Provision Services

Applications

The following sections provide information about applications.

About Application Visibility

The Application Visibility service lets you manage your built-in and custom applications and application sets.

The Application Visibility service, hosted as an application stack within Cisco DNA Center, lets you enable the Controller-Based Application Recognition (CBAR) function on a specific device to classify thousands of network and home-grown applications and network traffic.

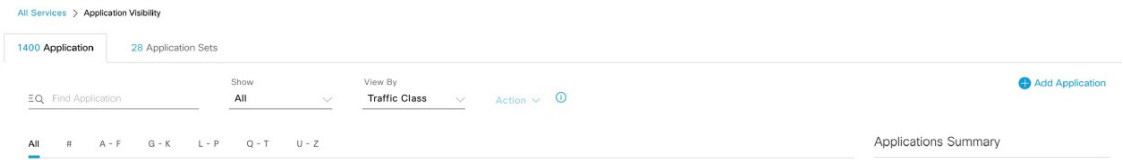
You can install the following packages:

- **Application Policy**: Lets you automate QOS policies across LAN, WAN, and wireless within your campus and branch.
- **Application Registry**: Lets you view, manage, and create applications and application sets.
- **Application Visibility Service**: Provides application classification using Network-Based Application Recognition (NBAR) and CBAR techniques.

  NBAR supports provisioning of up to 450 interfaces on Cisco Catalyst 9000 devices. Cisco DNA Center Application Visibility does not exceed this 450-interface limit.

Note To ensure compatibility, the preceding packages must have the same package version.

If you install Application Registry or both Application Registry and Application Policy, you can see the **Applications** and **Application Sets** tabs when you click the menu icon (☰) and choose **Provision** > **Services** > **Application Visibility**.



If you install Application Registry and Application Visibility Service or Application Registry, Application Policy, and Application Visibility Service, you can see the **Applications**, **Application Sets**, and **Discovered Applications** tabs when you click the menu icon (☰) and choose **Provision** > **Services** > **Application Visibility**.

The Application Visibility service has the following phases:

- Day zero: First-time service enablement.
- Day *n*: Ongoing monitoring and configuration changes.

Day-Zero Setup Wizard to Enable the Application Visibility Service

Follow the Day-Zero Setup wizard to enable the Application Visibility service in Cisco DNA Center.

Step 1 Click the menu icon (☰) and choose **Provision** > **Application Visibility**.

Step 2 In the **Application Visibility** window, click **Next**.
A dialog box for enabling the Application Visibility service is displayed.

Step 3 Click **Yes** to enable CBAR on Cisco DNA Center.

Step 4 Check the **Enable CBAR on all Ready Devices** check box, or choose the devices with **CBAR Readiness Status** in the **Ready** state.

If you want to choose a device that is not CBAR ready, follow the info message to move it to Ready state before proceeding in the **Setup** wizard.

Step 5 Click **Next**.

Step 6 Choose an external authoritative source, such as Microsoft Office 365 Cloud Connector, to either help classify the unclassified traffic or help generate improved signatures.

Step 7 If you want to exclude interfaces in the Application Visibility service, in the **Enable CBAR** slide-in pane do the following:

a) Search for the device name or locate the device, and click **View Interfaces**.
b) Locate the interface that you want to exclude.
c) In the **Status** column, click the toggle button to disable the interface.

By default, **All** is enabled in the **Show** toggle button, that displays all the available interfaces. You can choose **Excluded Interfaces** to view the excluded interfaces.

d) Click **Save**.

Step 8 Click **Finish**.

The **Overview** window shows the applications in registry, devices by active recognition method, CBAR readiness status, application observed in the network for the past 2, 24, and 48 hours (valid only if CBAR is enabled on at least one device), service health, and CBAR health score.

Day-*n* Application Visibility View

The Day-*n* Application Visibility page shows the application registry, device recognition method, device CBAR readiness, application observed in the network for the past 2, 24, or 48 hours (valid only in case CBAR was enabled on at least one device), and CBAR health.

The following table describes the charts that are available in the **Overview** tab in **Provision > Services > Application Visibility**.

Table 1: Day-n Application Visibility View: Charts

Chart	Description
Applications in Registry	This chart displays the number of applications available in the Cisco DNA Center application registry that can be used in Application Policy. The applications are classified as follows: • Custom: Applications added by a user • Built-in: Preinstalled applications in Cisco DNA Center • Discovered: Applications discovered by different recognition methods and imported into the application registry
Applications Observed in Network	This chart shows the applications observed in the past 2, 24, or 48 hours and lists the applications with highest network traffic ratio. **Note** The chart shows the applications observed only on CBAR-enabled devices.
Devices by Active Recognition Method	This chart displays the number of devices classified by each of the application recognition methods: • CBAR-enabled devices: Routers and switches • NBAR-based devices: Routers, switches, Cisco Wireless Controllers, and Cisco Catalyst 9800 Series Wireless Controller • IP/port-based devices: Switches • Not supported devices: Devices that are not supported by any of the preceding methods

Chart	Description
CBAR Readiness Status	This chart displays the device count in each CBAR readiness status. • Enabled: Devices that are CBAR-enabled • Ready: Devices that are ready for enabling CBAR **Note** The info icon next to **Ready** status shows the respective device is wireless enabled. • Not Ready: Devices that support CBAR but are not ready for enabling CBAR due to some issues • Not Supported: Devices that do not support CBAR
Service Health and CBAR Health	This widget displays the service health and the average health score for all CBAR-enabled devices. The device is healthy if there are no outstanding errors or warnings on that device. The CBAR health score is calculated across all CBAR-enabled devices. You can view the CBAR health of each CBAR-enabled device. A 0% CBAR health score indicates that the device has at least one error (P1). A 50% CBAR health score indicates that the device has no errors but has at least one warning (P2). A 100% CBAR health score indicates a healthy device. This widget also shows the service issues and remedies (P1, P2, and P3). The green tick mark indicates healthy service. The red cross mark indicates at least one P1 issue. The warning icon indicates at least one P2 issue. Click P1, P2, and P3 to view more about the services issues and remedies.
CBAR Health Issues and Remedies	All issues are classified by priority: • Errors (P1) • Warnings (P2) • Others (P3) Click the **P1**, **P2**, and **P3** tabs to view the device issues and remedy details.

Site Devices Table: This table provides device information and statuses. You can filter the devices using the **Quick Filter** and **Device Table Filter**.

Table 2: Day-n Application Visibility View: Site Devices Table

Column	Description
Device Name	Name of the device. Click the device name to view the CBAR Service Status.
Management IP	IP address of the device.
Device Type	Group of related devices, such as routers, switches and hubs, or wireless controllers.

Column	Description
Site	The site to which the device is assigned.
Fabric	The fabric domain to which the device is assigned.
Role	Role assigned to each discovered device during the scan process. The device role is used to identify and group devices according to their responsibilities and placement within the network. If Cisco DNA Center cannot determine a device role, it sets the device role to Unknown.
Active Recognition Method	Shows the device recognition method (CBAR, NBAR, IP/Port, or Not Supported).
OS Version	Cisco IOS software that is currently running on the device.
CBAR Readiness Status	Hover over the status displayed in the CBAR Readiness Status column to view the Remedy message.
Protocol Pack Version	Shows the current version of the protocol pack installed on the device and the protocol pack update status.
Device Registry Status	Shows the synchronization status of the device with the application registry. Hover over the info icon or the error icon to view more details about the synchronization status.
Deployment Status	Shows the CBAR deployment status. For more information, see Reconfigure CBAR, on page 5.
Service Health Status	Click the issues in the Service Health Status column to open the CBAR Service status page, which displays a complete list of issues and the service status information of a device. If you click the Cisco Catalyst 9K device name, you can view the footprint (service load, CPU, and flows) of the CBAR service.
Application QoS Policy	The application policy applied to the device. For Cisco Wireless Controllers with more than one application policy, the number of application policies applied and the name of all the applied application policies are displayed.
WAN Interfaces	Shows the number of WAN interfaces. Click the WAN interface details to view the WAN connectivity settings for the device.

Reconfigure CBAR

You can include or exclude interfaces from **Site Devices** table in the **Overview** window.

Step 1 Click the menu icon (☰) and choose **Provision** > **Services** > **Application Visibility**.

Step 2 In the **Overview** page, scroll down to view the **Site Devices** table.

Step 3 Click **Re-Configure** in the **Deployment status** column for the device you want to configure and do the following:

a) In the **Enable CBAR** slide-in pane, search for the device name or locate the device and click **View Interfaces**.

b) Locate the interface that you want to exclude.
c) In the **Status** column, click the toggle button to disable the interface and click **Save**.

Step 4 To include interfaces, choose **Excluded Interfaces** and enable the toggle button next to the desired interfaces, and click **Save**.

Step 5 Click **Enable**.

What to do next

Applications and Application Sets

Applications are the software programs or network signaling protocols that are used in your network. Cisco DNA Center supports all of the applications in the Cisco Next Generation Network-Based Application Recognition (NBAR2) library of approximately 1400 distinct applications.

Applications are grouped into logical groups called application sets. An application set can be assigned a business relevance within a policy.

Applications are mapped into industry standard-based traffic classes, as defined in RFC 4594, that have similar traffic treatment requirements. The traffic classes define the treatments (such as Differentiated Services Code Point [DSCP] marking, queuing, and dropping) that will be applied to the application traffic, based on the business relevance group that is assigned.

If you have additional applications that are not included in Cisco DNA Center, you can add them as custom applications and assign them to application sets.

Unidirectional and Bidirectional Application Traffic

Some applications are completely symmetrical and require identical bandwidth provisioning on both ends of the connection. Traffic for such applications is described as bidirectional. For example, if 100 kbps of Low-Latency Queueing (LLQ) is assigned to voice traffic in one direction, 100 kbps of LLQ must also be provisioned for voice traffic in the opposite direction. This scenario assumes that the same Voice over IP (VoIP) coder-decoders (codecs) are being used in both directions and do not account for multicast Music-on-Hold (MoH) provisioning. However, certain applications, such as streaming video and multicast MoH, are most often unidirectional. Therefore, it might be unnecessary, and even inefficient, to provision any bandwidth guarantees for such traffic on a branch router for the branch-to-campus direction of traffic flow.

Cisco DNA Center lets you specify whether an application is unidirectional or bidirectional for a particular policy.

On switches and wireless controllers, NBAR2 and custom applications are unidirectional by default. However, on routers, NBAR2 applications are bidirectional by default.

Custom Applications

Custom applications are applications that you add to Cisco DNA Center. An orange bar is displayed next to custom applications to distinguish them from the standard NBAR2 applications and application sets. For wired devices, you can define applications based on server name, IP address and port, or URL. You can define custom applications for Cisco Catalyst 9800 Series Wireless Controllers and not for Cisco AireOS controllers.

When you define an application according to its IP address and port, you can also define a DSCP value and port classification.

To simplify the configuration process, you can define an application based on another application that has similar traffic and service-level requirements. Cisco DNA Center copies the other application's traffic class settings to the application that you are defining.

Cisco DNA Center does not configure ACLs for port numbers 80, 443, 53, 5353, and 8080, even if they are defined as part of a custom application. If the custom application has a transport IP defined, Cisco DNA Center configures the application on the devices.

Note For a custom application to be programmed on devices when a policy is deployed, you must assign the custom application to one of the application sets defined in the policy.

Discovered Applications

Discovered applications are applications that are discovered by importing from recommended customization such as an Infoblox DNS server or by importing from the recommended unclassified applications flow.

The unclassified traffic can come from any flow that the CBAR-enabled device identifies but that is not recognized by the NBAR engine. In such cases, the applications that have a meaningful bit rate are reported as unclassified and can be imported and used as applications in Cisco DNA Center.

The Application Visibility service lets Cisco DNA Center connect with external authoritative sources like the Microsoft Office 365 Cloud Connector to help classify the unclassified traffic or help generate improved signatures.

Note You must configure an NBAR cloud connector before configuring the Microsoft Office 365 Cloud Connector.

The discovered applications are imported to the application registry.

Favorite Applications

Cisco DNA Center lets you flag applications that you want to configure on devices before all other applications. Flagging an application as a favorite helps to ensure that the QoS policies for your favorite applications get configured on devices. For more information, see Processing Order for Devices with Limited Resources.

When custom applications are created they are marked as favorite applications.

Although there is no limit to the number of applications that you can mark as favorites, designating only a small number of favorite applications (for example, fewer than 25) helps to ensure that these applications are treated correctly from a business-relevance perspective in deployments with network devices that have limited ternary content addressable memory (TCAM).

Favorite applications can belong to any business-relevance group or traffic class and are configured system-wide, not on a per-policy basis. For example, if you flag the Cisco Jabber video application as a favorite, the application is flagged as a favorite in all policies.

Keep in mind that not only can business-relevant applications be flagged as favorites, even business-irrelevant applications can be flagged as such. For example, if administrators notice a lot of unwanted Netflix traffic on

the network, they might chose to flag Netflix as a favorite application (despite it being assigned as business-irrelevant). In this case, Netflix is programmed into the device policies before other business-irrelevant applications, ensuring that the business intent of controlling this application is realized.

Configure Applications and Application Sets

The following subsections describe the various tasks that you can perform in the context of applications and application sets.

Note You can edit or delete only custom and discovered applications. You can edit or delete a maximum of 100 custom and discovered applications at one instance. If you choose NBAR applications for editing or deleting, a notification message indicates the number of applications that can be edited or deleted, excluding the number of chosen NBAR applications.

Change an Application's Settings

You can change the application set or traffic class of an existing NBAR, custom, or discovered application.

Step 1 Click the menu icon (☰) and choose **Provision** > **Services** > **Application Visibility** > **Application**.

Step 2 Use the **Search**, **Show**, or **View By** fields to locate the application that you want to change.

You can search applications based on their name, port number, and traffic class.

Step 3 Click the application name.

Step 4 In the dialog box, change one or both settings:

- **Traffic Class**: Choose a traffic class from the drop-down list. Valid traffic classes are BROADCAST_VIDEO, BULK_DATA, MULTIMEDIA_CONFERENCING, MULTIMEDIA_STREAMING, NETWORK_CONTROL, OPS_ADMIN_MGMT, REAL_TIME_INTERACTIVE, SIGNALING, TRANSACTIONAL_DATA, VOIP_TELEPHONY.
- **Application Set**: Choose an application set from the drop-down list. Valid application sets are authentication-services, backup-and-storage, collaboration-apps, consumer-browsing, consumer-file-sharing, consumer-gaming, consumer-media, consumer-misc, consumer-social-networking, database-apps, desktop-virtualization, email, enterprise-ipc, file-sharing, generic-browsing, generic-media, generic-misc, tunneling, local-services, naming-services, network-control, network-management, remote-access, saas-apps, signaling, software-development-tools, software-updates, streaming-media.

Step 5 Click **Save**.

Create a Server Name-Based Custom Application

If you have applications that are not in Cisco DNA Center, you can add them as custom applications.

Step 1 Click the menu icon (☰) and choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Application** tab.

Step 3 Click **Add Application**.

Step 4 In the dialog box, provide the necessary information in the following fields:

- **Application name**: Name of the custom application. The name can contain up to 24 alphanumeric characters, including underscores and hyphens. The underscore and hyphen are the only special characters allowed in the application name.
- **Type**: Method by which users access the application. Choose **Server Name** for applications that are accessible through a server.
- **Server name**: Name of the server that hosts the application.
- **Similar to**: Application with similar traffic-handling requirements. Click the radio button to select this option, and then select an application from the drop-down list. Cisco DNA Center copies the other application's traffic class to the application that you are defining.
- **Traffic class**: Traffic class to which the application belongs. Valid values are BULK_DATA, TRANSACTIONAL_DATA, OPS_ADMIN_MGMT, NETWORK_CONTROL, VOIP_TELEPHONY, MULTIMEDIA_CONFERENCING, MULTIMEDIA_STREAMING, BROADCAST_VIDEO, REAL_TIME_INTERACTIVE, and SIGNALING.
- **Application set**: Application set is where you want the application to reside. Valid application sets are authentication-services, backup-and-storage, collaboration-apps, consumer-browsing, consumer-file-sharing, consumer-gaming, consumer-media, consumer-misc, consumer-social-networking, custom applications, database-apps, desktop-virtualization, email, enterprise-ipc, file-sharing, generic-browsing, generic-media, generic-misc, tunneling, local-services, naming-services, network-control, network-management, remote-access, saas-apps, signaling, software-development-tools, software-updates, streaming-media.

Step 5 Click **OK**.

Create an IP Address and Port-Based Custom Application

If you have applications that are not in Cisco DNA Center, you can add them as custom applications.

Step 1 Click the menu icon ( ) and choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Application** tab.

Step 3 Click **Add Application**.

Step 4 In the **Application name** field, enter a name for the custom application. The name can contain up to 24 alphanumeric characters, including underscores and hyphens. The underscore and hyphen are the only special characters allowed in the application name.

Step 5 In the **Type** area, click the **Server IP/Port** radio button to indicate that the application is accessible through an IP address and port.

Step 6 Check the **DSCP** check box and define a DSCP value. If you do not define a value, the default value is Best Effort. Best-effort service is essentially the default behavior of the network device without any QoS.

Step 7 Check the **IP/Port Classifiers** check box to define the IP address and subnet, protocol, and port or port range for an application. Valid protocols are IP, TCP, UDP, and TCP/UDP. If you select the IP protocol, you do not define a port number or range. Click to add more classifiers.

Step 8 Define your application traffic-handling requirements using one of the following methods:

- **Similar To**: If your application has similar traffic-handling requirements as an existing application, click the **Similar To** radio-button and choose the application from the drop-down list. Cisco DNA Center copies the traffic class of the other application to the application that you are defining.
- **Traffic Class**: If you know the traffic class that you want to define for your application, click the **Traffic Class** radio button and choose the traffic class from the drop-down list. Valid values are BULK_DATA, TRANSACTIONAL_DATA, OPS_ADMIN_MGMT, NETWORK_CONTROL, VOIP_TELEPHONY, MULTIMEDIA_CONFERENCING, MULTIMEDIA_STREAMING, BROADCAST_VIDEO, REAL_TIME_INTERACTIVE, and SIGNALING.

Step 9 From the **Application Set** drop-down list, choose the application set to which the application will belong. Valid application sets are authentication-services, backup-and-storage, collaboration-apps, consumer-browsing, consumer-file-sharing, consumer-gaming, consumer-media, consumer-misc, consumer-social-networking, custom applications, database-apps, desktop-virtualization, email, enterprise-ipc, file-sharing, generic-browsing, generic-media, generic-misc, tunneling, local-services, naming-services, network-control, network-management, remote-access, saas-apps, signaling, software-development-tools, software-updates, streaming-media.

Step 10 Click **OK**.

Create a URL-Based Custom Application

If you have applications that are not in Cisco DNA Center, you can add them as custom applications.

Step 1 Click the menu icon (☰) and choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Application** tab.

Step 3 Click **Add Application**.

The **Add Application** dialog box appears.

Step 4 In the **Application name** field, enter the name of the custom application. The name can contain up to 24 alphanumeric characters, including underscores and hyphens. (Underscores and hyphens are the only special characters allowed in the application name.)

Step 5 For **Type**, click the **URL** radio button.

Step 6 In the **URL** field, enter the URL used to reach the application.

Step 7 Configure the traffic class:

- To use the same traffic class as another application with similar traffic-handling requirements, click the **Similar To** radio button and choose an application from the drop-down list.
- To specify the traffic class, click the **Traffic Class** radio button and choose a traffic class from the drop-down list. Valid values are BULK_DATA, TRANSACTIONAL_DATA, OPS_ADMIN_MGMT, NETWORK_CONTROL, VOIP_TELEPHONY, MULTIMEDIA_CONFERENCING, MULTIMEDIA_STREAMING, BROADCAST_VIDEO, REAL_TIME_INTERACTIVE, and SIGNALING.

Step 8 From the **Application Set** drop-down list, choose an application set in which you want the application to reside.

Step 9 Click **OK**.

Edit or Delete a Custom Application

If required, you can change or delete a custom application.

Note You cannot delete a custom application that is directly referenced by an application policy. Application policies typically reference application sets and not individual applications. However, if a policy has special definitions for an application (such as a consumer or producer assignment or bidirectional bandwidth provisioning), the policy has a direct reference to the application. As such, you must remove the special definitions or remove the reference to the application entirely before you can delete the application.

Step 1 Click the menu icon ( ) and choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Application** tab.

Step 3 Use the **Search**, **Show**, or **View By** fields to locate the application that you want to change.

You can search applications based on their name, port number, and traffic class.

Step 4 To edit the application:

a) Click the application name and make the required changes. For information about the fields, see Create a Server Name-Based Custom Application, on page 8, Create an IP Address and Port-Based Custom Application, on page 9, or Create a URL-Based Custom Application, on page 10.

b) Click **OK**.

Note When policy is redeployed, the edited custom applications are not reconfigured on Cisco Catalyst 9800 Series Wireless Controller.

Step 5 To delete the application, click in the application box, and then click **OK** to confirm.

Mark an Application as Favorite

You can mark an application as a favorite to designate that the application's QoS configuration must be deployed to devices before other applications' QoS configuration. An application marked as favorite has a yellow star next to it.

When you add or edit a policy, applications marked as a favorites are listed at the top of the application set.

Applications are configured system-wide, not on a per-policy basis. For more information, see Favorite Applications, on page 7.

Step 1 Click the menu icon ( ) and choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Application** tab.

Step 3 Locate the application that you want to mark as a favorite.

Step 4 Click the star icon.

Create a Custom Application Set

If none of the application sets fits your needs, you can create a custom application set.

Step 1 Click the menu icon ( ) and choose **Provision** > **Services** > **Application Visibility**.

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

Step 3 Click **Add Application Set**.

Step 4 In the dialog box, enter a name for the new application set.

Cisco DNA Center creates the new application set; however, it contains no applications.

Step 5 Click **OK**.

Step 6 Use the **Search**, **Show**, or **View By** fields to locate the application set.

You can search applications based on their name, port number, and traffic class.

Step 7 Locate the applications that you want to move into the new application set.

Step 8 Check the check box next to the applications that you want to move.

Step 9 Drag and drop the applications into the new application set.

Edit or Delete a Custom Application Set

If required, you can change or delete a custom application set.

Note You cannot delete a custom application set that is referenced by an application policy. You must remove the application set from the policy before you delete the application set.

Step 1 Click the menu icon ( ) and choose **Provision** > **Services** > **Application Visibility**.

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

Step 3 Use the **Search**, **Show**, or **View By** fields to locate the application set that you want to change.

You can search applications based on their name, port number, and traffic class.

Step 4 Do one of the following:

- To edit the application set, drag and drop applications into or out of the application set. Click **OK** to confirm each change.
- To delete the application set, click in the application set box, and then click **OK** to confirm.

Update the Protocol Pack on a CBAR-Enabled Device

You can upgrade the protocol pack on any device that supports CBAR to the latest or any specific protocol pack.

Before you begin

- Configure Cisco credentials on **System Settings**. For more information about configuring Cisco credentials, see the Cisco DNA Center Administrator Guide.
- Devices must support CBAR.
- CBAR must be enabled on the device.
- Protocol packs for the device must be available on cisco.com.

Step 1 Click the menu icon (☰) and choose **Provision** > **Services** > **Application Visibility**.

Step 2 On the **Overview** page, displaying day-*n* information, scroll down to view the **Site Devices** table.

Step 3 Check the status shown in the **Protocol Pack Version** column in the **Site Devices** table.

You can click the **Outdated** status to view the list of applicable protocols packs in the **Update Protocol Pack** window.

Step 4 Click **Update** corresponding to the required protocol pack version in the **Update Protocol Pack** window.

The **Protocol Pack Version** column shows **In progress** status. Click the info icon to view the current updating version. If the **Protocol Pack Version** column shows **Update failed** status, click the error icon to view the failure reason.

Step 5 If you want to update all the devices or selected devices to the latest protocol pack, do the following:

To update the protocol pack on all applicable CBAR-enabled devices:

- From the **Update Protocol Pack** drop-down list, choose **All Devices** and click **Yes** in the subsequent warning pop-up windows.

To update the protocol pack on the selected devices:

- Choose the devices in the **Site Devices** table.
- From the **Update Protocol Pack** drop-down list, choose **Selected Devices** and click **Yes** in the subsequent warning pop-up windows.

Discover Unclassified Applications

The Application Visibility service in Cisco DNA Center obtains information on classified and unclassified domains and sockets from devices and displays that information in the **Observed Traffic** chart. The number of unclassified server names and IP/ports that are discovered by the Application Visibility service is shown under **Recommendations**.

You can add the unclassified server names and IP/ports to the Application Registry.

Note You can add a maximum of 1100 discovered applications in the Application Registry.

Step 1 Click the menu icon (☰) and choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Discovered Applications** tab.

Step 3 Under **Recommendations**, click the **discovered server names** link or the **discovered IP/Ports** link.

The table lists the discovered servers or IP/ports that are not classified. Choose the server and check the **Hide Ignored Applications** check box if you want to hide the selected server or IP/ports in the table.

Step 4 Choose the server or IP/ports that you want to import as an application in the Application Registry.

Step 5 Choose the required **Application**, **Application Set**, and **Traffic Class** from the drop-down list.

Step 6 Click **Import**.

Step 7 Click the **Applications** tab and choose **Show** > **Discovered** to view the imported application.

Configure the NBAR Cloud Connector

The Application Visibility service uses the NBAR cloud connector to enrich the protocol pack and enhance visibility for unknown applications by sending and receiving data from the cloud.

Step 1 Click the menu icon (☰) and choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Discovered Applications** tab.

Step 3 In the **NBAR Cloud** window, click **Configure**.

Step 4 In the **Configure NBAR Cloud** window, click the toggle button to **Enable**.

Step 5 Click the **Cisco API Console** link to retrieve the key and client secret.

Step 6 Enter your Cisco credentials to open the **Cisco API Console** in a new browser tab and do the following:

a) In the **My Apps & Keys** tab, click **Register a New App**.

b) Complete the following fields in the **Register an Application** screen.

- **Name of Your Application**: Enter the application name.
- **Application Type**: Check the **Service** check box.
- **Grant Type**: Check the **Client Credentials** check box.
- **Select APIs**: Check the **Hello API** check box.

c) Click **Register**.

The registered application details appear in the **My Apps & Keys** tab.

d) Copy the key and client secret of the registered application from the **Cisco API Console**.

Step 7 Complete the following fields in the **Configure NBAR Cloud** window:

a) In the **Client ID** field, enter the key that you copied from the **My Apps & Keys** tab in the preceding step.

b) In the **Client Secret** field, enter the client secret that you copied from the **My Apps & Keys** tab in the preceding step.

c) In the **Organization Name** field, enter the organization name.

d) Confirm that the **Enable Protocol Pack Auto Update** check box is checked. (It's checked by default.)

e) Confirm that the **Improve my network using NBAR Cloud telemetry** check box is checked. (It's checked by default.)

f) Under **NBAR classification telemetry data is being sent to region**, choose the desired location.

Step 8 Click **Save**.

Application Visibility Service Support for the Cisco DNA Traffic Telemetry Appliance

The Cisco DNA Traffic Telemetry Appliance generates endpoint telemetry from mirrored IP network traffic and shares the telemetry data with Cisco DNA Center for endpoint visibility and segmentation.

The prerequisites for enabling CBAR on the Cisco DNA Traffic Telemetry Appliance include:

- The device must be assigned to a site.
- The device role must be set to **Distribution** mode.

You can configure custom applications with attribute sets and maps on the Cisco DNA Traffic Telemetry Appliance without configuring a QoS policy. For more information, see Create an Application Policy and Deploy an Application Policy.

Discover Infoblox Applications

You can integrate Cisco DNA Center with an organizational Infoblox DNS server to resolve unclassified traffic based on server names.

Before you begin

- The Infoblox WAPI version must be 1.5 or later. To check the Infoblox WAPI version, log in to the Infoblox server and choose **Help** > **Documentation** > **WAPI Documentation**.
- Create a role with at least Read Only permissions and assign the role to the Infoblox user. For more information, see Manage Users in the Cisco DNA Center Administrator Guide.

Step 1 Click the menu icon (☰) and choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Discovered Applications** tab.

Step 3 Under **Infoblox DNS Server**, click **Configure**.

Step 4 In the **Infoblox Connector Settings** window, click the **Here** link to configure IPAM/DNS server credentials in Cisco DNA Center.

Step 5 Complete the IPAM settings. For more information, see Configure an IP Address Manager in the Cisco DNA Center Administrator Guide.

Step 6 Go back to **Infoblox Connector Settings** and complete the following settings:

- Check the **All DNS Zones** check box, or choose the required DNS zones from the **DNS Zones to Inspect** drop-down list. The drop-down list shows the DNS zones defined in the Infoblox server.
- From the **Inspect** drop-down list, choose the required inspection record.
- Check the **Read Application name from** check box and click the **Extensible Attribute** or **AVC RRTYPE format** radio button. If you click the **Extensible Attribute** radio button, enter the extensible attribute name that contains descriptive application names.

- From **Default Traffic Class**, choose the default traffic class for classifying the Infoblox applications.
- From **Default Application Set**, choose the default application set for classifying the Infoblox applications.

Step 7 Click **Save**.

The **Poll Infoblox to Import Applications** link appears under **Recommendations**.

Step 8 Click the **Poll Infoblox to Import Applications** link to get a list of applications from the DNS zones configured in the **Infoblox Connector Settings**.

Step 9 Choose the application that you want to import and complete the following:

- If the application does not have a name defined in the Infoblox server, edit the application name.
- Choose the required application set and traffic class from the drop-down list if you want to change the default application set and traffic class defined in the **Infoblox Connector Settings**.

Step 10 Click **Import**.

Step 11 Click the **Applications** tab and choose **Discovered** in the **Show** drop-down list to view or edit the imported Infoblox applications.

If you change the server name of an application after importing the application, the **Application Status** column in the **Infoblox Discovered Applications** window shows the status of the application as **Updated**. The application name that you see in the **Application Status** column is the new server name of the application. Click the info icon to view the old server names of the application.

Resolve Unclassified Traffic Using Microsoft Office 365 Cloud Connector

Cisco DNA Center can connect to external authoritative sources like Microsoft Office 365 Cloud Connector that can help classify the unclassified traffic or help generate improved signatures.

Before you begin

- Ensure that Cisco DNA Center has connectivity to the internet.
- Ensure that the NBAR cloud is enabled.

Step 1 Click the menu icon (☰) and choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Discovered Applications** tab.

Step 3 Click the **MS Office 365 Cloud** toggle button to enable polling of MSFT signatures.

- When you enable Microsoft Office 365 Connector, the controller starts importing the new domains' information from Microsoft Office 365 and finds the correct application for the new domains.
- The new secondary pack is installed along with the Cisco DNA Center-based protocol pack and new domains are supported automatically.

Edit or Delete a Discovered Application

If required, you can edit or delete a discovered application.

Step 1 Click the menu icon ( ) and choose **Provision** > **Services** > **Application Visibility**.

Step 2 Click the **Application** tab.

Step 3 Use the **Search**, **Show**, or **View By** fields to locate the discovered application that you want to change.

You can search for applications based on their name, port number, and traffic class.

Step 4 To edit the application:

a) Click the application name and make the required changes.

For discovered applications, you can edit only the **Attribute Set** and **Traffic Class**.

b) Click **OK**.

Step 5 To delete the application, click in the application box, and then click **OK**.

Application Hosting

The following sections provide information about application hosting.

About Application Hosting

Application hosting lets you manage the lifecycle of third-party applications on devices managed by Cisco DNA Center. You can host third-party docker applications on Cisco Catalyst 9300 Series switches running Cisco IOS-XE software version 16.12.1s or later, Cisco Catalyst 9100 Series Access Points running Cisco IOS-XE software version 17.3.1 or later, and Cisco Catalyst 9400 Series switches running Cisco IOS-XE software version 17.1 or later.

Note The disk space allocated in Cisco DNA Center for the hosted applications is limited to 5 GB.

Install or Update the Application Hosting Service Package

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.

Step 1 Click the menu icon ( ) and choose **System** > **Software Updates**. Alternatively, click the cloud icon and click the **Go to Software Updates** link.

Step 2 In the Software Updates window, review the following tabs:

- **Updates**: Shows the system and application updates. System Update shows the system version that is installed and the system updates that are available and have been downloaded from the Cisco cloud. Application Updates shows the available applications that can be downloaded and installed from the Cisco cloud, the size of the application, and the appropriate action (**Download**, **Install**, or **Update**). Hover your cursor over the package to view the available version and a basic description.
- **Installed Apps**: Shows the application packages that are currently installed.

Step 3 To download the Application Hosting package, click **Install** next to the Application Hosting name under **Updates** > **Application Updates**.

Step 4 To update the Application Hosting package, click **Update** next to the Application Hosting name under **Updates** > **Application Updates**.

Step 5 Ensure that the application has been updated by reviewing the version on the **Installed Apps** tab.

Note After installing the Application Hosting service package, you must log out of Cisco DNA Center, clear your browser cache, and log in to Cisco DNA Center again.

Prerequisites for Application Hosting

To enable application hosting on a Cisco Catalyst 9000 device, the following prerequisites must be fulfilled:

- Configure NETCONF port on the device before discovery.
- Configure a secure HTTP server on the switch where the applications will be hosted.
- Configure local or AAA authentication server for HTTPS user authentication on the switch. You must configure the username and password with privilege level 15.
- Ensure Cisco Catalyst 9300 Series switches are running Cisco IOS XE 16.12.x or later version and Cisco Catalyst 9400 Series switches are running Cisco IOS XE 17.1.x or later version.
- Ensure that the device has an external USB SSD pluggable storage (only for the switches of 9300 family).
- Verify that the configuration on the switch is correct. Open the WebUI on the switch and log in as the HTTPS user.

  The following example shows a working configuration on a switch:

```
prompt# sh run | sec http
ip http server
ip http authentication local
ip http secure-server
ip http max-connections 16
ip http client source-interface Loopback0
```

  Additional configuration for switches with a Cisco IOS XE release that is earlier than 17.3.3:

```
ip http secure-active-session-modules dnac
ip http session-module-list dnac NG_WEBUI
ip http active-session-modules none
```

  Additional configuration for switches with Cisco IOS XE 17.3.3 or later:

```
ip http secure-active-session-modules webui
ip http session-module-list webui NG_WEBUI
```

```
ip http session-module-list pki OPENRESTY_PKI
ip http active-session-modules pki
```

- On Cisco DNA Center, configure the HTTPS credentials while manually adding the device. The HTTPS username, password, and port number are mandatory for application hosting. The default port number is 443. You can also edit the device credentials; see Update Network Device Credentials. If you edit a device that is already managed, resynchronize that device in the inventory before it is used for application hosting-related actions.

Note Application hosting HA is not supported on three-node Cisco DNA Center clusters.

View Device Readiness to Host an Application

You must check the readiness of the Cisco Catalyst 9300 Series switch to host the application before you can install an application on the switch.

Step 1 Click the menu icon (☰) and choose **Provision** > **Services** > **App Hosting for Switches**.

Step 2 Click **All Devices**.

Step 3 View the list of devices that are capable of hosting applications. The **App Hosting Status** indicates the readiness of the device to host an application. Click **See Details** to view the list of readiness checks performed on the device.

Add an Application

You can add a Cisco package or a docker application.

Before you begin

- **Cisco Package**: You must package the application using IOS SDK tools so that the application is compatible with IOS XE operating systems.
- **Docker**: You must save the docker image as a tar file. Enter the following command to store the docker image as a tar file:

```
docker save -o <path for generated tar file> <image name:tag>
Example: docker save -o alpine-tcpdump.tar itsthenetwork/alpine-tcpdump:latest
```

Step 1 Click the menu icon (☰) and choose **Provision** > **Services** > **App Hosting for Switches**.

Step 2 Click **New Application**.

Step 3 Choose the application and category from the drop-down list.

Step 4 Click **Select** and choose the application to upload.

Step 5 Click **Upload**.

You can view the newly added application in the **App Hosting** page.

Automatic Download of ThousandEyes Enterprise Agent Application

The ThousandEyes Enterprise Agent application lets you monitor your network and oversee the network traffic paths across internal, external, carrier, and internet networks in real time. The advantage of the ThousandEyes Enterprise Agent application is that you do not have to import this application manually in your Cisco DNA Center Application Hosting Service. When the switches and hubs in the network are enabled, the ThousandEyes Enterprise Agent application is downloaded automatically within 10 minutes of starting the Application Hosting Service. To manually download the application, click the following link to the ThousandEyes Enterprise Agent .tar file:

thousandeyes-enterprise-agent.cat9k.tar

If there is no internet connection, you can set a proxy connection from the console using the following command:

```
magctl service setenv app-hosting http_proxy <proxy-value>
```

Set the proxy value to connect to the ThousandEyes Enterprise Agent application.

Update an Application

You can update the application added in Cisco DNA Center.

Step 1 Click the menu icon (☰) and choose **Provision** > **Services** > **App Hosting for Switches**.

You can view the available applications in the **App Hosting** window.

Step 2 Choose the application that you want to update.

Step 3 Click **Update App**.

Step 4 Choose a new version of the application to be uploaded.

Step 5 Click **Upload**.

Start an Application

You can start an application in Cisco DNA Center.

Step 1 Click the menu icon (☰) and choose **Provision** > **Services** > **App Hosting for Switches**.

Step 2 Choose the application and click **Manage** to view the devices that use the application.

Step 3 Choose the device that has the application that you want to start.

Step 4 From the **Actions** drop-down list, choose **Start App**.

Stop an Application

You can stop an application in Cisco DNA Center.

Step 1 Click the menu icon (☰) and choose **Provision** > **Services** > **App Hosting for Switches**.

Step 2 Choose the application and click **Manage** to view the devices that use the application.

Step 3 Choose the device that has the application that you want to stop.

Step 4 From the **Actions** drop-down list, choose **Stop App**.

View Applications Hosted on Device

Before you begin

Complete the prerequisites. For more information, see Prerequisites for Application Hosting.

Step 1 Click the menu icon (☰) and choose **Provision** > **Services** > **App Hosting for Switches**.

Step 2 To view all devices, click **All Devices** at the top-right corner, or to view only the devices that use a particular application, choose the application and click **Manage**.

If you chose to view all devices, the **All Devices** page shows the following information about the devices that are capable of hosting applications: **Hostname**, **IP Address**, **Image Version**, **App Hosting Status**, and **Last Updated**.

If you chose to view a list of devices for a particular application, the **Devices** page shows the following information about the devices that are capable of hosting applications: **Hostname**, **Device IP**, **App Version**, **App Status**, **Last Heard,** **Platform Version**, and **Action Status**.

Step 3 In the **Devices** page, click **Summary** to view a summary of failed, stopped, and running applications on a device.

Step 4 To take an action on an application, click the **Action** drop-down list and choose **Start**, **Stop**, **Edit**, **Upgrade**, or **Uninstall**.

Step 5 Click the device link in which you want to view the installed hosting applications.

The **Applications** page shows the **Name**, **Version**, **App Status**, **Monitor App**, **Health**, and **Details** of the installed applications.

Note **Monitor App** contains the link to the Application Monitoring Dashboard. This link is provided in the, Cisco DNA Center application package controller, .yaml file. If this file does not contain application dashboard URL, then this **Monitor App** column will not be applicable.

Step 6 In the **Details** column, click **View** to get more information about an application status on the device.

App details window shows the **RESOURCES**, **NETWORK**, and **DOCKER RUNTIME OPTIONS** information of an application.

Step 7 To download the log for a particular application, select the application and click **Application Logs**.

Step 8 To download tech support from the device, click **Tech Support Logs**.

Install an Application on a Cisco Catalyst 9300 Device

Cisco DNA Center allows you to install an application on a Cisco Catalyst 9300 Series switch.

Before you begin

- Complete the prerequisites. For more information, see Prerequisites for Application Hosting, on page 18.
- Add the application to Cisco DNA Center. For more information, see Add an Application, on page 19.
- Check the readiness of the switch to host the application. For more information, see View Device Readiness to Host an Application, on page 19.

Step 1 Click the menu icon (☰) and choose **Provision** > **Services** > **App Hosting for Switches**.

Step 2 Choose the application and click **Install**.

Step 3 In the **Get Started** window, enter a unique name for your workflow in the **Task Name** field and click **Next**.

Step 4 In the **Select Site** window, choose the site where you want to enable the application, and click **Next**.

Step 5 In the **Select Switches** window, choose the devices on which you want to install the application and click **Next**.

You can choose the devices that are in **Ready** and **Partially Ready** status. Click **See Details** to view the list of readiness checks performed on the device.

For devices that are in **Partially Ready** status, click the **Check Now** link in the **Readiness Check** window to validate the HTTPS credentials.

If you don't find your device in the **Devices Table**, click **Import** to add devices from a CSV file.

Step 6 In the **Configuration App** window, complete the following settings:

- **Network Settings**:
  - From the **Select Network** drop-down list, choose a VLAN to configure the application.
  - From the **Address Type** drop-down list, choose **Static** or **Dynamic**. If you choose **Static**, click the thumbnail icon and enter the **IP Address**, **Gateway**, **Prefix/Mask**, and **DNS** for the application.
- **App Resources**: Check the **Allocate all resources available on a device** or the **Customize resource allocation** check box. You can check the **Customize resource allocation** check box and modify the maximum **CPU**, **Memory**, and **Persistent Storage** values to a lower value.
- **Custom Settings**: Applicable only for Cisco package applications. Enter the configuration details for the attributes that are specified by the application.
- **App Data**: Browse and upload the application-specific files. For information about how to identify the required application-specific files, see the relevant application document.
- **Docker Runtime Options**: Enter the docker runtime options required by the application.

Step 7 In the **Summary** window, review the application configuration settings.

Step 8 (Optional) Click **Configuration Preview** to view the configuration template used to push the configuration settings on the selected devices.

Step 9 Click **Provision**.

Step 10 In the confirmation window, click **Yes** to complete the application installation on the selected devices.

Note The installation of the application also modifies the Cisco IOS-XE configuration on the device. This change in the running configuration must be copied to the startup configuration to ensure applications function as expected after a router reload. After the application installation is complete, use the **Template Hub** to copy the running configuration to the startup configuration.

Uninstall an Application from a Cisco Catalyst 9300 Device

You can uninstall an application from a Cisco Catalyst 9300 Series switch.

Step 1 Click the menu icon (☰) and choose **Provision** > **Services** > **App Hosting for Switches**.

Step 2 Choose the application and click **Manage** to view the devices that use the application.

Step 3 Choose the devices that have the application that you want to uninstall.

Step 4 From the **Actions** drop-down list, choose **Uninstall App**.

Edit an Application Configuration in a Cisco Catalyst 9300 Device

You can edit an application configuration if the application requires a configuration to be up and running in a Cisco Catalyst 9300 Series switch.

Step 1 Click the menu icon (☰) and choose **Provision** > **Services** > **App Hosting for Switches**.

Step 2 Choose the application and click **Manage** to view the devices that use the application.

Step 3 Choose the device that has the application that you want to edit.

Step 4 From the **Actions** drop-down list, choose **Edit App Config**.

Delete an Application

You can delete an application from Cisco DNA Center.

Before you begin

You must uninstall the application from all devices that are using it. For more information, see Uninstall an Application from a Cisco Catalyst 9300 Device, on page 23.

Step 1 Click the menu icon (☰) and choose **Provision** > **Services** > **App Hosting for Switches**.

You can view the available hosted applications in the **App Hosting** window.

Step 2 Choose the application that you want to delete.

Step 3 Click **Delete Application**.

Step 4 In the confirmation dialog box, click **OK**.

The application is deleted only if it is not used by any of the devices managed by Cisco DNA Center.

Otherwise, an error message shows the number of devices that are using the application. Click **Cancel** in the confirmation dialog box and uninstall the application. For more information, see Uninstall an Application from a Cisco Catalyst 9300 Device, on page 23.

Download App Logs

You can download application logs from Cisco DNA Center.

Step 1 Click the menu icon (☰) and choose **Provision** > **Services** > **IoT Services**.

Step 2 Click **All Devices**.

You can view the list of devices that are capable of hosting applications.

Step 3 Click **App logs** to download the application logs from Cisco DNA Center.

Step 4 In the **App Logs** pop-up window, choose the application logs file that you want to download and click **Download**.

Download Device Tech Support Logs

You can download the device tech support logs from Cisco DNA Center for troubleshooting purposes.

Step 1 Click the menu icon (☰) and choose **Provision** > **Services** > **IoT Services**.

Step 2 Click **All Devices**.

A list of devices that are capable of hosting applications is displayed.

Step 3 Click **Tech Support logs** to download the device tech support logs.

Application Hosting on Cisco Catalyst 9100 Series Access Points

The following sections provide information about application hosting on Cisco Catalyst 9100 Series Access Points.

About Application Hosting on Cisco Catalyst Access Points

The move to virtual environments has prompted the need to build applications that are reusable, portable, and scalable. Application hosting gives administrators a platform for leveraging their own tools and utilities. An application, hosted on a network device, can serve a variety of purposes. This ranges from automation, configuration management monitoring, and integration with existing tool chains.

Application hosting lets you manage the lifecycle of third-party applications on devices managed by Cisco DNA Center. This release lets you bring in the third-party SES-imagotag IoT Connector application on Cisco Catalyst 9100 Series Access Points with Cisco IOS-XE software version 17.3 or later.

The SES-imagotag IoT Connector on Cisco Catalyst 9100 Series Access Points can handle all Electronic Shelf Label (ESL) communication.

Application Hosting Workflow to Install and Manage USB on Cisco Catalyst 9100 Series Access Points

Before you begin

To enable application hosting on a device, the following prerequisites must be completed:

- Enable NETCONF and set the port to 830 to discover Cisco Catalyst 9100 Series Access Points.
- Make sure that the Cisco Catalyst 9100 Series Access Points have direct IP reachability to Cisco DNA Center.
- Make sure that the Cisco Catalyst 9800 Series Wireless Controller is running Cisco IOS XE 17.3.x or later software.
- Make sure that the Cisco DNA Center appliance is running the latest Cisco DNA Center ISO.
- Make sure that the USB dongle is inserted in the AP. This is required for the SES-imagotag Connector application to run.

Step 1 Check the readiness of the Cisco Catalyst 9800 Series Wireless Controller and Cisco Catalyst 9100 Series Access Points to host the application before you install it.

For more information, see View Device Readiness to Host an Application, on page 19.

Step 2 Install the Application Hosting service on Cisco DNA Center.

For more information, see Install or Update the Application Hosting Service Package, on page 17.

Step 3 Add the Cisco Catalyst 9800 Series Wireless Controller to Cisco DNA Center.

For more information, see Add a Network Device.

Note Make sure that you enable NETCONF and set the port to 830.

You must wait for the Cisco Catalyst 9800 Series Wireless Controller to move to a Managed state.

Step 4 Assign APs to a floor on the Network Hierarchy window.

For more information, see Work with APs on a Floor Map.

Step 5 Upload the USB application (the SES-imagotag Connector) to Cisco DNA Center.

For more information, see Add an Application, on page 19.

Step 6 Enable the IoT services.

For more information, see Enable IoT Services on Cisco Catalyst 9100 Series Access Points.

Step 7 Configure the container as described in the Application Hosting on Catalyst APs Deployment Guide.

View Installed Hosting Applications on Cisco Catalyst 9100 Series Access Points

Before you begin

Make sure the prerequisites have been met. For more information, see Prerequisites for Application Hosting.

Step 1 Click the menu icon (☰) and choose **Provision** > **Services** > **IoT Services**.

Step 2 To view all devices, click **All Devices** at the top-right corner, or to view only the devices that use a particular application, choose the application and click **Manage**.

If you chose to view all devices, the **All Devices** page shows the following information about the devices that are capable of hosting applications: **Hostname**, **IP Address**, **Image Version**, **App Hosting Status**, and **Last Updated**.

Note When the **App Hosting Status** of an AP is **Ready**, to configure the updates on the AP, check the check box next to the required hostname and click **Resync**.

If you chose to view a list of devices for a particular application, the **Devices** page shows the following information about the devices that are capable of hosting applications: **Hostname**, **Device IP**, **App Version**, **App Status**, **Last Heard,** **Platform Version**, and **Action Status**.

Step 3 In the **Devices** page, click **Summary** to view the summary of failed, stopped, and running applications on a device.

Step 4 Click the **Action** drop-down list to start, stop, edit, upgrade, and uninstall an application.

Step 5 Click the device link in which you want to view the installed hosting applications.

The **Applications** page shows the **Name**, **Version**, **App Status**, **IP Address**, **Health**, and **Details** of the installed applications.

Step 6 In the **Details** column, click **View** to get more information about an application status on the device.

App details window shows the **REOURCES** and **NETWORK** information of an application.

Step 7 To download the application log, select an application for which you want to download the application log and click **Application Logs**.

Step 8 To download the tech support log, select an application for which you want to download the tech support log and click **Tech Support Logs**.

Uninstall an Application from a Cisco Catalyst 9100 Device

You can uninstall an application from a Cisco Catalyst 9100 Series AP.

Step 1 Click the menu icon (☰) and choose **Provision** > **Services** > **IoT Services**.

Step 2 Choose the application and click **Manage** to view the devices that use it.

Step 3 Choose the devices that have the application that you want to uninstall.

Step 4 From the **Actions** drop-down list, choose **Uninstall App**.

Delete an Application from a Cisco Catalyst 9100 Device

You can delete an application from a Cisco Catalyst 9100 Series AP.

Before you begin

You must uninstall the application from all devices that are using it. For more information, see Uninstall an Application from a Cisco Catalyst 9100 Device.

Step 1 Click the menu icon (☰) and choose **Provision** > **Services** > **IoT Services**.

You can view the available hosted applications in the **IoT Services** page.

Step 2 Choose the application that you want to delete.

Step 3 Click **Delete Application**.

Step 4 In the confirmation dialog box, click **OK**.

The application is deleted only if it is not used by any of the devices managed by Cisco DNA Center.

Otherwise, an error message shows the number of devices using the application. Click **Cancel** and uninstall the application. For more information, see Uninstall an Application from a Cisco Catalyst 9100 Device.

Configure a Site-to-Site VPN

You can create a site-to-site VPN and edit or delete existing site-to-site VPNs.

Create a Site-to-Site VPN

This procedure shows how to create a site-to-site VPN.

Before you begin

- Define the sites within the network hierarchy. See Network Hierarchy Overview.
- Configure IP address pools to be used for the VPN tunnels. The IP address pools must have a minimum of six free IP addresses. See Configure IP Address Pools.

Step 1 Click the menu icon (☰) and choose **Provision** > **Site to Site VPN**.

Alternatively, you can create a site-to-site VPN from the **Workflows** > **Site to Site VPN** window.

Step 2 To create a VPN, click **Add**.

The **Choose Your Sites** workflow is displayed.

Step 3 In the **Choose Your Sites** workflow, do the following:

a) Enter a VPN name in the first field.
b) Select the first site, a device in that site, and a WAN interface on that device from the Site 1 drop-down lists. The WAN interface is set by default if the device is provisioned.
c) Select the second site, a device in that site, and a WAN interface on that device from the Site 2 drop-down lists. The WAN interface is set by default if the device is provisioned.

Step 4 In the **Select Networks** window, do the following:

a) From the **Tunnel IP Pool** drop-down list, choose an IP address pool.
b) Check the boxes next to the subnets that you want to use for each site.
c) (Optional) If you want to add a custom network for a site, click the **Add Custom Networks** link at the bottom and complete the required fields.

Step 5 In the **Configure VPN** window, do the following:

a) Enter a preshared key for encryption.
b) Set the encryption and integrity algorithms as desired. We recommend that you use the default settings. If you change any settings, you can go back to the default choices by checking the **Use Cisco recommended IKEV2 & Transform Set Values** check box.

Step 6 In the **Summary** window, review the VPN settings. To make any changes, click **Edit**.

Step 7 To proceed, click **Create VPN**.

In the status screen that follows, a check mark is shown next to each step as it is completed. Click **Services** to return to the **Site to Site VPN** window, which shows the newly created VPN.

Edit a Site-to-Site VPN

Step 1 Click the menu icon (☰) and choose **Provision** > **Site to Site VPN**.

Step 2 Check the check box next to the VPN that you want to edit.

Step 3 Click **Edit** in the menu bar above the list.

Step 4 In the **Summary** window, review the VPN settings. To make any changes, click **Edit**.

Step 5 Click **Edit VPN** to submit the changes.

In the status screen that follows, a check mark is shown next to each step as it is completed. Click **Services** to return to the **Site to Site VPN** screen.

Delete a Site-to-Site VPN

Step 1 Click the menu icon (☰) and choose **Provision** > **Site to Site VPN**.

Step 2 Check the check box next to the VPN that you want to delete.

Step 3 Click **Delete** in the menu bar above the list.

A confirmation dialog box is displayed.

Step 4 Click **Yes** to confirm that you want to delete the VPN.

Create a User-Defined Network Service

Cisco DNA Center allows you to configure **Cisco User Defined Network** services from **Provision** > **Service Catalog** > **Cisco User Defined Network** page. Alternatively, you can create **Cisco User Defined Network** service from **Workflows** > **Configure Cisco UDN** page. For more information, see Configure Cisco User Defined Network.

View the User-Defined Network Service Provisioning Status

This procedure shows you how to view the Cisco User-Defined Network service provisioning status from the **Provision** > **All Services** window. You can also click the **View Provisioning Status** button in the **Configure Cisco User Defined Network** screen after configuring a Cisco User-Defined Network successfully.

Before you begin

Configure and provision the Cisco User-Defined Network service from the **Workflows** > **Configure Cisco User Defined Network** window.

Step 1 Click the menu icon (☰) and choose **Provision** > **All Services** > **Cisco User Defined Network**.

The **Site Provisioning Status** window displays the site name, device name, number of SSIDs used, and status of site provisioning.

Step 2 Click **Refresh** to see the latest provisioning status.

Step 3 Click the site name to view additional details for the provisioned device, such as SSID name, User-Defined Network (UDN) status, and Unicast Traffic Containment.

Step 4 Click **Activities** to track the scheduled task status in the **Scheduled Tasks** window.

Enable Telemetry on Switches

You can configure Switch Port Analyzer (SPAN) and Encapsulated Remote Switch Port Analyzer (ERSPAN) sessions on switches to share IP traffic for application assurance and endpoint analytics.

Before you begin

Confirm that the switches and the Traffic Telemetry Appliance (TTA) are reachable and managed through Cisco DNA Center. The switches must be assigned to a site and the **Distribution** device role.

Step 1 Click the menu icon (☰) and choose **Provision** > **Service Catalog** > **Telemetry Appliance Setup**.

Step 2 Click **+ Setup** to create a new workflow.

Step 3 In the **Get Started** window, enter a workflow name and a description.

Step 4 In the **Choose Source Endpoint** window, choose a device to source traffic to a telemetry appliance.

Note Switches and hubs are the supported source devices for your workflow that is managed with the Distribution role.

Step 5 In the **Choose Destination Endpoint** window, choose the TTA device as the destination endpoint.

Note You can choose only one TTA device from the list.

Step 6 In the **Choose Type for Configuration** window, choose **SPAN** or **ERSPAN**.

Step 7 In the **Choose Mapping Between Source and Destination** window, do the following:

For SPAN:

a. Choose the source interface on which to monitor incoming traffic.

b. Choose the destination interface on the switch where the traffic telemetry appliance is connected and traffic can be forwarded.

c. Choose the receiver interface to process the incoming traffic for analytics.

For ERSPAN:

a. Choose the source interface on which to monitor incoming traffic.

b. Enter the VLAN to filter the incoming traffic.

c. Choose the receiver interface to process the incoming traffic for analytics.

d. Enter the destination IP address for the receiver interface.

e. Enter the destination netmask for the receiver interface.

Step 8 In the **Scheduler** window, click **Now** or **Later** to indicate when you want to start the configuration.

Step 9 In the **Summary** window, review the configuration settings. To make any changes, click **Edit**.

Step 10 To proceed, click **Deploy**.

Step 11 Click **View Status** to view the provisioning status of the individual devices.

Configure Cisco Umbrella

The following sections provide information about integrating Cisco Umbrella with Cisco DNA Center.

About Cisco Umbrella

The DNS-layer security in Cisco Umbrella provides the fastest and easiest way to improve your network security. It helps improve security visibility, detect compromised systems, and protect your users on and off the network by stopping threats over any port or protocol before they reach your network or endpoints.

Cisco DNA Center supports Cisco Umbrella configuration on the following devices:

- Cisco Catalyst 9800 Series Wireless Controllers with Cisco IOS-XE software version 16.12 or later

- Cisco Catalyst 9100 Series APs
- Cisco Catalyst 9200 Access Switch with Cisco IOS-XE software version 17.3.1 or later
- Cisco Catalyst 9300 Access Switch with Cisco IOS-XE software version 17.3.1 or later

Role-Based Access Control Settings for Cisco Umbrella

To configure Cisco Umbrella with Cisco DNA Center and to provision Cisco Umbrella on network devices, you must create a user role with the necessary RBAC permission for Cisco Umbrella. For more information, see "Manage Users" in the Cisco DNA Center Administrator Guide.

Table 3: RBAC Permission Matrix for Cisco Umbrella

Function	Access	Permission
Configure Cisco Umbrella with Cisco DNA Center	Network Design > Advanced Network Settings	Write
Add Umbrella dashlet in System 360	Network Design > Advanced Network Settings	Write
Provision Cisco Umbrella on network devices	Network Provision > Provision	Write
	Network Design > Network Hierarchy	Read
	Network Provision > Inventory Management	Read
	System	Read
	Network Provision > Scheduler	Write
	Network Services > Umbrella	Write

Configure Cisco Umbrella with Cisco DNA Center

Before you begin

- Create a Cisco Umbrella account.
- Log in to *login.umbrella.com* and create the necessary keys, such as the API key, legacy token, management key, and secret.
- Note down the organization ID from the Cisco Umbrella login URL.
- Create the local bypass domains in Cisco Umbrella.
- If Cisco DNA Center has a proxy server configured as an intermediary between itself and the network devices it manages or the Cisco cloud from which it downloads software updates, you must configure access to the proxy server. For more information, see the Configure the Proxy section in the Cisco DNA Center Administrator Guide.

- Install the Cisco Umbrella package in Cisco DNA Center. See the Download and Install Packages and Updates section in the Cisco DNA Center Administrator Guide.
- Create a user role with necessary RBAC permission for Cisco Umbrella. See Role-Based Access Control Settings for Cisco Umbrella, on page 31.

Note You cannot install Cisco Umbrella package on a Cisco DNA Center cluster configured with IPv6.

Step 1 Click the menu icon (☰) and choose **System** > **Settings** > **External Services** > **Umbrella**.

Step 2 Enter the following details that you retrieved manually from Cisco Umbrella:

- **Organization ID**
- **Network Device Registration API Key**
- **Network Device Registration Secret**
- **Management API Key**
- **Management Secret**
- **Legacy Device Registration Token**

Step 3 Click **Save**.

Add the Umbrella Dashlet

You can add the **Umbrella** dashlet in the **System 360** page. The **Umbrella** dashlet shows the configuration status of Cisco Umbrella with Cisco DNA Center.

Before you begin

You must install the Cisco Umbrella package.

Step 1 Click the menu icon (☰) and choose **System** > **System 360**.

Step 2 From the **Actions** menu, choose **Edit Dashboard** and click **Add Dashlet**.

Step 3 Choose **Umbrella Dashlet** and click **Add**.

The **Umbrella** dashlet appears under **Externally Connected Systems** in the **System 360** page. The **Umbrella** dashlet shows the status as **Available** and displays the organization ID, if Cisco Umbrella is configured with Cisco DNA Center.

If Cisco Umbrella is not configured with Cisco DNA Center, you can click the **Configure** link and complete the fields in **System** > **Settings** > **External Services** > **Umbrella**. See Configure Cisco Umbrella with Cisco DNA Center, on page 31.

If the keys are changed in Cisco Umbrella, you can click the **Update** link and update the keys in **System** > **Settings** > **External Services** > **Umbrella**. See Configure Cisco Umbrella with Cisco DNA Center, on page 31.

View the Umbrella Service Statistics Dashboard

Click the menu icon (≡) and choose **Provision** > **Services** > **Umbrella** to view the **Umbrella Service Stats** dashboard.

The dashboard displays the following dashlets:

- **Total Umbrella DNS Queries**: Shows the number of blocked DNS queries and allowed DNS queries for the selected site.
- **Blocked Umbrella DNS Queries**: Shows the number of DNS queries blocked by security policy and content policy for the selected site.

By default, the dashlet shows statistics for the last 3 hours. You can view statistics for the last 24 hours or 7 days by choosing the required time from the drop-down list in the top-left corner of the **Umbrella Service Stats** page.

Prerequisites for Provisioning Cisco Umbrella on Network Devices

Before provisioning Cisco Umbrella on network devices, ensure that:

- Cisco Umbrella is configured with Cisco DNA Center.
- Wireless provisioning is complete for the devices on which you want to provision Cisco Umbrella.
- The SSID configuration is nonfabric.
- The AP is provisioned, if the device is configured with a nonfabric SSID in FlexConnect mode.
- The device has direct internet access to establish connection with Cisco Umbrella.
- The Cisco Umbrella root certificate is available in the Cisco DNA Center trustpool. See Configure Trustpool in the Cisco DNA Center Administrator Guide.
- If the device has a Cisco Umbrella configuration that is not set from Cisco DNA Center, remove the Cisco Umbrella configuration from the device and resync the device with Cisco DNA Center.

Provision Cisco Umbrella on Network Devices

Before you begin

Make sure the prerequisites have been met. For information, see Prerequisites for Provisioning Cisco Umbrella on Network Devices, on page 33.

Note Cisco umbrella deployment on your organization's network can be monitored only from *login.umbrella.com*.

Step 1 Click the menu icon (☰) and choose **Workflows** > **Umbrella Deployment**.

Alternatively, do the following:

- Click the menu icon (☰) and choose **Provision** > **Umbrella**.
- Choose a site from the network hierarchy for which you want to deploy Cisco Umbrella.
- The **Select Devices** window appears. Go to Step 4 to continue the deployment workflow.

Step 2 If a task overview window appears, click **Let's Start** to go directly to the workflow.

Step 3 The **Choose Site** window appears.

a) You can view the device readiness status in each site, as follows:

- **Eligible Devices**: Devices that are eligible for Cisco Umbrella configuration. See Prerequisites for Provisioning Cisco Umbrella on Network Devices, on page 33.
- **Enabled Devices**: Devices that are already configured from Cisco DNA Center.

b) Choose a site to deploy and click **Next**.

Note You can choose only one site at a time. If you choose a parent site, Cisco Umbrella can be deployed on all child sites at the same time.

Step 4 In the **Select Device Type** window, choose **Switches** or **Wireless Controllers**.

Step 5 If you have chosen **Switches** in the **Select Device Type** window, do the following:

a) In the **Select Devices** window, choose the wired device.

b) In the **Configure Interface** window, do the following:

1. Choose the ports you want to configure and click **Define Umbrella Interfaces**.
2. In the **Select Configuration** dialog box, click the **Define Umbrella Interfaces** drop-down list and choose **IN(LAN)**, **OUT(WAN)** or **Disable Umbrella** and click **Save**.

Note You must choose at lease one **IN** and one **OUT** interface to proceed further.

c) In the **Define Umbrella Policy Mapping (Wired)** window, choose Umbrella policies at a global or interface level.

d) In the **Configure Policies for Your Devices** window, choose the **IN(LAN)** interface and click **Define Umbrella Policies**.

e) In the **Select Policy** dialog box, choose the policy for the selected interfaces and click **Save**.

Step 6 If you have chosen **Wireless Controllers** in the **Select Device Type** window, do the following:

a) In the **Select Devices** window, choose the wireless device.

b) Choose the SSIDs and select the required Cisco Umbrella policy for each SSID.

Note

- Only nonfabric SSIDs are listed on this page.
- If you choose an SSID and don't select the Cisco Umbrella policy, the default policy is mapped with the SSID.
- If you choose multiple policies, the order of enforcement of policies is defined in the Cisco Umbrella cloud portal.

c) In the **Umbrella Policy Association (Wireless)** window, view the default policies applied to the SSIDs.

If you want to change the policies associated with the SSIDs, click the **Cisco Umbrella** link. In the Cisco Umbrella console, you can see the network identity after you have completed the deployment of Cisco Umbrella from Cisco DNA Center. For devices with Cisco IOS-XE software version 16.xx, the network identity is shown as global. For devices with a Cisco IOS-XE software version later than 16.xx, the network identity is shown as a custom name created based on the site and SSID name.

Step 7 In the **Review Internal Domains** window, add or delete the list of internal domains. The DNS queries that match a domain in the **Internal Domain** list are forwarded to the local DNS server instead of Cisco Umbrella.

Step 8 The **DNS Crypt** window appears. The **Enable DNS Packet Encryption** option is selected by default.

a) In the **DNS Crypt** window, click **Next**.

b) If you don't want DNS packet encryption, uncheck the **Enable DNS Packet Encryption** check box.

Step 9 In the **Summary** window, review the details. To make any changes, click **Edit**.

Step 10 To proceed, click **Deploy**.

Step 11 In the **Schedule** window, choose whether you want to deploy the configuration now or schedule it later.

Step 12 To proceed, click **Apply**.

Step 13 In the **Deployment** window, click **View Status** to view the deployment status in the **Scheduled Tasks** window.

You can view the Cisco Umbrella deployment status of the device and the device configuration status in Cisco Umbrella. You can also view the Cisco Umbrella deployment logs in the **Audit Logs** window.

Disable Cisco Umbrella on Network Devices

Step 1 Click the menu icon (☰) and choose **Workflows** > **Umbrella Deployment**.

Alternately, do the following:

- Click the menu icon (☰) and choose **Provision** > **Services** > **Umbrella**.
- Choose a site from the network hierarchy from which you want to disable Cisco Umbrella.
- The **Select Devices** window appears. Go to Step 4 to continue the disable workflow.

Step 2 If a task overview window appears, click **Let's Start** to go directly to the workflow.

Step 3 The **Choose Site** window appears.

a) You can view the device readiness status in each site, as follows:

- **Ready Devices**: Devices that meet the prerequisites for Cisco Umbrella configuration. See Prerequisites for Provisioning Cisco Umbrella on Network Devices, on page 33.
- **Not Ready Devices**: Devices that do not meet the prerequisites.
- **Enabled Devices**: Devices that are already configured from Cisco DNA Center.

b) Choose the site that you want to disable, and click **Next**.

Note You can choose only one site at a time. If you choose a parent site, Cisco Umbrella is disabled on all the child sites at the same time.

Step 4 In the **Select Device Type** window, choose **Switches** or **Wireless Controllers**.

Step 5 In the **Select Devices** window, click the **Enabled** tab and choose the devices.

Step 6 Click the **Disable** radio button and choose the devices.

Step 7 In the **Summary** window, review the details. To make any changes, click **Edit**.

Step 8 To proceed, click **Deploy**.

Step 9 In the **Schedule** window, choose whether you want to deploy the configuration now or schedule it later.

Step 10 To proceed, click **Apply**.

Step 11 In the Deployment window, click **View Status** to view the deployment status in the **Scheduled Tasks** window.

You can view the Cisco Umbrella deployment logs in the **Audit Logs** window.

Update the Cisco Umbrella Configuration on Network Devices

Step 1 Click the menu icon (☰) and choose **Workflows** > **Umbrella Deployment**.

Alternately, do the following:

- Click the menu icon (☰) and choose **Provision** > **Services** > **Umbrella**.
- Choose a site from the network hierarchy for which you want to update the Cisco Umbrella configuration.
- The **Select Devices** window appears. Go to Step 4 to continue the update workflow.

Step 2 If a task overview window appears, click **Let's Start** to go directly to the workflow.

Step 3 The **Choose Site** window appears.

a) You can view the device readiness status in each site, as follows:

- **Ready Devices**: Devices that meet the prerequisites for Cisco Umbrella configuration. See Prerequisites for Provisioning Cisco Umbrella on Network Devices, on page 33.
- **Not Ready Devices**: Devices that do not meet the prerequisites.
- **Enabled Devices**: Devices that are already configured from Cisco DNA Center.

b) Choose the site that you want to update and click **Next**.

Note You can choose only one site at a time. If you choose a parent site, Cisco Umbrella is updated on all child sites at the same time.

Step 4 In the **Select Device Type** window, choose **Switches** or **Wireless Controllers**.

Step 5 If you have chosen **Switches** in the **Select Device Type** window, do the following:

a) In the **Select Devices** window, choose the wired device and click the **Update** radio button.

b) In the **Configure Interface** window, do the following:

1. Choose the ports and click **Define Umbrella Interfaces**.
2. In the **Select Configuration** dialog box, click the **Define Umbrella Interfaces** drop-down list and choose **IN(LAN)**, **OUT(WAN)** or **Disable Umbrella** and click **Save**.

Note You must choose at lease one **IN** and one **OUT** interface to proceed further.

c) In the **Define Umbrella Policy Mapping (Wired)** window, choose Umbrella policies at a global or interface level and click **Next**.
d) In the **Configure Policies for Your Devices** window, choose the **IN(LAN)** interface and click **Define Umbrella Policies**.
e) In the **Select Policy** dialog box, choose the policy for the selected interfaces and click **Save**.

Step 6 If you have chosen **Wireless Controllers** in the **Select Device Type** window, do the following:
a) In the **Select Devices** window, choose the wireless device and click the **Update** radio button.
b) In the **Define Umbrella Policy Map (Wireless)** window, choose the SSIDs and select the desired Cisco Umbrella policies to map, or unselect SSIDs to disable Cisco Umbrella.

Step 7 In the **Review Internal Domains** window, add or delete the list of internal domains. The DNS queries that match a domain in the **Internal Domain** list are forwarded to the local DNS server instead of Cisco Umbrella.

Step 8 The DNS Crypt window appears. The **Enable DNS Packet Encryption** option is selected by default.

If you don't want DNS packet encryption, uncheck the **Enable DNS Packet Encryption** check box.

Step 9 In the **Summary** window, review the details. To make any changes, click **Edit**.

Step 10 To proceed, click **Deploy**.

Step 11 In the **Schedule** window, choose whether you want to deploy the configuration now or schedule it later.

Step 12 To proceed, click **Apply**.

Step 13 In the Deployment window, click **View Status** to view the deployment status in the **Scheduled Tasks** window.

You can view the Cisco Umbrella deployment logs in the **Audit Logs** window.

Create Secure Tunnel

Cisco DNA Center allows the user to plan and deploy VPN Tunnels, which establishes secure connection between enterprise and branch location.

Note This feature is currently supported only on the Cisco Catalyst 9300X Series Switches.

Configure Secure Tunnel

You can use this procedure to plan and deploy secure tunnels on day *n*.

Step 1 Click the menu icon (☰) and choose **Provision** > **Secure Tunnels**.

Alternatively, you can create a secure tunnel from the **Workflows** > **Create Secure Tunnel** window.

Step 2 In the **Secure Tunnel** window, click **Create Secure Tunnel**.

Step 3 If the task overview window opens, click **Let's Do it** to go directly to the workflow.

Step 4 In the **Select Tunnel Type** window, choose the type of secure tunnel to create by clicking the **Site To Secure Access Service Edge (SIG/SASE)** tile.

This action creates a secure tunnel between the Cisco Catalyst 9300X Series switch and the Secure Internet Gateway.

Step 5 In the **Select Secure Internet Gateway** window, click the drop-down list to choose the **Secure Internet Gateway**.

Do one of the following for the chosen Secure Internet Gateway:

- **Umbrella**: Ensure that you created a tunnel in Cisco Umbrella. You will need the tunnel ID and preshared key in the subsequent steps. For more information, see Configure Cisco Umbrella with Cisco DNA Center, on page 31. If the tunnel is created in the Cisco Umbrella portal, check the confirmation check box.
- **Zscaler**: Ensure that the tunnel is already created on the Zscaler portal. After you create the tunnel in Zscaler, the preshared key and the FQDN defined there are required to configure the tunnel parameters on the selected Cisco Catalyst 9300X Series switch. If the tunnel is created in the Zscaler portal, check the confirmation check box.

Step 6 In the **Choose Site and Device** window, do the following for site and tunnel mapping:

a. Choose the **Site** from the drop-down list.

b. Choose the **Device** from the drop-down list.

c. Choose the **Number of Tunnels** to create from the drop-down list.

d. For Zscaler, choose the **Tunnel Type** from the drop-down list.

e. Enter the **Tunnel Name**.

f. Choose the **Tunnel Source Interface**.

g. Check the check box if you want to use the same interface for the tunnel IP. If you do not want to use the same interface, uncheck the check box and choose the **Interface**.

h. Enter the **Data Center Location**.

Step 7 In **Define Tunnel Settings** window, do the following:

a. For Umbrella, enter the **Pre-Shared Key (PSK)** for authentication.

b. If the Secure Internet Gateway integration is not complete, do the following:

1. Enter the **Tunnel ID** and choose one of the following:
   a. **Fully Qualified Domain Name (FQDN)**: Use the **Tunnel ID** generated in Cisco Umbrella or the **User ID** generated in Zscaler.
   b. **IP Address**: Use the IP address to which you want to connect.

c. Check the check box to use the Cisco-recommended settings. To customize the values, uncheck the check box.

Step 8 In the **Configure Tunnel Traffic** window, choose from the following options to route the traffic:

- **Send all traffic**: To send all traffic through the IPsec tunnel to Umbrella.
- **Send Selected Traffic**: Enter the subnet and ingress interface for the subnet. You can add more subnets by clicking  .

Step 9 In the **Schedule Task** window, choose whether you want to create the tunnel now or schedule it for later. Also, you can choose to **Generate CLI Preview**.

Step 10 In the **Summary** window, review the configuration settings. To make any changes, click **Edit**.

Step 11 Click **Create Secure Tunnel**.

The **Done!** window appears.

Step 12 Click the **View all Tunnels** tab to view the status of the tunnel creation.

This process might take some time. Click **Refresh**. When the tunnel is up, the status changes from Provision to Up.