



Using Device Center

Device Center provides a one stop place where you can see a summary for a device, and launch troubleshooting tools, management tasks, and reports for the selected device. Since Device Center is based on a device-centric navigation paradigm, it helps you to concentrate on device centric features and information from a single location.

After launching Device Center, you can perform device-centric activities, such as changing device attributes, updating inventory, and perform telnet on a device selected from the Device Center Window.

You can also launch Element Management tools, reports, and management tasks.

Since all this information and reports for a single device are available from a single location, Device Center helps you in troubleshooting devices.

Device Center caters to a broad variety of device centric features from a single location. After launching Device Center, you can invoke many tools on the selected device from a single location.

The various features in Device Center come from the CiscoWorks applications installed on the server.

Device Center features and functions are available only from applications that reside on the same server on which Common Services is installed. You cannot launch tools, reports, and perform management tasks that pertain to applications installed on a different server.

The following sections of this chapter provide information on:

- [Launching Device Center](#)
- [Invoking Device Center](#)
- [Using Device Center Functions](#)

Launching Device Center

You can launch Device Center using any of the following options:

- From CiscoWorks Homepage.
Launch the Device Center main page from the CWHP and select a device.
To launch device center from CWHP select **CiscoWorks Homepage > Device Troubleshooting > Device Center**.
- Bookmark the Device Center URL and launch directly from the browser window.
- Launch Device Center for a device from one of the application functions such as reports.
For example, you can launch Device Center by clicking the Device name from RME Inventory Reports.
- From Third Party applications by passing the device context as a parameter.

Invoking Device Center

To invoke Device Center:

Step 1 Select **CiscoWorks Homepage > Device Troubleshooting > Device Center**.

The Device Center page appears with the Device Selector on the left pane and Device Center overview information on the right pane.

Step 2 Enter the IP address or device name of the device and click **Go**.

Or,

Select a device from the list-tree, in the Device Selector field,.

The Device Summary, and Functions Available panes appear.

Step 3 Click any of the links under the Functions Available pane to launch the corresponding application function.

The links are launched in a separate window.

If you enter the device name or IP address of a device not managed by any of the applications installed on the Common Services server, the Functions Available pane displays only the default connectivity tools from Common Services.

Using Device Center Functions

You can use the following Device Center modules to select devices, get a summary on the devices, get reports, debug, and perform management tasks.

- [Device Selector](#)
- [Device Summary](#)
- [Management Functions](#)

Device Selector

Device Selector displays the list of devices managed by applications installed on Common Services. Device Selector populates the devices for device selection in Device Center.

The devices shown in the Device Selector are those managed locally by applications that are installed in local server have some information that can be shown in Device Center.

Device Selector displays devices in groups. This is the entry point for the Device Center page. You can view and select devices using the device selector.

**Note**

After you select a device using Device Selector, you will get information on the applications that manage the device.

Device Selector allows you to:

- Change device selection to see related information for the selected device.
- Troubleshoot or manage the device selected.
- Select a device from the list-tree or by entering in the IP address or device name. Selecting a device displays Device summary and Functions Available panes.

Device Summary

The Device Summary content in the Device Center displays a summary of the device. You can see the IP Address, Device Type, OS version, and Last Reload Date in the Device Summary content area.

The summary page displays information grouped on the basis of application providing the information.

Management Functions

The Management Functions dialog box in the Device Center Functions Available page helps you to get the list of Debugging Tools, the list of Reports, and the list of Management Tasks on a selected device.

You can launch the management functions (Tools, Tasks, Reports) by:

- Selecting a device from device selector.
- Entering a device IP address or device name in the text box provided and clicking the button.
- Passing device context as parameters. Passing device context as parameter is meant for applications only.

Management Functions helps you perform these tasks:

- [Enabling Debugging Tools](#)
- [Displaying Reports](#)
- [Performing Management Tasks](#)

**Note**

You must have the required privileges to use some of the functions.

Enabling Debugging Tools

The Tools pane in the Device Center page displays the list of debugging tools that are used with the device. This module helps to debug device related problems.

Tools enable you to test device connectivity, and troubleshoot nonresponsive devices. They are available for all devices.

Checking Device Connectivity

To troubleshoot problems with un-managed or non-responding devices, you can check the device connectivity by protocol. The Management Station to Device tool helps you diagnose Layer 4 (application) connectivity problems.

Layer 4 tests include the key services Essentials needs to manage network devices: debugging and measurement tools (UDP and TCP), the web server (HTTP), file transfer (TFTP), the terminal (Telnet), and read-write access (SNMP).

If a hostname is entered instead of an IP address, the program always does a name lookup to find out the address. The test will fail if it cannot find an address.

You can test:

- UDP (echo test, port 7)
Sends an echo request to UDP port 7.
- TCP (echo test, port 7)
Sends an echo request to TCP port 7.
- HTTP (availability test, port 80)
Sends an HTTP request to the HTTP port 80 of the destination device.
- TFTP (availability test, port 69; device must be configured as a TFTP server)
Sends a TFTP request to the TFTP port (69) of the destination device.
- Telnet (service test, port 23)
Checks whether Telnet is enabled on the device and if the destination device responds to a Telnet request. It does not verify that the Telnet password in the database works.

Since Telnet runs on top of TCP, when Telnet succeeds, it means TCP is enabled on the device. If Telnet fails, there is no way to automatically determine if TCP is enabled or not. Perform a TCP test to check whether TCP is up or not.

- SNMP (service test, port 161)
Sends an **snmp get** request to the destination device for an SNMP read test (SNMPR). It also sends an **snmp set** request to the device to test SNMP write (SNMPW). This protocol is supported for the versions of v1, v2c, and, v3.
- SSH (service test, port 22)
Checks whether SSH is enabled on the device. If the destination device responds to SSH requests, this also tests whether CiscoWorks Server can make SSH requests to that device. It does not verify the password in the database.

If you launch Management Station To Device with Network Operator/Help Desk privilege, device credential fetching fails and the fields of read/write community strings of SNMP v1/v2c, read/write SNMPv3 credentials are set to default values. You have to manually enter SNMP v1/v2c/v3 credentials.

To invoke Management Station to Device tool:

-
- Step 1** Select **Device Troubleshooting > Device Center**.
- Step 2** Enter the name or IP address, fully qualified domain name, or hostname of the device you want to check in the Device Selector field and click **GO**.
- Or
- Select the device from the list tree.
- The Summary and Functions Available panes appear.
- Step 3** From the Functions Available pane, click **Management Station to Device**.
- The Management Station to Device dialog box appears.
- Step 4** Select the connectivity applications you want to select
- All information you enter in the fields are case sensitive.
- If you select SNMP v1/v2c, enter the following:
- The Read Community string.
 - The Write Community string.
 - Time out in seconds.

If you select SNMP v3, enter the following.

- The Read User name.
- The Read Auth PassPhrase.
- The Read Auth Protocol. Select MD5 or SHA from the drop-down list.
- The Write Username.
- The Write Auth PassPhrase.
- The Write Auth Protocol. Select MD5 or SHA from the drop-down list.
- The Security Level (authNoPriv).
- Timeout (in seconds, the default is 2 seconds).

Step 5 Click **OK**.

The Interface Test Results popup appears with the results. The Interface Details results screen shows the interfaces tested and the test results for each option.

Using Ping

Use the Ping tool to test whether the device is reachable. A **ping** tests an ICMP echo message and its reply. Since **ping** is the simplest test for a device, use it first. You can view the packets transmitted, and received, percentage of packet loss, and round-trip time in milliseconds. If **ping** fails, try using traceroute.

Step 1 Select **Device Troubleshooting > Device Center**.

Step 2 Enter the name or IP address, fully qualified domain name, or hostname of the device you want to check in the Device Selector field and click **GO**.

Or,

Select the device from the list tree.

The Summary and Functions Available panes appear.

Step 3 From the Functions Available pane, click **Ping**.

The Ping window appears with the results of the ping.

Using Traceroute

Use the Traceroute tool to detect routing errors between the network management station and the target device.

Traceroute helps you understand why ping fails or why applications time out. It does this by diagnosing TCP/IP Layer 3 (transport) problems. You can view each hop (or gateway) on the route to your device and how long each took.

-
- Step 1** Select **Device Troubleshooting > Device Center**.
- Step 2** Enter the name or IP address, fully qualified domain name, or hostname of the device you want to check in the Device Selector field and click **GO**.
- Or
- Select the device from the list tree.
- The Summary and Functions Available panes appear.
- Step 3** From the Functions Available pane, click **Traceroute**.
- The results of the trace appear in the Traceroute window.
-

Using SNMP Walk

SNMP Walk allows you to trace the MIB tree of a device starting from a given OID for purposes of troubleshooting, or gathering information about a certain device.

You should have System Administrator privileges to use this feature.

-
- Step 1** Select **Device Troubleshooting > Device Center**.
- Step 2** Enter the name or IP address, fully qualified domain name, or hostname of the device you want to check in the Device Selector field and click **GO**.
- Or
- Select the device from the list tree.
- The Summary and Functions Available panes appear.

Step 3 From the Functions Available pane, click **SNMP Walk**.

The SNMP Walk dialog box appears.

Step 4 Enter the IP address or DNS name.

Step 5 For SNMP Version 1 and 2c (if it is a 64-bit counter, use SNMP v2):

- Enter the Read community string.
- Enter the starting OID (optional). If this field is left blank, the tool will start from 1.
- Enter the SNMP Timeout.
- Select the check box to get output OIDs numerically.

For SNMP Version 3:

- Provide the SNMPv3 Username and password
- Specify the SNMP v3 Auth Protocol. Select either the MD5 radio button or the SHA radio button.
- Enter the starting OID (optional). If this field is left blank, the tool will start from 1.
- Enter the SNMP Timeout. The default is 10 seconds.
- Select the check box to get output OIDs numerically.

The fields are case sensitive.

Step 6 Click **OK** to get the results.

The results will be based on the parameters you entered. When the walk is complete, you can save it as text. A full walk may take a long time.

If you launch SNMP Walk feature with Network Operator/Help Desk privilege, device credential fetching fails and the fields of read/write community strings of SNMP v1/v2c, read/write SNMPv3 credentials are set to default values.

You have to manually enter SNMP v1/v2c/v3 credentials.

Using SNMP Set

You can use this option to set an SNMP object or multiple objects on a device for controlling the device.

You should have System Administrator privileges to use this feature.

-
- Step 1** Select **Device Troubleshooting > Device Center**.
- Step 2** Enter the name or IP address, fully qualified domain name, or hostname of the device you want to check in the Device Selector field and click **GO**.
- Or
- Select the device from the list tree.
- The Summary and Functions Available panes appear.
- Step 3** From the Functions Available pane, click **SNMP Set**.
- The SNMP set dialog box appears.
- Step 4** Enter the IP address or the DNS name.
- Step 5** For SNMP Version 1 and 2c (if it is a 64-bit counter, use SNMP v2):
- Enter the ReadWrite community string.
 - Enter the object ID that you are trying to set along with the instance ID or number.
 - Select the Object Type from the drop-down list. The values vary with the SNMP version selected.
 - Enter a new value. This will depend on the Object Type you specify.
 - Enter the SNMP Timeout. The default is 10 seconds.
- For SNMP Version 3:
- Provide the SNMPv3 Username and password.
 - Specify the SNMP v3 Auth Protocol. Select either the MD5 radio button or the SHA radio button.
 - Enter the object ID that you are trying to set along with the instance ID or number.

- Select the Object Type from the drop-down list.
- Enter a new value. This will depend on the Object Type you specify
- Enter the SNMP Timeout. The default is 10 seconds.

Step 6 Click **Next** if you wish to add more SNMP objects on the device.

The SNMP Set dialog box appears.

Step 7 Fill in all required fields and click **Next**. Repeat this until you have added as many objects as you want.

Step 8 Click **OK** to get the results.

The results will be based on the parameters you entered. When you have completed setting the SNMP objects, you can save it as text and mail the output.

If you launch SNMP Set feature with Network Operator/Help Desk privilege, device credential fetching fails and the fields of read/write community strings of SNMP v1/v2c, read/write SNMPv3 credentials are set to default values.

You have to manually enter SNMP v1/v2c/v3 credentials.

Using Packet Capture

The Packet Capture tool can be used to capture live data from the CiscoWorks machine to aid in troubleshooting.

You should have System Administrator privileges to use this feature.



Note WinPcap must be installed to use this feature on Windows machines. The executable is available at: NMSROOT\objects\jet\bin\winpcap.exe

Step 1 Select **Device Troubleshooting > Device Center**

Step 2 Enter the name or IP address, fully qualified domain name, or hostname of the device you want to check in the Device Selector field and click **GO**.

Or

Select the device from the list tree.

The Summary and Functions Available panes appear.

Step 3 From the Functions Available pane, click **Packet Capture**.

The Packet Capture dialog box appears.

A list of archived capture files is displayed. If no capture files are archived, then this screen will indicate that there are no records.

Creating a New Packet Capture File

Step 1 Click **Create** in the Packet Capture dialog box.

The Packet Capture Inputs dialog that lets you configure packets to be captured appears.

If you click **OK** with the default values (without setting any of the parameters) the screen will try to capture for the next 60 seconds.

Then it terminates and displays the Packet Capture dialog box with the new packet capture file added to the list of the archived capture files.

Click on the new packet capture file link to get a sniffer output of packets received by the CiscoWorks Server.

Step 2 In the Packet Capture dialog box:

- Specify the interface.
- Specify the address.

This field accepts one or more addresses (separated by a single space) to match when capturing.

You may select Protocol and Port if you know the number of the port. all protocols not specified under Applications can be captured using this option.

Step 3 Select the protocols, TCP, UDP, or ICMP.

Then, if required, fill in the list of ports to capture for TCP and UDP. The Port(s) field accepts one or more TCP or UDP ports, separated by a single space. If you specify port but not the address, it provides an output for that port for all the active devices.

You can stop a capture cycle after:

- A certain period time.
- The filter has captured a certain amount of data.
- A certain number of packets have been captured.

By default, capture cycles stop after 60 seconds.

Step 4 Click **OK**.

The Packet Capture dialog box with the new packet capture file added to the list of the archived capture files is displayed after the capture is performed.

Step 5 Click on the new packet capture file link to get the result.

While the capture is being performed, if you click **OK**, Packet Capture status popup appears with the current status of the capture.

If you click **Stop Capture** in the popup, capture stops and packet capture information till then is added in the Packet Capture dialogue box, among the archive files.

The result can be opened in any sniffer application, like Ethereal. These files are in binary libpcap format with a .jet extension.

You can download these files directly through your web browser, then email them to the TAC for further analysis.

Editing Device Credentials

You can edit device information for the selected device, using this feature. You can select a device from the list-tree or enter the IP address or device name, and click **Go**.

The Edit Device Credential link launches the Edit Credentials dialog box (**Device and Credentials > Device Management**).

See [“Editing Device Credentials” section on page 4-13](#) for details.

You need to have System Administrator or Network Administrator privileges to use this feature.

If the IP address or the device name you enter is not present in Device and Credential Repository (DCR), the Edit Credential link will not be displayed.

Displaying Reports

The Report pane in the Device Center page displays the list of the reports that can be launched for a device.

The reports displayed in the Report pane depends on the applications installed on the server.

Performing Management Tasks

The Tasks pane in the Device Center page displays the list of management tasks that can be performed on the Device.

The management tasks displayed in the Management Task pane vary depending upon the applications installed on the server.

