Monitor Application Health

About Application Experience and Application Visibility

Assurance processes complex application data and presents the findings in Assurance health dashboards to provide insight into the performance of applications.

You can view the health data from a device perspective (**Device 360** window), from the user perspective (**Client 360** window), or from the application perspective (**Application 360** window).

Depending from where the data is collected, you can see some or all of the following:

- Application Name
- Throughput
- DSCP Markings
- Performance Metrics (Latency, Jitter, and Packet Loss)

Application Name and Throughput are collectively referred to as **Quantitative** metrics. Data for the Quantitative metrics comes from enabling **Application Visibility**.

DSCP Markings and Performance Metrics (Latency, Jitter, and Packet Loss) are collectively referred to as **Qualitative** metrics. Data for the Qualitative metrics comes from enabling **Application Experience**.

Application Visibility

Application Visibility data is collected from switches running IOS-XE, and from wireless controllers running AireOS.

For switches running IOS-XE, Application Visibility data is collected using a predefined NBAR template that is applied bidirectionally (ingress and egress) to the physical layer access switch ports.

For wireless controllers running AireOS, Application Visibility data is collected at the wireless controller, and then streaming telemetry is used to transport this data to Cisco DNA Center.

Application Experience

Application Experience data is collected from Cisco IOS-XE router platforms, specifically using the Cisco Performance Monitor (PerfMon) feature and the Cisco Application Response Time (ART) metrics.

Examples of router platforms include ASR 1000, ISR 4000, and CSR 1000v. For device compatibility with Cisco DNA Center, see Cisco DNA Center Supported Devices.

To view the Cisco Performance Monitor feature availability, use the Cisco Feature Navigator tool. Click **Research Features**, and then add **Easy Performance Monitor Phase II** in the filter field.

Optimized Application Performance Monitoring

Optimized Application Performance Monitoring (APM) is a feature on the device that reduces the overhead in collecting NetFlow data. APM is supported on Cisco IOS-XE routers, Cisco 9800 series wireless controllers, and the Cisco DNA Traffic Telemetry Appliance. For minimum software versions, see Supported Platforms, on page 2.

Supported Platforms

The following table lists the supported platforms, type of data collection, and software and license requirements.

Note For device compatibility with Cisco DNA Center, see Cisco DNA Center Supported Devices.

Cisco Platform Support for Application Experience and Application Visibility in Cisco DNA Center		
Platform	**Data Collection**	**Notes**
Cisco IOS-XE Routers	Application Experience data collection.	• Requires active NBAR2 license. • IOS XE 16.3 minimum software version. • For Optimized APM—IOS XE 17.3 minimum software version.

Cisco Platform Support for Application Experience and Application Visibility in Cisco DNA Center		
Platform	**Data Collection**	**Notes**
Catalyst 9000 Series Switches	Application Visibility data collection for 9200, 9300, 9400.	• Requires Cisco DNA Advantage license. • IOS XE 16.10.1 minimum software version.
Cisco AireOS Wireless Controllers	Application Visibility data collection.	• Requires Cisco DNA Advantage license. • Requires 8.8 MR2 software version—8.8.114.130 or later.
Cisco 9800 Series Wireless Controller	Application Visibility data collection for Flex/Fabric SSIDs. Application Experience data collection for central switching/local SSIDs.	• For Optimized APM—IOS XE 16.12.1 minimum software version.
Cisco DNA Traffic Telemetry Appliance	Application Experience data collection.	• Requires Cisco DNA Advantage license. • For Optimized APM—IOS XE 17.3 minimum software version.

Criteria for Enabling Application Telemetry on Devices

Cisco DNA Center automatically enables application telemetry on all applicable interfaces or WLANs that are selected based on the new automatic interfaces or WLAN selection algorithm.

Application telemetry is pushed to WLANs that are provisioned through Cisco DNA Center.

Note

- The conventional tagging-based algorithm is supported and has precedence over the newer automatic interfaces or WLAN selection algorithm.
- If you want to switch over from automatic selection algorithm to tagging-based algorithm, you must disable telemetry before provisioning the tagged SSIDs to the devices.

The following table provides the criteria for selecting interfaces and WLANs based on the conventional tagging-based algorithm (with **lan** keyword) and the new automatic selection algorithm for all the supported platforms:

Platform	Conventional Tagging-Based Algorithm	Automatic Selection Algorithm

Router	• Interface description has the **lan** keyword.[1][2]
	• Interface is a physical interface.
	• Interface has an IP address other than the management IP address.
		• Interface has an IP address other than the management IP address.
		• Interface is not any of the following:
		  • WAN
		  Note An interface is treated as a WAN-facing interface if it has a public IP address, and if there is a route rule with a public IP address that routes through the interface.
		  In this context, a public IP address is not in a private range (for example, not in 192.168.x.x, 172.16.y.y, 10.z.z.z), or is an IP address that is not in the system's IP pools.
		  Route rules can be dynamically learned. In this context, the **show ip route** command does not show a route to a public IP address that goes through this interface.
		  • Loopback.
		  • Management interface: GIGABITETHERNET0, GIGABITETHERNET0/0, MGMT0, FASTETHERNET0, or FASTETHERNET1.

Switch	• Interface description has the **lan** keyword.[1, 2]
	• Switch port is configured as an access port.
	• Switch port is configured with the **switch-mode access** command.
		• Interface is a physical interface.
		• Access port does not have neighbors.
		• Interface is not any of the following:
		  • Management interface: FASTETHERNET0, FASTETHERNET1, GIGABITETHERNET0/0, or MGMT0
		  • LOOPBACK0, Bluetooth, App Gigabit, WPAN, Cellular, or Async
		  • VSL interface.

Platform	Conventional Tagging-Based Algorithm	Automatic Selection Algorithm

Cisco AireOS Controller	• WLAN profile name is tagged with the **lan** keyword.[1, 2]	• Not a Guest SSID:
		  • WLAN is not configured as a guest type.
		  • Name of the SSID does not contain the **guest** keyword.
		• SSID is configured in Local mode.

Cisco Catalyst 9800 Series Wireless Controller with Optimized Application Performance Monitoring (APM) profile and IOS release 16.12.1 and later.	• WLAN profile name is tagged with the **lan** keyword.[1, 2]
	• WLAN is configured in Local mode.
		• Not a Guest SSID:
		  • WLAN is not configured as a guest type.
		  • Name of the SSID does not contain the **guest** keyword.
		• If the SSIDs are mixed, that is Local mode, Flex mode, and Fabric mode, the Cisco Application Visibility and Control (AVC) basic record is configured. If all the SSIDs are in Local mode, the Optimized APM record is configured.

	Note If you want to update the telemetry configuration, you must disable telemetry and then enable it after making the configuration changes.	
Cisco DNA Traffic Telemetry Appliance with Optimized APM profile and IOS release 17.3 and later.	• Interface description has the **lan** keyword.[1, 2] • Interface is a physical interface.	• Interface is a physical interface. • Interface is not a management interface: GIGABITETHERNET0, GIGABITETHERNET0/0, MGMT0, FASTETHERNET0, and FASTETHERNET1.

[1] The **lan** keyword is case insensitive and can be separated by a space, hyphen, or underscore.
[2] Resynchronize the network device to read the **lan** interface description.

Application Health Prerequisites

This topic provides the prerequisites relating to application health for routers, AireOS wireless controllers, and switches.

Application Experience Prerequisites on Routers

- Requires Cisco IOS XE software with an active NBAR2 license.
- Application flows within the Layer 3 network are not visible.
- Traffic associated with the management interface is not part of Application Experience.
- Ports cannot be enabled for ETA.

- Clocks must be synchronized between Cisco DNA Center and the device for Assurance to display Application Health data.
- The conventional tagging-based algorithm (with keyword **lan**) is supported, but the newer automatic interface or WLAN selection algorithm allows you to enable Application Telemetry on interfaces or WLANs without tagging them with the keyword **lan**. For information about the criteria that is used, see Criteria for Enabling Application Telemetry on Devices, on page 3.

Application Visibility Prerequisites on Switches

- Requires Cisco IOS XE software.
- Requires a Cisco DNA Advantage license.
- Implemented only on access ports that contain the command **switchport mode access**.
- Support for L2 logical interfaces is not available.
- Limited visibility if the switch port is connected to an AP and configured with **switchport mode access**.
- Ports cannot be enabled for ETA.
- Only IPv4 flows are monitored.
- Management interface Gig0/0 cannot be used as the source interface of a NetFlow export.
- Clocks must be synchronized between Cisco DNA Center and the device for Assurance to display Application Health data.
- The conventional tagging-based algorithm (with keyword **lan**) is supported, but the newer automatic interface or WLAN selection algorithm allows you to enable Application Telemetry on interfaces or WLANs without tagging them with the keyword **lan**. For information about the criteria that is used, see Criteria for Enabling Application Telemetry on Devices, on page 3.

Application Visibility Prerequisites on AireOS Wireless Controllers

- Requires a Cisco DNA Advantage license.
- Supported only on wireless controllers that have AireOS software and not on wireless controllers that have IOS XE software.
- NetFlow must be enabled on the Cisco AireOS wireless controllers.
- Clocks must be synchronized between Cisco DNA Center and the device for Assurance to display Application Health data.
- Flexible NetFlow (FNF) flow monitors are not implemented. Instead, Application Visibility data is collected using streaming telemetry by subscribing to the Client-app-stat-events channel.
- The SSID is configured in Local mode (not Flex or Fabric).
- The conventional tagging-based algorithm (with keyword **lan**) is supported, but the newer automatic interface or WLAN selection algorithm allows you to enable Application Telemetry on interfaces or WLANs without tagging them with the keyword **lan**. For information about the criteria that is used, see Criteria for Enabling Application Telemetry on Devices, on page 3.

Application Visibility Prerequisites on Cisco 9800 Series Wireless Controller

- Requires IOS XE software for Optimized APM. See Criteria for Enabling Application Telemetry on Devices, on page 3.
- Clocks must be synchronized between Cisco DNA Center and the device for Assurance to display Application Health data.

Application Experience Prerequisites on Cisco DNA Traffic Telemetry Appliance

- Requires a Cisco DNA Advantage license.
- Requires IOS XE software for Optimized APM. See Criteria for Enabling Application Telemetry on Devices, on page 3.
- Clocks must be synchronized between Cisco DNA Center and the device for Assurance to display Application Health data.
- To enable visibility of CAPWAP-encapsulated wireless traffic, manually enter the **ip nbar classification tunneled-traffic CAPWAP** command on the Cisco DNA Traffic Telemetry Appliance.

Provision Application Telemetry Settings

Configure global telemetry settings as described in Configure Syslog, SNMP Traps, NetFlow Collector Servers, and Wired Client Data Collection Using Telemetry.

Step 1 Click the menu icon (☰) and choose **Provision** > **Network Devices** > **Inventory**.

The Inventory page displays the device information gathered during the Discovery process. To view devices available in a particular site, expand the Global site in the left pane, and select the site, building, or floor.

Step 2 Choose the devices that you want to provision.

Step 3 From the **Actions** drop-down list, choose **Telemetry** and do one of the following:

Note The application telemetry option is enabled only if the device supports application telemetry enablement from Cisco DNA Center.

a) **Enable Application Telemetry**: To configure application telemetry for the selected devices.
b) **Disable Application Telemetry**: To remove the application telemetry configuration from the chosen devices.

Step 4 Click **Apply**.

The **Application Telemetry** column shows the telemetry configuration status. If you don't see the Application Telemetry column in the default column setting, click the **More** icon (⋮) at the right end of the column headings and check the **Application Telemetry** check box.

View Application Experience of a Host

Use this procedure to view the qualitative and quantitative metrics of the applications running on a host.

Before you begin

- Make sure that the devices (routers, switches, wireless controllers, and access points) are discovered. See Discover Your Network Using an IP Address Range, Discover Your Network Using CDP, or Discover Your Network Using LLDP.
- Enable and configure Application Telemetry profile on network devices. See Provision Application Telemetry Settings, on page 7.
- See Application Health Prerequisites, on page 5.

Step 1 From the **Client 360** window, expand the **Application Experience** category.

Step 2 From the **Application Experience** category, you can do the following:

a) View the Application Experience data in table format from a specific business relevance group by clicking its corresponding tab. The tabs are: **Business Relevant**, **Business Irrelevant**, or **Default**.

Note The displayed data is based on the time you selected from the drop-down menu in the **Client 360** window. Options are: **3 Hours**, **24 Hours**, and **7 Days**. Default is **24 Hours**.

b) View Application Experience data in the table.

- **Name**: The application name.
- **Health**: The health score is calculated on the basis of a combination of metrics of packet loss, latency, and jitter. You can also include application delay for health score calculation. For more information, see Individual Application Health Score, on page 19.
- **Usage Bytes**: The number of bytes transferred by the client for this application.
- **Average Throughput**: The rate of the application traffic (in Mbps) flowing between the client and the server.
- **DSCP**: The application's current (**Observed**) and default (**Expected**) DSCP value.

  Note This metric is not available for Optimized APM.

- **Packet Loss**: The percentage (maximum and average) of packet loss.
- **Network Latency**: The network latency time (maximum and average) in milliseconds.
- **Jitter**: The variance in time delay in milliseconds (maximum and average) between data packets over your network.

c) To view the Application Experience metrics in chart format, click the radio button next to an application. The metrics are: **Throughput**, **Packet Loss**, **Jitter**, **Network Latency**, **Client Network Latency**, **Server Network Latency**, and **Application Server Latency**.

Note Application Visibility data that is exported by a Cisco Catalyst 9200 switch, Cisco Catalyst 9300 switch, or a Cisco AireOS wireless controller only provides data for Application Name, Usage, and Throughput.

View Application Experience of a Network Device

Use this procedure to view the qualitative and quantitative metrics of the applications running on a network device.

Before you begin

- Make sure that the devices (routers, switches, wireless controllers, and access points) are discovered. See Discover Your Network Using an IP Address Range, Discover Your Network Using CDP, or Discover Your Network Using LLDP.
- Enable and configure Application Telemetry profile on network devices. See Provision Application Telemetry Settings, on page 7.
- See Application Health Prerequisites, on page 5.

Step 1 From the **Device 360** window, expand the **Application Experience** category.

Step 2 From the **Application Experience** category, you can do the following:

a) View the Application Experience data in table format from a specific business relevance group by clicking its corresponding tab: **Business Relevant**, **Business Irrelevant**, or **Default**.

Note The displayed data is based on the time you selected from the drop-down menu in the **Device 360** window. Options are **3 Hours**, **24 Hours** (the default), and **7 Days**.

b) Filter the Application Experience data for a specific VRF or a specific router interface by using the appropriate filters: **All VRFs** and **All Interfaces**.

Note The **All VRFs** and **All Interfaces** filters are only available for routers.

c) View Application Experience data in the table:

- **Name**: The application name.
- **Health**: The health score is calculated on the basis of a combination of metrics of packet loss, latency, and jitter. You can also include application delay for health score calculation.

  Note The health score is not available for Cisco Catalyst 9000 Series Switches and Cisco AireOS wireless controller. These devices do *not* poll the KPIs that are required to calculate a health score.

- **Usage Bytes**: The number of bytes transferred by the client for this application.
- **Average Throughput**: The rate of the application traffic (in Mbps) flowing between the client and the server.
- **DSCP**: The application's current (**Observed**) and default (**Expected**) DSCP value.

  Note This metric is not available for Optimized APM.

- **Packet Loss**: The percentage (maximum and average) of packet loss.
- **Network Latency**: The network latency time (maximum and average) in milliseconds.
- **Jitter**: The variance in time delay in milliseconds (maximum and average) between data packets over your network.

d) To view the Application Experience metrics in chart format, click the radio button next to an application. The metrics are **Throughput**, **Packet Loss**, **Jitter**, **Network Latency**, **Client Network Latency**, **Server Network Latency**, **Application Server Latency**, and **Application Response Time**.

Note Application Visibility data that is exported by a Cisco Catalyst 9200 switch, Cisco Catalyst 9300 switch, or a Cisco AireOS wireless controller only provides data for Application Name, Usage, and Throughput.

Monitor the Health of All Applications

Use this procedure to get a global view of applications at a site.

Before you begin

- Make sure that the devices (routers, switches, wireless controllers, and access points) are discovered. See Discover Your Network Using an IP Address Range, Discover Your Network Using CDP, or Discover Your Network Using LLDP.
- Enable and configure Application Telemetry profile on network devices. See Provision Application Telemetry Settings, on page 7.
- See Application Health Prerequisites, on page 5.

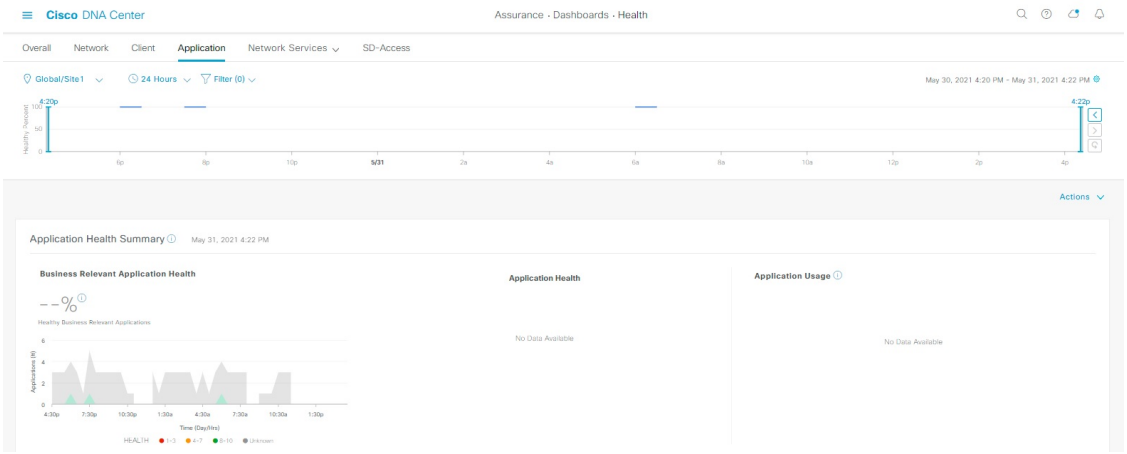
Step 1 Click the menu icon (☰) and choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

Step 2 Click the **Application** tab.

The **Application** health dashboard appears.

Figure 1: Application Health Dashboard



Step 3 Use the **Application** health dashboard top-menu bar for the following functionality:

Application Health Dashboard Top-Menu Bar	
Item	**Description**
Global **Location** drop-down list	Click to display the location icon. Click the location icon to display the **Site List View**. To view the application information from a specific site or building, click **Apply** in the appropriate row. The information is refreshed in the dashboard based on your selection.
Time Range setting	Enables you to display data within a specified time range on the dashboard. Do the following: **a.** From the drop-down menu, choose the length of the range: **3 Hours**, **24 Hours**, or **7 Days**. **b.** Specify the **Start Date** and time; and the **End Date** and time. **c.** Click **Apply**.
Filter	Choose the SSID from the drop-down list and then click **Apply**. Depending on your selection, the information in the dashboard is refreshed.
Actions drop-down list	Enables you to customize the dashboard display when you choose **Edit Dashboards** from the drop-down list. See Change the Position of a Dashlet and Create a Custom Dashboard.
Application Health Timeline Slider	Enables you to view the healthy business relevant application percentage for a more granular time range. Hover your cursor within the timeline to view the health score percentage at a specific time. You can click and drag the timeline boundary lines to specify the time range. This sets the context for application data that is displayed in the dashboard dashlets. You can use the arrow buttons on the right of the timeline to view data for up to 30 days.

Step 4 Use the **Application Health Summary** dashlet for the following functionality:

Application Health Summary Dashlet	
Item	**Description**
Business Relevant Application Health	Contains a health score for business relevant applications. The health score is the percentage of healthy (good) business relevant applications in your overall network, or selected site. See Understand Application Health Score and KPI Metrics, on page 18. The following charts are displayed: • Application count distribution trend chart that shows the count of all business relevant applications over time, which is shown as a stacked area chart based on their health scores. • Circle chart that shows the count of business relevant applications categorized by the application's health score. You can click a category to show the list of applications with the lowest health score within the category.
Application Usage	• Circle chart: Shows the total application usage categorized by the application's business-relevance group. You can click a category to show the list of the top 10 applications by usage within the category. **Note** The application usage is the taken from the application's bidirectional traffic. • **View Details**: Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can: • Click the **All Applications**, **Business Relevant**, **Business Irrelevant**, and **Default** tabs to display a chart with its application usage and the top 10 applications by usage. • Filter the chart by application group or traffic class with the drop-down list at the top right of the slide-in pane. • Click a category in the chart to display the applications and its detailed information in the **Application** table.

Step 5 Use the **Application** dashlet for the following functionality:

Application Dashlet	
Item	**Description**
Type	Filter the table based on the business-relevance groups: Options are **Business Relevant**, **Business Irrelevant**, and **Default**.

Application Dashlet	
Item	**Description**
Health	Filter the table based on the application's health scores. Options are: • **Poor**: Applications with a health score range from 1 to 3. • **Fair**: Applications with a health score range from 4 to 7. • **Good**: Applications with a health score range from 8 to 10. • **All**: All applications. • **Unknown**: Applications missing qualitative metrics for determining a health score.
Application table	View detailed application information in a table format. The application table displays the following information by default: • **Name**: Displays the application name. The names are based on the standard applications from Cisco Next Generation Network-Based Application Recognition (NBAR). **Note** Changing an application's name with the Application Policy package does not show the changed name in Application Experience. Currently there is no integration between the Application Policy package and Application Experience. **Note** If an application is not a standard application from the NBAR, its HTTP host name or SSL common name is displayed, if available. These applications are assigned to the **Default** business-relevance group. You can click the name to display a 360° view of an application. See Monitor the Health of an Application, on page 14. • **Health**: Displays the health score of the application. • **Business Relevance**: Possible values are **Business Relevant**, **Business Irrelevant**, and **Default**. • **Usage Bytes**: The number of bytes transferred for this application. • **Average Throughput**: The rate of application traffic (in Mbps) flowing between the client and server. • **Packet Loss (%)**: The percentage of packet loss. • **Network Latency**: The network latency time in milliseconds. For Transmission Control Protocol (TCP) based applications. • **Jitter**: The variance in time delay in milliseconds between data packets over your network. For Real-time Transport Protocol (RTP) based applications.

Application Dashlet	
Item	**Description**
⋮	Customize the data you want displayed in the table: **a.** Click ⋮ . A list of options appears. **b.** Check the check boxes for the data you want displayed in the table. **c.** Click **Apply**.
Export	Click **Export** to export the table data to a CSV file. **Note** The data from all available columns is included even if the column is not selected for the table. Filters applied to the application table are applied to the exported data.

Monitor the Health of an Application

Use this procedure to view details about a specific application.

Step 1 Click the menu icon (☰) and choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

Step 2 Click the **Application** tab.

The **Application** health dashboard appears.

Step 3 In the **Application** table, click the name of an application.

The **Application 360** window appears, which provides a 360° view of the application.

Step 4 Click the time range setting (🕓) at the top-left corner to specify the time range for the data that you want displayed on the window:

a) From the drop-down menu, choose a time range: **3 hours**, **24 hours**, or **7 days**.
b) Specify the **Start Date** and time; and the **End Date** and time.
c) Click **Apply**.

Step 5 To display application information for a particular location, choose the location from the *Location* drop-down list.

Step 6 From the **Filter** drop-down list, choose the SSID and click **Apply** to display the information for a particular SSID.

Step 7 Use the application health timeline slider to view the application's health score for a more granular time range and to view the application quality information.

Hover your cursor within the timeline to view the following information:

Health Score: The health score at a specific time is displayed. Metrics that are color-code in the Quality area contribute to the health score.

Quality: The Quality information area displays information about latency, jitter, and packet loss. For latency, the following aspects of delay between the client and the application are displayed:

- LAN delay—The delay in milliseconds between the client and router.
- WAN delay—The delay in milliseconds between the router and server.
- Application delay—The delay in milliseconds between the server and the application.

You can click and drag the timeline boundary lines to specify the time range. This sets the context for the application data that is displayed in the Application 360 window.

Step 8 Use the **Application Details** area, below the timeline, to view the following information:

Application Details	
Item	**Description**
Health Score	The health score of an application is calculated based on the weighted average of the application's qualitative metrics, which include packet loss, network latency, and jitter. **Note** The health score is not available for Cisco Catalyst 9000 Series Switches and Cisco AireOS wireless controller. These devices do *not* poll the KPIs that are required to calculate a health score.
Time and Date range	Displays the time and date range for the data that is displayed in the **Application 360** window.
Business Relevance **Traffic Class** **Category**	Displays the application's Next Generation Network-Based Application Recognition (NBAR) classifying information.
Issues tab	Click to view the list of issues. See step 8.
Exporters tab	Click to view the list of devices that send NetFow traffic to Cisco DNA Center and other details. See step 9.

Step 9 Click **Issues** to view the following information:

Issues
Displays any issues that must be addressed. Issues are listed based on the timestamp. The most recent issue is listed first. Click an issue to open a slide-in pane to view the corresponding details, such as the description of the issue, impact, and suggested actions. From the slide-in pane, you can do the following: • To resolve an issue: **a.** From the drop-down list, choose **Resolve**. **b.** To view the list of issues that have been resolved, click **Resolved Issues**. • To ignore an issue: **a.** From the drop-down list, choose **Ignore**. **b.** Set the number of hours to ignore the issue on the slider. **c.** Click **Confirm**. **d.** To view the list of issues that have been ignored, click **Ignored Issues**. For information about the types of issues, see View and Manage Issues.

Step 10 Click **Exporters** to view the following information:

Exporters	
Item	**Description**
Device	Displays the list of devices that is sending NetFlow traffic to Cisco DNA Center such as router, switch, wireless controller, and appliance.
Health Score	The last 5-minute health score. The health score is calculated on the basis of the application's qualitative metrics, which include packet loss, network latency, and jitter. **Note** The health score is not available for Cisco Catalyst 9000 Series Switches and Cisco AireOS wireless controller. These devices do *not* poll the KPIs that are required to calculate a health score.
Traffic Class	Displays the application's NBAR classifying information if available.
Go to Device 360	Click to open the **Device 360** window for a specific device.

Step 11 To view metric charts, do the following:

- For routers and appliances, click the exporter row to display charts (below the row) for the following metrics: usage, average throughput, packet loss, jitter, and latency.
- For switches and wireless controllers, click the device name to open a slide-in pane to view charts for the following metrics: usage and average throughput.

You can also click **Device 360** in the slide-in pane to open the **Device 360** window for a specific device.

Metric Charts	
Charts	**Description**
Usage	The number of bytes transferred by the client for the particular application.
Throughput	The rate of the application traffic (in Mbps) flowing between the client and the server.
Packet Loss	The percentage (maximum and average) of packet loss. **Note** This metric is not available for switches and wireless controllers.
Latency	The network latency time (maximum and average) in milliseconds. The following latency charts are available: • Network Latency • Client Network Latency • Server Network Latency • Application Network Latency **Note** This metric is not available for switches and wireless controllers.
Jitter	The variance in time delay in milliseconds (maximum and average) between data packets over your network. **Note** This metric is not available for switches and wireless controllers.
DSCP	• **Observed**: The application's current DSCP value. • **Expected**: The default DSCP value assigned by NBAR. **Note** This metric is not available for Optimized APM.

Step 12 View the list of clients that are accessing the application in the **Application Endpoint** table (displayed after the metric charts).

Click the **Managed Clients** tab, if you want to view only the clients that are managed by Cisco DNA Center.

Details about each client is provided in the table, such as identifier (user ID, hostname, IP address, or MAC address, whichever is available in that order), client, client health, app health, usage, device type, MAC address, and VLAN ID.

For active clients, you can click the **Identifier** column to open the **Client 360** window.

You can view up to 100 clients in this table. To view additional clients, click **Show More**.

Step 13 (Optional) Customize the data you want displayed in the table:

a) Click ⋮.
A list of options appears.
b) Check the check boxes for the data you want displayed in the table.

c) Click **Apply**.

Step 14 (Optional) To export the table data to a CSV file, click **Export**.

Note The data from all available columns is included even if the column is not selected for the table. Filters applied to the application table are applied to the exported data.

Configure Health Score Settings for Applications

Use this procedure to configure the health score settings for applications. You can customize the health score calculation for applications by changing the KPI thresholds on a per-traffic class basis and specifying the KPIs that are included for the calculation.

Step 1 Click the menu icon (☰) and choose **Assurance** > **Manage** > **Health Score Settings**.

Step 2 Click the **Application Health** tab.

Step 3 Click the tab of the application category to customize its health score calculation settings.

The tab displays the KPIs that affect the health score calculation of the application.

Step 4 From the **KPI Name** column, click the KPI name link.

The slide-in pane for the KPI appears.

Step 5 Configure the KPI health score settings:

a) Customize the KPI threshold value for **Poor**, **Fair**, and **Good** health score.
b) **Weight**: Valid weights are between 1–10. The higher the weight is, the KPI has more impact on the application health.
c) Check **Include for health score** check box if you want this KPI to be included in the health score calculation.
d) Click **Reset to Default** to restore the default KPI settings.

Step 6 Click **Apply**.

Understand Application Health Score and KPI Metrics

This section provides information about how the overall and individual application health scores and KPI metrics are computed.

Overall Application Health Score

The Application Health score is the percentage of the number of healthy business-relevant applications (a health score from 8 to 10), divided by the total number of business relevant applications. The score is calculated over the latest 5-minute interval.

Example: 90% (health score) = 90 (business-relevant applications with a health score from 8 to 10) ÷ 100 (total number of business-relevant applications)

Individual Application Health Score

The Individual Application Health score is calculated based on the weighted average of the application's qualitative metrics, which include packet loss, network latency, and jitter.

The Individual Application health is measured on a scale of 1 to 10, with 10 being the best score. The following formula is used to calculate the Individual Application Health score:

Individual Application Health Score = (Latency_Weight * Latency_VoS_Score + Jitter_Weight * Jitter_VoS_Score + PacketLoss_Weight * PacketLoss_VoS_Score) ÷ (Latency_Weight + Jitter_Weight + PacketLoss_Weight)

Note The health score is not available for Cisco Catalyst 9000 Series Switches and Cisco AireOS wireless controller. These devices do *not* poll the KPIs that are required to calculate a health score.

The workflow for calculating the Individual Application Health score is as follows:

1. Obtain the KPIs: Jitter, Latency, and Packet Loss.
2. Determine the application's Traffic Class based on the DSCP value from the flow record.
3. Convert the KPI numbers into Validation of Service score (VoS score) using the Cisco Validated Design (CVD) thresholds for each Traffic Class and KPI metric.
4. Get the weightage of the KPIs based on the application's Traffic Class and Tolerance level. The weightage is based on RFC4594.
5. Calculate the Application Health score. This is the weighted average of packet loss, network latency, and jitter.