What's New in Security Cloud Control

Cisco Security Cloud Control
Updated NaN,

Preface

Welcome to Cisco Security Cloud Control

Read about all of the new features in Cisco Security Cloud Control.

This document announces all the new features implemented in Cisco Security Cloud Control and its integrated products.

Overview of Security Cloud Control

Describes Cisco Security Cloud Control as a unified platform for onboarding, managing, and navigating integrated Cisco security products.

Security Cloud Control is a security platform that

- allows you to manage your security products and achieve security outcomes from a single integrated interface
- provides streamlined integration of security products with a single claim code for all purchased subscriptions, and
- enables intuitive navigation between products with standardized platform menu and toolbar for all integrated products.

Core services and features

Security Cloud Control provides these core services to all integrated products on the platform:

- **Platform Management**: Common services such as managing role-based access control, claiming subscriptions and standardized regional deployment of product instances are provided by Security Cloud Control. By centralizing these functions, Security Cloud Control ensures a consistent user experience in provisioning and managing access across all Cisco security products managed from the platform. Administrators reach these common services from the Platform Management menu in the main navigation bar of Security Cloud Control.
- **AI Assistant**: The Cisco AI Assistant in Security Cloud Control is designed to streamline security operations by providing AI-driven insights, automation, and contextual guidance. It assists administrators in managing security policies, troubleshooting issues, and optimizing configurations across Cisco's security products, including Firewall, Duo, Hypershield, and Secure Access. By leveraging natural language processing and cross-platform intelligence, the assistant enhances efficiency, accelerates incident response, and simplifies security workflows.
- **Global Search**: Search for device names, policy names, object names, or values such IP addresses and CIDR blocks in supported objects managed by Security Cloud Control Firewall Management.
- **Shared Objects**: Creating and managing objects that can be shared across devices and policies.
- **Unified documentation portal**: A documentation "Help" experience where all documentation is accessible in one portal.
- **User and group management**: Within Security Cloud Control, user and group management occurs at the platform level. Roles are assigned to these users and groups to define their privileges for administering Security Cloud Control and the integrated products.

Integrating Security Products

Integrating security products in the platform is a streamlined experience. After purchasing your subscriptions to Cisco security products, you receive a single email, with a single claim code for all the subscriptions you purchased. Entering the claim code in your new Security Cloud Control organization provisions all your products to Security Cloud Control simultaneously.

From Security Cloud Control, you can manage all of these security products:

- AI Defense
- Firewall Management
- Mesh Policy Engine
- Multicloud Defense
- Secure Access
- Secure Workload

From Security Cloud Control, you can open these security products. After they open, these products operate as standalone products and you cannot manage them through Security Cloud Control. You can only claim or deactivate the licenses of such products from Security Cloud Control.

In the Security Cloud Control toolbar, click the nine-dot menu to launch these products:

- Cisco Secure Email Threat Defense
- Cisco Secure Endpoint
- Cisco XDR
- Cisco Duo

How Security Cloud Control is Different from Security Provisioning and Administration

Existing customers of Security Provisioning and Administration for Government will enjoy the new features and product support available to them in Security Cloud Control

As part of our platform upgrade, your environment will be transitioned from Security Provisioning and Administration to Security Cloud Control to provide enhanced capabilities and continued platform support.

Additional details regarding the migration timeline, scope, and any required customer actions will be communicated in advance of the transition.

Security Provisioning and Administration for Government customers benefited from these centralized functions:

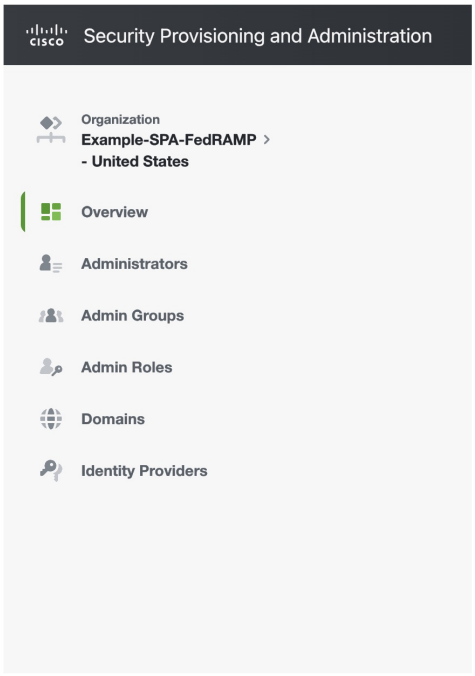
- User management
- Subscription management
- Domain management
- Identity Provider management

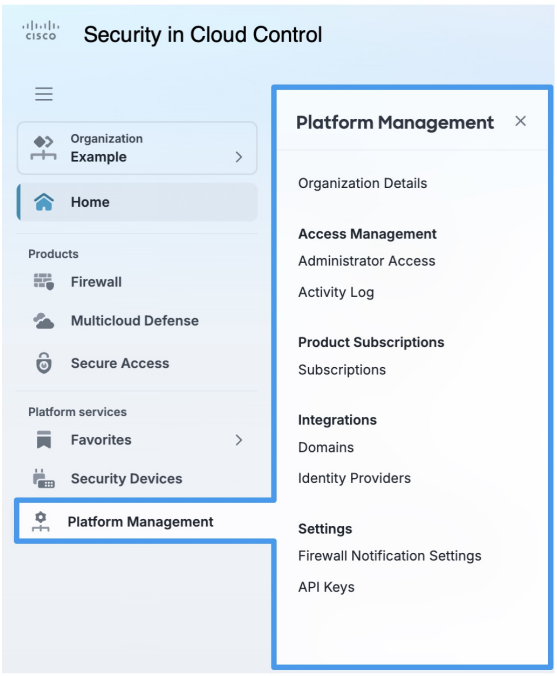
Security Provisioning and Administration for Government supported one Cisco security product, Secure Access. After using the centralized functions in Security Provisioning and Administration for Government, users would then configure Secure Access after connecting to that tenant separately.

Security Cloud Control provides all of those centralized functions, as well as others. Users can also manage all of these supported products in one integrated platform:

- Secure Access
- Firewall in Security Cloud Control
- Multicloud Defense

Figure 1: Comparing Security Provisioning and Administration to Security Cloud Control





Products and solutions supported by Security Cloud Control

Lists products and solutions supported by Security Cloud Control and how they can be integrated or launched from the platform.

Currently, these are the products you can integrate with Security Cloud Control.

AI Defense: AI Defense addresses risks for users and providers of AI. Using network visibility and enforcement points in the Security Cloud Control, AI Defense adds detection and enforcement measures to discover sanctioned and unsanctioned AI workloads, applications, models, data, and user access across your distributed cloud environment. For organizations that develop and deliver AI-powered services, AI Defense detects vulnerabilities in your AI models before they're delivered. For your running AI applications, AI Defense guardrails intercept rapidly evolving threats, including prompt injections, denial of service, and data leakage. See AI Defense Documentation for more information.

SASE Management: SASE Management is a cloud-delivered security solution designed to simplify and unify your network and security policy management. SASE Management enables seamless management of Secure Internet Access (SIA) and Secure Private Access (SPA) for your Catalyst SD-WAN infrastructure and device policy with Cisco Secure Access cloud access rules in a single, integrated platform. If SASE Management is enabled on your organization, you can share some network object and network object groups between Cisco Secure Access and Catalyst SD-WAN security policies. See the Cisco SASE Management Administration Guide and Common Objects and Object Groups for more information.

Security Cloud Control Firewall Management: Security Cloud Control Firewall Management (formerly Cisco Defense Orchestrator) is a cloud-based security policy manager that simplifies and unifies policy across your Cisco firewalls and other devices. See Firewall in Security Cloud Control Documentation for more information.

Multicloud Defense: Multicloud Defense provides a simplified and highly automated approach to multicloud security. This solution allows organizations to manage and secure their multicloud environments using a single SaaS delivered control plane, and centralized or distributed PaaS-delivered data plane architectures. Multicloud Defense provides continuous visibility, unified protection and dynamic policy updates across all major cloud providers, thereby eliminating the need for separate point solutions for each cloud provider. See Multicloud Defense Documentation for more information.

Secure Access: Cisco Secure Access is a cloud-based platform that provides multiple levels of defense against internet-based threats. Connect securely to the internet, SaaS apps, and private digital resources from your organization's network or roaming off-network. Using policy rules, configure and enforce security controls on collections of resources,

users, and devices. See Secure Access Documentation for more information. Secure Access subscriptions also include the Identity Intelligence integration via Security Cloud Control at no additional charge—this does not include access to the standalone Identity Intelligence dashboard. For more information, see Integrate Cisco Identity Intelligence with Secure Access.

Secure Workload: Cisco Secure Workload (formerly Tetration) seamlessly delivers zero-trust micro-segmentation across any workload, environment, or location from a single console. With comprehensive visibility into every workload interaction and powerful AI/ML-driven automation, Secure Workload reduces the attack surface by preventing lateral movement, identifies workload behavior anomalies, helps rapidly remediate threats, and continuously monitors policy compliance. See Secure Workload Documentation for more information.

Cisco XDR (Extended Detection and Response): Cisco XDR is a cloud-native, extensible security solution designed to simplify security operations and accelerate incident response. It collects and analyzes telemetry from multiple sources—including endpoint, network, firewall, email, identity, and DNS—to detect sophisticated threats with enriched context and threat intelligence from Cisco Talos.

Cisco XDR prioritizes threats based on potential risk and impact, reduces false positives, and provides AI-driven guidance and automation to streamline investigations and remediation. This unified approach enables Security Operations Center (SOC) teams to act faster, improve productivity, and build security resilience by integrating both Cisco and third-party security tools in a multi-vector, multi-vendor environment. See Cisco XDR Help Center for more information.

1 AI Defense

Topics:

- Jan 6, 2026 (2026.1.1 release)
- Dec 9, 2025 (2025.12.1 release)
- Nov 12, 2025 (2025.11.1 release)
- Jul 23, 2025 (2025.7.1 release)

AI Defense provides discovery, validation, and real time security for AI models, applications, and users.

In this section, we list new software features, enhancements, behavior changes, and product improvements added to AI Defense.

Jan 6, 2026 (2026.1.1 release)

List of AI Defense feature updates provided in the 2026.1.1 release

These are the new features and improvements provided in the AI Defense 2026.1.1 release on January 6, 2026.

- AI Defense Adopts New AI Threat Taxonomy on page 7
- AI Defense MCP Server Catalog on page 7
- AI Defense Hybrid Deployment on Azure on page 8

AI Defense Adopts New AI Threat Taxonomy

AI Defense introduces Cisco's Integrated AI Security and Safety Framework, a comprehensive threat taxonomy for describing and managing AI-specific security threats. AI Defense now presents results and events according to this taxonomy's categories.

AI Defense introduces Cisco's Integrated AI Security & Safety Framework, a comprehensive threat taxonomy for describing and managing AI-specific security threats. AI Defense now presents results and events according to this taxonomy's categories. The framework provides a clear and comprehensive framework for describing, managing, and addressing AI-specific security threats throughout the lifecycle of AI systems. Learn about the taxonomy in the Cisco Integrated AI Security and Safety Framework Report.

The following features of AI Defense now present their results according to this taxonomy's categories, enabling organizations to quickly categorize discovered AI risks:

- AI Defense runtime protection
- AI Defense validation
- AI Defense model scanning
- AI Defense MCP scanning

Our taxonomy of AI threats has four layers: objectives (the "why" behind attacks), techniques (the "how"), subtechniques (specific variants of "how"), and procedures (real-world implementations). This hierarchy creates a logical, traceable pathway from high-level motivations to detailed implementations.

When AI Defense discovers or blocks a threat, we label it with the attacker objectives, techniques, and subtechniques that we observed:

- Attacker objectives: The nineteen attacker objectives range from goal hijacking and jailbreaks to communication compromise, data privacy violations, privilege escalation, harmful content generation, and cyber-physical manipulation. These objectives map to observed patterns, threats and vulnerabilities.
- Techniques and subtechniques: The 150+ techniques and subtechniques cover tactics such as prompt injections (both direct and indirect), jailbreaks, multi-agent manipulation, memory corruption, supply chain tampering, environment-aware evasion, tool exploitation, and dozens more. By identifying a technique and subtechnique, AI Defense provides the specificity necessary for your operational team to address risks.

To learn more, see out recent blog post.

AI Defense MCP Server Catalog

AI Defense MCP gateway scanning adds an MCP catalog with API endpoints to register and scan MCP servers for security vulnerabilities.

AI Defense MCP gateway scanning, available as a beta release feature, adds an MCP catalog. This feature provides API endpoints to register and scan MCP servers for security vulnerabilities.

- Registration Endpoint: Register MCP servers by providing details such as server URL, authentication credentials, and server type.
- Scanning Endpoint: Trigger vulnerability scans for registered MCP servers on-demand or at scheduled intervals.

AI Defense MCP scanning inspects tool descriptions to detect tool poisoning attempts and create unique tool signatures for integrity validation. If a tool description contains malicious or misleading content, interactions with it are blocked.

AI Defense Hybrid Deployment on Azure

AI Defense now supports hybrid deployment on Azure, allowing AI Validation and AI Runtime processing to run in your Azure cloud environment.

AI Defense now supports hybrid deployment on Azure. This deployment option is supported in controlled availability. In an AI Defense hybrid deployment on Azure, AI Validation and AI Runtime processing run in your Azure cloud environment, allowing you to avoid having to publicly expose model endpoints. The AI Defense control plane remains SaaS (log in via Security Cloud Control). For details, see the AI Defense Hybrid Deployment Guide.

Dec 9, 2025 (2025.12.1 release)

AI Defense released new features on December 9, 2025.

AI Defense version 2025.12.1 was released on December 9, 2025, providing these updates.

AI Runtime Protection

- Better reporting of AI Runtime events on page 8
- New AI Runtime batch event retrieval API on page 8

New AI Runtime batch event retrieval API

The AI Defense Management API adds a new batch event retrieval API that allows your team to retrieve records of AI runtime enforcements actions in bulk. This endpoint improves data retrieval efficiency by allowing your team to fetch details for multiple AI Runtime events in a single API call, replacing the need for per-event calls.

In this release, the AI Defense Management API introduces a new batch event retrieval API that allows your team to retrieve records of AI runtime enforcements actions in bulk. This endpoint improves data retrieval efficiency by allowing your team to fetch details for multiple AI Runtime events in a single API call, replacing the need for per-event calls.

Better reporting of AI Runtime events

When the AI Defense runtime gateway detects a violation in a prompt or response, it now records a unique Event ID in the policy violation event that is logged. In addition, each policy violation event now includes the model name and model provider name.

When the AI Runtime gateway detects a violation in a prompt or reponse, it now records a unique Event ID in the policy violation event that is logged. In addition, each policy violation event now includes the model name and model provider name. You can retrieve and inspect policy violation events via the AI Defense management API or in the Events section of the AI Defense UI.

AI Defense MCP server catalog

AI Defense MCP gateway scanning adds an MCP catalog. New API endpoints enable you to register and scan MCP servers for security vulnerabilities.

MCP server catalog

The advanced MCP gateway scanning feature, available as an alpha release feature since the 25.9.3 release, adds an MCP catalog. This feature provides an API endpoint for MCP server registration and scanning. With this API endpoint, you can register and scan an MCP server for security vulnerabilities.

- Registration Endpoint: Register MCP servers by providing details such as server URL, authentication credentials, and server type.
- Scanning Endpoint: Trigger vulnerability scans for registered MCP servers on-demand or at scheduled intervals.

AI Defense MCP scanning inspects tool descriptions to detect tool poisoning attempts and create unique tool signatures for integrity validation. If a tool description contains malicious or misleading content, interactions with it are blocked.

Nov 12, 2025 (2025.11.1 release)

New runtime and validation features in November 2025

AI Defense version 2025.11.1 was released on November 12, 2025, providing these updates.

- Support for runtime protection of Japanese content on page 9
- Support for validation of Japanese language models on page 9

Support for runtime protection of Japanese content

AI Defense runtime protection can now inspect prompts and responses in Japanese.

AI Defense runtime protection can now inspect prompts and responses in Japanese. In the **Policy** add or edit panel of AI Defense, use the **Language rule configuration** field to specify that the primary language for model interaction is Japanese.

Support for validation of Japanese language models

AI Defense model validation now supports the testing of Japanese language models. In the **Run validation** panel of AI Defense, use the **Language** field to specify that the primary language of your model is Japanese.

AI Defense model validation now supports the testing of Japanese language models. In the **Run validation** panel of AI Defense, use the **Language** field to specify that the primary language of your model is Japanese.

Jul 23, 2025 (2025.7.1 release)

First release of AI Defense

AI Defense version 2025.7.1 released with these features.

- Azure AI Services Support on page 9
- Runtime Updates in July 2025 on page 10
- Validation Updates in July 2025 on page 10
- User Activity Log Added on page 10

Azure AI Services Support

AI Defense AI asset visibility now supports Azure AI Services, allowing you to secure Azure OpenAI-hosted models.

This release introduces AI asset visibility support for Azure AI Services. AI Defense can now validate Azure OpenAI-hosted models, building on existing support for AWS Bedrock-hosted models. This includes new support for asset types in Azure, including deployments, assistants, vector stores, and data files.

Runtime Updates in July 2025

AI Defense Runtime protection adds a new Management REST API and Python SDK to register and policy-protect your AI applications with AI Defense.

AI Defense runtime protection adds the following in the July 2025 release:

- New Management API for setting up runtime protection: Integrate with your CI/CD pipeline to register and policy-protect your AI applications with AI Defense: https://developer.cisco.com/docs/ai-defense-management/ (customer login required)
- SDK: New Python SDK for the AI Defense Inspection API: https://github.com/cisco-ai-defense/ai-defense-python-sdk

Validation Updates in July 2025

AI Defense validation runs can now be launched from the AI Defense Management API, and each validation run tests your models more broadly using a larger prompt bank.

AI Defense validation offers number of improvements in this release:

- API-based testing: Launch and manage validation runs from the new AI Defense Management API (customer login required)
- New support for validation of guardrail-protected enforcement points
- Broader test coverage, now applying an expanded prompt bank with over 50 techniques and over 100 intents (up by 30 and 100 percent, respectively)

User Activity Log Added

New AI Defense user activity log tracks user interactions.

The new AI Defense user activity log tracks user interactions within AI Defense. The activity log is accessible to AI Defense administrators via the Administration panel. This feature ensures accountability and supports regulatory compliance by tracking all changes, allowing identification of unauthorized or erroneous modifications.

2 Firewall Management

Topics:

- Oct 29, 2026
- Oct 8, 2026
- Oct 1, 2026
- Sep 17, 2026
- Sep 10, 2026
- Sep 3, 2026
- Aug 6, 2026
- Jul 31, 2026
- Jul 24, 2026
- Jun 5, 2026
- May 8, 2026
- Apr 24, 2026
- Mar 27, 2026
- Mar 13, 2026
- Jan 30, 2026
- Dec 12, 2025
- Dec 4, 2025
- Nov 20, 2025
- Nov 14, 2025
- Nov 6, 2025
- Oct 23, 2025
- Sep 18, 2025
- Aug 21, 2025
- Aug 14, 2025
- Jul 23, 2025
- Jul 3, 2025
- Jun 12, 2025

Describes new software features, enhancements, behavior changes, and product improvements added to Security Cloud Control Firewall Management.

Firewall Management (formerly Cisco Defense Orchestrator) is a cloud-based security policy manager that simplifies and unifies policy across your Cisco firewalls and other devices.

In this section, we list new software features, enhancements, behavior changes, and product improvements added to Firewall Management.

Oct 29, 2026

New features and improvements deployed on October 29, 2026 in Security Cloud Control Firewall Management.

These are the new features and improvements deployed on October 29, 2026 in Security Cloud Control Firewall Management.

- Streamline Configuration Deployment for Firewall Devices on page 13
- Global Search now finds pages across your organization on page 13

Streamline Configuration Deployment for Firewall Devices

You can now deploy pending configuration changes to Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense devices directly from Security Cloud Control. This update allows you to manage deployments efficiently from either the Security Devices page or the dedicated Deployments page.

You can now deploy pending configuration changes to Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense devices directly from Security Cloud Control. This update allows you to manage deployments efficiently from either the Security Devices page or the dedicated Deployments page.

For more information, see Deploy Configuration Changes to Firewall Devices.

Global Search now finds pages across your organization

Global Search now shows matching navigation pages across the products available in your Security Cloud Control organization. For instance, search for network to find relevant features and pages. This helps you get to the right destination faster.

Global Search now shows matching navigation pages across the products available in your Security Cloud Control organization. For instance, search for network to find relevant features and pages. This helps you get to the right destination faster.

For more information, see Global Search.

Oct 8, 2026

New features and improvements deployed on October 08, 2026 in Security Cloud Control Firewall Management

This new feature is deployed in Security Cloud Control Firewall Management.

- Cisco Secure Dynamic Attributes Connector Health Notification

Cisco Secure Dynamic Attributes Connector Health Notification

Security Cloud Control offers notifications regarding the health of all configured Cisco Secure Dynamic Attributes Connectors (CSDAC). To help you maintain optimal functionality, Security Cloud Control offers continuously monitors key Cisco Secure Dynamic Attributes Connector components, including connectors, adapters, and filters, and promptly notifies you of any transitions to error or recovery states. These early notifications enable you to address service issues before they impact production.

Security Cloud Control Firewall Management offers notifications regarding the health of all configured Cisco Secure Dynamic Attributes Connectors (CSDAC). To help you maintain optimal functionality, Security Cloud Control continuously monitors key Cisco Secure Dynamic Attributes Connector components, including connectors, adapters, and filters, and promptly notifies you of any transitions to error or recovery states. These early notifications enable you to address service issues before they impact production.

To receive the CSDAC health notifications in the Security Cloud Control portal, select the **All Dynamic Attributes Connector health notifications** check box in the **Firewall Notifications** > **Notification Preferences** page.

You can configure notifications through e-mail, as well as webhook endpoints including Cisco Webex, Microsoft Teams, and Slack to receive notifications directly in those applications.

For details, refer to *Manage user notification preferences* section in the Security Cloud Control Firewall Management documentation.

Oct 1, 2026

New features and improvements deployed on October 1, 2026 in Security Cloud Control Firewall Management.

This is the new feature deployed on October 1, 2026 in Security Cloud Control Firewall Management.

- Search Cisco Secure Firewall Events in Splunk with Federated Search on page 14

Search Cisco Secure Firewall Events in Splunk with Federated Search

Security Cloud Control now enables you to leverage Splunk Federated Search to search and analyze Cisco Secure Firewall Threat Defense events stored in Cisco Security Analytics and Logging (SaaS), without the need to ingest them directly into Splunk Cloud Platform. This integration enhances operational efficiency, provides end-to-end visibility by correlating real-time alerts with historical data, supports security investigations and compliance readiness, and helps reduce data ingestion and storage costs. You can also run reports and investigate incidents directly from the Splunk Cloud Platform interface.

Security Cloud Control now enables you to leverage Splunk Federated Search to search and analyze Cisco Secure Firewall Threat Defense events stored in Cisco Security Analytics and Logging (SaaS), without the need to ingest them directly into Splunk Cloud Platform. This integration enhances operational efficiency, provides end-to-end visibility by correlating real-time alerts with historical data, supports security investigations and compliance readiness, and helps reduce data ingestion and storage costs. You can also run reports and investigate incidents directly from the Splunk Cloud Platform interface.

For more information, see Splunk with Federated Search SAL

Sep 17, 2026

New features and improvements deployed on September 17, 2026 in Security Cloud Control Firewall Management.

These are the new features and improvements deployed on September 17, 2026 in Security Cloud Control Firewall Management.

- ASA Secure Client upgrades for MSSP (BETA) on page 14
- Introducing Agent Workforce in Security Cloud Control on page 15
- Introducing Compliance Posture in AgenticOps on page 15
- Introducing Policy Change Impact Analyzer in AgenticOps on page 15

ASA Secure Client upgrades for MSSP (BETA)

Security Cloud Control now supports Cisco Secure Client package upgrades for ASA Remote Access VPN headends across all of your managed organizations from your manager organization. This support extends centralized upgrade capabilities to ASA RA VPN deployments, including guided upgrade workflows, multi-device package deployment, visibility into currently installed Secure Client packages, compatibility-based version selection, platform-specific package targeting for Windows, macOS, and Linux, and real-time upgrade status monitoring from the Upgrades page.

Security Cloud Control now supports Cisco Secure Client package upgrades for ASA Remote Access VPN headends across all of your managed organizations from your manager organization. This support extends centralized upgrade capabilities to ASA RA VPN deployments, including guided upgrade workflows, multi-device package deployment, visibility into currently installed Secure Client packages, compatibility-based version selection, platform-specific package targeting for Windows, macOS, and Linux, and real-time upgrade status monitoring from the Upgrades page.

For more information, refer to Upgrade ASA Secure Client packages.

Introducing Compliance Posture in AgenticOps

AgenticOps now includes Compliance Posture, a capability that evaluates firewall configurations against PCI DSS 4.0.1 requirements. Identify configuration gaps and potential policy issues, generate detailed compliance reports for your devices, and review findings and remediation recommendations to prioritize corrective actions.

AgenticOps now includes Compliance Posture, a capability that evaluates firewall configurations against PCI DSS 4.0.1 (Payment Card Industry Data Security Standard) requirements. Identify configuration gaps and potential policy issues, generate detailed compliance reports for your devices, and review findings and remediation recommendations to prioritize corrective actions.

Compliance Posture is available for deployments in the US, EU, and AUS regions. For more information, see About compliance insights.

Introducing Policy Change Impact Analyzer in AgenticOps

AgenticOps now includes Policy Change Impact Analyzer, helping you assess the potential impact of pending access-control policy changes before deployment. Analyze affected devices, rules, traffic segments, historical connection activity, and inferred impacts to identify possible threat exposure, service disruption, access expansion, or improved security posture.

AgenticOps now includes Policy Change Impact Analyzer, helping you assess the potential impact of pending access-control policy changes before deployment. Analyze affected devices, rules, traffic segments, historical connection activity, and inferred impacts to identify possible threat exposure, service disruption, access expansion, or improved security posture.

Policy Change Impact Analyzer is available for deployments in the US, EU, and AUS regions. For more information, see About policy change impact insights.

Introducing Agent Workforce in Security Cloud Control

Agent Workforce is now available in Security Cloud Control. It provides specialized agents that help you analyze firewall data, troubleshoot site-to-site VPN connectivity, and remediate high-bandwidth traffic affecting firewall performance and stability.

Agent Workforce is now available in Security Cloud Control. It provides specialized agents that help you analyze firewall data, troubleshoot site-to-site VPN connectivity, and remediate high-bandwidth traffic affecting firewall performance and stability.

- **Firewall insight agent**: Analyzes firewall inventory, configurations, policies, routing, and device status.
- **VPN agent**: Troubleshoots site-to-site VPN connectivity, routing, and traffic-flow issues.
- **Elephant flow agent:** Remediates high-bandwidth traffic flows affecting firewall performance and stability.

Agent Workforce capabilities are available for deployments in the US, EU, and AUS regions. For more information, see Agent Workforce.

Sep 10, 2026

New features and improvements deployed on September 10, 2026 in Security Cloud Control Firewall Management.

This is the new feature deployed on September 10, 2026 in Security Cloud Control Firewall Management.

- Secure Client upgrades for ASA Remote Access VPN on page 16

Secure Client upgrades for ASA Remote Access VPN

Security Cloud Control now supports Cisco Secure Client package upgrades for ASA Remote Access VPN head-ends. This support extends centralized upgrade capabilities to ASA RA VPN deployments, including guided upgrade workflows, multi-device package deployment, visibility into currently installed Secure Client packages, compatibility-based version selection, platform-specific package targeting for Windows, macOS, and Linux, and real-time upgrade status monitoring from the Upgrades page.

Security Cloud Control now supports Cisco Secure Client package upgrades for ASA Remote Access VPN head-ends. This support extends centralized upgrade capabilities to ASA RA VPN deployments, including guided upgrade workflows, multi-device package deployment, visibility into currently installed Secure Client packages, compatibility-based version selection, platform-specific package targeting for Windows, macOS, and Linux, and real-time upgrade status monitoring from the Upgrades page.

For more information, see to Upgrade ASA Secure Client packages.

Sep 3, 2026

New features and improvements deployed on September 3, 2026 in Security Cloud Control Firewall Management.

This is the new feature deployed on September 3, 2026 in Security Cloud Control Firewall Management.

- Security Cloud Control Firewall Management automation tools and AI skills on page 16

Security Cloud Control Firewall Management automation tools and AI skills

Manage and automate Security Cloud Control Firewall Management using a simple CLI and Cisco Ansible collection. Built in AI skills help coding agents find the right commands and modules, validate inputs, handle authentication safely, and verify results. This makes Firewall Management workflows faster, safer, and easier to automate.

Manage and automate Security Cloud Control Firewall Management using a simple CLI and Cisco Ansible collection. Built in AI skills help coding agents find the right commands and modules, validate inputs, handle authentication safely, and verify results. This makes Firewall Management workflows faster, safer, and easier to automate.

For more information, refer to Automation tools and AI agents.

Aug 6, 2026

New features and improvements deployed on August 6, 2026 in Security Cloud Control Firewall Management.

This is the new feature deployed on August 6, 2026 in Security Cloud Control Firewall Management.

- Software Upgrade Planner now highlights bugs impacting your device on page 16

Software Upgrade Planner now highlights bugs impacting your device

Software Upgrade Planner now separates bugs into **Impacting bugs** and **Other bugs** on the device details page. Impacting bugs are identified as affecting the selected device and its environment. This helps you focus on the bugs most relevant to the device when reviewing software upgrade options.

Software Upgrade Planner now separates bugs into **Impacting bugs** and **Other bugs** on the device details page. Impacting bugs are identified as affecting the selected device and its environment. This helps you focus on the bugs most relevant to the device when reviewing software upgrade options.

For more information, refer to Manage software upgrades.

Jul 31, 2026

New features and improvements deployed on July 31, 2026 in Security Cloud Control Firewall Management.

This is the new feature deployed on July 31, 2026 in Security Cloud Control Firewall Management.

- Network Address Translation policy analysis

NAT policy anomaly analysis for Firewall Threat Defense devices

Policy Analyzer and Optimizer now identifies shadowed and redundant NAT rules for Firewall Threat Defense devices, with anomaly details and PDF reports for audit and compliance.

Policy Analyzer and Optimizer now provides visibility into Network Address Translation (NAT) policy anomalies for Firewall Threat Defense devices managed by Cloud-Delivered Firewall Management Center or On-Premises Firewall Management Center. This feature enables users to identify shadowed and redundant NAT rules, analyze anomaly details, and generate comprehensive PDF reports for audit and compliance.

For more information, refer to Network Address Translation policy analysis.

Jul 24, 2026

New features and improvements deployed on July 24, 2026 in Security Cloud Control Firewall Management.

These are the new features and improvements deployed on July 24, 2026 in Security Cloud Control Firewall Management.

- Introducing Capacity and Trend Analyzer
- AgenticOps support for On-Premises Firewall Management Center
- Enhanced Software Upgrade Planner with remediation guidance and threat campaign insights

Introducing Capacity and Trend Analyzer

Capacity and Trend Analyzer helps you proactively monitor infrastructure health by analyzing CPU, memory, throughput, and connection trends. Use anomaly detection and predictive forecasting to identify potential capacity risks, receive alerts for threshold breaches, and plan for future resource demands.

Capacity and Trend Analyzer helps you proactively monitor infrastructure health by analyzing CPU, memory, throughput, and connection trends. Use anomaly detection and predictive forecasting to identify potential capacity risks, receive alerts for threshold breaches, and plan for future resource demands.

For more information, see Capacity and Trend Analyzer

AgenticOps support for On-Premises Firewall Management Center

AgenticOps now supports Firewall Threat Defense devices managed by an On-Premises Firewall Management Center integrated with Cisco Security Cloud. This support extends AgenticOps features, including Capacity and Trend Analyzer, Software Upgrade Planner, Best Practices and Recommendations, and Feature Adoption, to your on-prem managed devices.

AgenticOps now supports Firewall Threat Defense devices managed by an On-Premises Firewall Management Center integrated with Cisco Security Cloud. This support extends AgenticOps features, including Capacity and Trend Analyzer, Software Upgrade Planner, Best Practices and Recommendations, and Feature Adoption, to your on-prem managed devices.

For information about supported versions of the on-prem Firewall Management Center, see AgenticOps Support for On-Prem Firewall Management Center.

Enhanced Software Upgrade Planner with remediation guidance and threat campaign insights

Software Upgrade Planner now provides remediation guidance with AI-generated summaries for security vulnerabilities and bugs, helping you understand root causes, available workarounds, and remediation guidance. It also highlights active threat campaigns affecting your devices and links to Cisco Talos Intelligence resources for additional context, enabling you to make more informed upgrade decisions.

Software Upgrade Planner now provides remediation guidance with AI-generated summaries for security vulnerabilities and bugs, helping you understand root causes, available workarounds, and remediation guidance. It also highlights active threat campaigns affecting your devices and links to Cisco Talos Intelligence resources for additional context, enabling you to make more informed upgrade decisions.

For more information, see About software upgrade insights.

Jun 5, 2026

New features and improvements deployed on June 5, 2026 in Security Cloud Control Firewall Management.

These are the new features and improvements deployed on June 5, 2026 in Security Cloud Control Firewall Management.

- Updates to Cloud-delivered Firewall Management Center

Updates to Cloud-delivered Firewall Management Center

This document lists updates to the Cloud-Delivered Firewall Management Center.

Security Cloud Control Firewall Management released an update to the Cloud-Delivered Firewall Management Center. For more information, read Release Notes for Cloud-Delivered Firewall Management Center.

May 8, 2026

New features and improvements deployed on May 8, 2026 for managed service providers and users of multi-organizations in Security Cloud Control.

New features and improvements deployed on May 8, 2026 for managed service providers and users of multi-organizations in Security Cloud Control.

- Multitenant Device Upgrades Now Available for ASAs

Multitenant Device Upgrades Now Available for ASAs

You can now bulk upgrade ASAs across multiple tenants in addition to performing bulk upgrades for Cloud-Delivered Firewall Management Center-managed Secure Firewall Threat Defense devices.

You can now bulk upgrade ASAs across multiple tenants in addition to performing bulk upgrades for Cloud-Delivered Firewall Management Center-managed Secure Firewall Threat Defense devices.

For more information, see About device upgrades.

Apr 24, 2026

New features and improvements deployed on April 24, 2026 in Security Cloud Control Firewall Management.

These are the new features and improvements deployed on April 24, 2026 in Security Cloud Control Firewall Management.

- Simplify Your Multicloud Security Setup with Cloud Deployment.
- Updates to Cloud-Delivered Firewall Management Center.

Simplify Your Multicloud Security Setup with Cloud Deployment

The new Cloud Deployment feature streamlines the configuration of Cisco Secure Firewall Threat Defense Virtual (FTDv) and Multicloud Defense across Amazon Web Services (AWS), Azure, and Google Cloud Platform (GCP). Additionally, Oracle Cloud Infrastructure (OCI) is supported in this release by Multicloud Defense gateway only. This guided configuration tool helps you select and launch the optimal enforcement point for your specific use case, ensuring high performance and scalable network security in complex multicloud environments. With its simplified, step-by-step setup, Cloud Deployment lets you define account settings, traffic flows, and architectural requirements with ease.

The new Cloud Deployment feature streamlines the configuration of Cisco Secure Firewall Threat Defense Virtual (FTDv) and Multicloud Defense across Amazon Web Services (AWS), Azure, and Google Cloud Platform (GCP). Additionally, Oracle Cloud Infrastructure (OCI) is supported in this release by Multicloud Defense gateway only. This guided configuration tool helps you select and launch the optimal enforcement point for your specific use case, ensuring high performance and scalable network security in complex multicloud environments. With its simplified, step-by-step setup, Cloud Deployment lets you define account settings, traffic flows, and architectural requirements with ease.

For more information, see Cloud Deployment.

Updates to Cloud-delivered Firewall Management Center

Provides the list of new updates to the Cloud-delivered Firewall Management Center.

Security Cloud Control Firewall Management released an update to the Cloud-delivered Firewall Management Center. Read the Release Notes for Cloud-Delivered Firewall Management Center for more information.

Mar 27, 2026

New features and improvements deployed on March 27, 2026 in Security Cloud Control Firewall Management and Security Cloud Control.

These are the new features and improvements deployed on March 27, 2026 in Security Cloud Control Firewall Management and Security Cloud Control.

- Firewall MSP Portal Now Integrated into Security Cloud Control.

Firewall MSP Portal Now Integrated into Security Cloud Control

The Security Cloud Control Multi-Org view is designed for enterprises that need to manage multiple organizations for a single company. It is now also available for managed service providers who need to manage multiple organizations for different companies.

The Managed Service Provider (MSP) portal is now fully integrated into Security Cloud Control's Multi-Org experience. This unified platform empowers managed service providers to efficiently manage multiple customer organizations from a single, centralized interface.

Key capabilities include:

- Centralized management: Seamlessly manage multiple customer organizations within one portal.
- Comprehensive monitoring: Monitor device health, configurations, and connectivity status across all managed environments.

- Bulk upgrades: Perform upgrades on Secure Firewall Threat Defense devices managed by the Cloud-Delivered Firewall Management Center (cdFMC) across all tenants.
- Enhanced visibility: Access detailed, consolidated information for all managed firewall organizations.

What this means for you:

- Access: Use the new portal directly from security.cisco.com
- Legacy Portal Retirement: The previous MSP portal will be retired soon.
- Support: Going forward, support will be provided exclusively for the integrated Security Cloud Control platform.

For more information, see Overview of Security Cloud Control Firewall Management for Managed Service Providers.

Mar 13, 2026

New features and improvements deployed on March 13, 2026 in Security Cloud Control Firewall Management.

These are the new features and improvements deployed on March 13, 2026 in Security Cloud Control Firewall Management.

- New Smart Licensing Dashboard on page 20
- New Smart Licensing Dashboard for MSSP Portal on page 20

New Smart Licensing Dashboard

Smart Licensing Dashboard has been introduced in Cisco Secure Firewall. This dashboard offers a unified view of license usage, license types, and compliance status, helping you ensure that your devices are licensed and remain compliant. This feature is currently available in limited release. To request access to this limited release feature, please contact your account team or Cisco representative.

Smart Licensing Dashboard has been introduced in Cisco Secure Firewall. This dashboard offers a unified view of license usage, license types, and compliance status, helping you ensure that your devices are licensed and remain compliant. This feature is currently available in limited release. To request access to this limited release feature, please contact your account team or Cisco representative.

For more information, see Overview of Smart Licensing Dashboard.

New Smart Licensing Dashboard for MSSP Portal

Smart Licensing Dashboard has been introduced in the MSSP Portal for Cisco Secure Firewall. This dashboard offers a unified view of license usage, license types, and compliance status, helping you ensure that your devices are licensed and remain compliant. This feature is currently available in limited release. To request access to this limited release feature, please contact your account team or Cisco representative.

Smart Licensing Dashboard has been introduced in the MSSP Portal for Cisco Secure Firewall. This dashboard offers a unified view of license usage, license types, and compliance status, helping you ensure that your devices are licensed and remain compliant. This feature is currently available in limited release. To request access to this limited release feature, please contact your account team or Cisco representative.

For more information, see Overview of Smart Licensing Dashboard.

Jan 30, 2026

New features and improvements deployed on January 30, 2026 in Security Cloud Control Firewall Management.

These are the new features and improvements deployed on January 30, 2026 in Security Cloud Control Firewall Management.

- Multitenant Device Upgrades in MSSP Portal on page 21

Multitenant Device Upgrades in MSSP Portal

With the new upgrades view in the MSSP portal, you can now bulk upgrade Secure Firewall Threat Defense devices managed by Cloud-Delivered Firewall Management Center (cdFMC) across multiple tenants.

With the new upgrades view in the MSSP portal, you can now bulk upgrade Secure Firewall Threat Defense devices managed by Cloud-Delivered Firewall Management Center (cdFMC) across multiple tenants.

For more information, see About Multitenant Device Upgrades in MSSP Portal.

Dec 12, 2025

New features and improvements deployed on December 12, 2025 in Security Cloud Control Firewall Management.

These are the new features and improvements deployed on December 12, 2025 in Security Cloud Control Firewall Management.

- Updates to Cloud-Delivered Firewall Management Center
- Introducing Security Insights in AIOps

Updates to Cloud-delivered Firewall Management Center

Provides the list of new updates to the Cloud-delivered Firewall Management Center.

Security Cloud Control Firewall Management released an update to the Cloud-delivered Firewall Management Center. Read the Release Notes for Cloud-Delivered Firewall Management Center for more information.

Introducing Security Insights in AIOps

Security Insights offers enhanced visibility into suspicious activities within your organization.

In this release, we have introduced **Security** insights to provide visibility into suspicious activities across your organization. You can now identify and respond to evolving security risks, such as **User Risk Spike**, which indicates escalating trust levels and other suspicious user behavior.

See View AIOps Dashboard.

Dec 4, 2025

New features and improvements deployed on December 04, 2025 in Security Cloud Control Firewall Management.

These are the new features and improvements deployed on December 04, 2025 in Security Cloud Control Firewall Management.

- New Health Dashboard for MSSP Portal

New Health Dashboard for MSSP Portal

Provides a health dashboard for Secure Firewall ASA devices to display critical performance indicators.

In this release, a Health dashboard is introduced for Secure Firewall ASA devices.

This dashboard displays critical performance indicators such as CPU, memory, disk usage, and interface statistics. You can now detect performance bottlenecks early and take proactive actions to maintain optimal operations.

For more information, see About Health Dashboard in the MSSP Portal.

Nov 20, 2025

New features and improvements deployed on November 20, 2025 in Security Cloud Control Firewall Management.

These are the new features and improvements deployed on November 20, 2025 in Security Cloud Control Firewall Management.

- Updates to Cloud-Delivered Firewall Management Center

Updates to Cloud-Delivered Firewall Management Center

Provides the list of new updates to the Cloud-Delivered Firewall Management Center.

Security Cloud Control Firewall Management released an update to the Cloud-Delivered Firewall Management Center. Read the Release Notes for Cloud-Delivered Firewall Management Center for more information.

Nov 14, 2025

New features and improvements deployed on November 14, 2025 in Security Cloud Control Firewall Management.

These are the new features and improvements deployed on November 14, 2025 in Security Cloud Control Firewall Management.

- MSSP Device Upgrades Using Public APIs

MSSP Device Upgrades Using Public APIs

Provides the list of new updates to the MSSP device upgrades using public APIs.

Security Cloud Control Firewall Management now provides new API endpoints for MSSPs to upgrade Secure Firewall Threat Defense devices across their tenants. An MSSP portal is required for this.

For more information, see Security Cloud Control Firewall Management API Documentation.

Nov 6, 2025

New features and improvements deployed on November 06, 2025 in Security Cloud Control Firewall Management.

These are the new features and improvements deployed on November 06, 2025 in Security Cloud Control Firewall Management.

- Security Cloud Control Now Manages Catalyst SD-WAN NGFW features
- Introducing Tiered Subscription Model for Cisco Security Analytics and Logging

Security Cloud Control Now Manages Catalyst SD-WAN NGFW features

Provides new updates on Catalyst SD-WAN NGFW features.

Security Cloud Control now integrates with Catalyst SD-WAN Manager, enabling you to centrally manage next-generation firewall (NGFW) features, including security policies and objects managed by Catalyst SD-WAN Manager.

With Security Analytics and Logging, you gain visibility into network activity, making it easy to monitor, analyze, and respond to security events. You can also view allowed and blocked intrusion and malware events detected in your network.

For more information, see Managing Cisco Catalyst SD-WAN Firewall Capabilities with Security Cloud Control.

Introducing Tiered Subscription Model for Cisco Security Analytics and Logging

Provides the list of new updates to Cisco Security Analytics and Logging licensing.

In this release, we have updated Cisco Security Analytics and Logging licensing to offer a new tiered subscription model. This new structure provides a longer default retention period, starting at 1 year, and increased storage options up to 10 TB. You can choose from Essentials, Advantage, or Premier tiers to match your specific needs. This update simplifies pricing and provides you with greater flexibility and value in managing your firewall logs.

For more information, see Cisco Security Analytics and Logging Licenses.

Oct 23, 2025

New features and improvements deployed on October 23, 2025 in Security Cloud Control Firewall Management.

These are the new features and improvements deployed on October 23, 2025 in Security Cloud Control Firewall Management.

- CLI Support for Firewall Threat Defense Devices Managed byCloud-Delivered Firewall Management Center

CLI Support for Firewall Threat Defense Devices Managed by Cloud-delivered Firewall Management Center

Provides new updates about CLI support for Firewall Threat Defense devices managed by Cloud-delivered Firewall Management Center.

You can now access the CLI of Firewall Threat Defense devices managed by Cloud-delivered Firewall Management Center, through the Security Cloud Control interface. Navigate to **Security Devices** > **FTD**, select the FTD, and choose **Command Line Interface** on the right pane.

For more information, see Use the Security Cloud Control Command Line Interface Tool.

Sep 18, 2025

New features and improvements deployed on September 18, 2025 in Security Cloud Control Firewall Management.

These are the new features and improvements deployed on September 18, 2025 in Security Cloud Control Firewall Management.

- Introducing New AIOps Capabilities on page 23
- Introducing Device Health Metrics for Secure Firewall ASA Devices on page 24

Introducing New AIOps Capabilities

Provides the list of new updates to AIOps.

AIOps brings AI-driven intelligence to firewall management, delivering proactive insights and actionable guidance to simplify operations and strengthen security.

New capabilities include:

- AIOps Summary Dashboard: A unified view that consolidates insights, giving you a clear snapshot of your device's performance.
- Best Practices and Recommendations: Detailed assessments that highlight deviations from best practices and provide remediation guidance.
- Feature Adoption: Visibility into actively used features categorized by licenses, adoption rates across the tenant, and guidance to improve utilization.
- Software Upgrade Planner: Suggestions on the most suitable upgrade versions for Secure Firewall Threat Defense devices, including visibility into resolved bugs and security vulnerabilities, to streamline upgrade decisions.

These enhancements add to the existing capabilities such as the Policy Analyzer and Optimizer, positioning AIOps as the central hub for proactive and efficient firewall management.

Introducing Device Health Metrics for Secure Firewall ASA Devices

Provides new updates on device health metrics for Secure Firewall ASA

In this release, we have introduced the Device Health Metrics for Secure Firewall ASA. The dashboard displays critical performance indicators such as CPU, memory, disk usage, fan status, and interface statistics. With this visibility, you can detect performance bottlenecks and take proactive action to maintain optimal operations.

For more information, refer to Device Health Metrics.

Aug 21, 2025

New features and improvements deployed on August 21, 2025 in Security Cloud Control Firewall Management.

These are the new features and improvements deployed on August 21, 2025 in Security Cloud Control Firewall Management.

- Security Cloud Control Firewall Management Now Manages Catalyst SD-WAN NGFW Features
- Security Cloud Control Firewall Management Notifications in Microsoft Teams

Security Cloud Control Firewall Management Now Manages Catalyst SD-WAN NGFW Features

Security Cloud Control Firewall Management now integrates with Catalyst SD-WAN Manager.

Security Cloud Control Firewall Management now integrates with Catalyst SD-WAN Manager, enabling you to centrally manage next-generation firewall (NGFW) features, including security policies and objects managed by Catalyst SD-WAN Manager.

With Security Analytics and Logging, you gain visibility into network activity, making it easy to monitor, analyze, and respond to security events. You can also view allowed and blocked intrusion and malware events detected in your network.

For more information, refer to Managing Cisco Catalyst SD-WAN Firewall Capabilities with Security Cloud Control.

Security Cloud Control Firewall Management Notifications in Microsoft Teams

Now you can get Security Cloud Control Firewall Management notifications in Microsoft Teams, generate an incoming webhook in Teams, and enter the webhook URL in Security Cloud Control Firewall Management.

To get Security Cloud Control Firewall Management notifications in Microsoft Teams, generate an incoming webhook in Teams and enter the webhook URL in Security Cloud Control Firewall Management (**Administration** > **Notification Settings**).

For more information, refer to Incoming Webhooks for Microsoft Teams.

Aug 14, 2025

New features and improvements deployed on August 14, 2025 in Security Cloud Control Firewall Management.

These are the new features and improvements deployed on August 14, 2025 in Security Cloud Control Firewall Management.

- Updates to Cloud-Delivered Firewall Management Center

Updates to Cloud-Delivered Firewall Management Center

Provides the list of updates to Cloud-Delivered Firewall Management Center.

Security Cloud Control released an update to the Cloud-Delivered Firewall Management Center. Read the Release Notes for Cloud-Delivered Firewall Management Center for more information.

Jul 23, 2025

New features and improvements deployed on July 23, 2025 in Security Cloud Control Firewall Management.

These are the new features and improvements deployed on July 23, 2025 in Security Cloud Control Firewall Management.

- Security Cloud Control Firewall Management Video
- MSSP Portal: Enhanced Pagination and Sorting of Security Devices
- Updates to Security Cloud Control Firewall Manager APIs
- Updates to the Event Log Search Feature
- Updates to the Cloud-Delivered Firewall Management Center Device Backups

Security Cloud Control Firewall Management Video

A new video presentation providing an overview of the Firewall manager in Security Cloud Control is available on YouTube.

A new video presentation providing an overview of the Firewall manager in Security Cloud Control is available on YouTube https://www.youtube.com/watch?v=iwKW3tfZS_M in the Cisco Secure Firewall channel.

This video may be of special interest to customers of Cisco Defense Orchestrator who were migrated to the Security Cloud Control platform. The video orients users to these ares of the Firewall manager:

- Firewall Management navigation
- Objects
- Policies
- Security Devices
- Integrations
- User Management

MSSP Portal: Enhanced Pagination and Sorting of Security Devices

The **Security Devices** page in the MSSP portal now includes dedicated tabs for **Devices**, **Cloud Services**, **Templates**, and **Firewall Managers**.

The **Security Devices** page in the MSSP portal now includes dedicated tabs for **Devices**, **Cloud Services**, **Templates**, and **Firewall Managers**. This enhancement improves page performance and streamlines pagination and filtering, enabling a more efficient management of your security assets.

For more information, refer to Security Devices Details.

Updates to Security Cloud Control Firewall Manager APIs

The Security Cloud Control Firewall Manager APIs have been updated to add multiple new API endpoints to collect and view health metrics for ASA devices and view MSSP portal inventory.

The Security Cloud Control Firewall Manager APIs have been updated to add multiple new API endpoints to collect and view health metrics for ASA devices and view MSSP portal inventory.

Updates to the Event Log Search Feature

The **Background Search** button in the **Event Logging** page has been renamed to **Reports**.

The **Background Search** button in the **Event Logging** page has been renamed to **Reports**. The button's functionality remains the same, allowing you to perform event log searches in the background and manage generated reports.

For more information, refer to Search Historical Events in the Background.

Updates to the Cloud-delivered Firewall Management Center Device Backups

From the next upgrade of Cloud-delivered Firewall Management Center, only the five most recent Firewall Threat Defense backups will be retained; all older backups will be automatically deleted.

From the next upgrade of Cloud-delivered Firewall Management Center, only the five most recent Firewall Threat Defense backups will be retained; all older backups will be automatically deleted.

In the event that you have not downloaded the required backups to your private environment following our announcement on May 1, 2025, download the necessary backups before July 31, 2025, to ensure continuous access to your data.

See Restore a Firewall Firewall Threat Defense device for information on how to download device backups.

Jul 3, 2025

New features and improvements deployed on July 3, 2025 in Security Cloud Control Firewall Management.

These are the new features and improvements deployed on July 3, 2025 in Security Cloud Control Firewall Management.

- Updates to Cloud-Delivered Firewall Management Center
- Updates to Firewall Migration Tool
- Enhanced Event Searching with Sample Filters

Updates to Cloud-Delivered Firewall Management Center

Provides the list of new updates to the Cloud-Delivered Firewall Management Center.

Security Cloud Control Firewall Management released an update to the Cloud-delivered Firewall Management Center. Read the Release Notes for Cloud-delivered Firewall Management Center for more information.

Updates to Firewall Migration Tool

Provides the list of new updates to Secure Firewall Migration Tool.

Security Cloud Control Firewall Management released an updated version of the Secure Firewall Migration Tool. The key updates include Azure firewall migration to Threat Defense, Checkpoint and Fortinet firewall migrations to Multicloud Defense, simplified policy management, and more. Refer to Cisco Secure Firewall Migration Tool Release Notes for more information.

Enhanced Event Searching with Sample Filters

Security Cloud Control Firewall Management has now introduced sample filters in the Event Logging page to enhance your search experience.

Security Cloud Control Firewall Management introduced sample filters in the Event Logging page to enhance your search experience. These filters instantly populate the search bar with common search queries. This reduces the need to manually type search queries. Simply select a sample filter and edit the search parameters to suit your specific needs. See Use Sample Filters for more information.

Jun 12, 2025

New features and improvements deployed on June 12, 2025 in Security Cloud Control Firewall Management.

These are the new features and improvements deployed on June 12, 2025 in Security Cloud Control Firewall Management.

- Cisco Security Cloud Control Integrated Platform is Now Available
- Simplified Site-to-Site VPN Wizard
- New Widgets in Storage Utilization Dashboard

Cisco Security Cloud Control Integrated Platform is Now Available

Security Cloud Control integrated platform is now available and the Cisco Security Cloud Control tenants from APJ, AUS, the EU, India, and the U.S. have been migrated to it.

We are excited to announce the migration of Cisco Security Cloud Control tenants from APJ, AUS, the EU, India, and the U.S. to the Cisco Security Cloud Control integrated platform.

To access the Security Cloud Control integrated platform, go to https://security.cisco.com/ and navigate to **Products > Firewall** from the homepage.

Note that you can continue to access all your current firewall settings and configurations from the **Firewall** dashboard in the Security Cloud Control integrated platform.

Simplified Site-to-Site VPN Wizard

Security Cloud Control now features an enhanced, consolidated wizard designed to simplify and accelerate the creation of site-to-site VPN tunnels.

The Security Cloud Control now features an enhanced, consolidated wizard designed to simplify and accelerate the creation of site-to-site VPN tunnels. With this intuitive, step-by-step guided wizard, you can seamlessly configure and manage multiple VPN connections in just a few clicks. The VPN tunnel creation is supported for Secure Firewall ASA, Cloud-Delivered Firewall Management Center-managed Firewall Threat Defense, Multicloud Defense, and extranet devices, providing a centralized and streamlined approach to VPN management.

For more information, see Introduction to Site-to-Site Virtual Private Network.

New Widgets in Storage Utilization Dashboard

New widgets to help you identify logging trends and manage storage effectively are available in the optimized version of SAL event logging.

We've introduced new widgets to help you identify logging trends and manage storage effectively. Note that these widgets are available only if you are using the optimized version of SAL event logging.

- EPS Trends for tracking event ingest rates.
- Utilization by Event Type and Device Type Trends for monitoring storage usage patterns.
- Utilization by Device Trends, which highlights storage usage of the top devices.

For more information, see View Security Analytics and Logging Storage Usage and Event Ingest Rate.

3 Mesh Policy Engine

Topics:

- Nov 10, 2026
- Mar 13, 2026
- Feb 25, 2026

Mesh Policy Engine is a policy management and automation service in Security Cloud Control.

Mesh Policy Engine is a centralized, intent-based policy automation service in Security Cloud Control. It translates your intent-based access requests into specific, outcome-driven firewall policy rules and places them correctly in your network. UsingMesh Policy Engine, you can orchestrate and manage your network policies across heterogeneous firewall environments. See *Security Cloud Control: Mesh Policy Engine* for more information.

Nov 10, 2026

Mesh Policy Engine features released on Novenber 10, 2026.

This section lists new features for Mesh Policy Engine.

- Reinvented Mesh Policy Engine on page 31
- Hierarchical policy on page 31
- Secure Access support on page 31
- Rules and objects pushed to the enforcer match the authored rules on page 32

Reinvented Mesh Policy Engine

An all new version with better integration with Cisco enforcers, hierarchical policy, and integration with Common Objects and Audit Logs.

The new version of Mesh Policy Engine integrates more closely with Cisco enforcers. You can organize policies in a hierarchy and use Common Objects and Audit Logs as you manage policy.

For more information, refer to Introduction to Mesh Policy Engine.

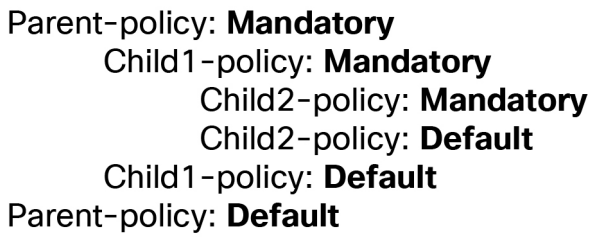
Hierarchical policy

The Mandatory sections are evaluated in order from parent to child. The Default sections are evaluated in reverse order, from child to parent. For Firewall Threat Defense and Secure Access, the mesh policy acts as the parent policy to the existing policy for each enforcer.

Policy hierarchy (parent and child policies) works with Mandatory and Defualt rules sections. With hierarchy:

1. The Mandatory sections are evaluated in order from parent to child.
2. The Default sections are evaluated in reverse order, from child to parent.

Figure 2: Mandatory and Default section evaluation order



For Firewall Threat Defense and Secure Access, the mesh policy acts as the parent policy to the existing policy for each enforcer.

For more information, refer to Policy hierarchy.

Secure Access support

You can now share policy with Secure Access.

You can now share policy with Secure Access. Secure Access supports rules from a network object to a network object and/or service object.

The mesh policy acts as the parent policy to the existing policy in Secure Access. Mesh policy is hierarchical: Mandatory sections are evaluated in order from parent to child, and Default sections are evaluated in reverse order, from child to

parent. The mesh policy Mandatory rules are evaluated first, then the existing Secure Access rules, and finally the mesh policy Default rules.

Rules and objects pushed to the enforcer match the authored rules

Formerly, rules were compressed and optimized. Now what you see is what you get.

Previously, Mesh Policy Engine compressed and optimized rules before sending them to enforcers. Now enforcers receive rules and objects that match what you authored.

For more information, refer to Deploy policy changes to enforcers.

Mar 13, 2026

Mesh Policy Engine features released on March 13, 2026.

This section lists new features for Mesh Policy Engine.

- Manage Credentials page on page 32

Manage Credentials page

You can now add credentials through the Mesh Policy Engine GUI. To securely connect to the install targets, Mesh Policy Engine must authenticate the install targets using their credentials.

You can now add credentials through the GUI. To securely connect to the install targets, Mesh Policy Engine must authenticate the install targets using their credentials. Create a local copy of your credentials using JSON. Each credential is a reusable object that you can use for one or more install targets by name. This page lets you upload all of your credentials in bulk. If you want to update a credential, you need to paste in the complete credential set; Mesh Policy Engine replaces any existing credentials with the ones you upload.

Feb 25, 2026

Mesh Policy Engine features released on February 25, 2026.

This section lists new features for Mesh Policy Engine.

- Capabilities of Mesh Policy Engine on page 32

Capabilities of Mesh Policy Engine

Mesh Policy Engine is a centralized, intent-based policy automation service within Security Cloud Control.

Mesh Policy Engine is a centralized, intent-based policy automation feature within Security Cloud Control. Its primary capabilities include:

- Multi-vendor policy orchestration—Supports a diverse range of enforcement points, including Cisco Secure Firewall (ASA and Firewall Threat Defense), Palo Alto Networks, Fortinet, Juniper, and AMD Pensando DPUs. It uses vendor-supported APIs to write policies directly to non-Cisco devices.
- Intent-based policy translation—Instead of manually writing complex firewall rules, you define your intent (e.g., "App A needs to talk to App B"). Mesh Policy Engine translates your intent into specific, outcome-based rules and places them correctly across your network.
- Comprehensive policy ingestion—Ingests existing policy and enforcement state from managed security devices, ensuring that legacy rules are maintained and integrated with new intent-based policies.

- Dynamic object and group management—Supports static IPv4 objects and dynamic objects. When you update dynamic objects using the APIs, Mesh Policy Engine updates the relevant policies automatically.
- Advanced rule ordering and optimization—Categorizes rules into Priority, Core, and Default to influence ordering, and removes overlapping or duplicate rules before deployment.
- Topology-aware policy deployment—You define the relationships between objects and enforcement points, and Mesh Policy Engine uses this topology to deploy policies only to devices relevant to the traffic path, avoiding unnecessary policies on other devices.
- Robust lifecycle management:
  - Every change is versioned, allowing for historical comparisons and rollbacks.
  - Detailed records track what was changed, when, and by whom.
  - RESTful APIs enable you to integrate Mesh Policy Engine into CI/CD workflows with tools such as Terraform or Ansible.

See *Security Cloud Control: Mesh Policy Engine (Legacy)* for more information.

4 Multicloud Defense

Topics:

- Apr 21, 2026
- Nov 6, 2025
- Jul 31, 2025
- Jun 6, 2025

Describes new software features, enhancements, behavior changes, and product improvements added to Multicloud Defense.

Multicloud Defense provides a simplified and highly automated approach to multicloud security. This solution allows organizations to manage and secure their multicloud environments using a single SaaS delivered control plane, and centralized or distributed PaaS-delivered data plane architectures. Multicloud Defense provides continuous visibility, unified protection and dynamic policy updates across all major cloud providers, thus eliminating the need for separate point solutions for each cloud provider.

In this section, we list new software features, enhancements, behavior changes, and product improvements added to Multicloud Defense.

Apr 21, 2026

Multicloud Defense released new features for Security Cloud Control customers on April 21, 2026:

The following products released new features for Security Cloud Control customers on April 21, 2026.

- See Multicloud Defense Controller Updates on page 35 for more information.

Multicloud Defense Controller Updates

Describes new software features, enhancements, behavior changes, and product improvements added to Multicloud Defense in 2026.

These are the new features released with Multicloud Defense Controller, version 26.04.

- **Firewall Threat Defense virtual (FTDv)** – Provides Next-Generation Firewall functionality to virtualized environments, enabling consistent security policies to follow workloads across your physical, virtual, and cloud environments. You can deploy Firewall Threat Defense Virtual gateway using Multicloud Defense. Azure and GCP require separate gateways for Ingress, and Egress or East-West traffic, whereas AWS utilizes a unified gateway for Ingress, Egress, and East-West traffic. For more information, refer to Cisco Multicloud Defense User Guide.
- **Cloud Deployment**–The Cloud Deployment for the Cisco Secure Firewall Threat Defense Virtual is a wizard which enables easy deployment of virtual firewalls across multicloud and private cloud environments. For more information, refer to Cloud Deployment.

Nov 6, 2025

Multicloud Defense released new features for Security Cloud Control customers on November 6, 2025:

Multicloud Defense released new features for Security Cloud Control customers on November 6, 2025.

See Multicloud Defense Updates in Security Cloud Control on page 35 for more information.

Multicloud Defense Updates in Security Cloud Control

Describes new software features, enhancements, behavior changes, and product improvements added to Multicloud Defense in 2025.

The following features and enhancements are included in this Release Version 25.10 on November 5, 2025:

- **Red Hat Enterprise Linux 9 (RHEL 9) Migration** – Multicloud Defense is now on Red Hat Enterprise Linux 9 (RHEL 9). This is supported on AWS and Azure only. While this migration may likely increase infrastructure costs for some customers, RHEL 9 offers enhanced security against vulnerabilities, with availability of the latest vulnerability patches.
- **Firewall Threat Defense Virtual (FTDv) Support for Azure** – Multicloud Defense now supports Standard_D8s_v5 and Standard_D16s_v5 instance types for FTDv for Azure. The existing instance type will be deprecated. The new instance types offer better performance.
- **Azure Dsv6 Support** – Fixed technical issues related to permissions in the Microsoft Marketplace for Azure Dsv6 instance. Azure Dsv6 is now supported in Multicloud Defense. You can see improved performance, and a likely increase in infrastructure costs as the Azure gateway instance will use Red Hat Enterprise Linux 9 (RHEL 9).
- **Bring Your Own Load Balancer (BYOLB) Support** – Resolved a limitation in Azure that did not allow the configuration of user-defined load balancers due to conflicts in user-configured and managed load balancer policies. You can now customize and enable the floating IP for your load balancer rules and attach the load balancer to the

Multicloud Defense Gateway. This is supported for the 25.08 Gateway release. For more information, see the Cisco Multicloud Defense User Guide.

Jul 31, 2025

New features for Security Cloud Control customers on July 31, 2025.

The following products released new features for Security Cloud Control customers on July 31, 2025.

- Multicloud Defense Updates in Security Cloud Control on page 36

Multicloud Defense Updates in Security Cloud Control

Describes new software features, enhancements, behavior changes, and product improvements added to Multicloud Defensein 2025.

This new feature was released in Multicloud Defense Controller version 25.07

Version 25.07 Multicloud Defense Controller, July 31, 2025

The following feature and enhancements are included in this release:

- **Virtual Network (VNet) flow log support** – Multicloud Defense will support NSG flow logs until it is deprecated by Microsoft Azure. Microsoft Azure is retiring Network Security Group (NSG) flow logs and replacing it with VNet flow logs. Multicloud Defense will continue to support NSG flow logs until it is deprecated, but users will not be able to create new NSG flow logs. Users can create VNet flow logs instead.
- Bug fixes and enhancements.

Jun 6, 2025

New features for Security Cloud Control customers on June 6, 2025.

The following products released new features for Security Cloud Control customers on June 6, 2025.

- Multicloud Defense Controller Updates on page 36

Multicloud Defense Controller Updates

Describes new software features, enhancements, behavior changes, and product improvements added to Multicloud Defensein 2025.

These are the new features released with Multicloud Defense Controller, version 25.05.

- **Secure Firewall Threat Defense Virtual Device Orchestration**. You can now orchestrate, deploy, and register a Secure Firewall Threat Defense Virtual Device (FTDv) using Multicloud Defense. This helps you retain the same firewall that you use for on premises and cloud environments, while managing policies in the same place. Multicloud Defense manages the deployment and makes it easy for you to deploy in the cloud. See the Secure Firewall Threat Defense Virtual documentation for more information.
- **Cloud Explorer** offers a single, unified view to visualize all your resources and their relationships. Cloud Explorer empowers you to build a robust security posture with ease. Using intuitive drag and drop functionality and simple clicks, you can form connections and use protective measures to safeguard your assets. See the Cloud Explorer documentation for more information.

5 SASE Management

Topics:

- Jul 6, 2026
- Mar 27, 2026

SASE Management is Cisco's cloud-delivered security solution designed to simplify and unify your network and security policy management. Available in the Cisco Security Cloud Control portal, SASE Management enables seamless management of your Catalyst SD-WAN infrastructure with Secure Access cloud access rules within a single, integrated platform.

Welcome to **Cisco SASE Management**, a cloud-delivered security solution designed to simplify and unify your network and security policy management. Available in the Cisco Security Cloud Control portal, SASE Management enables seamless management of Secure Internet Access (SIA) and Secure Private Access (SPA) for your **Catalyst SD-WAN** infrastructure and device policy with **Cisco Secure Access** cloud access rules within a single, integrated platform.

This configuration guide is designed to help you quickly adopt and benefit from the Cisco SASE Management solution, delivering a unified, simplified, and secure networking experience. For information about Cisco SASE architecture, see Cisco Secure Access Service Edge (SASE) and Security Service Edge (SSE) Architecture Guide.

Who should use SASE Management

- **Existing Catalyst SD-WAN Customers:** If you already use Catalyst SD-WAN Cloud, SASE Management allows you to extend your capabilities with unified security policy management. For more information, see the Cisco SD-WAN Cloud Guide

  Note

  Modifying your organization's subscription model or tier is not supported once you enable SASE Management.

- **New Secure Access Customers:** New Secure Access Customers: If you are adopting Secure Access capabilities for the first time, SASE Management provides an easy-to-use experience that is integrated with SD-WAN Manager. For more information, see Cisco Secure Access At-a-Glance and Cisco Secure Access Help.

Caution

After a Catalyst SD-WAN organization is linked to SASE Management, it cannot be detached from SASE Management.

Jul 6, 2026

Expore new SASE Management features!

Security Cloud Control now offers enhanced Secure Access Service Edge (SASE) management capabilities designed to improve the onboarding, provisioning, and lifecycle management of SASE services for existing and new customers. See Enhanced SASE Management capabilities on page 39 for more information.

Enhanced SASE Management capabilities

Enhanced Secure Access Service Edge (SASE) management capabilities designed to improve the onboarding, provisioning, and lifecycle management of SASE services for existing and new customers.

Key new features

- **SASE provisioning for existing customers**:

  Existing Secure Access customers in Security Cloud Control can now enable SASE features on existing subscriptions and organizations without reprovisioning.

- **Post-claim SASE enablement options**:

  After you activate your subscription, configure your features and integrations to streamline your SASE Management. To achieve this,

  - Enable or disable SASE features to align with your operational requirements.
  - Attach existing Catalyst SD-WAN instances automatically or via an activation code.
  - Complete user migration and role assignments to finalize your SASE experience.

- **SASE experience reactivation**:

  Reactivating your SASE Management experience is now faster and more reliable. Following a subscription renewal, the system automatically reinstates your prior SASE configuration and role assignments. This update simplifies the recovery process and ensures that your administrative environment is ready for use without additional setup.

- **Improved subscription and tenant management**:

  The system manages multiple subscription scenarios, including organizations with overlapping Secure Access and Firewall Management subscriptions. It uses Secure Access as the primary source to maintain consistent SASE enablement.

- **User experience consistency and messaging**:

  You experience these improvements:

  - A consistent SASE onboarding and enablement process that aligns with existing workflows.
  - The system follows existing processes for user and role selection, tenant attachment, and messaging.
  - The system provides alerts and guidance to help you understand the availability and status of SASE features.

Benefits for Administrators

Security Cloud Control administrators manage SASE services more efficiently while maintaining secure and seamless network access and consistent security policy enforcement across the organization. This is achieved by:

- Simplifying SASE enablement across existing and new Secure Access subscriptions.
- Reducing manual effort through automated tenant attachment and user role migration.

- Getting clear visibility and control over SASE activation and reactivation states.
- Streamlining operational workflows with consistent user interface and messaging.

For more information see the chapter, SASE Management in the Security Cloud Control Administration Guide.

Mar 27, 2026

New features and improvements deployed on March 27, 2026 in SASE Management.

These are the new features and improvements deployed on March 13, 2026 in SASE Management.

- SASE Management with Common Objects on page 40

SASE Management with Common Objects

Cisco's SASE Management integrates Catalyst SD-WAN and Cisco Secure Access into a single, cloud-native management experience integrated with Security Cloud Control.

SASE Management integrates Catalyst SD-WAN and Secure Access into a single, cloud-native management experience integrated with Security Cloud Control.

Who should use SASE Management

- **Existing Catalyst SD-WAN Customers:** If you already use Catalyst SD-WAN Cloud, SASE Management allows you to extend your capabilities with unified security policy management. For more information, see the Cisco SD-WAN Cloud Guide.

> **Note**
>
> Modifying your organization's subscription model or tier is not supported once you enable SASE Management.

- **New Secure Access Customers:** New Secure Access Customers: If you are adopting Secure Access capabilities for the first time, SASE Management provides an easy-to-use experience that is integrated with SD-WAN Manager. For more information, see Cisco Secure Access At-a-Glance and Cisco Secure Access Help.

> **Caution**
>
> After a Catalyst SD-WAN organization is linked to SASE Management, it cannot be detached from SASE Management.

Key benefits

- **Streamlined onboarding:** Easily onboard your Catalyst SD-WAN sites and devices into the SASE fabric through Security Cloud Control, with flexible deployment options and audit logs to track changes.
- **Unified policy management:** Manage Secure Internet Access (SIA) and Secure Private Access (SPA) policies for Catalyst SD-WAN and Secure Access devices from one consolidated interface. This reduces complexity and helps ensure consistent security enforcement across your entire environment.

- **Simplified operations:** Create, modify, deploy, and monitor policies without switching between multiple management tools, saving time, and reducing operational overhead.
- **Common objects:** After SASE Management has been enabled, define network objects once and reuse them across your Catalyst SD-WAN and security policies, improving consistency and reducing errors.
- **Integrated troubleshooting:** Access device and tunnel health information and perform basic troubleshooting directly within the unified platform to quickly resolve issues.

Learn more here:

- SASE Management Administration Guide
- Common Objects and Object Groups

6 Secure Access

Topics:

- Aug 14, 2025
- May 23, 2025

Aug 14, 2025

New features and improvements deployed on August 14, 2025 in Secure Access.

These are the new features and improvements deployed on August 14, 2025 in Secure Access.

- Universal Zero Trust Network Access in Firewall Management and Secure Access on page 43

Universal Zero Trust Network Access in Firewall Management and Secure Access

Introduces universal ZTNA, a secure access solution managed via Security Cloud Control using Firewall Management and Secure Access. It outlines key deployment requirements while referencing the Universal ZTNA Configuration and Solution Guides for detailed implementation and architectural guidance to ensure robust network resource protection.

Universal Zero Trust Network Access (universal ZTNA) is a comprehensive solution that provides secure access to internal network resources based on user identity, trust, and posture. It ensures that access to one application does not implicitly grant access to the entire network, minimizing potential vulnerabilities.

The solution requires Firewall Management (formerly Cisco Defense Orchestrator), and Secure Access, both provisioned on the Security Cloud Control platform. The platform provides a unified secure management plane, simplifying the administration of universal ZTNA policies across the applications.

For configuration details, see Universal Zero Trust Network Access Configuration Guide.

For details about the solution, see Universal Zero Trust Network Access Solution Guide.

May 23, 2025

Secure Access released 5 new AI skills to Security Cloud Control customers on May 23, 2025.

Secure Access released 5 new AI skills to Security Cloud Control customers on May 23, 2025. See Five new AI Assistant skills for Secure Access on page 43

Five new AI Assistant skills for Secure Access

Cisco Secure Access released 5 new AI assistant skills to Security Cloud Control users.

These AI Assistant skills are now available to customers that have integrated Secure Access with Security Cloud Control:

Policy Assistance

Policy assistance is designed to simplify the complex and often time-consuming process of policy creation. Here's what you can expect:

- **Natural language processing**: Administrators can now articulate their intent in plain language, and the system will automatically generate the necessary access control policies.
- **Intelligent Access Inference**: Our AI model intuitively understands whether the policy pertains to Internet or Private Access rules, ensuring accuracy and relevance.
- **Safety First**: To maintain the utmost security, all newly created rules will be disabled by default, giving you full control to review and enable them at your discretion.
- **Efficiency Gains**: Reduce the time you spend on rule creation by up to 70%, so you can focus on strategic tasks that matter.

For more information, see Add Rules with the Cisco Assistant.

Digital Experience Monitoring Assistance

The Digital Experience Monitoring (DEM) is a cutting-edge enhancement that empowers your environment with real time analytics and monitoring capabilities. By integrating AI-driven insights, DEM assistance provides these benefits:

- **Proactive Problem Detection**: Use DEM assistance to quickly inspect the entire endpoint landscape, aggregate available information and quickly identify potential performance issues before the impact becomes significant.
- **Enhanced Visibility**: Gain comprehensive insights into endpoint performance, user experience, enable faster and more informed digital experience troubleshooting and decision-making.
- **Operations at Scale**: Adapt to evolving challenges with scalable AI capabilities that grow alongside your network infrastructure, keep the operational effort under control.

See About Experience Insights for more information.

Troubleshooting Assistance

The AI Assistant for Secure Access is skilled at interpreting prompts to troubleshoot user access to private resources. For more information about how to construct a prompt to make the most of this skill, see Troubleshoot with the Cisco Assistant.

Documentation Assistance

Documentation assistance is designed to streamline the process of finding and understanding documentation, making it easier for Security Admins, Network Administrators, IT Administrators, and other users to quickly get the answers they need related to Secure Access. Here's what you can expect:

- **Instant Answers**: The Documentation Assistant can interpret your questions typed in natural language and provide immediate answers from our extensive Secure Access documentation.
- **Complex Query Handling**: It can manage complex queries that involve looking up multiple documents and pages to deliver comprehensive responses.

See Find Documented Answers with the Cisco Assistant for more information.

7 Secure Workload

Topics:

- 2026
- 2025

Describes new software features, enhancements, behavior changes, and product improvements added to Secure Workload.

Cisco Secure Workload seamlessly delivers zero-trust micro-segmentation across any workload, environment, or location from a single console. With comprehensive visibility into every workload interaction and powerful AI/ML-driven automation, Secure Workload reduces the attack surface by preventing lateral movement, identifies workload behavior anomalies, helps rapidly remediate threats, and continuously monitors policy compliance.

In this section, we list new software features, enhancements and behavior changes that are added to Secure Workload.

2026

Describes new software features, enhancements, behavior changes, and product improvements added to Secure Workload in 2026.

In this section, we list new software features, enhancements and behavior changes that are added to Secure Workload in 2026.

- Secure Workload New Features on page 47

Secure Workload New Features

Describes new software features, enhancements, behavior changes, and product improvements added to Secure Workload in 2026.

Cisco Secure Workload seamlessly delivers zero-trust micro-segmentation across any workload, environment, or location from a single console. With comprehensive visibility into every workload interaction and powerful AI/ML-driven automation, Secure Workload reduces the attack surface by preventing lateral movement, identifies workload behavior anomalies, helps rapidly remediate threats, and continuously monitors policy compliance.

For all Secure Workload features, see the release notes:

- Cisco Secure Workload Release Notes, SaaS Release 4.0.3.13

2025

Describes new software features, enhancements, behavior changes, and product improvements added to Secure Workload in 2025.

In this section, we list new software features, enhancements and behavior changes that are added to Secure Workload in 2025.

- Secure Workload Video Overview on page 47

Secure Workload Video Overview

A new video overview of Cisco Secure Workload in Security Cloud Control is available.

A new video presentation providing an overview of setting up Cisco Secure Workload in Security Cloud Control is available on YouTube Onboard and Configure CSW in the Cisco Secure Workload channel.

The video illustrates these tasks:

- Signing in to Security Cloud Control
- Creating an Organization
- Claiming a Secure Workload Subscription
- Launching Cisco Secure Workload
- Setting up the Secure Workload Dashboard and Scope Tree
- Installing Agents

8 Security Cloud Control Multi-Organizations

Topics:

- Sep 10, 2026
- May 8, 2026
- Mar 27, 2026
- Jan 30, 2026

Describes new software features, enhancements, behavior changes, and product improvements added to the multi-organization view of Security Cloud Control. The multi-organization view designed to support multi-organization users and managed service providers.

Security Cloud Control has new features, enhancements, behavior changes, and product improvements in its multi-organization view. The multi-organization view is designed to support multi-organization users and managed service providers.

Sep 10, 2026

New features and improvements deployed on September 10, 2026 in Multi-Organizations for Managed Service Providers.

These are the new features and improvements deployed on September 10, 2026 in Multi-Organizations for Managed Service Providers.

- ASA Secure Client upgrades for MSSP (BETA) on page 49

ASA Secure Client upgrades for MSSP (BETA)

Security Cloud Control now supports Cisco Secure Client package upgrades for ASA Remote Access VPN headends across all of your managed organizations from your manager organization. This support extends centralized upgrade capabilities to ASA RA VPN deployments, including guided upgrade workflows, multi-device package deployment, visibility into currently installed Secure Client packages, compatibility-based version selection, platform-specific package targeting for Windows, macOS, and Linux, and real-time upgrade status monitoring from the Upgrades page.

Security Cloud Control now supports Cisco Secure Client package upgrades for ASA Remote Access VPN headends across all of your managed organizations from your manager organization. This support extends centralized upgrade capabilities to ASA RA VPN deployments, including guided upgrade workflows, multi-device package deployment, visibility into currently installed Secure Client packages, compatibility-based version selection, platform-specific package targeting for Windows, macOS, and Linux, and real-time upgrade status monitoring from the Upgrades page.

For more information, refer to Upgrade ASA Secure Client packages.

May 8, 2026

New features and improvements deployed on May 8, 2026 for managed service providers and users of multi-organizations in Security Cloud Control.

New features and improvements deployed on May 8, 2026 for managed service providers and users of multi-organizations in Security Cloud Control.

- Multitenant Device Upgrades Now Available for ASAs
- Replace a trial subscription with a paid subscription on page 49

Multitenant Device Upgrades Now Available for ASAs

You can now bulk upgrade ASAs across multiple tenants in addition to performing bulk upgrades for Cloud-Delivered Firewall Management Center-managed Secure Firewall Threat Defense devices.

You can now bulk upgrade ASAs across multiple tenants in addition to performing bulk upgrades for Cloud-Delivered Firewall Management Center-managed Secure Firewall Threat Defense devices.

For more information, see About device upgrades.

Replace a trial subscription with a paid subscription

In Security Cloud Control multi-organizations, you can replace an enterprise or à la carte trial subscription claimed on a managed organization with a paid subscription claimed on its manager organization. You can also replace a trial à la carte subscription with a paid enterprise agreement subscription.

Now, in Security Cloud Control multi-organizations, you can replace an enterprise or à la carte trial subscription claimed on a managed organization with a paid subscription claimed on its manager organization. You can also replace a trial à la carte subscription with a paid enterprise agreement subscription.

See Replace a trial subscription with a paid subscription for more information.

Mar 27, 2026

New features and improvements deployed on March 27, 2026 for managed service providers and users of multi-organizations in Security Cloud Control.

New features and improvements deployed on March 27, 2026 for managed service providers and users of multi-organizations in Security Cloud Control.

- Support for Cisco XDR on page 50

Support for Cisco XDR

Security Cloud Control now supports Cisco XDR for managed service providers and users of multi-organizations.

Security Cloud Control now supports Cisco XDR for managed service providers and users of multi-organizations.

Cisco XDR prioritizes threats based on potential risk and impact, reduces false positives, and provides AI-driven guidance and automation to streamline investigations and remediation. This unified approach enables Security Operations Center (SOC) teams to act faster, improve productivity, and build security resilience by integrating both Cisco and third-party security tools in a multi-vector, multi-vendor environment. See Cisco XDR Help Center for more information.

Jan 30, 2026

New features and improvements deployed on January 30, 2026 in Multi-Organizations for Managed Service Providers.

These are the new features and improvements deployed on January 30, 2026 in Multi-Organizations for Managed Service Providers.

- Managed Service Provider Multi-Organization View on page 50

Managed Service Provider Multi-Organization View

The Security Cloud Control multi-organization view is designed for enterprises that need to manage multiple organizations for a single company. It is now also available for managed service providers who need to manage multiple organizations for different companies.

The Security Cloud Control multi-organization view is now available with specific features for Cisco's managed service providers (MSPs). The multi-organization view gives enterprises the ability to manage multiple organizations for a single company. Now the multi-organization view provides specific features to help MSPs manage multiple organizations for different companies.

The latest release introduces advanced features to further help mid-to-large enterprises and managed service providers (MSPs) efficiently manage thousands of organizations. Key enhancements of this release are:

- **Dedicated Tenant Creation Flow:** A streamlined workflow for organization creation, with role assignment and product provisioning for faster onboarding.
- **Public APIs:** Automate organization, access, and subscription management using new Security Cloud Control APIs, available on Cisco DevNet.
- **Robust Organization Management & RBAC:** Role-Based Access Control (RBAC) is now supported both at the manager level and at the managed organization level for all products within Security Cloud Control. Previously, RBAC management of a manager organization was available only for products that were fully onboarded to a manager organization (licensing sharing, provisioning, and so on).

- **Multi-organization Subscription Management:** Support for multiple active product subscriptions of the same product (in addition to different products) within manager organization with an enhanced Subscription page giving flexibility to manager administrators to choose licenses between various subscriptions as they assign product licenses to managed organization.
- **Performance and Scale:** Security Cloud Control backend architecture optimization to deliver a smooth and responsive management interface experience for thousands of organizations.
- **At-a-glance license auditing:** Easily view licensee details during license assignment to ensure the licenses are shared with the appropriate organizations according to Cisco Legal requirements. See View Subscription Information and Assign Subscriptions to a Managed Organization for more information.
- **MSEA Support (MSP-specific):** Support for advanced managed service buying models within enterprise agreements. See Claim a Managed Service Enterprise Agreement Subscription for more information.
- **Security Product Support:** The multi-organization view supports these Cisco Security products:
  - Secure Access
  - AI Defense
  - Multicloud Defense

9 Security Cloud Control Platform

Topics:

- November 2026
- Sep 29, 2026
- Jun 24, 2026
- Mar 26, 2026
- Mar 19, 2026
- Feb 19, 2026
- Jan 29, 2026
- Dec 04, 2025
- October 29, 2025
- Oct 15 2025
- Sep 24, 2025
- Sep 23, 2025
- Sep 04, 2025
- Aug 6, 2025
- Jul 23, 2025
- Jul 3, 2025
- Jun 25, 2025

Describes new software features, enhancements, behavior changes, and product improvements added to Security Cloud Control.

Security Cloud Control is a security platform that allows you to manage your security products and achieve security outcomes from a single integrated interface. Navigation between products and tools is intuitive and standardized with a common platform menu and toolbar for all integrated products.

Within Security Cloud Control. you can claim and distribute licenses for your integrated products, manage role based access control (RBAC) for users and groups, create organizations, and benefit from other centralized functions.

These are the new software features, enhancements, behavior changes, and product improvements added to Security Cloud Control.

November 2026

These are the new features and improvements to the Security Cloud Control platform deployed in November 2026.

Review these new features and improvements to the Security Cloud Control platform.

- Common Object New Features on page 53
- Subscription License to New Product Instance
- Device Posture on page 55

Common Object New Features

This release support service and service group objects in Common Objects, improves migration and integration paths, and adds clearer controls for access and audit across Cisco security products. These features were released on November 10, 2026.

This release supports service and service group objects in Common Objects, improves migration and integration paths, and adds clearer controls for access and audit. These updates help administrators manage definitions across Cisco security products and let integrated products work from consistent object data. These updates were released on November 10, 2026.

Service and service group objects

Customers can now create and manage service and port objects, including TCP, UDP, ICMP, IPv6 ICMP, and supported IANA protocols, through the Common Objects UI or API. Group objects can contain ports, ranges, and nested groups, with product-specific details preserved where supported.

This allows you to define service and port information once and reuse it across Firewall Threat Defense, Secure Access, and Mesh Policy Engine. Common Objects reduces repeated setup and helps prevent definitions from drifting between products.

System-defined network and service objects

Common Objects now provides predefined read-only network and service objects for each organization. During device onboarding and import, recognized predefined objects can be matched to those in Common Objects and policy references updated to use the predefined object.

These system-defined objects provide administrators with common definitions without recreating them in every device or product. Matching during import also reduces duplicate objects and helps preserve consistent references.

Wildcard mask network objects

You can now edit, import, and manage IPv4 wildcard mask objects as an explicit network subtype. Common Objects uses the cloud-delivered Firewall Management Center mask convention, translates values for Secure Access, and identifies the subtype as unsupported by SD-WAN and Mesh Policy Engine so it is not sent to those products.

You will be able to manage wildcard-based network definitions across Secure Access and Firewall Threat Defense from Common Objects. Compatibility guardrails help avoid unsupported objects being applied where they cannot be represented.

Organization-specific product compatibility

The compatible-products list now reflects the products provisioned in the organization when users create, edit, or view an object. It includes every provisioned product, even when the current user does not have a role in that product.

Users see product choices that match their deployment while still understanding the potential impact across all provisioned products. This makes object compatibility easier to review as products are added or removed.

Service object migration for existing Secure Access organizations

Existing Secure Access service and port definitions can be migrated to Common Objects service groups while policy references are updated. Duplicate definitions and conflicts are surfaced, and special Secure Access **Any** objects that cannot be represented uniformly are flagged with resolution guidance.

Customers can consolidate existing service definitions while keeping policy enforcement intact. Surfacing conflicts and compatibility issues helps administrators understand what needs attention during the transition.

Security Group Tags reference migration for existing organizations

Existing Secure Access and Hybrid Mesh Firewall policy references to security group tags are remapped to common objects identifiers during migration. The process is designed to run without customer action or changes to policy behavior.

Customers move to a single source for security group tag references without rebuilding policies. Consistent identifiers also reduce differences between organizations using legacy and newer security group tag paths.

Common object support for Mesh Policy Engine

Common Objects now supports Mesh Policy Engine. Mesh Policy Engine uses common objects in all its policies, extending the reusability of policy across multiple devices down to that policies objects. Changes in common objects automatically updates all the policies that use them.

Identity Services Engine Security Group Tags as Common Objects

Security group tags from Identity Services Engine appear in Common Objects with searchable names, tag values, and source information. Identity Services Engine remains the authoritative source, so these objects are read-only in Common Objects and can be retrieved for policy workflows through the API.

Administrators can discover and reference security group tags from a common place instead of looking up and re-entering values across products. The authoritative Identity Services Engine source helps keep identity-based policies aligned with current tag definitions.

Common Objects access enablement by product readiness

Common Objects roles and interfaces are enabled when a consuming product is ready and the organization has completed the required provisioning or migration steps. Secure Access and SD-WAN roles can receive Common Objects scopes automatically when the organization begins using the service.

Customers are less likely to encounter object management features before they are usable in their organization. Automatic scope updates also reduce role setup work and help preserve object access as product entitlements change.

Mesh Policy Engine service idle timeout

For service objects managed by Mesh Policy Engine, Common Objects preserves the idle timeout value as a read-only, Mesh Policy Engine-specific attribute. The value is shown in object details and the API, and is not present on native Common Objects services.

Customers and API integrations can review the Mesh Policy Engine service definition without cross-referencing Mesh Policy Engine. The product-specific label makes clear where the timeout is managed and which policy engine uses it.

Common Objects scopes in API key generation

Users with Common Objects read or read-write access can select those scopes when generating an API key. The scopes can be chosen independently of other product scopes for roles that grant Common Objects access.

Teams can create API keys limited to the object permissions an integration needs. This supports automation and reporting without requiring broader product scopes.

Apply the subscription license to a new product instance

You can now cancel an unused activation code to reassign your subscription license to a new product instance.

You can now cancel an unused activation code to reassign your subscription license to a new product instance.

Before you begin

Ensure that your activation code has not already been applied to a product instance.

Procedure

1. Navigate to the **Product and service activation** status section.
2. Select **Cancel activation code**.
3. Select **Create new instance**.

Device Posture

Device posture is a service that aggregates and standardizes endpoint device and compliance information from third-party mobile device management systems Jamf and Microsoft Intune. This enables Cisco security products to make access control decisions based on a standardized posture evaluation methodology. This feature was released November 2, 2026.

Device posture is a centralized platform within Security Cloud Control that aggregates and standardizes endpoint device and compliance information from third-party Mobile Device Management systems Jamf and Microsoft Intune.

This service provides consistent and uniform evaluations of device attributes and compliance checks. Cisco security products use these evaluations to make access control decisions based on a standardized posture evaluation methodology. This feature was released November 2, 2026.

Key Aspects of Posture

- **Standardized Posture Attributes and Policy Evaluation**: Normalizes posture data into a common schema including device management source, compliance status, operating system, and data freshness, enabling consistent access decisions across Cisco products and access methods such as virtual private network and Zero Trust Access.
- **Common Enrollment and Device Identity**: Each managed endpoint receives a unique cloud device identity and certificate through a common enrollment process. This identity is hardware-derived and persists through OS or agent reinstallations, allowing reliable correlation of posture data to the device.
- **Integration with Mobile Device Management Systems**: Supports integration with Microsoft Intune and Jamf to ingest device inventory and compliance events, with real-time updates via webhooks and periodic synchronization to maintain accurate posture information.
- **Access Control Enforcement**: Uses posture attributes to evaluate device compliance against configured posture profiles, enabling applications to grant or deny access based on the evaluated posture verdict.
- **Operational Features**: Includes resiliency mechanisms such as posture-cookie reuse to reduce load and tolerate transient outages, along with audit logs, metrics that provide operational visibility, and troubleshooting processes.

Key Benefits of Posture

- **Consistent Security Posture**: Ensures uniform device compliance evaluation across Cisco security products, reducing security gaps and improving enforcement.
- **Simplified Management**: Centralizes posture data and policy evaluation, reducing duplication and complexity in managing device compliance.

- **Improved Visibility**: Provides detailed audit logs and metrics to monitor posture service health and enforcement outcomes.
- **Scalability and Maintainability**: A shared posture platform supports scalable device management and simplifies future integrations.

For more information, see Device Posture in the Security Cloud Control Administration Guide.

Sep 29, 2026

You can now use dedicated Local Data Residency (LDR) subscriptions to keep all your security services within your sovereign region.

Cisco Security platform introduces dedicated Local Data Residency (LDR) subscriptions to ensure security services, telemetry, and administrative policies remain strictly contained within your sovereign cloud region.

Local data residency platform support

You can now use dedicated Local Data Residency (LDR) subscriptions to keep all your security services within your sovereign region.

Local Data Residency (LDR) is a dedicated compliance capability that enforces complete geographical isolation, guaranteeing that all security traffic inspection, event logging, telemetry, and administrative management remain strictly within designated sovereign borders.

Key benefits

- **Regulatory Compliance**: Satisfies strict regional data sovereignty and governance mandates (starting with Cisco Secure Access in Australia).
- **Guaranteed Isolation**: Enforces sovereign cloud boundaries across the entire lifecycle—from subscription claim to day-to-day operations.
- **Data Protection**: Eliminates cross-border data transfers by utilizing dedicated regional organizations that cannot be mixed with standard commercial offers.

For more information, see Local data residency platform support in the Security Cloud Control Administration Guide.

Jun 24, 2026

Changes and improvements released on June 24, 2026 in Security Cloud Control.

- Security Cloud Control no longer requires 30 days for a newer subscription. See Replace one paid subscription with another on page 57 for more information.
- Security Cloud Control provides a 15-day grace period with full access and a daily countdown to prevent service disruption before potential suspension. See Platform grace period for more information.

Platform grace period

Security Cloud Control provides a 15-day grace period with full access following your term expiration, featuring a visible countdown timer before service is suspended.

Security Cloud Control provides a 15-day platform-enabled grace period following full end of term, including any subscription-level grace period or extension expiration, with full access maintained and a daily countdown displayed until expiration, after which product access is suspended.

See Platform grace period for more information.

Replace one paid subscription with another

Security Cloud Control no longer requires 30 days to end the active subscription.

The 30-day subscription override restriction in Security Cloud Control has been removed, enabling you to seamlessly activate a new subscription at any point before your current one expires with no service interruption.

See Replace a subscription for more information.

Mar 26, 2026

Changes and improvements released on March 26, 2026 in Security Cloud Control.

Security Cloud Control now offers enhanced capabilities for managing common objects, designed to streamline network and security policy administration across your enterprise. These new features provide a unified, consistent, and efficient approach to managing network objects used in both Catalyst SD-WAN and Secure Access environments. See Common Objects on page 57 for more information.

Security Cloud Control no longer supports Google Authenticator. See Switch from Google Authenticator to Duo MFA on page 58 for more information.

Common Objects

Cisco Security Cloud Control now offers enhanced capabilities for managing common objects, designed to streamline network and security policy administration across your enterprise. These new features provide a unified, consistent, and efficient approach to defining and managing network objects used in both Catalyst SD-WAN and Secure Access environments.

These new common object features in Security Cloud Control simplify network and security policy management by providing a single source of truth, reducing errors, and enabling seamless integration across your enterprise's security and networking infrastructure.

- **Unified Common Objects Store:**

  A centralized repository for network objects and object groups that can be shared across Catalyst SD-WAN and Secure Access policies. This eliminates duplication and ensures consistency across products.

- **Create and Manage Network Objects:**

  Administrators can create network objects that include IPv4 and IPv6 hosts and networks, with support for CIDR notation and single host addresses. Objects can be defined once and used in multiple policies, reducing operational overhead.

- **Support for Object Groups:**

  Network object groups allow consolidation of multiple network objects or other groups into a single named entity. Changes to group membership automatically propagate to all referencing policies, improving manageability, and policy consistency.

- **Compatibility and Validation:**

  The system enforces compatibility rules to ensure that common objects and groups are usable in both Catalyst SD-WAN and Secure Access. Local validation warns users of potential configuration breaks before changes are committed.

- **Edit and Delete with Impact Awareness:**

Changes to common objects propagate across all dependent products. The platform provides warnings and confirmation dialogs to prevent accidental disruptions. Deletion of objects requires removal from all referencing policies, ensuring safe cleanup.

- **Search and Filter Capabilities:**

  Enhanced search and filtering allow administrators to quickly find objects by name, value, description, or creator, with support for partial and case-insensitive matches.

- **SASE Management Integration:**

  Common objects are available only to organizations with SASE Management enabled, enabling unified policy management for Secure Internet Access and Secure Private Access alongside Catalyst SD-WAN.

- **Auditability and Governance:**

  Every change to common objects is recorded with versioning and audit trails, capturing who made changes and when. Role-Based Access Control spans both Catalyst SD-WAN and Secure Access, ensuring proper administrative governance.

- **Programmatic Access:**

  Common objects can be managed using APIs, supporting automated workflows.

- **Object Limits and Naming:**

  The platform supports up to 100,000 network objects and 10,000 groups per organization, with group nesting up to three levels. Object names must be unique, up to 64 characters, and use only alphanumeric characters, underscores, or periods.

For more information see the chapter, Common Objects and Object Groups in the Security Cloud Control Administration Guide.

Switch from Google Authenticator to Duo MFA

Security Cloud Sign On now supports only Duo for multi-factor authentication (MFA). Google Authenticator is no longer supported.

Security Cloud Sign On now supports only Duo for multi-factor authentication (MFA). Google Authenticator is no longer supported.

If you have configured Google Authenticator as an additional MFA during the Security Cloud Control account setup, switch to Duo MFA.

See Switching from Google Authenticator to Duo MFA FAQs for more information.

Mar 19, 2026

New features and improvements released on March 19, 2026 in Security Cloud Control.

Security Cloud Control released new features on March 19, 2026.

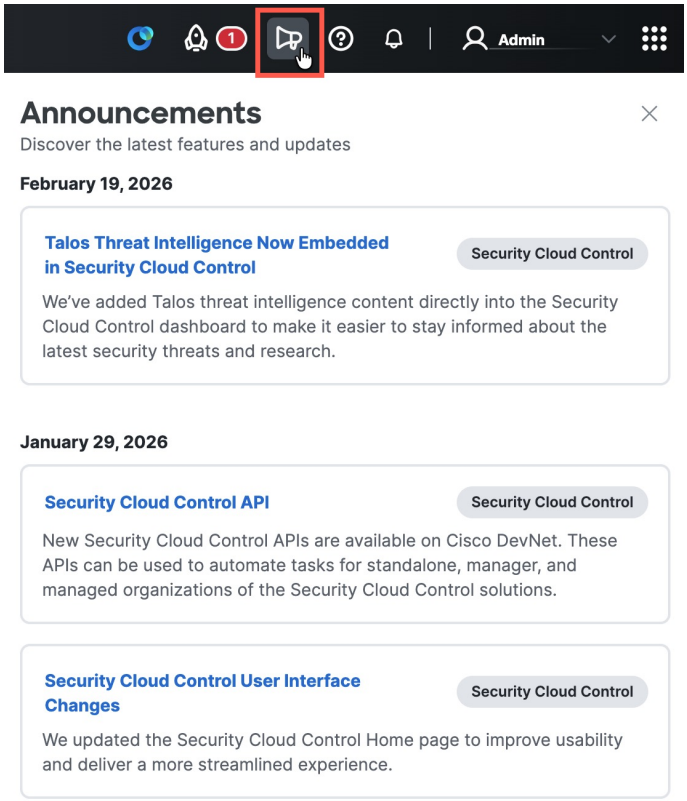
- In-Product Announcements on page 58

In-Product Announcements

Now you can easily see what new features were released by the products you use in Security Cloud Control. Click the megaphone in the toolbar for a short description of the feature and a link to more information.

Now you can easily see what new features were released by the products you use in Security Cloud Control.

Click the megaphone in the Security Cloud Control toolbar to read a brief summary of the latest features. For more information about a feature, click the title of the summary in the Security Cloud Control's What's New guide. If there is additional documentation, we provide you with a link.



Feb 19, 2026

These are the new features and improvements to the Security Cloud Control platform deployed on February 19, 2026.

These are the new features and improvements to the Security Cloud Control platform deployed on February 19, 2026.

- Talos Threat Intelligence Now Embedded in Security Cloud Control on page 59

Talos Threat Intelligence Now Embedded in Security Cloud Control

We've added Talos threat intelligence content directly into the Security Cloud Control dashboard to make it easier to stay informed about the latest security threats and research.

We've added Talos threat intelligence content directly into the Security Cloud Control dashboard to make it easier to stay informed about the latest security threats and research.

Customers logging into Security Cloud Control will now see the latest public Talos blog posts, highlighting timely threat analysis and security insights. Customers with Cisco security products provisioned will also have access to customer-exclusive Talos Intelligence Bulletins, available for download directly from the dashboard.

This update helps bring Cisco Talos expertise closer to where you already manage your security, so you can quickly understand emerging threats and why they matter.

The dashboard also includes a direct link to request Talos emergency incident response services, providing a clear path to expert help when it's needed most.

See Talos Intelligence for more information.

Jan 29, 2026

These are the new features and improvements to the Security Cloud Control platform deployed on January 29, 2026.

These are the new features and improvements to the Security Cloud Control platform deployed on January 29, 2026.

- Security Cloud Control API on page 60
- Security Cloud Control User Interface Changes on page 60

Security Cloud Control API

New Security Cloud Control APIs are available on Cisco DevNet. These APIs can be used to automate tasks for standalone, manager, and managed organizations of the Security Cloud Control solutions.

New Security Cloud Control APIs are available on Cisco DevNet. These APIs can be used to automate tasks for standalone, manager, and managed organizations of the Security Cloud Control solutions.

The Security Cloud Control API implements a REST interface that is described by version 3.x of the OpenAPI specification. The API operations use JSON for all requests and responses.

To access the Security Cloud Control API, you must first get an access token from the user interface. With this access token, you can use any REST client to make requests to the API.

The Security Cloud Control API provides the following capabilities:

- **Organizations** - Create, view, and update manager, managed, and standalone organizations provisioned on Security Cloud Control.
- **Subscriptions** - Create, view, update, activate, and deactivate software subscriptions on a Security Cloud Control organization.
  - **ClaimInfo** - Validate a claim code and retrieve details about the claim code for a specific organization.
- **Users** - List all users, view user details, suspend and enable users, resend email invites, reset passwords, reset multi-factor authentication, and modify user information.
  - **User Groups** - List all admin groups that include the user.
- **Admin Groups** - List all admin groups within an organization. List which organizations can access an admin group, view details for an admin group, add or remove users and managed organizations from an admin group. Modify admin group details, and delete admin groups.
  - **Roles** - List roles, view details for a role, and assign or remove roles from users.
  - **Refresh Token** - Get a new access and refresh token.

See Security Cloud Control API on Cisco DevNet for more information.

Security Cloud Control User Interface Changes

We updated the Security Cloud Control Home page to improve usability and deliver a more streamlined experience.

Changed default home page behavior

We have stopped automatically redirecting users to a product-specific landing page instead of the platform home page if they only have one product. If you still prefer to land directly on the page for a specific product, you can click the "Set default homepage" link to configure your landing page preference. See Set Your Default Landing Page for more information.

Removed redundant shared objects menu

We have removed the "Shared Objects" choice from the platform menu under Platform Services because it currently only supports Security Cloud Control Firewall Management, and there is a Shared Objects menu choice in the Security Cloud Control Firewall Management menu.

Hiding non-applicable Security Cloud Control Firewall Management features from menu bar

For users who do not have subscriptions for Security Cloud Control Firewall Management, we removed the search box and "Devices with Pending Changes" icon from the menu bar because these items are currently only applicable to organizations with Security Cloud Control Firewall Management.

Dec 04, 2025

Security Cloud Control platform released a new feature on December 04, 2025.

Security Cloud Control platform released Limited Use Cisco Duo Licenses on page 61 on December 04, 2025.

Limited Use Cisco Duo Licenses

You can now use Cisco Duo and Cisco Identity Intelligence services with a Secure Access or a Cisco XDR subscription. After you claim either of these products, some features of Duo and Identity Intelligence services are available for you.

You can use the Cisco Duo and Identity Intelligence services with a Secure Access or a Cisco XDR subscription. After you claim either of these products, some features of Duo and Identity Intelligence services are available for you. To know more about the limited use of Duo license, see Activate Cisco Duo and Cisco Identity Intelligence Services.

October 29, 2025

New features and improvements deployed on October 29, 2025 in Security Cloud Control.

These are the new features and improvements deployed on October 29, 2025 in Security Cloud Control.

- Enabling Cisco Multicloud Defense in a Security Cloud Control Organization on page 61
- Activating Trial on a Paid Subscription on page 61

Enabling Cisco Multicloud Defense in a Security Cloud Control Organization

With a single click on the banner in the Subscriptions page, you can now enable Cisco Multicloud Defense in your organization—no claim code is required. You get immediate access to Multicloud Defense Visibility for real-time insight into multicloud traffic and threats, with centralized monitoring and simple dashboards for security and compliance.

With a single click on the banner in the Subscriptions page, you can now enable Cisco Multicloud Defense in your organization—no claim code is required. You get immediate access to Multicloud Defense Visibility for real-time insight into multicloud traffic and threats, with centralized monitoring and simple dashboards for security and compliance.

Multicloud Defense requires Firewall Management to be active in your organization. If Firewall Management is not already enabled, you will be prompted to set it up before activating Multicloud Defense.

Activating Trial on a Paid Subscription

You can apply a product or a suite trial directly to your existing active paid subscription in Security Cloud Control. When a trial ends, Security Cloud Control automatically and seamlessly reverts the entitlements back to the original paid subscription with no user action required and no loss of service.

You can apply a product or a suite trial directly to your existing active paid subscription in Security Cloud Control. When a trial ends, Security Cloud Control automatically and seamlessly reverts the entitlements back to the original paid subscription with no user action required and no loss of service.

With this option, you can upgrade and trial higher product tiers on your existing subscription, gaining access to additional features and capabilities. You can also apply suite trials to standalone product subscriptions. This option enables you to activate more products within a suite and experience the benefits of integrated multi-product or suite solutions within your existing environment.

Oct 15 2025

New features and improvements deployed on October 15, 2025 in Security Cloud Control.

These are the new features and improvements deployed on October 15, 2025 in Security Cloud Control.

- Resend Activation Email to New Users on page 62

Resend Activation Email to New Users

Security Cloud Control provides you with an option to resend email invitations to new users, allowing them to activate a Security Cloud Sign On account.

You can now resend an email invitation to new users.

When you invite new users to an organization, the users receive an email with a link to activate their Security Cloud Sign On account. If the users do not activate their account within seven days, the activation link expires. Security Cloud Control provides you with an option to resend the email invitation, enabling the users to activate their account.

Sep 24, 2025

New features and improvements deployed on September 24, 2025 in Security Cloud Control

These are the new features and improvements deployed on September 24, 2025 in Security Cloud Control.

- Import users from a CSV file on page 62
- Retain user roles on product deactivation on page 62

Import users from a CSV file

This feature enables you to invite multiple users to an organization at one time by importing a CSV file containing a list of user details.

This feature enables you to invite multiple users to an organization at one time by importing a CSV file containing a list of user details. See Import Users for more information.

Retain user roles on product deactivation

When you deactivate a product instance, the product and its services are suspended, but the user roles are retained and made available when the product is reactivated.

When you deactivate a product instance, the product and its services are suspended, but the user roles are retained and made available when the product is reactivated. See Deactivate a product instance for more information.

Sep 23, 2025

Security Cloud Control released new features on September 23, 2025:

Security Cloud Control released Security Cloud Control Multi-Organizations on September 23, 2025.

Security Cloud Control Multi-Organizations

Announcement of new multi-organization capabilities in Security Cloud Control.

We are excited to announce the release of multi-organization capabilities for Security Cloud Control. These new features are designed to support organizations managing multiple organizations, delivering a streamlined and scalable approach to subscription entitlement and access management.

Manager Organization Landing Page and Navigation

- A newly designed landing page tailored to manager organization users in multi-organization environments.
- Step-by-step guidance to help manager organizations onboard and manage effectively.
- Updated navigation for quick access to essential management pages.
- Seamless switching between organizations.

Create and View Managed Organization

- Effortlessly navigate to manage subscription entitlements or access for each organization.
- Perform key actions for managed organizations without switching contexts.
- View comprehensive organization details.

Subscription Claiming and Cross-Organization Entitlement Management

- Flexible subscription options for large enterprise customers with multiple managed organizations.
- Claim subscriptions at both the manager and managed organization levels.
- Share subscription entitlements across multiple managed organizations from the manager organization level.
- Support for Secure Access, Multicloud Defense, and AI Defense.

Access Management

- Enhanced transparency and control using user groups for access to managed organizations.
- Manager administrator user groups can be shared with select managed organizations.
- Managed organization users can also be added individually from within managed organizations, without requiring user groups.

Multi-Organization Activity Logging

- Comprehensive logging of events across all organizational contexts.
- Captures event datetime, organization context, user actor details, and IP address.
- Searchable activity log fields for efficient filtering and retrieval.

For more information, use Security Cloud Control Multi-Organizations as a supplement to the Security Cloud Control Administration Guide.

Sep 04, 2025

New features and improvements deployed on September 4, 2025 in Security Cloud Control.

These are the new features and improvements deployed on September 4, 2025 in Security Cloud Control.

You can now choose your background theme in the Security Cloud Control portal.

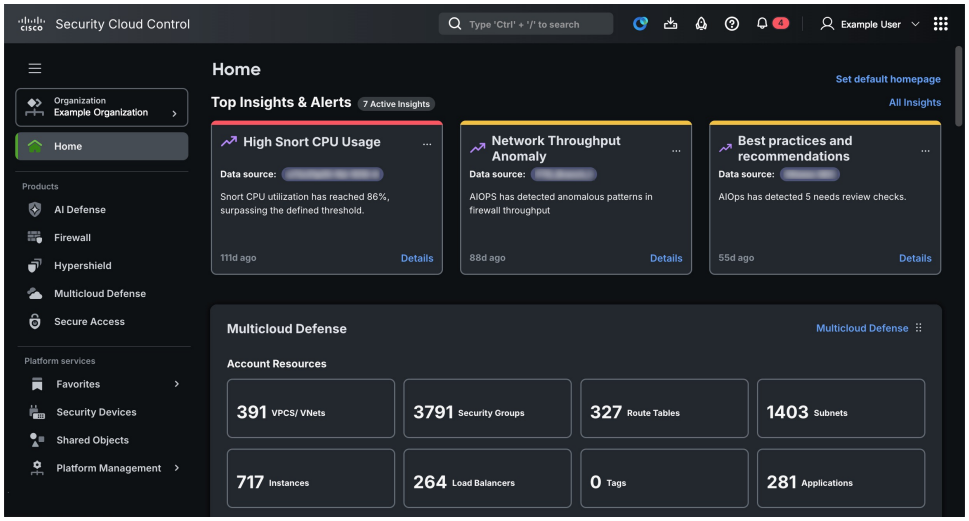
Choose your background theme

Security Cloud Control now lets you choose your background theme. Choose light theme, dark theme, or the setting your browser uses. Most integrated products and platform pages in Security Cloud Control use the theme you set.

Security Cloud Control now lets you choose your background theme. Choose light theme, dark theme, or the setting your browser uses. Most integrated products and platform pages in Security Cloud Control use the theme you set.

> **Note**
>
> Cisco Secure Access does not support dark theme. If dark theme is enabled, Secure Access-specific UI elements will still be rendered using light theme.

This is an example of Security Cloud Control using dark theme:



See Set Background Theme for more information.

Aug 6, 2025

Security Cloud Control released new features for customers on August 6, 2025.

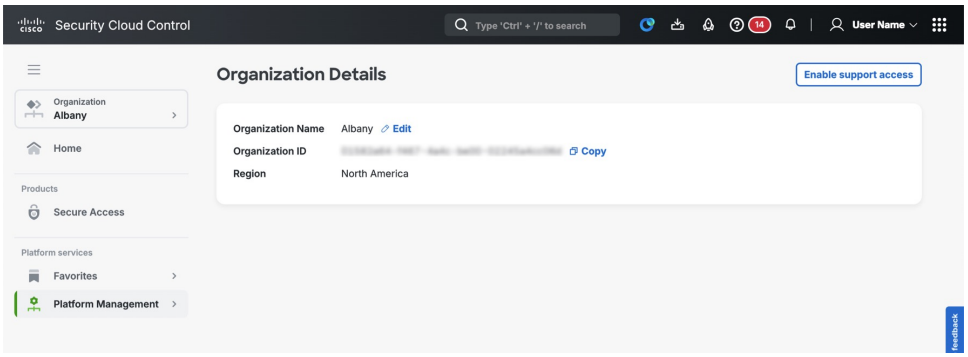
Security Cloud Control released new features for customers on August 6, 2025.

- New Organization Details Page on page 65

New Organization Details Page

The new organization details page displays the organization name, organization ID, and region. It also allows you to enable or disable organization access for Cisco TAC and change the name of your organization.

There is a new organization details page in Security Cloud Control.



From that page you can perform these tasks:

- View information about your organization
- Enable or disable access to your organization by Cisco Technical Support
- Rename your organization
- Copy the organization ID

Navigate to the organization details page using these steps:

1. In the Security Cloud Control platform menu, select your organization from the organization picker list.
2. In the organization menu, choose **Platform services** > **Platform Management** > **Organization Details**.

Jul 23, 2025

Security Cloud Control released new features for customers on July 23, 2025, 2025.

Security Cloud Control released new features for customers on July 23, 2025.

- Immediate Updates to User Privileges on page 65

Immediate Updates to User Privileges

When a user in an organization changes the privileges of another user by changing their user role, disabling their account, changing their membership in a group, or changing the group itself, that user's privileges are updated within 30 seconds. The user does not need to log out and log back in to experience the updated privileges.

When a user in an organization changes the privileges of another user by changing their user role, disabling their account, changing their membership in a group, or changing the group itself, that user's privileges are updated within 30 seconds. The user does not need to log out and log back in to experience the updated privileges.

Jul 3, 2025

Security Cloud Control released a customer feedback feature on July 3, 2025.

Security Cloud Control released a customer feedback feature on July 3, 2025. See Give us your feedback! on page 66

Give us your feedback!

We want to hear from you! The "Give Feedback" tool in Security Cloud Control is designed to gather your insights and opinions so that we can enhance the platform and its features.

We want to hear from you! The "Give Feedback" tool in Security Cloud Control is designed to gather your insights and opinions so that we can enhance the platform and its features. This tool allows you to share your experiences, whether related to the ease of use, the effectiveness of specific features, or suggestions for improvement. See Give us your Feedback for more information.

Jun 25, 2025

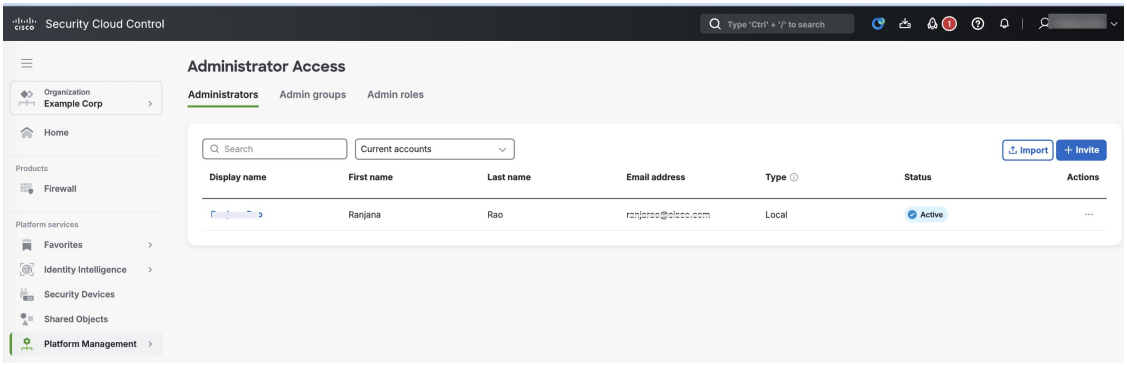
Security Cloud Control released an update on June 25, 2025.

Security Cloud Control simplified the Access Management menu on June 25, 2025. See Simplified Access Management Menu on page 66

Simplified Access Management Menu

The Access Management menu under Platform Management in Security Cloud Control has been simplified. An administrator can now view the administrators, administrator groups, and administrator roles, all on the same page.

The Access Management menu under Platform Management in Security Cloud Control has been simplified. An administrator can now view the administrators, administrator groups, and administrator roles, all on the same page.



10 Additional Documentation and Support

Topics:

- Security Cloud Control Documentation
- AI Defense Documentation
- Security Cloud Control Firewall Management Documentation
- Multicloud Defense Documentation
- SASE Management with Common Objects
- Secure Access Documentation
- Secure Workload Documentation
- Browsers Supported by Security Cloud Control

Provides links to additonal documentation and content that pertains specifically to products that can be integrated in Cisco Security Cloud Control as well as Cisco customer support information.

Users integrate many different Cisco products with Security Cloud Control. Many of those integrated products manage other Cisco products. These integrations and managed products have their own documentation sets. This section provides links to relevant product documents and documentation summaries.

Security Cloud Control Documentation

Provides links to additional documentation and content that pertains to Cisco Security Cloud Control.

Administration Guide

The Cisco Security Cloud Control Administration Guide is intended for Security Cloud Control administrators and describes Security Cloud Control core functionality.

Getting Started Guides

These guides will help you get Security Cloud Control up and running quickly:

- Getting Started Guide for New Customers of Security Cloud Control
- Getting Started Guide for Existing Security Product Customers

Videos

Watch these videos to see visual demonstrations of Security Cloud Control platform operations.

- Create an organization
- Claim a subscription to activate a new instance of a product
- Invite a user to Security Cloud Control
- Import multiple users to Security Cloud Control
- Add users to a group and assign group roles

AI Defense Documentation

Provides links to additonal documentation and content that pertains specifcially to Cisco AI Defense.

AI Defense addresses risks for users and providers of AI. Using network visibility and enforcement points in the Security Cloud Control, AI Defense adds detection and enforcement measures to discover sanctioned and unsanctioned AI workloads, applications, models, data, and user access across your distributed cloud environment. For organizations that develop and deliver AI-powered services, AI Defense detects vulnerabilities in your AI models before they're delivered. For your running AI applications, AI Defense guardrails intercept rapidly evolving threats, including prompt injections, denial of service, and data leakage.

See the AI Defense User Guide for detailed information.

Security Cloud Control Firewall Management Documentation

Provides links to additional documentation and content that pertains specifically to Security Cloud Control Firewall Management.

Security Cloud Control Firewall Management: Security Cloud Control Firewall Management (formerly Cisco Defense Orchestrator) is a cloud-based security policy manager that simplifies and unifies policy across your Cisco firewalls and other devices.

See Security Cloud Control Firewall Management documentation for more information.

Multicloud Defense Documentation

Provides links to additonal documentation and content that pertains specifcially to Multicloud Defense.

Multicloud Defense provides a simplified and highly automated approach to multicloud security. This solution allows organizations to manage and secure their multicloud environments using a single SaaS delivered control plane, and centralized or distributed PaaS-delivered data plane architectures. Multicloud Defense provides continuous visibility, unified protection and dynamic policy updates across all major cloud providers, thereby eliminating the need for separate point solutions for each cloud provider.

These documents describe the new features and functionality of Multicloud Defense:

- Multicloud Control Release Notes
- Multicloud Defense User Guide

SASE Management with Common Objects

Cisco's SASE Management integrates SD-WAN and Cisco Secure Access into a single, cloud-native management experience integrated with Cisco Security Cloud Control.

SASE Management integrates SD-WAN and Secure Access into a single, cloud-native management experience integrated with Security Cloud Control.

Who should use SASE Management

- **Existing SD-WAN Customers:** If you already use SD-WAN Cloud, SASE Management allows you to extend your capabilities with unified security policy management. For more information, see the SD-WAN Cloud Guide.

> **Note**
>
> Modifying your organization's subscription model or tier is not supported once you enable SASE Management.

- **New Secure Access Customers:** If you are adopting Secure Access capabilities for the first time, SASE Management provides an easy-to-use experience that is integrated with SD-WAN Manager. For more information, see Cisco Secure Access At-a-Glance and Secure Access Help.

> **Caution**
>
> After a SD-WAN organization is linked to SASE Management, it cannot be detached from SASE Management.

Key benefits

- **Streamlined onboarding:** Easily onboard your SD-WAN sites and devices into the SASE fabric through Security Cloud Control, with flexible deployment options and audit logs to track changes.

- **Unified policy management:** Manage Secure Internet Access (SIA) and Secure Private Access (SPA) policies for SD-WAN and Secure Access devices from one consolidated interface. This reduces complexity and helps ensure consistent security enforcement across your entire environment.
- **Simplified operations:** Create, modify, deploy, and monitor policies without switching between multiple management tools, saving time, and reducing operational overhead.
- **Common objects:** After SASE Management has been enabled, you can define network objects once and reuse them across your SD-WAN and security policies, improving consistency and reducing errors.
- **Integrated troubleshooting:** Access device and tunnel health information and perform basic troubleshooting directly within the unified platform to quickly resolve issues.

Learn more here:

- SASE Management Administration Guide
- Common Objects and Object Groups

Secure Access Documentation

Provides links to additonal documentation and content that pertains specifcially to Cisco Secure Access.

Cisco Secure Access is a cloud-based platform that provides multiple levels of defense against internet-based threats. Connect securely to the internet, SaaS apps, and private digital resources from your organization's network or roaming off-network. Using policy rules, configure and enforce security controls on collections of resources, users, and devices.

These documents describe the new features and functionality of Secure Access:

- Secure Access Release Notes
- Secure Access Help

Secure Workload Documentation

Provides links to additonal documentation and content that pertains specifcially to Cisco Secure Workload.

Secure Workload: Cisco Secure Workload (formerly Tetration) seamlessly delivers zero-trust micro-segmentation across any workload, environment, or location from a single console. With comprehensive visibility into every workload interaction and powerful AI/ML-driven automation, Secure Workload reduces the attack surface by preventing lateral movement, identifies workload behavior anomalies, helps rapidly remediate threats, and continuously monitors policy compliance. See Secure Workload Documentation for more information.

See Cisco Secure Workload Documentation Roadmaps for more information.

Browsers Supported by Security Cloud Control

Security Cloud Control supports the latest version of Google Chrome, Microsoft Edge, and Mozilla Firefox; and provides partial support for Apple Safari.

Fully Supported Browsers

Security Cloud Control supports the latest version of these browsers.

- Google Chrome
- Microsoft Edge

- Mozilla Firefox

Safari Support

Security Cloud Control supports the use of Apple Safari for most platform-level tasks such as user and subscription management. Safari supports Security Cloud Control platform features, including user and subscription management, and Secure Access. Firewall Management and Multicloud Defense are not supported in Safari.

If Safari does not support a particular product or feature, the user sees a banner message explaining, "This (product or feature) does not support the Safari browser. For the best experience, use a recent version of Google Chrome, Microsoft Edge, or Mozilla Firefox."

This table lists the Safari support for Security Cloud Control integrated products and services.

Product / Service	Supported (✓) Unsupported (✗)
AI Assistant	✓
AI Defense	✓
SD-WAN	✓
Duo Security	✓
Firewall Management	✗
Hypershield	✓
Identity Intelligence	✓
Multicloud Defense	✗
Security Cloud Control platform features	✓
Secure Access	✓
Secure Workload	✓