Oracle® Fusion Middleware

Installing Mobile Security Access Server

Release 11.1.2.3

E58403-01

April 2015

Describes how to install Oracle Mobile Security Access Server in an Oracle Mobile Security Manager domain.

ORACLE

Oracle Fusion Middleware Installing Mobile Security Access Server, Release 11.1.2.3

E58403-01

Contents

Preface

This guide describes how to install Oracle Mobile Security Access Server in either interactive or silent mode. It also describes how to create a Mobile Security Access Server instance using either interactive or silent mode, and how to configure the identity store and keystores for the instance.

Audience

This document is intended for administrators who are responsible for installing Oracle Mobile Security Access Server in an Oracle Access Manager environment. This document assumes that you have experience installing enterprise components. Basic knowledge about Oracle Access Manager, Mobile Security Manager, and Oracle WebLogic Server is recommended.

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 Mobile Security Suite and Oracle Identity Management documentation sets:

- *Release Notes for Oracle Identity Management*
- *Administering Oracle Mobile Security Access Server*
- *Installation Guide for Oracle Identity and Access Management*
- *Administering Oracle Mobile Security Suite*
- *Help Reference for Oracle Mobile Security Suite Consoles*
- *Policy and Assertion Template Reference for Oracle Mobile Security Access Server*
- *WebLogic Scripting Tool Command Reference for Identity and Access Management*

- *High Availability Guide*
- *Administrator's Guide for Oracle Access Management*
- *Securing Applications with Oracle Platform Security Services*

Conventions

The following text conventions are used in this document:

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

1

Installing Oracle Mobile Security Access Server

This chapter describes how to install and configure Oracle Mobile Security Access Server (MSAS).

This chapter contains the following topics:

1.1 Prerequisites for Installing Oracle Mobile Security Access Server

Before installing Mobile Security Access Server, ensure required prerequisites are installed. For more information, see "Section 6.2.4 Installing Oracle Mobile Security Access Server on Linux Requires compat-libtermcap-2.0.8" in *System Requirements and Specifications for Oracle Identity and Access Management 11g Release 2 (11.1.2.x)*.

Prior to configuring MSAS after installation, the Mobile Security Manager (MSM) Managed Server must be running.

For information about Oracle Mobile Security Manager, see "Configuring Oracle Mobile Security Suite" in *Installation Guide for Oracle Identity and Access Management*.

1.2 Installing Mobile Security Access Server

This section describes how to obtain and run the installer for MSAS. It contains the following topics:

1.2.1 Obtaining the Installer

You can download the MSAS installer from the Oracle Technology Network (OTN):

http://www.oracle.com/technetwork/indexes/downloads/index.html

You can also download the software from the Oracle Software Delivery Cloud at:

https://edelivery.oracle.com

1.2.2 Starting the MSAS Installer

Prior to starting the installation, note that MSAS must have a different Middleware home directory than the one in which MSM is installed.

To start the MSAS installer:

1. Extract the contents of the downloaded ZIP file to a directory of your choice. An `omsas` directory will be created in this directory.
2. Change to the `omsas/Disk1` directory.
3. Enter the following command. For *`jdk_directory`*, enter the full path to the JDK that you want to use for the installation (for example, `/jdk1.7.0_51`). This JDK should be the same as the one that was used for the prerequisite MSM installation.

   ```
   ./runInstaller -jreloc jdk_directory
   ```

When the Installer starts, the Welcome screen appears. Continue to the next section.

1.2.3 Installation Flow

To install MSAS, refer to the instructions in Table 1–1. If you need additional help with any of the Installer screens, click **Help**.

Table 1–1 Installation Flow

Screen	Description and Action
Welcome	Click **Next** to continue
Install Software Updates	Select one of the following options: ▪ **Skip Software Updates**—Do not check for software updates. ▪ **Search My Oracle Support for Updates**—You must have a My Oracle Support account to select this option. Enter your My Oracle Support username and password. If you use a proxy server, click **Proxy Settings** to configure it and then click **Test Connection**. ▪ **Search Local Directory for Updates**—Enter the local directory to search for updates or click **Browse** to select a directory that contains updates. When done, click **Search for Updates**. Click **Next** to continue.
Prerequisite Checks	The installer performs operating system, kernel, memory, and other checks to ensure that your system meets the prerequisite requirements. If successful, click **Next** to continue. If a system check fails, reference the information in the box at the bottom of the screen to determine a cause. Click **Cancel** to exit the installer. Resolve the issue before restarting the installer.

Table 1–1 (Cont.) Installation Flow

Screen	Description and Action
Installation Location	Enter the following information: ■ **Oracle Middleware Home**—Enter the path to the Middleware home you want to use for the MSAS installation; for example, /u01/oracle/omsas. This directory is referred to as MW_HOME in this document. **Note:** You *cannot* install MSAS into the same Middleware home directory as MSM. MSAS must be installed in its own unique Middleware home directory. ■ **Oracle Home Directory**—Enter the home directory for MSAS here. This directory will be created under the specified Oracle Middleware Home. For example, if you enter Oracle_MSAS, the MSAS home will be /u01/oracle/omsas/Oracle_MSAS. This directory is referred to as ORACLE_HOME in this document.
Installation Summary	Verify that the directory details are correct. If you want to save a response file to use for silent installation of MSAS on other machines, click **Save**. Enter a name for the response file, navigate to the directory in which you want to store the file, and then click **Save**. When done, click **Install** to begin the installation.
Installation Progress	The Progress bar indicates the progress of the installation. When the installation completes, click **Next**.
Installation Complete	Click **Save** if you want to save the installation details. Otherwise click **Finish** to exit the installer.

1.2.4 Post-Installation Tasks

After exiting the installer, refer to the following sections for post-installation tasks:

- Section 1.3, "Verifying the Installation"
- Section 1.4, "Configuring an MSAS Instance"
- Section 1.5, "Configuring the Identity Store and Keystores for the MSAS Instance"

1.3 Verifying the Installation

To verify the installation:

1. Open *MW_HOME*/orainst.loc to determine the location of your Oracle inventory directory. For example, if you installed MSAS in /u01/oracle/omsas/Oracle_OMSAS, open /u01/oracle/omsas/Oracle_OMSAS/orainst.loc.
2. Switch to the logs directory in the Oracle inventory directory indicated by the inventory_loc property in this file. For example, if inventory_loc=/u01/oracle/omsm:

   ```
   cd /u01/oracle/omsm/logs
   ```

3. Examine the file install*Date-timestamp*.out for any issues.

1.4 Configuring an MSAS Instance

After completing the installation, you can create and configure an MSAS instance using the `configMSAS.sh` tool:

- Interactively by responding to prompts; see Section 1.4.2, "Configuring an MSAS Instance Interactively."
- In silent mode using a properties file; see Section 1.4.3, "Using Silent Mode to Configure an MSAS Instance."

`configMSAS` performs the following operations:

- If the provided MSAS instance ID does not exist in the MSM environment, it creates and registers the instance ID with MSM. If the provided instance ID already exists in the MSM environment, it binds the MSAS instance with the machines on which that instance ID is configured.
- On the machine on which you run `configMSAS`, creates an HTTPS port and optionally an HTTP port on which the MSAS instance will listen for requests.
- Creates a bootstrap configuration that enables the MSAS instance to connect to the MSM machine identified by the MSM URL.
- Optionally, it also performs additional configuration in:
  - OAuth (Mobile and Social), when MSAS acts as an OAuth client
  - OAM when MSAS acts as a WebGate

If you are using OAuth, prior to creating the instance, ensure that the OAuth Service Profile that you want to use for this instance already exists.

1.4.1 configMSAS Options

`configMSAS` syntax is as follows.

```
configMSAS.sh -properties input_properties_file -help -debug_level level -debug_
file debug_file_name -update
```

Table 1–2 configMSAS Options

Option	Description
`-properties`	Required for interactive mode. If included, you must include the name of the properties file to use immediately after this parameter.
`-input_properties_file`	The full path of the properties file to use for interactive mode.
`-help`	Displays help for the `configMSAS` command.
`-debug_level`	The Java logging level. Specify one of SEVERE, WARNING, INFO, CONFIG, FINE, FINER, FINEST. If you include this parameter, you must also include the debug file to use.
`-debug_file`	The full path of the debug file in which to log debug messages.
`-update`	Causes `configMSAS` to run in update mode. Only MSM URL and credential update is supported.

1.4.2 Configuring an MSAS Instance Interactively

To configure an MSAS instance interactively:

1. Ensure that the MSM server is in a RUNNING state. If not, start the MSM server on which the MSAS instance will be registered.
2. Change to the *ORACLE_HOME*/omsas/bin directory, where *ORACLE_HOME* is the directory you specified for **Oracle Home** when you installed MSAS, for example, /u01/oracle/omsas/Oracle_MSAS.
3. Enter the following command to start the MSAS configuration tool:

   ```
   sh configMSAS.sh
   ```

4. Respond to each prompt as described in Table 1–3. If you make an error and need to exit configMSAS without completing the configuration, press Ctrl-c.

Table 1–3 MSAS Configuration Tool Prompts

Prompt	Description
Enter the MSAS Instance ID	Enter a unique name to identify the MSAS instance, for example, msas-instance-1. The name must adhere to the XML xs:NCNname format using only valid NC Name ASCII characters. For example, it must start with a letter or underscore (_) and cannot contain any space characters or colons (:). For the NCName format definition, see the W3C document Namespaces in XML1.0 (Third Edition at http://www.w3.org/TR/REC-xml-names/#NT-NCName.
Enter the MSAS Instance Root Dir	This is the full path to the root directory in which you want to store MSAS instances. It defaults to *MW_HOME*/instances, where *MW_HOME* is the Middleware home for MSAS. Oracle strongly recommends that you use this location. Press **Enter** to accept the default location (recommended) or enter the full path to a directory of your choice. The MSAS instance directory will be created in *instance_root_dir*/*instance_id*, where *instance_id* is what you entered for the previous prompt.
Enter the SSL Port Number where MSAS Instance will be running	Enter an available port number. This is the port on which MSAS will listen for an SSL connection. Use the same value for the OMSS_MSAS_SERVER_PORT property in the properties file for idmConfigTool.
Do you want to enable Non-SSL Port	If you want to MSAS to also listen for non-SSL connections, enter y, and then enter the port number in the next prompt. Press **Enter** to accept the default n.
Enter the Port Number where MSAS Instance will be running	This prompt is displayed only if you entered y for the previous prompt. Enter an available port number to use for non-SSL communication.

Table 1–3 (Cont.) MSAS Configuration Tool Prompts

Prompt	Description

`Enter the Mobile Security Manager (MSM) URL`	This is the URL for the MSM server that you want this MSAS instance to be registered with. Enter the URL for the MSM server in the following format, where *host* is either the host name or the IP address of the MSM server and the port number is the listen port for the MSM server.
	`http://host:port_number`
	or
	`https://host:ssl_port_number`
	If you have only one MSM server, the port number is typically port 14180 (non-SSL) or 14181 (SSL) unless you configured other ports when you created the MSM domain.
	Oracle recommends that you use the SSL port in this URL.
	Note: If a Load Balancer Router (LBR) is being used as a front end for the MSM server, enter the URL of the LBR for this prompt.

`Enter the Username to connect to Mobile Security Manager`	Enter the WebLogic Server administrator username for the MSM domain.
`Enter the Password to connect to Mobile Security Manager`	Enter the password for the WebLogic Server administrator.
Optional Configuration	The following ten prompts are relevant only if you are configuring OMSS in a joint deployment with OAM using OAuth for authentication, or with MSAS acting as a WebGate. If this does not apply to your configuration, you can enter any values for these prompts. OAM configuration will fail, but the MSAS instance will be created successfully.
`Enter the OAM Admin Server Hostname`	This is the hostname of the Administration Server for the domain in which the OAM Managed Server is configured. Press **Enter** to accept the default, or if necessary, enter the host name for the OAM Managed Server's Administration Server.
`Enter the OAM Admin Server Port`	This is the listen port you entered for the Administration Server in the Configuration Wizard (or WLST) when you created the domain in which the OAM Managed Server resides. Press **Enter** to accept the default, or if necessary, enter the listen port for the OAM Managed Server's Administration Server.
`Is the connection with the OAuth Managed Server over SSL`	Press **Enter** to accept the default `n`. If you want the connection to the OAuth Managed Server to use SSL, enter `y`.

Table 1–3 (Cont.) MSAS Configuration Tool Prompts

Prompt	Description
`Enter the OAM Admin Username`	Enter the existing administrator login username for connecting to the running OAM Administration Server. Enter the same username that you specified for the IDSTORE_OAMADMINUSER property when you ran the `idmConfigTool -configOAM` command during OAM configuration.
`Enter the OAM Admin Password`	Enter the password for the OAM administrator username account.
`Enter the OAuth Managed Server Host`	(Optional) Enter the host where the OAuth Managed Server is running, or press **Enter** to use the default, which is the OAM Administration Server you previously specified if the OAuth Manager Server is running on the same host as the OAM Administration Server.
`Enter the OAuth Managed Server Port`	OAuth is deployed on the OAM server in the domain. Enter the port number that is configured for the OAM server. Typically this is `14101` for SSL communication (or `14100` for non-SSL communication), unless you entered another value when you configured the domain.
`Enter the OAuth Service Profile Endpoint`	This is an OAuth service profile name. Press **Enter** to accept the default, `/oauthservice`, which is the Default OAuth Service Profile. Only the default profile is supported in this release.
`Enter the OAM Protected Resource`	Specifies the path for resources to be protected, for example, /myapp/login. This applies only when you are using MSAS as Webgate. Press **Enter** to accept the default (/), which matches all request URLs.
`Enter the Domain name for which the cookie is to be set`	Press **Enter** to accept the default, which is the fully qualified domain name (FQDN) of the MSAS host. If necessary, enter the FQDN manually. The value you enter must start with a dot (.), for example: `.mydomain.com`

The following message displays when the process completes successfully:

`The Instance for MSAS Instance ID - instance_name Configured Successfully.`

1.4.3 Using Silent Mode to Configure an MSAS Instance

To create and configure an MSAS instance using silent mode:

1. Create a `.properties` file containing the properties described in Table 1–4. A property is required unless otherwise indicated.

> **Note:** If you do not specify the password properties in the file, you will be prompted for the passwords when you run `configMSAS.sh`.

Table 1–4 Properties for Silent Mode

Property Name	Description

MSM_URL	Specify the URL for the MSM server that you want this MSAS instance to be registered with. Enter the URL for the MSM server in the following format, where *host* is either the host name or the IP address of the MSM server and the port number is the listen port for the MSM server.
	`http://host:port_number`
	or
	`https://host:ssl_port_number`
	If you have only one MSM server, the port number is typically port 14180 (non-SSL) or 14181 (SSL) unless you configured other ports when you created the MSM domain.
	Oracle recommends that you use the SSL port in this URL.
	Note: If a Load Balancer Router (LBR) is being used as a front end for the MSM server, specify the URL of the LBR for this property.

MSM_USER_NAME	Enter the WebLogic Server Administrator username for the MSM domain.
MSM_PASS	Enter the WebLogic Server Administrator password.
MSAS_INSTANCE_ID	Specify a unique name to identify the MSAS instance, for example, `msas_instance-1`. The name must adhere to the XML xs:NCNname format using only valid NC Name ASCII characters. For example, it must start with a letter or underscore (_) and cannot contain any space characters or colons (:). For the NCName format definition, see the W3C document Namespaces in XML1.0 (Third Edition at `http://www.w3.org/TR/REC-xml-names/#NT-NCName`.
MSAS_INSTANCE_ROOT_DIR	Specify the full path to the root directory in which you want to store this MSAS instance. Oracle strongly recommends that you specify *MW_HOME*`/instances`, where *MW_HOME* is the Middleware home for MSAS. The MSAS instance will be created at *MSAS_INSTANCE_DIR*`/`*MSAS_INSTANCE_ID*. If this property is not included, it defaults to *MW_HOME*`/instances`.
MSAS_INSTANCE_SSL_PORT	Specify an available port number to use as the SSL port on which MSAS will run. Use the same value for the `MSAS_INSTANCE_SSL_PORT` property in the properties file for `idmConfigTool` when you configure the identity store for the instance.
MSAS_INSTANCE_PORT	(Optional) If you want MSAS to listen for connections on a non-SSL port, include this property and specify the port to use for MSAS non-SSL communication.
Optional Configuration	You must include the following properties only if you are configuring OMSS in a joint deployment with OAM using OAuth for authentication, or with MSAS acting as a WebGate.
OAM_HOST	Specify the hostname of the Administration Server for the domain in which the OAM Managed Server is configured.

Table 1–4 (Cont.) Properties for Silent Mode

Property Name	Description
OAM_PORT	Specify the listen port you entered for the Administration Server in the Configuration Wizard (or WLST) when you created the domain in which the OAM Managed Server resides.
OAM_USER_NAME	Specify the existing administrator login username for connecting to the running OAM Administration Server. Use the same username that you specified for the IDSTORE_OAMADMINUSER property when you ran the `idmConfigTool -configOAM` command during OAM configuration.
OAM_PASSWORD	Specify the password for the OAM administrator username account.
OAM_PROTECT	Specifies the path for resources to be protected, for example, /myapp/login. This property applies only when you are using MSAS as Webgate. You can enter /, which matches all request URLs. For more information about resource patterns, see "About Query String Name and Value Parameters for Resource Definitions" in *Administrator's Guide for Oracle Access Management*.
OAUTH_PORT	OAuth is deployed on the OAM server in the domain. Specify the port number that is configured for the OAM server. Typically this is `14101` for SSL communication (or `14100` for non-SSL communication), unless you entered another value when you configured the domain.
OAM_COOKIE_DOMAIN	Specify the fully qualified domain name (FQDN) of the MSAS host. The value you enter must start with a dot (.). For example, specify: `.mydomain.com`
OAUTH_HOST	(Optional) Specify the host where the OAuth Managed Server is running. If not included, the OAM_HOST will be used.
OAUTH_SP_ENDPOINT	Required only if you are using OAuth. This is an OAuth service profile name, for example: `/oauthservice` **Note:** OAuth comes with a Default OAuth Service Profile, which is accessible at `/oauthservice`. Only the Default OAuth Service Profile is supported in this release.
OAUTH_IS_SSL	Specify `false` for a non-SSL connection to OAuth, or specify `true` for an SSL connection to OAuth.

2. Ensure that the MSM Managed Server to which you want to bind this MSAS instance is in a RUNNING state. If not, start this server.
3. Change to the *ORACLE_HOME*/bin directory, where *ORACLE_HOME* is the directory you specified for **Oracle Home** when you installed MSAS, for example, /u01/oracle/omsas/Oracle_MSAS.
4. Enter the following command to start the MSAS configuration tool, where *propfile* is the name of the .properties file you created in Step 1:

   ```
   sh configMSAS.sh -properties propfile
   ```

The following message displays when the process completes successfully:

```
The Instance for MSAS Instance ID - instance_name Configured Successfully.
```

1.4.4 Binding a Logical MSAS Instance to a Physical Instance

There are two situations in which you can use `configMSAS.sh` to bind a logical MSAS instance ID to a physical machine:

- You have already run `configMSAS.sh` on a machine to create a logical MSAS instance ID that is bound to that machine and port and you want to bind the same logical instance to another machine and port to create a cluster for that instance ID. You can bind a logical MSAS instance ID to as many physical instances as needed. This is the most common scenario in a high-availability production environment. See Section 1.4.4.1, "Binding a Logical Instance ID to Multiple Physical Instances."

  For more information about clustered instances, see "Configuring High Availability for Oracle Mobile Security Access Server" in *High Availability Guide*.

- You use the MSAS console to create a logical instance (which only registers a new logical MSAS instance ID), and you then need to run `configMSAS.sh` to bind that logical instance to a machine and port. See Section 1.4.4.2, "Binding a New Logical Instance ID to a Physical Instance."

1.4.4.1 Binding a Logical Instance ID to Multiple Physical Instances

You can bind an existing logical MSAS instance ID to other physical instances (machine:port combinations) by running `configMSAS.sh` interactively or in silent mode on each machine to which you want to bind the instance ID. You can create multiple physical instances on the same machine on different ports.

- When running `configMSAS.sh` interactively:
  - For the `Enter the MSAS Instance ID` prompt, enter the same logical instance ID that you used when you first created the logical MSAS instance.
  - For the `Enter the Mobile Security Manager (MSM) URL` prompt, specify the same MSM URL as was used when you first created the logical MSAS instance. For example, enter `http://machine2:14180`.
  - Use the same MSAS instance ID and MSM details as specified for other MSAS instances. The MSAS instance root directory, and the MSAS SSL and non-SSL ports can be different, but all other properties must be same.
- When running `configMSAS.sh` in silent mode:
  - For the `MSAS_INSTANCE_ID` property, specify the same logical instance ID that you used when you created the logical MSAS instance in the MSAS console.
  - For the `MSM_URL` property, specify the specify the same MSM URL as was used when you first created the MSAS instance ID. For example, enter `http://machine2:14180`.
  - Use the same MSAS instance ID and MSM details as specified for other MSAS instances. The MSAS instance root directory, and the MSAS SSL and non-SSL ports can be different, but all other properties must be same.

For example, if you have MSAS installed on two machines (machineA and machineB), and you want to create Instance1 using port 9000 as the SSL listen port on each machine:

1. Run `configMSAS` on machineA, specify Instance1 as the MSAS Instance ID and 9000 as the SSL listen port. This creates the logical instance ID Instance1 and binds it to machineA:9000.

2. Run `configMSAS` on machineB, specify Instance1 as the MSAS Instance ID and 9000 as the SSL listen port. This binds the existing logical instance ID Instance1 to machineB:9000. In addition, specify the same MSM URL as you used when you created the instance.

1.4.4.2 Binding a New Logical Instance ID to a Physical Instance

When you create and register a new logical MSAS instance ID using the MSAS console, you must run `configMSAS.sh` on an MSAS machine to bind that logical instance ID to a port on that machine and also to an MSM server.

To do so:

1. Run `configMSAS.sh` as described in either Section 1.4.2, "Configuring an MSAS Instance Interactively," or Section 1.4.3, "Using Silent Mode to Configure an MSAS Instance."
2. For the MSAS instance ID, specify the same value that you used when you created the logical instance ID in the MSAS console.
3. Use the appropriate values for all other prompts or properties as described in either Table 1–3 or Table 1–4.

This binds the logical instance to the an MSAS machine:port and the MSM server you specified with either the `Enter the Mobile Security Manager (MSM) URL` prompt or `MSM_URL` property, and updates the settings for the logical instance ID in the console.

1.5 Configuring the Identity Store and Keystores for the MSAS Instance

After creating the MSAS instance, use `idmConfigTool.sh` to configure the identity store, SSL keystore, and MSAS keystore to use for the instance. You must run `idmConfigTool` on the host on which MSM is installed. In a high-availability environment with multiple MSM servers, you can run `idmConfigTool` on any one of the MSM servers. Run `idmConfigTool` exactly once for each logical instance ID to configure the identity store and keystores for that ID, after binding the first MSAS instance to the logical instance ID.

Prior to running `idmConfigTool`:

- Ensure that the OMSM Managed Server is running
- Ensure that you have added any security certificates that are specific to this installation to the trust store; for example, certificates in the LDAP server trust chain, certificates in the OAM server trust chain, and certificates in the OAuth server trust chain, if any of them are accessed over SSL.

  When you ran `idmConfigTool -configOMSS` during OMSS configuration, any certificates that are located in the directory specified by the OMSS_OMSAS_AUX_CERTIFICATES_LOCATION property were automatically loaded. You must manually load any certificates that are not located in that directory.

When running `idmConfigTool.sh`, use the same properties file you used when you configured Oracle Mobile Security Suite. For more information, see "Running idmConfigTool to Configure Oracle Mobile Security Manager" in *Installation Guide for Oracle Identity and Access Management*.

For more information about `idmConfigTool`, see "Using the idmConfigTool Command" in *Integration Guide for Oracle Identity Management Suite*.

1.5.1 Running idmConfigTool

To run `idmConfigTool`:

1. Set the following environment variables:
   - Set `MW_HOME` to the full path of the MSM installation Middleware Home. This is the directory you specified for **Oracle Middleware Home** when you installed MSM for example, `/u01/oracle/omsm`.
   - Set `ORACLE_HOME` to the full path of the MSM Oracle home directory. This is the directory you specified for **Oracle Home** when you installed MSM, for example, `/u01/oracle/omsm/omsm`.
   - Set `WL_HOME` to the full path of the WebLogic Server home directory. This is the wlserver_10.3 for your WebLogic Server installation, for example, `/u01/oracle/wls/wlserver_10.3`.
   - Set `JAVA_HOME` to the full path of the JDK directory.
2. Update the `.properties` file that was previously used when running `idmConfigTool.sh -configOMSS mode=OMSM` by adding the following properties with the appropriate values for the MSAS instance for which you are configuring the identity store.

idmConfigTool Property	Use the same value as ...
OMSS_MSAS_SERVER_HOST	The hostname on which you created the MSAS instance specified by the MSAS_INSTANCE_ID.
OMSS_MSAS_SERVER_PORT	`Enter the SSL Port Number where MSAS Instance will be running` prompt or MSAS_INSTANCE_SSL_PORT property from `configMSAS`.
OMSS_OMSAS_IDSTORE_PROFILENAME	This value does not exist yet. A new identity store profile will be created with the specified name.
OMSS_GATEWAY_INSTANCE_ID	`Enter the MSAS Instance ID` prompt or MSAS_INSTANCE_ID property from `configMSAS`.

3. Enter the following command, where *`IAM_HOME`* is the Oracle Identity and Access Manager home directory for your Oracle Mobile Security Suite installation, for example, `/u01/oracle/omsm/Oracle_IDM/`:

   ```
   cd IAM_HOME/idmtools/bin
   ```

4. Enter the following command, where *`propsfile`* is the same properties file you used when you configured Oracle Mobile Security Suite.

   ```
   -sh idmConfigTool.sh -configOMSS mode=OMSAS input_file=propsfile
   ```

   If you want to get a log file of the configuration session, include the following two parameters at the end of the command:

   ```
   -log_level=FINEST log_file=logfilename
   ```

   For more information about the properties in this file on the properties file and the complete set of Oracle Mobile Security Suite configuration properties, see "Creating the Oracle Mobile Security Suite Properties File" in *Installation Guide for Oracle Identity and Access Management*.

   For more information about `idmConfigTool`, see "Using the idmConfigTool Command" in *Integration Guide for Oracle Identity Management Suite*.

5. When prompted, enter the password of the account used to connect to the identity store.
6. When idmConfigTool completes, you can start the MSAS server; refer to Section 1.6, "Starting and Stopping the MSAS Server."

1.6 Starting and Stopping the MSAS Server

To start or stop an MSAS server instance:

1. Change to the *instance_root*/*instance_name*/bin directory, where *instance_root* is the root directory you specified for the MSAS instance when you created it and *instance_name* is the name of the MSAS instance. By default, *instance_root* is *MW_HOME*/instances, where *MW_HOME* is the Middleware home for MSAS.
2. Enter the following command to start the server instance:

   ```
   sh startServer.sh
   ```

3. Enter the following command to stop the server instance:

   ```
   sh stopServer.sh
   ```

1.7 Deinstalling Oracle Mobile Security Access Server

When removing the Oracle Mobile Security Access Server software, use the instructions in this section. Oracle recommends that you not remove the software manually.

To deinstall Oracle Mobile Security Access Server:

1. Change to the *MW_HOME*/msas/oui/bin directory, where *MW_HOME* is the Middleware home directory in which you installed MSAS.
2. Enter the following command:

   ```
   ./runInstaller -deinstall
   ```

3. If necessary, manually delete the Middleware home directory in which MSAS was installed.

1.8 Installing Oracle Mobile Security Access Server Using Silent Installation

Prior to installing Oracle MSAS in silent mode, you must either have created a response file during a previous session of the MSAS installer or have manually created a response file. The following example shows a typical response file for MSAS. In this example, software updates are skipped. Save the file in text format with a .rsp extension (such as msas_silent.rsp) to a directory of your choice.

```
[ENGINE]

#DO NOT CHANGE THIS
Response File Version=1.0.0.0.0

[GENERIC]
SPECIFY_DOWNLOAD_LOCATION=false

SKIP_SOFTWARE_UPDATES=true
```

```
SOFTWARE_UPDATES_DOWNLOAD_LOCATION=

ORACLE_HOME=/u01/oracle/products/omsas/omsas

MIDDLEWARE_HOME=/u01/oracle/products/omsas

[SYSTEM]
[APPLICATIONS]
[RELATIONSHIPS]
```

In this example:

- **ORACLE_HOME** is the full path to use for the MSAS ORACLE_HOME. This directory path consists of *MIDDLEWARE_HOME*/*directory*, for example, /u01/oracle/product/omsas/omsas.
- **MIDDLEWARE_HOME** is the Middleware home directory to use for MSAS. For example /u01/oracle/product/omsas.

To perform a silent installation:

1. Extract the contents of the downloaded ZIP file to a directory of your choice. An omsas directory will be created in this directory.
2. Change to the omsas/Disk1 directory.
3. Enter the following command: For *jdk_directory*, enter the full path to the JDK that you want to use for the installation (for example, /jdk1.7.0_51). This JDK should be the same as the one that was used for the prerequisite MSM installation.

   ```
   ./runInstaller -jreloc jdk_directory -invPtrLoc absolute_path_of_oraInst.loc
   -silent -response absolute_path_of_response_file
   ```

   In this command:

   - ***jdk_directory*** is the absolute path to the JDK you want to use for the installation, for example, /u01/jdk1.7.0_15. This should be the same as the one that was used for the prerequisite MSM installation.
   - ***absolute_path_of_oraInst.loc*** is either *ORACLE_HOME*/oraInst.loc, where *ORACLE_HOME* is the Oracle home directory for MSAS, or the path to an existing oraInst.loc file on the system. If the file does not exist in the specified location, it is created by the installer.
   - ***absolute_path_of_response_file*** is the absolute path to the response file you created, for example, /home/myname/msas_silent.rsp.