

Oracle® Communications Offline Mediation Controller System Administrator's Guide



Release 15.0
F89034-01
December 2023

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

ORACLE®

Copyright © 2017, 2023, Oracle and/or its affiliates.

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

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

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

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

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

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

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

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

Contents

Preface

Audience	vii
Documentation Accessibility	vii
Diversity and Inclusion	vii

1 Configuring Offline Mediation Controller

Configuring the ProcessControl Script to Run Components	1-1
Starting and Stopping Offline Mediation Controller	1-2
Starting and Stopping Offline Mediation Controller by Using the ProcessControl Script	1-2
Starting and Stopping Node Manager	1-3
Starting and Stopping Administration Server	1-3
Starting Administration Client	1-4
Changing the IP Address of a Mediation Host	1-4
Modifying Attribute Names Displayed in Record Editor	1-5
Managing Ports	1-6
Managing Mediation Host Security	1-6
Setting Up an Offline Mediation Controller Administration Server Firewall	1-6
Defining Administration Server Port Number	1-7
Defining Administration Client Port Numbers	1-7
Configuring Node Manager Memory Limits	1-7
Configuring the Java Virtual Machine Memory Usage when Running Administration Client	1-8
Configuring the Java Virtual Machine Memory Usage when Running Administration Server	1-8
Using the Offline Mediation Controller Shell Tool	1-9
About SNMP Trap Hosts	1-11

2 Managing Offline Mediation Controller Security

About Offline Mediation Controller Security	2-1
About Secure Communication Using Secure Sockets Layer	2-1
Creating Secure Connections	2-1
Enabling and Disabling SSL Mode	2-2
Securely Connecting Administration Server to Other Node Manager Instances	2-2

Configuring Session Timeout Between Administration Server and Administration Client	2-3
About Users in Offline Mediation Controller	2-3
About Managing Users in Offline Mediation Controller	2-5
About Managing the Administrator User Password in Oracle Unified Directory	2-5
About Managing Passwords	2-5
Storing Passwords	2-5
About the Default Password Policy	2-5
Modifying the Default Password Policies	2-6

3 Managing Nodes Using NMShell Command-Line Components

Logging Into NMShell	3-1
Starting Nodes	3-2
Stopping Nodes	3-2
Deleting Nodes	3-3
Adding Node Routes	3-3
Adding a Round-Robin Node Route	3-3
Adding a Multicast Node Route	3-4
Adding a Modulus Node Route	3-4
Adding a Directed Node Route	3-5
Deleting an Existing Node Route	3-6
Adding Mediation Hosts to Node Manager	3-6
Compiling the NPL Rule File	3-7
Changing Existing Node-Level Configuration	3-7
Adding Back-End Only Configurations at Node Level	3-8
Checking Node Status	3-9
Listing Node ID and Type	3-9
Checking NMShell Command Status	3-9
Importing and Exporting Node Configuration	3-10
Importing Node Configuration and Node Customization	3-10
Exporting Node Configuration and Node Customization	3-11
Incrementally Import Node Chain Configurations and Customizations	3-12
Incrementally Export Node Chain Configurations and Customizations	3-13

4 Monitoring Offline Mediation Controller

Monitoring Node Performance in Administration Client	4-1
Monitoring Node Performance with Prometheus and Grafana	4-1
Configuring the Node Manager Metric Endpoint	4-2
Monitoring System Processes	4-2
Using the Disk Status Monitor	4-3

Using the Memory Monitor	4-3
Using the CPU Usage Monitor	4-4
Monitoring How Offline Mediation Controller Components are Running	4-4
Using Server Monitoring	4-5
Using Logs to Monitor Offline Mediation Controller Components	4-8
Types of Log Files	4-8
Log Files for Offline Mediation Controller Components	4-8
Log Files for Offline Mediation Controller Nodes on the Mediation Host	4-8
Location of Log Files	4-8
Default Log File Locations	4-9
About the Logger Properties Files	4-9
Setting the Reporting Level for Logging Messages	4-10

5 Backing Up and Restoring Offline Mediation Controller

About Backup and Restore Options	5-1
About Standard Configuration Backups	5-1
About Complete System Backups	5-2
Backing Up a Standard Configuration	5-2
Backing Up a Complete System	5-3
Restoring Offline Mediation Controller	5-3
Restoring a Standard System Configuration	5-4
Restoring a Complete System Backup	5-4
Preserving Data When No Backup Exists	5-5
Backing Up and Restoring NAR Files	5-6
Backing Up NAR Files	5-7
Restoring NAR Files	5-7

6 Troubleshooting Offline Mediation Controller

Troubleshooting Checklist	6-1
Using Error Logs to Troubleshoot Offline Mediation Controller	6-1
Getting Help for Offline Mediation Controller Problems	6-2
Common Problems and Their Solutions	6-2
Problem: ps: illegal option	6-2
Problem: keytool error: java.io.FileNotFoundException While Creating Administration Server Certificate	6-3
Problem: keytool error: java.io.FileNotFoundException While Creating Node Manager Certificate	6-3
Problem: com.maverick.ssh.SshException When FTP is Used in Collection or Distribution Cartridge Pack	6-4

A Offline Mediation Controller Directory Structure and Contents

Directory Structure and Contents

A-1

Preface

This guide provides instructions for administrating Oracle Communications Offline Mediation Controller.

Audience

This guide is intended for system administrators, database administrators, and developers who maintain and manage Offline Mediation Controller.

This guide assumes that you:

- Have a working knowledge of the Linux operating system
- Understand your network configuration and the equipment from which Offline Mediation Controller collects data

Documentation Accessibility

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

Access to Oracle Support

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

Diversity and Inclusion

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

1

Configuring Offline Mediation Controller

Learn how to start, stop, and manage Oracle Communications Offline Mediation Controller components.

Topics in this document:

- [Configuring the ProcessControl Script to Run Components](#)
- [Starting and Stopping Offline Mediation Controller](#)
- [Changing the IP Address of a Mediation Host](#)
- [Modifying Attribute Names Displayed in Record Editor](#)
- [Managing Ports](#)
- [Managing Mediation Host Security](#)
- [Setting Up an Offline Mediation Controller Administration Server Firewall](#)
- [Configuring Node Manager Memory Limits](#)
- [Configuring the Java Virtual Machine Memory Usage when Running Administration Client](#)
- [Configuring the Java Virtual Machine Memory Usage when Running Administration Server](#)
- [Using the Offline Mediation Controller Shell Tool](#)
- [About SNMP Trap Hosts](#)

Configuring the ProcessControl Script to Run Components

You can use the **ProcessControl** script to start or stop Offline Mediation Controller components. To do so, you must first configure the **offline_mediation.conf** file to include the components that are running, the installation they run from, and the ports and IP addresses they use. The **ProcessControl** script uses the information in the **offline_mediation.conf** file to start or stop multiple servers from multiple Offline Mediation Controller installations.

To configure the **ProcessControl** script to run components:

1. Open the *OMC_home/offline_mediation/offline_mediation.conf* file in a text editor, where *OMC_home* is the directory in which Offline Mediation Controller is installed.
2. Specify the Offline Mediation Controller components to start or stop using the following syntax:

```
daemon_name:OMC_home:port:[IP_Address]:[Y|N]
```

where:

- *daemon_name* is the name for the Offline Mediation Controller component:
 - **admnsvr** (Administration Server)
 - **nodemgr** (Node Manager)

- *port* is the port on which the server component runs. The port number range is between **49152** and **65535**.
- *IP_Address* is the IP address for the host computer to start, stop, and monitor multiple servers from multiple Offline Mediation Controller installations.
- **Y/N** indicates whether this component is started when the system starts or not.

For example:

```
admsvr:/OMC_home:55105::Y  
nodemgr:/OMC_home:55109::Y
```

3. Save and close the file.

Starting and Stopping Offline Mediation Controller

You can start and stop Offline Mediation Controller by using the following methods:

- The **ProcessControl** script. See "[Starting and Stopping Offline Mediation Controller by Using the ProcessControl Script](#)".
- The individual component commands. See:
 - [Starting and Stopping Node Manager](#)
 - [Starting and Stopping Administration Server](#)
 - [Starting Administration Client](#)

Starting and Stopping Offline Mediation Controller by Using the ProcessControl Script

You can start or stop Offline Mediation Controller by using the **ProcessControl** script. This script preserves the node status when you restart Node Manager.



Note:

Before running the **ProcessControl** script, ensure that you have run the **configure** script. For more information, see "Adding Offline Mediation Controller Service to System Startup" in *Offline Mediation Controller Installation Guide*.

To start and stop Offline Mediation Controller by using the **ProcessControl** script:

1. Go to the *OMC_home/bin* directory.
2. Run the following command, which starts the Offline Mediation Controller components that are defined in the **offline_mediation.conf** file on the appropriate ports:

```
./ProcessControl start
```

3. Run the following command, which stops the Offline Mediation Controller components that are defined in the **offline_mediation.conf** file:

```
./ProcessControl stop
```

Starting and Stopping Node Manager

To start and stop Node Manager:

1. Go to the *OMC_home/bin* directory.
2. Run the following command, which starts Node Manager:

```
./nodemgr [-d | -f | -F | -j] [-p port] [-i IP_Address]
```

where:

- **-d** runs Node Manager in the background with debug output redirected to *OMC_home/log/nodemgr_port.out*.
This option uses a large amount of the CPU during its processes.
- **-f** runs Node Manager in the foreground.
- **-F** runs Node Manager in the foreground with debug output.
- **-j** runs Node Manager, with the just-in-time (JIT) compiler enabled, in the background with debug output redirected to *OMC_home/log/nodemgr_port.out*.
- **-p port** runs Node Manager on *port*.
- **-i IP_Address** specifies the IP address of the host computer on which Node Manager is installed. Use this parameter to start Node Manager installed on multiple computers.

If you run this command with no options, Node Manager starts in the background with no debug output.

3. Run one of the following commands, which stops Node Manager:

- To shut down Node Manager:

```
./nodemgr -s [-p port]
```
- To stop the Node Manager process:

```
./nodemgr -k [-p port]
```

Starting and Stopping Administration Server

To start and stop Administration Server:

1. Go to the *OMC_home/bin* directory.
2. Run the following command, which starts Administration Server:

```
./adminsrv [-d | -f | -F | -j] [-x] [-p port] [-i IP_Address]
```

where:

- **-d** runs Administration Server in the background with debug output redirected to *OMC_home/log/adminsrv_port.out*.
- **-f** runs Administration Server in the foreground.
- **-F** runs Administration Server in the foreground with debug output.
- **-j** runs Administration Server, with the JIT compiler enabled, in the background with debug output redirected to *OMC_home/log/adminsrv_port.out*.

- **-x** disables user authentication.
- **-p port** runs Administration Server on *port*.
- **-i IP_Address** specifies the IP address to be used. It is used for multi-home systems.

If you run this command with no options, Administration Server starts in the background with no debug output.

3. Run one of the following commands, which stops Administration Server:

- To shut down Administration Server:

```
./adminsvr -s [-p port]
```

- To stop the Administration Server process:

```
./adminsvr -k [-p port]
```

Starting Administration Client

To start Administration Client:

1. Go to the *OMC_home/bin* directory.
2. Run the following command:

```
./gui [-d | -f | -F]
```

where:

- **-d** runs Administration Client in the background with debug output redirected to *OMC_home/log/gui_port.out*.
- **-f** runs Administration Client in the foreground.
- **-F** runs Administration Client in the foreground with debug output.

If you run this command with no options, Administration Client starts in the background with no debug options.

Changing the IP Address of a Mediation Host

You cannot change the IP address of a mediation host. Instead, you must remove the mediation host using that IP address, and reassign the IP address in the **offline_mediation.conf** file.

To change the IP address of a mediation host:

1. Write down the port number on which Offline Mediation Controller is connected.
2. In the Admin Client, delete the mediation host running on the Offline Mediation Controller workstation. To do so:
 - a. Delete nodes from the node chain from left to right. Otherwise, the dependence of one node on the previous node may prevent you from removing it.
 - b. Delete the mediation host.
3. Stop all Offline Mediation Controller related processes on the workstation.

4. For Linux machines, modify the **/etc/hosts** file with the new IP addresses and reboot the workstations. Restart the Offline Mediation Controller processes.
5. Look in the directory **OMC_home/offline_mediation** for the **offline_mediation.conf** file and replace any occurrences of the old IP address with the new IP address, where **OMC_home** is the directory in which you installed Offline Mediation Controller. Entering an IP address is optional in this file, so if the field has no value, you can leave it as is.
6. When you log in to the Administration Client, enter the new IP address of the workstation on which the **adminsvr** will be running.
7. In the Admin Client, add a mediation host for each workstation.
8. Restart the **adminsvr** and **nodemgr** processes on the workstation.
9. Restart all nodes on the workstation.
10. Ensure the file **SystemModel.cfg** in the Administration Server **config** directory (**OMC_home/config/adminserver**) have the new IP addresses and the correct port number.
11. Ensure the files **dataflowmap.cfg** and **nmPort** in the Node Manager **config** directory (**OMC_home/config/nodemgr**) have the new IP addresses and the correct port number.
12. Should this fail, stop all nodes, stop all processes (Client, **adminsvr**, **nodemgr**), and manually change all of the **config** files that have not been changed to the new IP addresses in the **config** directories.
13. Restart the **adminsvr** and **nodemgr** processes on the primary workstation (**nodemgr** only on the backup workstation).
14. Restart all of the nodes on the primary workstation (for backup workstations, restart the CC node only).

Modifying Attribute Names Displayed in Record Editor

By default, Record Editor uses the name **Network Accounting Record** for each NAR in your system. This means that each NAR will be displayed as **Network Accounting Record** in the left pane of the Record Editor window. When you expand a NAR, the NAR attribute names are listed.

To modify the attribute name:

1. Open the **OMC_home/datadict/Data_Dictionary.xml** file in a text editor, where **OMC_home** is the directory in which Offline Mediation Controller is installed.
2. Search for the attribute ID.
3. Change the **<Attr>** element to **<Attr tagForName="true">**.

The **tagForName** option overrides the default attribute name.

4. Set the **<Name>** element to the attribute name you want to display in Record Editor.

 **Note:**

If you leave the **<Name>** element blank, Record Editor displays the attribute ID as the attribute name.

5. Save the file.

6. Restart Record Editor.

Managing Ports

Offline Mediation Controller uses specific ports to send data to and to receive data from external devices and applications. Use the port information in [Table 1-1](#) when you are planning the network and configuring routers and firewalls that communicate between Offline Mediation Controller components.

Table 1-1 Port Information

Application	Protocol	Source	Source Port	Destination	Destination Port
GTP	UDP	GSN	1024 or higher	Offline Mediation Controller	3386
Open FTP and FTP	TCP	MSC, Application Server or Offline Mediation Controller	20 or 21	Application Server or Offline Mediation Controller	20 or 21
SNMP	UDP	Offline Mediation Controller	161	EMS	162
RADIUS	UDP	GSN or RADIUS Server	1814	Offline Mediation Controller	1813
DBSR	TCP	Offline Mediation Controller	1521	Oracle database	1521

Managing Mediation Host Security

By default, all Administration Servers can connect to the mediation host (also called a Node Manager). You can limit access to a mediation host by using its associated `OMC_home/config/nodemgr/nodemgr_allow.cfg` file. The file lists the IP addresses for all Administration Servers that are allowed to connect to the mediation host. You can edit the list at any time to allow or disallow Administration Server access to the mediation host.

Setting Up an Offline Mediation Controller Administration Server Firewall

You can set up a network firewall between the Offline Mediation Controller servers and the corporate intranet or external Internet. Administration Client can connect with and operate the Offline Mediation Controller servers through this firewall.

To set up a firewall, perform the following tasks:

- [Defining Administration Server Port Number](#)
- [Defining Administration Client Port Numbers](#)

These port numbers are defined during the installation process but can be modified to accommodate your particular firewall configuration.

Defining Administration Server Port Number

To change the default Administration Server's port number for the firewall:

1. Stop all Offline Mediation Controller components.
2. Open the `OMC_home/config/adminserver/firewallportnumber.cfg` file in a text editor.
3. Change the value of the following entry:

```
AdminServer=port
```

where *port* is the port on which Administration Server runs. The suggested port number range is between **49152** and **65535**. The default port number in the configuration file is **55110**.

4. Save and close the file.

Defining Administration Client Port Numbers

To change the default firewall port number range values:

1. Stop all Offline Mediation Controller components.
2. Open the `OMC_home/config/GUI/firewallportnumber.cfg` file in a text editor.
3. Change the values of the following entries:

```
RangeFrom=port
```

```
RangeTo=port
```

where *port* is the port on which Administration Client runs. The suggested port number range is between **49152** and **65535**. The default port number range in the configuration file is **55150** to **55199**.

4. Save and close the file.

Configuring Node Manager Memory Limits

To configure Node Manager memory limits:

Note:

The performance of the system can be affected by changing these settings, which by default are optimized for most Offline Mediation Controller applications.

1. Go to the `OMC_home/customization` directory and verify that the `nodemgr.var` file exists. On a newly installed system, the `nodemgr.var` file may not yet exist.

If the file does not exist, run the following command, which creates the file:

```
cp OMC_home/config/nodemgr/nodemgr.var.reference OMC_home/customization/nodemgr.var
```

2. Open the `nodemgr.var` file in a text editor.

3. Specify the upper memory size by modifying the `NM_MAX_MEMORY` parameter. The default is 3500 megabytes. The valid range for an Oracle/Red Hat Enterprise Linux installation is from **500** to **3500**.
4. Specify the lower memory size by modifying the `NM_MIN_MEMORY` parameter. The default is 1024 megabytes. The valid range for a Oracle/Red Hat Enterprise Linux installation is from **50** to **3500**.
5. Save and close the file.
6. Restart Node Manager.

Configuring the Java Virtual Machine Memory Usage when Running Administration Client

You can configure the maximum and minimum memory sizes the Java Virtual Machine (JVM) uses when running Administration Client. By configuring the maximum memory size, you can reduce the amount of memory JVM uses when running Administration Client.

To set the maximum and minimum memory sizes:

1. Open the `OMC_home/bin/gui` file in a text editor, where `OMC_home` is the directory in which Administration Client is installed.
2. Add or modify the following entries:

```
InitializeExternalConfig() {  
    NM_MIN_MEMORY=value  
    NM_MAX_MEMORY=value  
}
```

where *value* is the appropriate value for the respective entry.

For example:

```
InitializeExternalConfig() {  
    NM_MIN_MEMORY=1024  
    NM_MAX_MEMORY=3500  
}
```

3. Save and close the file.

Configuring the Java Virtual Machine Memory Usage when Running Administration Server

You can configure the maximum and minimum memory sizes the JVM uses when running Administration Server. By configuring the maximum memory size, you can reduce the amount of memory JVM uses when running Administration Server.

To set the maximum and minimum memory sizes:

1. Open the `OMC_home/bin/adminsvr` file in a text editor.
2. Add or modify the following entries:

```
InitializeExternalConfig() {  
    NM_MIN_MEMORY=value
```

```

    NM_MAX_MEMORY=value
}

```

where *value* is the appropriate value for the respective entry.

For example:

```

InitializeExternalConfig(){
    NM_MIN_MEMORY=1024
    NM_MAX_MEMORY=3500
}

```

3. Save and close the file.

Using the Offline Mediation Controller Shell Tool

You can use the Offline Mediation Controller Shell (NMShell) tool to access Offline Mediation Controller system information, discover node status, and perform start and stop operations, basic alarm monitoring, traffic monitoring, and node configuration changes. The NMShell tool runs on Linux workstations and is useful for low-speed connections or for accessing Offline Mediation Controller from behind a firewall that does not allow GUI access.

NMShell navigation is similar to the navigation in a file system. The components of the file system (the Administration Server, Node Managers, and nodes) make up a tree of contexts you can access with the **cd** command. To list the information available in a specific context, you can use the **ls** command. Certain contexts have other, context-specific commands available. For example, if you run the **cd** command to access a Node Manager context, you can then use the start and stop commands for the nodes. If you are starting or stopping more than one node, list the node IDs with a space between each one.

Before accessing the system information, you must use the login command, which logs you on to the Administration Server. You can then navigate the Offline Mediation Controller system.

The NMShell tool is located in the `OMC_home/bin/tools` directory.

[Table 1-2](#) lists the NMShell commands for the Administration Server.

Table 1-2 NMShell Commands for Administration Server

Command	Description
login	Log on to the specified Administration Server.
cd	Change to the specified Node Manager. If no Node Manager is specified, change to the parent Administration Server.
ls	Display the list of Node Managers configured for this Administration Server.
lsNodesWithName	List the node ID and type of all nodes having a specified name.
cmd -status	Display whether the last NMShell command was successful or failed.
status	Check the status of all nodes in a mediation host, all nodes for a specific Node Manager, or a specific node.
import	Import the node configuration from an XML file.
export	Export the node configuration to an XML file.

Table 1-2 (Cont.) NMSHELL Commands for Administration Server

Command	Description
addhost	Add a mediation host to the specified Node Manager.
startNodes or startNode	Start all nodes in the currently running mediation host, all nodes for a specific mediation host, or a specific node.
deleteNodes or deleteNode	Delete all nodes in the currently running mediation host, all nodes for a specific mediation host, or a specific node.
stopNodes or stopNode	Stop all nodes in a mediation host, all nodes for a specific mediation host, or a specific node.
compileNpl	Compile the NPL rule file.
addRoute	Add a route between the two nodes you specify.
removeRoute	Remove an existing route between the two nodes you specify.
help	Display the list of available commands.

Table 1-3 lists the NMSHELL commands for the Node Manager.

Table 1-3 NMSHELL Commands for Node Manager

Command	Description
cd	Change to the specified node. If no node is specified, change to the parent Node Manager.
ls	Display the list of nodes controlled by this Node Manager.
ls	Display the list of configuration parameters for a specific node.
start	Start one or more nodes on the Node Manager. Separate the node IDs with a space.
startall or start all	Start all nodes on this Node Manager.
stop	Stop one or more nodes on the Node Manager. Separate the node IDs with a space.
stopall or stop all	Stop all nodes on this Node Manager.
topalarm	Display the top level Node Manager alarm.
addattribute	Add back-end only configurations at the node level.
change	Change the value of an existing configuration at the node level.
perf or performance	Display the current node's performance window.
help	Display the list of available commands.

Table 1-4 lists the NMSHELL commands for nodes.

Table 1-4 NMSHELL Commands for Nodes

Command	Description
cd	Return to the parent Node Manager.
ls	List the configuration for the node.

[Table 1-5](#) lists the NMSHELL commands for all components.

Table 1-5 NMSHELL Commands for All Components

Command	Description
exit/quit	Exit the NMSHELL tool.
help	List the available commands for the current context.
pwd	Show the current context.

For more information about running NMSHELL commands, see "[Managing Nodes Using NMSHELL Command-Line Components](#)".

About SNMP Trap Hosts

An SNMP trap host is an IP host designated to receive SNMP trap messages from the Offline Mediation Controller system. Offline Mediation Controller sends SNMP trap messages to one or more external SNMP-based network management systems when:

- The Mediation Host or Node Manager experiences critical, warning, major, or minor events. You define the supported severity levels and their meanings in the Offline Mediation Controller SNMP trap management information base (MIB).
- You manually start or stop the Administration Server or Node Manager. For example, when you start the Administration Server, Offline Mediation Controller sends the "Server run state change" trap message with the additional text "Admin server has been started".

You can view trap message text on an external SNMP management system, such as the Hewlett Packard OpenView system, in the Offline Mediation Controller client, and in the host and node log files.

To ensure trap messages are received from both the local and remote Node Managers, when adding the target host, enter the IP address or the host name of the local machine and not the string "localhost". Offline Mediation Controller supports the generation of SNMP V1 and V2C traps.

2

Managing Offline Mediation Controller Security

Learn how to manage security in Oracle Communications Offline Mediation Controller.

Topics in this document:

- [About Offline Mediation Controller Security](#)
- [About Secure Communication Using Secure Sockets Layer](#)
- [About Users in Offline Mediation Controller](#)
- [About Managing Passwords](#)

About Offline Mediation Controller Security

Offline Mediation Controller security includes the following aspects:

- Secure communication
- User and password management
- Secure centralized storage for users and user's role information

About Secure Communication Using Secure Sockets Layer

Secure Sockets Layer (SSL) enables secure communication between applications. SSL enables authentication, data integrity, and data encryption. It helps to secure transmitted data using encryption.

By default, Administration Client communicates with Administration Server through SSLs. Administration Server communicates with Node Manager through SSL. During authentication, Administration Server provides the information using a certificate. It also provides data integrity through an integrity check value.

Creating Secure Connections

In Offline Mediation Controller, one-way SSL is used to create secure connections before sharing any data between the components. To use one-way SSL from a client to a server, configure identity for the server and trust store for the client. The trusted Certification authority (CA) certificates need to include the trusted CA certificate that issued the peer's identity certificate. This certificate does not necessarily have to be the root CA certificate.

In the communication between Administration Client and Administration Server, Administration Server has its own certificate in a secure KeyStore. This certificate will have a private and public key pair. Administration Server will share the certificate containing only the public key with all its known Administration Clients. Administration Client adds the server's certificate to its trust store, indicating that Administration Server is added to the trusted list.

In the communication between Administration Server and Node Manager, Node Manager acts as the server. Node Manager creates the key pair and store in a secure KeyStore. Node Manager shares its public key to the known Administration Server to ensure a secure communication. Administration Server adds Node Manager's certificate to its trust store.

To acquire a digital certificate for your server, generate a public key, a private key, and a Certificate Signature Request (CSR), which contains your public key. You send the CSR request to a certificate authority and follow its procedures for obtaining a signed digital certificate.

After you have your private keys, digital certificates, and any additional trusted CA certificates that you may need, store the private keys and certificates in KeyStores.

See "Enabling Secure Communication Using Certificates" in *Offline Mediation Controller Installation Guide*.

Enabling and Disabling SSL Mode

By default, Offline Mediation Controller runs in SSL mode, but the provision for enabling and disabling SSL communication is provided in a common configuration parameter.



Note:

If one of the Offline Mediation Controller components is running in SSL mode, the other components must be in SSL mode.

To enable or disable SSL mode for Offline Mediation Controller:

1. Open the `OMC_home/bin/UDCEnvironment` script in a text editor, where `OMC_home` is the directory in which Offline Mediation Controller is installed.
2. Add or modify the following entry:

```
SSL_ENABLED = value
```

where *value* is:

- **TRUE** to enable SSL mode.
 - **FALSE** to disable SSL mode.
3. Save and close the file.
 4. Restart Offline Mediation Controller.

Securely Connecting Administration Server to Other Node Manager Instances

You can securely connect Administration Server to other Node Manager instances or node hosts to collect data from Node Manager instances.

To securely connect Administration Server to other Node Manager instances:

1. Log on to the system on which Administration Server is installed.

2. Securely copy Node Manager's **nodeManager.cer** file from the machine on which Node Manager is installed to a temporary directory.
3. Run the following command:

```
OMC_home/jre/bin/keytool -import -v -trustcacerts -alias alias_name -file  
File_path -keystore OMC_home/config/adminserver/adminServerTruststore.jks
```

where:

- *alias_name* is the name of the new keystore entry. You must specify a different alias for each Node Manager.
- *File_path* is the path to the temporary directory and **nodeManager.cer** file that you securely copied.

Administration Server's truststore password prompt appears.

4. Enter Administration Server's truststore password.
The **Trust this certificate** prompt appears.
5. Confirm to trust the certificate.
The certificate is successfully imported into Administration Server's truststore.
6. Restart Administration Server and Administration Client.

Configuring Session Timeout Between Administration Server and Administration Client

The session timeout depends solely on the type of components between which the connection is established. Only the session between Administration Client and Administration Server supports session timeout after a preconfigured idle time. The session should never expire between an Administration Server and Node Manager, where user intervention is not expected.

To set the session timeout:

1. Open the *OMC_home/web/htdocs/AdminServerImpl.properties* file in a text editor.
2. Add or modify the following entry:

```
com.nt.udc.admin.server.AdminServerImpl.timeoutVal value
```

where *value* specifies a timeout value in minutes. The default is **30**.

3. Save and close the file.
4. Restart Administration Server and Administration Client.

About Users in Offline Mediation Controller

You can create, modify, and delete user login accounts through the Offline Mediation Controller administration client. The Offline Mediation Controller software authenticates all users prior to allowing them access to system configuration views.

When a login attempt fails, the system prompts again for the username and password for authentication. The Administration Server logs all user authentication events.

Offline Mediation Controller provides the following user roles:

- **Administrator:** Can create or delete login accounts and reset usernames and passwords. The administrator can also create, modify, and delete all functional components of the system (administration servers, node managers, nodes, node chains, and so on).
- **Designer:** Can perform all of the tasks that an Administrator can, except user-management tasks.
- **Operator:** Can start and stop nodes, view logs and alarms, and edit NARs.
- **Guest:** Can view logs and alarms.

All users can change their own passwords.

Table 2-1 lists the Offline Mediation Controller functions and user access based on the role.

Table 2-1 Role-Based Access to Functions

Functions	Administrator	Designer	Operator	Guest
Change the node/node host configuration	Yes	Yes	No	No
Start or stop any node	Yes	Yes	Yes	No
Create or delete any node host, node chain, or individual node	Yes	Yes	No	No
Add, change, and delete an SNMP host	Yes	Yes	No	No
Add, change, and delete users	Yes	No	No	No
Change own details	Yes	Yes	Yes	Yes
View alarms and alarm's level for both Node Manager and individual node	Yes	Yes	Yes	Yes
View the log details for messages, exceptions, etc.	Yes	Yes	Yes	Yes
Export configurations	Yes	Yes	No	No
Import configurations	Yes	Yes	No	No
Import customizations	Yes	Yes	No	No
Launch Record Editor	Yes	Yes	Yes	No
Manage poll list	Yes	Yes	No	No
Manage statistics reporting	Yes	Yes	No	No
View Administration Server log	Yes	Yes	Yes	Yes
Create or delete or edit routing between the nodes	Yes	Yes	No	No
Clear alarms	Yes	Yes	No	No

▲ Caution:

When you start Administration Server with the **-x** parameter, user authentication is disabled and you cannot perform the user management operations in Administration Client.

About Managing Users in Offline Mediation Controller

You manage Offline Mediation Controller users by using Administration Client. The Offline Mediation Controller software authenticates all users prior to allowing them access to system configuration views. The Administration Server logs all user authentication events.

To log in to a newly installed or upgraded Offline Mediation Controller system for the first time, use the default User ID (Admin) and password (admin). Customize your own login profile, and then create user login profiles. Each profile requires a username and a password.

About Managing the Administrator User Password in Oracle Unified Directory

You can modify the administrator user password by accessing the Oracle Unified Directory server. For information regarding managing users in Oracle Unified Directory, see "[Managing Users and Groups](#)" in *Oracle Fusion Middleware Administering Oracle Unified Directory*.

About Managing Passwords

Passwords are very important for security of the system, so the provided password should be strong and not hard-coded for users like Administrator.

By default, the password management policy is applied to users in Offline Mediation Controller. Disabling of user authentication is possible by starting Administration Server using the `-x` parameter.

Storing Passwords

The Offline Mediation Controller installer stores account passwords (for the Administrator and general users) in encrypted format in Oracle Unified Directory. By default, the passwords in Oracle Unified Directory are encrypted in the salted SHA-256 format.

About the Default Password Policy

When you create a user account in Offline Mediation Controller, it assigns a default password policy to that user account. The default password policy includes the following rules:

- Passwords expire automatically after 90 days.
- The last three passwords cannot be reused during a password change.
- The password must comply with the following standards:
 - Contain at least six characters
 - Contain at least one lowercase letter
 - Contain at least one uppercase letter
 - Contain at least one special character (for example, \$)
 - Contain at least one number
- The user is locked out for 10 minutes after three consecutive failed log in attempts.

- The user must change the password after the first successful authentication after a password is set or reset by the administrator.

Modifying the Default Password Policies

The default password policy is assigned to user accounts during Offline Mediation Controller installation. You can modify the default password policies by modifying the parameters in the `OMC_home/bin/createPasswordPolicy` script.

To modify the default password policy:

1. Ensure that the Oracle Unified Directory server instance is running.
2. Open the `OMC_home/bin/createPasswordPolicy` file in a text editor.
3. Enter or modify the parameter values. For example:
 - To have passwords expire every 120 days, you would set **max-password-age** to **120**.
 - To require users to enter their current password when setting a new password, you would set **password-change-requires-current-password** to **true**.

For information about each password policy parameter, see "[Managing Password Policies](#)" in *Oracle Fusion Middleware Administering Oracle Unified Directory*.

4. Save and close the file.
5. Go to the `OMC_home/bin` directory.
6. Run the following command:

```
./createPasswordPolicy -p OUD_password
```

where `OUD_password` is the Oracle Unified Directory server instance administrator password.

7. Restart Administration Server and Administration Client.

3

Managing Nodes Using NMShell Command-Line Components

You can manage Oracle Communications Offline Mediation Controller nodes by using NMShell command-line components.

Topics in this document:

- [Logging Into NMShell](#)
- [Starting Nodes](#)
- [Stopping Nodes](#)
- [Deleting Nodes](#)
- [Adding Node Routes](#)
- [Deleting an Existing Node Route](#)
- [Adding Mediation Hosts to Node Manager](#)
- [Compiling the NPL Rule File](#)
- [Changing Existing Node-Level Configuration](#)
- [Adding Back-End Only Configurations at Node Level](#)
- [Checking Node Status](#)
- [Listing Node ID and Type](#)
- [Checking NMShell Command Status](#)
- [Importing and Exporting Node Configuration](#)

Logging Into NMShell

To log into the NMShell application:

1. Start the Offline Mediation Controller Administration Server and Node Manager daemons.
 - a. Go to the `OMC_home/bin` directory, where `OMC_home` is the directory in which you installed Offline Mediation Controller.
 - b. Start the Administration Server daemon:

```
./adminsvr
```
 - c. Start the Node Manager daemon:

```
./nodemgr
```
2. Go to the `OMC_home/bin/tools` directory, and then enter the following command:

```
./NMShell
```

The prompt changes to `nmsh>`.

3. Enter the following command:

```
login server_hostname port
```

where:

- *server_hostname* is the IP address or host name of the computer on which Administration Server is running.
 - *port* is the Administration Server port number.
4. When prompted, enter your username and password.
NMShell is connected to Administration Server.

You can now enter NMShell commands to start nodes, stop nodes, add node routes, and so on.

Starting Nodes

You can use NMShell to start all nodes in a mediation host, all nodes for a specific Node Manager, or a specific node. To do so, log into NMShell and then do the following:

1. Change to the Administration Server context:

```
cd adminSvrHost adminSvrPort
```

where *adminSvrHost* is the host name or IP address of the computer on which Administration Server is installed, and *adminSvrPort* is the port number for Administration Server.

2. Enter one of these commands depending on which nodes you want to start.

- To start all nodes in the currently running mediation host:

```
startNodes
```

- To start all nodes managed by a specific Node Manager:

```
startNode -ip mediation_hostname -p port
```

where *mediation_hostname* is the mediation host's IP address or host name, and *port* is the mediation host port number.

- To start a specific node:

```
startNode node_id_1 node_id_2...
```

Stopping Nodes

You can use NMShell to stop all nodes in the currently running mediation host, all nodes for a specific mediation host, or a specific node. To do so, log into NMShell and then do the following:

1. Change to the Administration Server context:

```
cd adminSvrHost adminSvrPort
```

2. Enter one of these commands depending on which nodes you want to stop.

- To stop all nodes in the currently running mediation host:

```
stopNodes
```

- To stop all nodes in a specific mediation host:

```
stopNode -ip mediation_hostname -p port
```

where *mediation_hostname* is the mediation host's IP address or host name, and *port* is the mediation host port number.

- To stop a specific node:

```
stopNode node_id_1 node_id_2...
```

Deleting Nodes

You can use NMShell to delete all nodes in a mediation host, all nodes for a specific Node Manager, or a specific node. To do so, log into NMShell and then do the following:

1. Change to the Administration Server context:

```
cd adminSvrHost adminSvrPort
```

2. Enter one of these commands depending on which node you want to delete.

- To delete all nodes in the currently running mediation host:

```
deleteNodes
```

- To delete all nodes managed by a specific Node Manager:

```
deleteNode -ip mediation_hostname -p port
```

where *mediation_hostname* is the mediation host's IP address or host name, and *port* is the mediation host port number.

- To delete a specific node:

```
deleteNode node_id_1 node_id_2...
```

Adding Node Routes

You can use NMShell to add the following types of routes between nodes:

- [Adding a Round-Robin Node Route](#)
- [Adding a Multicast Node Route](#)
- [Adding a Modulus Node Route](#)
- [Adding a Directed Node Route](#)

For more information, see "About Node Routing" in *Offline Mediation Controller User's Guide*.

Adding a Round-Robin Node Route

Round-robin routing allows you to branch a node chain to multiple instances of the same processing node type, such as from one CC node to three instances of the EP node, to improve performance. NAR files are routed by rotating through the different destination nodes. That is, the first NAR file is sent to destination node 1, the second NAR file is sent to

destination node 2, and the third NAR file is sent to destination node 3. This routing process is repeated for all subsequent NAR files.

To add a round-robin route between two nodes, log into NMSHELL and then do the following:

1. Change to the Administration Server context:

```
cd adminSvrHost adminSvrPort
```

2. Enter the **addRoute** command:

```
addRoute -o originNodeId -t targetNodeId -rFunc ROUND_ROBIN
```

where:

- *originNodeId* is the ID of the source node.
- *targetNodeId* is the ID of the destination node.

For example:

```
addRoute -o rtvv91-16it-kzrxghq2 -t rtvv91-16it-kzrzle10p -rFunc  
ROUND_ROBIN
```

Adding a Multicast Node Route

Multicast routing allows you to branch a node chain, such as from a source node to two destination nodes. All NAR files are routed in parallel to both destination nodes.

To add a multicast route between two nodes, log into NMSHELL and then do the following:

1. Change to the Administration Server context:

```
cd adminSvrHost adminSvrPort
```

2. Enter the **addRoute** command:

```
addRoute -o originNodeId -t targetNodeId -rFunc MULTICAST
```

where:

- *originNodeId* is the ID of the source node.
- *targetNodeId* is the ID of the destination node.

For example:

```
addRoute -o rtvumc-16it-106o6w2p -t rtvumc-16it-y85f6e8d -rFunc  
MULTICAST
```

Adding a Modulus Node Route

Modulus routing allows you to branch a node chain to multiple instances of the same processing node, such as from one CC node to three instances of the EP node, to improve performance. NAR files are routed to a destination node based on an attribute value in the file, such as the starting time.

To add a modulus route between two nodes, log into NMSHELL and then do the following:

1. Change to the Administration Server context:

```
cd adminSvrHost adminSvrPort
```

2. Enter the **addRoute** command:

```
addRoute -o originNodeId -t targetNodeId -rFunc MODULUS -rField RoutingAttribute
```

where:

- *originNodeId* is the ID of the source node.
- *targetNodeId* is the ID of the destination node.
- *RoutingAttribute* is an attribute from the NPL file, such as **calling_number**, **session_id**, **start_time**, **end_time**, or **seq_no**.

For example:

```
addRoute -o rtvumc-16it-106o6w2p -t rtvumc-16it-y85f6e8d -rFunc MODULUS -  
rField seq_no
```

Adding a Directed Node Route

Directed routing allows you to branch a node chain, such as from a source node to two destination nodes. NAR files are routed to a destination node based on an attribute value in the file. For example, NAR files with sequence numbers 1 through 1000 are sent to destination node A, and NAR files with sequence numbers 1001 through 2000 are sent to destination node B.

To add a directed route between two nodes, log into NMSHELL and then do the following:

1. Change to the Administration Server context:

```
cd adminSvrHost adminSvrPort
```

2. Enter the **addRoute** command:

```
addRoute -o originNodeId -t targetNodeId -rFunc DIRECTED -rField RoutingAttribute -  
rOperator RoutingOperator -rOperand1 CommaSeparatedValues [-rOperand2  
CommaSeparatedValues]
```

where:

- *originNodeId* is the ID of the source node.
- *targetNodeId* is the ID of the destination node.
- *RoutingAttribute* is an attribute from the NPL file, such as **calling_number**, **session_id**, **start_time**, **end_time**, or **seq_no**.
- *RoutingOperator* is the operator type: **EQUALS**, **NOT_EQUALS**, **LESS_THAN**, **GREATER_THAN**, **IN_BETWEEN**, **LIST_EQUALS**, **LIST_NOT_EQUALS**, **SUBSET_OF**, or **NOT_SUBSET_OF**.
- *CommaSeparatedValues* is a comma-separated list of all operands.

For example:

```
addRoute -o rtvumc-16it-106o6w2p -t rtvumc-16it-y85f6e8d -rFunc  
DIRECTED -rField seq_no -rOperator IN_BETWEEN -rOperand1 20,60 -  
rOperand2 30,70
```

In this example, the output of `rtvumc-16it-106o6w2p` is routed to `rtvumc-16it-y85f6e8d` when an NPL file contains a sequence number from 20 through 30, or from 60 through 70.

Deleting an Existing Node Route

To delete an existing route between two nodes, log into NMShell and then do the following:

1. Change to the Administration Server context:

```
cd adminSvrHost adminSvrPort
```

2. Enter the **removeRoute** command:

```
removeRoute -o originNodeId -t targetNodeId
```

where:

- *originNodeId* is the ID of the source node.
- *targetNodeId* is the ID of the destination node.

For example:

```
removeRoute -o rtvv91-16it-kzrxghq2 -t rtvv91-16it-kzrze10p
```

Adding Mediation Hosts to Node Manager

Before you import the node configuration or customization into a mediation host, you must first add the mediation host to Node Manager.

To add a mediation host to Node Manager, log into NMShell and then do the following:

1. Change to the Administration Server context:

```
cd adminSvrHost adminSvrPort
```

2. Enter the **addhost** command:

```
addhost -n mediation_name -ip node_mgr_hostname -p port
```

where:

- *mediation_name* is the name of the mediation host you are adding to Node Manager.
- *node_mgr_hostname* is the IP address or host name of the computer on which Node Manager is running.
- *port* is the port number at which the mediation host communicates with Node Manager.

The mediation host is added to Node Manager.

Compiling the NPL Rule File

To compile the NPL rule file, log into NMSHELL and then do the following:

1. Change to the Administration Server context:

```
cd adminSvrHost adminSvrPort
```

2. Enter the **compileNpl** command:

```
compileNpl -f npl_file_name -d complied_npl_class -majorType  
major_type_of_the_node -minorType minor_type_of_the_node -id node_id
```

where:

- **-f npl_file_name** specifies the absolute path of the NPL file that you want to compile.
- **-d complied_npl_class** specifies the absolute path of the compiled NPL class after running the command.
- **-majorType major_type_of_the_node** specifies the major type of the node for which the NPL rule file is compiled. This parameter is not applicable if node ID is defined using the ID argument.
- **-minorType minor_type_of_the_node** specifies the minor type of the node for which the NPL rule file is compiled. This parameter is not applicable if node ID is defined using the ID argument.
- **-id node_id** specifies the unique ID assigned to the node for which the NPL rule file is compiled. This parameter is not applicable if **-majorType** and **-minorType** are specified.

The NPL rule file is compiled. If the compilation fails, update the rule file and recompile.

You can store the compiled NPL rule file in the **classpath** directory in the **config** folder of the node and update the **general.cfg** file to use the compiled NPL rule file.



Note:

After compiling the NPL rule file, you must start and stop nodes only by using NMSHELL command-line components. Using the GUI to start or stop nodes uses only the attributes and NPL that are defined in GUI components.

Changing Existing Node-Level Configuration

You can change the value of an existing configuration at the node level. To do so, log into NMSHELL and then do the following:

1. Change to the Node Manager context:

```
cd nodeMgrHost nodeMgrPort
```

where *nodeMgrHost* is the host name or IP address of the computer on which Node Manager is installed, and *nodeMgrPort* is the port number for Node Manager.

2. Enter one of these commands depending on whether the configuration key is a password or not.

- If the configuration key is not a password:

```
change NodeID configKey configValue
```

where:

- *NodeID* is the unique ID assigned to the node.
- *configKey* is the name of the configuration key.
- *configValue* is the value of the configuration key.

- If the configuration key is for an encoded password:

```
change NodeID passwordKey encodedPassword
```

where *passwordKey* is either the password of the FTP user (**ftppasswd**) or the password of the database user (**dbpassword**), and *encodedPassword* is the password in Base64 encoded format.

- If the configuration key is for a password that is not encoded:

```
change NodeID passwordKey
password: password
```

Adding Back-End Only Configurations at Node Level

To add back-end only configurations at the node level, log into NMShell and then do the following:

1. Change to the Node Manager context:

```
cd nodeMgrHost nodeMgrPort
```

where *nodeMgrHost* is the host name or IP address of the computer on which Node Manager is installed, and *nodeMgrPort* is the port number for Node Manager.

2. Enter the **addAttribute** command:

```
addAttribute NodeID configKey configValue
```

where:

- *NodeID* is the unique ID assigned to the node.
- *configKey* is the name of the configuration key, such as Idle Write Time.
- *configValue* is the value of the configuration key, such as 60.

Checking Node Status

You can use NMSHELL to check the status of all nodes in a mediation host, all nodes for a specific Node Manager, or a specific node. To do so, log into NMSHELL and then do the following:

1. Change to the Administration Server context:

```
cd adminSvrHost adminSvrPort
```

2. Enter one of these commands.

- To check the status of all nodes for the currently running mediation host:

```
status
```

- To check the status of all nodes managed by a specific Node Manager:

```
status -ip mediation_hostname -p port
```

where *mediation_hostname* is the mediation host's IP address or host name, and *port* is the mediation host port number.

- To check the status of a specific node:

```
status node_id_1 node_id_2...
```

Listing Node ID and Type

To list the node ID and type of all nodes having a specified name, log into NMSHELL and then do the following:

1. Change to the Administration Server context:

```
cd adminSvrHost adminSvrPort
```

2. Enter the **lsNodesWithName** command:

```
lsNodesWithName [nodeName]
```

where *nodeName* is the name of the node.

For example:

```
lsNodesWithName testNode
```

Checking NMSHELL Command Status

To check whether the last NMSHELL command was successful or failed, log into NMSHELL and then do the following:

1. Change to the Administration Server context:

```
cd adminSvrHost adminSvrPort
```

2. Enter this command:

```
cmd -status
```

One of the following results is returned:

- **-1** specifies that the last run command failed or there are no commands run before.
- **0** specifies that the last run command was successful.

 **Note:**

When multiple nodes are started or stopped by using NMSHELL, the status of the command can be retrieved only by running the **status** command. See "[Checking Node Status](#)" for more information.

Importing and Exporting Node Configuration

You can import or export node configuration and customization from:

- All mediation hosts configured in Node Manager
- One or more node chains under the Node Manager

See the following topics:

- [Importing Node Configuration and Node Customization](#)
- [Exporting Node Configuration and Node Customization](#)
- [Incrementally Import Node Chain Configurations and Customizations](#)
- [Incrementally Export Node Chain Configurations and Customizations](#)

 **Note:**

If you stop the export or import process, the system fails, or an error occurs repeatedly, intermediate files, data files, and folders are created in the nodes directory in *OMC_home*. If this occurs, create an offline copy of these files and then delete the nodes before running the command again.

Importing Node Configuration and Node Customization

To import the node configuration and node customization from all mediation hosts configured in Node Manager, log into NMSHELL and then do the following:

1. Change to the Administration Server context:

```
cd adminSvrHost adminSvrPort
```

2. Enter the **import** command:

```
import -n mediation_name@mediation_hostname:port -f filename -c value
```

where:

- *mediation_name* is the mediation host's name configured in Node Manager.
- *mediation_hostname* is the IP address or host name of the mediation host.
- *port* is the port number of the mediation host.
- *filename* specifies the name and path of the input file. Use *filename.xml* file to import the node configuration and use *filename.nmx* file to import the node customization.
- *value* is one of the following:
 - **Y** specifies to import only the node customization. Use this value with the *filename.nmx* file.
 - **N** specifies to import only the node configuration. Use this value with the *filename.xml* file.

For example:

```
import -n linux1@10.10.10.111:55109 -f import.xml -c N
```

The node configuration is imported from the **import.xml** file into the specified mediation hosts (**linux1@10.10.10.111:55109**).

Exporting Node Configuration and Node Customization

You can use NMSHELL to export the node configuration and customization details from all mediation hosts configured in Node Manager, or from a specified mediation host. To do so, log into NMSHELL and then do the following:

1. Change to the Administration Server context:

```
cd adminSvrHost adminSvrPort
```

2. Enter one of these **export** commands:

- To export from all mediation hosts configured in Node Manager:

```
export -n ALL -f filename [-c value]
```

- To export from a specified mediation host:

```
export -n mediation_name@mediation_hostname:port -f filename [-c value]
```

where:

- *mediation_name* is the mediation host's name configured in Node Manager.
- *mediation_hostname* is the mediation host's IP address or host name. To export multiple hosts, enter the mediation hosts separated by a comma (,).
- *port* is the port number at which the mediation host communicates with Node Manager.
- *filename* is the name and path of the output files. Do not include the file extension.
- *value* is one of the following:
 - * **Y** specifies to export both the node configuration and node customization. Two files are generated: *filename.xml* with the node configuration, and *filename.nmx* with the node customization. This is default.

- * **N** specifies to export only the node configuration. One file named *filename.xml* file is generated.

For example:

```
export -n linux1@10.10.10.111:55109,linux2@10.10.10.112:55110 -f export -c N
```

Only the node configuration from the mediation hosts (**linux1@10.10.10.111:55109** and **linux2@10.10.10.112:55110**) is exported to the **export.xml** file.

Incrementally Import Node Chain Configurations and Customizations

Note:

Before you incrementally import node change configurations and customizations:

- Ensure that Administration Server and Node Manager are available in the same *OMC_home* directory. If Node Manager is in a different directory, the node IDs are regenerated during the import by default and a backup of the old node chain is not created.
- Ensure that you stop the nodes for which you want to import the customization or configuration before importing the node chain configuration or customization. See "[Stopping Nodes](#)" for more information.

To incrementally import one or more node chain configurations and customizations, log into NMSHELL and then do the following:

1. Change to the Administration Server context:

```
cd adminSvrHost adminSvrPort
```

2. Enter the **import** command:

```
import [-n mediation_name@mediation_hostname:port] -f filename [-c value -nc y -r y]
```

where:

- *mediation_name* is the mediation host's name configured in Node Manager.
- *mediation_hostname* is the IP address or host name of the mediation host.
- *port* is the port number of the mediation host.
- *filename* specifies the name and path of the input file. Use *filename.xml* file to import the node configuration and use *filename.nmx* file to import the node customization.
- *value* is one of the following:
 - **Y** specifies to import only the node customization. Use this value with the *filename.nmx* file.
 - **N** specifies to import only the node configuration. Use this value with the *filename.xml* file.

- **-nc y** specifies to import only the node chain customization or configuration.
- **-r y** specifies to regenerate the *node_id* of the nodes for which the configuration or customization is imported. This value must be set if you importing node chain configuration or customization.

The node chain configuration or customization is imported into the specified mediation host. After the import, a backup of the existing nodes is created in the *OMC_home/importbackup* directory.

For example:

```
import -n linux1@10.10.10.111:55109 -f import.xml -c N -nc y -r y
```

The node chain configuration is imported from the **import.xml** file into the specified mediation host (**linux1@10.10.10.111:55109**).

After importing the node chain configuration or customization, you need to manually map the nodes that are not part of the imported node chain and delete undesired nodes.

Incrementally Export Node Chain Configurations and Customizations

To incrementally export one or more node chain configurations and customizations, log into NMSHELL and then do the following:

1. Change to the Administration Server context:

```
cd adminSvrHost adminSvrPort
```

2. Enter the **export** command:

```
export -n mediation_name@host_name:port -f filename -c value -nc y -id node_id
```

where:

- *mediation_name* is the mediation host's name configured in Node Manager.
- *mediation_hostname* is the IP address or host name of the mediation host.
- *port* is the port number of the mediation host.
- **-f filename** specifies the name and path of the output files. Do not include the file extension.
- **-c value** is one of the following:
 - **Y** specifies to export both the node configuration and node customization. Two files are generated: *filename.xml* with the node configuration, and *filename.nmx* with the node customization. This is default.
 - **N** specifies to export only the node configuration. One file named *filename.xml* file is generated.
- **-nc y** specifies to export only the node chain configuration and customization.
- **-id node_id** specifies to export the node chain configuration and customization from the specified node. To export from multiple nodes, separate the node IDs by commas.

For example:

```
export -n abc@localhost:55109 -f ../testnodechain/test/exportfile -c y -nc y -id 31a80o-16it-jrzysls9
```

The node configuration and customization from the **31a80o-16it-jrzysls9** node chain in the mediation host (**abc@localhost:55109**) are exported successfully to the specified file.

4

Monitoring Offline Mediation Controller

Learn how to monitor your components in Oracle Communications Offline Mediation Controller.

Topics in this document:

- [Monitoring Node Performance in Administration Client](#)
- [Monitoring Node Performance with Prometheus and Grafana](#)
- [Monitoring System Processes](#)
- [Monitoring How Offline Mediation Controller Components are Running](#)
- [Using Server Monitoring](#)
- [Using Logs to Monitor Offline Mediation Controller Components](#)

Monitoring Node Performance in Administration Client

You can monitor node performance in Administration Client in the following ways:

- For a current view of node performance, use the Node Performance View. This view displays a list of nodes running on the selected host. You can monitor node up time, current NARs, current rate, average rate, and total NARs.
- To get node performance statistics, you can configure statistics reporting: input records, output records, duplicate records, aggregated records, and discarded records. You can enable or disable statistics reporting for each node, for all nodes, or for no nodes.

Monitoring Node Performance with Prometheus and Grafana

You can monitor node performance in Offline Mediation Controller by using Prometheus and Grafana. For the list of compatible Prometheus and Grafana software versions, see "Additional Offline Mediation Controller Software Requirements" in *Offline Mediation Controller Compatibility Matrix*.

By default, Offline Mediation Controller tracks and exposes the following Node Manager-level statistics through a single endpoint in Prometheus format:

- The total network account records (NARs) processed
- The current NARs processed
- The current processing rate
- The average processing rate

The metric data for all Node Manager components are exposed at **http://localhost:8082/metrics**, but you can change the port number where the metrics are exposed or disable the metric endpoint altogether. See "[Configuring the Node Manager Metric Endpoint](#)".

You can then configure Prometheus to scrape the Node Manager metrics from the endpoint and store them for analysis and monitoring. You can also set up a visualization tool, such as Grafana, to display your metric data in a graphical format.

You can use the following sample Grafana Dashboard templates to visualize the Offline Mediation Controller metrics:

- **OCOMC_JVM_Dashboard.json**: Allows you to view JVM-related metrics for Offline Mediation Controller.
- **OCOMC_Node_Manager_Summary.json**: Allows you to view NAR processing metrics for the Node Manager.
- **OCOMC_Node_Summary.json**: Allows you to view NAR processing metrics for all nodes.
- **OCOMC_Summary_Dashboard.json**: Allows you to view NAR-related metrics for all Offline Mediation Controller components.

To use the sample dashboards, import the JSON files from the *OMC_home/sampleData/dashboards* directory into Grafana. For information about importing dashboards, see "[Manage Dashboards](#)" in the *Grafana Dashboards* documentation.

Configuring the Node Manager Metric Endpoint

You can configure Offline Mediation Controller to expose Node Manager metric data at a port other than 8082 as well as disable or enable the metric endpoint.

To configure the Node Manager metric endpoint:

1. Open your *OMC_home/bin/UDCEnvironment* file in a text editor.
2. Set the **IS_METRIC_ENABLED** environment variable to one of the following:
 - **true**: Enables the metric endpoint. This is the default.
 - **false**: Disables the metric endpoint.
3. Set the **METRIC_PORT** key to the port number at which you want to expose the Node Manager metrics. The default is **8082**.
4. Save and close the **UDCEnvironment** file.
5. Restart Node Manager. See "[Starting and Stopping Node Manager](#)".

Monitoring System Processes

You can monitor Offline Mediation Controller system processes such as disk, memory, and CPU usage levels by setting thresholds in the *OMC_home/config/nodemgr/nodemgr.cfg* file. You use this file to set a warning threshold, an error threshold, and the action that is triggered when a process's threshold is crossed.

Note:

If you do not modify the **nodemgr.cfg** file, Offline Mediation Controller uses the default threshold values.

- To monitor disk errors, see "[Using the Disk Status Monitor](#)".

- To monitor memory errors, see "Using the Memory Monitor".
- To monitor CPU usage levels, see "Using the CPU Usage Monitor".

By default, Offline Mediation Controller generates a single alarm for each error condition, even if the error condition occurs multiple times. To generate an alarm or trap for every error occurrence, open the **nodemgr.cfg** file and change the SUPPRESS_MULTIPLE_ALARMS parameter value to **No**.

Using the Disk Status Monitor

You use the disk status monitor to alert you to potential disk issues, so you can take action to avoid unrecoverable errors.

Table 4-1 lists the parameters you can add or modify in the **nodemgr.cfg** file.

Table 4-1 Disk Status Monitor Parameters

Parameter	Description
DISK_STATUS_CMD	The full path to the metastat command. The default is /usr/sbin/metastat .
DISK_STATUS_POLLTIME	Amount of time to wait between polling intervals.

Using the Memory Monitor

You use the memory monitor to alert you when memory usage exceeds a specified threshold. In addition to the threshold, you can configure the memory monitor to log memory usage statistics.

Table 4-2 lists the parameters you can add or modify in the **nodemgr.cfg** file.

Table 4-2 Memory Monitor Parameters

Parameter	Description
LOG_MEMORY_USAGE	Set to Y to log memory usage statistics. The default is N .
MEMORY_MAJOR_THRESH OLD	The level at which a major alarm is raised, as a percentage. The default is 85 .
MEMORY_WARNING_THRE SHOLD	The level at which a warning alarm is raised, as a percentage. The default is 70 .
MEMORY_SAMPLE_TIME	A time interval, in seconds, during which the memory usage must be above a specific threshold level before an alarm is raised. The default is 60 .
MEMORY_SAMPLE_FREQ	The number of polls that are taken during each sample period. The default is 4 .

For example, using the default values for MEMORY_SAMPLE_TIME (60 seconds) and MEMORY_SAMPLE_FREQ (4), the memory usage polls would occur every 15 seconds (60 seconds divided by 4). In this case, an alarm would be generated if the memory usage level was above the specified threshold for 4 consecutive polls.

Using the CPU Usage Monitor

The CPU usage monitor generates a critical or major alarm if the CPU usage level reaches a specified value.

Table 4-3 lists the parameters you can add or modify in the **nodemgr.cfg** file.

Table 4-3 CPU Usage Monitor Parameters

Parameter	Description
CPU_REDTHRESHOLD	The percentage of CPU in use that will generate a critical alarm. The default is 90 .
CPU_YELLOWTHRESHOLD	The percentage of CPU in use that will generate a major alarm. The default is 80 .
CPU_SAMPLETIME	The period, in seconds, in which to poll a fixed number of times. The default is 60 .
CPU_SAMPLEFREQ	How often to poll during the fixed period. The default is 3 .

For example, using the default values for CPU_SAMPLETIME (60 seconds) and CPU_SAMPLEFREQ (3), a poll will take place every 20 seconds (60 seconds divided by 3).

Monitoring How Offline Mediation Controller Components are Running

You can monitor Offline Mediation Controller components to ensure that they are still running and to restart the server by using the **ProcessControl** script. The script periodically monitors the status of the Offline Mediation Controller components that are defined in the **offline_mediation.conf** file. See "[Configuring the ProcessControl Script to Run Components](#)" for information about editing the **offline_mediation.conf** file.

To monitor how the Offline Mediation Controller server and components are running:

1. Stop all Offline Mediation Controller components.
2. Open the **/etc/inittab** file in a text editor.
3. Add the following entry:


```
NT:3:respawn:/etc/init.d/ProcessControl monitor
```
4. Save and close the file.
5. Run the following command, which periodically monitors the status of the Offline Mediation Controller components that are defined in the **offline_mediation.conf** file:


```
./ProcessControl monitor
```

Using Server Monitoring

The Offline Mediation Controller server monitoring feature creates log files that report hardware performance at all times, and divides that data into convenient statistical categories.

Statistical Categories

Each statistical category has an entry in the **nodemgr.cfg** file to indicate if performance logging is desired. The default values are pre-set in this file and you can change them where necessary. The **nodemgr.cfg** file is located at *OMC_home/config/nodemgr*. The statistical categories are listed in the following sections.

Disk Utilization

This function monitors the percentage of total disk space currently used on the Offline Mediation Controller partition. The corresponding entry in the **nodemgr.cfg** file is: **SERVERMONITOR_DISK_UTILIZATION**.

The disk utilization log file is located in *OMC_home/serverMonitoring/IP_Port/diskUtilization*.

The log file values are as follows:

- **partition** = Offline Mediation Controller installation, used to determine partition being monitored
- **kbytes** = Total disk space in partition, measured in kbytes
- **used** = Total disk space in partition used, measured in kbytes
- **available** = Disk space not in use
- **capacity** = Percentage of disk space in used

Here is an example of the disk utilization log file:

```
<poll date="2005/09/27" time="14:44:18" partition="/opt/nm500" kbytes="5886725"
used="5139094" avail="688764" capacity="89%" />
<poll date="2005/09/27" time="14:49:19" partition="/opt/nm500" kbytes="5886725"
used="5139129" avail="688729" capacity="89%" />
<poll date="2005/09/27" time="14:54:19" partition="/opt/nm500" kbytes="5886725"
used="5139137" avail="688721" capacity="89%" />
<poll date="2005/09/27" time="14:59:20" partition="/opt/nm500" kbytes="5886725"
used="5139144" avail="688714" capacity="89%" />
<poll date="2005/09/27" time="15:04:20" partition="/opt/nm500" kbytes="5886725"
used="5139150" avail="688708" capacity="89%" />
```

Disk Status

This function monitors the health of the disk containing Offline Mediation Controller using the **metastat** command. Note: the **metastat** command must be previously installed on the system to correctly use this feature. The corresponding entry in the **nodemgr.cfg** file is: **SERVERMONITOR_DISK_STATUS**.

The disk status log file is located in *OMC_home/serverMonitoring/IP_Port/diskStatus*.

Here is an example of the disk status log file:

```
<poll date="2005/09/27" time="16:26:15" diskHealth="healthy" />
<poll date="2005/09/27" time="16:36:15" diskHealth="healthy" />
<poll date="2005/09/27" time="16:46:15" diskHealth="healthy" />
```

CPU Utilization

This function monitors the percentage of the processor(s) currently in use in the system. The corresponding entry in the **nodemgr.cfg** file is: **SERVERMONITOR_CPU_UTILIZATION**.

The CPU utilization log file is located in *OMC_home/serverMonitoring/IP_Port/cpuUtilization*.

The log file values are as follows:

- **cpuActive** = Percentage of CPU taken up with user processes
- **cpuSystem** = Percentage of CPU taken up with system processes
- **cpuIdle** = Percentage of CPU not being used

Here is an example of the CPU utilization log file:

```
<poll date="2005/09/27" time="14:39:46" cpuActive="34" cpuSystem="4"
cpuIdle="62" />
<poll date="2005/09/27" time="14:40:06" cpuActive="62" cpuSystem="3"
cpuIdle="35" />
<poll date="2005/09/27" time="14:40:26" cpuActive="38" cpuSystem="4"
cpuIdle="58" />
<poll date="2005/09/27" time="14:40:46" cpuActive="16" cpuSystem="3"
cpuIdle="81" />
```

Memory Utilization

This function monitors the percentage of the memory currently in use in the system. The corresponding entry in the **nodemgr.cfg** file is: **SERVERMONITOR_MEMORY_UTILIZATION**.

The memory utilization log file is located in *OMC_home/serverMonitoring/IP_Port/memoryUtilization*.

The log file values are as follows:

- **freeMemory** = Amount of memory not used in the heap, measured in bytes
- **maxMemory** = Memory limit available for process to grow into (**-Xmx** option), measured in bytes
- **usedMemory** = The following calculation: $\text{maxMemory} - \text{freeMemory}$, measured in bytes
- **memory Utilization** = The following calculation: $(\text{currently allocated process limit} - \text{freeMemory}) / \text{maxMemory}$, measured in bytes

Here is an example of the memory utilization log file:

```
<poll date="2005/09/27" time="14:36:07" memoryUtilization="2.8679903"
usedMemory="5.4105304E7" freeMemory="1.23482E7" maxMemory="6.6453504E7" />
<poll date="2005/09/27" time="14:36:22" memoryUtilization="2.4237578"
usedMemory="5.6333232E7" freeMemory="1.0120272E7" maxMemory="6.6453504E7" />
<poll date="2005/09/27" time="14:36:37" memoryUtilization="2.577369"
usedMemory="5.6435312E7" freeMemory="1.0018192E7" maxMemory="6.6453504E7" />
<poll date="2005/09/27" time="14:36:52" memoryUtilization="2.6964898"
usedMemory="5.6514472E7" freeMemory="9939032.0" maxMemory="6.6453504E7" />
```

Open Files - System File Monitoring

This function tracks the number of files open on the operating system. To enable system file monitoring in Offline Mediation Controller, the open source package "Isof" must be installed in a location accessible from the \$PATH variable. The corresponding entry in the **nodemgr.cfg** file is: `SERVERMONITOR_OPEN_FILES`.

The log file is located in `OMC_home/serverMonitoring/IP_Port/systemFiles`.

The log file value "**openFiles**" is the number of open files in the entire system.

Here is an example of the open files log file:

```
<poll date="2005/09/27" time="16:19:55" openFiles="2203" />
<poll date="2005/09/27" time="16:20:58" openFiles="2222" />
<poll date="2005/09/27" time="16:22:02" openFiles="2298" />
<poll date="2005/09/27" time="16:23:05" openFiles="2298" />
<poll date="2005/09/27" time="16:24:09" openFiles="2201" />
<poll date="2005/09/27" time="16:25:12" openFiles="2247" />
<poll date="2005/09/27" time="16:26:15" openFiles="2201" />
```

Log File Information

Log File Format

A server monitor log is an XML file, which tracks performance values gathered at each poll instance. Each log contains a date and timestamp, followed by the statistical values gathered during that period. Each statistical category has its own performance log file. For example:

```
<poll date="04/27/2005" time="13:49:07" cpuActive= "4" cpuIdle= "96" />
<poll date="04/27/2005" time="13:50:07" cpuActive= "6" cpuIdle= "94" />
<poll date="04/27/2005" time="13:51:07" cpuActive= "5" cpuIdle= "95" />
<poll date="04/27/2005" time="13:52:07" cpuActive= "5" cpuIdle= "95" />
```

Log File Duration

A server monitor log file contains performance data spanning a day or month, depending on which value you select in the **nodemgr.cfg** file. The default value is daily. For example:

```
SERVERMONITOR_LOG_GRANULARITY 'monthly/daily'
```

Log File Retention

You can specify the number of performance logs the Node Manager will retain. The default value of 180 allows for half of a year of data retention. For example:

```
SERVERMONITOR_LOG_RETENTION '###'
```

Log File Rollover

As a new day or month begins, the Node Manager automatically opens a file for the new period. At that time, the Node Manager also performs post-processing on the XML file from the previous day or month. The post-processing involves adding opening and closing tags to the XML file to ensure the data is well-formed.

CSV File Creation

For each performance log XML file, the Node Manager creates a corresponding CSV file. This command-delimited file mirrors the information present in the performance log XML file, and is suitable for importing into Microsoft Excel. For example:

```
Date,time,cpuActive,cpuIdle
04/27/2005,13:49:07,4,96
04/27/2005,13:49:07,6,94
04/27/2005,13:49:07,5,95
```

Log File Naming

The performance log files (XML and CSV), are named according to the statistical category and time period to which they pertain. The datestamp is in the format: YearMonthDay. For example:

```
cpu_utilization_20050431.xml (daily)
cpu_utilization_20050431.csv
cpu_utilization_200504.xml (monthly)
cpu_utilization_200504.csv
```

Using Logs to Monitor Offline Mediation Controller Components

Offline Mediation Controller records system activity in log files. One log file is generated for each Offline Mediation Controller component and for each node on the mediation host. Review the log files daily to monitor your system and detect and diagnose system problems.

Types of Log Files

Offline Mediation Controller generates log files for Offline Mediation Controller components and for the nodes you create.

Log Files for Offline Mediation Controller Components

For Offline Mediation Controller components such as Administration Server, Node Manager, and Administration Client, log files are named *component.log*; for example, **nodemgr.log**, **adminserver.log**, and **GUI.log**. The closed log files are saved using the Offline Mediation Controller component or cartridge node name, and an incrementing number; for example, **nodemgr.log.1**, **nodemgr.log.2**.

Log Files for Offline Mediation Controller Nodes on the Mediation Host

For each node on the mediation host, the log file is named *nodeID.log*, where *nodeID* is the unique ID that is assigned by Administration Server when you create a node on a mediation host; for example, if the unique ID of the node is **2ys4tt-16it-hslskvi1**, the log file name is **2ys4tt-16it-hslskvi1.log**.

Location of Log Files

The following are the minimum Offline Mediation Controller log files:

- **nodemgr.log**
- **adminserver.log**
- **GUI.log**

Depending on the number of nodes you create, your installation will have one or more node log files.

Default Log File Locations

The log files for Offline Mediation Controller components are stored in the *OMC_home/log/component* directory; for example, the Node Manager log file is in the *OMC_home/log/nodemgr* directory.

The log files for the nodes are stored in the *OMC_home/log/nodeID* directory; for example, if the node ID of the node is **2ys4tt-16it-hslskvi1**, the node log file is in the *OMC_home/log/2ys4tt-16it-hslskvi1* directory.



Note:

Oracle recommends that you not change the default location of the log files. If you change the location of the log files, you cannot access the log information from Administration Client.

Table 4-4 lists the components and their corresponding log file locations.

Table 4-4 Offline Mediation Controller Components and Log File Locations

Component	Log File Locations
Node Manager	<i>OMC_home/log/nodemgr/nodemgr.log</i>
Administration Server	<i>OMC_home/log/adminserver/adminserver.log</i>
Administration Client	<i>OMC_home/log/gui/GUI.log</i>
Node	<i>OMC_home/log/nodeID/nodeID.log</i>

About the Logger Properties Files

Each Offline Mediation Controller component or node has its own logger properties file. When an Offline Mediation Controller component or a node is started for the first time, the logger properties file is dynamically created in the *OMC_home/config/component* directory. By default, the logger properties file is set to the default logging level.

Table 4-5 lists the components and their corresponding logger properties file locations.

Table 4-5 Offline Mediation Controller Components and Logger Properties File Locations

Component	Logger Properties File Locations
Node Manager	<i>OMC_home/config/nodemgr/nodemgrLogger.properties</i>
Administration Server	<i>OMC_home/config/adminserver/adminserverLogger.properties</i>
Administration Client	<i>OMC_home/config/GUI/GUILogger.properties</i>
Node	<i>OMC_home/config/nodeID/nodeIDLogger.properties</i>

Setting the Reporting Level for Logging Messages

By default, Offline Mediation Controller components report information messages. You can set Offline Mediation Controller to report or to not report information messages. The following levels of reporting are supported:

- **NO** = No logging
- **WARN** = Log only warning messages
- **INFO** = Log information messages (default)
- **DEBUG** = Log debug messages
- **ALL** = Log warning, information, and debug messages



Note:

To avoid performance degradation, use INFO level logging for debugging.

To change the severity level for logging:

1. Open the logger properties file for the component in a text editor. See "[About the Logger Properties Files](#)".
2. Search for the following entry:

```
log4j.logger.componentName.component=severity,componentAppender
```

where:

- *componentName* is the name of the Offline Mediation Controller component.
- *component* is the Offline Mediation Controller component or the node ID.
- *severity* is the current severity level for the logging.

For example:

```
log4j.logger.NodeManager.nodemgr=WARN,nodemgrAppender
```

3. Change the entry to the desired severity level for logging.

For example, to change the log level from WARN to INFO for Node Manager:

```
log4j.logger.NodeManager.nodemgr=INFO,nodemgrAppender
```

4. Save and close the file.



Note:

You do not need to restart the running process to enable the changes in the logging level. A predefined delay of two minutes is set before the changed logger configuration takes effect.

5

Backing Up and Restoring Offline Mediation Controller

Learn about the tasks that you perform to back up and restore Oracle Communications Offline Mediation Controller.

Topics in this document:

- [About Backup and Restore Options](#)
- [Backing Up a Standard Configuration](#)
- [Backing Up a Complete System](#)
- [Restoring Offline Mediation Controller](#)
- [Preserving Data When No Backup Exists](#)
- [Backing Up and Restoring NAR Files](#)

About Backup and Restore Options

After installing or upgrading an Offline Mediation Controller system, perform one or both of the following backups as a safety measure:

- Standard configuration backup
- Complete system backup

Repeat the backups whenever you make incremental changes to the system configuration or rule files.

If you have not backed up the system regularly, reinstall and reconfigure a system corrupted by an operational error such as an AC power interruption or a disk full condition. Reinstalling and reconfiguring eliminates any chance of recovering and reprocessing mediation data transitioning through the system at the time of the operational error.

About Standard Configuration Backups

The standard configuration backup captures the configuration of an entire Offline Mediation Controller host, provided that you have not made any modifications to it other than those possible through Administration Client.

Perform this backup as soon as you have configured Offline Mediation Controller, even if you have performed a complete system backup.

When you complete a standard configuration backup, you can use the backup configuration directory to restore the Offline Mediation Controller system.

You restore an Offline Mediation Controller system by replacing the damaged configuration directory with a copy of the backup configuration directory. In this circumstance, you restore the system with the same node IDs and data directory structure, and with user data retained in **input**, **output**, and **scratch** directories at the time of the operational error.

 **Note:**

If you require Offline Mediation Controller technical support, email a copy of your backup configuration directory to your Oracle Global Support representative. If you want to send a copy of your configuration directory, use the Linux **tar** command to create an archived version of that directory.

About Complete System Backups

The complete system backup backs up the configuration of an Offline Mediation Controller host that you have modified extensively by a means other than Administration Client. For example, you may want to perform this procedure if you modified rule files and applied software patches.

Perform this backup as soon as you have configured Offline Mediation Controller. After you perform this backup, use the resulting **tar** file to fully restore your customized Offline Mediation Controller system. You can use the restoration procedure to restore an existing system or to install the same Offline Mediation Controller system configuration on another host.

For information on complete system backups, refer to your operating system documentation.

Backing Up a Standard Configuration

To back up a standard Offline Mediation Controller system configuration:

 **Note:**

This procedure backs up node chain configurations; it does not back up data.

1. Stop all functional nodes in the system:
 - a. In Administration Client, select all nodes.
 - b. Right-click and select **stop node(s)**.
2. Go to *OMC_home*, where *OMC_home* is the directory in which Offline Mediation Controller is installed.

3. Copy the directory configuration with a new name:

```
cp -r config DirectoryName
```

4. Create an archive of the entire directory:

```
tar cvf DirectoryName.tar DirectoryName
```

5. Store the backup copy in a location outside of the Offline Mediation Controller system:

```
mv DirectoryName.tar new_directory
```

6. Restart the nodes:

- a. In Administration Client, select all nodes.
- b. Right-click and select **start node(s)**.

Backing Up a Complete System

This procedure backs up node chain configurations and data in transit, but it does not back up processed data outside of the installation directory.

To back up a complete system:

1. Ensure the disk partition in which your Offline Mediation Controller system resides has more than 70 percent of its total reserved space still available.
2. Go to *OMC_home/bin* and run the following command, which shuts down the entire system:

```
./ProcessControl stop
```

3. Create a copy of the installation directory.

This operation may take a few minutes to finish.

4. Go to the copy of the installation directory.

5. In the copy of the installation directory, remove the **input**, **output**, and **scratch** subdirectories:

```
rm -r input output scratch
```

This prevents the restoration of old and duplicate billing records when you restore a full installation.

6. Create an archive of the duplicate installation directory.

This operation may take a few minutes to finish.

7. Store a copy of the **tar** file image of your Offline Mediation Controller system at a different location.
8. Remove the copy of the installation directory.
9. Restart Offline Mediation Controller.

Restoring Offline Mediation Controller

This section outlines how to restore Offline Mediation Controller for standard configuration backups and complete system backups.

Note:

You must shut down all Administration Clients before performing a restore operation to ensure the restored configuration is accurate. Failure to shut down Administration Clients before performing a restore operation can result in overwriting the restored configuration.

If you customized any part of Offline Mediation Controller by a means other than Administration Client and the system is corrupt, restore the system as a standard configuration. If that procedure does not restore the system, restore it as a complete system.

If the disk partition in which Offline Mediation Controller resides is full, you must create, at the same level as the existing installation directory, enough space to restore your system. The amount of space that you create depends on whether you need to save data from the **input**, **output**, and **scratch** subdirectories.

- If you do not need to save data from the **input**, **output**, and **scratch** subdirectories, create at least three times the disk space normally occupied by your archived installation directory.
- If you need to save data from the **input**, **output**, and **scratch** subdirectories, create at least three times the disk space collectively occupied by your archived installation directory plus **input**, **output**, and **scratch** subdirectories.

In the following sample system restoration, you must create space within the installation directory **/ocomc**. The archive file containing the installation directory is **ocomcbackup.tar**.

Restoring a Standard System Configuration

To restore a standard system configuration:

1. Obtain the backup copy of your system **/config** directory.
2. If you retrieved a **tar** file copy of the backup configuration directory, extract the configuration directory.

```
tar xvf DirectoryName.tar
```

The *DirectoryName* directory and structure is created.

3. Go to *OMC_home* and run the following command, which stops Offline Mediation Controller:

```
./ProcessControl stop
```

4. Go to *OMC_home* and remove the damaged configuration directory:

```
rm -r config
```

5. Copy the backup configuration directory into the system installation directory:

```
cp -r DirectoryName config
```

6. Restart the Offline Mediation Controller system:

```
cd OMC_home/bin  
./ProcessControl start
```

Restoring a Complete System Backup

To restore a full Offline Mediation Controller system:

1. At the command prompt, run the following command to shut down the Offline Mediation Controller system:

```
cd OMC_home/bin  
./ProcessControl stop
```

2. Retrieve the backup **tar** file of your system installation directory.
3. Extract from the **tar** file the backup copy of your installation directory:

```
tar xvf /ocomcbackup.tar
```

The command re-creates the duplicate installation directory, in this example, **/ocomctmp**.

4. To save as much data as possible from Offline Mediation Controller, go to the existing installation directory.
5. If you determine the directory is not corrupt, copy the **input**, **output**, and **scratch** subdirectories into the duplicate installation directory.

```
cp -r input /ocomctmp/  
cp -r output /ocomctmp/  
cp -r scratch /ocomctmp/
```

 **Note:**

Duplicate records may occur because you do not know which records have already been sent to the billing system.

6. Delete or rename the corrupted installation directory.
 - To delete, run the following command:

```
rm -r /ocomc
```
 - To rename, run the following command:

```
mv /ocomc /ocomcdata
```
7. Rename the restored installation directory:

```
mv /ocomctmp /ocomc
```
8. Go to **/ocomc/bin** directory and run the following command to restart the system:

```
./ProcessControl start
```
9. The system recreates the **input**, **output**, and **scratch** directories in your restored installation directory, unless you have already copied them over.

Preserving Data When No Backup Exists

Oracle does not support any procedure for restoring an Offline Mediation Controller system that has not been backed up. If you have no backup and you want to save as much existing NAR data as possible, Oracle recommends the following procedure.

To preserve data:

1. Stop all functional nodes in the system:
 - a. In Administration Client, select all nodes.
 - b. Right-click and select **stop node(s)**.
2. Restart one node at a time, beginning with the node at the end of the corrupted chain.

A node may be unable to read corrupt NARs from its **input** directory and may stall during restart. After you finish observing the behavior of one node, stop it and move on to the next node in the chain.

3. Run the following command:

```
iostat int 1
```

The output resembles the following listing:

```
iostat int 1
tty sd0 sd1 sd2 cpu
tin tout Kps tps serv Kps tps serv Kps tps serv us sy wt id
1 0 1 0 64 0 0 274 0 0 486 0 0 0 100
0 66 0 0 0 0 0 0 0 0 0 0 0 0 100
0 66 0 0 0 0 0 0 0 0 0 0 0 0 100
0 66 0 0 0 0 0 0 0 0 0 0 0 0 100
```

The last column on the right represents the percentage of total CPU idle time. The lower the number in this column, the more CPU time is being used to service functional nodes running in the system. When a node stalls, the CPU idles more frequently, causing the idle percentage value to rise.

4. Periodically list or monitor the number of NAR files in the node input directory by running one of the following commands:

```
ls | wc
```

While a functional node runs, it consumes at least 50 percent of the CPU idle time on a dual processor machine. If the CPU percentage idle is near 100 percent and the number of NAR files in the **input** directory is not going down, then it is possible that the NAR file currently being read by the functional node from its **input** directory is corrupt. The NAR file currently being processed is the one with the oldest time stamp in its name.

5. Stop the node and use the **rm** or **mv** command to remove the suspect NAR file from the **input** directory.
6. Restart the node.

If the CPU idle percentage number decreases, then there is an increased level of CPU usage for node processing. If you do not observe this, then the NAR file you removed probably was not corrupt. In this case, stop the node, remove the contents of its **scratch** directory, and restart the node. The node resumes processing the NAR files from its **input** directory.

If the node continues to stall, stop it, and remove the entire contents of its **input** directory. Restart the node and it resumes processing the NAR files from its **input** directory.

7. Repeat these actions for each node in the chain, as necessary, to identify the corrupt NAR files and to restore system operation.

Call Oracle Global Support for further assistance restoring an Offline Mediation Controller system that has not been backed up.

Backing Up and Restoring NAR Files

If an adverse operational event, such as AC power interruption, mediation host failure, or a hardware or software error corrupts NAR data or prevents one or more processed NARs from being delivered to their destinations, you can restore and reprocess the

previously backed up NAR files. You can also engage safe mode on an E250 workstation.

The NAR file backup is available for certain nodes and is enabled through the node configuration window.

During a NAR backup, the system moves each processed NAR file from the **input** directory to the backup directory of a node and changes the NAR file extension from **.arch** to **.archbkup**.

When you restore a backed-up NAR file, you change its file extension from **.archbkup** to **.arch** in the backup directory and move or copy the renamed file into the node's **input** directory. Then, the node processes the NAR file and returns it to the backup directory with the file's last-modification date or timestamp intact. The system processes the NAR files according to their last-modification timestamp, starting with those having the earliest timestamp.

How you restore a backup file determines when the file is reprocessed by the node and the length of time that the file remains in the backup directory after reprocessing.

- If you restore a NAR file by moving it from the backup directory to the **input** directory, the file's last modification time does not change.
- If you restore a NAR file by copying it from the backup directory to the **input** directory, the system creates a new file with a modification time set to the current system time.

Backing Up NAR Files

To restore NAR files backed up for a specific node, you must enable and configure the node's automated NAR file backup feature.

1. After you detect corrupted NAR data in the downstream mediation or OAM system, determine:
 - The time the problem began
 - The effect of the problem on your system
 - The source of the problem if possible
2. Before you restore any NAR files, identify and repair the source of the problem.
3. Clean up any suspect downstream data. You may need to delete some or all of the affected data.
4. Determine which backup NAR files need to be restored by comparing the time the problem began to the timestamp contained in the name of each backup NAR file associated with the affected node chains.

The NAR file timestamp indicates the moment the backup file was created. The file contains data captured from that time forward, up to the configured NAR file size. Restore the sequence of backup NAR files that covers the full interval during which the problem occurred. See "[Restoring Offline Mediation Controller](#)" for more information.

Restoring NAR Files

To restore NAR files:

1. Log on to Administration Client and determine the ID of the node with the NAR file that you want to restore.
2. Select the mediation server on which the node that you want to examine resides.

3. Select the functional node and click **Edit**.
The Node dialog box opens displaying the node ID.
4. Stop the node.
5. Go to *OMC_home* and run the following command:

```
ls input backup
```

A list of subdirectories named for the ID of each node appears.

For example:

```
backup:
1hb48pz-8ha-cdyeaz08 1hb48pz-8ha-cdyex5zr 1hb48pz-8ha-cdyf91bt
1hb48pz-8ha-cdyek5t1 1hb48pz-8ha-cdyf5xxu 1hb48pz-8ha-cdyfabet
1hb48pz-8ha-cdyel3we 1hb48pz-8ha-cdyf7gvb 1hb48pz-8ha-cdynof9c
1hb48pz-8ha-cdyetth6 1hb48pz-8ha-cdyf8a5n
input:
1hb48pz-8ha-cdyeaz08 1hb48pz-8ha-cdyex5zr 1hb48pz-8ha-cdyf91bt
1hb48pz-8ha-cdyek5t1 1hb48pz-8ha-cdyf5xxu 1hb48pz-8ha-cdyfabet
1hb48pz-8ha-cdyel3we 1hb48pz-8ha-cdyf7gvb 1hb48pz-8ha-cdynof9c
1hb48pz-8ha-cdyetth6 1hb48pz-8ha-cdyf8a5n
```

6. Go to the **backup** directory that contains a NAR file that you want to restore.

For example:

```
cd 1hb48pz-8ha-cdyeaz08
```

7. Move or copy the NAR file from the node's backup directory to its **input** directory:

```
mv NAR_file_name .archbkup ../input/NAR_file_name.arch
```

8. Rename the file from *filename.archbkup* to *filename.arch*.
9. Start the node.

The node reprocesses the NAR file.

6

Troubleshooting Offline Mediation Controller

Learn how to troubleshoot problems in Oracle Communications Offline Mediation Controller.

Topics in this document:

- [Troubleshooting Checklist](#)
- [Using Error Logs to Troubleshoot Offline Mediation Controller](#)
- [Getting Help for Offline Mediation Controller Problems](#)
- [Common Problems and Their Solutions](#)

Troubleshooting Checklist

When any problems occur, it is best to do some troubleshooting before you contact Oracle Global Support:

- You know your installation better than Oracle Global Support does. You know if anything in the system has been changed, so you are more likely to know where to look first.
- Troubleshooting skills are important. Relying on Oracle Global Support to research and solve all of your problems prevents you from being in full control of your system.

If you have a problem with your Offline Mediation Controller system, ask yourself these questions first, because Oracle Global Support will ask them of you:

- What exactly is the problem? Can you isolate it?
Oracle Global Support needs a clear and concise description of the problem, including when it began to occur.
- What do the log files say?
This is the first thing that Oracle Global Support asks for. Check the error log for the Offline Mediation Controller component you are having problems with.
- Has anything changed in the system? Did you install any new hardware or new software? Did the network change in any way? Does the problem resemble another one you had previously? Has your system usage recently jumped significantly?
- Is the system otherwise operating normally? Has response time or the level of system resources changed? Are users complaining about additional or different problems?

Using Error Logs to Troubleshoot Offline Mediation Controller

Offline Mediation Controller error log files provide detailed information about system problems. If you are having a problem with Offline Mediation Controller, look in the log files.

Offline Mediation Controller logs specific details about actions performed in the Offline Mediation Controller GUI in Administration Server log files.

Getting Help for Offline Mediation Controller Problems

If you cannot resolve the Offline Mediation Controller problem, contact Oracle Global Support.

Before you contact Oracle Global Support, try to resolve the problem with the information logged in the log files. If this does not help to resolve the problem, note the following information:

- A clear and concise description of the problem, including when it began to occur.
- Relevant portions of the relevant log files.
- Relevant configuration files.
- Recent changes in your system after which the problem occurred, even if you do not think they are relevant.
- List of all Offline Mediation Controller components and patches installed on your system.

When you are ready, report the problem to Oracle Global Support.

Common Problems and Their Solutions

Although Offline Mediation Controller is designed to be trouble free, you might encounter a problem. You can view descriptions of some common problems along with their solutions:

- [Problem: ps: illegal option](#)
- [Problem: keytool error: java.io.FileNotFoundException While Creating Administration Server Certificate](#)
- [Problem: keytool error: java.io.FileNotFoundException While Creating Node Manager Certificate](#)
- [Problem: com.maverick.ssh.SshException When FTP is Used in Collection or Distribution Cartridge Pack](#)
- [Problem: Error While Starting Node Manager with SSL Enabled](#)

Problem: ps: illegal option

When you start Node Manager or the Administrative Server, you receive a "ps: illegal option" error message.

Possible Cause

The **ps** script from the **ucb** package is used. You must use the **ps** script in the **/usr/bin** or **/bin** directory.

Solution

In the PATH environment variable, make sure that **/usr/bin** and **/bin** appear before **/usr/ucb**.

Problem: keytool error: java.io.FileNotFoundException While Creating Administration Server Certificate

After installing only Administration Server, when you run the **createAdminSvrCert** script to create the Administration Server certificate, you receive the "keytool error: java.io.FileNotFoundException: *OMC_home/config/GUI/adminClientTruststore.jks* (No such file or directory)" error message, where *OMC_home* is the directory in which Offline Mediation Controller is installed.

Possible Cause

The *OMC_home/config/GUI/adminClientTruststore.jks* file does not exist.

Solution

You must manually import the Administration Server's public certificate into the Administration Client's TrustStore.

To manually import the Administration Server's public certificate into the Administration Client's TrustStore:

1. Log on to the system on which Offline Mediation Controller is installed.
2. Run the following command:

```
OMC_home/jre/bin/keytool -import -v -trustcacerts -alias adminServer -file  
OMC_home/config/adminserver/adminServer.cer -keystore OMC_home/config/GUI/  
adminClientTruststore.jks
```

The **Enter keystore password** prompt appears.

3. Enter the Administration Client's TrustStore password.

The **Trust this certificate** prompt appears.

4. Enter **y**, which trusts the certificate.

The Administration Server's public certificate is imported into the Administration Server's TrustStore.

Problem: keytool error: java.io.FileNotFoundException While Creating Node Manager Certificate

After installing only Node Manager, when you run the **createNodeMgrCert** script to create the Node Manager certificate, you receive the "keytool error: java.io.FileNotFoundException: *OMC_home/config/adminserver/adminServerTuststore.jks* (No such file or directory)" error message.

Possible Cause

The *OMC_home/config/adminserver/adminServerTuststore.jks* file does not exist.

Solution

You must manually import the Node Manager's public certificate into the Administration Server's TrustStore.

To manually import the Node Manager's public certificate into the Administration Server's TrustStore:

1. Log on to the system on which Offline Mediation Controller is installed.
2. Run the following command:

```
OMC_home/jre/bin/keytool -import -v -trustcacerts -alias nodeManager -file  
OMC_home/config/nodemgr/nodeManager.cer -keystore OMC_home/config/  
adminserver/adminServerTruststore.jks
```

The **Enter KeyStore password** prompt appears.

3. Enter the Administration Server's KeyStore (TrustStore) password.

The **Trust this certificate** prompt appears.

4. Enter **y**, which trusts the certificate.

The Node Manager's public certificate is imported into the Administration Server's TrustStore.

Problem: com.maverick.ssh.SshException When FTP is Used in Collection or Distribution Cartridge Pack

When File Transfer Protocol (FTP) is used in the Collection or Distribution cartridge pack, you receive the "com.maverick.ssh.SshException" error.

Possible Cause

All of the required security providers are not included in the Java security files.

Solution

Manually copy the following JAR files into the *Java_home\jre\lib\ext* directory (where *Java_home* is the directory in which the supported version of Java is installed) and then restart the system:

- **bcprov-ext-jdk15on-158.jar**
- **bcprov-jdk15on-158.jar**

To restart the system, see "[Starting and Stopping Offline Mediation Controller](#)".

Problem: Error While Starting Node Manager with SSL Enabled

When you start Node Manager with Secure Sockets Layer (SSL) enabled, you receive the following error:

```
Cannot support TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 with currently installed  
providers
```

Possible Cause

All of the required security providers are not included in the Java security files.

Solution

Manually copy the JARs from the **jce_policy-8.zip** file into the *Java_home\jre\lib* directory and then restart the system. You can download this file from Oracle Technology Network:

<https://www.oracle.com/java/technologies/javase-jce8-downloads.html>

To restart the system, see "[Starting and Stopping Offline Mediation Controller](#)".

A

Offline Mediation Controller Directory Structure and Contents

Learn about the Oracle Communications Offline Mediation Controller directory structure and contents.

Topics in this document:

- [Directory Structure and Contents](#)

Directory Structure and Contents

The main install directory for the system contains several sub-directories. Each contains specific types of files for various purposes. The following lists all of the directories used by the system:

- **3rdparty_jars**: Contains all custom JAR files.
- **bin**: Contains script files used to run Offline Mediation Controller.
- **cartridges**: Contains all cartridge pack JAR files.
- **config**: Contains the nodes' configuration data. This data is input through the configuration GUI.
- **customization**: Contains the customized classes, rules files, and templates.
- **datadict**: Holds the dictionary of attributes for the entire system. This dictionary is not referenced in real-time by the system. It is a static reference.
- **datafiles**
- **input**: Contains the input directories for all nodes. Collection cartridges may not make use of these input directories.
- **jre**:
- **licenses**
- **log**
- **output**: Contains the output directories for all nodes. Distribution cartridges may not make use of these output directories.
- **rules**: Contains the NPL files, which are also referred to as rule files. The sub-directories are organized by node type. For example, CC, DC, and Processor nodes are referred to as the major node types. Further sub-directories are organized by the minor node types. For example "FlatFileOI".
- **scratch**: Contains the scratch area for all nodes. The scratch is used as a temporary area for all nodes prior to the data being passed to its output.
- **web**: Contains compiled NPL files, or class files. The sub-directories here are also organized by node types similar to the rules directories.
- **xslt**