Insecure Configuration Management

Feature history for insecure configuration management

This table describes the developments of this feature, by release.

Table 1: Feature history

Feature name	Release information	Description
Insecure configuration management	Cisco Catalyst SD-WAN Manager Release 26.1.1 Cisco IOS XE Catalyst SD-WAN Release 26.1.1	Provides centralized visibility and actionable remediation for insecure feature configurations to strengthen network security in Cisco Catalyst SD-WAN.

Resilient infrastructure

Cisco's resilient infrastructure significantly strengthens the security posture of network devices. This multi-layer framework reduces the attack surface and protects sensitive data by modernizing security capabilities.

Core objectives

- Strengthen security: Ensures devices remain inherently secure against evolving threats.
- Reduce attack surface: Deprecates and removes obsolete capabilities to eliminate exploitation risks.
- Protect data: Deploys advanced security features to safeguard sensitive information.

For more information on resilient infrastructure, see <sd-wan playbook>

Insecure configurations tab overview

Configurations that no longer meet current security requirements and increase the risk of exploitation are considered insecure. The Insecure Configurations tab in Cisco Catalyst SD-WAN enables administrators to identify and remediate these vulnerabilities. It offers centralized visibility and actionable insights into insecure settings across devices, configuration groups, and templates managed by Cisco SD-WAN Manager.

Benefits of visibility into insecure configurations

- **Centralized visibility**

  Offers a consolidated dashboard to track insecure configurations present in the network.

- **Actionable guidance**

  Provides remediation steps for each detected insecure configuration, helping maintain compliance and security.

- **Operational assurance**

  Enables administrators to identify, prioritize, and resolve insecure settings before critical operations such as upgrades.

Enable insecure configuration management

Use these steps to enable insecure configuration management.

For new networks: Insecure configuration mode is disabled by default. Administrators cannot deploy insecure configuration commands unless explicitly enabled.

For existing networks upgrading to Cisco Catalyst SD-WAN Manager Release 26.1.x: Insecure configuration mode will remain enabled. Administrators can review and remediate any insecure configurations already in use, then disable the mode if desired.

To view additional tabs such as Field Notices and Security Advisories, Cloud Services must be enabled in Admin Settings.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Admin** > **Settings** > **Insecure Configuration Mode**.

Step 2 Click **enable**.

View insecure configurations

Use these steps to view and manage insecure configurations in Cisco SD-WAN Manager.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Advisories**.

Step 2 Select the **Insecure Configurations**.

Step 3 Select **Devices** to view devices with insecure configurations.

Step 4 Select **Configuration Groups** to view insecure configuration groups in your network.

Step 5 Select **Device Templates** to view templates running insecure configurations.

What to do next

Review each insecure configuration by clicking its link to navigate directly to the relevant remediation section and apply the recommended fix. A periodic scan happens every 30 minutes to ensure the latest insecure configuration details are displayed.