMTP Port	The port number that the SMTP service is listening on. The default port number is 25.
SSL	Select this option if the system should use a Secure Sockets Layer connection to send notifications over e-mail. Clear this option if the system should use an unencrypted connection. When using SSL to connect to the SMTP server, import the certificate into the WebLogic keystore.
SMTP User	The SMTP user account name used to send outgoing e-mail messages.
SMTP Password	The SMTP user's password.
Admin Email	The e-mail address to which bounce-back notifications should be sent.

### Related Topics

*Administering Oracle Mobile Security Suite*

## 7.6 Exchange Server Settings

Use this tab to configure mail server settings if your organization uses Microsoft Exchange.

Element	Description
Refresh/Apply/Revert	Click <b>Refresh</b> to update the screen with any changes made on the (back-end) server. Click <b>Apply</b> to save your changes. Click <b>Revert</b> to erase your unsaved changes and restore the screen to its previous state.
Domain Name	Enter the name of the Windows domain to which the Exchange server belongs.
Server URL	Enter the Exchange Web Service URL exposed by the Exchange server for the Mobile Security Notification Server to connect to.
Service User	Enter the Exchange service account that you created to establish a connection between Oracle Mobile Security Suite and Microsoft Exchange.
Service Password	Enter the service account password.
Server Version	Enter the version of the Exchange server, for example: <code>2010_SP1</code> .
Heartbeat Frequency	Enter a value in seconds that specifies how frequently Exchange server should ping the Mobile Security Notification Server, for example: <code>5</code> .
Listener URL	Enter the URL where the Mobile Security Manager is listening for Exchange notifications. By default this is <code>http://&lt;msm_hostname&gt;:&lt;msm_port&gt;/msm/exchange</code>

**Related Topics**

"Configuring Microsoft Exchange (Secure Mail) to Work With Mobile Security Manager" in *Administering Oracle Mobile Security Suite*

## 7.7 Device Notification Settings

Use this tab to configure notifications that the Mobile Security Manager sends to users. This tab is organized into the following sections:

- [Device Notification Settings](#)
- [Notification Thread Pool Size Setting](#)

Element	Description
Refresh/Apply/Revert	Click <b>Refresh</b> to update the screen with any changes made on the (back-end) server. Click <b>Apply</b> to save your changes. Click <b>Revert</b> to erase your unsaved changes and restore the screen to its previous state.

### Device Notification Settings

Element	Description
Include the e-mail sender in the notification message	Select to include sender details in the notification e-mail.
Include the e-mail subject in the notification message	Select to include the e-mail subject in the notification message.
Notification Server	The name of the notification server.
New E-mail Message	Enter the default message that should populate the Subject line in e-mail messages to the user.
New Calendar Message	Enter the default message that should populate the Subject line in new calendar messages to the user.
New Event Message	Enter the default message that should populate the Subject line in new event messages to the user.

### Notification Thread Pool Size Setting

Element	Description
iOS	Set the number of threads to allocate for iOS device notifications.
Android	Set the number of threads to allocate for Android device notifications.

**Related Topics**

*Administering Oracle Mobile Security Suite*

## 7.8 Apple Push Notification Service (APNS) Settings

Use this tab to manage and upload the required APNS certificates that are used to securely communicate with the Apple Push Notification service. To send push notifications, the certificate uploaded here must be trusted by the Apple APNS server. More information can be found on the Apple development website:

<http://developer.apple.com>



To learn how to obtain an Apple MDM certificate, see "Configuring the APNS Certificate" in *Administering Oracle Mobile Security Suite*.

---

**Note:** Refer to the following Apple support page if you are unable to use the Apple Push Notification service. Devices connected to Wi-Fi that do not have cellular data service require specific ports to be open on network firewalls.

<http://support.apple.com/en-us/HT203609>

---

Element	Description
Refresh/Apply/Revert	Click <b>Refresh</b> to update the screen with any changes made on the (back-end) server. Click <b>Apply</b> to save your changes. Click <b>Revert</b> to erase your unsaved changes and restore the screen to its previous state.
View	Click and choose from the menu to control how the data in the table is displayed: <ul style="list-style-type: none"> <li>▪ <b>Columns</b> - Choose a column name from the menu to quickly show or hide the column. Click <b>Manage Columns</b> to open a dialog that lets you show, hide, and reorder multiple columns.</li> <li>▪ <b>Detach</b> - Click to open the table separately in a larger window.</li> <li>▪ <b>Reorder Columns</b> - Click to open a dialog that lets you change the order of the table columns.</li> </ul>
Add / Remove	Use the buttons in the command bar to update the settings table. <ul style="list-style-type: none"> <li>▪ <b>Add</b> - Click to create a new row in the settings table.</li> <li>▪ <b>Remove</b> - Click to remove the selected (highlighted) row from the settings table.</li> </ul>
Certificate Name	A name for the certificate. Defaults to the certificate file name uploaded, but can be changed. If the certificate is to be used for MDM, the Certificate Name should be <code>MDM</code> . If the certificate is to be used for Exchange E-mail Notifications, it should be named <code>Secure Mail</code> .
Certificate Password	Enter the password for this certificate. This password is required to decrypt the APNS certificate file.
Certificate File	Click <b>Choose File</b> to navigate to the certificate file on your system. The certificate file should be saved in the PKCS12 format. The file will upload to Mobile Security Manager when you save your Apple Push Notification Service settings.

### Related Topics

"Configuring the APNS Certificate" in *Administering Oracle Mobile Security Suite*

## 7.9 Google Cloud Messaging (GCM) Settings

Use this tab to configure the values needed to communicate with the Google Cloud Messaging service. To learn how to create a GCM key, see "Configuring the GCM Entry" in *Administering Oracle Mobile Security Suite*.

---

**Note:** Be sure to configure your firewall to allow connectivity with GCM in order for Android devices to receive messages. Refer to the Android developer documentation for details.

<https://developer.android.com/google/gcm/http.html#request>

---

Element	Description
Refresh/Apply/Revert	Click <b>Refresh</b> to update the screen with any changes made on the (back-end) server. Click <b>Apply</b> to save your changes. Click <b>Revert</b> to erase your unsaved changes and restore the screen to its previous state.
View	Click and choose from the menu to control how the data in the table is displayed: <ul style="list-style-type: none"> <li>■ <b>Columns</b> - Choose a column name from the menu to quickly show or hide the column. Click <b>Manage Columns</b> to open a dialog that lets you show, hide, and reorder multiple columns.</li> <li>■ <b>Detach</b> - Click to open the table separately in a larger window.</li> <li>■ <b>Reorder Columns</b> - Click to open a dialog that lets you change the order of the table columns.</li> </ul>
Add / Remove	Use the buttons in the command bar to update the settings table. <ul style="list-style-type: none"> <li>■ <b>Add</b> - Click to create a new row in the settings table.</li> <li>■ <b>Remove</b> - Click to remove the selected (highlighted) row from the settings table.</li> </ul>
Application ID	The Android app that is registering to receive messages. The Android app is identified by the package name from the manifest. This ensures that the messages are targeted to the correct Android application. The Application ID should be 'MDM' if the GCM entry is to be used for MDM notifications. For Exchange E-mail notifications it should be com.nitrodesk.honey.nitroid.
Sender ID	A project number that you acquire from the API console when building an Android application. The sender ID is used in the registration process to identify a third-party application server that is permitted to send messages to the device.
API Key	A server authentication key that is saved on the third-party application server that gives the application server authorized access to Google services. The API key is included in the header of POST requests that send messages.

### Related Topics

"Configuring the GCM Entry" in *Administering Oracle Mobile Security Suite*

## 7.10 Notification Templates

Use this tab to manage the Invite templates that the system uses to provide notification to users. Multiple instances of a template can be created in different languages. First select a template, then click **Add New Language**.

Element	Description
Create Template	Click to open the New Template dialog.
List of Templates	Shows Invite templates in a column on the left side of the page. Click a template to open it.
Add New Language	Click to create a new instance of a template in another language. First open a template, then click <b>Add New Language</b> and choose a language from the menu. A new tab shows the name of the selected language. Use the editor to format the message content as needed.
Remove	Click to delete the selected language version of the selected template. You can delete a specific language from the template or the entire template. In the Confirm Delete dialog, click <b>Yes</b> , or select the <b>Delete all language versions from template</b> option and then click <b>Yes</b> .

Element	Description
Edit	Click to open a template, then click <b>Edit</b> to modify the verbiage or formatting.

This table describes the elements in the New Template dialog.

Element	Description
Template Type	Specifies the type of template to create. Preset to <b>Invite Template</b> .
Template Name	Give the template a unique, descriptive name.
Language	Choose the language that will be used for the initial instance of the template.

This table describes the placeholders that can be used in an invite template. When the system sends a notification to a user, it replaces the placeholder with data configured in the system.

Element	Description
`\${recipient_name}`	The name of the person that the notification is sent to.
`\${recipient_upn}`	The user's principal name (unique name) in the LDAP directory.
`\${recipient_tlp}`	The passcode that the user should enter when presented with the Request Certificate Page.
`\${tlp_expiration_time}`	The number of minutes that the passcode will remain valid after the invitation is sent.
`\${access_service_host}`	The MSAS Runtime Server Base URL used to construct invitation links.
`\${ios_app_download_link}`	The link to download the Secure Workspace for iOS devices.
`\${android_app_download_link}`	The link to download the Secure Workspace for Android devices.
`\${ios_mdm_registration_link}`	The link to the iOS Device Management (MDM) registration web page.

### Related Topics

*Administering Oracle Mobile Security Suite*

## 7.11 MDM Agent Settings

Use this tab to edit iOS Mobile Device Management (MDM) settings. These settings go into effect during MDM registration. This tab is organized into the following sections:

- [Android](#)
- [iOS](#)

Element	Description
Refresh/Apply/Revert	Click <b>Refresh</b> to update the screen with any changes made on the (back-end) server. Click <b>Apply</b> to save your changes. Click <b>Revert</b> to erase your unsaved changes and restore the screen to its previous state.

**Android**

**Note:** The Android client does not accept the following settings. Instead, to configure these values, see "Change MDM Agent Settings" in *Administering Oracle Mobile Security Suite*.

Element	Description
Display Name	The name of the MDM profile.
Description	A brief note on the MDM profile.
Organization Name	The organization that created the MDM profile.

**iOS**

Element	Description
Display Name	The name of the MDM profile. This value is shown on the device following MDM enrollment.
Description	A brief note on the MDM profile.
Organization Name	The organization that created the MDM profile.

**Related Topics**

*Administering Oracle Mobile Security Suite*

## 7.12 Blacklisted Apps

Use this tab to manage prohibited apps on the device. Apps can only be blacklisted on managed devices. Mobile security policies can check for blacklisted apps during enrollment and take action if a blacklisted app is found on the device. Following device enrollment, mobile security policies can check for blacklisted apps and, if one is found, take appropriate action as defined in the policy.

Element	Description
Refresh/Apply/Revert	Click <b>Refresh</b> to update the screen with any changes made on the (back-end) server. Click <b>Apply</b> to save your changes. Click <b>Revert</b> to erase your unsaved changes and restore the screen to its previous state.
View / Add / Remove	<ul style="list-style-type: none"> <li>■ Click <b>View</b> &gt; <b>Detach</b> to open the table in a larger window.</li> <li>■ <b>Add</b> - Click to create a new row in the settings table.</li> <li>■ <b>Remove</b> - Click to remove the selected (highlighted) row from the settings table.</li> </ul>
App Name	Enter the name of the app package to prohibit on the device.

**Related Topics**

*Administering Oracle Mobile Security Suite*

# Part II

## Mobile Security Access Server (MSAS) Console Help

This part contains reference documentation that describes how to use the Mobile Security Access Server (MSAS) console.

This part contains the following chapters:

- [Chapter 8, "MSAS Applications Help"](#)
- [Chapter 9, "Environments Help"](#)
- [Chapter 10, "Access Policies Help"](#)



---

---

## MSAS Applications Help

This chapter documents the Applications page in the Mobile Security Access Server (MSAS) console. To open this page from the Mobile Security **Launch Pad**, select **Applications** in the Mobile Security Access Server section.

The following topics are covered:

- [MSAS Applications Page](#)
- [MSAS Applications Detail Page](#)
- [Proxy URLs Page](#)
- [URLs Page](#)
- [URL Policy Configuration Page](#)
- [Application Roles Summary Page](#)
- [Application Roles Page](#)

### 8.1 MSAS Applications Page

The Mobile Security Access Server (MSAS) provides a central access control point in the DMZ to secure traffic from mobile devices to back-end URLs. It can act as a reverse proxy (URL virtualization) and a forward proxy.

For URL virtualization you create a virtual URL for an existing back-end URL, where the virtual URL acts like a reverse proxy for the back-end URL. In reverse proxy, the client does not know anything about the back-end URL. It is hidden and the client sees only the virtual URL. In the forward proxy case, the clients know about the back-end URL and can hit it directly with MSAS as the proxy server.

Mobile Security Access Server applications group related URLs to be proxied through the server. Each application:

- Contains the definition of one or more virtual URLs or proxy URLs.
- Contains related security artifacts and access policies attached to each URL.

The applications are deployed to MSAS instances, and can be exported and imported from test to production environments.

When you create an MSAS instance, several reserved applications are created by default. For details about these applications, see "Reserved Applications in MSAS" in *Administering Oracle Mobile Security Access Server*.

Use the MSAS Applications page to:

- View a list of applications across all MSAS instances or an individual instance.

- Search for applications.
- Import an application.
- Create a virtual or proxy application.
- Navigate to the MSAS Applications Detail page where you can view, edit, and export an application.
- Delete or export an application.

The MSAS Applications page is arranged in the following sections:

- [Search](#)
- [Applications Table](#)

### Search

Use the **Search** section of the MSAS Applications page to perform an advanced search for applications in the repository. The results that are returned are the applications that meet the conditions specified in the **Search** and **Type** fields, and sorted as specified in the drop-down.

Element	Description
Search	<p>Select the operator to use to refine the search and enter the search value in the search field. Valid search operators are:</p> <ul style="list-style-type: none"> <li>■ <b>Name</b>—Returns all applications with a name matching the value specified.</li> <li>■ <b>MSAS Instance Name</b>—Returns all applications in an MSAS instance that match the MSAS instance ID specified.</li> <li>■ <b>Tags</b>—Returns all applications that contain the tag matching the value specified.</li> </ul> <p>Use percent % as a wildcard. Asterisk * is not recognized as a wildcard and is treated as plain text. Searches using the Name and Tag operator are case insensitive, but searches using the MSAS Instance Name operator are case sensitive.</p>
Type	<p>Specify the type of applications for which you want to search and display in the results. Valid options are:</p> <ul style="list-style-type: none"> <li>■ <b>Virtual Application</b>—Applications defined in the MSAS environment that specify virtual URLs for back-end URLs.</li> <li>■ <b>Proxy Application</b>—Applications defined in the MSAS environment that specify back-end URLs that will be proxied directly through the Mobile Security Access Server.</li> <li>■ <b>Direct URL</b>—URLs, defined in a DIRECT application, that are directly accessed and are not intercepted by the Mobile Security Access Server.</li> <li>■ <b>Blocked URL</b>—URLs, defined in a BLOCK application, that are designated as inaccessible, or blacklisted.</li> <li>■ <b>ALL</b>—All types of applications in the environment.</li> </ul>
Sort By	<p>Select the order in which the results are displayed: Name, MSAS Instance Name, or Last Modified.</p>

Perform the following actions on this page to add applications to the instance.








Action	Description
Import	<p>Import a zip archive containing an MSAS application. You can use this feature in combination with <b>Export</b> to move applications between different repositories. Click <b>Import</b>, then click <b>Browse</b> to locate the zip archive in your local directory that contains the application to be imported, and click <b>Import</b>.</p> <p>The imported application is added to the list of applications in the Applications table.</p> <p><b>Notes:</b></p> <p>The applications to be imported must use the following directory structure:</p> <p><code>META-INF/virtualapplication/MSASInstanceName/application_name</code></p>
+Create	<p>Use this action to create a new virtual or proxy application.</p> <p>Virtual applications include one or more virtual URLs, or reverse-proxy URLs. In reverse-proxy, you create a virtual URL to hide the actual URL from the client.</p> <p>Proxy applications include one or more forward proxy URLs. In forward proxy, the client is aware of the URL and can access it directly using a proxy server configured on the client side.</p>
Virtual Application	Select <b>Virtual Application</b> to display the Create Virtual Application window.
Name	<p>Enter an application name that adheres to the XML <code>xs:NCName</code> format using only valid NCName ASCII characters. For example, it must start with a letter or underscore (<code>_</code>), and cannot contain any space characters or colons (<code>:</code>). It must be unique within the MSAS instance. Non-ASCII characters are not supported. This field is required.</p> <p>The NCName format is defined in the W3C document <i>Namespaces in XML 1.0 (Third Edition)</i> at <a href="http://www.w3.org/TR/REC-xml-names/#NT-NCName">http://www.w3.org/TR/REC-xml-names/#NT-NCName</a></p>
Display Name	Optionally, enter a name used to clearly identify the instance in the console.
Description	Optionally, provide a description of the application.
MSAS Instance	Select the MSAS instance that will contain this application. This field is required.
Save	Save the application and display the URL summary page where you can add URLs to the application.
Cancel	Exit the Create Virtual Application window without creating the application.
Proxy Application	Select <b>Proxy Application</b> to display the Create Proxy Application window.
Name	<p>Enter an application name that adheres to the XML <code>xs:NCName</code> format using only valid NCName ASCII characters. For example, it must start with a letter or underscore (<code>_</code>), and cannot contain any space characters or colons (<code>:</code>). It must be unique within the MSAS instance. Non-ASCII characters are not supported. This field is required.</p> <p>The NCName format is defined in the W3C document <i>Namespaces in XML 1.0 (Third Edition)</i> at <a href="http://www.w3.org/TR/REC-xml-names/#NT-NCName">http://www.w3.org/TR/REC-xml-names/#NT-NCName</a></p>
Display Name	Optionally, enter a name used to clearly identify the application in the console.
Description	Optionally, provide a description of the application.

Action	Description
MSAS Instance	Select the MSAS instance that will contain this application. This field is required.
Save	Save the application and display the URL summary page where you can add URLs to the application.
Cancel	Exit the Create Proxy Application window without creating the application.

### Applications Table

The **Applications** table displays a list of the applications in the repository that match the criteria specified in the Search fields. The results are displayed as specified in the **Sort By** field.

The following information is provided for each application.

Element	Description
Icon	<p>Each application is indicated by an icon that represents the type of application. Click the icon to open the MSAS Applications Detail page to view or edit the application.</p> <p> Virtual application—Applications defined in the MSAS environment that specify virtual URLs for back-end URLs. In this case, the Mobile Security Access Server acts as reverse-proxy and hides the actual back-end URL from the clients.</p> <p> Proxy application—Applications defined in the MSAS environment that specify back-end URLs that will be proxied directly through the Mobile Security Access Server. In this case, the Mobile Security Access Server acts as a forward proxy. The back-end URLs are visible to the client but the requests are proxied through the Mobile Security Access Server.</p> <p> <b>Direct</b> application—Reserved application per MSAS instance that you can edit to specify URLs that are directly accessed and are not intercepted by the Mobile Security Access Server.</p> <p> <b>Block</b> application—Reserved application per MSAS instance that you can edit to specify URLs that are designated as inaccessible, or blacklisted.</p>
Name/Instance	Application name and the associated MSAS instance. Click the application name to access the MSAS Applications Detail page to view or edit the application.
Type	Type of application, either Virtual Application, Proxy Application, Direct URL, or Blocked URL.
Tag	Optional user-defined tag used to categorize the applications.
Updated By/Last Modified	Name of the user that updated the application and the length of time that has elapsed since it was last updated.
 Options menu	Click to access the <b>Delete</b> and <b>Export</b> actions.

Element	Description
Delete	<p>Delete an application in the instance. In the Delete Application window click <b>Delete</b> to delete the application or <b>Cancel</b> to cancel the operation.</p> <p><b>Note:</b> Reserved applications, such as BLOCK, DIRECT, msm, and msm-reverse-proxy, cannot be deleted.</p>
Export	<p>Export a zip archive containing the application to your local directory. Reserved applications, such as BLOCK, DIRECT, msm, and msm-reverse-proxy, cannot be exported. You can use this feature in combination with <b>Import</b> to move applications between different repositories.</p> <p>Select <b>Export</b> from the menu and save the zip archive to your file system.</p> <p>The directory structure for each application is maintained in the archive file using the following structure:</p> <p><code>META-INF/virtualapplication/MSASInstanceName/application_name</code></p>
Load More Items	<p>Use this action to view additional applications in the Applications table. By default, five rows are displayed. Each time you click <b>Load More Items</b> an additional five rows are shown.</p>

### Related Topics







"Managing Mobile Security Access Server Applications" in *Administering Oracle Mobile Security Access Server*

## 8.2 MSAS Applications Detail Page

Use the MSAS Applications Detail page to:

- View and edit the details of an application.
- View the number of URLs configured in the application and navigate to a page where you can view or search for configured URLs and add URLs.
- Navigate to the Application Roles page where you can view or search for configured roles and add roles.
- View and edit the tags associated with the application.
- Export the application.

The MSAS Applications Detail page provides general summary information about the application and the ability to edit the configuration.

Element	Description
Icon	Indicates representing the type of application: <ul style="list-style-type: none"> <li>  Virtual application—Applications defined in the MSAS environment that specify virtual URLs for back-end URLs. In this case, the Mobile Security Access Server acts as reverse-proxy and hides the actual back-end URL from the clients.         </li> <li>  Proxy application—Applications defined in the MSAS environment that specify back-end URLs that will be proxied directly through the Mobile Security Access Server. In this case, the Mobile Security Access Server acts as a forward proxy. The back-end URLs are visible to the client but the requests are proxied through the Mobile Security Access Server         </li> <li>  DIRECT application—Reserved application per MSAS instance that you can edit to specify URLs that are directly accessed and are not intercepted by the Mobile Security Access Server.         </li> <li>  BLOCK application—Reserved application per MSAS instance that you can edit to specify URLs that are designated as inaccessible, or blacklisted.         </li> </ul>
Name	Name that you specified in the <b>Display Name</b> field when you created the application. If you did not provide a display name, this field is blank. To edit or add a display name, click in the name field and make the desired changes.
Description	Description of the application. To add or edit the description, click in the description field and make the desired changes.
 URLs	The number of URLs configured in the application. Click the search icon to open the URL or Proxy URL page. Use this page to view or search for configured URLs, and to edit the security configuration of the URL.
 Application Roles	Click the search icon to display the Application Roles page. Use this page to view or search for configured application roles, and to add roles. From the Application Roles page you can click <b>Add Roles</b> to display the Create Application Role pages. For more information, see <a href="#">Application Roles Summary Page</a> .
Tags	List of tags configured for the application. You can use tags to categorize applications to make them easier to locate in the console. Click the icon to open the Tags window where you can edit existing tags or add new tags. To add a tag, click <b>Add</b> and enter the tag name in the Tag field. When finished, click <b>OK</b> .
Application Information	Summary information about the application.
MSAS Instance Name	Name of the MSAS instance on which the application is deployed.
Security Context	App stripe used for security artifacts such as authorization policies.
Last Modified	The length of time that has elapsed since the application was updated.
Updated By	User that last updated the application.

Perform the following actions on the MSAS Applications Detail page.

Action	Description
Export	<p>Export a zip archive containing the application to your local directory. Reserved applications, such as BLOCK and DIRECT, cannot be exported. You can use this feature in combination with <b>Import</b> to move applications between different repositories.</p> <p>Select <b>Export</b> from the menu and save the zip archive to your file system.</p> <p>The directory structure for each policy is maintained in the archive file using the following structure:</p> <p><code>META-INF/virtualapplication/MSASInstanceName/application_name</code></p>
Apply	If you have made changes to the application, click <b>Apply</b> to save the changes.
Revert	Click <b>Revert</b> to cancel any changes made to the application.

### Related Topics

"Managing Mobile Security Access Server Applications" in *Administering Oracle Mobile Security Access Server*

## 8.3 Proxy URLs Page

Use the Mobile Security Access Server Proxy URLs page to:

- View a list of the proxy URLs configured in a proxy application.
- Search for proxy URLs in the application.
- Add proxy URLs to an application.
- Delete proxy URLs from an application.
- Navigate to the URL Policy Configuration page where you can secure the URL using policies and assertions.

The Proxy URLs page is arranged in the following sections:

- [Search](#)
- [Proxy URLs Table](#)

### Search

Use the **Search** section of the Proxy URLs page to search for URLs configured in the application. The results that are returned are the URLs that meet the conditions specified in the **Search** field, and sorted as specified in the **Sort By** drop-down.

Element	Description
Search	<p>Enter all or part of a proxy URL name in the search field and click the search icon.</p> <p>Use percent % as a wildcard. Asterisk * is not recognized as a wildcard and is treated as plain text. Searches are case-insensitive.</p>
Sort By	Select the order in which the results should be sorted, either by Name or by Last Modified date.



Perform the following action on this page to add proxy URLs to the application.

Action	Description
+ ProxyURL	Use this action to add a proxy URL to the application.
Add	Click <b>Add</b> to add one or more proxy URLs to the application. To add multiple URLs, click <b>Add</b> multiple times.
Host URL	Enter the URL to add to the application. It must be unique to all applications in the MSAS instance.
Name	Enter a meaningful name for the proxy URL.
Description	Optionally, provide a description of the proxy URL.
2-Way SSL	Reserved for future use.
Save	Save the proxy URL in the application and display the URL summary page.
Cancel	Exit the Add Proxy URL window without adding the proxy URLs to the application.

### Proxy URLs Table

The Proxy URLs table displays a list of the proxy URLs configured in the application and that match the criteria specified in the Search field. The results are displayed as specified in the **Sort By** field.

The following information is provided for each proxy URL.

Element	Description
 Proxy URL Icon	Click the Proxy URL icon to access the URL configuration page to attach policies or assertions to secure the access.
Name	Name of the proxy URL that you specified in the <b>Name</b> field when you added the URL to the application. Click the URL name to access the URL configuration page to secure the URL.
URL	URL that you specified in the <b>Host URL</b> field that you added to the application.
Updated By/Last Modified	Name of the user that updated the application and the length of time that has elapsed since it was last updated.
 Options menu	Click the options menu icon to access the <b>Delete</b> and <b>Edit</b> actions.
Delete	Delete the URL from the application. In the Delete URL window, click <b>Delete</b> to delete the URL or <b>Cancel</b> to cancel the operation.
Edit	Edit the proxy URL. In the Edit Proxy URL window, enter the desired changes in the fields and click <b>Apply</b> to save the changes or <b>Cancel</b> to exit the window without saving the changes.
Load More Items	Use this action to view additional URLs in the Proxy URLs table. By default, five rows are displayed. Each time you click <b>Load More Items</b> an additional five rows are shown.

### Related Topics

"Managing URLs in an MSAS Application" in *Administering Oracle Mobile Security Access Server*

## 8.4 URLs Page

Use the Mobile Security Access Server URLs page to:

- View a list of URLs configured in a virtual application.
- Search for URLs in the application.
- Add URLs to an application.
- Delete URLs from an application.
- Navigate to the URL Policy Configuration page where you can secure the URL using policies and assertions.

The URLs page is arranged in the following sections:

- [Search](#)
- [URLs Table](#)

### Search

Use the **Search** section of the URLs page to search for URLs configured in the application. The results that are returned are the URLs that meet the conditions specified in the **Search** field, and sorted as specified in the **Sort By** drop-down.

Element	Description
Search	Enter the URL name, or partial name, in the search field and click the search icon.  Use percent % as a wildcard. Asterisk * is not recognized as a wildcard and is treated as plain text. Searches are case-insensitive.
Sort By	Select the order in which the results should be sorted, either by Name or by Last Modified date.

Perform the following actions on this page to add virtual URLs to the application.



Action	Description
+URL	Use this action to add a virtual URL to the application.
Add	Click <b>Add</b> to add one or more URLs to the application. To add multiple URLs, click <b>Add</b> multiple times.
Host URL	Enter the URL to add to the application. This URL will not be visible to clients.
Name	Enter a name for the virtual URL.
MSAS URI	Enter the virtual URL that will be visible to clients. It must be unique within the MSAS instance. For example <code>virtualURL01</code> .
Description	Optionally, provide a description of the virtual URL.

Action	Description
HTTP Method	<p>HTTP method to use for the virtual URL. Valid options are:</p> <ul style="list-style-type: none"> <li>■ GET—Retrieves the information specified in the request URI.</li> <li>■ POST—Requests that the origin server accept the entity enclosed in the request as a new subordinate of the resource identified by the Request URL.</li> <li>■ PUT—Requests that the target resource be created or modified with the entity enclosed in the request message.</li> <li>■ HEAD— Identical to GET but without the message body in the response.</li> <li>■ OPTIONS—Returns the HTTP methods that the server supports for the URL.</li> <li>■ TRACE—Loops the received request back to the client so that they can see what was received by the server and any intermediaries.</li> <li>■ CONNECT—Not supported.</li> <li>■ DELETE—Delete the resource specified in the request URL.</li> <li>■ All—All HTTP verbs.</li> </ul> <p>For details about HTTP methods, see the <i>Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content</i> RFC document at <a href="https://tools.ietf.org/html/rfc7231">https://tools.ietf.org/html/rfc7231</a>.</p>
2-Way SSL	Reserved for future use.
Save	Save the URL in the application and display the URL summary page.
Cancel	Exit the Add URL window without adding the URLs to the application.

### URLs Table

The URLs table displays a list of the virtual URLs configured in the application and that match the criteria specified in the Search field. The results are displayed as specified in the **Sort By** field.

The following information is provided for each virtual URL.

Element	Description
	Click the URL icon to access the URL configuration page to attach policies or assertions to secure the access to the URL.
Name/Description	Name and description of the virtual URL that you specified when you added the URL to the application. Click the URL name to access the URL configuration page to secure the access to the URL.
HTTP Method	The MSAS URI and the associated HTTP method that you specified when you added the URL.
Updated By/Last Modified	Name of the user that updated the application and the length of time that has elapsed since it was last updated.
	Click the options menu icon to access the <b>Delete</b> and <b>Edit</b> actions.
Options menu	
Delete	Delete the virtual URL from the application. In the Delete URL window click <b>Delete</b> to delete the URL or <b>Cancel</b> to cancel the operation.



Element	Description
Edit	Edit the virtual URL. In the Edit URL window, enter the desired edits in the fields and click <b>Apply</b> to save the changes or <b>Cancel</b> to exit the window without saving the changes.
Load More Items	Use this action to view additional URLs in the URLs table. By default, five rows are displayed. Each time you click <b>Load More Items</b> an additional five rows are shown.

### Related Topics

"Managing URLs in an MSAS Application" in *Administering Oracle Mobile Security Access Server*

## 8.5 URL Policy Configuration Page

Use the URL Policy Configuration page to:

- View the policies or assertions attached to a URL.
- Attach policies or assertions to policy enforcement points of a URL. You can attach policies and assertions on request from the client to MSAS, at invoke from MSAS to the back-end web application, and on response from MSAS to the client.
- View the details of a policy attached to a URL.
- Override configuration properties for an attached policy.
- Validate that the policy attachments adhere to the validation rules.

The URL Policy Configuration page provides the ability to attach policies and assertions to policy enforcement points in URLs and to configure property overrides in a policy.

Element	Description
Icon/Name	URL icon and name of the URL that you specified when you added the URL to the application. This field is read-only.
Host URL	The URL to be secured in the application. For virtual URLs, this represents the back-end URL to be hidden from the client. This field is read-only.
Description	Description that you provided when you added the URL to the application. This field can be blank.
2-way SSL	Indicates whether 2-way SSL is enabled or disabled
MSAS URI	The virtual URI that will be exposed to the client in place of the host URL. This field appears for virtual URLs only.
HTTP Method	Action that should be performed when the URI is invoked. This field is displayed for virtual URLs only.
Policies tab	Displays the policy enforcement points to which you can attach policies and assertions.
On-Request	Use this field to attach one or more policies or assertions to secure access from the client to MSAS. Click the options menu and select <b>Add Assertion</b> , <b>Add Policy</b> , or <b>Reorder</b> from the menu.

Element	Description
Add Assertion	<p>Attach one or more assertions to the policy enforcement point. The Add Assertion page is displayed with a list of all the available assertions that are applicable. Use this page to search for existing assertion templates and use them to attach assertions to the policy enforcement point.</p> <p>In the Add Assertion page, provide search parameters in the <b>Name</b> and <b>Category</b> fields and click <b>Search</b>. The results that match the search criteria are displayed in the search results table.</p> <p>In the search results table, select the assertion or assertions to be attached and click <b>Add Selected</b>. To attach all the listed assertions, click <b>Add All</b>. The selected assertions are displayed in the Selected Assertion Templates table.</p> <p>In the Selected Assertion Templates table, review the selections. To remove one or more assertions from this table, click <b>Remove Selected</b> or <b>Remove All</b>. When you have confirmed the assertion selection, click <b>Add Assertion</b>.</p> <p>Click <b>Add Assertion</b> to attach the assertions to the policy enforcement point, or <b>Cancel</b> to exit the window without attaching assertions.</p> <p><b>Note:</b> When you attach an assertion to the on-request policy enforcement point, the compatible assertion is automatically attached to the on-response endpoint.</p>
Add Policy	<p>Attach one or more policies to the policy enforcement point. The Attach Policies page is displayed with a list of all the available policies that are applicable. Use this page to search for existing policies and use them to attach policies to the policy enforcement point.</p> <p>In the Attach Policies page, provide search parameters in the <b>Name</b> and <b>Category</b> fields and click <b>Search</b>. The results that match the search criteria are displayed in the search results table.</p> <p>In the search results table, select the policy or policies to be attached and click <b>Add Selected</b>. To attach all the listed policies, click <b>Add All</b>. The selected policies are displayed in the Selected Policies table.</p> <p>In the Selected Policies table, review the selections. To remove one or more policies from this table, click <b>Remove Selected</b> or <b>Remove All</b>. When you have confirmed the policy selection, click <b>Attach Policies</b>.</p> <p><b>Note:</b> When you attach a policy to the on-request policy enforcement point, the compatible policy is automatically attached to the on-response endpoint.</p>
Reorder	<p>Reorder the attached policies and assertions. In the Reorder window, select the desired assertion or policy and click the up or down arrow to change the order. Click <b>OK</b> when finished to save the changes, or <b>Cancel</b> to exit the window without changing the assertion order.</p>
Invoke Proxy/Invoke	<p>Use this field to attach policies or assertions used to invoke the back-end web application (URL). Click the options menu icon and select <b>Add Assertion</b>, <b>Add Policy</b>, or <b>Reorder</b> from the menu.</p>
Add Assertion	<p>Attach one or more assertions to the policy enforcement point. The Add Assertion page is displayed with a list of all the available assertions that are applicable. Use this page to search for existing assertion templates and use them to attach assertions to the policy enforcement point.</p> <p>In the Add Assertion page, provide search parameters in the <b>Name</b> and <b>Category</b> fields and click <b>Search</b>. The results that match the search criteria are displayed in the search results table.</p> <p>In the search results table, select the assertion or assertions to be attached and click <b>Add Selected</b>. To attach all the listed assertions, click <b>Add All</b>. The selected assertions are displayed in the Selected Assertion Templates table.</p> <p>In the Selected Assertion Templates table, review the selections. To remove one or more assertions from this table, click <b>Remove Selected</b> or <b>Remove All</b>. When you have confirmed the assertion selection, click <b>Add Assertion</b>.</p>

Element	Description
Add Policy	<p>Attach one or more policies to the policy enforcement point. The Attach Policies page is displayed with a list of all the available policies that are applicable. Use this page to search for existing polices and use them to attach policies to the policy enforcement point.</p> <p>In the Attach Policies page, provide search parameters in the <b>Name</b> and <b>Category</b> fields and click <b>Search</b>. The results that match the search criteria are displayed in the search results table.</p> <p>In the search results table, select the policy or policies to be attached and click <b>Add Selected</b>. To attach all the listed policies, click <b>Add All</b>. The selected policies are displayed in the Selected Policies table.</p> <p>In the Selected Policies table, review the selections. To remove one or more policies from this table, click <b>Remove Selected</b> or <b>Remove All</b>. When you have confirmed the policy selection, click <b>Attach Policies</b>.</p>
Reorder	<p>Reorder the attached policies and assertions. In the Reorder window, select the desired assertion or policy and click the up or down arrow to change the order. Click <b>OK</b> when finished to save the changes, or <b>Cancel</b> to exit the window without changing the assertion order.</p>
On-Response	<p>Use this field to attach policies or assertions to secure the response message sent back to the client. Click the options menu icon and select <b>Add Assertion</b>, <b>Add Policy</b>, or <b>Reorder</b> from the menu.</p>
Add Assertion	<p>Attach one or more assertions to the policy enforcement point. The Add Assertion page is displayed with a list of all the available assertions that are applicable. Use this page to search for existing assertion templates and use them to attach assertions to the policy enforcement point.</p> <p>In the Add Assertion page, provide search parameters in the <b>Name</b> and <b>Category</b> fields and click <b>Search</b>. The results that match the search criteria are displayed in the search results table.</p> <p>In the search results table, select the assertion or assertions to be attached and click <b>Add Selected</b>. To attach all the listed assertions, click <b>Add All</b>. The selected assertions are displayed in the Selected Assertion Templates table.</p> <p>In the Selected Assertion Templates table, review the selections. To remove one or more assertions from this table, click <b>Remove Selected</b> or <b>Remove All</b>. When you have confirmed the assertion selection, click <b>Add Assertion</b>.</p> <p>Click Add Assertion to attach the assertions to the URL, or Cancel to exit the window without attaching assertions.</p> <p><b>Note:</b> When you attach an assertion to the on-request policy enforcement point, the compatible assertion is automatically attached to the on-response endpoint.</p>
Add Policy	<p>Attach one or more policies to the policy enforcement point. The Attach Policies page is displayed with a list of all the available policies that are applicable. Use this page to search for existing polices and use them to attach policies to the policy enforcement point.</p> <p>In the Attach Policies page, provide search parameters in the <b>Name</b> and <b>Category</b> fields and click <b>Search</b>. The results that match the search criteria are displayed in the search results table.</p> <p>In the search results table, select the policy or policies to be attached and click <b>Add Selected</b>. To attach all the listed policies, click <b>Add All</b>. The selected policies are displayed in the Selected Policies table.</p> <p>In the Selected Policies table, review the selections. To remove one or more policies from this table, click <b>Remove Selected</b> or <b>Remove All</b>. When you have confirmed the policy selection, click <b>Attach Policies</b>.</p> <p><b>Note:</b> When you attach a policy to the on-request policy enforcement point, the compatible policy is automatically attached to the on-response endpoint.</p>

Element	Description
Reorder	Reorder the attached policies and assertions. In the Reorder window, select the desired assertion or policy and click the up or down arrow to change the order. Click <b>OK</b> when finished to save the changes, or <b>Cancel</b> to exit the window without changing the assertion order.

When you attach a policy or assertion to a policy enforcement point, it is listed beneath the policy enforcement point to which it is attached. Click the options menu icon for an attached policy or assertion to perform the following actions.

Action	Description
Edit	Use this action to view or edit the details for an attached policy or assertion.
General	<p>For attached policies, this tab displays general information about the policy in read-only format, including the name, display name, description, the type of endpoints to which the policy can be attached, and so on.</p> <p>For attached assertions, this tab displays details about the assertion including the name, the category to which the assertion belongs (for example security/authentication or security/msg-protection), the type of assertion (for example http-jwt-token), and whether the assertion is enforced and advertised.</p> <p>The Details or Settings section provides the ability to view the settings for the selected assertion. Assertion template details vary based on the type of assertion. For example, assertions that include message protection will include settings that are specific to message security.</p>
Versioning History	<p>Click Versioning History to open the Policy Version History page that you use to view a list of all versions of the policy, view the details of any policy version in read-only format, activate any version of a policy, and delete or export any version of a policy.</p> <p>You cannot edit a policy from the Policy Version History page. You must edit and save the policy in the Policy Details page.</p>
Assertions	<p>If you selected an attached policy, click this tab to view the assertions in the policy. Click an assertion to view details about the assertion including the name, the category to which the assertion belongs (for example security/authentication or security/msg-protection), the type of assertion (for example http-jwt-token), and whether the assertion is enforced and advertised.</p> <p>The Details section provides the ability to view the settings for the selected assertion. Assertion template details vary based on the type of assertion. For example, assertions that include message protection will include settings that are specific to message security.</p>
Overrides	<p>Click this tab to view the configuration properties for the policy/assertion. Configuration properties vary based on the assertion. Use these fields to override a property on a per-attachment basis.</p> <p>To override a property, enter the override value in the <b>Value</b> field and press Enter or click anywhere on the page to activate <b>Apply</b> and <b>Revert</b>. To save your changes, click <b>Apply</b>. To cancel the changes before saving, click <b>Revert</b>.</p> <p>Note that for some policies that contain a <code>csf.key</code> property, you can press <b>Click to Add</b> to add username/password credentials for creating a token on the outbound request. After adding a <code>csf.key</code>, you can delete it if necessary by clicking <b>X</b>.</p>

After attaching or detaching policies or assertions, or overriding the configuration properties for an attached policy or assertion, perform the following actions to validate and save and changes.

Action	Description
Validate	When you have finished attaching policies or assertions to the policy enforcement points, click <b>Validate</b> to dynamically check whether the combination of attached policies and assertions is valid.
Apply	Click <b>Apply</b> to save changes to the application or overrides on a policy or assertion.
Revert	Click <b>Revert</b> to cancel any changes.

### Related Topics

"Securing Mobile Security Access Server Resources" in *Administering Oracle Mobile Security Access Server*

## 8.6 Application Roles Summary Page

In Mobile Security Access Server, the scope of an application role is the MSAS application. That is, the roles in one MSAS application apply only to that application and are not visible to other MSAS applications. Application roles are supported in both virtual and proxy applications and are used with the authorization policy to configure role-based authorization.

Use the Mobile Security Access Server Application Roles Summary page to:



- View a list of the application roles configured in the application.
- Search for application roles in the application.
- Navigate to the Application Roles page where you can create and add roles to an application, edit existing roles, manage application role hierarchy, and map users to application roles.
- Delete application roles from an application.

Perform the following actions on this page to search for roles and to add roles to the application.

Action	Description
Search	Enter all or part of a role name in the search field and click <b>Search</b> .  Wildcards are not recognized and are treated as plain text. Searches are case-insensitive.
Add Role	Use this action to access the Create Application Roles page where you can add roles to the application.

### Application Roles Table

The Application Roles table displays a list of the roles configured in the application and that match the criteria specified in the Search field.

Element	Description
	Click the icon to access the Application Roles page where you can add or change the role hierarchy and mappings.
Role Icon	
Name	Name or display name that you specified when you created the role. If specified, this field uses the display name. If no display name was specified, it uses the application role name.
Description	The role description you specified when you created the role.
	Click the options menu icon to access the <b>Delete Role</b> and <b>Edit Role</b> actions.
Options menu	
Edit Role	Edit the application role. When you click <b>Edit Role</b> the Application Roles page displays. Enter the desired edits in the fields and click <b>Apply</b> to save the changes or <b>Revert</b> to exit the window without saving the changes.
Delete Role	Delete a role in the application. In the Remove App Role window, click <b>Remove</b> to delete the application role or <b>Cancel</b> to cancel the operation.
Load More Items	Use this action to view additional application roles in the table. By default, five rows are displayed. Each time you click <b>Load More Items</b> an additional five rows are shown.

### Related Topics

"Configuring Authorization in MSAS Applications" in *Administering Oracle Mobile Security Access Server*

"Managing Roles in an MSAS Application" in *Administering Oracle Mobile Security Access Server*

## 8.7 Application Roles Page

Use the Application Roles page to:

- View the details for an application role.
- Create a new application role in the application if you access this page using **Add Role** on the Application Roles Summary page.
- Edit an existing application role in the application.
- Manage Application Role hierarchy—Roles can be combined in a hierarchy where higher-level roles subsume permissions owned by sub-roles.
- Map application roles to external roles
- Map application roles to users

The Application Roles page provides general information about the role.

Element	Description
Name	Name of the application role. It must be unique in the application. This field is required.
Display Name	Optionally, enter a name used to clearly identify the role in the console.
Description	Optionally, provide a description for the application.

The page also provides three tabs which allow you to define the role hierarchy and map the role to users and externally.

- [App Role Hierarchy](#)
- [External Role Mapping](#)
- [User Mapping](#)

### App Role Hierarchy

The App Role Hierarchy tab creates role relationships between roles. Roles can be combined in a hierarchy where higher-level roles subsume permissions owned by sub-roles.

Field	Description
Inherits From	Specify the application roles from which the current application role (the role being created or edited) should inherit permissions.
Search	Enter all or part of a role name and click <b>Search</b> to display the results. Empty strings fetch all roles in the application.
Add to hierarchy	Create a role relationship between the current role and the selected role. The selected role is added to the App Roles table.
App Roles	Table listing the application roles from which the current role has inherited permissions.
Remove	Remove the relationship between the selected role in the App Roles table and the current role.
Inherited By	Click this tab to view the application roles that inherit the permissions of this role.

### External Role Mapping

Use the **External Role Mapping** tab to map the selected role to external roles.

Field	Description
Search	Enter all or part of a role name and click <b>Search</b> to display the results. Empty strings fetch all roles configured in the WebLogic Server domain.
Map to Role	Select the external role to map to the application role and click <b>Map to Role</b> . The selected role is added to the Mapped Roles table.
Mapped Roles	Table listing the external roles mapped to the application role. Each row lists the role name and description.
Remove	Remove the mapping between the selected external role and the application role.

### User Mapping

Use the **User Mapping** tab to map the selected role to existing users.

Field	Description
Search	Enter all or part of a user name and click <b>Search</b> to display the results. Empty strings fetch all users with the appropriate privileges in the identity store.
Map to Role	Select the user to map to the application role and click <b>Map to Role</b> . The selected user is added to the Mapped Users table

<b>Field</b>	<b>Description</b>
Mapped Users	Table listing the users mapped to the application role. Each row lists the user name and description.
Remove	Remove the user mapping from the application role.

**Related Topics**

"Configuring Authorization in MSAS Applications" in *Administering Oracle Mobile Security Access Server*

"Managing Roles in an MSAS Application" in *Administering Oracle Mobile Security Access Server*



---



---

## Environments Help

This chapter documents the Environments pages in the Mobile Security Access Server (MSAS) console and describes how to configure security for individual MSAS instances. To open this page from the Mobile Security Launch Pad, select **Environments** in the Mobile Security Access Server section.

This chapter contains the following topics:

- [Environments Page](#)
- [MSAS Instances Summary Page](#)
- [MSAS Instance Configuration Page](#)

### 9.1 Environments Page

Use the Environments page to perform the following tasks in the MSAS environment:

- View the total number of MSAS instances configured in the environment.
- View the total number of applications deployed on the MSAS instances.
- View the total number of URLs configured in the MSAS instances.
- Navigate to the MSAS Instances Summary page to see summary information for each instance.
- Navigate to the Mobile Security Access Server Applications Summary page to view summary details about each application.
- Register a new MSAS instance with the MSM server.

The Environments page provides a high-level summary of the MSAS instances, applications, and URLs.

Element	Description
MSAS	Instances in the environment. Click to navigate to the MSAS Instances Summary page.
Instances	Total number of MSAS instances registered in the environment. Click to navigate to the MSAS Instances Summary page.
Applications	Total number of Mobile Security Access Server applications in all the MSAS instances in the environment. Click to navigate to the Mobile Security Access Server Applications Summary page.
URLs	Total number of URLs configured in all the MSAS applications in the environment.

Element	Description
Register Instance	Click to create a new logical MSAS instance and register the instance with the MSM server. When you register the instance you can configure it in the MSAS Instance Configuration page.
Display Name	Meaningful name that will be used to identify the instance in the console.
Name	<p>Unique name used to identify the MSAS instance that adheres to the XML xs:NCName format using only valid NCName ASCII characters. For example, it must start with a letter or underscore (_), and cannot contain any space characters or colons (:). It must be unique within the MSAS environment. Non-ASCII characters are not supported. This field is required.</p> <p>The NCName format is defined in the W3C document <i>Namespaces in XML 1.0 (Third Edition)</i> at <a href="http://www.w3.org/TR/REC-xml-names/#NT-NCName">http://www.w3.org/TR/REC-xml-names/#NT-NCName</a></p>
Description	Brief description of the instance.
OK	Save the new instance. The MSAS Instance Configuration page displays where you can provide configuration details.
Cancel	Exit the Register MSAS Instance dialog without registering the instance.

### Related Topics

"Managing Mobile Security Access Server Instances" in *Administering Oracle Mobile Security Access Server*

## 9.2 MSAS Instances Summary Page

Use the MSAS Instances Summary page to perform the following tasks in the Mobile Security Access Server environment:

- Search for instances in the environment. You also can use this field to filter the number of instances displayed on the page.
- View summary details for all instances in the environment, including number of applications and URLs.
- Navigate to the MSAS Instance Configuration page for each instance.
- Navigate to the MSAS Applications Summary page for each instance.
- Delete MSAS instances.

Element	Description
Search	<p>Enter all or part of an MSAS instance name in the search field and click <b>Search</b>. You can use the search field to filter the number of instances displayed. Empty strings display all instances in the environment.</p> <p>Wildcards are not recognized and are treated as plain text. Searches are case-insensitive.</p>
Instance name	Name of the instance that you specified when you created the instance. Click the instance name to access the MSAS Instance Configuration page.
X	<p>Delete the instance from the environment. Click <b>X</b>, then in the Delete MSAS Instance window, click <b>OK</b> to delete the instance or <b>Cancel</b> to cancel the operation.</p> <p>When you delete the instance, all associated applications and URLs are also deleted.</p>

Element	Description
Applications	Total number of applications configured in the instance. Click <b>Applications</b> to access the Applications Summary page for the instance.
URLs	Total number of URLs configured in all applications in the instance.
Configure	Click to access the MSAS Instance Configuration Page.
Synchronize	Synchronize the MSAS instance configuration with the MSAS runtime server. Typically, synchronization occurs at a user-specified polling interval. Clicking <b>Synchronize</b> forces immediate synchronization and avoids having to wait for the polling interval for the changes to take effect.
Show more	View additional instances in the environment. By default, ten instances are displayed. Each time you click <b>Show More</b> an additional five instances are shown.  <b>Note:</b> You can adjust the screen width of the display area to view all of the instances. To do so, select the username in the upper right corner, then Screen Width, then the desired width.

### Related Topics

"Managing Mobile Security Access Server Instances" in *Administering Oracle Mobile Security Access Server*

## 9.3 MSAS Instance Configuration Page

Use the MSAS Instance Configuration page to perform the following tasks on an MSAS instance:

- View or modify general configuration information.
- View or configure identity store profiles.
- View or configure authentication settings for the instance, such as trusted issuers.
- View or configure keystore and message security settings.
- View or configure the connection between the Mobile Security Access Server and the Mobile Security Manager.
- View or configure the authentication endpoints for the instance.
- View or configure outbound message, proxy server, and server settings.

The MSAS Instance Configuration page is arranged in the following tabs:

- [General](#)
- [Identity Store Profiles](#)
- [Authentication](#)
- [Message Security](#)
- [Policy Access](#)
- [Authentication Endpoints](#)
- [System Settings](#)

### General

The **General** tab of the MSAS Instance Configuration page displays the instance name and description, the URL of the physical MSAS instance to which this logical instance is bound, the number of URLs and applications in the instance, and version data. You

can modify the display name and the description for the instance. It also provides version information for the configuration.

Element	Description
Name	Unique identifier for the instance. This field is read-only.
Display Name	Meaningful name used to identify the instance in the user interface. This field is editable.
Description	Description of the instance. This field is editable.
MSAS URLs	URLs of the physical MSAS instances to which this logical instance is bound. For details about creating a physical MSAS instance, see "Configuring an MSAS Instance."  A logical MSAS instance can be bound to more than one physical instance. How?
Host	Physical MSAS instance host.
Port	Physical MSAS instance port.
Stats	General statistics about the instance in read-only mode.
URLs	Total number of URLs added to all the applications in the MSAS instance.
Applications	Total number of applications in the MSAS instance.

### Version Information

The **Version Information** section provides details about the version of the MSAS instance in read-only mode.

Element	Description
Version Number	Number of times the MSAS instance has been updated.
Last Updated	Timestamp of the last update to the MSAS instance.
Updated By	User who last updated the MSAS instance.

### Identity Store Profiles

The Identity Store Profiles tab of the MSAS Instance Configuration page provides the ability to add an identity store profile to the MSAS instance, edit an existing profile, and set the default profile to be used by the instance. An identity store profile is a logical representation of a user repository. There can be multiple profiles associated with an MSAS instance, and one profile can be marked as the default against which all authentication and user profile queries will occur.

The Identity Store Profile table displays a list of the profiles defined in the MSAS instance.

Element	Description
Profile Name	Name of the identity profile unique in the MSAS instance.
Directory Info	Host and port of the server hosting the directory configured in the profile.

Perform the following actions for an identity store profile.

Action	Description
Add	Add identity store profiles to the MSAS instance.

Action	Description
Edit	Edit an existing identity store profile. Select the profile name in the table and click <b>Edit</b> to display the Identity Store Profile page where you can edit the fields as desired.
Remove	Remove the identity store profile from the MSAS instance. Select the profile name in the table and click <b>Remove</b> .
Set as default	Select the profile to use as the default. When set, all authentication and user profile queries will occur against the default identity store profile. Select the profile name in the table and click <b>Set as default</b> .

Use the Identity Store Profile page to define the identity store for the MSAS instance. You access this page using the **Add** or **Edit** actions on the Identity Store Profiles tab of the MSAS Instance Configuration page. It includes the following sections:

- [Directory Information](#)
- [User](#)
- [Group](#)

Element	Description
Name	Name of the identity store profile.
Description	General description for the profile.

### Directory Information

The **Directory Information** section enables you to set the directory type, hostname, and credential details for the identity store, and to test the connection to the identity store.

Element	Description
Directory Type	Type of directory. Supported types are: <ul style="list-style-type: none"> <li>■ Active Directory</li> <li>■ OID (Oracle Internet Directory)</li> <li>■ ODSEE (Oracle Directory Server Enterprise Edition)</li> <li>■ OUD (Oracle Unified Directory)</li> <li>■ WLS_LDAP (Embedded LDAP in WebLogic Server)</li> </ul>
Host Name	Host name of the server running the selected directory.
Port	Port used to access the selected directory.
Bind DN	DistinguishedName (DN) of the user to connect to the LDAP Directory.
Bind Password	Password to use to connect to the selected directory.
Confirm Password	Reenter the password to use to connect to the selected directory.
Base DN	LDAP Searchbase under which all users and groups are located in the LDAP directory. For example, <code>cn=ldap, dn=example, dc=com</code> .
SSL	If connecting using an SSL port, select this control to enable SSL.
Trust Store Type	Type of the trust store. For Mobile Security Access Server, the supported trust store is <code>KSS</code> . This field is read only.

Element	Description
Trust Store Path	Fully qualified path to the trust store. By default, this path is <code>kss://msas_id/ssltruststore</code> , where <code>msas_id</code> is the MSAS ID of the instance with which this identity store profile is associated. This field is read only.
Test Connection	After completing all the required fields, click <b>Test Connection</b> to test the connection to the directory.

### User

The **User** Searchbase section enables you to set the user names, base DN, and object classes for the identity store profile.

Element	Description
Base DN	Container under which the users exist. For example, <code>cn=users, dn=example, dc=com</code> .
Login ID Attribute	Attribute that contains the users login ID. Typically this is <code>uid</code> or <code>mail</code> attribute in LDAP. In Active directory this refers to the <code>UserPrincipalName</code> .
Object Classes	Fully qualified names of the schema classes used to represent users. By default it is set to the standard LDAP objectclass <code>inetOrgPerson</code> .
Add	Click <b>Add</b> to add an object class and enter the value in the Object Class Name field.
Remove	Select an object class name from the table and click <b>Remove</b> to remove the name from the profile.

### Group

The **Group** section enables you to set the group names, base DN, and object classes for the identity store profile.

Element	Description
Base DN	Searchbase for the group entries in the LDAP directory. For example, <code>cn=group, dn=example, dc=com</code> .
Group Name Attribute	Attribute that uniquely identifies the name of the group or role. For example, <code>cn</code> .
Object Classes	Fully qualified names of the schema classes used to represent groups. By default, this refers to the LDAP standard objectclass of <code>groupofuniqueNames</code> . In Active Directory this is <code>group</code> .
Add	Click <b>Add</b> to add an object class and enter the value in the Object Class Name field.
Remove	Select an object class name from the table and click <b>Remove</b> to remove the name from the profile.

### Authentication

The **Authentication** tab of the MSAS Instance Configuration page provides the ability to define the trusted issuers and clients for the MSAS instance. It includes the following sections:

- [SAML Trust](#)
- [JWT Trust](#)

### SAML Trust

The **SAML Trust** section enables you to define SAML trusted issuers and a list of trusted distinguished names (DNs) for SAML signing certificates for trusted servers and clients. You can also define token attribute rules, which allow you to define additional security constraints for the trusted STS server and for the trusted SAML client.

The list of SAML issuers that you define on this page becomes the default list that is applicable to all applications in this MSAS instance.

This configuration option is optional; it is available for users that require more fine-grained control to associate each issuer with a list of one or more signing certificates. If you do not define a list of DN for a trusted issuer, then MSAS allows signing by any certificate, as long as that certificate is trusted by the certificates present in the MSAS keystore.

Use the **Trusted STS** table to define a trusted DN list for trusted STS servers. Use this list for SAML HOK and SAML bearer.

Use the **Trusted Clients** table to define a trusted DN list for trusted clients. Use this list for SAML sender vouches.

Element	Description
Issuer Name	Name of the trusted issuer. The default value for the predefined SAML client policies is <code>www.oracle.com</code> .
Issuer DN	Trusted DN for the trusted issuer. Select the row containing the issuer for which you want to define the DN list and enter it here. Use a string that conforms to RFC 2253.  For example, the trusted DN for the trusted issuer <code>www.oracle.com</code> is <code>CN=weblogic, OU=Oracle Test Encryption Purposes Only, O=Oracle, C=US</code> .
Token Rules	Place your mouse over the icon to view the token rules configured for the DN in a pop-up window.

Perform the following actions to add or delete SAML trusted issuers and DN, and to configure token rules.

Action	Description
View	Select the <b>Columns</b> and <b>Reorder Columns...</b> options in this menu to specify the columns that are visible and their order.
Add	Add a trusted issuer. Click <b>Add</b> to add a new row to the table and enter the trusted issuer and associated DN in the <b>Issuer Name</b> and <b>Issuer DN</b> fields.
Delete	Delete a trusted issuer. Select the row containing the issuer to be deleted and click <b>Delete</b> .
Configure Token Rule	Specify a token attribute rule for a trusted DN. Each rule has two parts: a name ID and an attributes part for user attributes that a DN for a signing certificate can assert. The name ID and the attribute can contain a filter with multiple value patterns.  Select the row containing the DN for which you want to configure the rule and click <b>Configure Token Rule</b> . In the Token Rule window, add new rules, delete or edit existing rules as required.

## JWT Trust

The **JWT Trust** section enables you to define JWT trusted issuers and a list of trusted distinguished names (DNs) for JWT signing certificates. You can also define token attribute rules, which allow you to define additional security constraints for the trusted issuer.

The list of trusted issuers that you define on this page becomes the default list that is applicable to all applications in this MSAS instance.

This configuration option is optional; it is available for users that require more fine-grained control to associate each issuer with a list of one or more signing certificates. If you do not define a list of DN for a trusted issuer, then MSAS allows signing by any certificate, as long as that certificate is trusted by the certificates present in the MSAS keystore.

Use the **Trusted Issuer** table to define a trusted DN list for trusted JWT Issuers.

Element	Description
Issuer Name	Name of the trusted issuer. The default value for the predefined JWT client policies is <code>www.oracle.com</code> .
Issuer DN	Trusted DN for the trusted issuer. Select the row containing the issuer for which you want to define the DN list and enter it here. Use a string that conforms to RFC 2253.  For example, the trusted DN for the trusted issuer <code>www.oracle.com</code> is <code>CN=weblogic, OU=Orakey Test Encryption Purposes Only, O=Oracle, C=US</code> .
Token Rules	Place your mouse over the icon to view the token rules configured for the DN in a pop-up window.

Perform the following actions to add or delete JWT trusted issuers and DN, and to configure token rules.

Action	Description
View	Select the <b>Columns</b> and <b>Reorder Columns...</b> options in this menu to specify the columns that are visible and their order.
Add	Add a trusted issuer. Click <b>Add</b> to add a new row to the table and enter the trusted issuer and associated DN in the <b>Issuer Name</b> and <b>Issuer DN</b> fields.
Delete	Delete a trusted issuer. Select the row containing the issuer to be deleted and click <b>Delete</b> .
Configure Token Rule	Specify a token attribute rule for a trusted DN. Each rule has two parts: a name ID and an attributes part for user attributes that a DN for a signing certificate can assert. The name ID and the attribute can contain a filter with multiple value patterns.  Select the row containing the DN for which you want to configure the rule and click <b>Configure Token Rule</b> . In the Token Rule window, add new rules, delete or edit existing rules as required.

## Message Security

The **Message Security** tab of the MSAS Instance Configuration page provides the ability to configure the message protection settings required for the environment. It includes the following sections:

- [Key Store](#)
- [Security Settings](#)



## Key Store

The **Keystore** section enables you to select the signature and encryption aliases for the default KSS keystore.

Element	Description
Key Store	Keystore to be used with the MSAS instance. For Mobile Security Access Server, the supported keystore is KSS. You cannot change the keystore type.
Path	The KSS URI that points to the location of the keystore in KSS. By default, this path is <code>kss://msas_id/keystore</code> where <code>msas_id</code> is the ID of the MSAS instance with which the keystore is associated and <code>keystore</code> is the stripeID. This field is read only.
Sign Alias	Alias of the key used to sign the messages. This value must match the value in the keystore.  Press <b>Click to Add</b> to add a signature alias using the Private Key for Signing window.
Generate Keypair	Click to generate a keypair to use for the signature key.
Alias	Alias of the keypair entry.
Distinguished Name	Distinguished name of the certificate wrapping the keypair.
Algorithm	Symmetric key algorithm. The default is RSA.
Key Size	RSA key size. The default is 1024 bytes.
Generate Keypair	Use this action to generate the keypair using the information provided. The keypair is added to the Pick a key table.
Import from Keystore	Click to import a signature keypair and alias from the keystore.
Choose File	Use this action to select a keypair to be imported from the file system.
Keystore Password	Password for the keystore from which the signature key will be imported.
Alias	Alias of the keypair to be imported.
Alias Password	Alias password for the keypair to be imported.
Import	Use this action to import the selected keypair into the keystore. It is added to the Pick a key table.
Pick a key	List of the signature alias keys available. Select the alias from the table and click OK.
Encrypt Alias	Alias of the key used to encrypt the messages. This value must match the value in the keystore.
Generate Keypair	Click to generate a keypair to use for the encryption key.
Alias	Alias of the keypair entry.
Distinguished Name	Distinguished name of the certificate wrapping the keypair.
Algorithm	Symmetric key algorithm. The default is RSA.
Key Size	RSA key size. The default is 1024 bytes.
Generate Keypair	Use this action to generate the keypair using the information provided. The keypair is added to the Pick a key table.
Import from Keystore	Click to import an encryption keypair and alias from the keystore.

Element	Description
Choose File	Use this action to select a keypair to be imported from the file system.
Keystore Password	Password for the keystore from which the keypair key will be imported.
Alias	Alias of the keypair to be imported.
Alias Password	Alias password for the keypair to be imported.
Import	Use this action to import the selected keypair into the keystore. It is added to the Pick a key table.
Pick a key	List of the encryption keys available. Select the alias from the table and click <b>OK</b> .

### Security Settings

The **Security Settings** section enables you to tune security policy enforcement by adjusting the default message timestamp skews between system clocks. You can also set the message expiration time.

Element	Description
Clock Skew	<p>Tolerance of time differences, in seconds, between client and server machines. For example, when timestamps are sent across in a message to a service that follows a different time zone, this property allows for a tolerance. The default value is 360,000 milliseconds (6 minutes). Enter a new value in the field or click the up/down arrows to increase or decrease the default value.]</p> <p>You should configure this property to:</p> <ul style="list-style-type: none"> <li>■ Increase the clock skew when the client and service are running on different systems and their system clocks are not in-sync, which could result in the service rejecting messages from the client, with an error indicating the timestamp validation failed. Increasing clock skew accounts for the difference in clocks between the client and the service.</li> <li>■ Decrease the clock skew if you want to narrow the window in which the service is willing to accept messages from clients to avoid replay attacks.</li> </ul>
Client Clock Skew	<p>Tolerance of time, in seconds, that is used to calculate the <code>NotBefore</code> and <code>NotOnOrAfter</code> conditions for SAML or JWT token generation. Together, these conditions define the lower and upper boundaries to limit the validity of the token. The default is 0. Enter a new value in the field or click the up/down arrows to increase or decrease the default value.]</p>
Message Expiration Time	<p>Duration of time, in seconds, before a message expires after its creation. This property is used in cases where a timestamp is sent across in the token to verify if the timestamp has expired or not. The default value is 300,000 milliseconds (5 minutes). Enter a new value in the field or click the up/down arrows to increase or decrease the default value.</p> <p>You should configure this property to:</p> <ul style="list-style-type: none"> <li>■ Increase the message expiration time to ensure that the message is valid for a longer duration than the default time.</li> <li>■ Decrease the message expiration time to ensure that message is valid for a shorter duration than the default time.</li> </ul>

### Policy Access

The **Policy Access** tab of the MSAS Instance Configuration page provides the ability to configure the cache refresh time. It includes the following sections:

- [Cache Management](#)

### Cache Management

The **Cache Management** section provides the ability to configure the cache refresh time.

Element	Description
Cache Refresh Time	Number of milliseconds to wait between cache refreshes. The default is 86,400,000 milliseconds (24 hours). Enter a new value in the field or click the up/down arrows to increase or decrease the default value.
Failure Retry Delay	Reserved for future use.
User Record Delay	Reserved for future use.
Failure Retry Count	Reserved for future use.
Missing Documents Retry Delay	Reserved for future use.
Initial Cache Refresh	Reserved for future use.

### Authentication Endpoints

The **Authentication Endpoints** tab of the MSAS Instance Configuration page provides the ability to configure the KINIT/PKINIT and OAUTH2 endpoints, and the Crypto service. It includes the following sections:

- [KINIT & PKINIT](#)
- [OAuth2 Confidential Client](#)
- [OAuth2 Mobile Client](#)
- [Crypto Service](#)

#### KINIT & PKINIT

The KINIT and PKINIT section of the Authentication Endpoints tab enables you to configure the properties of the Kerberos `krb5.conf` file, which is required for Kerberos Password Authentication (KINIT) and Public Key Cryptography for Initial Authentication (PKINIT) to work. The `krb5.conf` file contains Kerberos configuration information, including the locations of KDCs and administration daemons for the Kerberos realms of interest, the default realm, default domain, default encryption types, and for Kerberos applications, and mappings of host names onto Kerberos realms. The values entered here will be stored in the MSAS repository.

It includes the following sections:

- [Realms](#)
- [Domains](#)
- [Encryption](#)
- [Logging](#)
- [PKINIT Trust anchors](#)

**Realms** The KINIT & PKINIT **Realms** section provides the ability to add, edit, and delete Kerberos realms. You must specify one realm as the default realm.

The Realms table displays a list of the realms defined in the MSAS instance.

Element	Description
Realm Name	Name of the Kerberos realm.
Default	Flag indicating the default realm.

Perform the following actions for Kerberos realms.

Action	Description
Add	Add a Kerberos realm to the MSAS instance. Click <b>Add</b> to display the Realm page. In the Realm page, complete the fields, click <b>OK</b> , then click <b>Apply</b> .
Name	Realm names can consist of any ASCII string. The realm name must match the REALM name defined during the Active Directory setup.
KDC host	Host for the KDC server running the realm specified in the <b>Name</b> field.
KDC port	Optional port of the KDC server running the realm specified in the <b>Name</b> field.
Default Domain	Enter the name of the default domain in the field or select a default domain from the menu.
Edit	Edit an existing Kerberos realm. Select the realm name in the table and click <b>Edit</b> to display the Realm page where you can edit the fields as desired.
Remove	Delete the Kerberos realm from the MSAS instance. Select the realm name in the table and click <b>Remove</b> .
Set as default	Select the realm to use as the default. Select the realm name in the table and click <b>Set as default</b> .

**Domains** The KINIT & PKINIT **Domains** section provides the ability to add and delete DNS domains in the MSAS instance.

The Domains table displays a list of the domains defined in the realm.

Element	Description
Domain	DNS domain name
Realm	Kerberos realm associated with the domain.



Perform the following actions for a domain.

Action	Description
Add	Add a DNS domain to the MSAS instance. Click <b>Add</b> and enter the name of the domain in the Domain field. Typically, the domain name is in lower case, for example <code>example.com</code> . Select the associated Realm from the menu, then click <b>Apply</b> .
Remove	Remove the domain from the MSAS instance. Select the domain name in the table and click <b>Remove</b> , then click <b>Apply</b> .



**Encryption** The KINIT & PKINIT **Encryption** section provides the ability to specify the type of Kerberos encryption the client must use when making requests to the KDC.

Element	Description
default TKT encytypes	Supported list of session key encryption types that the client should request when making an AS-REQ, in order of preference from highest to lowest. Select the encryption type from the menu.
default TGS encytypes	Supported list of session key encryption types that the client should request when making a TGS-REQ, in order of preference from highest to lowest. Select the encryption type from the menu.

**Logging** The KINIT & PKINIT Logging section provides the ability to configure logging location for the Kerberos and KCM messages.



Element	Description
krb5	Select the log location to be used for the Kerberos configuration. Supported options are: <ul style="list-style-type: none"> <li>▪ <b>STDERR</b>—Log messages using the standard error stream.</li> <li>▪ <b>File</b>—Log messages to a specified file. Select <b>File</b>, then enter the log file location in the empty field.</li> </ul>
KCM	Select the log location to be used for the Kerberos Cache Manager (KCM). Supported options are: <ul style="list-style-type: none"> <li>▪ <b>STDERR</b> - Log messages using the standard error stream.</li> <li>▪ <b>File</b>—Log messages to a specified file. Select <b>File</b>, then enter the log file location in the empty field.</li> </ul>
Edit Policy	Use this action to open the URL Policy Configuration page for the KINIT endpoint. It displays the internal policies attached to the on-request and on-response subjects. You can use this page to view details about the endpoint and attached policies.
On-Request	The Http Kerberos password Authentication Service Policy is attached On-Request. This internal policy enables the Kerberos password authentication.  Select the policy name, or click the <b>Options</b> menu icon  then <b>Edit</b> , to view the policy details and configure policy overrides.  Optionally, click the <b>Overrides</b> tab to configure property overrides or to add a <code>keystore.sig.csf.key</code> to the keystore. To add a key, press <b>Click to add</b> to generate a keypair, or to import a key from a keystore. Then pick the key from the table and click <b>OK</b> .  <b>Note:</b> To ensure proper authentication on this endpoint, you should not delete the default policy attachments, or attach additional policies.
On-Response	The Http Session Token Issue Policy is attached On-Response. This policy issues a session token with the authenticated user ID to the client.  Select the policy name, or click the <b>Options</b> menu icon  then <b>Edit</b> , to view the policy details and configure policy overrides.  Optionally, click the <b>Overrides</b> tab to configure property overrides or to add a <code>keystore.sig.csf.key</code> or <code>keystore.enc.csf.key</code> to the keystore. To add keys, press <b>Click to add</b> to generate a keypair, or import a key from a keystore. Then pick the key from the table and click <b>OK</b> .  <b>Note:</b> To ensure proper authentication on this endpoint, you should not delete the default policy attachments, or attach additional policies.

**PKINIT Trust anchors** Use the KINIT & PKINIT **PKINIT Trust anchors** section to enable the use of trust anchors for PKINIT authentication. PKINIT trust anchors are stored in the keystore.

Element	Description
Enable	Select this action to enable the use of PKINIT anchors to trust the authority issuing the KDC certificate, then select the trusted certificate from the table, or import a certificate into the truststore. The certificate you select must be the first certificate in the certificate chain. MSAS will automatically fetch the complete chain using the selected certificate as the starting point.
Truststore Location	Specifies the location of trusted anchor (root) certificates which the client trusts to sign KDC certificates. Only KSS keystores are supported. This field is read only.
Choose File	Use this action to select a certificate to be imported from the file system.
Alias	Alias of the PKINIT trust certificate to be imported.
Import	Use this action to import the selected certificate into the truststore. It is added to the trusted certificate table.
Select	Select the certificate to set the alias for the PKINIT trust anchor.
X	To delete a certificate, click X in the row of the certificate to be deleted. In the Delete Key window, click <b>Yes</b> to confirm the deletion.
Edit Policy	Use this action to open the URL Policy Configuration page for the PKINIT endpoint. It displays the internal policies attached to the on-request and on-response endpoints. You can use this page to view details about the endpoint and attached policies.
On-Request	<p>The Http Kerberos PKI Authentication Service Policy is attached On-Request. This internal policy enables Kerberos PKI authentication.</p> <p>Select the policy name, or click the <b>Options</b> menu icon  then <b>Edit</b>, to view the policy details and configure policy overrides.</p> <p>Optionally, click the <b>Overrides</b> tab to configure property overrides or to add a <code>keystore.sig.csf.key</code> to the keystore for signing the outbound message. To add a key, press <b>Click to add</b> to generate a keypair, or import a key from a JKS keystore. Then pick the key from the table and click <b>OK</b>.</p> <p><b>Note:</b> To ensure proper authentication on this endpoint, you should not delete the default policy attachments, or attach additional policies.</p>
On-Response	<p>The Http Session Token Issue Policy is attached On-Response. This policy issues a session token with the authenticated user ID to the client.</p> <p>Select the policy name, or click the <b>Options</b> menu icon  then <b>Edit</b>, to view the policy details and configure policy overrides.</p> <p>Optionally, click the <b>Overrides</b> tab to configure property overrides or to add a <code>keystore.sig.csf.key</code> or <code>keystore.enc.csf.key</code> to the keystore for signing the outbound message. To add keys, press <b>Click to add</b> to generate a keypair, or import a key from a JKS keystore. Then pick the key from the table and click <b>OK</b>.</p> <p><b>Note:</b> To ensure proper authentication on this endpoint, you should not delete the default policy attachments, or attach additional policies.</p>


### OAuth2 Confidential Client


Use the OAuth2 Confidential Client section of the Authentication Endpoints tab to specify the OAuth2 endpoint and specify the client ID and secret in the Credential Store Framework (CSF) for the OAuth2 confidential client.

Element	Description
Endpoint	OAuth Service Profile Endpoint to which the MSAS server creates JWT User Token and OAM Tokens for OAuth2 Confidential Client Authentication flow.
Edit Policy	Use this action to open the URL Policy Configuration page for the endpoint. It displays the internal policies attached to the on-request and on-response subjects. You can use this page to view details about the endpoint and attached policies.
On-Request	<p>The Http OAuth2 Confidential Client Over SSL Policy is attached On-Request. This internal policy performs OAuth2 Confidential Client Authentication and creates OAuth and OAM tokens.</p> <p>Select the policy name, or click the <b>Options</b> menu icon  then <b>Edit</b>, to view the policy details and configure policy overrides.</p> <p>Click the <b>Overrides</b> tab and enter the OAuth2 client CSF key in the <b>Value</b> field.</p> <p><b>Note:</b> To ensure proper authentication on this endpoint, you should not delete the default policy attachments, or attach additional policies.</p>
On-Response	<p>The Http Session Token Issue Policy is attached On-Response. This policy issues a session token with the authenticated user ID to the client.</p> <p>Select the policy name, or click the <b>Options</b> menu icon  then <b>Edit</b>, to view the policy details and configure policy overrides.</p> <p>Optionally, click the <b>Overrides</b> tab to configure property overrides or to add a <code>keystore.sig.csf.key</code> or <code>keystore.enc.csf.key</code> to the keystore for signing the outbound message. To add keys, press <b>Click to add</b> to generate a keypair, or import a key from a JKS keystore. Then pick the key from the table and click <b>OK</b>.</p> <p><b>Note:</b> To ensure proper authentication on this endpoint, you should not delete the default policy attachments, or attach additional policies.</p>

### OAuth2 Mobile Client


Use the OAuth2 Mobile Client section of the Authentication Endpoints tab to specify the OAuth2 endpoint to which the client can connect, and specify the mobile client ID in the CSF for the OAuth2 Mobile Client flow.

Element	Description
Endpoint	OAuth Service Profile Endpoint to which the MSAS Server registers a container mobile application and can create JWT User Token & OAM Tokens for OAuth2 Mobile Client Authentication flow.
Edit Policy	Use this action to open the URL Policy Configuration page for the endpoint. It displays the internal policies attached to the on-request and on-response subjects. You can use this page to view details about the endpoint and attached policies.
On-Request	<p>The Http OAMMS Mobile Client Token Over SSL Service Policy. is attached On-Request. This internal policy performs OAMMS Mobile Client Authentication and creates OAUTH and OAM tokens.</p> <p>Select the policy name, or click the <b>Options</b> menu icon  then <b>Edit</b>, to view the policy details and configure policy overrides.</p> <p>Click the <b>Overrides</b> tab and enter the mobile client ID in the <b>Value</b> field.</p> <p><b>Note:</b> To ensure proper authentication on this endpoint, you should not delete the default policy attachments, or attach additional policies.</p>

Element	Description
On-Response	<p>The Http Session Token Issue Policy is attached On-Response. This policy issues a session token with the authenticated user ID to the client.</p> <p>Select the policy name, or click the <b>Options</b> menu icon  then <b>Edit</b>, to view the policy details and configure policy overrides.</p> <p>Optionally, click the <b>Overrides</b> tab to configure property overrides or to add a <code>keystore.sig.csf.key</code> or <code>keystore.enc.csf.key</code> to the keystore for signing the outbound message. To add keys, press <b>Click to add</b> to generate a keypair, or import a key from a JKS keystore. Then pick the key from the table and click <b>OK</b>.</p> <p><b>Note:</b> To ensure proper authentication on this endpoint, you should not delete the default policy attachments, or attach additional policies.</p>

### Crypto Service

Use the Crypto service section of the Authentication Endpoints tab to configure the Crypto Service with archive key aliases.

Element	Description
Key Rollover Aliases	Alias for the keystore used by the keystore rollover feature for the archived keys. These key aliases are maintained as an ordered list. The first alias is the oldest and second is next and so on.
Edit Policy	Use this action to open the URL Policy Configuration page for the endpoint. It displays the internal policies attached to the on-request and on-response subjects. You can use this page to view details about the endpoint and attached policies.
On-Request	<p>Two policies are attached by default:</p> <ul style="list-style-type: none"> <li>The HTTP Session Token Verify Policy verifies the session token, including the timestamp and signature, decrypts the encrypted data, and asserts the identity using the user ID from session token. The request is rejected if the verification fails.</li> </ul> <p>Select the policy name, or click the <b>Options</b> menu icon  then <b>Edit</b>, to view the policy details and configure policy overrides.</p> <p>Optionally, click the <b>Overrides</b> tab to configure property overrides or to add a <code>keystore.sig.csf.key</code> or <code>keystore.enc.csf.key</code> to the keystore for signing the outbound message. To add keys, press <b>Click to add</b> to generate a keypair, or import a key from a JKS keystore. Then pick the key from the table and click <b>OK</b>.</p> <ul style="list-style-type: none"> <li>The HTTP Action Security Policy enables the Action Security Policy that performs Server Key Encryption Key (SKEK) encryption and decryption.</li> </ul> <p><b>Note:</b> To ensure proper authentication on this endpoint, you should not delete the default policy attachments, or attach additional policies.</p>
On-Response	Click the <b>Options</b> menu icon to attach policies or templates if desired. There are no policies attached by default.

### System Settings

The **System Settings** tab of the MSAS Instance Configuration page provides the ability to configure the system settings for the instance. It includes the following sections:

- [Outbound Message Settings](#)
- [Proxy Server Settings](#)
- [Server Settings](#)



- [SSL Settings](#)
- [Log Configuration](#)

### Outbound Message Settings

The **Outbound Message Settings** section enables you to configure the client connection to back-end services.

Element	Description
Total Connections in pool	Maximum number of connections in a pool that a client can handle. The default is 512.
Maximum Connections per host	Maximum number of connections in a pool, per host, that a client can handle. The default is 25.
Connection Timeout	Maximum time in milliseconds a client can wait when connecting to a back-end host. The default is 20,000 ms.
Idle Connection pool Timeout	Maximum time in milliseconds a client will keep idle connections in the pool. The default is 180,000 ms (3 minutes).
Request Timeout	Maximum time in milliseconds a client can wait for a response. The default is 60,000 ms (1 minute).

### Proxy Server Settings

The **Proxy Server Settings** section enables you to configure the proxy server used for outbound calls to the internet through MSAS for back-end applications and services.

Element	Description
Name	Name of proxy server to uniquely identify it. This field is optional.
Host Name	Host name of proxy server.
Port	Port number of proxy server.
User Name	User ID to connect to the proxy server. <b>Note:</b> The User Name and Password is required only if the proxy server requires authentication.
Password	Password corresponding to the User ID to connect to the proxy server.
Hostnames without proxy	List of hosts that will not use the proxy server. It supports the asterisk * wildcard, but only as a suffix and prefix. By default, this field contains the value localhost, 127.0.0.1.

### Server Settings

The **Server Settings** section enables you to specify general settings for the MSAS server.

Element	Description
Load Balancer URL	Front ending Load Balancer non-SSL URL, for example <code>http://lbr.example.org:80</code> .
Load Balancer SSL URL	Front ending Load Balancer SSL URL, for example <code>https://lbr.example.org:443</code> .

Element	Description
Service Principal Name	This property maps a URL with Service Principal Name. Service Principal Name is required for NTLM and SPNEGO.  Click <b>Add</b> to add a Service Principal Name and URL. To remove a Service Principal Name and URL, select the table row and click <b>Remove</b> .
URL	Service Principal Name URL It supports the asterisk * wildcard anywhere in the URL, for example, <code>http*://example.host*80/*</code> or <code>*.example.org</code> .
Service Principal Name	Service Principal Name in the form of <code>SPN_SERVICECLASS/SPN_HOSTNAME</code> .

### SSL Settings

The **SSL Settings** section enables you to add certificates and keys for the outbound and inbound SSL HTTPS connections.

Element	Description
SSL TrustStore Location	Read only field that specifies the location of SSL trust store. Only KSS keystore type is supported so the value must be a KSS URI.
Server Certificate	To import a certificate, select <b>Click to import</b> to open the Server Certificate page where you can import a certificate to the truststore. <b>Note:</b> Only Base64-encoded certificates are supported.
Choose File	Use this action to select the certificate to be imported from the file system.
Alias	Truststore alias.
Certificate Type	Type of certificate to be imported. Supported options are: <ul style="list-style-type: none"> <li>Trusted Certificate</li> </ul>
Import	Use this option to import the selected certificate into the truststore. It is added to the certificate table.
X	To delete a certificate, click <b>X</b> in the row of the certificate to be deleted. Click <b>Yes</b> to confirm the deletion.
SSL Keystore Location	Read only field that specifies the location of SSL keystore. The SSL keystore is used for inbound SSL connections to MSAS and as the MSAS identity keystore. Only KSS keystore type is supported so the value must be a KSS URI.
Private Key	To add a private key, click <b>Click to add</b> to open the Private Key page where you can generate a keypair or import a key from a JKS keystore.
Generate Keypair	Use this option to generate a private keypair for the MSAS SSL identity key.
Alias	Alias of the keypair entry.
Distinguished Name	Distinguished name of the certificate wrapping the keypair.
Algorithm	Symmetric key algorithm. The default is RSA.
Key Size	RSA key size. The default is 1024 bytes.
Generate Keypair	Generate the keypair using the information provided. The key is added to the keypair table.
Import from Keystore	Click to import the Java keystore file into the keystore service.

Element	Description
Choose File	Use this option to select a Java keystore file.
Keystore Password	Password for the JKS keystore from which the keypair will be imported.
Alias	Alias of the keypair to be imported.
Alias Password	Alias password for the keypair to be imported.
Import	Import the selected keypair into the KSS keystore. It is added to the keypair table.
X	To delete a keypair, click X in the row of the keypair to be deleted. Click <b>Yes</b> to confirm the deletion.

### Log Configuration

The **Log Configuration** section enables you to configure run-time logging levels for MSAS sub-components. The configuration specified here applies to the logical MSAS instance, and is used by all physical MSAS instances to which the logical instance is bound.

Element	Description
Logger Name	Name of the logger. The root logger is populated by default. All loggers for which the level is not explicitly configured will inherit from the root logger.
Logging Level (Java Level)	<p>Select a logging level from the menu. Valid values are:</p> <ul style="list-style-type: none"> <li>▪ SEVERE—A serious problem that requires immediate attention from the administrator and is not caused by a bug in the product.</li> <li>▪ WARNING—A potential problem that should be reviewed by the administrator.</li> <li>▪ INFO—A major lifecycle event such as the activation or deactivation of a primary sub-component or feature.</li> <li>▪ CONFIG—Configuration information to assist in debugging problems that may be associated with particular configurations.</li> <li>▪ FINE— Detailed tracing messages that can cause a small performance impact. You can enable this level occasionally on a production environment to debug problems.</li> <li>▪ FINER—Fairly detailed tracing messages that can cause a high performance impact. This level should <i>not</i> be enabled on a production environment, except on special situations to debug problems.</li> <li>▪ FINEST—Highly detailed tracing messages that can cause a very high performance impact. This level should <i>not</i> be enabled in a production environment. It is intended to be used to debug the product on a test or development environment.</li> </ul>

Perform the following actions for log level configuration.

<b>Action</b>	<b>Description</b>
Add	<p>Add an MSAS logger to the MSAS instance. Click <b>Add</b> and enter the name of the logger in the <b>Logger Name</b> field. Available loggers are:</p> <ul style="list-style-type: none"><li>■ <code>oracle.idm.gateway.grs</code>—MSAS runtime server</li><li>■ <code>oracle.idm.gateway.gmsclient</code>—MSAS management client</li><li>■ <code>oracle.idm.gateway.snapshot</code>—MSAS security artifacts snapshot manager</li><li>■ <code>oracle.idm.gateway.common</code>—MSAS common libraries</li><li>■ <code>oracle.wsm</code>—Oracle Web Services Manager runtime libraries</li><li>■ <code>oracle.security.jps</code>—Oracle Platform Security Service (OPSS) libraries</li><li>■ <code>com.sun.jersey</code>—Jersey</li></ul> <p>Then select the desired logging level from the menu and click <b>Apply</b> at the top of the page.</p>
Remove	<p>Remove the logger from the MSAS instance. Select the logger name in the table and click <b>Remove</b>.</p>

**Related Topics**

"Configuring a Mobile Security Access Server Instance" in *Administering Oracle Mobile Security Access Server*

# 10

## Access Policies Help

This chapter documents the Access Policies page in the Mobile Security Access Server console. To open this page from the Mobile Security Launch Pad, select **Access Policies** in the Mobile Security Access Server section.

This chapter contains the following topics:

- [Access Policies Page](#)
- [Policy Details Page](#)
- [Policy Version History Page](#)
- [Assertion Templates Page](#)
- [Assertion Templates Details Page](#)

### 10.1 Access Policies Page

Use the Access Policies page to:

- Search for policies.
- Navigate to a page where you can create a policy.
- Navigate to a page where you can view an existing policy.
- Navigate to a page where you can make changes to a policy.
- Import or export one or more policies.

Click **Assertion Templates** to display the Assertion Templates page.

The Access Policies page is arranged in the following sections:

- [Search](#)
- [Policies Table](#)

#### Search

Use the **Search** section of the Access Policies page to perform an advanced search for policies in the repository. The results that are returned are the policies that meet the conditions specified in the **Name** and **Category** fields

Element	Description
Name	<p>Enter a policy name or part of a name and select the operator to use to refine the search. Valid options are:</p> <ul style="list-style-type: none"> <li>■ <b>Starts with</b>—Returns all policies that start with the value specified.</li> <li>■ <b>Ends with</b>—Returns all policies that end with the value specified.</li> <li>■ <b>Equals</b>—Returns all policies that exactly match the value specified.</li> <li>■ <b>Contains</b>—Returns all policies that contain the value specified.</li> </ul> <p>You can use percent % as a wildcard, any place in the name. Asterisk * is not recognized as a wildcard and is treated as plain text. Searches are case-insensitive.</p>
Category	Select the policy category for which you want to search. Valid values include: All, Management, and Security.
Search	Perform the search using the specified parameters.
Reset	Clear the specified search parameters.

### Policies Table

The **Policies** table displays the policies in the repository that match the criteria specified in the Search fields. The following information is provided for each policy.

Element	Description
Name	Unique identifier for the policy. The policy name includes the directory in which the policy is located. By default, all predefined policies are located in the <code>oracle</code> directory, and, therefore, <code>oracle/</code> is prefixed to the beginning of each policy name.
Category	Category of the policy. A policy may belong to only one category, and may only contain assertions that belong to the selected category.
Status	Field that specifies whether the policy is enabled or disabled.
Description	Brief description of the policy behavior.

Perform the following actions to manage access policies.

Action	Description
Actions	Drop-down menu that provides an alternate method to perform the available actions.
View	<p>Use this menu as follows:</p> <ul style="list-style-type: none"> <li>■ Use the <b>Columns</b> and <b>Reorder Columns...</b> options to specify the columns that are visible and their order.</li> <li>■ Use the <b>Detach</b> option to detach the policies table from the console pane and expand to the full width of the console window. Use the <b>Attach</b> option to reattach the window to the console pane. Alternatively, you can use the <b>Detach</b> icon to attach and detach the table. To reattach, you can also click the Close icon.</li> </ul>
Create	<p>Create a new policy. Click <b>Create</b> to display the Policy Details page, which you can use to create the new policy.</p> <p><b>Note:</b> You can create policies in the Security and Management categories only.</p>

Action	Description
Create Like	<p>Create a new policy that is based on an existing policy. Select a policy from the Policies table and click <b>Create Like</b> to display the Policy Details page.</p> <p><b>Note:</b> You can copy and create new policies in the Security and Management categories only.</p>
Open	Use this action to display the Policy Details page where you can review and edit the details of a policy.
Delete	Delete a policy. Select a policy from the Policies table, and click <b>Delete</b> .
Export	<p>Export a zip archive containing one or more policies to your local directory. You can use this feature in combination with <b>Import</b> to move one or more policies between different repositories.</p> <p>Select one or more policies from the Policies table and click <b>Export</b> to save the zip archive to your file system.</p> <p>The directory structure for each policy is maintained in the archive file using the following structure:</p> <pre>META-INF/policies/directory/policyname</pre>
Import	<p>Import a zip archive containing one or more policies. You can use this feature in combination with <b>Export</b> to move one or more policies between different repositories. Click <b>Import</b>, then click <b>Choose File</b> to locate the zip archive in your local directory that contains the policies to be imported, and click <b>Import</b>.</p> <p>An Information window is displayed listing the policies that were imported. Click <b>OK</b> to close the window.</p> <p>The imported policies are added to the list of policies in the Policies table.</p> <p><b>Notes:</b></p> <p>The policies to be imported must use the following directory structure:</p> <pre>META-INF/policies/directory/policyname</pre> <p>If an error is encountered with one of the policies, the import process stops. For example, if there are five policies to be imported and an error is encountered in the third one, the first two will be imported but the remaining policies will not.</p>
Detach	Click the <b>Detach</b> option to detach the policies table from the console pane and expand to the full width of the console window. Use the <b>Attach</b> option or click the Close icon to reattach the window to the console pane.

### Related Topics

"Managing Policies and Assertion Templates" in *Administering Oracle Mobile Security Access Server*

## 10.2 Policy Details Page

Use the Policy Details page to:

- Create a valid new policy, from scratch, with no attributes predefined.
- Create a new policy using an existing policy as a template that you edit.
- View and edit an existing policy.

Navigate to this page using **Create**, **Create Like**, or **Open** on the Access Policies page.

The Policy Details Page is arranged in the following tabs:

- [General](#)

- [Assertions](#)

### General

The **General** tab of the Policy Details page provides general summary information about the policy, such as the policy name, category, description, if the policy is enabled or disabled, optimization settings, and so on.

Element	Description
Display name	<p>Name used to identify the policy in the user interface.</p> <p>If you clicked <b>Create Like</b> to get to this page, then <code>_Copy</code> is appended to the name of the copied policy. This is the default name assigned to the new policy, however you should rename it to make it more meaningful in your environment.</p>
Name	<p>Unique name used as an identifier for the policy. The name includes the full path to the policy. All predefined policies are in the oracle directory. Therefore, the names of all predefined policies begin with <code>oracle/</code>, for example, <code>oracle/wss_username_token_service_policy</code>.</p> <p>If you clicked <b>Create Like</b> to get to this page, then <code>_Copy</code> is appended to the name of the copied policy. This is the default name assigned to the new policy, however you should rename it to make it more meaningful in your environment.</p> <p>The valid characters for directory and policy names are:</p> <ul style="list-style-type: none"> <li>■ Uppercase and lowercase letters</li> <li>■ Numerals</li> <li>■ Currency symbol (\$)</li> <li>■ Underscore (_)</li> <li>■ Hyphen (-)</li> <li>■ Spaces</li> </ul> <p><b>Note:</b> The first character in the name cannot be a hyphen or space. In addition, you cannot prefix the name of a policy with <code>oracle_</code>. If you do so, you will receive exceptions when you try to use the policy.</p> <p>Encode as much information as possible into the name of the policy so that you can tell, at a glance, what the policy does. For example, the path location, any web services standard (such as <code>wss10</code> or <code>wss11</code>), type of authentication token if applicable, transport security, message protection, and policy type (service or client.)</p> <p><b>Note:</b> You cannot edit the name of a policy after the policy is created. To change the policy name you need to make a copy of the policy and assign it a different name.</p>
Category	<p>Category to which the policy belongs. A policy may belong to only one category, and may only contain assertions that belong to the selected category.</p> <p>Valid values include: Management and Security.</p>
Description	<p>Text that provides a brief explanation of the policy behavior. If you are creating or editing a policy, this field is optional.</p>
Enabled	<p>Flag that specifies whether the policy is enabled or not. By default, the policy is enabled. Specific assertions within a policy can be enabled or disabled on the <b>Assertions</b> tab.</p>

**Attachment Attributes** The **Attachment Attributes** section specifies the type of policy subjects to which the policy can be attached and the number of subjects to which the policy is attached, if applicable.



Element	Description
Applies To	Type of endpoints to which the policy can be attached. Valid values include: <b>All</b> and <b>Service Bindings</b> . The Service Bindings choice requires further specification with the Service Category field.
Service Category	This option applies only when <b>Applies To</b> is set to <b>Service Bindings</b> . When the policy can be attached to URLs, use the Service Category option to further specify whether the policy can be attached to services ( <b>Service Endpoint</b> ), clients ( <b>Client</b> ), or both.

**Version Information** The **Version Information** section provides details of a policy version in read-only mode.

Element	Description
Version Number	Version number of the currently active policy.
Last Updated	Timestamp of the last update to the policy.
Updated By	User who last updated the policy.
Versioning History	Click this link to view the version history of a policy in the Policy Version History page. Whenever a change to a policy is saved, a new version of the policy is automatically created and the version number is incremented.

### Assertions

The **Assertions** tab of the Policy Details page provides the ability to add or edit assertions in a policy.

If you accessed this page by selecting **Create Like** or **Open** on the Access Policies page, the **Assertions** table lists the assertions that are contained in the base policy.

If you are creating a new policy, you must add any required assertions.

The **Assertions** table provides the following information for each assertion.

Element	Description
Name	Name of the assertion. The assertion name must be unique within the policy. If you are adding the assertion to the policy using an assertion template, this name is assigned when the assertion is added.
Category	<p>Category of the assertion. You can add only assertions that are in the same category as the category selected in the <b>General</b> tab. For example, if the policy category is set to <b>Security</b>, then only Security assertions can be added to the policy.</p> <p>The Security category has subcategories: security/authentication, security/msg-protection, security/authorization, and security/logging. A security policy can contain multiple security assertions; however, there can be only one assertion of each authentication, msg-protection, or authorization subcategory in a policy. This restriction can be altered for these subcategories, however, by creating an OR group, which can have multiple security assertions from the same subcategory, but only one of which can be executed. More.</p> <p>A security policy can have multiple assertions from the security/logging subcategory.</p>
Type	Type of assertion within a category. For example, wss-10-saml-token is a type of authentication within the security/authentication category.

Element	Description
Options	Indicates whether the Enforced and/or Advertised options are set for the assertion. When one of those options is set, as described below, the icon associated with the option appears in this field.
Enforced	Flag that specifies whether the policy assertion is enabled. The default is enabled.
Advertised	Reserved for future use.

Select an assertion in the Assertions table to display information about it. The details are displayed below the table.

Perform the following actions to manage the assertions in the policy.

Action	Description
Add	Add assertions or OR Groups to the policy. Select <b>Assertion</b> , <b>OR Group</b> , or <b>Assertion to OR Group</b> from the drop-down menu.
Assertion	Add one or more assertions to the policy. The Add Assertion page is displayed with a list of all the available assertions. Use this page to search for existing assertion templates and use them to add assertions to the policy.
Add Assertion	<p>Provide search parameters in the <b>Name</b> and <b>Category</b> fields and click <b>Search</b>. The results that match the search criteria are displayed in the Search Results table.</p> <p>In the Search Results table, select the assertion or assertions to be added to the policy and click <b>Add Selected</b>. To add all the listed assertions to the policy, click <b>Add All</b>. The selected assertions are displayed in the Selected Assertion Templates table.</p> <p>In the Selected Assertion Templates table, review the selections. To remove one or more assertions from this table, click <b>Remove Selected</b> or <b>Remove All</b>. When you have confirmed the assertion selection, click <b>Add Assertion</b>.</p>
OR Group	<p>Add a subset of security policy assertions. An OR group enables you to define multiple security subcategory options, but only one of which can be executed. For example, a subset can contain both a SAML Token and a Username Token security/authentication subcategory assertion, so a web service application can use either one or the other, but not both.</p> <p>You can only combine assertions that are in the same security category set in the Policy Information section. For example, if the policy category is set to the security/authentication subcategory, then only those assertion types can be added to the Only-One Subset. In addition, a subcategory that is used within the Only-One Subset cannot also be present outside of the Only-One Subset.</p> <p><b>Note:</b> Only service-side policies can contain OR groups.</p>
Assertion to OR Group	Add one or more assertions to the OR group. The Add Assertion page is displayed with a list of all the available assertions. Use this page to search for existing assertion templates and use them to add assertions to the OR group.

Action	Description
Add Assertion	<p>Provide search parameters in the <b>Name</b> and <b>Category</b> fields and click <b>Search</b>. The results that match the search criteria are displayed in the Search Results table.</p> <p>In the Search Results table, select the assertion or assertions to be added to the OR group and click <b>Add Selected</b>. To add all the listed assertions to the OR group, click <b>Add All</b>. The selected assertions are displayed in the Selected Assertion Templates table.</p> <p>In the Selected Assertion Templates table, review the selections. To remove one or more assertions from this table, click <b>Remove Selected</b> or <b>Remove All</b>. When you have confirmed the assertion selection, click <b>Add Assertion</b>.</p>
Delete	Delete an assertion from the policy. Select the assertion to be deleted and click <b>Delete</b> .
Move Up/Down	Reorder the assertions. Assertions are executed in the order in which they appear in the list. Select the assertion in the list and click <b>Move Up</b> or <b>Move Down</b> to reorder the assertion on the list.
Configuration	<p>Use this button to configure the property overrides for the selected assertion.</p> <p>Click <b>Add</b> to add a new property and complete the <b>Name</b> and <b>Value</b> fields. To delete a configuration property, select the property and click <b>Delete</b>. Click <b>OK</b> when you are done editing the configuration properties.</p>

### Details

The **Details** section provides the ability to view and specify the settings for the selected assertion. The settings displayed in the this section vary depending on the assertion selected.

### Validate and Save a Policy

After creating a new policy, or cloning or editing an existing policy, perform the following actions to validate, and then save the policy.

Action	Description
Validate	<p>If you clicked <b>Open</b> to view or edit an existing policy, click <b>Validate</b> to dynamically check whether the modified policy adheres to the policy subject and policy rules. More]</p> <p>If the policy is invalid, it is disabled as a precaution. After you correct the validation issues, enable the policy.</p>
Save	<p>If you clicked <b>Open</b> to view or edit an existing policy, after validating the policy, click <b>Save</b> to save the changes to the policy.</p> <p>If you clicked <b>Create</b> or <b>Create Like</b> to create a new policy or clone an existing policy, click <b>Save</b> to validate and save the policy and return to the Access Policies page.</p> <p>If the policy is invalid, it is disabled as a precaution. After you correct the validation issues, enable the policy.</p>
Cancel	Click <b>Cancel</b> to exit the Policy Details page and return to the Access Policies page.

### Related Topics

"Managing Policies" in *Administering Oracle Mobile Security Access Server*

## 10.3 Policy Version History Page

Use the Policy Version History page to:

- Review all versions of a policy.
- View the details of any policy version.
- Activate any version of a policy.
- Delete any version of a policy.
- Export a version of a policy.

---



---

**Notes:** You cannot edit a policy from the Policy Version History page. You must edit and save the policy in the Policy Details page.

---



---

The Policy Version history page provides details about each of the policy versions.

Element	Description
Name	Name of the policy to which the policy versions apply. The policy name includes the directory in which the policy is located. By default, all predefined policies are located in the <code>oracle</code> directory, and, therefore, <code>oracle/</code> is prefixed to the beginning of each policy name.
Display Name	Name used to reference the policy in the console.

Perform the following actions to manage policy versions.

Action	Description
View	Use the <b>Columns</b> and <b>Reorder Columns...</b> options to specify the columns that are visible and their order.
Make Current	Activate a previous version of a policy. Select a version in the policy version table and click <b>Make Current</b> . The policy version that is activated is moved to the top of the list and becomes the current active policy. The current version number is incremented by 1. The earlier version of the policy is retained.
Delete	Delete a policy version. Select the policy version from the policy version table, and click <b>Delete</b> .  You can delete all versions except the active policy version. To delete all versions of the policy, including the active version, you must delete the policy from the Access Policies page.
Export	Export a zip archive containing the version of the policy to your local directory. Select the policy version from the policy version table, and click <b>Export</b> to save the zip archive to your file system.

Policy details, in read-only format, are provided for the selected version. The policy details section of the page is arranged in the following tabs:

- [General](#)
- [Assertions](#)

## General

The **General** tab provides general summary information about the policy, such as the policy name and display name, category, description, if the policy is enabled or disabled, optimization settings, and so on.

Element	Description
Display name	Name used to identify the policy in the console.
Name	Unique name used as an identifier for the policy. The name includes the full path to the policy. All predefined policies are in the oracle directory. Therefore, the names of all predefined policies begin with <i>oracle/</i> , for example, <i>oracle/wss_username_token_service_policy</i> .
Category	Category to which the policy belongs. A policy may belong to only one category, and may only contain assertions that belong to the selected category.  Valid values include Management and Security.
Description	Text that provides a brief explanation of the policy behavior.
Enabled	Flag that specifies whether the policy is enabled or not. By default, the policy is enabled.

**Attachment Attributes** The **Attachment Attributes** section specifies the type of policy subjects to which the policy can be attached and the number of subjects to which the policy is attached, if applicable.

Element	Description
Applies To	Type of policy subjects to which the policy can be attached. Valid values include: <b>All</b> and <b>Service Bindings</b> . The Service Bindings choice requires further specification with the Service Category field.
Service Category	This option applies only when <b>Applies To</b> is set to <b>Service Bindings</b> . When the policy can be attached to URLs, the Service Category option is used to further specify whether the policy can be attached to services ( <b>Service Endpoint</b> ), clients ( <b>Client</b> ), or both.

**Version Information** The **Version Information** section provides details of a policy version in read-only mode.

Element	Description
Version Number	Version number of the currently active policy.
Last Updated	Timestamp of the last update to the policy.
Updated By	User who last updated the policy.

## Assertions

The **Assertions** tab provides the ability to view the assertions in the policy.

The **Assertions** table provides the following information for each assertion.

Element	Description
Name	Name of the assertion. The assertion name must be unique within the policy.

Element	Description
Category	<p>Category of the assertion. A policy can only contain assertions that are in the same category as the category specified in the <b>General</b> tab. For example, if the policy category is set to <b>Security</b>, then only Security assertions can be contained in the policy.</p> <p>The Security category has subcategories: security/authentication, security/msg-protection, security/authorization, and security/logging. A security policy can contain multiple security assertions; however, there can be only one assertion of each authentication, msg-protection, or authorization subcategory in a policy. This restriction can be altered for these subcategories, however, by creating an OR group, which can have multiple security assertions from the same subcategory, but only one of which can be executed. More.</p> <p>A security policy can have multiple assertions from the security/logging subcategory.</p>
Type	Type of assertion within a category. For example, an assertion may belong to the security/authentication category, and have a type wss10-saml-token.
Options	Indicates whether the Enforced and/or Advanced options are set for the assertion. When one of those options is set, as described below, the icon associated with the option appears in this field.
Enforced	Flag that specifies whether the policy assertion is enabled. The default is enabled.
Advertised	Reserved for future use.

### Details

The **Details** section provides the ability to view the settings for the selected assertion. Assertion template details vary based on the type of assertion. For example, templates that include message protection will include settings that are specific to message security. Details for the individual assertion templates are described in *Policy and Assertion Template Reference for Mobile Security Access Server*.

### Related Topics

"Versioning Policies" in *Administering Oracle Mobile Security Access Server*

## 10.4 Assertion Templates Page

Use the Assertion Templates page to:

- Search for assertion templates.
- Clone an assertion template.
- View and edit an existing assertion template.
- Import or export one or more assertion templates.

The Assertion Templates page is arranged in the following sections:

- [Search](#)
- [Assertion Templates Table](#)

### Search

Use the **Search** section of the Assertion Templates page to perform an advanced search for assertion templates in the repository. The results that are returned are the assertion templates that meet the conditions specified in the Name and Category fields

Element	Description
Assertion Name	<p>Enter an assertion template name or part of a name and select the operator to use to refine the search. Valid options are:</p> <ul style="list-style-type: none"> <li>■ <b>Starts with</b>—Returns all assertion templates that start with the value specified.</li> <li>■ <b>Ends with</b>—Returns all assertion templates that end with the value specified.</li> <li>■ <b>Equals</b>—Returns all assertion templates that exactly match the value specified.</li> <li>■ <b>Contains</b>—Returns all assertion templates that contain the value specified.</li> </ul> <p>You can use percent % as a wildcard, any place in the name. Asterisk * is not recognized as a wildcard and is treated as plain text. Searches are case-insensitive.</p>
Category	Select the assertion template category for which you want to search.
Search	Perform the search using the specified parameters.
Reset	Clear the specified search parameters.

### Assertion Templates Table

The **Assertion Templates** table displays the assertion templates in the repository that match the criteria specified in the **Search** fields. The following information is provided for each assertion template.

Element	Description
Name	Unique name used as an identifier for the assertion template. The assertion template name includes the directory in which the assertion template is located. By default, all predefined assertion templates are located in the <code>oracle</code> directory, and, therefore, <code>oracle/</code> is prefixed to the beginning of each assertion template name. Assertion templates are identified by the suffix <code>_template</code> at the end, for example, <code>oracle/wss10_message_protection_service_template</code> .
Category	Category of the assertion template. An assertion template may belong to only one category, and may only contain assertions that belong to the selected category.
Description	Brief description of the assertion template behavior.

Perform the following actions to manage assertion templates.

Action	Description
Actions	Drop-down menu that provides an alternate method to perform the available actions.
View	<p>Use this menu as follows:</p> <ul style="list-style-type: none"> <li>■ Use the <b>Columns</b> and <b>Reorder Columns...</b> options to specify the columns that are visible and their order.</li> <li>■ Use the <b>Detach</b> option to detach the Assertion Templates table from the console pane and expand to the full width of the console window. Use the <b>Attach</b> option to reattach the window to the console pane. Alternatively, you can use the <b>Detach</b> icon to attach and detach the table. To reattach, you can also click the Close icon.</li> </ul>

Action	Description
Create Like	Create a new assertion template that is based on an existing assertion template. Select an assertion template from the Assertion Templates table and click <b>Create Like</b> to display the Assertion Template Details page.
Open	Use this action to display the Assertion Template Details page where you can review and edit the details of an assertion template.  <b>Note:</b> Oracle recommends that you do not edit the predefined assertion templates so that you will always have a known set of valid templates.
Delete	Delete an assertion template.
Export	Export a zip archive containing one or more assertion templates to your local directory. You can use this feature in combination with <b>Import</b> to move one or more assertion templates between different repositories.  Select one or more assertion templates from the Assertion Templates table and click <b>Export</b> to save the zip archive to your file system.  The directory structure for each assertion template is maintained in the archive file using the following structure:  <code>META-INF/assertiontemplates/directory/assertiontemplatename</code>  where <code>directory/assertiontemplatename</code> are the values you provided when you created the assertion template.
Import	Import a zip archive containing one or more assertion templates. You can use this feature in combination with <b>Export</b> to move one or more assertion templates between different repositories. Click <b>Import</b> , then click <b>Browse</b> to locate the zip archive in your local directory that contains the assertion templates to be imported, and click <b>Import</b> .  An Information window is displayed listing the assertion templates that were imported. Click <b>OK</b> to close the window.  The imported assertion templates are added to the list of templates in the Assertion Templates table.  <b>Notes:</b>  The assertion templates to be imported must use the following directory structure:  <code>META-INF/assertiontemplates/directory/assertiontemplatename</code>  If an error is encountered with one of the assertion templates, the import process stops. For example, if there are five assertion templates to be imported and an error is encountered in the third one, the first two will be imported but the remaining assertion templates will not.
Detach	Click the <b>Detach</b> option to detach the assertion templates table from the console pane and expand to the full width of the console window. Use the <b>Attach</b> option or click the Close icon to reattach the window to the console pane.

### Related Topics

"Managing Policy Assertion Templates" in *Administering Oracle Mobile Security Access Server*

## 10.5 Assertion Templates Details Page

Use the Assertion Template Details page to:

- Create a new assertion template using an existing assertion template as a template that you edit.
- View or edit an existing assertion template.



- Validate an assertion template.

The assertion template details page provides a detailed description of the selected assertion. The assertion template name is displayed at the top of the page.

If you accessed this page using the **Create Like** button, then `_Copy` is appended to the name of the cloned assertion template.

Element	Description
Name	<p>Unique name used as an identifier for the assertion template. The assertion template name includes the directory in which the assertion template is located. By default, all predefined assertion templates are in the <code>oracle</code> directory, and, therefore, <code>oracle/</code> is appended to the beginning of the assertion template name. The assertion templates are identified by the suffix <code>_template</code> at the end, for example, <code>oracle/wss10_message_protection_service_template</code>.</p> <p>It is recommended that you follow the recommended naming conventions, and keep any assertion templates that you create in a directory that is separate from the <code>oracle</code> directory where the predefined assertion templates are located. You can organize your assertion templates at the root level, in a directory other than <code>oracle</code>, or in subdirectories.</p>
Display Name	Name used to reference an assertion template in the console.
Description	Brief description of the assertion template behavior.
Category	Category of the assertion template. An assertion template may belong to only one category, and may only contain assertions that belong to the selected category.
Type	Type of assertion within a category. For example, an assertion may belong to the <code>security/authentication</code> category, and have a type <code>wss10-saml-token</code> .
Configuration	Click to display the configuration properties for the assertion template. If you are cloning or editing an assertion template, you can specify values for the configuration properties in the Configuration pop-up window. How?
Settings	Configuration settings that define the behavior of the assertion. The settings vary based on the type of assertion. For example, templates that include message protection will include settings that are specific to message security. Details for the individual assertion templates are described in <i>Policy and Assertion Template Reference for Mobile Security Access Server</i> .

### Validate and Save an Assertion Template

After cloning or editing an assertion template, perform the following actions to save and validate the assertion template.

Action	Description
Validate	<p>If you clicked <b>Open</b> to view or edit an assertion template, click <b>Validate</b> to dynamically check whether the modified assertion template adheres to the validation rules. More]</p> <p><b>Note:</b> When you validate an assertion template you ensure that the assertion contained in the template has the correct syntax and contains all the information that is required for it to function properly during runtime.</p> <p>If the policy is invalid, it is disabled as a precaution. After you correct the validation issues, enable the policy.</p>

Action	Description
Save	If you clicked <b>Open</b> to view or edit an existing assertion template, after validating the template, click <b>Save</b> to save the changes.  If you clicked <b>Create</b> or <b>Create Like</b> to create a new assertion template or clone an existing template, click <b>Save</b> to validate and save the assertion template and return to the Assertion Templates page.  If the assertion template is invalid, it is disabled as a precaution. After you correct the validation issues, enable the template.
Cancel	Click <b>Cancel</b> to exit the Assertion Template Details page and return to the Assertion Templates page.

**Related Topics**

"Managing Policy Assertion Templates" in *Administering Oracle Mobile Security Access Server*