

Oracle® Communications Session Element Manager

User Guide for the EnterpriseExt Plug-in
Release 1.0

August 2017

Notices

Copyright© 2017, 2017, 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

About This Guide	5
Revision History.....	7
1 Overview	9
Session Element Manager Parts.....	9
Oracle Communications Session Element Manager Prerequisites.....	10
Information for Oracle Enterprise Operations Monitor Users.....	10
Information for Oracle Interactive Session Recorder Users.....	11
2 Device Manager	13
Configure Device Groups.....	13
Using the Default Home Device Group.....	13
Add a Device Group.....	14
Move a Device Group to Another Device Group.....	14
Rename a Device Group.....	14
Delete a Device Group.....	14
Manage Network Functions and Devices.....	15
Add a Network Function with Devices.....	15
Manage Network Functions.....	16
View Network Function Information.....	18
Export Device Information from Device Manager.....	20
Export Detailed Device Information from Device Manager.....	20

About This Guide

The Oracle® *Communications Session Element Manager User Guide for the EnterpriseExt Plug-in* provides the concepts and procedures that you need to know for managing the modular framework of Oracle's network session delivery and control infrastructure elements.

Documentation Library

The following tables describe the documentation library for Session Element Manager products.

Table 1: Oracle Communications Session Delivery Plug-in Documentation Library

Document Name	Description
Session Element Manager User Guide	Provides information for managing and optimizing network infrastructure elements and functions with comprehensive tools and applications used to provision Fault, Configuration, Accounting, Performance, and Security (FCAPS) support for managed network functions and their associated devices in Oracle Communications Session Delivery Manager (SDM).

Table 2: Oracle Communications Session Delivery Manager Documentation Library

Document Name	Document Description
Administration Guide	Provides the following administration information: <ul style="list-style-type: none">• Implement SDM on your network as a standalone server or a High Availability (HA) server.• Log in to the SDM application, access GUI menus including Help, customize the SDM application, and change your password.• Access the product plug-in service through the GUI to manage product plug-in tasks, including how to upload and install product plug-ins.• Manage security, faults, and transport layer security certificates for east-west peer SDM server communication, and southbound communication with Network Function (NF) devices.• Configure northbound interface (destination) fault trap receivers and configure the heartbeat trap for northbound systems.• Monitor SDM server health to detect heartbeat messages and display the server status to prevent health problems, or view server disk utilization information and server directory statistics.• Maintain SDM server operations, which includes database backup and database

About This Guide

Document Name	Document Description
	<p>restoration and performing server cluster operations.</p> <ul style="list-style-type: none">• Use available SDM server scripts, the contents of fault trap notifications, and a list of northbound notification traps generated by the SDM server.
Installation Guide	<p>Provides the following installation information:</p> <ul style="list-style-type: none">• Perform pre-installation tasks, which include reviewing system requirements, adjusting Linux and firewall settings, completing SDM server settings, and configuring your NNCentral account for security reasons.• Perform the typical installation to set the minimal configuration required to run the SDM server.• Perform the custom installation to set more advanced configurations including the mail server, cluster management, Route Manager, Transport Layer Security (TLS), and Oracle database configuration.
Release Notes	<p>Provides information about the administration and software configuration of the SDM feature support new to this release.</p>
Security Guide	<p>Provides the following security information:</p> <ul style="list-style-type: none">• Guidelines for performing a secure installation of SDM on your server, which includes methods for securing the server, firewall settings, system support for encryption and Random Number Generators (RNG), using HTTPS, and password guidelines.• Security Manager features for configuring groups, users, operations, privileges, and managing access to the system.• A checklist for securely deploying SDM in your network and maintaining security updates.
REST API for Oracle Communications Session Delivery Manager, Release 8.0	<p>Provides information for the supported REST APIs and how to use the REST API interface. The REST API interface allows a northbound client application, such as a Network Service Orchestrator (NSO), to interact with SDM and supported product plug-ins.</p>

Revision History

The following table lists the date and changes for each release of the *Oracle® Communications Session Element Manager User Guide for EnterpriseExt Plug-ins*.

Date	Description
August 2017	Initial release

Overview

Oracle Communications Session Element Manager is used to manage and optimize network infrastructure elements and their functions with comprehensive tools and applications on Oracle Communications Session Delivery Manager to provision fault, configuration, accounting, performance, and security (FCAPS) support for managed devices.

Session Element Manager Parts



Data Variables

Data variables (DVs) are used in offline configurations to allow network administrators to target elements that require device-specific information. All data variables must have new values to push the configuration to a device. An offline configuration requires DVs that have different values for each device that the template is assigned to support. This allows the template to be finely adjusted to the specific needs of a device and continue to provide a common baseline configuration for many devices. The template editor allows you to apply data variables to any element attribute that the offline configuration supports. A derived value can be specified when the DV that you are configuring shares the same value as another DV (dependency).

Overview

Device

A device is the atomic object that cannot be sub-divided and represents the component that does the required work. The element manager supports a network function (NF), but also manages the devices the NF contains.

Device group

A device group can contain or group NFs and devices.

Element Manager

The Oracle Communications Session Element Manager (SEM) provides alarm, configuration, fault, loading and provisioning capabilities for devices, performance management for infrastructure elements, and security capabilities.

Geo-redundant group

A geo-redundant group has active and standby devices that are not co-located.

Network Element

A network element is a manageable logical entity uniting one or more physical devices.

Network Function

An NF can be composed of device groups and devices. An NF can be simple or complex. A simple NF can be a standalone device or a high-availability (HA) pair. A complex NF can consist of device groups that further define topological constructs and complex structures for device containment.

Oracle Communications Session Element Manager Prerequisites

The following prerequisites are required before you can access product plugin FCAPS functionality in the Session Delivery Manager GUI.

 **Note:** Unsupported features are hidden or disabled by the product plugin.

- You must install the Session Delivery Manager server before you can install your product plugin through the Session Delivery Manager GUI. See the *Oracle Communications Session Delivery Manager Installation Guide, Release 8.0* for Session Delivery Manager server installation instructions.
- You must upload and install the product plugin in the Session Delivery Manager GUI. See the *Session Delivery Manager Software Distribution Media* section in the *Oracle Communications Session Delivery Manager Release Notes, Release 8.0* for the file name of your product plugin, and the *Oracle Communications Session Delivery Manager Administration Guide* for product plugin upload and installation instructions.

Information for Oracle Enterprise Operations Monitor Users

The Oracle Communications Session Element Manager (SEM) supports using the Oracle Enterprise Operations Monitor (EOM) with the Device Manager, where you add and manage devices and device groups in SEM. SEM does not support the EOM in any of the other SEM managers.

You can launch the EOM login page from SEM and perform operations on the EOM.

SEM does not support applying work order administration to the EOM. The work order does provide the EOM as a selection.

SEM does not support the **Show Details** functionality for the EOM.

Note that the Managed Devices - Group View page in SEM displays the following additional controls for working with Enterprise Plug-ins.

- Add—Launch the SEM dialogs for adding Enterprise devices.
- View—View the selected Enterprise device.
- Launch—Launch the login page for the selected Enterprise device.

For information about using Device Manager, see *Device Manager*.

Information for Oracle Interactive Session Recorder Users

The Oracle Communications Session Element Manager (SEM) supports using the Oracle Interactive Session Recorder (ISR) with the Device Manager, where you add and manage devices and device groups in SEM. SEM does not support the ISR in any of the other SEM managers.

You can launch the ISR login page from SEM and perform operations on the ISR.

SEM does not support applying work order administration to the ISR. The work order does provide the ISR as a selection.

SEM does not support the **Show Details** functionality for the ISR.

Note that the Managed Devices - Group View page in SEM displays the following additional controls for working with Enterprise Plug-ins.

- Add—Launch the SEM dialogs for adding Enterprise devices.
- View—View the selected Enterprise device.
- Launch—Launch the login page for the selected Enterprise device.

For information about using Device Manager, see *Device Manager*.

Device Manager

The **Device Manager** slider is used to create a grouping hierarchy and add one or more network functions (NFs) to this grouping schema.

You can assign individual devices to a network function (NF) group, which can contain a standalone device or a high-availability (HA) pair that is managed by Oracle Communications Session Element Manager. Device groups can exist in a grouping hierarchy that can be set up to contain any number of levels according to the needs of your organization. For example, you can structure your hierarchy based on geography. User permissions can be managed based on operation and device group privileges. Summary and detailed information can be displayed for individual devices and device groups.

The **Device Manager** slider contains the following nodes and folder nodes:

- **Devices**—Add, manage, and remove managed devices.
- **Device Groups**—With the appropriate permissions, you can add, manage, rename, and remove groups.

Configure Device Groups

You can configure a device group topology.

One or more device groups can be nested to define the topology of the network, which can include naming conventions such as geographical references and location names. Once a device group is specified, user privileges must be assigned to the group appropriately. For example, if the user is only allowed to view the NF and its devices, then the privilege is set to **VIEW**. If the user is allowed to add or run commands on the NF and its devices, the privilege is set to **FULL**. See the *Security Manager* chapter in the *Oracle Communications Session Delivery Manager Administration Guide* and the *Configure a Network Function for Devices* section later in this chapter for more information respectively.

Using the Default Home Device Group

You can add your NFs to the default **Home** device group if no other groups need to be created. Use this group with the following conditions:

- You must be assigned full administrative privileges to view this device group.
- You cannot rename this device group.
- You cannot delete this device group.
- When adding a device, the **Home** device group displays in the **Add device group** dialog box only if you have not targeted a previous device group from the table.

Add a Device Group

Use the following naming conventions when you add a device group:

- It must start with an alphabetic character.
- It can contain a minimum of three characters and a maximum of 50 characters.
- It can contain the following characters: alphabetic, numeric, hyphens (-), and underscores (_).
- It can be a mix of upper-case and lower-case characters.
- It cannot contain symbols or spaces.
- It cannot be the same name as an existing group name within the same level in the hierarchy (sibling).

1. Expand the **Device Manager** slider and click **Device Groups**.
2. In the **Device Groups** pane, click **Add**.
3. In the **Add device group** dialog box, enter the name for the device group in the **Device group name** field and click **OK**.

The device group now appears in the **Device Groups** pane.

Move a Device Group to Another Device Group

When a device group is moved, all devices within that device group are moved.

 **Note:** A device group cannot be moved into one of its child groups.

1. Expand the **Device Manager** slider and click **Device Groups**.
2. In the **Device Groups** pane, click the device group you want to move and click **Admin > Move**.
3. In the **Move device group(s) to** dialog box, click the device group in which you want to move your device group and click **OK**.

Rename a Device Group

You can rename a device group if it does not belong to another device group at the same hierarchical level.

1. Expand the **Device Manager** slider and click **Device Groups**.
2. In the **Device groups** pane, select the device group you want to rename and click **Rename**.
3. In the **Rename device group** dialog box, enter the new name in the **Rename device group to** field and click **OK**.

The new name appears in the **Device Groups** pane.

Delete a Device Group

You can delete a device group (folder) from the **Device Groups** list with the appropriate permissions, and under the following conditions:

- Empty the device group folder and move all devices to another device group folder or delete the devices from the device group folder in order to delete the device group folder.
- You cannot delete a device group if it causes a duplicate device group in the tree hierarchy.

1. Expand the **Device Manager** slider and click **Device Groups**.
2. In the **Device Groups** pane, click the device group and click **Delete**.
3. In the **Delete device group** confirmation dialog box, click **Yes** to delete the device group.
4. In the success dialog box, click **OK**.

Manage Network Functions and Devices

Add a Network Function with Devices

When preparing to use Device Manager, you set up device groups and add Network Functions (NF) to the groups. After you successfully add a NF, the system can communicate with the associated device and you can launch the login page for the device by way of the Session Element Manager.

- Optional—If you do not want to use the default device group, named Home, add the device group that you want. See "Configure Device Groups for Network Function."
- Configure SNMP community on each device that you plan to add to the device to Device Manager. See the device documentation.

Use the following procedure to add a Network Function (NF) to a managed device group. You can add more NFs by repeating the procedure.

 **Note:** The table in the following procedure displays all possible configuration attributes, but the system displays only the set that corresponds to the selections that you make in this configuration.

1. Expand the **Device Manager** slider, and click **Devices**.
2. In the **Managed Devices - Group View** pane, select a device group, and click **Add**.
3. In the **Select Network Function Type** dialog, do the following:
 - a) Select a **Category** from the drop-down list.
 - b) Select a **Network Function** from the drop-down list.
4. Click **Continue**.
5. In the **Add Network Function: Device** dialog, do the following:

Name	Description
Network Function Name	Enter the NF name that you want to use for the device you are configuring.
Description	Enter the description of the NF.
Component type	Select a device from the drop-down list.
Redundancy type	Select High Availability or Standalone.
Primary IP address	Enter the IP address for this device.
Secondary IP address	Enter the IP address for the second device, when this device is part of an HA pair.
SNMP agent mode	Select the SNMP version number that the SNMP agent supports, and click Load . Valid versions: v1, v2 and v3. When you select v3, SEM displays the authentication configuration fields for SNMP version 3.  Note: After you add the SNMP version for an existing device, you cannot change the version unless you remove the device and add it again.
SNMPv3 user name	Enter the SNMPv3 user name.
SNMPv3 authentication protocol	Select the SNMPv3 authentication protocol from the drop-down list.
SNMPv3 authentication password	Enter the SNMPv3 authentication password.

Device Manager

Name	Description
SNMPv3 privacy protocol	Select the SNMP version 3 authentication protocol from the drop-down list.
SNMPv3 privacy password	Enter the SNMPv3 privacy password.
SNMP community name	Enter the SNMP community name for this device, which is the name of an active community where the device can send or receive SNMP performance and fault information.
SNMP port	Enter the SNMP port number.
User Name	Enter the device user name.
User Password	Enter the device password.
Web Protocol	Select HTTP or HTTPS from the drop-down list.
Web Port	Enter the web port.

6. Click **Apply**.

The system adds the NF to the specified managed device group and displays a green icon by the name of the device in the Managed Devices - Group View table upon successful addition.

Manage Network Functions

Once you have added one or more NFs with a group hierarchy, you can manage them as described in the following sections.

Launch a Managed Device Login Page

You can use Oracle Communications Session Element Manager as a single source from which to access and manage multiple products. When you select a device and click **Launch**, the system communicates to the device and displays the login page.

1. Expand the **Device Manager** slider, and click **Devices**.
2. On the **Managed Devices - Group View** page, select the device that you want to login to.
3. Click **Launch**.
The system displays the login page for the selected device.

Edit a Network Function with Devices

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, expand the appropriate group folder hierarchy, select the NF folder and click **Edit**.
3. In the **Edit device group** dialog box, change the appropriate parameters:

 **Note:** You cannot edit the NF name or its device(s) IP address(es).

 **Note:** The table in the following procedure displays all possible configuration attributes, but the system displays only the set that corresponds to the selections that you make in this configuration.

Name	Description
User Name field	The new device user name.
User Password field	The new device password.

Name	Description
SNMP community name field	<p> Note: This field applies only to SNMP version 1 and 2.</p> <p>Enter the SNMP community name for this device, which is the name of an active community where the device can send or receive SNMP performance and fault information.</p> <p> Note: The SNMP community must be configured on the device before adding the device to the Session Delivery Manager. Use the device CLI to configure the ip-addresses parameter found in the configure terminal > system > snmp-community element. For more information, See the device product documentation for more information.</p>
SNMP port field	The SNMP port number. The default SNMP port number is 161.
SNMP community name field	<p> Note: This field applies only to SNMP version 1 and 2.</p> <p>Enter the SNMP community name for this device, which is the name of an active community where the device can send or receive SNMP performance and fault information.</p> <p> Note: The SNMP community must be configured on the device before adding the device to the Session Delivery Manager. Use the device CLI to configure the ip-addresses parameter found in the configure terminal > system > snmp-community element. For more information, See the device product documentation for more information.</p>
SNMPv3 user name field	The SNMP version 3 user name.
SNMPv3 authentication protocol drop-down list	<p>Select the SNMP version 3 authentication protocol:</p> <ul style="list-style-type: none"> • SHA—Secure hash algorithm (SHA-1). • MD5—MD5 hash algorithm. • NONE
SNMPv3 authentication password field	The SNMP version 3 authentication password.
SNMPv3 privacy protocol drop-down list	<p>Select the SNMP version 3 privacy protocol:</p> <ul style="list-style-type: none"> • DES—Data encryption standard algorithm (DES) for the encryption of electronic data. • AES128—Advanced encryption standard (AES) encryption algorithm. • NONE

Device Manager

Name	Description
SNMPv3 privacy password field	The SNMP version 3 privacy password.
Web protocols	Select the web protocol from the drop-down list.
Web port	Enter the web port.

4. Click **Apply**.
A success dialog box displays that the NF was changed.

Move a Network Function to Another Group

You cannot move the NF if it is locked unless you are the owner of the lock or an administrator overrides the lock. An error message appears in both situations. See [Override a Locked Network Function](#) section for more information about unlocking an NF.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** page, expand the appropriate group folder hierarchy, select the NF folder and click **Admin > Move**.
3. In the **Move Device** dialog box, click the device group folder to which you want to move the NF and click **OK**.
4. In the **Success** dialog box, click **OK**.
The NF moves to the new folder location that you specified.

Override a Locked Network Function

 **Note:** You must have the appropriate privileges assigned by your administrator to override a lock set on an NF by another user.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, click the NF folder icon you want to override lock and click **Admin**.
3. From the **Admin** pop-up menu, select **Override lock**.
4. In the **Confirm** dialog box, click **Yes**.
5. In the **Managed Devices** pane, click **Refresh**.
The padlock icon no longer appears next to the NF folder and IP address(es) of the device(s).

View Network Function Information

Use the following sections to view and manage Oracle session delivery product NF information, which includes its devices and the way detailed and summary NF information is displayed for its device node(s).

View Device States and Columns

You can monitor a variety of information for devices by viewing the state of their colored, round icons, and by using the column information presented for each device.

Expand the **Device Manager** slider and click **Devices**. The system displays a device group hierarchy showing the group, subgroup, and the network function (NF) that contains the devices, as shown in the following example.

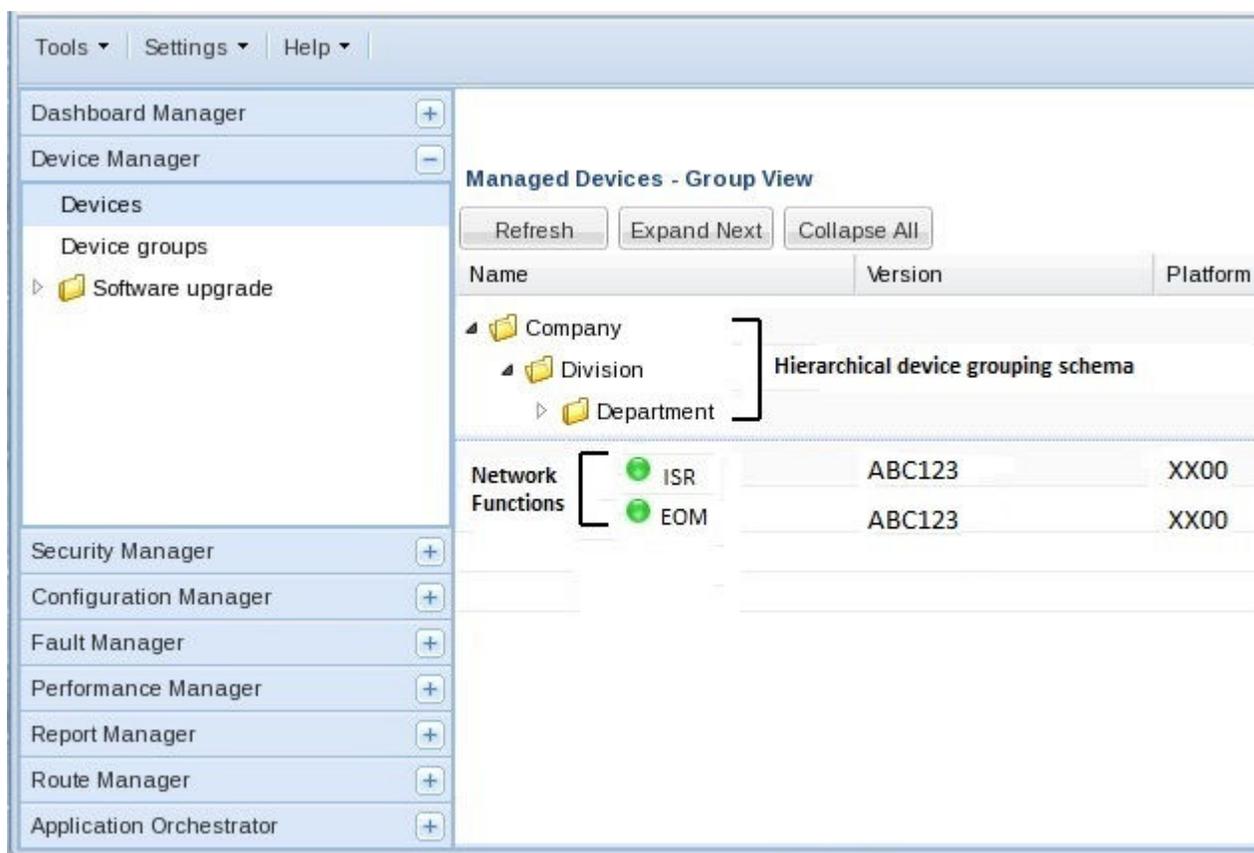


Figure 1: Device groups and their associated NF devices

The following states of a device in the **Managed Devices** table indicate if it can be reached by Oracle Communications Session Element Manager:

- Green—The Oracle Communications Session Element Manager can reach the device and retrieve information about the device through SNMP.

The following columns appear in the **Managed Devices** table:

Name	Description
Name	The group, subgroup, network function (NF) and device that belong to each NF. The grouping structure of the NF and its device is determined by the Session Delivery plug-in.
Version	The full software release version, including patch number of the NF HA device pair or standalone device.
Platform	The device hardware platform.
IP Address	The device IP address.
Serial Number	(Hidden) Serial number of the standalone device or the primary device in an HA deployment.
Group ID	(Hidden) The group element ID.
Object ID	(Hidden) Internal database object ID.

Device Manager

Manage How Groups for Network Functions are Displayed

Use the buttons at the top of the **Managed Devices** pane to affect the display of hierarchical groups, NFs and their associated devices.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, you can use the following buttons to manage how devices are displayed:

Name	Description
Refresh	Click to refresh the data displayed on the screen for hierarchical groups, NFs and their associated devices.
Collapse All	Click to collapse all folders.

View Serial Numbers for a Physical Device

Primary and secondary serial numbers of managed physical devices can be displayed by enabling hidden columns in the **Managed Devices** table.

 **Note:** Serial number information is pulled from a physical device through SNMP. Virtual devices return a value of N/A.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, click on the right side of a column header. The arrow icon appears with a drop-down menu.
3. Mouse over the **Columns** selection and click and the column options that you want to enable:
 - **Primary Serial Num**—Enables the Primary Serial Number column in the **Managed Devices** table.
 - **Secondary Serial Num**—Enables the Secondary Serial Number column in the **Managed Devices** table.

Export Device Information from Device Manager

You can export network function (NF) device information to your local system (PC, server, and so on) in the format of a comma-separated values (CSV) file which allows data to be saved in a table-structured format for auditing or management purposes.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, select the NF and click **Save to file**.
3. In the dialog box that appears, click **OK** to download the information in the form of a CSV file to your system.

 **Note:** The information in the CSV file that is saved to your system corresponds to the NF information displayed in the **Managed Devices** pane.

Export Detailed Device Information from Device Manager

You can also export detailed network function (NF) device information from the **Device details** pane in Device Manager to your local system.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, select the NF and click **Show details**.
3. In the **Device Details** pane, select only the tabs for which you want to save information and click **Save to File**.



Note: Only the tabs you select are saved. For example, if you select the **Hardware** tab and next the **Software** tab, the information for these tabs is saved only.

4. In the dialog box that appears, click **OK** to download the information in the form of a CSV file to your system.

