

Oracle® Communications Session Monitor

Mediation Engine Connector User's Guide

Release 4.0

E89195-02

January 2018

Copyright © 2017, 2018, Oracle and/or its affiliates. All rights reserved.

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

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

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

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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

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

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

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

Contents

Preface	v
Audience	v
Downloading Oracle Communications Documentation	v
Documentation Accessibility	v
Document Revision History	v
 1 Overview of the Mediation Engine Connector User Interface	
Logging In to Mediation Engine Connector	1-1
About the Mediation Engine Connector Dashboard	1-1
Adding a Dashboard Panel	1-2
Removing a Dashboard Panel	1-2
Adding a Group Tab	1-2
Rearranging Dashboard Panels	1-3
Enabling Dashboard Panel Refresh	1-3
About Dashboard Panels	1-3
Call Search Panel	1-3
Active Calls Counter Panel	1-5
About Mediation Engine Selection and View	1-6
 2 Configuring Mediation Engine Connector	
Changing the Default Administrator Password	2-1
Configuring Users and Realms	2-1
Configuring Realms	2-2
Configuring User Access	2-3
Configuring External Authentication Authorization	2-3
Configuring the Mediation Engine Connector URL and Authentication Secret	2-3
Connecting Mediation Engine with Mediation Engine Connector	2-4
Disconnecting Mediation Engine from Mediation Engine Connector	2-5
Setting the Timeout for Call Searches in Mediation Engine Connector	2-6
Adding Mediation Engines	2-7
Password Settings for User Account	2-9
 3 Configuring Mediation Engines	
Setting Mediation Engine Connector Configurations	3-1
Setting Mediation Engine Configurations	3-2

Setting a Node Connection Timeout	3-2
Testing Connections between Mediation Engines.....	3-3
Understanding Mediation Engine Connection Testing Error Codes	3-3
Understanding Call Correlation	3-4
Implementing Call Correlation	3-4
Configuring Multiple Mediation Engine Nodes for Call Correlation.....	3-6
Setting the Authentication of a Mediation Engine.....	3-6
Setting the Authentication of Mediation Engine Connector	3-6
Adding the Mediation Engines to the Mediation Engine Connector Node List	3-7
Testing the Connection	3-7
Setting the Platform Devices for Each Mediation Engine	3-8
Applying Configuration Changes	3-8
(Optional) Setting the Timeout for Call Searches.....	3-8
Viewing Correlation Calls	3-9

Glossary

Preface

This guide describes how to configure and use Oracle Communications Session Monitor Mediation Engine Connector.

The Oracle Communications Session Monitor product family includes the following products:

- Operations Monitor
- Enterprise Operations Monitor
- Fraud Monitor
- Control Plane Monitor

Audience

This guide is intended for SIP and IMS network operators who install and administer Oracle Communications Session Monitor.

Downloading Oracle Communications Documentation

Oracle Communications Session Monitor documentation and additional Oracle documentation is available from the Oracle Help Center Web Site:

<http://docs.oracle.com>

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.

Document Revision History

The following table lists the revision history for this document:

Version	Date	Description
E89195-01	November 2017	Initial release.
E89195-02	January 2018	Made multiple updates in the document.

Overview of the Mediation Engine Connector User Interface

This chapter provides an overview of the Oracle Communications Session Monitor Mediation Engine Connector user interface.

Logging In to Mediation Engine Connector

You must first install an instance of Mediation Engine Connector, connect it to your network, and access the user interface using a web browser. See the referenced sections when changing settings for additional details.

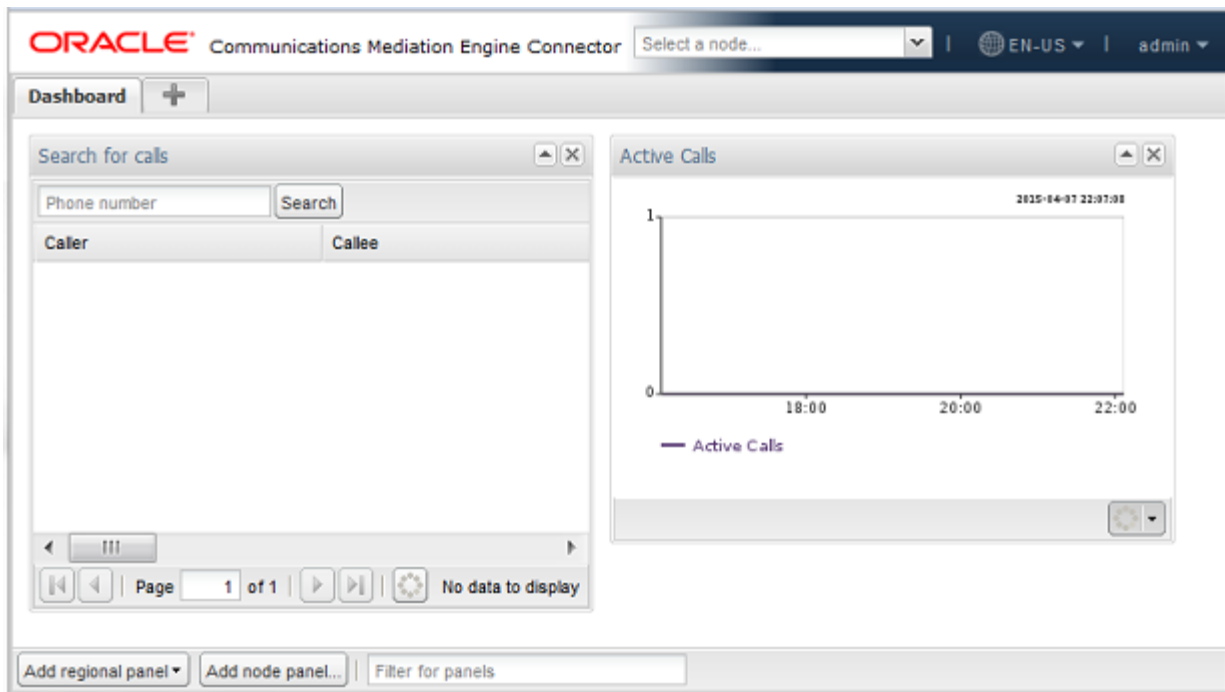
Note: Your browser must have JavaScript enabled. Additionally, allowing "[HTTP cookie](#)" is recommended for several of the features.

Point the browser to the configured IP address of the management interface to load the login screen. Log in with user name **admin** and password **oracle**.

About the Mediation Engine Connector Dashboard

After you log in, you should see the Mediation Engine Connector dashboard. In the top-right corner, a drop down menu displays the current user and contains links to the Mediation Engines window, the HTML version of this manual (opens in a new browser window), and the option to logout.

[Figure 1-1](#) shows the Mediation Engine Connector dashboard.

Figure 1–1 Mediation Engine Connector Dashboard

The Mediation Engine Connector dashboard is similar to the dashboard of the mediation engines. It allows you to view at a glance important information retrieved from single probes, as well as information aggregated from all mediation engines. The dashboard contains a configurable number of panels, which can be added or removed by the user. The following functionality is available for the Mediation Engine Connector dashboard.

Adding a Dashboard Panel

To add a dashboard panel:

1. Right-click on the dashboard.

A context menu appears.

2. Select **Add a panel...**

A wizard appears in a new window, which guides you through the creation of the new dashboard panel.

Removing a Dashboard Panel

To remove a dashboard panel:

1. Click the cross button in the upper-right corner of the panel.

A dialog box appears.

2. Click **Yes**.

Adding a Group Tab

To add a group tab:

1. Click **Add group tab** beside the **Dashboard** tab.

A **New Group 1** tab is created.

2. Double click the **New Group 1** tab and rename the panel group. You can create multiple dashboard panels.

Note: When a new widget is added in the **Dashboard** tab which is not the default, the widget gets added in the default dashboard.

Rearranging Dashboard Panels

Dashboard panels can be rearranged using drag and drop. Drag a dashboard panel by clicking and holding the title bar and drop it where you would like it to stay on the page.

Enabling Dashboard Panel Refresh

The information in a dashboard panel refreshes only when it is active in a dashboard tab. Panels refresh only when they are visible to the user in an active browser window. You can change this behavior to enable panels to continue to refresh when they are not displayed in an active browser window.

Note: Enabling panel refresh can cause decreased system performance.

To enable dashboard panels to refresh:

1. Select the menu title that displays your user name.
2. Click **My Profile**.

The **Edit own user information** menu appears.

3. From the **Widgets Refresh** list, select refresh options that you would like to enable.
4. Click **Finish**.

About Dashboard Panels

This section describe only panels containing aggregated information. Panels containing mediation engine-related information are the same as the panels for the dashboard of the mediation engine.

The Mediation Engine Connector dashboard can have the following types of panels:

- Panels containing aggregated information
- Panels containing information retrieved from a single mediation engine

Call Search Panel

The Call Search panel allows you to specify the search criteria and display matching unique calls on all probes simultaneously.

[Figure 1–2](#) shows the Call Search panel.

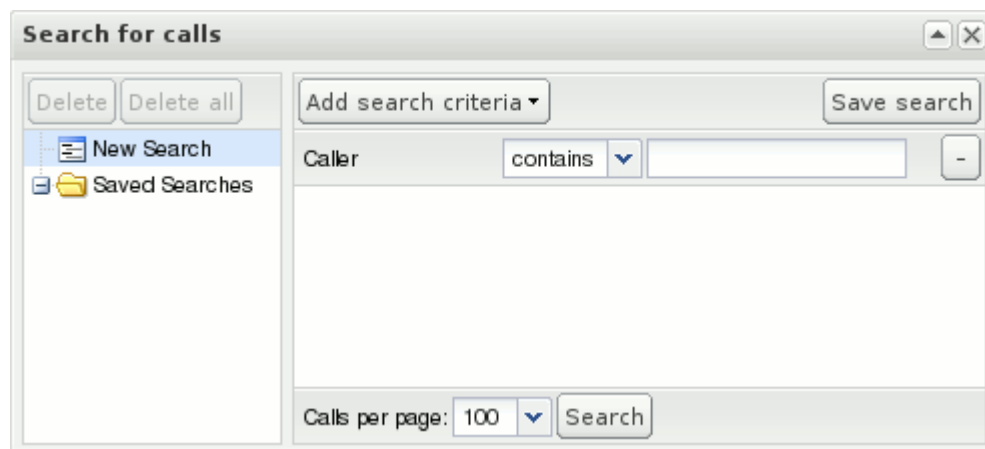
The Call Search panel provides the following functionality:

Enter search criteria: To enter the search criteria, click **Add search criteria** button and select the field for which you want to enter a search criterion. A new row appears in the center-right area of the Call Search panel. You can enter a comparison operator and a comparison value for the criterion in this row.

Execute a search: Click **Search** to execute the active search. The Call Search Results page appears.

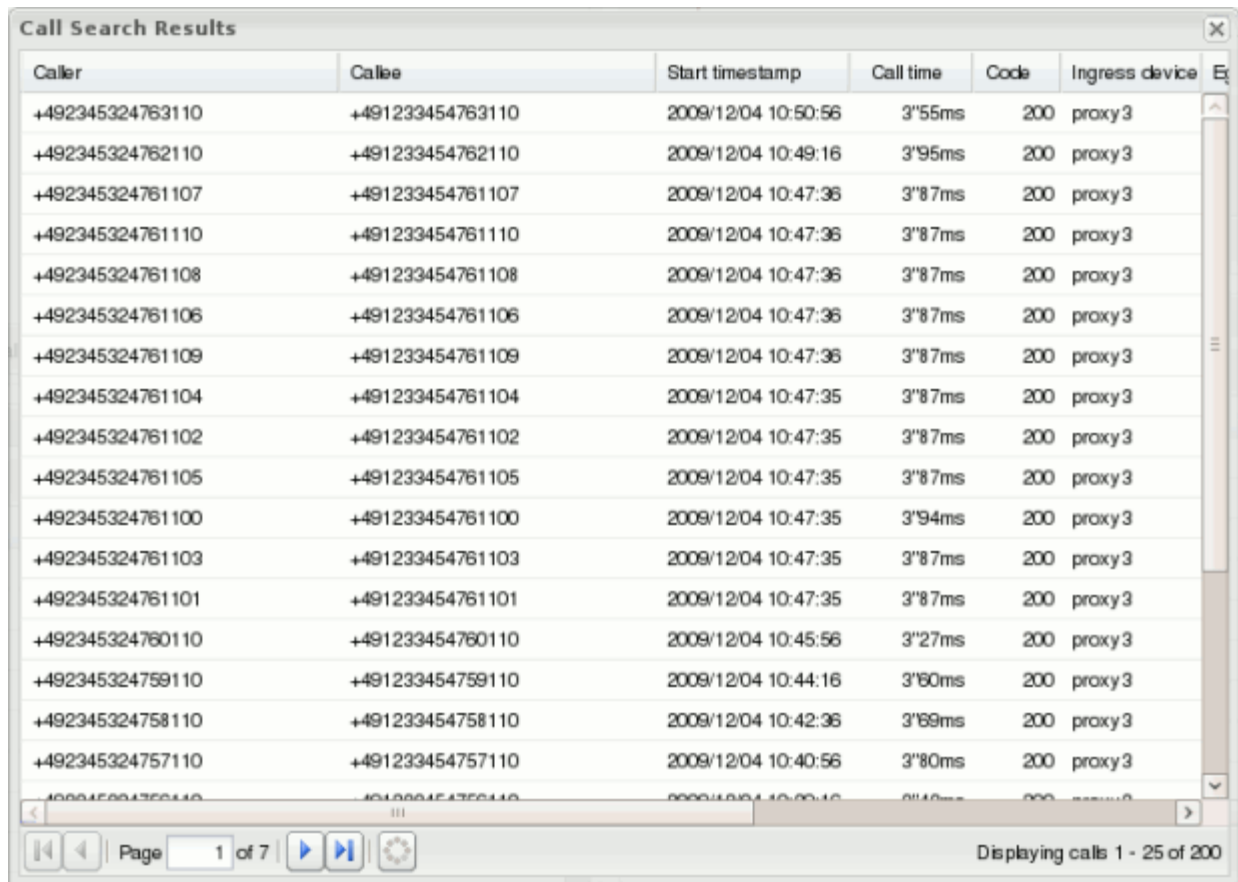
Save search and retrieve saved searches: You can save a search by clicking **Save Search**. A new node appears in the tree to the left of the panel, under the **Saved Searches** folder. To give a name to the saved search, click the tree node for the search and enter a name. To retrieve a previously saved search, click select a node from under the **Saved Searches** folder. You can also delete a saved search by selecting its node and clicking **Delete**. Clicking **Delete all** deletes all saved searches. Note, that saved searches will be gone, once you reload the page or logout from Mediation Engine Connector and login again.

Figure 1–2 Call Search Panel



Call Search Results page: The Call Search Results page appears after you execute a search and displays unique calls that match the search criteria found on all mediation engines.

Figure 1–3 shows an example of the call search results.

Figure 1–3 Call Search Results Page


Caller	Callee	Start timestamp	Call time	Code	Ingress device	Ex
+492345324763110	+491233454763110	2009/12/04 10:50:56	3"55ms	200	proxy3	
+492345324762110	+491233454762110	2009/12/04 10:49:16	3"95ms	200	proxy3	
+492345324761107	+491233454761107	2009/12/04 10:47:36	3"87ms	200	proxy3	
+492345324761110	+491233454761110	2009/12/04 10:47:36	3"87ms	200	proxy3	
+492345324761108	+491233454761108	2009/12/04 10:47:36	3"87ms	200	proxy3	
+492345324761106	+491233454761106	2009/12/04 10:47:36	3"87ms	200	proxy3	
+492345324761109	+491233454761109	2009/12/04 10:47:36	3"87ms	200	proxy3	
+492345324761104	+491233454761104	2009/12/04 10:47:35	3"87ms	200	proxy3	
+492345324761102	+491233454761102	2009/12/04 10:47:35	3"87ms	200	proxy3	
+492345324761105	+491233454761105	2009/12/04 10:47:35	3"87ms	200	proxy3	
+492345324761100	+491233454761100	2009/12/04 10:47:35	3"94ms	200	proxy3	
+492345324761103	+491233454761103	2009/12/04 10:47:35	3"87ms	200	proxy3	
+492345324761101	+491233454761101	2009/12/04 10:47:35	3"87ms	200	proxy3	
+492345324760110	+491233454760110	2009/12/04 10:45:56	3"27ms	200	proxy3	
+492345324759110	+491233454759110	2009/12/04 10:44:16	3"60ms	200	proxy3	
+492345324758110	+491233454758110	2009/12/04 10:42:36	3"69ms	200	proxy3	
+492345324757110	+491233454757110	2009/12/04 10:40:56	3"80ms	200	proxy3	
+492345324756110	+491233454756110	2009/12/04 10:40:16	3"10ms	200	proxy3	

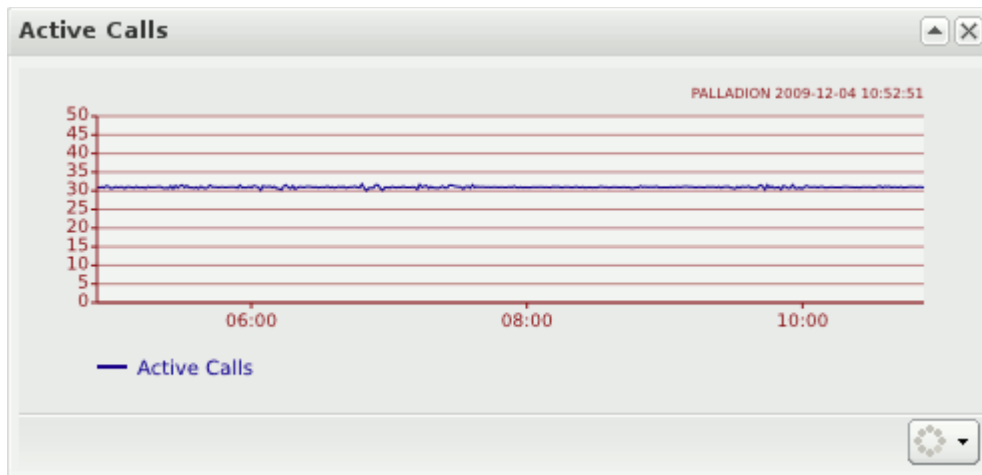
Page 1 of 7

Displaying calls 1 - 25 of 200

Active Calls Counter Panel

The Active Calls counter panel displays a chart which is computed based on values aggregated from all mediation engines. Currently the active calls counter is available. It is the only option present in the dashboard add panel wizard, when you choose **Display a counter**.

Figure 1–4 shows the Active Calls counter panel.

Figure 1–4 Active Calls Counter Panel

About Mediation Engine Selection and View

Mediation Engine Selection refers to the controls in the header bar of the Mediation Engine Connector user interface. These controls allow you to select a mediation engine to display in the mediation engine view.

Figure 1–5 shows the Mediation Engine selection drop-down list.

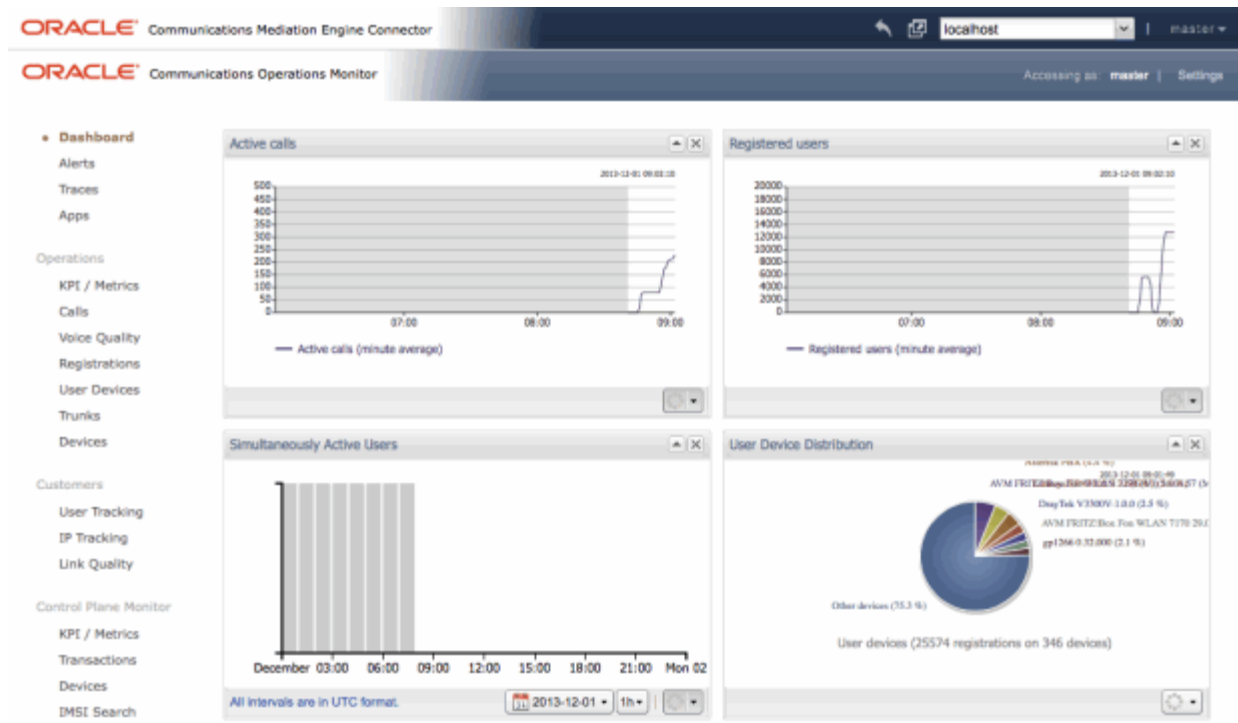
Figure 1–5 Mediation Engine Selection

Select the mediation engine you want to view from the drop-down list and the Mediation Engine view for this mediation engine is displayed. The Mediation Engine view is displayed in an iframe inside the Mediation Engine Connector user interface. You are automatically logged in with the user name that you are already log into the Mediation Engine Connector user interface.

Figure 1–6 shows the Mediation Engine view page.

You can also display the Mediation Engine view in its own window by clicking **Open in new window** button.

Figure 1–6 Mediation Engine View Page



Configuring Mediation Engine Connector

This chapter describes how to configure Oracle Communications Session Monitor Mediation Engine Connector.

Changing the Default Administrator Password

Start by changing the default administrator password. Click on the user name in the top-right corner and then on the **My Profile** link. The Edit own user information dialog box appears. Enter the new password twice and click **Finish**.

Warning: The default administrator password is easy to guess and is given in the product documentation, which is generally available to sub-users. Oracle strongly recommends changing the administrator password before creating any sub-users.

Configuring Users and Realms

Due to the powerful visibility that Mediation Engine Connector offers inside a network and the associated user privacy risks, a comprehensive user rights management system is available to restrict Mediation Engine Connector users to defined views and functionalities.

When using multiple Mediation Engines with a Mediation Engine Connector, the Mediation Engine Connector is responsible for managing users and realms. The user database and the realm definitions are entered using the Mediation Engine Connector user interface, which then distributes the information across the Mediation Engines. User database and realm definitions should be set up before the Mediation Engines are connected.

Note: When using multiple Mediation Engines with a Mediation Engine Connector, the Mediation Engine is not responsible for managing users, passwords, and realms.

When a user is created in the Mediation Engine Connector, the information about the user is propagated to all the nodes, but the KPIs for the user are not created. For creating the KPIs for the user, you should login into the Mediation Engine. However, when a user is deleted from the Mediation Engine Connector, the KPIs are also deleted for that user.

Configuring Realms

Realms are used to partition the captured data for presenting a separate view to each Mediation Engine Connector user. This is especially useful in cases where different resellers share the same Mediation Engine Connector instance, each being allowed to view only the SIP users served by themselves.

In the Mediation Engine Connector, a realm is defined by a pattern containing a set of telephone numbers, a set of domains, or both. Realms defined only by a range of telephone numbers should be used when the resellers share the same domain, but have different SIP users. Realms defined only by domain should be used when the Mediation Engine Connector is analyzing the traffic from multiple domains. A combination of both cases defines a pattern with a domain and a telephone number range.

Figure 2–1 shows the Realms Definitions section on the Mediation Engine Connector Settings page.

To add a pattern that defines a realm, click the **Add pattern** button. A new row appears at the top of the table. The pattern is editable by double clicking on the row.

Name: The name of the realm that defines a reseller.

First Number: The lower limit of the telephone numbers range.

Last Number: The higher limit of the telephone numbers range.

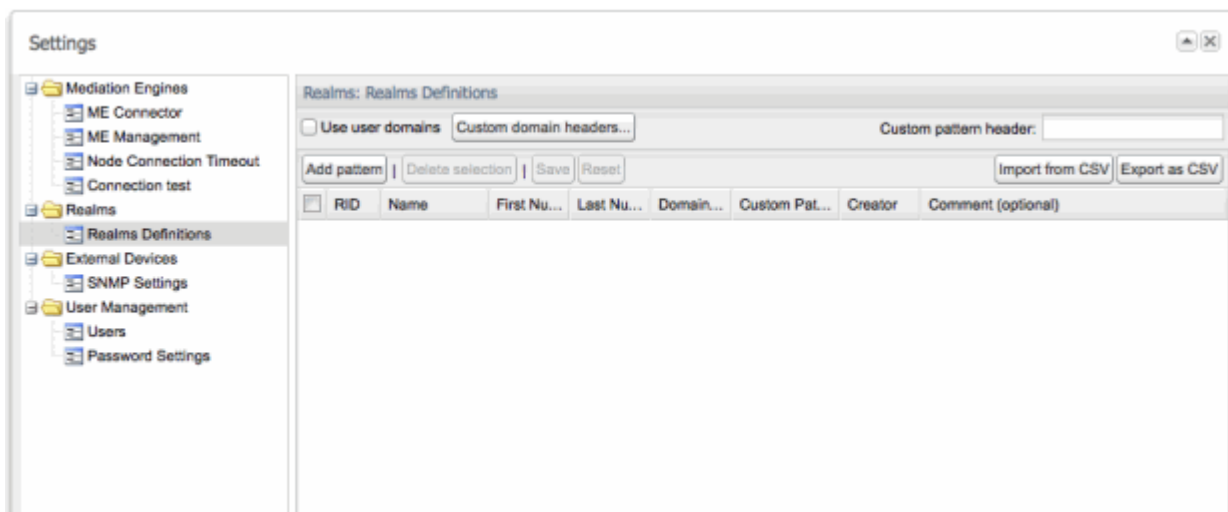
Domain: The domain name. The field is optional as the realm might be identified only by number range.

Comment: An optional comment line, only for convenience.

To delete a selected pattern, click **Delete selection**. You can import and export realm configuration to and from CSV files, which helps in maintaining the realm configuration when many patterns have been defined.

You may also provision realm patterns automatically by uploading a similar CSV file via FTP.

Figure 2–1 Realm Configuration



Configuring User Access

A *user* is identified by a name, a set of access rights, a set of relations with other users, a realm to which the user belongs, an e-mail address, and a logo image file.

Users are organized hierarchically, with **admin** being the root user (default password **oracle**) with unrestricted access. Every user can create a set of *sub-users*, who have less permissions than their parent user.

User interface access is defined by permissions, that control which pages or sections from the user interface the user can see and use, and should be defined by the parent user when the user is created.

User management is similar to the process in the Mediation Engines. The difference being that users provisioned in the Mediation Engine Connector are duplicated to all Mediation Engines belonging to it.

Configuring External Authentication Authorization

The Mediation Engine Connector supports authenticating users using an external authentication provider, like LDAP, RADIUS, or single sign-on authentication. This authentication must be configured on the reverse proxy (NGINX or Apache) which acts as a gateway for the Mediation Engine Connector. Authorization for the user must be done using Mediation Engine Connector permissions, as described in the section, "[Configuring User Access](#)".

If external authentication is enabled in the Mediation Engine Connector settings, the **X-Forwarded-User** HTTP header set by the reverse proxy must contain the authenticated user's login name. Configuration file for Apache, which sets up HTTP basic external authentication, can be found at the location, `/opt/oracle/ocsm/etc/httpd/conf.d`.

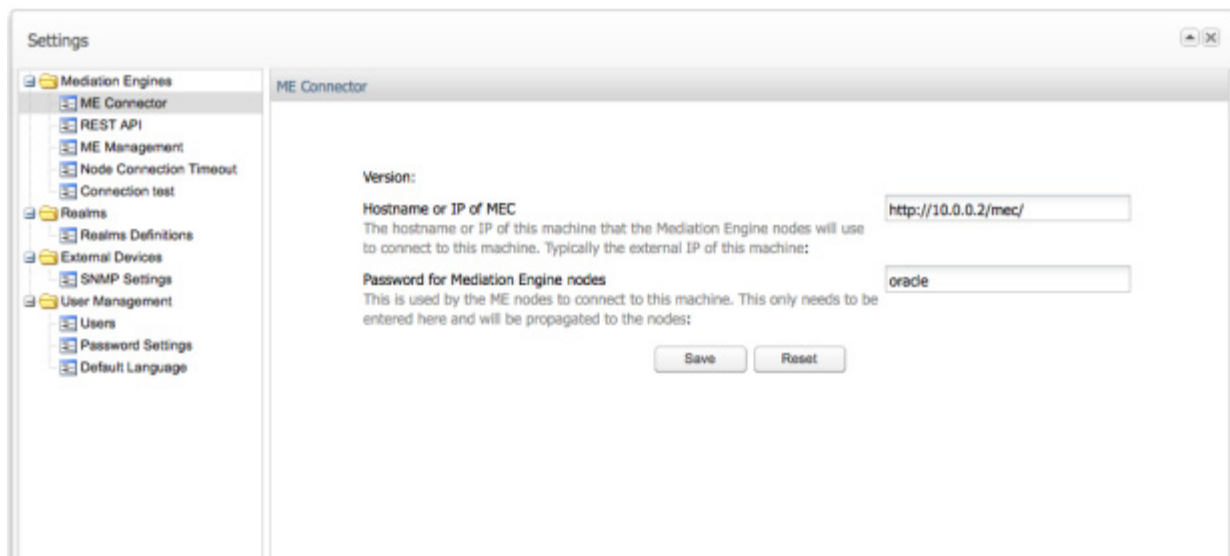
Configuring the Mediation Engine Connector URL and Authentication Secret

Mediation Engines communicate with their Mediation Engine Connector using an http address under which Mediation Engine Connector is reachable. In most cases, it appears in the form of `http://fully.qualified.hostname/`, where *fully.qualified.hostname* is the fully qualified hostname of the Mediation Engine Connector in your network.

You also need to enter an authentication secret, which is used to authenticate the Mediation Engines to Mediation Engine Connector.

These two settings can be entered on the Settings page in the Mediation Engine: ME Connector section.

[Figure 2-2](#) shows an example of Mediation Engine Connector settings.

Figure 2–2 Mediation Engine Connector Settings

Connecting Mediation Engine with Mediation Engine Connector

To connect Mediation Engine with Mediation Engine Connector:

1. Log into Mediation Engine.
2. Under Settings, click **ME Management**.
3. Select the desired node, double-click the disabled column field, and select yes from the drop-down list or click **Add** to add a new node.
4. (Optional) Add a new node by doing the following:
 - a. Click **Add**.
A new row gets added.
 - b. Double-click the **Node name** field, and enter the Mediation Engine node name.
 - c. Double-click the **Hostname or IP** field, enter the IP address or Hostname of the Mediation Engine.
 - d. Double-click the **Shared secret** field, enter the shared secret of the Mediation Engine.
 - e. The Connection responsive field auto populates as following:
 - True. If node entries are valid and node connection is successful.
 - False. If either node entries are not valid or the node connection is unsuccessful.
 - f. Double-click the **Disabled** field, select the option **yes** or **no** from the drop-down list for enabling or disabling the node.
5. Click **Save**.

Result: Mediation Engine node is added.

Important: When adding a new Mediation Engine, the list of local users on the Mediation Engine might be lost. Any local users and realms in the Mediation Engine will be replaced with the current list of users and realms that exist on the Mediation Engine Connector. If there are users and realms on the Mediation Engine that do not exist on the Mediation Engine Connector, these will be lost.

6. Log into Operation Monitor.
7. Click **Admin** and then click **Settings**.
8. Click **Mediation Engine Connector**.
9. In the **Authentication Token** field, enter your choice of token details for the Mediation Engine, and click **Update**.

Note: For Mediation Engine Connector to connect to Mediation Engine, the token values entered while adding the Mediation Engine node must match with the value mentioned in the Authentication Token field.

You must note down the token details for future reference.

Result: Mediation Engine connects with the Mediation Engine Connector.

Note: It is not possible to retrieve information about the calls in other nodes on that Mediation Engine node. By this procedure, the Mediation Engine and the Mediation Engine Connector are disconnected so the Mediation Engine will be on its own when it comes to information, it can use at that time. No other implications are known.

Disconnecting Mediation Engine from Mediation Engine Connector

To disconnect Mediation Engine from Mediation Engine Connector:

1. Log into Operation Monitor.
2. Click **Admin** and then click **Settings**.
3. Click **Network**.
4. Click **Mediation Engine Connector**.
5. Click **Unlink MEC...**

Note: You can only unlink Mediation Engine from Mediation Engine Connector by clicking Unlink MEC.... To connect back, you have to configure the Mediation Engine by logging into Mediation Engine Connector.

Hint: To view the details of the Mediation Engine you are disconnecting, click System Settings and then double-click the entry, Name of this Mediation Engine.

Result: The Mediation Engine is disconnected from Mediation Engine Connector.

Note: Though, Mediation Engine disconnected from Mediation Engine Connector, Mediation Engine details appears in the mediation engine list. To remove the Mediation Engine from the list, navigate to **ME Management**, select the node, click **Delete Selected** and then click Save. If you click **Replicate Configuration**, the mediation engine will connect back to the Mediation engine connector. Make sure to note down all the fields of this entry before disconnecting for future reference.

Setting the Timeout for Call Searches in Mediation Engine Connector

In Mediation Engine Connector, the setting, **Timeout for call searches in seconds** controls the time a call search is performed in the nodes, using simple search, advanced search, or user tracking search

When searching for a call event in the Mediation Engine Connector, all mediation engine nodes are queried. If a Mediation Engine node identifies a call event, it queries the neighboring nodes to check for additional call legs.

Use the setting, **Timeout for call searches in seconds** to set the timeout for the full call search from the Mediation Engine Connector nodes to the Mediation Engine nodes.

To set the timeout for call searches:

1. In a web browser, log in to **Mediation Engine Connector**.
The Mediation Engine Connector screen appears.
2. From the *user* list, select **Settings**, where user is your login name.
3. Under **Mediation Engines**, select **Node Connection Settings**.
The Node Connection Settings screen appears.
4. In the **Timeout for call searches in seconds** field, enter the number of seconds after which the call search ends.
5. Click **Save**.

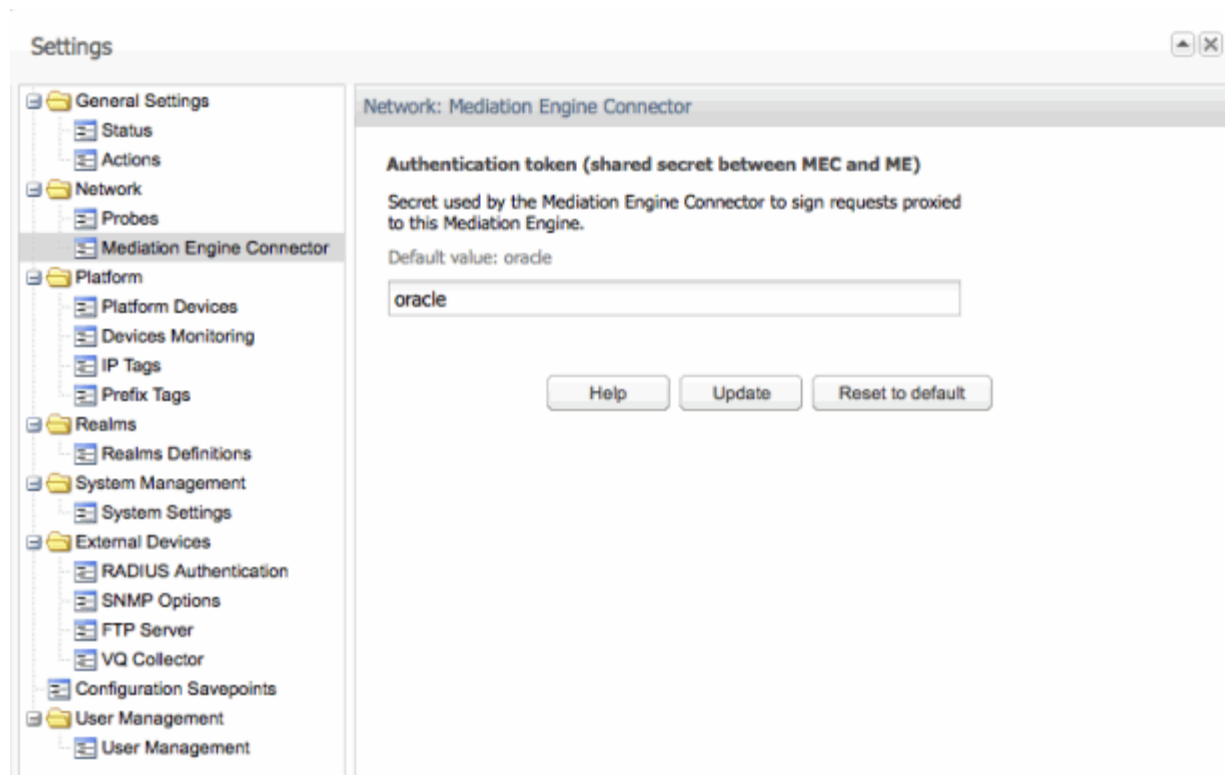
Table 2–1 Node Connection Settings Fields

Field	Description
Timeout for node connection in seconds	This timeout applies to <i>any</i> request sent from the Mediation Engine Connector to the Mediation Engine nodes.
Time range for call searches in seconds in simple search	When searching for a call in the Call Search panel, this is the amount of time (in seconds) traversed to search for queried call. The search displays only the calls not older than mentioned number of seconds. The default search limit for simple search is 900 seconds.
Time range for call searches in seconds in advanced search	When searching for a call, in the Advanced Search panel, this is the amount of time (in seconds) traversed to search for queried call. The search displays only the calls not older than mentioned number of seconds. The default search limit for advanced search is 86400 seconds.
Timeout for call searches in seconds	This timeout applies only to <i>call search</i> requests from the Mediation Engine Connector to the Mediation Engine nodes.
Use same timeout as for node connections	<p>If you select the checkbox, the setting, Timeout for call searches in seconds will have the same value as setting, Timeout for node connections in seconds.</p> <p>If the checkbox is not selected, then Timeout for call searches in seconds may have different value than Timeout for node connections in seconds.</p>

Adding Mediation Engines

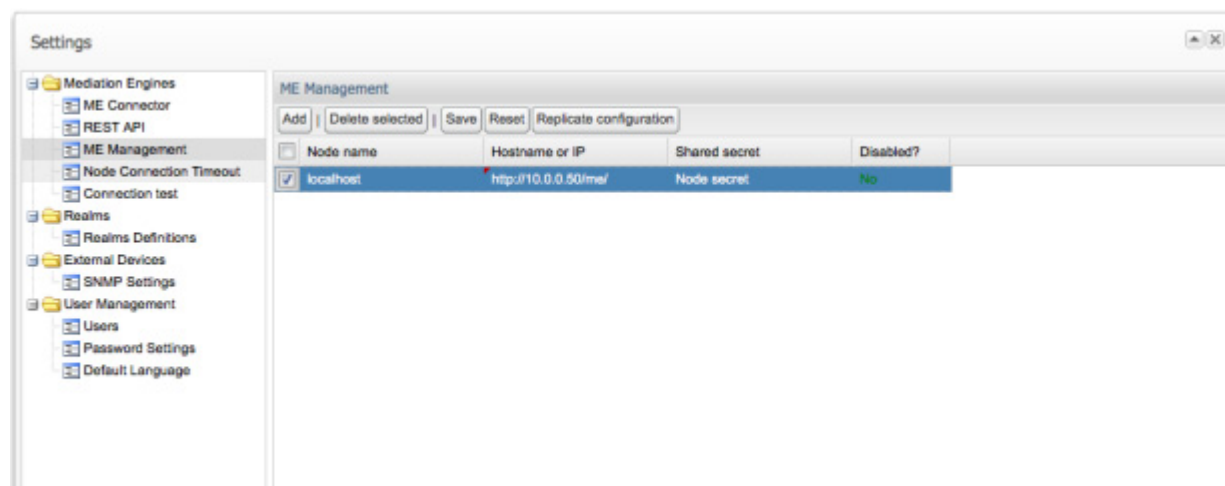
The last step in setting up Mediation Engine Connector is to add connections to the Mediation Engines. You must first prepare each Mediation Engine so that it is ready for connections from Mediation Engine Connector. To prepare probing for a connection from Mediation Engine Connector, go to the Settings page of the Mediation Engine, navigate to the Network: Mediation Engine Connector section, and set the secret key.

[Figure 2–3](#) shows an example of secret key setting.

Figure 2–3 Setting the Authentication Secret

You can now add the Mediation Engine to the Mediation Engine Connector configuration in the Mediation Engine Management section of the Settings page of Mediation Engine Connector.

Figure 2–4 shows an example of a Mediation Engine configuration.

Figure 2–4 Mediation Engine Management

Click **Add**, a new row appears at the top of the table. To edit a field, double click on it. Enter a name for the Mediation Engine. The name you enter forms part of the URL under which the Mediation Engine is reachable from the Mediation Engine Connector. You also must enter the Mediation Engine's base URL along with the Mediation Engine's secret. The former must be the HTTP URL under which the Mediation

Engine's user interface is reachable. The secret must match the one you entered while preparing the probe. Click **Save** when you are finished.

The Mediation Engine is added to Mediation Engine Connector and is available in the Mediation Engine selection in the header bar of the Mediation Engine Connector user interface.

When adding a new Mediation Engine, a warning is displayed when the connection is made, indicating that the following settings in Mediation Engine are going to be overridden by the settings in the Mediation Engine Connector:

- Custom header for realm definition
- Headers in which to look for realm URIs
- Use user domains
- Expire passwords periodically
- Enforce stringent password rules
- User default locale

Important: When adding a new mediation engine, the list of local users on the mediation engine might be lost. Any local users and realms in the mediation engine will be replaced with the current list of users and realms that exist in Mediation Engine Connector. If there are users and realms on the mediation engine that do not exist in Mediation Engine Connector, these will be lost.

Password Settings for User Account

You can define the password settings for users using Mediation Engine Connector settings.

To modify the password settings:

1. Login to Mediation Engine Connector as an admin.
2. Click **admin** and select **Settings**.

The Settings screen appears.

3. From the Settings menu, click **Password Settings**.
4. To enforce users to change their password regularly, set the time period by doing the following:
 - a. Select **Force users to change their password regularly**.
 - b. Enter the number of days in the **Period in days to force password change for users with access to sensitive data** field. The default setting is 90 days.
 - c. Enter the number of days in the **Period in days to force password change for users without access to sensitive data** field. The default setting is 180 days.
 - d. Click **Save** to save the changes or click **Cancel**.

Note: The entries in these fields are applied when the user changes the password next time.

5. Enforce stringent password rules by doing the following:

- a. Select **Enforce stringent password rules** to increase the level of security required in user passwords.

Note: A stringent password:

- Should not begin with a digit
 - Must contain at least one uppercase letter
 - Must contain at least one lower case letter
 - Must contain at least one digit
 - Must contain a special character such as @, #, \$, -, _
 - Must be different from the previous password
-

- b. By default, the account gets locked after three unsuccessful attempts for 15 minutes.
- c. Click **Save**.

Configuring Mediation Engines

This chapter describes how to set the location of Oracle Communications Mediation Engine Connector and mediation engine URLs and test the connections between each mediation engine and Mediation Engine Connector and between every two mediation engines.

Setting Mediation Engine Connector Configurations

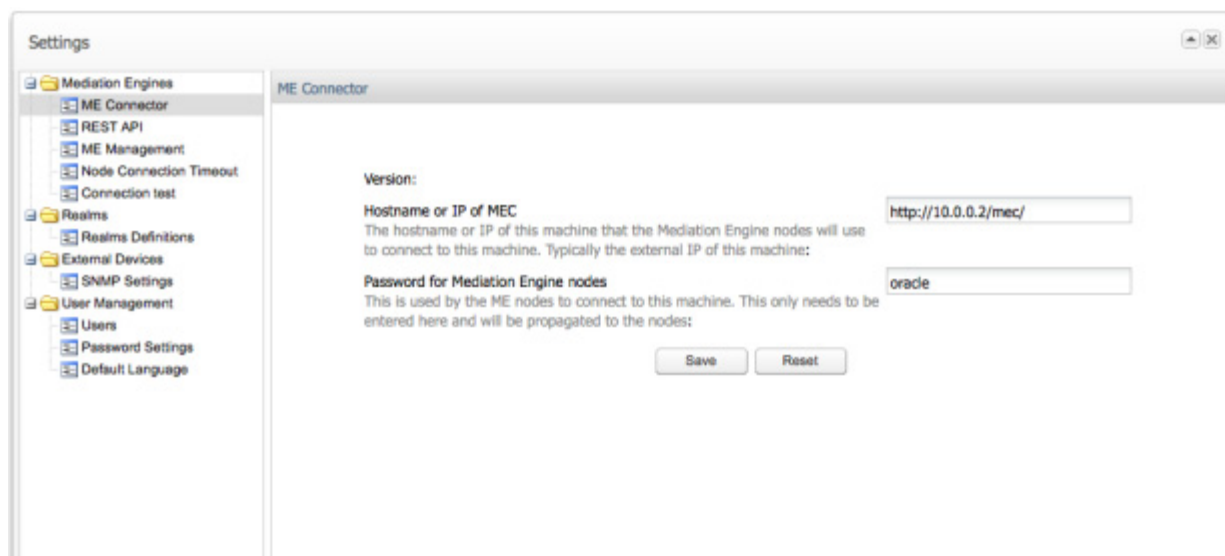
The URL of Mediation Engine Connector represents the location of the Mediation Engine Connector instance.

Mediation engines use the password for authenticating probes at Mediation Engine Connector. The default password is **oracle** and should be changed by the administrator. Its value should be identical with the password set in the mediation engines (**Proxy authentication secret** field of the System Settings panel).

Click **Save** to commit changes to these fields.

Figure 3–1 shows an example of Mediation Engine Connector configuration settings.

Figure 3–1 Mediation Engine Connector Configuration Settings



Note: When using multiple Mediation Engines with a Mediation Engine Connector, you can still login into the Mediation Engine directly without using the Mediation Engine Connector.

Setting Mediation Engine Configurations

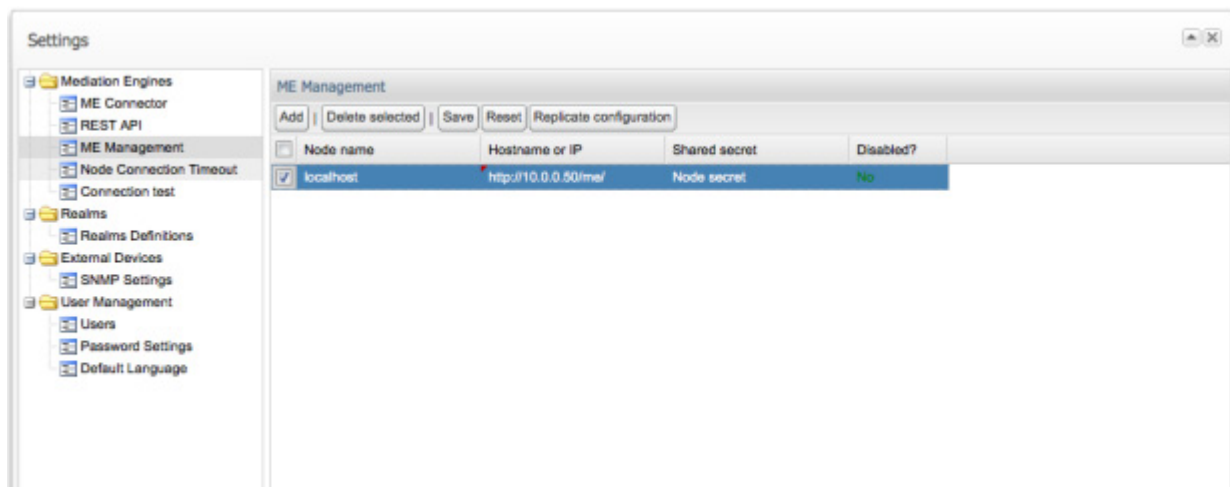
The mediation engines subordinated to Mediation Engine Connector can be configured from the **ME Management** section. To add a mediation engine, click **Add**. A new row appears at the top of the table.

To edit a field, double click on the table entry. Name, URL, and password should be given to each mediation engine. The name of the mediation engine is used by Mediation Engine Connector to form the URL under which the mediation engine is reached. The base URL field holds the address of the mediation engine's web user interface. The **Shared secret** is the password required by the mediation engine to authenticate itself while connecting to Mediation Engine Connector. The same password needs to be set in the connecting mediation engine from the **ME Management** page in the System Settings dialog box. To commit any changes done to the mediation engine's table, click **Save**.

To delete mediation engines from the table, select them and click **Delete selected** button. The **Disabled?** column is used to disconnect a mediation engine from Mediation Engine Connector. The configuration of Mediation Engine Connector (for example, users and realms) may be replicated to any mediation engine by clicking **Replicate configuration** button. Changes to the mediation engine configuration must be committed by clicking **Save**.

Figure 3–2 shows an example of mediation engine configuration.

Figure 3–2 Mediation Engine Management



Setting a Node Connection Timeout

Node connection timeout is the timeout value for connecting to nodes, for example when replicating settings to nodes. The value is given in seconds.

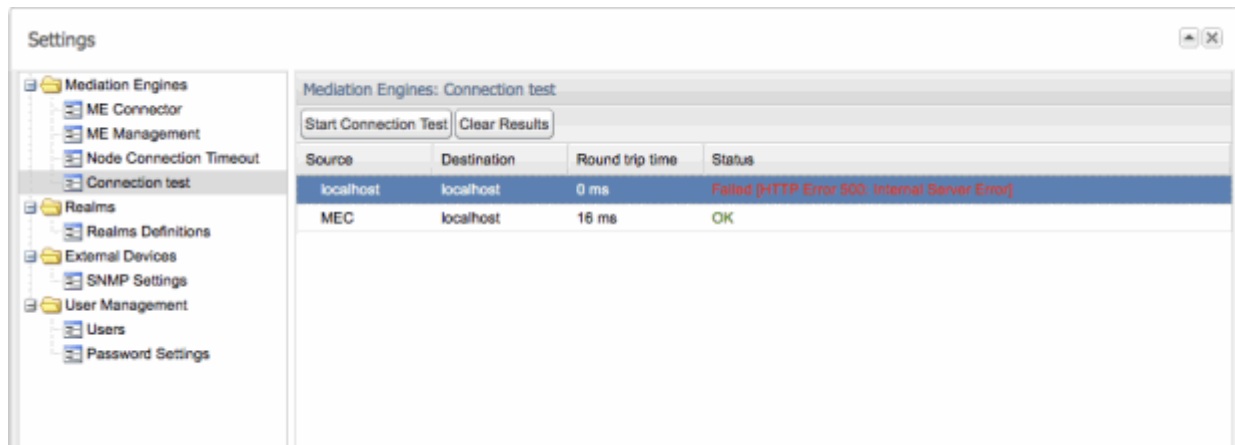
Testing Connections between Mediation Engines

After the mediation engines have been configured in the **ME Management** page, the link between any two mediation engines (including Mediation Engine Connector) may be tested by clicking **Start Connection Test** button. A ping is sent by each mediation engine and by Mediation Engine Connector to each other in order to determine the link quality presented by the **Round trip time** value.

The **Status** is displayed as **OK** in case the source and destination mediation engines are connected to each other, or **Failed** otherwise. The **Clear Results** button deletes the test results from the panel.

Figure 3–3 shows an example of mediation engine connection test results.

Figure 3–3 Connection Test



Understanding Mediation Engine Connection Testing Error Codes

The following table describes the error codes that appear in the connection testing of Mediation Engines:

Note: The connection errors are HTTP error codes defined in the <https://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html>.

The error codes could any on the 4XX or 5XX. The codes in the [Table 3–1](#) are only a subset of them.

Table 3–1 Mediation Engine Connection Testing Error Codes

Error Code	Brief Description	Error Description	Possible Required Actions
401	Unauthorized	A misconfiguration in the Node Secret or the Masterweb Secret.	Ensure that Secrets are correctly setup both in Mediation Engine Connector and Mediation Engine and that the same product versions are used for Mediation Engine and Mediation Engine Connector.
408	Timeout	A timeout occurs when trying to connect to the Mediation Engines.	Contact your System Administrator.
500	Internal Server Error	An unknown connection error occurs in the Node.	Contact your System Administrator.

Any other error code that appears is attributable to the local network connection error issues. Check the network connections and contact your System Administrator or Network Administrator for assistance.

Understanding Call Correlation

Message segments (call legs) of a call event can be distributed and stored on multiple mediation engines. Call correlation is the process of collecting all the distributed message segments of the call event from each mediation engine, merging them in the order of the call, and displaying the call event as a whole.

Mediation Engine Connector allows a user to monitor multiple mediation engines. Because each mediation engine contains its own list of call events, which may contain only call legs of the full call event, Mediation Engine Connector has to decide which of the call events from each mediation engine are from the same call. When passing a call event through a device monitored by multiple mediation engines, the Mediation Engine Controller locates any identical call events and consolidates the data. The consolidated call event data is displayed as one single call event flow in Mediation Engine Connector.

Note: If any error is encountered while connecting to any of the Mediation Engine, a warning is displayed besides the **Mediation Engine node selector** drop-down so that the users can check the connection nodes in the **Connection test** settings option.

Implementing Call Correlation

Mediation Engine Connector will correlate the call event when call events share a common call leg.

For each call leg that is a candidate for being the common call leg, the mediation engine runs a hash function over the INVITE message and stores it in the database together with a pointer to the call event of the call leg. A candidate call leg is a call leg where **one** of the two endpoints is a neighbor device. A neighbor device is a device configured on one of the other mediation engines, which is not marked as an **External** device.

When displaying the call event, each mediation engine is checked for an identical hash in their database. If true, the details of their call event are included in the display.

Note: In Operations Monitor, the **Mediation Engine Connector hash on P-Charging-Vector icid-value parameter** and the **Mediation Engine Connector hash search on all external legs** settings affect the generation of hashes.

For more information on the "Mediation Engine Connector hash on P-Charging-Vector icid-value parameter" and the "Mediation Engine Connector hash search on all external legs" settings, see "System Settings Summary" in *Operations Monitor User's Guide*.

For example:

You have a device configuration that contains multiple sites containing one mediation engine for each site. Each site also contains several devices and all of the call's event traffic involved in one of these devices is sent to the site's mediation engine.

To correlate a call event:

1. The call event leaves site **A** and directly enters site **B**, such as there is a call leg with one device on site **A** and one device on site **B**.
2. A device is configured as an **Internal** device on its site's mediation engine.
3. If there is direct traffic between a device on site **A** and a device on site **B**, the device on site **B** is configured as an **External** device on the mediation engine of site **A**. If there is direct traffic between a device on site **B** and a device on site **A**, the device on site **A** is configured as an **External** device on the mediation engine of site **B**.
4. Additional devices on a site can be configured as **External** devices on other sites mediation engines.

Note: This could have a small performance impact, but it ensures that the device name is available for display purposes on that mediation engine.

Configuration 1

The call event traverses five devices.

Devices DEV1 and DEV 2 are on site **A**, devices DEV 3, DEV 4, and DEV 5 are on site **B**. The following **Internal** assignments satisfy the requirement in point 2.

	DEV1 <--leg1-->	DEV2 <--leg2-->	DEV3 <--leg3-->	DEV4 <--leg4-->	DEV5
ME1	Internal	Internal			
ME2			Internal	Internal	Internal

Configuration 2

If there is traffic from DEV2 to DEV3, add **External** devices as follows:

	DEV1 <--leg1-->	DEV2 <--leg2-->	DEV3 <--leg3-->	DEV4 <--leg4-->	DEV5
ME1	Internal	Internal	External		
ME2		External	Internal	Internal	Internal

Because leg2 goes from DEV2 to DEV3 the above configuration satisfies the requirement in point 1 for this call event. This is a functioning configuration.

Configuration 3

This can be extended to the following, which satisfies point 4.

	DEV1 <--leg1-->	DEV2 <--leg2-->	DEV3 <--leg3-->	DEV4 <--leg4-->	DEV5
ME1	Internal	Internal	External	External	External
ME2	External	External	Internal	Internal	Internal

Configuring Multiple Mediation Engine Nodes for Call Correlation

To configure multiple mediation engine nodes for call correlation, do the following:

1. [Setting the Authentication of a Mediation Engine](#)
2. [Setting the Authentication of Mediation Engine Connector](#)
3. [Adding the Mediation Engines to the Mediation Engine Connector Node List](#)
4. [Testing the Connection](#)
5. [Setting the Platform Devices for Each Mediation Engine](#)
6. [Applying Configuration Changes](#)
7. [\(Optional\) Setting the Timeout for Call Searches](#)
8. [Viewing Correlation Calls](#)

Setting the Authentication of a Mediation Engine

Mediation engines communicate with Mediation Engine Connector using the fully qualified host name or IP address of Mediation Engine Connector and an authentication password, which is used by Mediation Engine Connector to verify the authentication of the mediation engines.

To set the authentication of a mediation engine:

1. In a web browser, log in to Mediation Engine Connector.
The Mediation Engine Connector window appears.
2. From the *user* list, select **Settings**, where *user* is your login name.
The Settings window appears.
3. Under **Mediation Engines**, select **ME Connector**.
The **ME Connector** page appears.
4. In the **Hostname or IP of MEC** text box, enter the host name of Mediation Engine Connector.
5. In the **Password for Mediation Engine nodes**, enter a secure password.
6. Click **Save**.

Setting the Authentication of Mediation Engine Connector

Before a connection is made between Mediation Engine Connector and a mediation engine, an authentication token (password) is used to verify the authentication of Mediation Engine Connector.

All mediation engines require their own individual authentication token. Apply the following steps to each mediation engine in your network.

To set the authentication of Mediation Engine Connector:

1. In a web browser, log in to Operations Monitor.

The Operations Monitor window appears.

2. From the *user* list, select **Settings**, where *user* is your login name.

The Settings window appears.

3. Under **System Management**, select **Systems Settings**.

The **System Settings** page appears.

4. Scroll down to the **Authentication token (shared secret between MEC and ME)** row.

5. Double-click the **Authentication token (shared secret between MEC and ME)** row.

The Update System Setting dialog box appears.

6. In the **Default value** text box, enter the mediation engine's authentication secret.

7. Click **Update**.

8. Under **Network**, select **Mediation Engine Connector**.

The **Mediation Engine Connector** page appears.

9. In the **Authentication token (shared secret between MEC and ME)** text box, enter the mediation engine's authentication secret.

10. Click **Update**.

11. Click **Close**, which closes the Settings window.

Adding the Mediation Engines to the Mediation Engine Connector Node List

Adding the mediation engines to the Mediation Engine Connector node list makes each mediation engine available as a node in the top menu bar of Mediation Engine Connector.

To add the mediation engines to the Mediation Engine Connector node list:

1. Verify that the Settings window is still open.

2. Under **Mediation Engines**, select **ME Management**.

The **ME Management** page appears.

3. In the **ME Management** toolbar, click **Add**.

4. In the **Node Name** column, enter a name for the mediation engine's node.

5. In the **Hostname or IP** column, enter the host name of the mediation engine.

6. In the **Share secret** column, enter the mediation engine's authentication secret.

7. Repeat step 3 to step 6 for all the mediation engines in your network.

8. In the **ME Management** toolbar, click **Replicate configuration**, which propagates the changes to all your mediation engines.

9. In the **ME Management** toolbar, click **Save**.

Testing the Connection

To test the connection:

1. Verify the Settings window is open.

2. Under **Mediation Engines**, select **Connection test**.

The **Connection test** page appears.

3. In the **Connection test** toolbar, click **Start Connection Test**.
4. Verify that the **Status** column displays **OK**, which confirms that the configuration is working and all the machines are reachable.
5. Click **Close**, which closes the Settings window.

Setting the Platform Devices for Each Mediation Engine

To set the platform devices for each mediation engine:

1. In a web browser, log in to Operations Monitor.
The Operations Monitor window appears.
2. From the *user* list, select **Settings**, where *user* is your login name.
The Settings window appears.
3. Under **Platform**, select **Platform Devices**.
The **Platform Devices** page appears.
4. Select the device you wish to set as an **External** device.
By default, devices are set as **Internal** devices.
5. In the **Platform Devices** toolbar, click **Toggle external**, which sets the device as an **External** device and makes it visible to other mediation engines on Mediation Engine Connector.
6. Click **Close**, which closes the Settings window.

Applying Configuration Changes

It is important to replicate the configuration after any change related to platform devices on any Mediation Engine node. When you have finished configuring your devices, apply the configuration changes.

To apply configuration changes:

1. In a web browser, log in to Mediation Engine Connector.
The Mediation Engine Connector window appears.
2. From the *user* list, select **Settings**, where *user* is your login name.
The Settings window appears.
3. Under **Mediation Engines**, select **ME Management**.
The **ME Management** page appears.
4. In the **ME Management** toolbar, click **Replicate configuration**, which propagates the changes to all your mediation engines.
5. In the **ME Management** toolbar, click **Save**.
6. Click **Close**, which closes the Settings window.

(Optional) Setting the Timeout for Call Searches

When searching for a call event in Mediation Engine Connector, all mediation engine nodes are queried. If a mediation engine node finds a call event, it queries the neighboring nodes to check for additional call legs. Use the **Timeout for Mediation**

Engine querying system setting to set the timeout for these queries on the mediation engine nodes.

To set the timeout for call searches:

1. In a web browser, log in to Operations Monitor.
The Operations Monitor window appears.
2. From the *user* list, select **Settings**, where *user* is your login name.
3. Under **System Management**, select **Systems Settings**.
The **System Settings** page appears.
4. Scroll down the **System Settings** page until you see the **Timeout for Mediation Engine querying** row.
5. Double-click the **Timeout for Mediation Engine querying** row.
The Update System Setting dialog box appears.
6. In the **Maximum value** text box, enter a number between 5 and 120.
7. Click **Update**.

Viewing Correlation Calls

A correlated call event is only viewable when a mediation engine is accessed from Mediation Engine Connector. If you access the mediation engine directly from a web browser and not from Mediation Engine Connector, only the call events content found in the mediation engine is displayed.

To view correlation calls:

1. In a web browser, log in to Mediation Engine Connector.
The Mediation Engine Connector window appears.
2. In the top menu bar, select a mediation engine from the **Select a node** list.
The Operations Monitor window appears.
3. From the Navigation pane under **Operations**, click **Calls**.
4. In the **Recent calls** table, right-click the row for which to display the correlated call event's message flow.
The **Message Flow for Call: *caller* and *callee*** window appears.
where *caller* is the number that initiated the call and *callee* is the call number that received the call.
5. When you have finished viewing the call event's message flow, press the **ESC** key, which closes the message flow window.

Glossary

AOR

Address Of Record.

B2BUA

Back-to-back User Agent. A logical entity that receives a request and processes it as a UAS. In order to determine how the request should be answered, it acts as a UAC and generates requests. See **RFC 3261** for details.

BSS

Business Support System.

Call leg

A call leg is the portion of the call between two SIP devices.

CDR

Call Detail Record.

Codec

COmpressor/DECompressor, algorithms for compressing and decompressing data.

CSV

Comma Separated Values. An exchange format for tabular data understood by Microsoft Excel, OpenOffice.org, and many other applications.

DHCP

Dynamic Host Configuration Protocol. Used for automatically assigning network addresses.

Diameter

Network protocol for data exchange, database access, accounting and policy control, successor of Radius.

DNS

Domain name service.

DoS

Denial of Service.

ENUM

Protocol based on DNS used within IMS for routing decisions.

E-Model

Computational model for use in transmission planning. Defined by the ITU in recommendation G.107.

Egress device

An egress device is the SIP device through which the call leaves the platform.

A more formal definition: An egress call leg is one which has as source a device from the platform, and the destination IP address is from outside the platform. A device is an egress device from a call if it is the source device of an egress call leg. If the call is terminated by a gateway device, this device is also considered an egress device.

Ethernet

Family of frame-based computer networking technologies for local area networks (LANs).

FTP

File Transfer Protocol.

HA

High Availability.

HTML

HyperText Markup Language.

HTTP cookie

Information unit from a web server for purposes of identification and customization. It is stored by the web browser and accessed by the server during subsequent visits.

H.248

Gateway control protocol.

H.323

VoIP protocol defined by ITU-T.

ICMP

Internet Control Message Protocol. Defined in **RFC 792**.

le-eff

Effective equipment impairment factor. See ITU recommendation G.107.

IMS

IP Multimedia Subsystem.

Ingress device

An ingress device is the SIP device through which the call enters the platform.

A more formal definition: An ingress call leg is one which has as destination a device from the platform, and the source IP address is from outside the platform. A device is an ingress device from a call if it is the destination device of an ingress call leg. If the call is created by a gateway device, this device is also considered an ingress device.

IP

Internet Protocol. Defined in **RFC 791**.

ISUP

ISDN user part.

ITU

International Telecommunication Union.

JavaScript

A scripting programming language most commonly used to add interactive features to web pages.

Jitter

A measure of the variability over time of the latency across a network. Term generally used in the VoIP environment describing the variation in delay between packets.

JSON

JavaScript Object Notation, a lightweight computer data interchange format.

LISP

Mature high-level programming language based on lambda calculus.

ME

Mediation Engine. The ME is the core of the Session Monitor product family running the real-time data processing and serves the frontend and interfaces.

Megaco

Gateway control protocol.

MEGACO ContextID

A Context is an association between a number of Terminations. The Context describes the topology (who hears/sees whom) and the media mixing and/or switching parameters if more than two Terminations are involved in the association.

MEGACO TerminationID

Termination IDs of physical Terminations are provisioned in the Media Gateway.

MEGACO Transaction

MEGACO Commands between the Media Gateway Controller and the Media Gateway are grouped into Transactions.

MGCP

Media Gateway Control Protocol.

MIB

Management Information Base.

MOS

The Mean Opinion Score (MOS) provides a numerical indication of the perceived quality of the received media. The MOS is expressed as single number in the range of 1 to 5. MOS is always measured by humans. Software products and devices like Session

Monitor Operations Monitor can only estimate it, the result being MOS-LQE (listening quality estimate).

The estimation is done based on a set of static parameters and taking into account a set of factors related to the flow of the voice packets throughout the network. The content of the packets is not deeply inspected. This can have an impact in such cases where a call is hopping over multiple media processors, resulting in multiple legs, some of which are not available to Session Monitor Operations Monitor (like foreign network segments, TDM etc). In these cases, only the maximum possible voice quality over the inspected segments is provided, rather than an absolute estimate, end-to-end.

In other words, if one of the media legs not accessible to Session Monitor Operations Monitor will degrade the quality, a processor downstream will decode the signal and re-package it to good parameters, but without enhancing it back, Session Monitor Operations Monitor might rate the call higher than the human listener will actually perceive it.

MOS	Quality	Impairment
5	Excellent	Imperceptible
4	Good	Perceptible but not annoying
3	Fair	Slightly annoying
2	Poor	Annoying
1	Bad	Very annoying

NIC

Network Interface Card.

NTP

Network Time Protocol.

OID

Object IDentifiers.

OSI

Open Systems Interconnection. A joint ISO and ITU-T standard for computer networks and communication protocols.

OSS

Operations Support System.

PCAP

Packet Capture file format. Used by many network analyzers including the open source tool Wireshark. The stored messages contain TCP/UDP headers, IP header and Layer 2 headers, plus the timestamp at which the message was received.

PDF

Portable Document Format. PDF is used for representing two-dimensional documents in a manner independent of the application software, hardware, and operating system.

Probe

A probe is software that collects raw signaling data and media traffic. You can configure probes to run locally within the Mediation Engine (embedded probe), or

integrated with Oracle Communications Session Border Controller (embedded probe), or run on dedicated machines (standalone probe).

Proxy

An intermediary entity that acts as both a server and a client for the purpose of making requests on behalf of other clients. A proxy server primarily plays the role of routing. See **RFC 3261** for details.

PSTN

Public Switched Telephone Network.

R-Factor

Voice quality score on a scale from 0 (worst) to 100 (best).

RADIUS

Remote Authentication Dial-In User Service is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service.

REST

Representational State Transfer. A convention for web services.

RSPAN

Remote SPAN.

RTP

Real-time Transport Protocol. Used for transporting media. Defined in **RFC 3550**.

RTCP

Real-time Transport Control Protocol. Used for reporting end point media quality information.

RTT

Round-Trip Time. The time elapsed for a message to a remote target and back again.

SBC

Session Border Controller. Used in some VoIP networks to offer decoupling, interoperability, and to hide the internal topology. They are typically involved in the signalling and often also relay the media streams. From the SIP point of view, they are usual B2BUAs.

SCTP

Stream Control Transmission Protocol. Is a Transport Layer protocol ensuring reliable, insequence transport of messages with congestion control.

SDP

Session Description Protocol. Defined in **RFC 4566**.

SIGTRAN

Suite of protocols to enable the use of SS7 over IP networks.

SIP

Session Initiation Protocol. Defined in **RFC 3261**.

SNMP

Simple Network Management Protocol.

SPAN

Switched Port Analyzer.

SPIT

SPAM over Internet Telephony.

SS7

Signaling System 7.

TCP

Transmission Control Protocol.

UAC

User Agent Client. The SIP element that creates a new request; usually the caller's SIP device in case of calls, or the user's SIP device in case of registrations. For details, see **RFC 3261**, Section 6.

UAS

User Agent Server. The SIP element answering the request; usually the callee's SIP device, or a SIP server. For details, see **RFC 3261**, Section 6.

UDP

User Datagram Protocol.

URI

Uniform Resource Identifier.

VLAN

Virtual Local Area Network.

VRRP

Virtual Router Redundancy Protocol. A redundancy protocol described in **RFC 3768**.

XML

The eXtensible Markup Language is a flexible text format for creating structured computer documents.