Framework Foundations: FedRAMP

Introduction to FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP) is a U.S. government-wide initiative designed to standardize the security assessment, certification, and continuous monitoring of cloud products and services. Its primary goal is to ensure that cloud service providers (CSPs) meet stringent security standards before they can be used by federal agencies.

FedRAMP Certification, formerly referred to as FedRAMP authorization, is the official determination by FedRAMP that a cloud service provider has met standardized federal security requirements and may be used by agencies to support Authorization to Operate (ATO) decisions.

FedRAMP is evolving through the FedRAMP 20x initiative, which aims to:

- Modernize the authorization process using automation and industry best practices.
- Simplify security requirements for cloud providers.
- Enhance continuous monitoring capabilities.
- Foster stronger collaboration between federal agencies and industry stakeholders.

These changes are expected to accelerate the adoption of secure cloud technologies across the federal landscape.

FedRAMP is built around four core objectives:

- **Standardization:** Create a unified security framework for federal cloud services.
- **Efficiency:** Reduce repeated security assessments to save time and resources.
- **Security:** Maintain strong protection of federal data with continuous monitoring.
- **Reuse:** Enable faster cloud deployment by reusing existing security authorizations.

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

Key Requirements

To achieve FedRAMP certification, cloud service providers (CSPs) must meet several critical requirements that ensure the security and integrity of federal data:

Security Assessment

FedRAMP mandates a comprehensive security assessment based on NIST SP 800-53 Rev. 5 controls. This is conducted by a FedRAMP-accredited Third Party Assessment Organization (3PAO).

FedRAMP Certification

Cloud Service Providers (CSPs) obtain FedRAMP Certification through a standardized assessment and review process. Federal agencies continue to issue Authorities to Operate (ATOs) based on a CSP's FedRAMP Certification.

Continuous Monitoring

After authorization, CSPs must implement a Continuous Monitoring (ConMon) program. This includes monthly vulnerability scans, incident reporting, and performance metrics, as outlined in the FedRAMP Continuous Monitoring Performance Management Guide.

Documentation

CSPs must submit a full authorization package, including:

- System Security Plan (SSP)
- Security Assessment Plan (SAP)
- Security Assessment Report (SAR)
- Plan of Action and Milestones (POA&M)

These are required to demonstrate control implementation and risk management.

Risk Management

FedRAMP emphasizes a structured approach to identifying and mitigating risks, especially those associated with inherited controls and shared responsibilities.

Configuration Management

CSPs must maintain strict control over system configurations, including change management procedures and baseline integrity checks. This is part of the NIST SP 800-53 control families required by FedRAMP.

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

How Cisco Security + Splunk Support Compliance

Cisco and Splunk offer FedRAMP-certified solutions that help federal agencies manage identity, network visibility, threat detection, and application performance in Class C (Moderate) and Class D (High) environments.

FedRAMP Class C (Moderate)

- **Cisco Meraki for Government** Cloud-managed networking platform with secure wireless, switching, firewalls, and SD-WAN.
- **Cisco Duo Federal**
  Authorized MFA with FIPS-compliant authentication and support for AAL2 and AAL3 authenticators, including biometric and hardware security tokens.
- **Cisco Catalyst SD-WAN for Government**
  Secure, application-aware networking optimized for cloud integration.
- **Cisco Cloudlock for Government**
  Cloud-native CASB securing identities, data, and applications with machine learning analytics.
- **Cisco ThousandEyes for Government**
  Network performance visibility and diagnostics.
- **Splunk Cloud Platform** Real-time operational insights for non-sensitive environments.
- **Cisco AppDynamics GovAPM**
  Real-time application performance monitoring for secure operations.

FedRAMP Class D (High)

- **Cisco Security Cloud Control for Government**
  Centralized policy management across distributed environments.
- **Cisco Secure Access for Government**
  Unified management with Zero Trust Network Access (ZTNA) and AI-driven threat intelligence.
- **Cisco Umbrella for Government**
  DNS-layer security, Secure Web Gateway (SWG), Cloud Delivered Firewall (CDFW), CASB, and Data Loss Prevention (DLP).
- **Cisco Secure Firewall for Government**
  Advanced threat protection and firewall capabilities tailored for federal environments.
- **Cisco Duo Federal**
  Authorized MFA for higher-impact federal workloads, supporting FIPS-compliant authentication and AAL2/AAL3 authenticators, including biometric and hardware security tokens.
- **Cisco Secure Email Threat Defense for Government**
  Cloud-native email security solution provides real-time inline scanning and remediation of email threats.
- **Splunk Cloud Platform**
  Robust analytics and monitoring for critical government operations.

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

Get Started with Cisco

As FedRAMP continues to evolve through initiatives such as FedRAMP 20x, agencies and contractors are being challenged to demonstrate security, streamline compliance activities, and accelerate cloud adoption. Success requires more than meeting requirements. It requires the ability to continuously monitor, assess, and improve security across increasingly complex environments.

Cisco Security and Splunk provide the visibility, automation, and operational insights needed to support these objectives. By helping teams reduce manual effort, strengthen security operations, and gain greater confidence in their compliance posture, Cisco can help organizations prepare for what's next.

Ready to take the next step?

Contact your Cisco account representative to learn how Cisco Security and Splunk can help advance your FedRAMP and cybersecurity goals.

Resources

For more information and guidance on FedRAMP certifications, please refer to the following resources:

- FedRAMP Marketplace
- Cisco Solutions for Federal Government
- Cisco Trust Portal
- Splunk Security Certifications and Attestations

© 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) 09/26