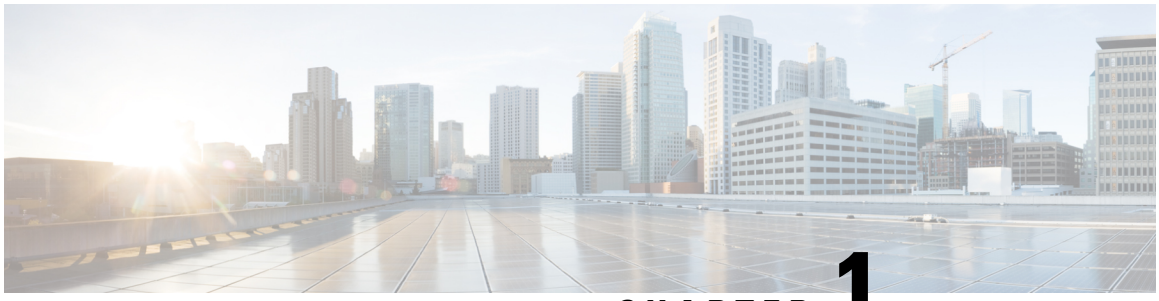
Cisco Catalyst SD-WAN Solution Overview

First Published: 2026-06-22

Last Modified: 2026-07-06

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Solution Overview

Overview

Cisco Catalyst SD-WAN is a secure, policy-driven software-defined WAN solution that

- helps enterprises connect users, branches, data centers, clouds, and SaaS applications over any transport,
- centralizes management,
- improves application experience,
- simplifies network operations,
- integrates security across the network, and
- integrates seamlessly with a variety of Cisco enterprise solutions.

Legacy Network Design

Describes legacy network design to compare with the Catalyst SD-WAN solution.

Legacy network design cannot scale to meet today's needs for these fundamental reasons:

- Lengthy installation times: Legacy networks that run on dedicated carrier circuits depend on the carrier to install new circuits, which can take several months. This can dramatically delay the launch of new branch locations.
- Routing complexity: Legacy networks operate on the model of a distributed control plane, which means that every node in the network must be configured with routing and security rules.

There's no separation between a control plane and a data plane. There's no separation between the hosts, devices, and servers on the service side of the network and the interconnects between routers on the transport side of the network.

Policy and control decisions are embedded at every hop across the enterprise network.

Security is time-intensive, requiring implementation of security policy either at every node in the network or by using centralized security servers to manage group keys.

- Maintenance complexity: Remote site management, change control, and network maintenance represent major logistical challenges.

Requirements of a multi-site enterprise

For the complex needs of a multi-site enterprise, legacy network design struggles to meet requirements such as

- Rigorous end-to-end security
- Disparate transport networks
- High-bandwidth cloud applications that are hosted in multiple data centers
- Ongoing increase in the number of mobile end users
- Any-to-any connectivity over fluid topologies

Cisco Catalyst SD-WAN Solution

Instead of treating each WAN circuit and router as a separate device-by-device configuration problem, Cisco Catalyst SD-WAN separates the control plane, management plane, and data plane.

Components of the Catalyst SD-WAN fabric

Cisco Catalyst SD-WAN employs three components, called SD-WAN Control Components, to manage the fabric.

- Cisco Catalyst SD-WAN Manager is the centralized management system. It provides dashboards for operational visibility across the Catalyst SD-WAN fabric, tools for provisioning and configuring devices, license management, tools for upgrading device software, and more. SD-WAN Manager communicates with devices and SD-WAN Controllers over secure connections.
- Cisco Catalyst SD-WAN Controllers manage the control plane of the overlay. They form secure control connections with edge routers, use the Overlay Management Protocol (OMP) to exchange routes, next hops, keys, and policy information, and distribute reachability information to the edge routers.
- Cisco Catalyst SD-WAN Validator coordinates initial device onboarding. It authenticates devices, helps edge routers and SD-WAN Controllers find each other, and so on.

In addition to the SD-WAN Control Components, the fabric includes the data plane edge devices at branches, campuses, data centers, cloud environments, and other sites. They create secure IPsec tunnels, forward traffic, run routing protocols such as OSPF and BGP on the service side, support configured routing policy, and more.

Underlay and overlay networks

- Underlay network: The set of transport-layer network connections between an organization's edge devices, across multiple locations, even distant geographies. The connections may include a mix of various transport types, such as the public internet, MPLS, broadband, LTE, and cloud connectivity.

  In this context, the underlay network is sometimes called the physical transports, but this is a shorthand, and does not imply that the underlay only includes layer 1, the physical layer, in the open systems interconnection (OSI) model.

- Overlay network: This virtual IP fabric created by Catalyst SD-WAN consists of a set of transport-layer tunnels, generally IPsec or GRE, managed by SD-WAN Controllers. It is a level of abstraction above the underlay network. In some scenarios, you can partition a network's underlay network into more than one overlay network, each optimized to meet diverse needs with distinct policies.

- Fabric: In the context of Catalyst SD-WAN, the overlay network mesh of connections between nodes, is often simply called the fabric. The nodes in this mesh include routers and SD-WAN Control Components.

While the terms overlay and fabric are often interchangeable, overlay is useful when specifically distinguishing between the physical and virtual layers. The overlay is the virtual layer managed by SD-WAN Controllers, while the underlay is the layer of transports.

Transport side and service side

Cisco Catalyst SD-WAN employs a distinction, not exclusive to this solution, between:

- Transport side: WAN-facing network, using the underlay transports tunnels between edge routers. The connections to edge routers use the Catalyst SD-WAN concept of transport locators (TLOCs), which are identifiers used for a connection between an edge device and a transport. The connections serve the control plane and the data plane, and use VPN 0, also called the transport VPN.

- Service side: Connections between edge routers and end users, which may involve intermediate devices as well. Service side connection use the VPN range 1 to 65527.

This distinction allows network administrators to create policy, such as security policy, that affects only the transport side.

How it works

How Catalyst SD-WAN creates a fabric, manages routes, and allows traffic to flow.

Cisco Catalyst SD-WAN builds an encrypted overlay across the underlay transports the organization uses, such as Multiprotocol Label Switching (MPLS), broadband internet, cellular, or cloud connectivity. The overlay abstracts transport details so that you can create policies in terms of business intent: which applications matter, which users or sites can communicate, which paths meet performance requirements, and so on.

- The control plane is centralized through SD-WAN Controllers.

- Edge routers advertise local routes to SD-WAN Controllers.

- SD-WAN Controllers provide reachability and policy information to the edges.

Application traffic flows directly between edge routers, according to configured policy. This gives the network centralized policy control without forcing every data flow through a central device.

Network planes in Cisco Catalyst SD-WAN

How the network planes of the Cisco Catalyst SD-WAN fabric operate.

The components of the Cisco Catalyst SD-WAN fabric can be described as operating in two planes:

- Data plane
- Control plane

Some discussions Catalyst SD-WAN further divide the control plane into a management plane mostly relating to SD-WAN Manager operations, and an orchestration plane for SD-WAN Validator operations that relate to onboarding devices into the fabric.

Data plane

In a Catalyst SD-WAN fabric, the data plane is the part that carries user traffic.

In practical terms, it is made up of the WAN edge devices and virtual edge routers such as Catalyst 8000V. These devices sit at branches, campuses, data centers, colocation sites, or cloud environments, and forward application packets between sites.

Relationship with the control plane

SD-WAN Controllers distribute routing and policy information, but do not carry the user traffic. The edge devices in the fabric learn the routes, policies, and security information from the control plane and build direct data plane connections to other edge devices. In short, the control plane manages the routing rules, while the data plane transports the traffic.

Data plane capabilities

Most data plane connections are secured with IPsec tunnels, but GRE is also supported. The tunnels form the secure SD-WAN overlay across whatever underlay transport is available.

The data plane enforces network segmentation, implemented with the Virtual Routing and Forwarding (VRF) technology, operationally equivalent to VPNs. This allows different business groups or traffic classes to remain isolated even while sharing the same Catalyst SD-WAN fabric and physical transports.

In addition, the data plane enforces routing policies, such as for QoS, application-aware routing, and so on.

Connection health

Bidirectional Forwarding Detection (BFD) is a protocol that monitors the health of the paths between devices, detecting failures so that Catalyst SD-WAN can respond quickly.

Catalyst SD-WAN uses BFD in data plane tunnels to measure path health, including reachability, packet loss, jitter, and delay. Edge devices use the measurements, together with configured policy, to choose the best paths for applications.

Control plane

In a Catalyst SD-WAN fabric, the control plane is the part that carries user traffic tells the WAN edge devices how to build the overlay and how to route traffic.

The main component of the control plane is the SD-WAN Controller, formerly called vSmart. SD-WAN Controllers exchange routing, policy, topology, and security information with WAN edge devices. In essence, they manage the rules, while the data plane carries the application traffic.

Overlay Management Protocol

For the control plane, the key protocol is the Overlay Management Protocol (OMP). OMP operates between SD-WAN Controllers and edge devices over secure control connections. It distributes overlay reachability, routes, transport locator (TLOC) information, policy updates, and encryption key information.

SD-WAN Controllers

Edge devices advertise their routing information to SD-WAN Controllers. The SD-WAN Controllers apply centralized policy, then advertise the appropriate routes and instructions back to other edge devices. This is how Catalyst SD-WAN can create different topologies, such as hub-and-spoke, full mesh, or per-VPN segment-specific designs, without manually configuring every edge-to-edge relationship.

Security

The control plane helps to secure the fabric. Edge devices generate encryption keys for each transport and send them to the SD-WAN Controllers. The SD-WAN Controllers distribute the keys to peers according to policy. This avoids traditional peer-by-peer internet key exchange (IKE) negotiation between every edge device pair, helping the fabric to scale efficiently.

In short, the control plane is the SD-WAN decision and distribution layer. It learns routes from WAN Edge routers, applies centralized policy, distributes routing and security information through OMP, helps build the overlay tunnels, and tells the data plane what paths are allowed or preferred, while never carrying the user data itself.

Multitenancy

Multitenancy is a Cisco Catalyst SD-WAN feature that supports multiple separate customers, business units, or organizations, called tenants, within a shared Catalyst SD-WAN infrastructure, while keeping their networks logically isolated.

The core idea is shared infrastructure, separate tenant experience. The value is reduced operational overhead. This can be important for small-scale organizations or business units that can benefit from Catalyst SD-WAN but don’t have the scale to warrant managing the entire infrastructure.

Deployment options

Cisco Catalyst SD-WAN deployment options are defined by where the SD-WAN Control Components are located, and who maintains them. Regardless of the deployment option, the edge devices of the fabric still operate at the branches, campuses, and data centers of the organization, and in the organization’s cloud infrastructures, if any.

Cisco cloud-hosted

Cisco builds, operates, and monitors the SD-WAN Control Components. This option reduces the operational burden on an organization because its network administrators can focus mainly on configuration and policy rather than infrastructure. With this deployment option, the organization handles fabric provisioning and maintenance through the Cisco Catalyst SD-WAN portal (formerly the Self Service Portal). The SD-WAN portal provides an easy to use interface for handling fabric operations.

Cisco cloud-hosted deployments include a range of options, depending on an organization's needs.

On-premises

Self-managed deployment options are more hands-on, and the organization has the responsibility to install and maintain the SD-WAN Control Components. Self-managed options give the most control, and also the most responsibility: deployment, operations, monitoring, maintenance, server capacity, and scaling.

For the on-prem option, an organization deploys the SD-WAN Control Components in its own data center. This can be preferred for regulated sectors such as government, finance, healthcare, and utilities.

Self-managed cloud-hosted

This self-managed deployment option is similar to an on-premises deployment, but the organization installs the SD-WAN Control Components in its own public-cloud environment, such as AWS or Azure. This avoids the cost of extra data center infrastructure and can make scaling easier than with an on-premises deployment.

Major features

This section describes some of the major features of Cisco Catalyst SD-WAN.

Centralized management and automation

Cisco SD-WAN Manager provides a single dashboard for configuration, monitoring, provisioning, software upgrades, and troubleshooting. Configuration groups enable configuring each edge device router centrally.

Transport independence

The SD-WAN overlay can use MPLS, broadband, public internet, cellular, and other IP transports. This lets organizations mix private and public connectivity while still applying consistent policy and security.

Secure overlay fabric

Catalyst SD-WAN authenticates devices, uses secure control connections, and automatically encrypts site-to-site traffic.

Segmentation

The fabric supports segmentation, enabling you to isolate different groups, applications, or business functions, without building separate physical networks.

Application-aware routing

Policies can control path selection for traffic, based on the source of each traffic flow. You can set routing policy based on the business relevance of each network application, such as giving priority to specific applications or traffic categories, and using cheaper or secondary links for low-priority traffic.

SaaS optimization

Cloud OnRamp for SaaS can dynamically select the best-performing path for specific SaaS applications.

Cloud services integration

Cloud OnRamp for Multicloud helps connect enterprise WANs to cloud services such as AWS, Azure, and Google Cloud.

Integrated security and SASE readiness

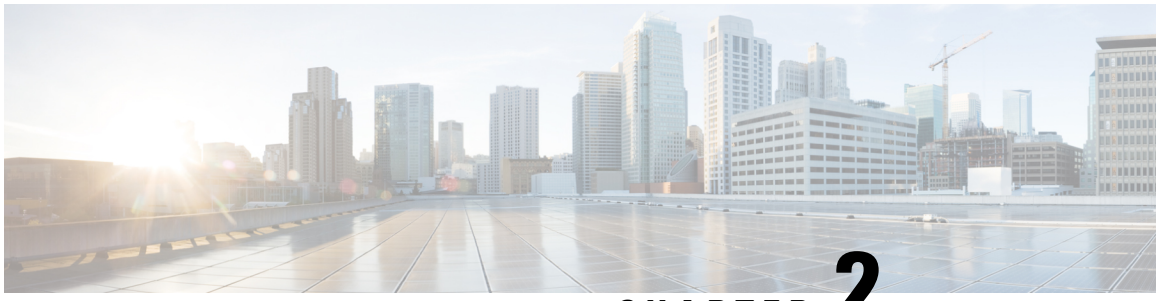
Catalyst SD-WAN supports on-premises and cloud-delivered security, including integration with Cisco Umbrella. Services include enterprise firewall features, secure web gateway, malware protection, intrusion prevention, URL filtering, DNS-layer protection, and more.

Cisco ThousandEyes

The integration of ThousandEyes brings end-to-end visibility into application delivery and network performance beyond the traditional enterprise network boundaries. Organizations can deploy ThousandEyes agents through SD-WAN Manager integration, and can quickly pinpoint the source of issues, resolve them faster, and manage performance.

Analytics and visibility

SD-WAN Analytics aggregates telemetry data and correlates application performance with underlying networks for operational insights, with easy-to-use visualizations. SD-WAN Analytics enhances network visibility, establishes historical benchmarks, and expedites root-cause isolation, ultimately enabling enterprises to take the necessary corrective actions.



CHAPTER 2

Cisco SD-WAN Manager Tools

SD-WAN Manager tools history

Developments in SD-WAN Manager tools, by release.

Table 1: Feature History

Feature Name	Release Information	Description
Global search for Cisco SD-WAN Manager	Cisco Catalyst SD-WAN Manager Release 20.18.1	The search box in the SD-WAN Manager header enables you to search for information related to devices, network, and so on. The integration of role-based access control (RBAC) ensures that only authorized users can access data.
TAC case access for AI Assistant in Cisco SD-WAN Manager	Cisco Catalyst SD-WAN Manager Release 20.18.2	With the AI Assistant you can open, view, and close Technical Assistance Center (TAC) cases. **Note** The foundational infrastructure of AI Assistant is included in this release. As a cloud-delivered component of Cisco Catalyst SD-WAN Manager, AI Assistant's capabilities will continue to expand, providing even greater value for customers.

Feature Name	Release Information	Description
Access to Cisco Support Assistant	Cisco Catalyst SD-WAN Manager Release 26.1.1.1	Support Assistant is a support tool that integrates TAC support functions directly into SD-WAN Manager. In previous releases, using Support Assistant required installing a browser extension. This is no longer needed. With Support Assistant, you can open TAC cases, record screens, and upload logs directly from SD-WAN Manager.

SD-WAN Manager header

Describes the tools available in the header of the SD-WAN Manager page, as viewed in a browser.

Icon	Description
Search	Use the search field to find information on devices, network, configurations, and so on within SD-WAN Manager. SD-WAN Manager maintains search history for each user session. The search results only include information a user is authorized to view, based on role-based access control (RBAC). In a multitenant environment, when a tenant uses the search, SD-WAN Manager returns results related to that tenant only.
AI Assistant	The Cisco AI Assistant is available within SD-WAN Manager. It can help with management tasks like configuration, optimization, task automation, and troubleshooting. The AI Assistant supports operational and management tasks such as monitoring, troubleshooting, and TAC case management.
Tasks	Shows a list of active and completed tasks.
Help	Shows product help, software version, online documentation, and so on. Allows access to Cisco Support Assistant.
Notifications	Shows the details of active and cleared alarms.
User Profile drop-down list	Sign out, or edit your profile.

Cisco Support Assistant

Describes Cisco Support Assistant, an in-product support tool that integrates TAC support functions directly into SD-WAN Manager.

To access Support Assistant, select **TAC Support** from the **Help** menu in the header. Support Assistant supports these functions in SD-WAN Manager:

- **Open support case**: Open TAC cases directly from SD-WAN Manager. You can attach relevant logs and files easily, ensuring faster case resolution with minimal manual steps.
- **Record screen**: Record on-screen activities to demonstrate issues visually during case submission. These recordings help TAC engineers quickly understand the problem context for more efficient troubleshooting.
- **Upload local file**: Upload diagnostic files and configuration logs to Cisco TAC. Secure file transfer is integrated directly within SD-WAN Manager. Share your files while maintaining compliance and privacy standards.

For more information on Support Assistant functions, refer to the Cisco Support Assistant website.

Note Support Assistant is enabled when you authenticate within SD-WAN Manager. You need to re-authenticate in each SD-WAN Manager session to use Support Assistant.

AI Assistant

Describes the AI Assistant available in SD-WAN Manager.

Cisco AI Assistant for SD-WAN Manager

The Cisco AI Assistant is a proprietary conversational AI interface designed to help optimize network management and promote proactive troubleshooting. Through AI-powered responses, recommendations, and insights, the AI assistant helps streamline network operations.

With AI-driven troubleshooting, the AI Assistant accelerates issue identification and resolution, helping administrators and engineers reduce troubleshooting time, minimize downtime, and maintain optimal network performance.

The AI assistant for SD-WAN Manager is available for Cisco SD-WAN Cloud and Cloud-Pro installations, and for on-premises self-hosted SD-WAN deployments that have cloud connectivity and have enabled cloud services. To enable AI Assistant functionality for on-premises deployments, choose **Administration** > **Settings** from the SD-WAN Manager menu, choose **Cloud Services** from the Data Collection & Statistics list, and enable the **Cloud Services** option.

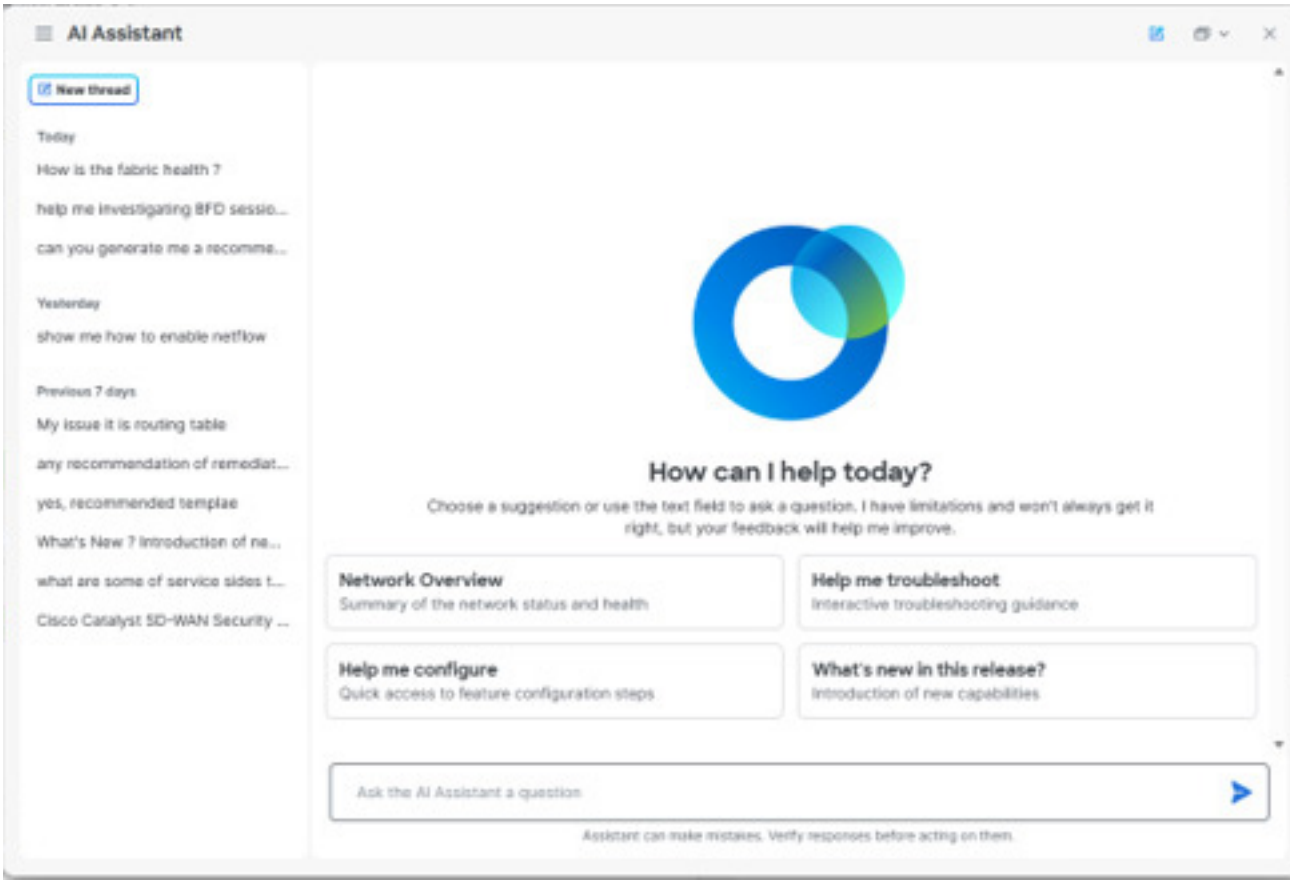
Access the AI Assistant

At the top of the SD-WAN Manager dashboard, select the **AI Assistant** icon.

Figure 1: AI Assistant icon

The AI Assistant opens.

Figure 2: AI Assistant



Select **New Thread** to start a new conversation with the AI Assistant, then choose one of the suggested topics or enter your question or task in the text box.

Your previous queries appear in the chat history pane.

The AI Assistant helps reduce management workload, increase productivity, and improve your networking experience. Start a conversation with the AI Assistant by asking, “What can you help me with?” to learn about its capabilities.

AI Assistant tasks in SD-WAN Manager

The AI Assistant can perform various tasks in SD-WAN Manager:

- Documentation search: Get information about SD-WAN features and capabilities:
  - What is Cloud OnRamp for SaaS?
  - How do I configure Cloud OnRamp for SaaS?
  - How do I configure Application Aware Routing?
- Monitoring and troubleshooting your network: Get information about network and application health:
  - What is the health of my network?

- Are there any link issues in the last 24 hours?
- Are there any application performance issues in the last 7 days?

Note To monitor and troubleshoot the network with the AI Assistant, enable Cloud Services with Analytics onboard.

- TAC case management: Open, view, or close a TAC case.

  To open a TAC case, you must have a support contract or product under warranty. The cisco.com user account that is used to sign on to the Support Case Manager portal must have permission to create, view, and close TAC cases.

  If you provide insufficient information to open a case, the AI assistant provides a TAC portal link with auto-filled information for request completion. You need to complete an authentication workflow for TAC-related actions.

Note Updating or uploading attachment files for existing TAC cases is not supported through the AI Assistant.

AI Assistant prompting

A prompt is a question or any text input that you provide to the Cisco AI Assistant to initiate a conversation or request information. The way you format and construct a prompt plays a crucial role in determining the response from the AI Assistant.

An effective prompt should include these components:

- Subject: Be clear and specific about what you're asking for.
- Context: Provide necessary background information.
- Purpose: State what you want to achieve with your prompt.

By providing precise input and context, you significantly increase the chances of receiving a targeted, relevant, and useful answer from the AI Assistant. Follow these additional guidelines to get the best results:

- Be specific and provide context: Draft your prompt with relevant information, using the correct device names, policy names, and so on to help the AI Assistant understand your request better.
- Use proper syntax: While AI Assistant can understand colloquial language, clear and grammatically correct sentences can improve response accuracy.
- Clarify the desired output: If you have a preferred format for the response, such as a list, a detailed explanation, or tables, mention it in your prompt.
- Provide feedback: If the response doesn't meet your expectations, you can provide feedback or ask for clarification in your next prompt.
- Request unique values: Include the keyword “unique” to request unique values from the AI Assistant.

- Use sequential questioning: Pose multiple inquiries as separate, follow-up questions to enhance clarity and context, rather than combining them into a single complex query.
- Use explicit multi-attribute queries: When requesting information about multiple characteristics or properties simultaneously, clearly state “both” or “all of the following”. Otherwise, the AI Assistant might select an attribute at random to respond to.

Example scenarios for using AI Assistant

Here are some typical scenarios where AI Assistant can help you manage your SD-WAN deployment.

Table 2: Example scenarios for using AI Assistant

Scenario	Prompt	Result
Monitor application performance and SLA.	“How are my applications performing, and are there any SLA violations in my SD-WAN network?"	The AI Assistant analyzes application telemetry such as latency, packet loss, and other performance metrics to detect SLA violations. It highlights affected applications and helps prioritize remediation for business-critical services.
Summarize current network status and get recommendations.	“Give me a summary of network and application health.”	The AI Assistant displays the steps it is taking to analyze and process the query. In this case, it recognizes the need to pull analytic data from a 24-hour window. Next, it determines the additional queries needed to identify any problem areas. Finally, it presents the key health metrics in a table along with lists of top applications by usage and key insights.
Troubleshoot and resolve issues.	“Are there any circuits with high latency?”	The AI Assistant analyzes data and identifies tunnels that show high latency. It then lists likely root causes and recommended actions to address the issue. You are given the option to open a support case or adjust traffic steering policies.

AI Assistant FAQs

How accurate are the recommendations from AI Assistant?

The AI Assistant is designed to provide suggestions by leveraging pre-trained models tuned for networking-specific tasks, integrating with real-time system data when applicable, as well as drawing from networking industry best practices and product documentation to help generate responses. While the AI Assistant aims to provide grounded information, you must validate its suggestions and actions, especially for critical configurations or troubleshooting.

Is my data being used to train the AI Assistant?

No, your data is not used to train the AI Assistant. Cisco handles your data responsibly. Refer to the Cisco AI Assistant Offer Disclosure for more information.