Oracle® Session Delivery Management Cloud

Getting Started Guide

F30727-12
November 2024

Oracle Session Delivery Management Cloud Getting Started Guide,

F30727-12

Contents

About This Guide

The *Getting Started Guide* provides information about installing the Oracle® Session Delivery Management Cloud(Oracle SDM Cloud) and its components.

The following table describes the documents included in the Oracle SDM Cloud documentation set.

Document Name	Document Description
Getting Started Guide	Contains conceptual and procedural information for system provisioning and software installations.
Users Guide	Contains information about the administration and software configuration of the OSDMC.
Security Guide	Contains information about security considerations and best practices from a network and application security perspective.
What's New	Contains a list of new features for a specific release as well as Known Issues pertaining to the release.

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with My Oracle Support registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select `2` for New Service Request.
2. Select `3` for Hardware, Networking, and Solaris Operating System Support.
3. Select one of the following options:
   - For technical issues such as creating a new Service Request (SR), select `1`.
   - For non-technical issues such as registration or assistance with My Oracle Support, select `2`.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click **Industries**.
3. Under the Oracle Communications sub-header, click the **Oracle Communications documentation** link.
   The Communications Documentation page appears. Most products covered by these documentation sets appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
4. Click on your Product and then Release Number.
   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

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.

Revision History

This section provides a revision history for this document.

Date	Description
July 2020	• Initial release.
December 2020	• Clarifies OS requirement for MCE.
January 2021	• Removes inaccurate references to OCSS. • Updated for 20C January 2021 release.
April 2021	• Updated for 20C April 2021 release. • Adds a note to "Install, Configure, and Activate CCS" regarding support of the CCS shared support model.
July 2022	• Updated for 20C July 2022 release.
November 2022	• Adds "Upgrading the CCS".
August 2023	• Updated for 23C August 2023 release.
February 2024	• Updated for 24A February 2024 release.
August 2024	• Updates "Install and Configure the MCE" and "Upgrading the MCE" for accuracy.
November 2024	• Adds "Traffic Flow and Firewall Port Recommendations". • Updates "Upgrading the MCE" for accuracy.

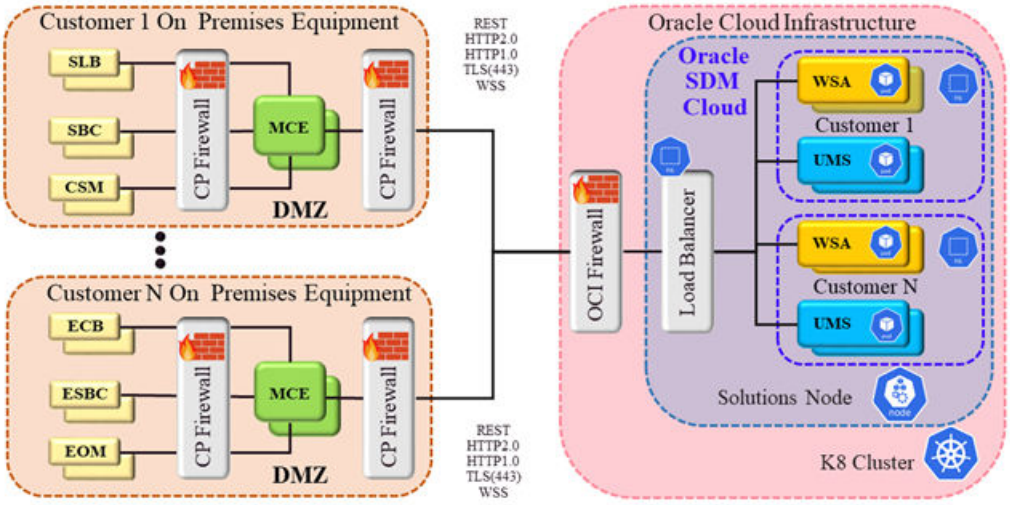
1

Oracle SDM Cloud Deployment Overview

The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) consists of two components that interact with one another to provide the service. These components are the Oracle SDM Cloud services and the Management Cloud Engine (MCE). The Oracle SDM Cloud service resides in the Oracle Cloud, while the MCE resides on premises. You can install the MCE, a Podman image, on a Virtual Machine.

- MCE: The MCE provides the protocol conversion from legacy Network Function (NF) to cloud centric REST-based APIs. MCE is deployed in its own container and you can deploy multiple instances of MCE. MCE is completely stateless. When it registers with Oracle SDM Cloud, the Unified Management Service (UMS) provide each MCE with instructions for load balancing of polling events, processing traps, and managing NFs.

The following image shows an example Oracle SDM Cloud setup interacting with the MCE component.



On-Premises Software Compatibility

For up to date information regarding on-premises software compatibility between Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) and Management Cloud Engine (MCE), see the Oracle SDM Cloud What's New guide.

Version Requirements for External Components

The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) requires the following versions, at minimum, for components external to the Oracle Cloud.

Management Cloud Engine

The following values reflect the minimum value for one MCE. For additional instances, you will need the appropriate resources.

- CPUs—4

- Memory—8GB
- Disk—24GB
- Interfaces—2
  - Throughput—1Gbps NIC capacity
- Podman v4.4.1 or higher
- Oracle Linux 8.8 or higher or Red Hat Compatible Kernel

> **Note:**
>
> The latest version of Oracle SDM Cloud is not tested on Red Hat Enterprise Linux (RHEL) and Oracle recommends using the base version of Linux on the 8.x release.

- Perl v5.26.3 or higher

MCE Deployment, Management, and Work Flow

When you deploy the Management Cloud Engine (MCE), you must run the supplied scripts to install, configure, activate, decativate, and uninstall the service. Oracle provides a unique set of scripts for MCE, and packs them all in the archive.tgz file that you download from either Oracle Software Delivery Cloud or My Oracle Support. The download creates the following directory tree on the host.

Directory tree:

```
mce-<version>.<build>
mce-<version>.<build>/mce/
mce-<version>.<build>/mce/perl/
mce-<version>.<build>/mce/perl/activate.pl
mce-<version>.<build>/mce/perl/config.pl
mce-<version>.<build>/mce/perl/deactivate.pl
mce-<version>.<build>/mce/perl/uninstall.pl
mce-<version>.<build>/mce/cfg/
mce-<version>.<build>/mce/ssl/
mce-<version>.<build>/mce/log/
mce-<version>.<build>/mce/img/
mce-<version>.<build>/mce/img/mce.tar
mce-<version>.<build>/mce/.version
mce-<version>.<build>/mce/.build
mce-<version>.<build>/install.pl
```

The initial installation process for the MCE includes running the scripts in the following order:

1. Install
2. Configure
3. Activate
   After the initial installation you can use the various scripts to manage the MCE, as follows:
   - Reconfigure and reactivate the installed version of the MCE.
   - Deactivate and reactivate the existing configuration.

- Uninstall the MCE.

Enable Communication Between the Oracle SDM Cloud and SBCs

When adding an SBC to the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) as a device, the SBC must use the Management Cloud Engine (MCE) to communicate with the Oracle SDM Cloud. In order to enable this communication, you must add the MCE to the SBC's SNMP community and as a trap receiver target.

> **Note:**
>
> For each MCE configured, you must configure a corresponding entry in the SBC's **snmp-community** and **trap-receiver** configurations. This includes redundancy pairs.

For more information on adding the SBC as a device, see https://docs.oracle.com/en/industries/communications/session-delivery-management-cloud/userguide/device-manager.html#GUID-9472A394-416E-4C48-9AAB-0FA8FFF144FE.

The following is a sample configuration of a device running ECZ810m1, which supports both SNMP v1 and v2. Enter the IP address of the MCE that is current registered with the Oracle SDM Cloud and the community name you use when adding the device to the Oracle SDM Cloud.

```
ecz25# configure terminal
ecz25(configure)# system
ecz25(system)# snmp-community
ecz25(snmp-community)# ip-addresses 15.122.0.00
ecz25(snmp-community)# community-name mce
ecz25(snmp-community)# done
snmp-community
        community-name              mce
        access-mode                 READ-ONLY
        ip-addresses                15.122.0.00
        last-modified-by            admin@15.122.0.00
        last-modified-date          2021-01-20 22:28:31
```

The following sample configuration shows the user adding the MCE's IP address to the SBC's trap-receiver configuration. During MCE installation, you are prompted to enter the trap reciever port for the MCE. This value must be the same on both the device and the MCE. The default value is 162.

```
ecz235# configure terminal
ecz235(configure)# system
ecz235(system)# trap-receiver
ecz235(trap-receiver)# ip-address 15.122.0.00
ecz235(trap-receiver)# filter-level Major
ecz235(trap-receiver)# community-name mce
ecz235(trap-receiver)# done
trap-receiver
        ip-address              15.122.0.00:162
        filter-level            Major
```

```
community-name              mce
last-modified-by            admin@15.122.0.00
last-modified-date          2021-01-20 22:40:31
```

2

Oracle SDM Cloud Deployment Process and Procedures

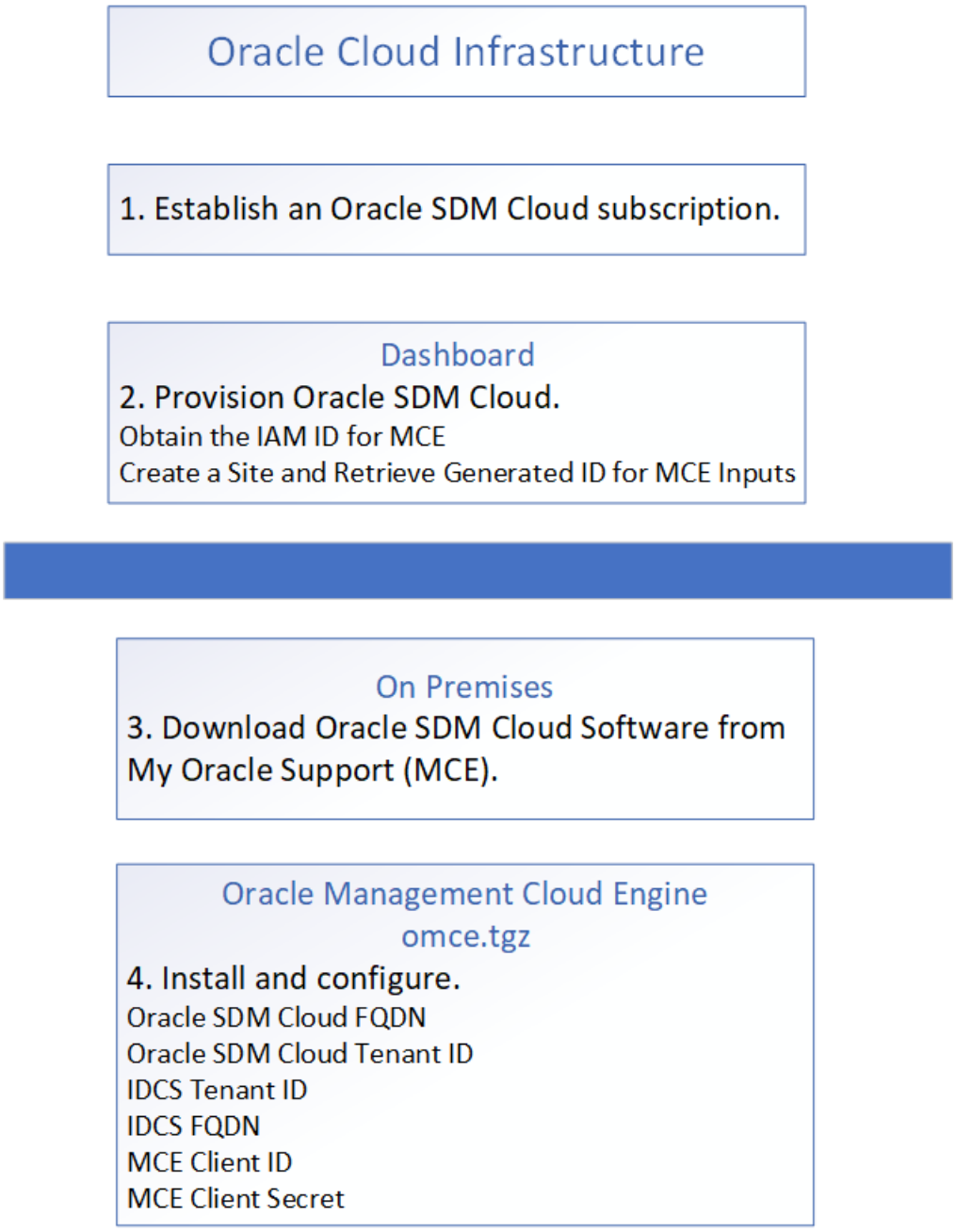
Obtaining and Installing the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) service requires a multi-step process that includes tasks for you to perform in the Oracle Cloud and on premises. New customers must take steps to establish and set up their Oracle Cloud account in addition to the procedures for installing the Oracle SDM Cloud service. See the following topics to guide you through the process.

- Oracle SDM Cloud Deployment Process
- Establish an Oracle SDM Cloud Service Subscription
- Login to Oracle SDM Cloud to obtain inputs for Management Cloud Engine (MCE)
- Establish a site with the Oracle SDM Cloud's Registration ID to which the Management Cloud Engine (MCE) can connect
- Install, Configure, and Activate the MCE

Oracle SDM Cloud Deployment Process

The high-level process for deploying the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) includes the following steps. You will perform some steps in the Oracle Cloud and others on-premises.

1. Oracle Cloud—Contact your Oracle Cloud sales representative to establish a subscription for Oracle SDM Cloud and activate your Oracle Cloud and Oracle Identity Cloud Services accounts.
2. Oracle Cloud—Login to Oracle SDM Cloud and obtain the Identity and Access Management (IAM) for inputs to Management Cloud Engine (MCE).
3. Oracle Cloud—While logged into Oracle SDM Cloud, create a site. Once created, select the site to edit and obtain the generated site Registration ID to use for MCE inputs.
4. On premises—Install the Management Cloud Engine (MCE) with the install, activate, and configuration scripts provided in the software download.
   The following diagram illustrates the deployment process and shows the parameters you need to set in each Oracle SDM Cloud component to establish the service.



Establish an Oracle SDM Cloud Service Subscription

To obtain the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) service, contact Oracle Cloud Sales to purchase a Cloud Services Agreement and the Oracle SDM Cloud service description.

Establishing an Oracle SDM Cloud service subscription is a multi-step process. Use the information provided in the following links to guide you through the process.

1. Go to https://docs.oracle.com/en/cloud/paas/identity-cloud/index.html for information about how to purchase a subscription to Oracle SDM Cloud.
2. Go to https://docs.oracle.com/en/cloud/get-started/subscriptions-cloud/index.html for information about how to activate your Oracle Applications account order.

3. Go to https://www.oracle.com/webfolder/technetwork/tutorials/obe/cloud/getting_started/create_cloud_account_admin_obe/create_cloud_acc_admin.html for information about how to manage your Oracle Cloud services.

Obtain the IAM Inputs for MCE

To connect the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) to the Management Cloud Engine (MCE), you must login to the Oracle SDM Cloud and obtain the Identity and Access Management (IAM) parameters.

1. Log on to the Oracle SDM Cloud using the URL that you received in your "Welcome" email from Oracle.
2. Browse to **Security Manager**, **IAM**.

   The Identity Access Management page displays showing the unique identifiers for the following components:

   - Oracle SDM Cloud FQDN
   - Oracle SDM Cloud Tenant ID
   - IDCS FQDN
   - IDCS Tenant ID
   - MCE IDCS Client ID
   - MCE IDCS Client Secret

Create a Site and Retrieve Generated ID for MCE Inputs

To connect the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) to the Management Cloud Engine (MCE), you must login to the Oracle SDM Cloud, create a Site, and retrieve the Generated ID for MCE inputs.

1. Logon to the Oracle SDM Cloud using the URL that you received in your "Welcome" email from Oracle.
2. Browse to **Device Manager**, **Sites**.

   The Sites page displays.
3. Click **Add**, enter a **Site name** and optionally a **Description** and click **Apply**.

   The Sites page displays showing the newly added Site.
4. Select the Site and click **Edit**.

   The Edit Site page displays with a Site ID with a unique identifier.
5. Use the Site ID when adding your MCE in Oracle SDM Cloud.

Install and Configure the MCE

The Management Cloud Engine (MCE) installation procedure requires the archive file containing the installation and configuration scripts that you downloaded from Oracle onto your host hardware. Oracle recommends running the two scripts consecutively in one session the first time you install the MCE. For that reason, this procedure includes the prerequisites and steps for running both scripts.

MCE Installation Prerequisites
Do the following before performing the procedure.

System Prerequisites

- Ensure that the host meets Operation System and resource requirements.
- Operating System Oracle Linux 8.8 or higher or Red Hat compatible Kernel

> **Note:**
>
> The latest version of Oracle SDM Cloud is not tested on Red Hat Enterprise Linux (RHEL) and Oracle recommends using the base version of Linux on the 8.x release.

- Install Perl V5.26.3 or higher on the host.
- Install Podman v4.4.1 or higher on the host.
- Ensure that you have Root access.
- Download the archive file (mce-<version>.tgz) from My Oracle Support (MOS) to the host server. This .tgz file includes all necessary scripts.

Installation Script Prerequisites

- Ensure that there is no MCE installation existing on the hardware. See the last step in this procedure for instructions.
- Ensure that you have root access.

Configuration Script Prerequisites

- Note the MCE WAN IP, MCE LAN IP, and MCE name.
- Navigate to Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) **Security Manager**, **IAM** page to configure IAM parameters.

Procedure

The following procedure provides instructions for installing the MCE initially and for re-installing the MCE later, for example, in a disaster recovery scenario.

> **Note:**
>
> Before re-installing, you must first uninstall the existing MCE.

1. Unpack the mce-<version>.tgz archive.

   ```
   tar -xvzf mce-<version>.<build>.tgz
   ```

   The system creates the mce-<version> directory and copies the unpacked files there in the following directory tree.

   ```
   mce-<version>.<build>/
   mce-<version>.<build>/mce/
   mce-<version>.<build>/mce/perl/
   mce-<version>.<build>/mce/perl/activate.pl
   mce-<version>.<build>/mce/perl/deactivate.pl
   mce-<version>.<build>/mce/perl/uninstall.pl
   mce-<version>.<build>/mce/perl/config.pl
   ```

```
mce-<version>.<build>/mce/perl/changeloglevel.pl
mce-<version>.<build>/mce/perl/showversion.pl
mce-<version>.<build>/mce/perl/collectinfo.pl
mce-<version>.<build>/mce/perl/helper.pl
mce-<version>.<build>/mce/cfg/
mce-<version>.<build>/mce/cfg/mce.properties
mce-<version>.<build>/mce/cfg/version
mce-<version>.<build>/mce/cfg/log4j2.xml
mce-<version>.<build>/mce/cfg/log4j2_debug.xml
mce-<version>.<build>/mce/ssl/
mce-<version>.<build>/mce/logs/
mce-<version>.<build>/mce/img/
mce-<version>.<build>/mce/img/mce.tar
mce-<version>.<build>/install.pl
mce-<version>.<build>/upgrade.pl
```

2. Log on to the server at root. Ensure the user logging in has the proper Linux permissions.
3. Run the **install.pl** script.

```
./install.pl
--------------------------------------------------------------------------------
----
Oracle Cloud Communications Service, (c) 2020 Oracle
MCE v1.0.0 install.pl @ 2020-07-14 12:00:59
--------------------------------------------------------------------------------
----
Checking pre-conditions...
Ok.
Proceed with install (y/n) : y
Installing mce to /opt/oracle ...
Installation successful.
[abcd@acme123 mce-1.0.0]$
```

The system checks for an existing MCE instance in Podman.

- If it exists, the script execution stops and you must uninstall it.

This creates the /oracle/mce directory under /opt. (If an oracle directory already exists, the install creates an mce directory only.)

4. From `/opt/oracle/mce/perl`, run the **config.pl** script and configure the attributes according to your environment.

```
--------------------------------------------------------------------------------
----
Oracle Cloud Communications Service, (c) 2020 Oracle
MCE v23.2.0.0.0  @ 2023-06-01 10:46:01
--------------------------------------------------------------------------------
----
Checking pre-conditions...
The following inputs are required for MCE to register with Oracle SDM
Cloud:
MCE Host Name               : cgbu-phx-347
Host WAN IP Address         : 100.77.50.195
Host LAN IP Address         : 10.196.248.92
Oracle SDM Cloud FQDN       : <From IAM page>
```

```
Oracle SDM Cloud tenant ID  : <From IAM page>
IDCS tenant ID              : <From IAM page>
MCE IDCS client secret      : <From IAM page>
Oracle SDM Cloud Site ID    : <From Device manager → Sites>
Enable proxy(y/n)           : y
Proxy server address        : 100.77.50.145
Proxy server port           : 3128
-----------------------------------------------------------------------
The following inputs are required for MCE KeyStore configuration:
MCE TLS Key Store Password   :
MCE TLS Key Store Password   confirm :
-----------------------------------------------------------------------
The following inputs are required for MCE operation:
Trap Receiver Port        : 162
-----------------------------------------------------------------------
Ready to process inputs
Proceed with configuration (y/n) : y
```

MCE Host Name	Set the local host name.
Host WAN IP Address	Set the host WAN IP address. (Provided by the customer)
Host LAN IP Address	Set the host LAN IP address. (provided by the customer)
Oracle SDM Cloud FQDN	Set the Oracle SDM Cloud FQDN from the **Security Manager**, **IAM** page of Oracle SDM Cloud.
Oracle SDM Cloud Tenant ID	Set the Oracle SDM Cloud Tenant ID from the **Security Manager**, **IAM** page of Oracle SDM Cloud.
IDCS Tenant ID	Set the IDCS Tenant ID from the **Security Manager**, **IAM** page of Oracle SDM Cloud.
IDCS FQDN	Set the IDCS FQDN from the **Security Manager**, **IAM** page of Oracle SDM Cloud.
MCE IDCS Client ID	Set the MCE IDCS FQDN from the
MCE IDCS Client Secret	Set the MCE IDCS Client Secret from the **Security Manager**, **IAM** page of Oracle SDM Cloud.
Oracle SDM Cloud Site ID	Set the site ID generated from Oracle SDM Cloud.
Enable Proxy	Enter **y** for yes and **n** for no.
Proxy Server Address	Set proxy server address, if proxy is enabled.
Proxy Port	Set proxy port.
Trap Receiver Port	Set the listening port for SNMP trap receiver on local host.

This creates a mce.properties file under `/opt/oracle/mce/cfg`, which contains all of the information entered in config.pl.

5. From `/opt/oracle/mce/perl`, run the **activate.pl** script to activate the MCE.

```
./activate.pl
--------------------------------------------------------------------------------
----
Oracle Cloud Communications Service, (c) 2020 Oracle
MCE v1.0.0  @ 2020-07-14 12:49:22
--------------------------------------------------------------------------------
----
Checking pre-conditions...
Ok.
MCE tomcat port:7070, Trap receiver port:162
Proceed with activate (y/n) : y
Activating container mce...
Start to run container mce, image id fb90a2c4b930 ...
Container mce with image id fb90a2c4b930 started.
Activation successful!
```

6. (Optional) Check your work with Podman.

   a. At the prompt type: **podman images**, and press Enter to list the MCE instances. Under TAG look for <version> <build> which is the new installation. The following code block shows an example.

```
% podman images
REPOSITORY                    TAG               IMAGE ID
CREATED    SIZE
cne-repos1.us.oracle.com:7744/apps/cgbu/ums/mce 1.0.0 fb90a2c4b930 4
days ago 434MB
```

   b. At the prompt type: **podman ps**, and press Enter to list the running images. In the list, under "NAMES", look for "mce". Under STATUS, look for the newest one of each. The following code block shows an example.

```
% podman ps
CONTAINERID  IMAGE        COMMAND    CREATED      STATUS  PORTS NAMES
ed6f90a7993d fb90a2c4b930 "/bin/bash ./start.sh"  3 days ago     mce
```

Traffic Flow and Firewall Port Recommendations

The following table provides traffic flow and firewall port recommendations for communication between the Management Cloud Engine (MCE) and Network Functions (NFs).

Port Number	Protocol	Service	Configurable	Purpose
161	UDP	SNMP	Y	SNMP traffic between the MCE and the NF.
162	UDP	SNMP	Y	SNMP trap reporting from the device to the MCE server.
22	TCP	SFTP/SSH	N	Used for secure file transfer (for example, software upgrades, Route Manager, and LRT updates) and SSH sessions between MCE and southbound NFs.

Port Number	Protocol	Service	Configurable	Purpose
3001/3000	TCP	ACP/ACLI	N	Used by the MCE to communicate with all versions of a NF.
443	TCP	HTTPS	N	Usec by MCE to communicate with Media Engines (MEs).

Upgrading the MCE

The Management Cloud Engine (MCE) upgrade procedure requires the archive file containing the installation and configuration scripts that you downloaded from Oracle onto your host hardware. For more information on the installation and configuration scripts and prerequisites, see "Install and Configure the MCE".

Use the following procedure to upgrade the MCE using the upgrade.pl.

1. Log onto the server as a root user and ensure the user logging in has the proper Linux permissions.
2. Shut down the existing version of MCE by running the **deactivate.pl** script.

   ```
   /opt/oracle/mce/perl/deactivate.pl
   ```

3. Install the latest version of the MCE (provided by development) from MOS.
4. Unpack the new **mce-<version>.<build>.tgz** archive.

   ```
   [root@cgbu-phx-604 perl]# tar -xvf  mce<version>.<build>.tgz
   ```

5. Run the **upgrade.pl** script (under the new **mce-<version>.<build>**/) to upgrade to the latest version.

   ```
   [root@cgbu-phx-604 perl]# ./upgrade.pl
   ```

   The upgrade.pl script displays a banner with information about the new MCE version.

   The MCE performs the following validations to ensure the upgrade is supported and valid:

   - Validation that an existing version of MCE exists under `/opt/oracle/mce`.
   - Validation that MCE is not currently activated.
   - Validation that the upgrade path is supported.
6. Once validation is complete, the user is prompted to continue. Either continue or opt out to abort the upgrade.
7. Run the **activate.pl** script under **/opt/oracle/mce/perl** script to activate the new version of MCE .

   ```
   [root@cgbu-phx-604 perl]# ./activate.pl
   ```

Persistent data files, including configuration properties and artifacts generated when MCE registers with Oracle SDM Cloud, are copied from the old installation of MCE to the new installation. During installation, the old installation of MCE gets moved from `/opt/oracle/mce` to `/opt/oracle/mce.bak` and the new version is moved to `/opt/oracle/mce`.

Use the following procedure to upgrade the MCE performing a fresh installation.

From Oracle Linux 7:

1. Log onto the server as a root user and ensure the user logging in has the proper Linux permissions.
2. Shut down the existing version of MCE by running the deactivate.pl script.

   ```
   /opt/oracle/mce/perl/deactivate.pl
   ```

3. Upgrade the operating system from Oracle Linux 7 to Oracle Linux 8.8.
   From Oracle Linux 8:
4. Log onto the server as a root user and ensure the user logging in has the proper Linux permissions.
5. Unpack the new mce-<version>.<build>.tgz archive. The system installs the files in the */opt/oracle/mce* directory.
6. Run the **install.pl** script.

   ```
   [root@cgbu-phx-604 mce-24.1.0.0.0]# ./install.pl
   ------------------------------------------------------------------------
   ----
   Oracle Cloud Communications Service,(c) 2020 Oracle
   MCE v24.1.0.0.0 install.pl @ 2023-12-10 16:58:00
   ------------------------------------------------------------------------
   ----
   Checking pre-conditions...
   Ok.
   Proceed with install (y/n) : y
   Installing mce to /opt/oracle ...
   Installation successful.
   ```

   Upon installation, the system checks for an existing MCE instance in Podman and if one exists, the script execution stops and you must uninstall the MCE.
   This creates the /oracle/mce directory under /opt. If an Oracle directory already exists, the install creates a MCE directory only.
7. Run the **config.pl** script from the /opt/oracle/mce/perl directory and configure the attributes according to your environment.

   ```
   [root@cgbu-phx-604 perl]# ./config.pl
   ------------------------------------------------------------------------
   ----
   Oracle Cloud Communications Service, (c) 2020 Oracle
   MCE v24.1.0.0.0  @ 2023-12-10 16:58:35
   ------------------------------------------------------------------------
   ----
   Checking pre-conditions...
   The following inputs are required for MCE to register with Oracle SDM
   Cloud:
   MCE Host Name               : cgbu-phx-604
   Host WAN IP Address         : 100.77.50.195
   Host LAN IP Address         : 10.196.248.92
   Oracle SDM Cloud FQDN       : <From IAM page>
   Oracle SDM Cloud tenant ID  : <From IAM page>
   ```

```
IDCS tenant ID              : <From IAM page>
IDCS FQDN                   : <From IAM page>
MCE IDCS client ID          : <From IAM page>
MCE IDCS client secret      : <From IAM page>
Oracle SDM Cloud Site ID    : <From Device manager     → Sites>
Enable proxy (y/n)          : y
Proxy server address        : 100.77.50.145
Proxy server port           : 3128
-----------------------------------------------------------------
The following inputs are required for MCE KeyStore configuration:
MCE TLS Key Store Password  :
MCE TLS Key Store Password  confirm  :
-----------------------------------------------------------------
The following inputs are required for MCE operation:
Trap Receiver Port          : 162
-----------------------------------------------------------------
Ready to process inputs
Proceed with configuration (y/n)    : y
Encrypting data ...
Generating local mce.properties...
Success.
```

This creates a mce.properties file under /opt/oracle.mce/cfg, which contains all of the information entered in config.pl.

8. Login to the Oracle SDM Cloud interface and delete the registered MCE from **Device Manager**. For more information, see "Device Manager" in the *User Guide*.
9. Run the **activate.pl** script from */opt/oracle.mce/perl* to activate the MCE.

```
[root@cgbu-phx-604 perl]# ./activate.pl
-------------------------------------------------------------------------------
----
Oracle Cloud Communications Service, (c) 2020 Oracle
MCE v24.1.0.0.0  @ 2023-12-10 17:01:15
-------------------------------------------------------------------------------
----
Checking pre-conditions...
Ok.
MCE tomcat port:7070, Trap receiver port:2000
Proceed with activate (y/n) : y
Activating container mce...
Start to run container mce, image id
          1cb6109fc65a ...
Container mce with image id 1cb6109fc65a started.
Activation successful!
```

10. Optionally, you can check your work with Podman.
    - List the MCE instances by typing **podman images** at the prompt and pressing **Enter**. Under TAG, look for <version> <build> to see the new installation. The following code block shows an example:

```
% podman images
REPOSITORY CREATED   SIZE     TAG     IMAGE ID
```

```
cne-repos1.us.oracle.com:7744/apps/cgbu/ums/mce 1.0.0 fb90a2c4b930 4
days ago 434MB
```

- List the running images by typing **podman ps** at the prompt and pressing **Enter**. In the list, under NAMES, look for mce. Under STATUS, look for the newest images. The following code block shows an example:

```
% podman ps
CONTAINERID   IMAGE   COMMAND   CREATED   STATUS   PORT NAMES
% podman psIMAGECOMMANDCREATEDSTATUSPORTS
ed6f90a7993dfb90a2c4b930"/bin/bash./start.sh" 3 days ago mce
```

Configure MCE Behind NAT or Firewall

Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) allows you to configure the Management Cloud Engine (MCE) to operate behind a Network Address Translation (NAT) or a firewall. Oracle SDM Cloud contacts the MCE using the value for the **mce.ip** in **mce.properties** or **wan-ip** on setting up *./config.pl* configuration.

The MCE supplies the **mce.ip** value when it registers with Oracle SDM Cloud. You can set the **mce.ip** value as a static IP address that maps to the NAT public interface or firewall. For example:

```
mce.ip : 10.x.x.x
```

Oracle SDM Cloud always uses port 443 for these connections, requiring any device placed between the MCE and Oracle SDM Cloud to dedicate port 443 to the MCE for all possible IP addresses.

A

Changes to IDCS and OCI IAM Operations

Oracle recently merged the Identity Cloud Services (IDCS) operations into the native Oracle Cloud Infrastructure (OCI) and Identity Access Management (IAM) service, no longer offering IDCS as a separate service. The following information describes the changes and what they mean to both IDCS and OCI IAM users.

New Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) customers will manage their tenancies through OCI Identity Domain.

Oracle begins migrating existing IDCS instances to the new OCI Identity Domain model. Existing customers can manage their tenancies through IDCS until their migration completes.

Tenancy management through IDCS ends. All customers manage their Oracle SDM Cloud tenancies through OCI Identity Domain from this date forward.

> **Note:**
>
> The updated service will not be deployed to all regions at once. Banners on the IDCS and OCI sign on screens will indicate when identity domains are enabled in your region and where to find more information.

OCI Identity Domains: What Oracle IDCS Customers Need to Know

Oracle recently merged the capabilities of Oracle Identity Cloud Service (IDCS) into the native Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) service. As a native OCI service, customers will see improved performance and scale, immediate availability in more global regions, and a new cross-region disaster recovery feature.

What is OCI Identity Domain?

Oracle Cloud Infrastructure (OCI) Identity Domain is the access control plane for Oracle Cloud. An identity domain is a container for managing users and roles, federating and provisioning of users, secure application integration through Oracle Single Sign-On (SSO) configuration, and SAML and OAuth based Identity Provider administration.

For more information about Identity Domains, see IAM with Identity Domains and Managing Identity Domains.

What Changed for IDCS and Identity Domain?

Oracle recently made new features and capabilities available for the Oracle Cloud Infrastructure (OCI) Identity Domain service. As part of the upgraded service, Oracle migrated the features and functionality of the existing Oracle Identity Cloud Service (IDCS) into OCI Identity Domain.

OCI Identity Domain supports the following core functions:

- OCI Identity Domain continues to serve as the critical access control plane for Oracle Cloud.
- OCI Identity Domain supports a wide range of enterprise Identity Domain use cases for complex, hybrid IT environments.
- OCI Identity Domain provides a developer-friendly Identity Domain engine for custom and consumer applications.

By unifying administration and user experiences across key Identity Domain functions, the new service helps simplify administration, reduce cost of ownership, and improve time-to-value. The service spans Cloud and on-premises, providing the flexibility to handle a wide variety of Identity Domain use cases across employee, partner, and consumer scenarios. As a native service of OCI, you can use the diverse feature set of OCI Identity Domain across any geography.

The updated OCI Identity Domain service introduces Identity Domains. Oracle will migrate your existing IDCS instances, called stripes, to Identity Domain instances. Existing Oracle SDM Cloud customer will see their access to IDCS portal diverted to Identity Domain. See Identity Domains.

- Identity domains are the next generation of IDCS instances. Each existing IDCS instance is now an identity domain.
- Each OCI identity domain represents a stand-alone identity and access management solution.
- Identity domains each have their own settings, configurations, and security policies to ensure optimal security.

How Does The Upgrade to OCI Identity Domain Impact Existing Identity Cloud Service Instances?

None of the existing Oracle Identity Cloud Service (IDCS) features or functionality will change as part of the migration to Oracle Cloud Infrastructure (OCI) Identity Domain. Oracle will merge IDCS into OCI Identity Domain, where it will become an integral component.

As a native service of OCI, OCI Identity Domain takes advantage of infrastructure that offers consistently high performance, enterprise scalability, availability in all the Oracle global cloud regions, and an extensive set of regulatory compliance and security certifications.

The OCI Identity Domain service will serve all current IDCS use cases, including providing a standalone Identity as a Service (IDaaS) solution for managing access across numerous third-party applications. IDCS customers migrating to OCI Identity Domain do not need to consume any other OCI services to continue using the services previously provided by IDCS.

Oracle will prepare each IDCS instance to be managed through the OCI console as an identity domain. All existing configurations, security settings, user and group populations, and access assignments will continue to exist with no interruption.

The system will re-route IDCS Administrators from the existing IDCS administrative console to the Identity Domain console where IDCS instances will be listed as OCI Identity Domains. Administrators can browse to their list of domains and will be able to manage domains in a way similar to the current IDCS console experience. See Managing Identity Domains.

The upgrade makes no changes to pricing, metering, or included features for Oracle SDM Cloud instances. You will continue to use your existing Oracle SDM Cloud entitlements and any others you are entitled to use.

What is New in OCI Identity Domain for IDCS Customers?

The migration to Oracle Cloud Infrastructure (OCI) Identity Domain and the introduction of identity domains adds Oracle Identity Cloud Service (IDCS) features natively to the OCI Identity Domain service.

- Single-Point of Identity Domain Management—Identity administration is now available through the OCI Admin console under Identity & Security, Domains. Administrators will see the same set of features and functionality that they are used to in IDCS for managing users, groups, applications, security settings, and other configurations.
- No Impact for Existing Users, Policies, Configuration, or Access—The OCI Identity Domain upgrade maintains all existing security policies, configurations, and user populations. Expect no impact to security settings or to the user experience. Oracle did not remove functionality or change any policy configurations.
- Disaster Recovery—In most regions, OCI Identity Domain now provides a cross-region disaster recovery feature for recovering identity domain data in a scenario where an entire OCI region becomes unavailable. The disaster recovery feature is included and does not require any changes or updates to existing applications.

Post-Upgrade Guidance

Administrative Access

Identity Cloud Service (IDCS) Administrators become Identity Domain Administrators upon migration. Identity Domain Administrators get full access to their identity domains. Be sure that use of the OCI Administrators group is consistent with your security policies.

The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) Administrators group grants access to many aspects of the service. Oracle recommends reserving the Oracle SDM Cloud Administrators group for emergency scenarios, rather than for day-to-day administration of the tenancy. Best practices include

- setting a complex password on the account.
- storing the Administrators account credentials safely in a secure location such as a physical safe.

Where Can I Get More Information?

Use the following resources to find more information about Oracle Cloud Infrastructure (OCI) and Identity Domains.

- IAM with Identity Domains
- oracle.com
- In North America, call +1.800.ORACLE1 (672-2531)
- Outside North America, find your local Oracle office at oracle.com/contact

OCI Identity Domains: What OCI Customers Need to Know

Oracle recently merged the capabilities of Oracle Identity Cloud Service (IDCS) into the native Oracle Cloud Infrastructure (OCI) service. The merger provides OCI customers with a rich,

enterprise-class set of identity and access management features for use with OCI and Oracle Cloud applications.

What is OCI Identity Domain?

Oracle Cloud Infrastructure (OCI) Identity Domain is the access control plane for Oracle Cloud. An identity domain is a container for managing users and roles, federating and provisioning of users, secure application integration through Oracle Single Sign-On (SSO) configuration, and SAML and OAuth based Identity Provider administration.

For more information about Identity Domains, see IAM with Identity Domains and Managing Identity Domains.

What Changed for Oracle SDM Cloud?

Oracle recently made new features and capabilities available for the Oracle Cloud Infrastructure Identity (OCI) and Identity Domain service. As part of the upgraded service, Oracle merged all features and functionality of the existing Oracle Identity Cloud Service (IDCS) into OCI Identity Domain.

OCI Identity Domain supports the following core functions:

- OCI Identity Domain continues to serve as the critical access control plane for Oracle® Session Delivery Management Cloud (Oracle SDM Cloud).
- OCI Identity Domain supports a wide range of enterprise Identity Domain use cases for complex, hybrid IT environments.
- OCI Identity Domain provides a developer-friendly Identity Domain engine for custom and consumer applications.

Identity Domain is also flexible enough to handle a wide variety of Identity Domain use cases across employee, partner, and consumer scenarios.

The updated OCI Identity Domain service introduces Identity Domains. Oracle will migrate your existing IDCS instances, called stripes, to Identity Domain instances. Existing Oracle SDM Cloud customer will see their access to IDCS portal diverted to Identity Domain. No changes are required to applications, users, or groups in domains that formerly existed as IDCS instances or to local users in OCI tenancies. See Identity Domains.

Identity Domain characteristics include:

- Each OCI Identity Domain represents a stand-alone identity and access management solution.
- Each identity domain represents a different user population, but certain use cases may require users to exist in multiple domains.
- Identity domains each use their own settings, configurations, and security policies to ensure optimal security.
- OCI Identity Domain is an Identity as a Service (IDaaS) solution with the flexibility to cover virtually any Identity Domain use cases across employees, partners, and consumers.

How Do the Changes to OCI IAM Impact Existing OCI Tenancies?

OCI administrators are already be familiar with the Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) service that enables authentication into OCI and management of access entitlements for OCI resources by way of OCI IAM policies. Many customers choose

to use Oracle Identity Cloud Service (IDCS) to also enable more advanced IAM deployments, which creates an additional layer of IAM to manage and sometimes incurs additional cost.

The introduction of identity domains adds the following features natively to the OCI IAM service to help simplify administration and operational management.

- Powerful IAM Functionality at No Additional Cost—Oracle brought all the enterprise IAM capabilities of IDCS into OCI IAM natively. IAM functionality such as advanced authentication techniques and user life cycle management are now natively available and included in your existing OCI tenancies for use with your subscribed* Oracle services.

> **Note:**
>
> *Upgrades are available to provide IAM support beyond subscribed Oracle services.

- Single-Point Authentication—The OCI IAM upgrade simplifies the OCI sign-on screen.
- Single-Point of IAM Management—Customers who previously used IDCS with OCI tenancies may notice simplified administration by way of a single pane for all users. Identity administration is now available through the OCI Admin console under Identity & Security, Domains.
- No Impact for Existing Users, Policies, Configuration, or Access—The OCI IAM upgrade maintains all existing security policies, configurations, and user populations. Expect no impact to security settings or to the user experience. Oracle did not remove functionality or change any policy configurations.
- Disaster Recovery—OCI IAM now provides a cross-region disaster recovery feature for recovering identity domain data in a scenario where an entire OCI region becomes unavailable. The disaster recovery feature is included and does not require any changes or updates to existing applications.

Post-Upgrade Guidance

Administrative Access

Identity Cloud Service (IDCS) Administrators become Identity Domain Administrators upon migration. Identity Domain Administrators get full access to their identity domains. Be sure that use of the OCI Administrators group is consistent with your security policies.

The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) Administrators group grants access to many aspects of the service. Oracle recommends reserving the Oracle SDM Cloud Administrators group for emergency scenarios, rather than for day-to-day administration of the tenancy. Best practices include

- setting a complex password on the account.
- storing the Administrators account credentials safely in a secure location such as a physical safe.

Where Can I Get More Information?

Use the following resources to find more information about Oracle Cloud Infrastructure (OCI) and Identity Domains.

- IAM with Identity Domains

- oracle.com
- In North America, call +1.800.ORACLE1 (672-2531)
- Outside North America, find your local Oracle office at oracle.com/contact