

New Features in 2026

These are the new Firewall features deployed in Security Cloud Control in 2026.

- September 2026, on page 1
- August 2026, on page 2
- July 2026, on page 3
- June 2026, on page 4
- May 2026, on page 4
- April 2026, on page 4
- March 2026, on page 5
- February 2026, on page 6
- January 2026, on page 7

September 2026

September 17, 2026

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.

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 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.

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

Introducing Agent Workforce

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.

September 10, 2026

Secure Client upgrades for ASA Remote Access VPN

Security Cloud Control now supports Cisco Secure Client package upgrades for ASA Remote Access VPN headends. 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 Upgrade ASA Secure Client packages.

September 3, 2026

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.

For more information, see Automation tools and AI agents.

August 2026

August 6, 2026

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.

For more information, see Manage software upgrades.

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.

July 2026

July 31, 2026

NAT policy anomaly analysis for Firewall Threat Defense devices

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, see Network Address Translation policy analysis.

July 23, 2026

Introducing Capacity and Trend Analyzer

Capacity and Trend Analyzerhelps 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.

For information about supported versions of the On-Premises 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.

For more information, see About software upgrade insights.

July 16, 2026

Monitor Security Analytics and Logging (SaaS) service status from Security Cloud Control

The Security Analytics and Logging (SaaS) service status monitoring option in the **Event Logging** page provides you with direct visibility into Security Analytics and Logging (SaaS) service availability from Security Cloud Control. You can monitor service availability, verify whether managed Firewall Threat Defense devices are sending events, and check the last received event details to identify possible ingestion delays or disruptions faster.

For more information, refer to Monitor Security Analytics and Logging (SaaS) service availability.

June 2026

June 04, 2026

Updates to Cloud-Delivered Firewall Management Center

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

May 2026

May 07, 2026

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.

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

April 2026

April 23, 2026

Simplify Your Multicloud Security Setup with Cloud Deployment

The new Cloud Deployment feature streamlines the configuration of 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

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

March 2026

March 26, 2026

Firewall MSP Portal Now Integrated into Security Cloud Control

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.

March 19, 2026

Updates to Cloud-Delivered Firewall Management Center

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

March 12, 2026

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.

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.

For more information, see Overview of Smart Licensing Dashboard.

February 2026

February 19, 2026

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.

For more information, see Overview of Smart Licensing Dashboard.

February 05, 2026

Introducing Application Insights

AIOps now features **Application Insights**, which uses ThousandEyes Internet Insights to proactively detect cloud application outages. It shows affected applications, impacted domains, outage duration, and affected regions for the monitored applications.

For more information, see Detect Application Outages.

January 2026

January 29, 2026

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.

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

January 29, 2026