# Troubleshooting

Cisco Prime Infrastructure provides the following for sophisticated monitoring and troubleshooting of end-user network access.

The following sections describe some typical troubleshooting tasks:

- Get Help from the Cisco Support Community and Technical Assistance Center (TAC), on page 1
- Troubleshoot User Problems, on page 2
- Monitor Applications and Their Performance, on page 5
- Troubleshoot Wireless Device Performance Problems, on page 6
- Root Cause and Impact Analysis of Physical and Virtual Data Center Components, on page 6

# Get Help from the Cisco Support Community and Technical Assistance Center (TAC)

- Open a Cisco Support Case, on page 1
- Join the Cisco Support Community, on page 2

## Open a Cisco Support Case

When you open a support case from the web GUI, Prime Infrastructure automatically populates the case form with information it can retrieve from a device. This includes technical details about the device, configuration changes on the device, and all device events that occurred in the last 24 hours. You can also attach your own files to the case.

### Before you begin

You can open a support case from the web GUI if:

- Your administrator has configured Prime Infrastructure to allow you to do so. See *Set Up Defaults for Cisco Support Requests* section in Cisco Prime Infrastructure Administrator Guide.
- The Prime Infrastructure server has a direct connection to the internet, or a connection by way of a proxy server.
- You have a Cisco.com username and password.

**Step 1** Choose one of the following:

- From **Monitor** > **Monitoring Tools** > **Alarms and Events**. Click a single alarm, then choose **Troubleshoot** > **Support Case**. If you do not see the **Troubleshoot** button, widen your browser window.
- From the Device 360 view. Hover your mouse over a device IP address, then click the information icon. Choose **Support Request** from the **Actions** drop-down menu.

**Step 2** Enter your Cisco.com username and password.

**Step 3** Click **Create**. Prime Infrastructure populates the form with data it retrieves from the device.

**Step 4** (Optional) Enter a Tracking Number that corresponds to your own organization's trouble ticket system.

**Step 5** Click **Next** and enter a description of the problem.

Prime Infrastructure populates the form with data it retrieves from the device and automatically generates the necessary supporting documents.

If desired, upload files from your local machine.

**Step 6** Click **Create Service Request**.

## Join the Cisco Support Community

You can access and participate in discussion forums in the online Cisco Support Community. You will need a Cisco.com username and password.

**Step 1** Choose one of the following:

- From **Monitor > Monitoring Tools > Alarms and Events**. Click a single alarm, then choose **Troubleshoot > Support Forum**. If you do not see the **Troubleshoot** button, widen your browser window.
- From the Device 360 view. Hover your mouse over a device IP address, then click the information icon. Choose **Support Community** from the **Actions** drop-down menu.

**Step 2** In the Cisco Support Community Forum page, enter your search parameters to find what you need.

# Troubleshoot User Problems

You can use the User 360° View to troubleshoot problems reported by users.

**Step 1** In the Search field on any page, enter the end user's name.

**Step 2** In the Search Results window, hover your mouse cursor over the end user's name in the User Name column, then click the User 360° view icon. See Get User Details from the User 360° View.

**Step 3** With the User 360° view displayed, identify where the problem is occurring using the information described in the following table.

| To Gather This Data | Click Here in User 360° View | Additional Information |
|---|---|---|
| Information about the device to which the user is attached, such as the endpoint, location, connections, and session information | Click a device icon at the top of the User 360° View. | Click available links to display additional information. For example, you can click the Authorization Profile link to launch ISE.<br>If the end user is not associated with the appropriate policy category, you can hand off the problem (for example, to an ISE admin or help tech) or perform actions outside Prime Infrastructure to investigate why the user was placed in the current policy category (Authorization Profile).<br>Check to see whether there are any indications of authentication errors (authentication failure could be due to various things, including an expired password). The visual indication of authentication errors allows you to see more data related to the authentication errors. At that point, you might need to hand off the problem (for example, to an ISE admin or help tech). |
| Alarms associated with the device to which the user is attached | Click a device icon at the top of the User 360° View, then click the **Alarms** tab. | Click the Troubleshoot Client icon 🔧to go to client troubleshooting. |

| To Gather This Data | Click Here in User 360° View | Additional Information |
|---|---|---|
| Applications running on the device to which the user is attached and Site Bandwidth Utilization | Click a device icon at the top of the User 360° View, then click the **Applications** tab. | Click an application to view the end-user data filtered for the user you specified.<br>To get more information about an application, choose **Dashboard** > **Performance** > **Application**.<br>To get more information about an application, including the bandwidth utilization of the application consumed by the end user (the bandwidth consumed for the conversation), choose **Dashboard** > **Performance** > **Application**.<br>**Note** This feature requires:<br>• Integration with an ISE server (to access endpoint information).<br>• For wired sessions, that AAA accounting information is being sent to ISE.<br>• That session information (netflow/NAM data, Assurance licenses) is available. |

| To Gather This Data | Click Here in User 360° View | Additional Information |
|---|---|---|
| Information about Site Network Devices | Click a device icon at the top of the User 360° View, then click the **Alarms** tab. | You can choose to view:<br>• Active alarms list for the site<br>• List of all site devices (with alarm indications)<br>• Topo map of site (with alarm indications)<br>If a problem with a site has been detected, an alarm icon will appear next to the site location. Click the icon to view all of the alarms associated with that site.<br>If a problem has been detected, it might not be appropriate to continue troubleshooting the problem; it is probably sufficient to note that fact and hand off the task to second tier support. If you want to continue detailed client troubleshooting, exit the User 360° View and launch the full client and user troubleshooting page (choose **Monitor** > **Monitoring Tools** > **Clients and Users**). |
| Information about network Attachment Devices | Click a device icon at the top of the User 360° View, then click the **Alarms** tab. | Click the Go to Client Details icon. |

# Monitor Applications and Their Performance

Use the following procedure to determine if there are any problem indications associated with any of the specific applications being run across the network by the end user.

**Before You Begin**

This feature requires:

- Integration with an ISE server (to access endpoint information).
- That session information (NetFlow/NAM data, Assurance licenses) is available.

**Step 1** To view the applications accessed by the end user and the response time for the applications for the user's devices, open the User 360° View for that user and click the **Applications** tab.

**Step 2** This tab displays the following information:

**a.** Endpoint

b. Mac address

c. Application

d. Last one hour volume (in MB)

To get more information about an application, choose **Dashboard** > **Performance** > **Application**.

# Troubleshoot Wireless Device Performance Problems

If an end user reports a problem with their wireless device, you can use the Site dashboard to help you determine the AP that is experiencing problems.

**Before You Begin**

This feature requires that session information (netflow/NAM data, Assurance licenses) is available.

**Step 1** Choose **Dashboard** > **Performance** > **Site** and view the site to which the client experiencing trouble belongs.

**Step 2** To see the AP that is experiencing trouble at this site, click the **Settings**icon, then click **Add** next to **Busiest Access Points**.

**Step 3** Scroll down to the Busiest Access Points dashlet. You can

a. Hover your mouse over a device to view device information. See Get Device Details from Device 360° View.

b. Click on an AP name to go to the AP dashboard from where you can use the AP filter option to view AP details such as Client Count, Channel Utilization, and, if you have an Assurance license, Top *N* Clients and Top *N* Applications.

- Utilization based on SNMP polling for the APs.
- Volume information based on Assurance NetFlow data, if you have an Assurance license. For example, you can see the traffic volume per AP.

# Root Cause and Impact Analysis of Physical and Virtual Data Center Components

The physical servers shows the list of UCS B-Series and C-series servers that are managed by Prime Infrastructure. It also shows the Host/Hypervisor running on these servers, only if the corresponding Vcenter is added.

The Cisco UCS Server Schematic shows the complete architecture of the UCS device. The Schematic tab shows a graph that can be expanded to show different elements of UCS device such as chassis and blades. You can view quick summary of the element by hovering your mouse over the operational status icon next to the chassis or blade. In addition, clicking on the operational status icon, which symbolizes each unique element (chassis or blade), would show the subsequent connection. You can view the connection to host and its VM if managed by Prime Infrastructure by clicking the operational status icon. The schematic view also shows the operational status of the data center components and the associated alarms using which you can trace the root cause of an application delivery failure to a UCS hardware problem of Cisco UCS device.

# Troubleshoot UCS Device Hardware Problems

Use the following procedure to trace the root cause of an application delivery failure to a UCS hardware problem of Cisco UCS B-series and C-series servers. You can identify whether the problem is in fabric interconnect port, chassis or blades.

To identify the issue in UCS chassis, blade server, fabric interconnect port:

**Step 1** Choose **Inventory** > **Device Management** > **Compute Devices**.

**Step 2** Choose Cisco UCS Servers in the Compute Devices pane.

**Step 3** Click the faulty UCS device in the **Cisco UCS Servers** pane to view the **Schematic** tab that shows the inter-connections of the UCS chassis and blades, and the up/down status of chassis and blade servers. Hover your mouse over the faulty chassis or blade server name to view the Quick Summary of the element.

If you want to view the detailed information about the faulty chassis or blade server, click **View 360**.

**Step 4** Click the **Chassis** tab and hover your mouse cursor over the faulty chassis name, then click the information icon to launch the chassis 360° view that shows up/down status of power supply unit and fan modules.

**Step 5** Click the **Servers** tab and hover your mouse cursor over the faulty blade server name, then click the information icon to launch the server 360° view.

The server 360° view provides detailed blade server information including the number of processors, memory capacity, up/down status of adapters, Network Interface Cards (NICs), and Host Bus Adapters (HBAs) and Service Profile.

**Step 6** Click the **Network** tab to view the entire network interface details of fabric interconnect such as port channel, Ethernet interface, vEthernet, and vFabric Channel.

**Step 7** Click the **IO Modules** tab to view the operational status of backplane ports and fabric ports.

**Step 8** Click the **Service Profile** tab to view the hardware faults that impacts the services.

**Step 9** In the **Service Profile** pane on the left, click the expand icon to view the service profiles.

**Step 10** Click the information icon corresponding to the service profile to view the alarm severity levels of that service profile.

**Step 11** Click the faulty service profile in the **Service Profile** pane on the left to view the **Service Profile** table that displays the Profile Name, Service Profile Template, Server, Overall Status, Associated status and Associated Alarms.

**Step 12** Click the information icon corresponding to the profile name in the **Service Profile** table to launch the Service Profile 360° view that shows the basic summary information of the service profile.

## Identify the bandwidth issue in fabric interconnect port

**Step 1** Choose **Inventory** > **Device Management** > **Network Devices**.

**Step 2** Click the faulty UCS device from the **All Devices** pane.

**Step 3** Click the expand icon corresponding to fabric interconnect switch.

**Step 4** Click **Fixed Modules**Fixed Modules to view the operational status of fabric interconnect ports.

**Step 5** Click **Interfaces** to view the operational status for fabric interconnect port and interfaces. This is same as the operational stays of fabric interconnect port and interfaces viewed from **Network** tab in Compute Devices page.

# Troubleshoot UCS Device Bandwidth Problems

You can view the details of a fabric interconnect port or a fabric interconnect port group using the Top-N Interface Utilization dashlet from the Overview and Performance dashboards. Use the following procedure to identify whether the overuse of bandwidth on the ports connecting the fabric interconnect to the UCS chassis is causing application performance issues such as slowness on Cisco UCS.

We recommend you to create a fabric interconnect port group and select the port group in the dashlet to view the bandwidth utilization details.

To identify the overuse of bandwidth on the fabric interconnect ports:

**Step 1** Choose **Dashboard** > **Performance** > **Interface** then choose the UCS device interface from the Interface drop-down list.

or

Choose **Dashboard** > **Overview** > **Network Interface**.

**Step 2** Click the **Settings** icon as shown in and choose **Add Dashlets**.

**Step 3** Choose **Top N Interface Utilization** dashlet and click **Add**.

**Step 4** Do the following if you have already created a fabric interconnect port group:

a) Click the **Dashlet Options** icon in the **Top N Interface Utilization** dashlet.

b) Select the fabric interconnect port group in the **Port Group** and click **Save And Close**.

The **Top N Interface Utilization** dashlet displays the list of interfaces with maximum utilization percentage. This dashlet also shows the average and maximum data transmission and reception details of the fabric interconnect ports.