Cisco 9800 Wireless Resilient Infrastructure

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

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

Resilient Infrastructure

This project is designed to significantly strengthen the security posture of Cisco network devices by introducing a comprehensive, multi-layer security framework to reduce the attack surface and protect sensitive data through the implementation of new and improved security capabilities. Some of which may require our customers to act accordingly. We are committed to making this transition as seamless and non-disruptive as possible. Here's what else you need to know.

Strategy, Timeline, and Customer Readiness

- **Proactive Security Enhancements**: To increase the security posture of Cisco devices, we are making changes to default settings, deprecating and eventually removing insecure capabilities, and introducing new security features.
- **Your Action is Key**: We encourage all customers to adopt improved security practices now and discontinue the use of insecure features. This will strengthen your security posture and prepare you for these essential enhancements.
- **Comprehensive Guidance:** This playbook provides information on these changes, our strategy for phasing them out, and specific actions you should take.

For more information, see Resilient Infrastructure.

Deprecation of Insecure Features

Insecure features are being phased out in three stages to minimize disruption:

Stage 1: Warning

Warnings are displayed on the console when insecure features are configured. We strongly recommend discontinuing their use immediately.

Stage 2: Restriction

In subsequent releases, key insecure features will be disabled by default or require explicit administrator action to enable. Existing deployments continue to function, but new installations require intentional enablement.

Some features on specific platforms may not have a restriction phase, with only warnings continuing for several releases before removal.

Stage 3: Removal

Obsolete features are planned to be removed entirely from future software releases.

The timing of removal will vary based on user impact and adoption (e.g., widely adopted features like SNMPv2 will phase out slower than less-used ones).

For more information, see the respective software Release Notes.

IOS-XE Wireless

These are the changes in Release 26.1.1:

Line Transport

This section addresses insecure configurations related to line transport protocols, specifically Telnet and Rlogin.

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

Insecure Protocols

- Telnet
- Rlogin

Impact of Non-Migration

If you upgrade to a later IOS-XE version that removes support for these protocols without migrating to SSH, the device could become completely inaccessible. You would require physical console access to recover the device.

Migration to SSH

To enable SSH, you must generate a cryptographic key and configure the transport input.

Secure Alternative Commands:

- Generate RSA Key: crypto key generate rsa
- Configure SSH Transport: line vty 0 15 transport input ssh transport output ssh
- Remote Login Example: ssh -l <USERNAME> <IP_ADDRESS>

Device Server Configuration

The primary protocol identified as insecure is HTTP (Port 80). The secure alternative is HTTPS (Port 443).

Impact of Non-Migration

Communications over port 80, including the WebUI, will fail in future releases.

Web Authentication Nuance

For guest portals, the WLC must often listen on port 80 to redirect clients. Use the following command to keep port 80 open for webauth redirection while disabling the HTTP admin server:

- webauth-http-enable
- no ip http server

Secure Alternative Commands

Enable HTTPS**:** ip http secure-server

Disable Insecure Ciphers

Migrate away from CBC-based ciphers (e.g., aes-128-cbc-sha) to modern alternatives.

File Transfer Protocols

TFTP, FTP, and RCP are unencrypted and considered insecure. SCP (Secure Copy Protocol) is the recommended alternative.

Prerequisites

SSH must be enabled on the device before SCP can function.

Secure Alternative Commands

- **Copy from WLC to Server:** copy scp:bootflash:<filename> <username>@<IP_ADDRESS>:
- **Copy from Server to WLC:** copy scp://<username>@<IP_ADDRESS>/<path-to-file> bootflash:

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

- **Specify VRF for SCP:** copy scp <source> <destination> vrf <vrf-name>

SNMP

Simple Network Management Protocol (SNMP) is a protocol used for communication between SNMP managers and agents to monitor and manage network devices.

SNMPv1, SNMPv2, SNMPv3 (noAuthNoPriv) are insecure SNMP configurations.

You are blocked from configuring the above in secure mode. Enable insecure mode using the system mode insecure command, which then triggers warnings.

Secure Alternative Commands

- snmp-server group <group-name> v3 priv read <view-name> write <view-name>
- snmp-server user <username> <group-name> v3 auth sha <auth-password> priv aes 256 <priv-password>
- snmp-server host <NMS-IP-Address> traps version 3 priv <priv-password>

Passwords and Credentials

Type 0 (plaintext), Type 5 (MD5), and Type 7 (proprietary Cisco) passwords are deemed insecure.

Recommended Types

- **Type 6:** AES-based encryption.
- **Type 8:** SHA-256 with PBKDF2.
- **Type 9:** Scrypt.

Secure Alternative Commands

- **Enable Secret:** enable secret 9 <password>
- **Username:** username <name> algorithm-type sha256 secret <password>

These are additional warning messages related to wireless on 9800 WLC:

Table 1. Wireless warning messages

Feature	Warning Message	Insecure Command	Secure Recommendation
NMSP	`%NMSP_SYSLOG-1-NMSP_INSECURE_CIPHER_NOTICE: Chassis 1 R0/0: nmspd: NMSP INSECURE CIPHER WARNING: no nmsp strong-cipher CLI uses Insecure cipher and alternative is nmsp strong-cipher`	`no nmsp strong-cipher`	Use this command: nmsp strong-cipher
Mobility	`SECURITY WARNING - Module: MM_MGR - Command: no wireless mobility high-cipher - Reason: Mobility DTLS with high cipher mode is not enabled`	`no wireless mobility high-cipher`	Enable High cipher mode
WLAN	`SECURITY WARNING - Module: WLANMGR - Command: security wpa akm dot1x - Reason: dot1x is not a secure`	`security wpa akm dot1x`	Consider using high secure methods like dot1x-sha256 or suite-B-192 for wlan

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

Feature	Warning Message	Insecure Command	Secure Recommendation
	authentication key management method		
WLAN	SECURITY WARNING - Module: WLANMGR - Command: security wpa akm psk - Reason: psk is not a secure authentication key management method	security wpa akm psk	Consider using high secure methods like psk-sha256 or SAE for wlan
AP DTLS Version 1.0	SECURITY WARNING - Module: CAPWAP, Command: ap dtls-version dtls_1_0 , Reason: Weak tls version, Description: Access Point DTLS version configured with DTLS 1.0 - deprecated and vulnerable to various attacks,	ap dtls-version dtls_1_0	Use stronger tls version to enhance security
AP DTLS Ciphersuite (AES128-SHA)	SECURITY WARNING - Module: CAPWAP, Command: ap dtls-ciphersuite priority 0 AES128-SHA , Reason: Weak cipher(s) are present in the command, Description: Access Point DTLS cipher suite configured with weak ciphers using SHA-1 - vulnerable to collision attacks	ap dtls-ciphersuite priority 0 AES128-SHA	Use stronger cipher(s) to enhance security
AP DTLS Ciphersuite (DHE-RSA-AES128-SHA)	SECURITY WARNING - Module: CAPWAP, Command: ap dtls-ciphersuite priority 0 DHE-RSA-AES128-SHA , Reason: Weak cipher(s) are present in the command, Description: Access Point DTLS cipher suite configured with weak ciphers using SHA-1 - vulnerable to collision attacks	ap dtls-ciphersuite priority 0 DHE-RSA-AES128-SHA	Use stronger cipher(s) to enhance security
AP DTLS Ciphersuite (DHE-RSA-AES256-SHA)	SECURITY WARNING - Module: CAPWAP, Command: ap dtls-ciphersuite priority 0 DHE-RSA-AES256-SHA , Reason: Weak cipher(s) are present in the command, Description: Access Point DTLS cipher suite configured with weak ciphers using SHA-1 - vulnerable to collision attacks	ap dtls-ciphersuite priority 0 DHE-RSA-AES256-SHA	Use stronger cipher(s) to enhance security

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