Security in Cisco Cloud Control Frequently Asked Questions

Q: What is Security in Cisco Cloud Control?

A: Security in Cisco Cloud Control brings security into Cisco Cloud Control's unified operations platform. It gives teams one governed environment for policy, visibility, and action across Cisco security enforcement points and selected third-party firewall policies. With AI Canvas, operators and AI agents can investigate together and connect security findings to broader operational context. Administrators retain control through review, approval, validation, and auditability.

Q: What products can you manage through Security in Cisco Cloud Control?

A: Security in Cisco Cloud Control brings together the management of:

- Cisco Secure Firewall (ASA and FTD)
- Cisco Multicloud Defense
- Cisco Hypershield
- Cisco Secure Workload (SaaS)
- Cisco Secure Access
- Cisco Secure Router (Catalyst SD-WAN and NGFW)
- Cisco AI Defense

Q: Can on-premises Firewall Management Center (FMC) users benefit from Security in Cisco Cloud Control?

A: Yes. On-premises FMC users can integrate with Security in Cisco Cloud Control while retaining their existing FMC for Firewall Threat Defense (FTD) management. Cloud integration provides policy analysis and optimization, best-practice recommendations, and feature adoption insights, with zero upfront cost. Customers can also choose full cloud management through Secure Firewall in Cloud Control to gain automatic management updates and backups, elastic scalability, unified FTD and ASA event visibility, and third-party policy management. You can learn more here.

If you're nearing renewal of your on-premises Firewall Management Center (FMC) appliance, use our interactive calculator to see how much you could save by moving your firewall management to Cisco Cloud Control.

Q: What are the key benefits of using Security in Cisco Cloud Control?

A: Security in Cisco Cloud Control brings policy, visibility, and agentic operations into one governed experience. It helps teams apply policy consistently across distributed enforcement points, reduce policy gaps, and simplify administration. Shared context and AI-assisted investigation improve productivity, while customers can start with existing Cisco and selected third-party infrastructure and add or move enforcement points over time.

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

Q: What AgenticOps features are there in Security in Cisco Cloud Control?

A: Security in Cisco Cloud Control helps teams investigate faster and prepare policy changes with shared context. With AI Canvas, operators and AI agents can correlate security findings with broader operational signals. Specialized security agents use conversational prompts to monitor, investigate, recommend remediation, and prepare candidate configurations. Administrators remain in control through review, approval, validation, and auditability.

Users can also utilize Natural Language Querying (NLQ) for documentation across Secure Firewall, Secure Access, Hypershield, XDR, and Duo. Additionally, Secure Firewall in Cloud Control offers AI Operations (AIOps), which identifies critical issues, provides recommendations, and delivers actionable insights to enhance security. The policy analyzer and optimizer identify policy gaps and suggest improvements, while feature adoption insights and best-practice recommendations help teams get more value from existing deployments.

Q: Is Security in Cisco Cloud Control suitable for businesses of all sizes?

A: Yes, Security in Cisco Cloud Control is scalable and can be tailored to meet the needs of small businesses, mid-sized companies, and large enterprises. Customers can start with existing Cisco and selected third-party infrastructure, then add or move enforcement points as their needs evolve.

Q: How is Security in Cisco Cloud Control priced?

A: Security in Cisco Cloud Control is a cloud-based subscription service available at no cost to customers who have purchased any of the following products: Secure Firewall, Multicloud Defense, Hypershield, Secure Workload (SaaS), Secure Access, or AI Defense. For additional capabilities, users can subscribe based on their specific needs. For more information, contact your Cisco sales representative or certified Cisco partner.

Q: Is Security in Cisco Cloud Control a part of the Cloud Protection Suite?

A: Yes, Security in Cisco Cloud Control is included in both the Essentials Segmentation and Essentials Gateway options of the Cloud Protection Suite.

Q: What deployment options are available for Security in Cisco Cloud Control?

A: Security in Cisco Cloud Control is offered as a cloud-based service, allowing for rapid deployment and minimal on-premises infrastructure. Customers can begin with existing Cisco and selected third-party infrastructure. Secure Firewall customers can integrate an on-premises FMC with cloud capabilities or choose full cloud management through Security in Cloud Control.

Q: How do I set up Security in Cisco Cloud Control for my organization?

A: To set up Security in Cisco Cloud Control:

1. Sign in to your Cisco Cloud Control account at security.cisco.com.
2. Create an organization and register your Cisco security products within the portal.
3. Configure user access and policies based on your organization's needs.
4. Start monitoring and managing security configurations from a centralized location.

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

Q: How does Security in Cisco Cloud Control handle data privacy and compliance?

A: Cisco is committed to data privacy and regulatory compliance. Security in Cisco Cloud Control is built with these principles in mind, ensuring that your data is handled securely and in accordance with applicable laws and regulations. For more information, please visit the Cisco Trust Center.

Q: What kind of support can I expect with Security in Cisco Cloud Control?

A: Cisco offers robust support for all its products, including 24/7 technical assistance, extensive online documentation, and a community of experts to help you get the most out of your investment in Security in Cisco Cloud Control.

Q: How does Security in Cisco Cloud Control manage the SASE experience?

A: Security in Cisco Cloud Control brings security into a multi-domain operating model, helping NetOps and SecOps teams manage security policy across branch, remote-access, and SASE environments. It brings together Cisco Secure Router (Catalyst SD-WAN and NGFW) and Cisco Secure Access operations in a centralized platform. Shared policy and operational context streamline onboarding, provisioning, and monitoring, reduce silos, and support consistent enforcement from branch to cloud edge.

Q: Where can I find more information about Security in Cisco Cloud Control?

A: You can find more information about Security in Cisco Cloud Control on our official product page or by reaching out to your Cisco account representative.



© 2026 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)