CISCO Connect

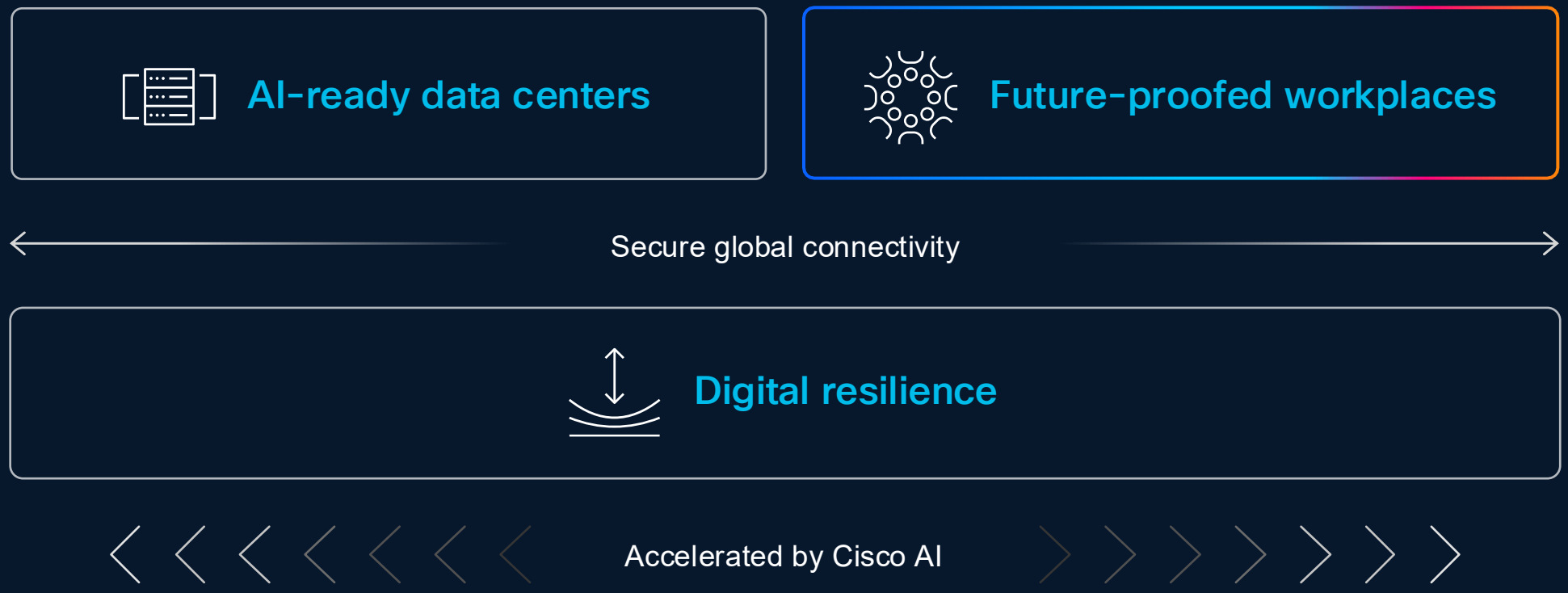
Modernize Your Branch Network with Cisco Secure Unified Branch



Tom Schauffler
Solutions Engineer

October 13, 2026

Cisco powers how people and technology work together across the physical and digital worlds



© 2026 Cisco and/or its affiliates. All rights reserved.

Future-proofed workplaces

Empower and secure every worker, anywhere work happens



Modernize and secure the network

With scalable devices, AgenticOps, and security fused into the network



Secure the human and agentic workforce

With identity, zero trust, SASE, and agent protection



Create intelligent workplace experiences

With collaboration and networking feeding data and intelligence

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

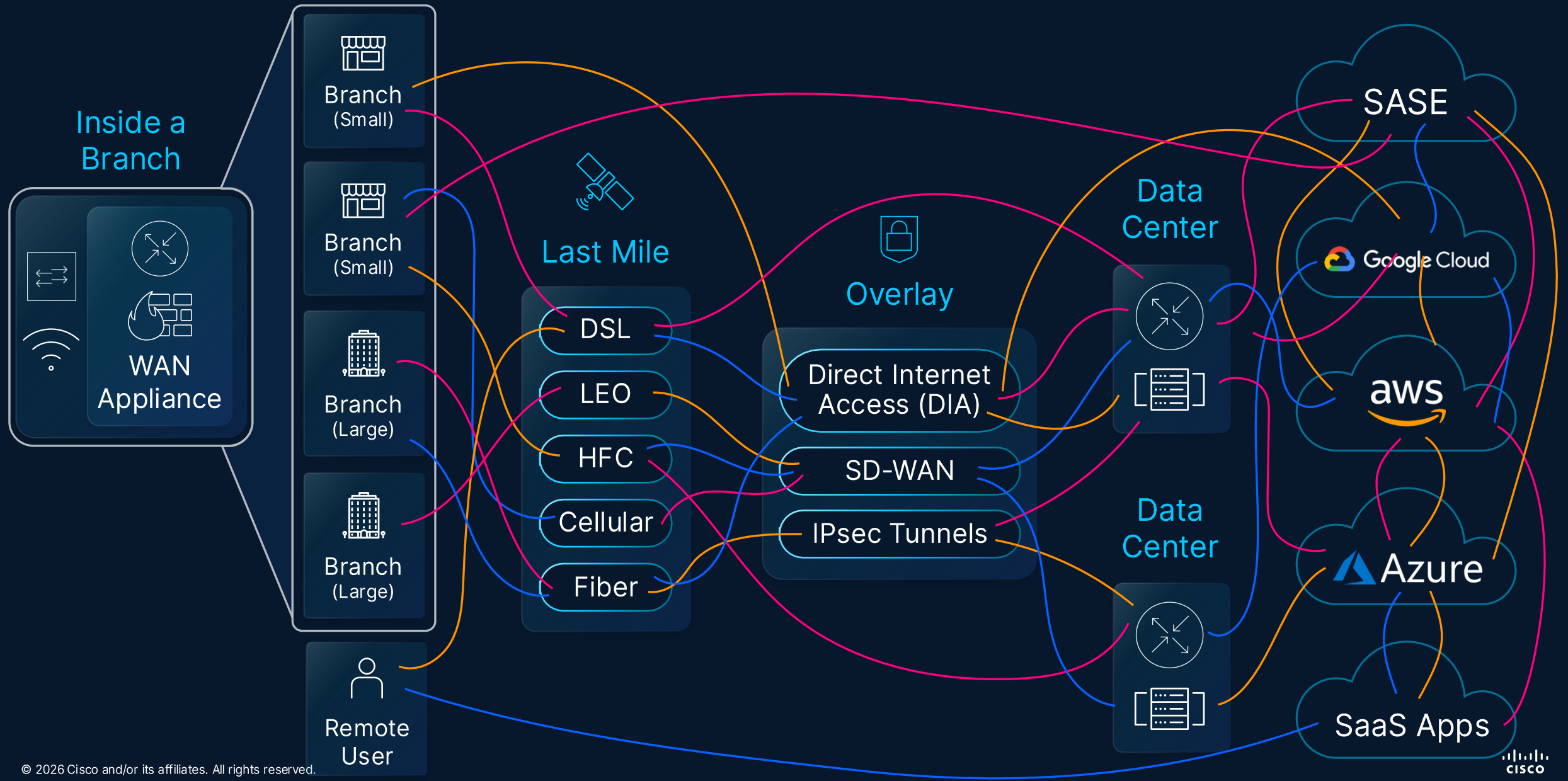
A resilient, secure branch is critical for delivering exceptional experiences

- Need for fast, reliable Wi-Fi and internet connection
- Reliable and secure access to SaaS, public cloud, and data center
- Simplify operations where there is no local IT support
- Enable AI powered operations and reduce risk from post-quantum computing



© 2026 Cisco and/or its affiliates. All rights reserved.

The state of the WAN



© 2026 Cisco and/or its affiliates. All rights reserved.

Challenges in the branch



Operational Complexity and Management Inefficiency

- Manual setup increases human error
- Complex processes delay rapid scaling
- Non-integrated systems drive high operational costs



Security Fragmentation and Policy Inconsistency

- Siloed tools create critical visibility gaps
- Inconsistent policies increase compliance risks
- Fragmented updates leave branches vulnerable to threats



Network Performance and Visibility Gaps

- Lack of app awareness causes poor performance
- Inefficient routing leads to low productivity
- Limited visibility makes troubleshooting difficult

© 2026 Cisco and/or its affiliates. All rights reserved.

These challenges requires a new branch architecture

© 2026 Cisco and/or its affiliates. All rights reserved.

Introducing the Unified Branch

Platform

Management | **Assurance** | **API / Integrations**

AgenticOps



Wi-Fi



Switching



Routing + NGFW + SASE

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Delivering value through a Unified Branch



Platform Advantage

A converged platform for the branch, providing centralized control and simplifying branch operations



Built in Assurance and AIOps

Proactive monitoring and faster troubleshooting to provide the best user experience



Prescriptive designs

Achieve high performance outcomes with Cisco Validated Designs built on Cisco's best practices and validated in real world scenarios



Designed for scale

Optimized to support growth – scale branches easily while maintaining consistent policies and configs

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Cisco Cloud Control

The power of one

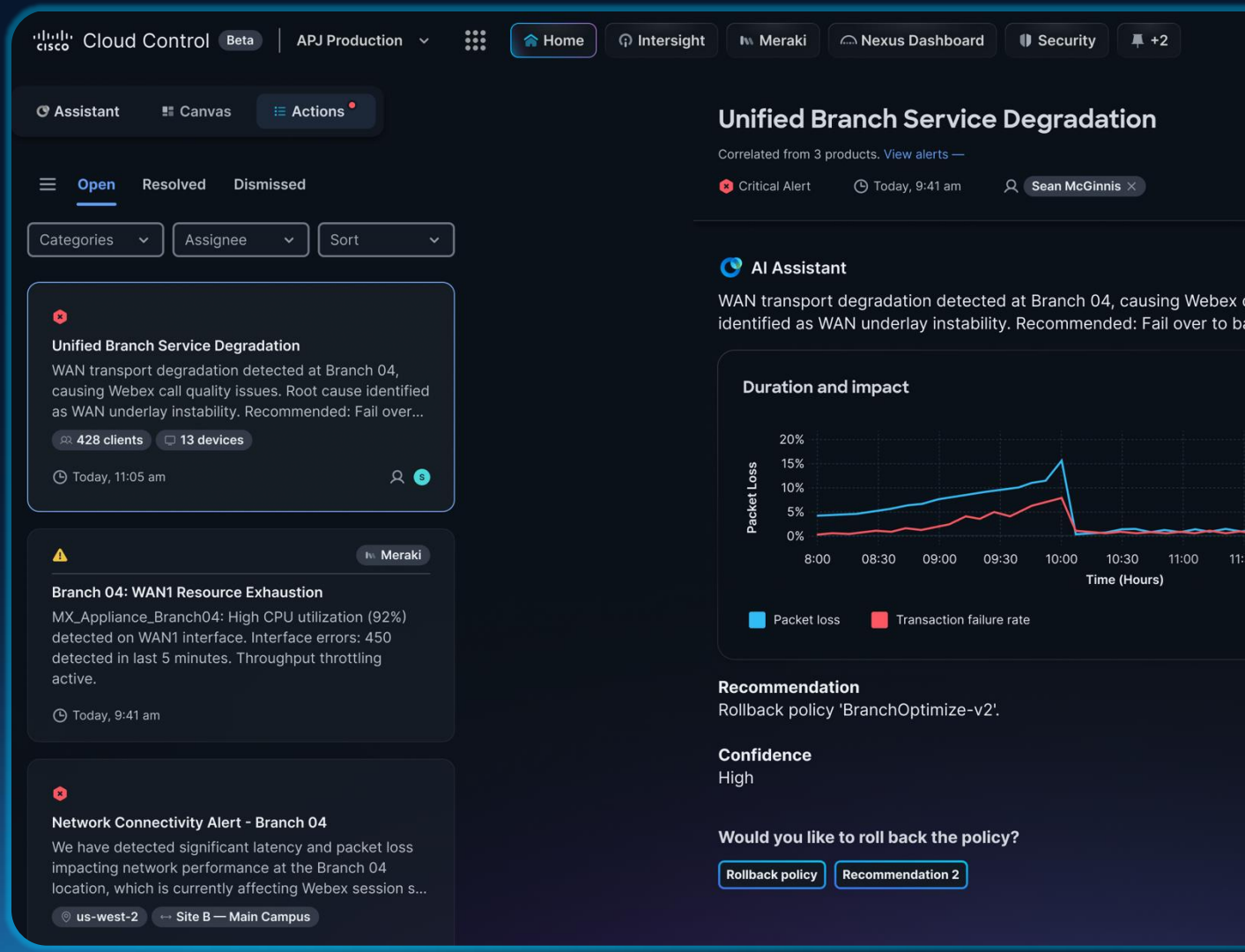
One login
Sign in once. See everything.

One inventory and topology
Every asset. See how it all connects, in real time.

One view for alerts
Actions correlates alerts across every product.

One assistant
Quick answers and tasks with AI Assistant.

One agentic workspace
Investigate, execute and resolve with AI Canvas.



© 2026 Cisco and/or its affiliates. All rights reserved.

Deploy branches in minutes, manage at scale

Unified Branch automation

cisco AI Assistant

Workflows for NetOps

Custom and pre-built workflows integrated to the Meraki Dashboard

Branch as Code for DevOps

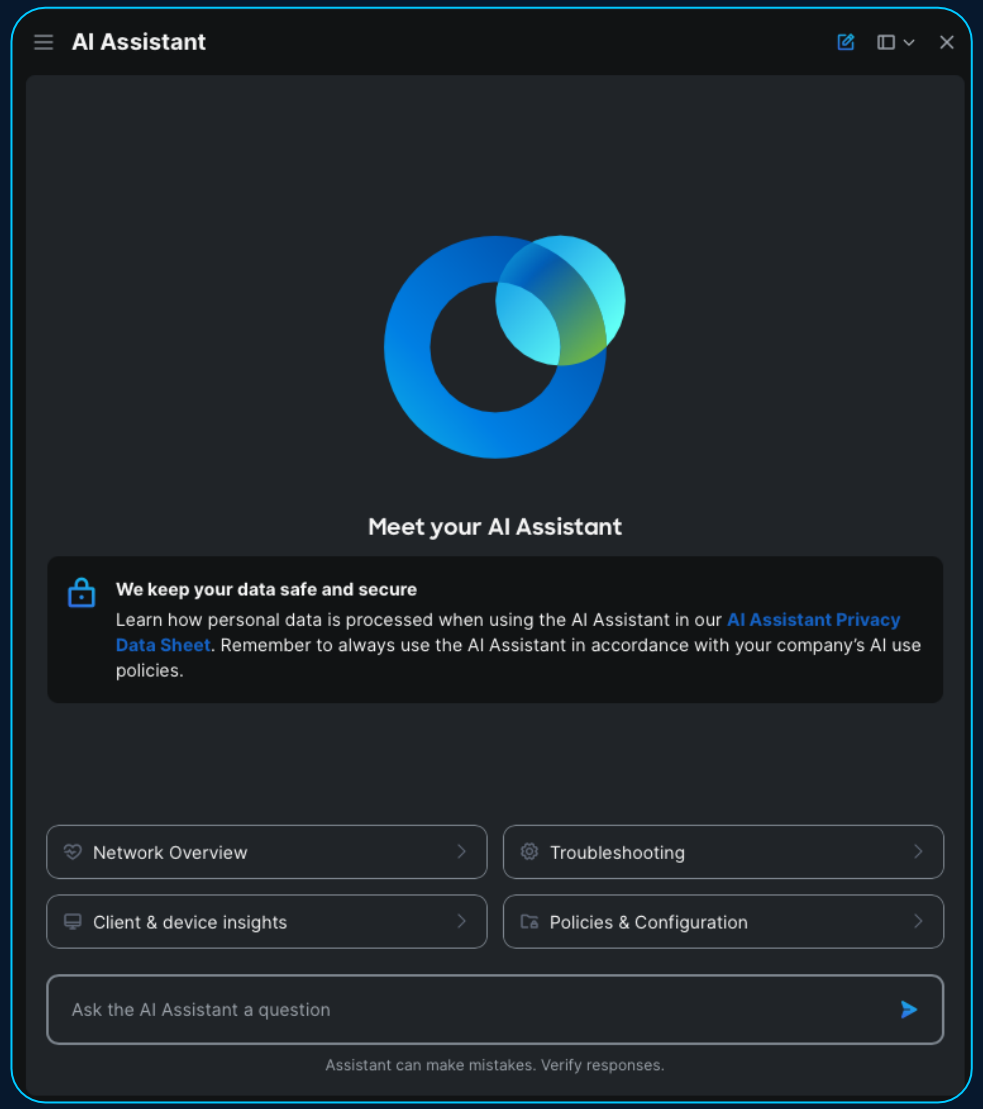
Terraform provisions branch infrastructure in code using data models and templates

Built on Cisco Validated Designs

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Unified Branch powered by AgenticOps



Interactive guidance on Unified Branch, branch-as-code and workflows to set up a full stack branch

Access pre-built and Cisco-Managed workflows directly from the Assistant

Accelerate Root Cause Analysis using simple prompts

Enhance operational efficiency and simplify management

© 2026 Cisco and/or its affiliates. All rights reserved.

Security fused into the network



Securing the device

Protecting and ensuring compliance of devices

Quantum-resistant secure boot



Securing network connectivity

Safeguarding and optimizing network connections

NGFW

XDR

Quantum-resistant:

- IPsec



Securing network access

Securing connectivity to the network

Authorization and scalable segmentation

- Identity Services Engine (ISE)
- Security Group Tags (SGT)



Securing application access

Protecting user access and application interactions

Continuous identity, posture and risk assessment across every session

- SASE
- UZTNA

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Scalable devices, ready for AI

- Unified hardware
- Unified software
- Unified management
- Post-quantum ready



Smart Switches



Secure Routers



Industrial devices



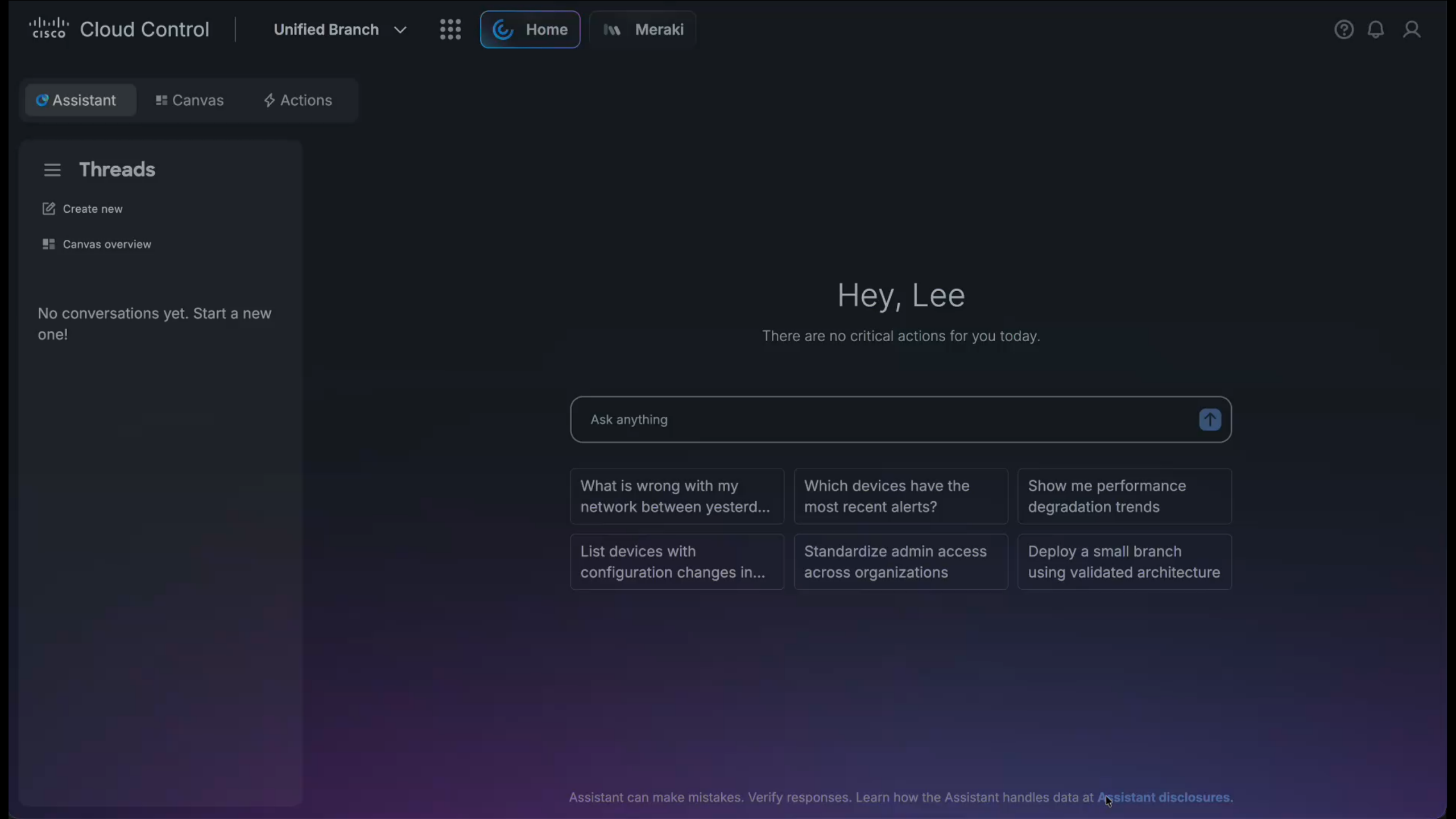
Secure Firewall

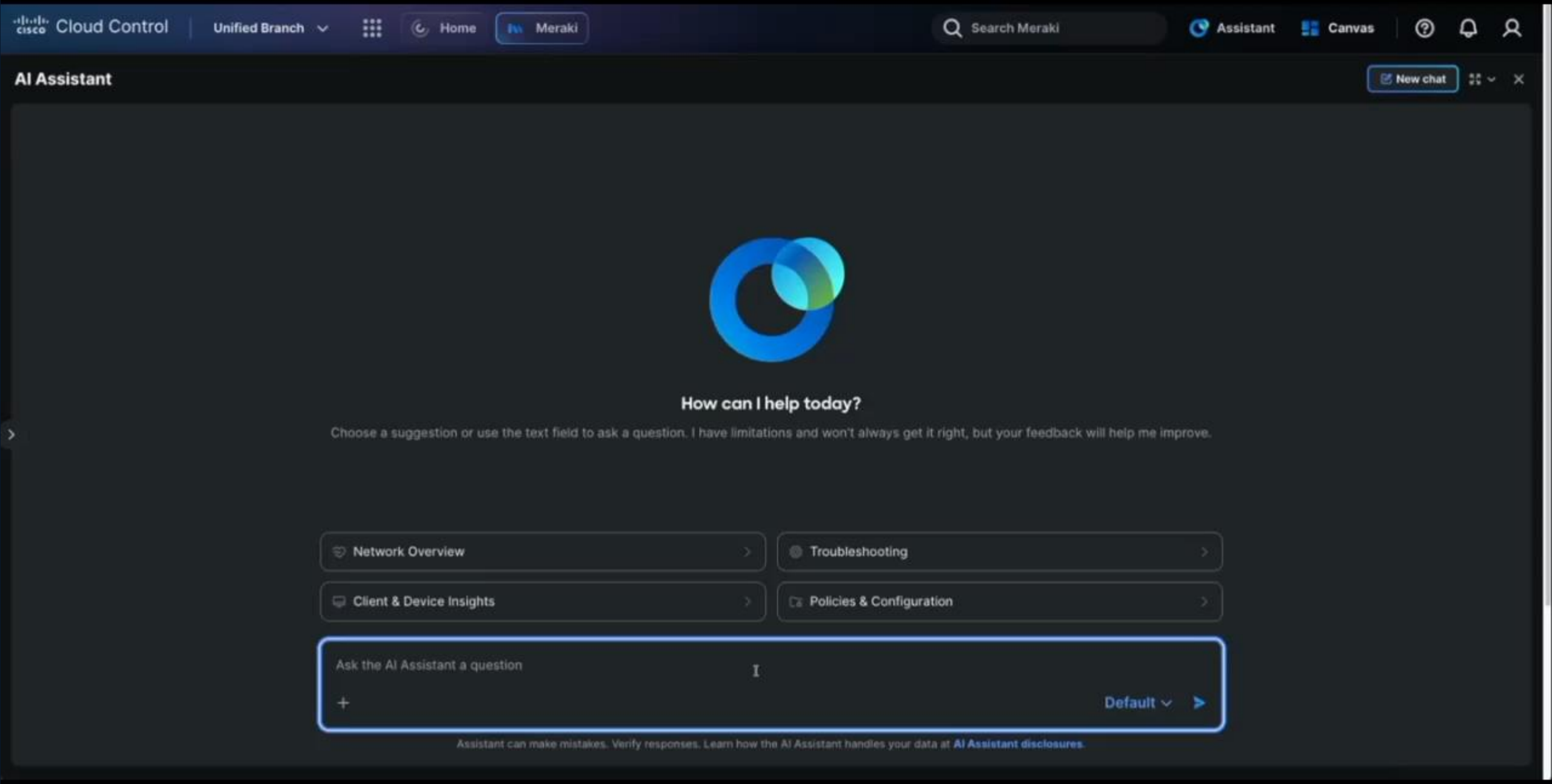


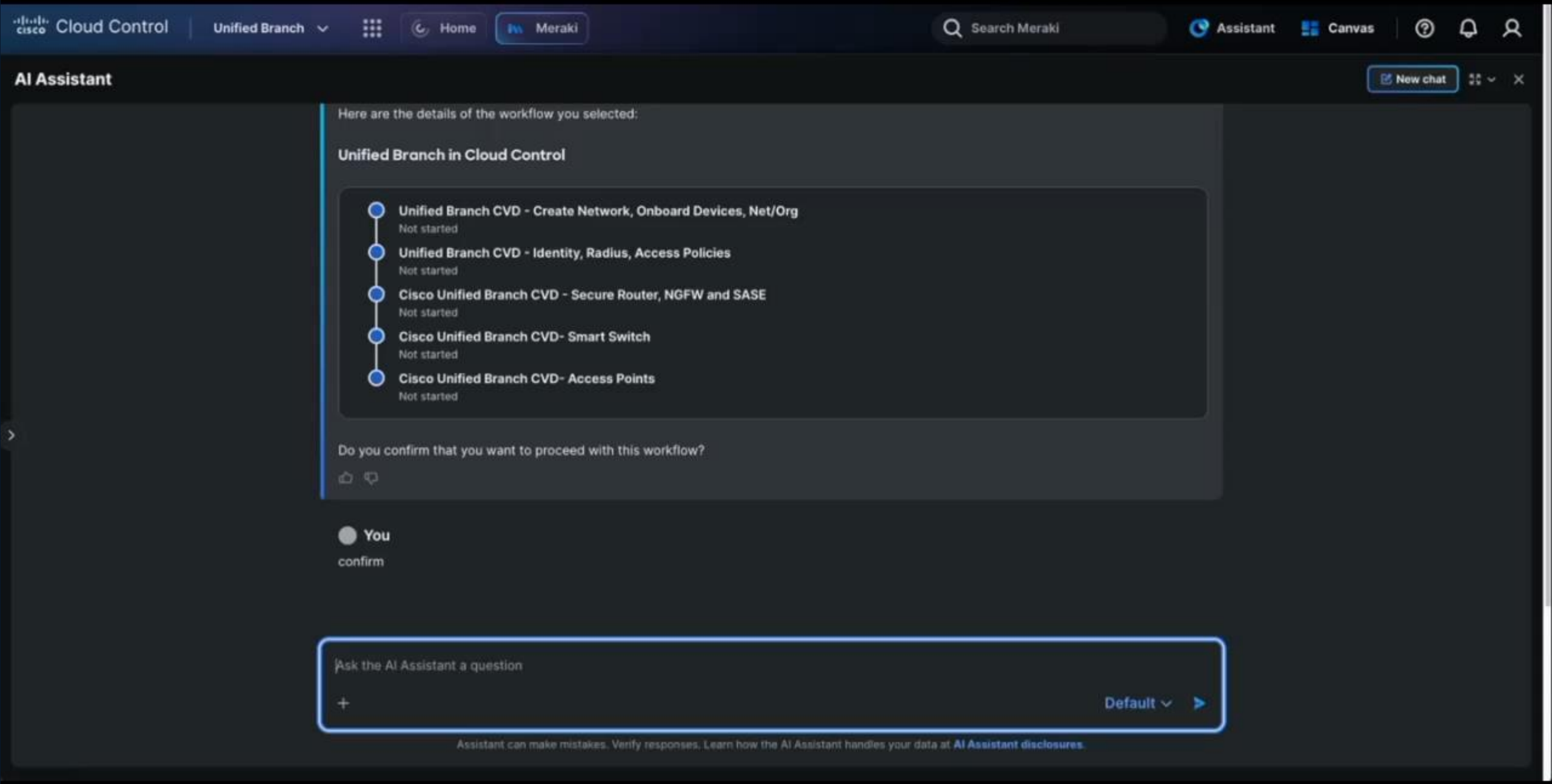
Scalable Wi-Fi 7

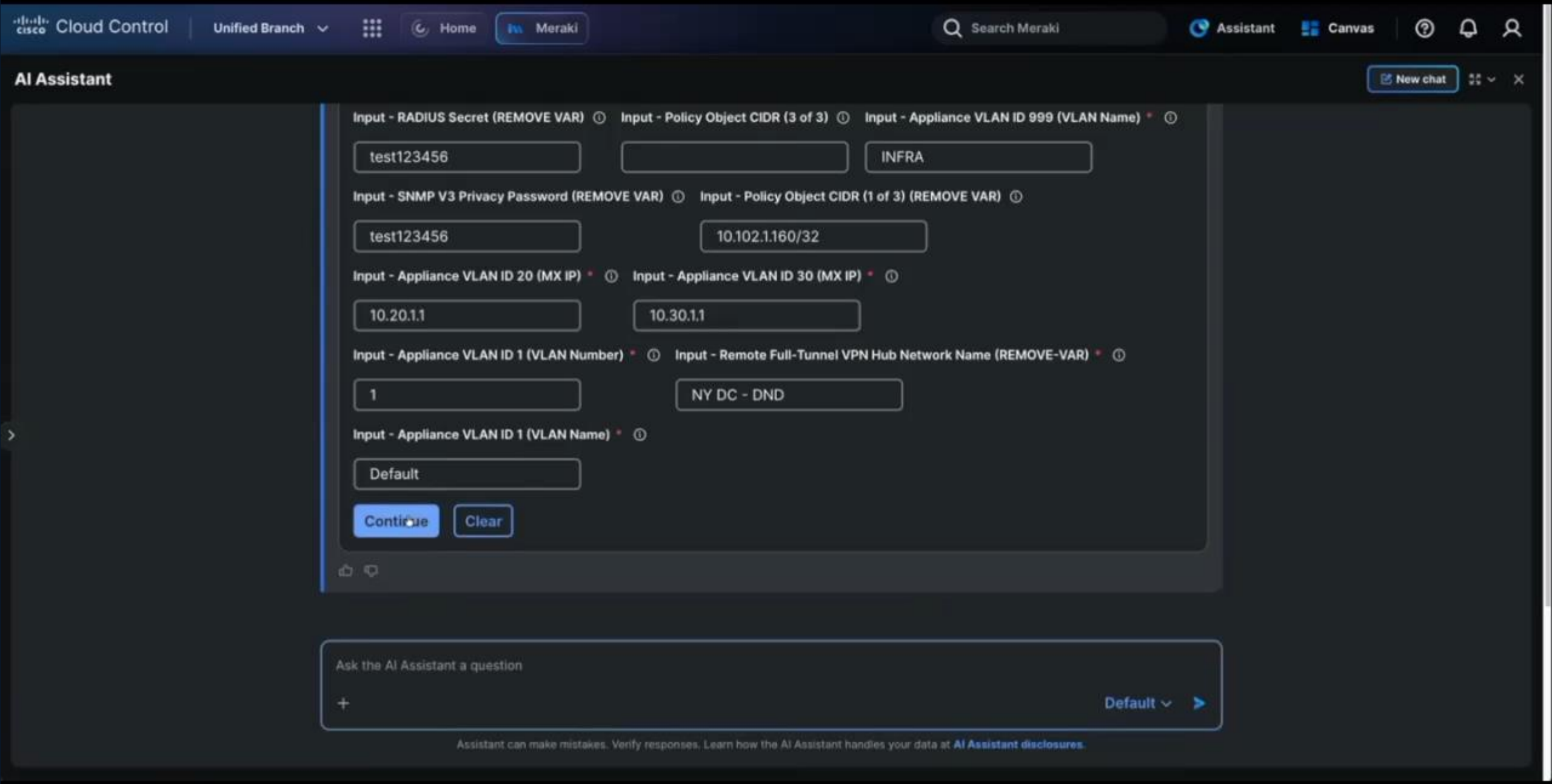
© 2026 Cisco and/or its affiliates. All rights reserved.

Unified Branch Demo


Cloud Control
Unified Branch
Home
Meraki
Assistant
Canvas
Actions
Threads
Create new
Canvas overview
No conversations yet. Start a new one!
Hey, Lee
There are no critical actions for you today.
Ask anything
What is wrong with my network between yesterd...
Which devices have the most recent alerts?
Show me performance degradation trends
List devices with configuration changes in...
Standardize admin access across organizations
Deploy a small branch using validated architecture
Assistant can make mistakes. Verify responses. Learn how the Assistant handles data at Assistant disclosures.


Cloud Control
Unified Branch
Home
Meraki
Search Meraki
Assistant
Canvas
AI Assistant
New chat
How can I help today?
Choose a suggestion or use the text field to ask a question. I have limitations and won't always get it right, but your feedback will help me improve.
Network Overview
Troubleshooting
Client & Device Insights
Policies & Configuration
Ask the AI Assistant a question
Default
Assistant can make mistakes. Verify responses. Learn how the AI Assistant handles your data at AI Assistant disclosures.


Cloud Control
Unified Branch
Home
Meraki
Search Meraki
Assistant
Canvas
AI Assistant
New chat
Here are the details of the workflow you selected:
Unified Branch in Cloud Control
Unified Branch CVD - Create Network, Onboard Devices, Net/Org
Not started
Unified Branch CVD - Identity, Radius, Access Policies
Not started
Cisco Unified Branch CVD - Secure Router, NGFW and SASE
Not started
Cisco Unified Branch CVD- Smart Switch
Not started
Cisco Unified Branch CVD- Access Points
Not started
Do you confirm that you want to proceed with this workflow?
You
confirm
Ask the AI Assistant a question
Default
Assistant can make mistakes. Verify responses. Learn how the AI Assistant handles your data at AI Assistant disclosures.


Cloud Control
Unified Branch
Home
Meraki
Search Meraki
Assistant
Canvas
AI Assistant
New chat
Input - RADIUS Secret (REMOVE VAR)
Input - Policy Object CIDR (3 of 3)
Input - Appliance VLAN ID 999 (VLAN Name)
test123456
INFRA
Input - SNMP V3 Privacy Password (REMOVE VAR)
Input - Policy Object CIDR (1 of 3) (REMOVE VAR)
test123456
10.102.1.160/32
Input - Appliance VLAN ID 20 (MX IP)
Input - Appliance VLAN ID 30 (MX IP)
10.20.1.1
10.30.1.1
Input - Appliance VLAN ID 1 (VLAN Number)
Input - Remote Full-Tunnel VPN Hub Network Name (REMOVE-VAR)
1
NY DC - DND
Input - Appliance VLAN ID 1 (VLAN Name)
Default
Continue
Clear
Ask the AI Assistant a question
Default
Assistant can make mistakes. Verify responses. Learn how the AI Assistant handles your data at AI Assistant disclosures.

AI Assistant

New chat

Input - SNMP V3 Authentication Password (REMOVE VAR)	test123456
Input - Remote Full-Tunnel VPN Hub Network ID	—
Input - RADIUS Secret (REMOVE VAR)	test123456
Input - Policy Object CIDR (3 of 3)	—
Input - Appliance VLAN ID 999 (VLAN Name)	INFRA
Input - SNMP V3 Privacy Password (REMOVE VAR)	test123456
Input - Policy Object CIDR (1 of 3) (REMOVE VAR)	10.102.1.160/32
Input - Appliance VLAN ID 20 (MX IP)	10.20.1.1
Input - Appliance VLAN ID 30 (MX IP)	10.30.1.1
Input - Appliance VLAN ID 1 (VLAN Number)	1
Input - Remote Full-Tunnel VPN Hub Network Name (REMOVE-VAR)	NY DC - DND
Input - Appliance VLAN ID 1 (VLAN Name)	Default

This workflow will configure a unified branch network in cloud control, including VLANs, device claims, policy objects, and network settings.

Please confirm if you would like to proceed with these settings.

confirm

Default

Assistant can make mistakes. Verify responses. Learn how the AI Assistant handles your data at AI Assistant disclosures.

AI Assistant

New chat

2 minutes ago

- **Unified Branch CVD - Identity, Radius, Access Policies**
  1 minute ago
- **Cisco Unified Branch CVD - Secure Router, NGFW and SASE**
  1 minute ago
- **Cisco Unified Branch CVD- Smart Switch**
  less than a minute ago
- **Cisco Unified Branch CVD- Access Points**
  less than a minute ago

Outcome

The workflow was executed successfully, returning a status message of "200 OK" and a status code of 200.

Results

- Output-StatusMessage: 200 OK
- Output-StatusCode: 200

Next Recommendations

- Review the detailed output to confirm all expected data was processed.
- If any fields are empty or missing, verify the input parameters and rerun the workflow as needed.
- Consider documenting the results for future reference or compliance purposes.

For more details, please check: Workflows → Run

Ask the AI Assistant a question

Default

Assistant can make mistakes. Verify responses. Learn how the AI Assistant handles your data at AI Assistant disclosures.