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:

Getting Help from Cisco

Prime Infrastructure provides helpful tools for network operators to connect to Cisco experts to diagnose and resolve problems. You can open support cases and track your cases from Prime Infrastructure. If you need help troubleshooting any problems, Prime Infrastructure allows you to:

- Connect with the Cisco Support Community to view and participate in discussion forums. See Launching the Cisco Support Community.
- Open a support case with Cisco Technical Support. See Opening a Support Case.

Launching the Cisco Support Community

You can use Prime Infrastructure to access and participate in discussion forums in the online Cisco Support Community. This forum can help you find information for diagnosing and resolving problems.

You must enter your Cisco.com username and password to access and participate in the forums.

Text Part Number:

To launch the Cisco Support Community:

Step 1 Choose **Monitor > Monitoring Tools > Alarms & Events**, select an alarm, then choose **Troubleshoot > Support Forum**.

Step 2 In the Cisco Support Community Forum page, enter additional search parameters to refine the discussions that are displayed.

Opening a Support Case

You can use Prime Infrastructure to open a support request and to track your support cases. Prime Infrastructure helps you gather critical contextual information to be attached to the support case, reducing the time it takes to create a support case.

To open a support case or access the Cisco Support Community, you must:

- Have a direct Internet connection on the Prime Infrastructure server
- Enter your Cisco.com username and password

To open a support case:

Step 1 Chose **Monitor > Monitoring Tools > Alarms & Events**, then hover your mouse cursor over the IP address of the device on which the alarm occurred.

Step 2 From the device 360° view, Select **Support Request** from **Actions** drop-down menu.

Step 3 Enter your Cisco.com username and password.

Step 4 Click **Login**.

Step 5 Click **Create** in **Update or Create a Support Case** window.

Prime Infrastructure gathers information about the device and populates the fields for which it can retrieve information. You can enter a Tracking Number that corresponds to your own organization's trouble ticket system.

Step 6 Click **Next** and enter a description of the problem.

By default, Prime Infrastructure enters information that it can retrieve from the device. Prime Infrastructure automatically generates the necessary supporting documents such as the technical information for the device, configuration changes, and all device events over the last 24 hours. You can also upload files from your local machine.

Step 7 Click **Create Service Request**.

Checking an End User's Network Session Status

When an end user calls the help desk, typically with a complaint that might not be very specific ("I can't log in" or "The network is really slow"), you will want to get an overall view of the user's current network session status, identify which individual session is associated with the problem, and examine the details for that session.

For example, how is the user attached to the network? Does this person have more than one endpoint (where an endpoint could be, for example, a laptop, desktop, iPad, iPhone, or Android)?

Before You Begin

This feature requires:

- Integration with an ISE server (to access endpoint information).
- Integration with LDAP (to display information about the end user).

To check an end user's network session status:

Step 1 In the system search field (see Search Methods), enter the name of the user (or client) who is experiencing the issue. If there are multiple matches, select the correct username from the list of matches.

Step 2 Start the User 360° View.

The information that is available from this view typically includes current information about the end user and all of that user's current or recently ended network sessions.

Troubleshooting Authentication and Authorization

Using the User 360° View, you can identify possible problems with the end user's authentication and authorization for network access.

For example, there could be authentication problems (such as the user's password being rejected), or there could be authorization issues (such as the user being placed in a policy category such as "guest" or "quarantine" that might result in unexpected behavior).

Before You Begin

This feature requires integration with an ISE server.

To troubleshoot the network:

Step 1 Open the User 360° View for that user and check the value in "Authorization Profile". This is a mnemonic string that is customer-defined, so it might not contain clear information (for example, "standard_employee" or "standard_BYOD" or "Guest").

Step 2 If this field is a link, click it to display information about the user's authorization profile. Based on this information:

- If the end user is associated with the appropriate policy category, this procedure is complete.
- 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).

Step 3 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).

Troubleshooting Network Attachments

Use the following procedure to determine if there are problems with the end user attaching to the network, such as errors on the access port (wired) or radio association problems (wireless).

To troubleshoot network attachments:

Step 1 Open the User 360° View for that user and click the Go to Client Details icon.

Step 2 If a problem has been detected, it might not be appropriate to continue troubleshooting the problem; it is probably sufficient to note the problem and hand it off 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**).

Troubleshooting Network Attachment Devices

Use the following procedure to troubleshoot any active alarms or error conditions associated with the network attachment device and port for the end user that might be causing problems for the end user's network session:

Step 1 To view any existing active alarms or error conditions associated with the network attachment device and port for the end user (available for the controller, switch, access point, and site), open the User 360° View for that user and click the **Alarms** tab.

Step 2 To see if a problem has been detected, click the Go to Client Details icon.

Step 3 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**).

Troubleshooting Site Network Devices

Use the following procedure to determine if there are any existing active alarms or error conditions associated with any of the network devices that are part of the site for the end user that could be causing problems for the user's network session.

Step 1 To view any existing active alarms or error conditions associated with network devices that are part of the site for the end user, open the User 360° View for that user and click the **Alarms** tab.

Step 2 You can choose to view:

- Active alarms list for the site
- List of all site devices (with alarm indications)
- Topo map of site (with alarm indications)

Step 3 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.

Step 4 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**).

Troubleshooting the User Application and Site Bandwidth Utilization

If an end user is experiencing high bandwidth utilization for a site on the interface dashboard, use the following procedure to identify the applications consumed by the user and the bandwidth consumed by every application for a given endpoint owned by the user.

Before You Begin

This feature requires:

- Integration with an ISE server (to access endpoint information).
- For wired sessions, that AAA accounting information is being sent to ISE.
- 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 The Applications tab displays information about the applications accessed by the end user (see Troubleshooting). 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**.

Troubleshooting 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 that appears as shown in Figure 60-6.

Step 3 With the User 360° view displayed, identify where the problem is occurring using the information described in Table 22-1.

Table 22-1 Using the User 360° View to Diagnose User Problems

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. See Troubleshooting Authentication and Authorization
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.
Applications running on the device to which the user is attached	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. See Troubleshooting the User's Experience.

Troubleshooting the User's Experience

If an end user reports a problem with accessing the application, use the User 360° View to troubleshoot the user's experience.

Before You Begin

This feature requires 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 The Applications tab displays information about the applications accessed by the end user (see Troubleshooting User Problems). To get more information about an application, choose **Dashboard > Performance > Application**.

Troubleshooting Voice/Video Delivery to a Branch Office

To successfully diagnose and resolve problems with application service delivery, network operators must be able to link user experiences of network services with the underlying hardware devices, interfaces, and device configurations that deliver these services. This is especially challenging with RTP-based services like voice and video, where service quality, rather than gross problems like outages, impose special requirements.

Note To use this feature, your Prime Infrastructure implementation must include Assurance licenses.

Prime Infrastructure with the licensed Assurance features makes this kind of troubleshooting easy. The following workflow is based on a typical scenario: The user complains to the network operations desk about poor voice quality or choppy video replay at the user's branch office. The operator first confirms that the user is indeed having a problem with jitter and packet loss that will affect the user's RTP application performance. The user further confirms that other users at the same branch are also having the same problem. The operator next confirms that there is congestion on the WAN interface on the edge router that connects the local branch to the central voice/video server in the main office. Further investigation reveals that an unknown HTTP application is using a high percentage of the WAN interface bandwidth and causing the dropouts. The operator can then change the unknown application's DSCP classification to prevent it from stealing bandwidth.

Step 1 Choose **Dashboard > Performance > End User Experience**.

Step 2 Next to **Filters**, specify:

- The IP address of the **Client** machine of the user complaining about poor service.
- The **Time Frame** during which the problem occurred.
- The ID of the problem **Application**.

Click **Go** to filter the Detail Dashboard information using these parameters.

Step 3 View **Average Packet Loss** to see the Jitter and Packet Loss statistics for the client experiencing the problem.

Step 4 View the **User Site Summary** to confirm that other users at the same site are experiencing the same issue with the same application.

Step 5 In the **User Site Summary**, under Device Reachability, hover your mouse cursor over the branch's edge router. Prime Assurance displays a 360° View icon for the device under the Device IP column. Click the icon to display the 360° View.

Step 6 In the 360° View, click the **Alarms** tab, to see alarms on the WAN interfaces, or on the Interfaces tab, to see congested WAN interfaces and the top applications running on them.

Troubleshooting Unjoined Access Points

When a lightweight access point initially starts up, it attempts to discover and join a wireless LAN controller. After joining the wireless controller, the access point updates its software image if needed and receives all of the configuration details for the device and network. Until the access point

successfully joins a wireless controller, it cannot be managed by Prime Infrastructure, and it does not contain the proper configuration settings to allow client access. Prime Infrastructure provides you with a tool that diagnoses why an access point cannot join a controller, and lists corrective actions.

Note To use this feature, your Prime Infrastructure implementation must include Assurance licenses.

The Unjoined AP page displays a list of access points that have not joined any wireless controllers. All gathered information about the unjoined access point is included on the page. This information includes name, MAC address, IP address, controller name and IP address, switch and port that the access point is attached to, and any join failure reason, if known.

To troubleshoot unjoined access points:

Step 1 Choose **Monitor > Wireless Technologies > Unjoined Access Points**.

Step 2 In the Unjoined APs page, select an access point to diagnose, then click **Troubleshoot**.

Step 3 After the troubleshooting analysis runs, check the results in the Unjoined APs page.

If the access point has tried to join multiple wireless controllers but has been unsuccessful, the controllers are listed in the left pane.

Step 4 Select a controller and check the middle pane for:

- A statement of the problem
- A list of error messages
- Controller log information

Step 5 Check the right pane for recommendations for solving any problems, and perform any recommended actions.

Step 6 (Optional) To further diagnose the problem, run RTTS through the Unjoined AP page by clicking the RTTS icon located to the right of the table. Examine the debug messages that appear in the table to determine a cause for the access point being unable to join the controllers.

RTTS Debug commands for Troubleshooting Unjoined Access Points

Table 22-2 contains the list of RTTS debug commands for Legacy controllers and NGWC controllers.

Table 22-2 RTTS Debug commands for Legacy controllers and NGWC controllers

Controller	Commands
Legacy	• debug capwap info enable • debug dot1x all enable • debug mobility directory enable
NGWC	• debug capwap ap error • debug dot1x events • debug capwap ios detail

Troubleshooting Wireless 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

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

Troubleshooting UCS 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.

To 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** 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.

Viewing Bandwidth on Fabric Interconnect Ports

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.