JUNIPER NETWORKS | Engineering Simplicity

Juniper Mist Secure Configuration Guide for US Government Cloud

Published
2026-02-27

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Mist Secure Configuration Guide for US Government Cloud

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide

This Secure Configuration Guide (SCG) defines the best security practices for configuration required to securely deploy and operate Juniper Mist Government Cloud within a FedRAMP Moderate Rev. 5 environment. It ensures that federal agencies configure their Mist managed networks in a manner consistent with NIST SP 800-53 Rev. 5 and FedRAMP requirements.

Scope

This Secure Configuration Guide (SCG) applies only to the following:

- Configuration for tenant/org
- Configuration for Identity and Access Management
- Configuration of API Token
- Configuration of Webhooks
- Configuration of Network segmentation and Zero Trust enforcement
- Logging, monitoring, and integration with agency SIEM per FedRAMP guidelines
- Change management and configuration baselines per FedRAMP guidelines
- Implementation of SSID/WLAN, and wired encryption settings per FedRAMP guidelines
- Ensure networking devices are running recommended firmware for security patches

Baseline Standards

Customer configurations must align with:

- FedRAMP Moderate Baseline (Rev. 5)
- NIST SP 800-53 Rev. 5
- Agency specific security policies

Customer Secure Configuration Requirements

Identity & Access Management (IA-2, IA-5, AC-5, AC-2)

Configuration for SSO/SAML integration

Customers should configure:

- MFA for agency accounts (required for FedRAMP)
- SAML/SSO integration with agency identity provider strongly recommended.
- Role based access control (RBAC)
- Disable unused local accounts as per FedRAMP guidelines.
- Review user access as per FedRAMP guidelines.

Network Device Configuration (CM-6, AC-6, AC-17)

The following are device-specific configuration for FedRAMP recommended security policies:

Access Points (APs)

Customers should:

- Configure SSID encryption for WLAN
- Enable rogue AP detection and alerting. See Juniper Mist Alert Types.
- Apply Mist recommended firmware and recommended security alerts.

Mist Edge

Customers should use Mist Edge best practices.

Wireless Configuration (AC-18, SC-18, SC-13)

Customers configure all WLAN security settings.

SSID Security

Use **WPA2 Enterprise** for internal networks.

Logging & Monitoring (AU-2, AU-6, SI-6, SI-4)

Customer should configure audit logs to agency SIEM or via API integration.

Encryption (SC-12, SC-13)

Customer should:

- Use TLS 1.2+ for API integrations.
- Follow FedRAMP guidelines for FIPS.

API Security (AC-3, IA-3, IA-5)

Customers should:

- Use API tokens based on RBAC privileges required.
- Rotate tokens every 90 days.
- Store tokens in a secure secrets manager.
- Disable unused tokens immediately.
- Use HTTPS and SSL verification for webhooks (if applicable).

Change Management (CM-3, CM-4)

Customers should document all Mist configuration changes.

Vulnerability Management (RA-5, SI-5, SI-2)

Customers should:

- Review Mist provided security advisories.
- Apply firmware updates as recommended by Juniper Mist.

Backup & Recovery (CP-9, CP-10)

Customers should perform customer org configuration API backups per FedRAMP guidelines.

References

- FedRAMP Moderate Baseline (Rev. 5)
- NIST SP 800-53 Rev. 5
- Juniper Mist SSP Package

Version History

Date	Description	Version	Author
02/25/26	Secure Configuration Guidance for FedRAMP (Moderate)	1.0	System Owner