Cisco 9800 Wireless Resilient Infrastructure

© 2026 Cisco Systems, Inc., 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.

As part of the overall deprecation and removal strategy, the second phase restricts the use of insecure features, but does not remove the feature entirely. When configuring a device from scratch, administrators must take additional action to indicate that they are intentionally enabling an insecure feature or protocol.

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 and syslog messages 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. This requires the box to be enabled in insecure mode (discussed later). 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.

Insecure mode and Secure mode

IOS-XE will implement restrictions by creating an "insecure mode" which must be enabled to use these features. This mode will be enabled automatically on upgrades to the target release if any of the insecure features are enabled prior to the upgrade. This ensures that networks remain operational when upgrading to the release with restrictions. New / fresh installations of these target releases will restrict the use of these features and protocols by default.

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

IOS-XE Wireless

For new installation on 26.1.x or upgrade to this release with no insecure configuration, the system will be in Secure mode:

```
9800-WLC#show system security mode
  System Security Mode : Secure
```

In Secure mode, configuring an insecure command is not permitted and a warning message is displayed:

```
9800-WLC(config)#line vty 0 4
9800-WLC(config-line)#transport input telnet
%Error:Insecure configurations are not permitted in secure mode. To proceed, set the system mode to insecure using the command system mode insecure, and then try again.
Module: LINE, Command: transport input telnet , Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of encryption and authentication, Remediation: Migrate to secure SSH-based remote access
%ERROR: Security policy check failed, configuration can't be applied
```

To configure the insecure command in Secure mode, you first need to enable insecure mode on the WLC:

```
9800-WLC(config)#system mode insecure
Mar 23 10:18:01.292: %SYS-4-SYSTEM_SECURITY_MODE_CHANGE: System Security Mode Changed from SECURE to INSECURE
9800-WLC(config)#do show system security mode
System Security Mode : Insecure
```

Insecure commands can be configured after entering insecure mode with a warning.

```
9800-WLC(config-line)#transport input telnet
 SECURITY WARNING - Module: LINE, Command: transport input telnet , Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of encryption and authentication, Description: Line transport configured with unencrypted protocols - allows plaintext transmission of sensitive data, Remediation: Migrate to secure SSH-based remote access
```

Insecure commands can be configured after entering insecure mode with a warning. The system will remain in insecure mode if upgrading to version 26.1.1 from older releases with an insecure configuration.

To transition from insecure mode to secure mode, use the “no security mode insecure” command. The system must scan for insecure commands for 30 minutes.

```
9800-WLC(config)#no system mode insecure
System secure mode cannot be changed to secure as insecure configuration scanning is in progress. Try after 23 min 29 sec.
```

After the scan is complete, all insecure CLIs are displayed:

```
9800-WLC(config)#no system mode insecure


System secure mode cannot be changed to secure as insecure cli(s) are present in system.
```

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

```
9800-WLC#show system insecure configuration
(snip)
+------------------------------------------------------------
| ACTIVE INSECURE CONFIGURATION ENTRY [1/1]
+------------------------------------------------------------
|               Module: LINE
|       Parent Command: line vty 0 4
|          CLI Command: transport input telnet
|          Description: Line transport configured with unencrypted protocols - allows plaintext transmission
of sensitive data
|               Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of
encryption and authentication
|       Remediation: Migrate to secure SSH-based remote access
```

Try removing the insecure commands which re-initiates the scan:

```
9800-WLC(config-line)#no transport input
9800-WLC(config)#no system mode insecure
System secure mode cannot be changed to secure as insecure configuration scanning is in progress. Try after
12 min 24 sec.
```

Once scan is complete, secure mode can be enabled again:

```
9800-WLC(config)#no system mode insecure
System secure mode cannot be changed to secure as insecure configuration scanning is in progress. Try after
0 min 9 sec.
9800-WLC(config)#no system mode insecure
Apr 7 11:03:44.761: %SYS-4-SYSTEM_SECURITY_MODE_CHANGE: System Security Mode Changed from INSECURE to SECURE
9800-WLC(config)#do show system security mode
System Security Mode : Secure
9800-WLC(config)#do sh system insecure configuration
============================================================
          ACTIVE INSECURE CONFIGURATION DATABASE
============================================================
Generated: Active Configuration Analysis
Total Active Insecure Commands: 0
```

Note: Also starting with IOS XE 17.18.2, error messages will display on boot/upgrade for all detected insecure configurations. The format of the generated log will be as follows: %SYS-4-INSECURE_CONFIG or %SYS-4-INSECURE_DYNAMIC_WARNING

Both the command output and syslog warnings are typically followed by one or more of the following sections (not all messages include all the sections):

- Module: The IOS XE component that generated the log message, for example, LOGGING, HTTP, or LINE
- Command: The specific command configured that triggered the warning message

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

- Reason: The reason why this feature or protocol is insecure
- Description: Additional details as to why the feature or protocol is insecure
- Remediation: Alternatives or action to take to migrate to a more secure alternative

Example:

```
SECURITY WARNING - Module: SNMP, Command: snmp-server community * * , Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of encryption and authentication, Description: SNMP community string configured - uses insecure SNMPv1/v2c protocol vulnerable to eavesdropping, Remediation: Configure snmp v3 user
```

We will now look at each type of command in more detail:

Line transport

Overview

This section covers insecure configurations pertaining to the line transport protocols. The major protocol that is marked insecure is the Telnet protocol. The secure alternative is the Secure Shell (SSH) protocol. Note that as a prerequisite to using SSH, you will need to generate a crypto key on the device. Just enabling the SSH transport without the crypto key would not permit SSH connections to the device.

The line transport protocols considered insecure as of IOS XE 26.1.1 are

- telnet
- rlogin

What happens if you do not migrate?

If you do not migrate to SSH before upgrading to a later IOS XE release that removes support for all insecure commands, the device will be completely locked out. This occurs since Telnet (and rlogin) commands will no longer be applicable, leaving no transport protocol configured.

If you are in the situation outlined above, to recover the device you will have to physically console into the device and configure SSH as the transport protocol. You will then have to generate a crypto RSA key and enable a username and password. This will enable you to log in remotely to the device. The commands for achieving this are given below.

Commands for restoring remote access to a device via SSH:

Step 1. Generate a crypto RSA key

```
crypto key generate rsa
```

Step 2. Remove existing configurations (line transport configurations and enable SSH)

```
Line #/vty#/console
  Transport input ssh
  Transport output ssh
```

If a username/password is configured, SSH will now be enabled for remote access to the device.

If you are using device consoles to connect to neighboring devices, after SSH is enabled, you can use SSH to log in to the neighboring devices. You will have to ensure that the neighboring devices are also configured to support SSH connections:

```
ssh -l <USERNAME> <IP_ADDRESS>
```

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

List of affected line transport commands

The following table lists the full set of line transport commands affected by this announcement. If you are running any of these commands, we strongly recommended migrating to SSH as outlined above.

Table 1. Insecure line transport commands

Global Config	line <x/y/z> transport output <rlogin| telnet>
Global Config	line <x/y/z> transport output all
Global Config	line <x/y/z> transport input <rlogin| telnet>
Global Config	line <x/y/z> transport input all
Global Config	line <x/y/z – x/y/z> transport output <rlogin| telnet>
Global Config	line <x/y/z – x/y/z> transport output all
Global Config	line <x/y/z – x/y/z> transport input <rlogin| telnet>
Global Config	line <x/y/z – x/y/z> transport input all
Global Config	line vty 0 n transport output <rlogin| telnet>
Global Config	line vty 0 n transport output all
Global Config	line vty 0 n transport input <rlogin| telnet>
Global	line vty 0 n

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

Config	transport input all

Global Config	telnet <IP_address>

Device Server Configurations

Overview

This section covers insecure configurations with respect to HTTP. The major protocol that is considered insecure is HTTP. The secure alternative is HTTPS.

The device server protocols considered insecure as of IOS XE 26.1.1 is

```
ip http server
```

What happens if you do not migrate?

If you do not migrate to HTTPS before upgrading to a later IOS XE release that removes support for all insecure commands, communications over port 80 to the device will not work. This includes the webUI for the device. If you use webUI for configuring the device, you will be locked out of accessing the webUI.

Note that communications over port 80 across the switch (pass-through traffic) will be unaffected. Only traffic over port 80 that is initiated or terminated on the switch in question will be affected.

Additionally, some of the ciphers that can be used over port 443 (HTTPS) are considered insecure, and we recommend migrating to a secure cipher instead.

Command for migrating to HTTPS

We recommend migrating to an HTTPS server (over port 443) instead of port 80. An example configuration is as follows:

```
(config) ip http secure-server
```

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
```

List of affected device server commands and commands for configuring a secure cipher

The following table lists the full set of device server commands affected by this announcement. In addition, some ciphers over port 443 are also considered insecure. The table lists commands for specifying secure ciphers.

Table 2. Insecure device server commands and commands for configuring secure ciphers

Global Config mode	ip http server

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

Global Config mode	ip http tls-version <TLSv1.0/1.1>
Global Config mode	ip http client tls-version <TLSv1.0/1.1>
Global Config mode	ip http secure-ciphersuite ecdhe-rsa-aes-128-cbc-sha
Global Config mode	ip http secure-ciphersuite aes-128-cbc-sha
Global Config mode	ip http secure-ciphersuite aes-256-cbc-sha
Global Config mode	ip http client secure-ciphersuite aes-256-cbc-sha
Global Config mode	ip http client secure-ciphersuite aes-128-cbc-sha

File Transfer Protocols

Overview

This section covers insecure configurations pertaining to the file transfer protocols. The major protocols that are considered insecure are TFTP and FTP. The secure alternative is the Secure Copy Protocol (SCP). Note that as a prerequisite to using SCP, you will need to enable SSH access on the device. Refer to the Line Transport section above for details on how to do this. Performing an SCP transfer without SSH configured will lead to failure of the transfer.

The file transfer protocols considered insecure as of IOS XE 26.1.1 are

- FTP
- TFTP
- RCP

What happens if you do not migrate?

If you do not migrate to SSH and SCP before upgrading to a later IOS XE release that removes support for all insecure commands, you will be unable to perform file transfer operations using FRP, TFTP, or RCP. This applies to both transfer operations from the switch and operations to the switch.

If you are in the situation described above, you will first need to enable SSH connections on the device (as outlined in the Line Transport section). Once this is done, you will be able to run SCP transfers.

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

Secure alternative commands

Once SSH is enabled, use the following command to initiate SCP transfers to and from the WLC:

```
copy scp source: destination:
```

Examples:

Copy a file from a WLC to a server (IP address 10.1.1.1):

```
copy scp bootflash:test_file username@10.1.1.1
```

Copy a file from a server (10.1.1.1) to a WLC:

```
copy scp username_10.1.1.1:<path-to-file> bootflash:
```

There are several commands that are used to specify connection details. These include specifying source interfaces (or IP addresses) to be used for the file transfers. Most of these can just be included in the SCP command itself and do not require a command to be configured. Other examples include the username and password for the connection. Again, these can just be included in the SCP command syntax itself.

Examples:

```
ip rcmp source-interface <>
ip ftp source-interface <>
ip tftp source-interface <>
```

For the above commands, you can use SCP with the VRF simply specified as follows:

```
copy scp <source> <destination> vrf [vrf-name]
```

In the case of TFTP connections, the blocksize can be specified with the following command:

```
ip tftp blocksize <>
```

While an alternative is not needed in most cases, you can use the command below to tweak the block size:

```
ip ssh bulk-mode <>
```

List of affected file transfer commands

Table 3. Insecure file transport commands

Exec mode	copy ftp
Global Config mode	ip ftp passive
Global Config mode	ip ftp password <uint8 0..7>
Global Config mode	ip ftp password < uint8 0..7> <string>
Global Config mode	Switch(config) ip ftp source-interface <type> <string>

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

Global Config mode	ip ftp username <string>
Exec mode	copy <> ftp:
Global Config mode	ip rcmd domain-lookup
Global Config mode	ip rcmd rcp-enable
Global Config mode	ip rcmd rsh-enable
Exec mode	copy <> rcp:
Exec mode	copy rcp: <>
Global Config mode	ip rcmd remote-host
Global Config mode	ip rcmd remote-username
Global Config mode	ip rcmd rsh-disable-command
Global Config mode	ip rcmd source-interface
Global Config mode	ip tftp blocksize <>
Global Config mode	ip tftp source-interface
Exec mode	copy tftp: <>
Exec mode	copy <> tftp:

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

Simple Network Management Protocol (SNMP)

Overview

This section covers insecure configurations with respect to SNMP. Collecting telemetry from switches is an important aspect of network maintenance and troubleshooting. SNMP itself is a mature solution that can be used to collect a lot of information about different features and processes from the switch. Due to its age, however, SNMP contains a lot of commands that are deemed insecure. The recommendation is to migrate to newer technologies like NETCONF or RESTCONF and using YANG models or streaming telemetry technologies like gNMI or gRPC for richer data collection over a better, more secure transport protocol such as HTTPS.

If, however, you cannot migrate away from SNMP, the recommendation is to use SNMPv3, as it provides robust user-based authentication and message integrity compared with SNMPv1 and v2, which rely on weak, unencrypted community strings. With SNMPv3, the recommendation would be to use a more secure cipher and password type.

What happens if you do not migrate?

If you do not migrate to either NETCONF/RESTCONF with API calls or to SNMPv3 with secure ciphers and passwords, and you upgrade to an IOS XE release that removes support for insecure commands, your SNMP functionality will fail. This means that you will no longer be able to collect information from the switch using SNMP. To recover, you will have to reconfigure your SNMP using SNMPv3 with the recommended ciphers, or you will have to migrate to NETCONF/RESTCONF using API calls instead.

Secure alternative commands

Given the nature of SNMP, it is difficult to provide one-to-one mapping of insecure and alternative commands. The amount of information collected depends on the object identifiers (OIDs) that were polled from the switch, and the scope of the commands makes collating them all in this document impossible.

If you are migrating to SNMPv3 instead, one advantage is that the OIDs in use will remain the same if you were using SNMP v2 or v2c. The only change will be to the format in which the messages are sent. For this, you will have to enable SNMPv3 using the commands below:

```
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>
```

Table 4. Insecure SNMP commands

Global Config mode	snmp-server user <> <> v3 auth (sha/sha2/md5) | (0, 6,7) <> priv <des> | (0,6,7) <> access <ipv6>
Global Config mode	snmp-server user <> <> v3 auth (sha/sha2/md5) | (0, 6,7) <> priv <des> | (0,6,7) <> access <1-99>
Global Config mode	snmp-server user <> <> v3 auth (sha/sha2/md5) | (0, 6,7) <> priv <des> | (0,6,7) <> access <std-acl>

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

Global Config mode	snmp-server user <> <> v3 auth (sha/sha2/md5) | (0, 6,7) <> priv <3des> | (0,6,7) <> access <ipv6>
Global Config mode	snmp-server user <> <> v3 auth (sha/sha2/md5) | (0, 6,7) <> priv <3des> | (0,6,7) <> access <1-99 >
Global Config mode	snmp-server user <> <> v3 auth (sha/sha2/md5) | (0, 6,7) <> priv <3des> | (0,6,7) <> access <std-acl>
Global Config mode	snmp-server user <> <> v3 encrypted auth (md5) access <ipv6 | (1-99) | std-acl>
Global Config mode	snmp-server user <> <> v3 encrypted auth (sha/sha2/md5) | (0, 6,7) <> priv <des> | (0,6,7) <> access <ipv6>
Global Config mode	snmp-server user <> <> v3 encrypted auth (sha/sha2/md5) | (0, 6,7) <> priv <des> | (0,6,7) <> access <(1-99)>
Global Config mode	snmp-server user <> <> v3 encrypted auth (sha/sha2/md5) | (0, 6,7) <> priv <des> | (0,6,7) <> access <std-acl>
Global Config mode	snmp-server user <> <> v3 encrypted auth (sha/sha2/md5) | (0, 6,7) <> priv <3des> | (0,6,7) <> access <ipv6>
Global Config mode	snmp-server user <> <> v3 encrypted auth (sha/sha2/md5) | (0, 6,7) <> priv <3des> | (0,6,7) <> access <(1-99) >
Global Config mode	snmp-server user <> <> v3 encrypted auth (sha/sha2/md5) | (0, 6,7) <> priv <3des> | (0,6,7) <> access <std-acl>
Global Config mode	snmp context <> user <> auth sha <> priv aes (128|192|256) <> >router ospf 1/bgp 1/isis 1 >snmp context ctx community *
Global Config mode	snmp context <> user <> auth sha <> priv aes (128|192|256) <> access <ipv6> >router ospf 1/bgp 1/isis 1 >snmp context ctx community *
Global Config mode	snmp context <> user <> auth sha <> priv aes (128|192|256) <> access <std-acl> >router ospf 1/bgp 1/isis 1

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

	>snmp context ctx community *
Global Config mode	snmp context <> user <> auth sha <> priv aes (128|192|256) <> access <1-99> >router ospf 1/bgp 1/isis 1 >snmp context ctx community *
Global Config mode	snmp context <> user <> auth sha <> priv aes (128|192|256) <> access <ipv6> >router ospf 1/bgp 1/isis 1 >snmp context ctx community *
Global Config mode	snmp context <> user <> auth sha <> priv aes (128|192|256) <> access <std-acl> >router ospf 1/bgp 1/isis 1 >snmp context ctx community *
Global Config mode	Snmp-server community <0|7> < > <ro|rw> access <ipv6 | (1-99) | std-acl>
Global Config mode	snmp mib community-map <0|7> <> context <> (engineid | security-name|target-list)
Global Config mode	snmp-server user <> <> v3 auth md5 | (0, 6,7) <> priv <des> | (0,6,7) <>
Global Config mode	snmp-server user <> <> v3 auth md5 | (0, ,7) priv <3des> | (0,6,7) <>
Global Config mode	snmp-server user <> <> v3 auth md5 | (0,7) <> priv <des/3des> | (0,7) <>
Global Config mode	snmp-server user <> <> v3 auth md5 | (0, 6,7) <> priv <des/3des> | (0,6,7) <>
Global Config mode	Snmp-server group <> v3 <auth|noauth> access (ipv6| (1-99) | std-acl)
Global Config mode	Snmp-server group <> v3 priv context <>access (ipv6| (1-99) | std-acl)
Global Config mode	snmp-server host <> version {1|2c} * {0|7} <community>
Global Config mode	snmp-server host <> version {1|2c}* {0|7} <community> udp-port <0-65535>

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

Global Config mode	snmp-server host <> vrf <1-65535> version {1|2c}* {0|7} <community>
Global Config mode	snmp-server host <> vrf <1-65535> version {1|2c} * {0|7} udp-port <0-65535>
Global Config mode	snmp-server host <> version {3} (auth|noauth) <username>
Global Config mode	snmp-server host <> version (auth|noauth) <community> udp-port <0-65535>
Global Config mode	snmp-server host <> vrf <1-65635> version {3} (auth|noauth) <username>
Global Config mode	snmp-server host <> vrf <1-65635> version {3} (auth|noauth) <username> udp-port <0-65535>
Global Config mode	snmp-server host <> version {1|2c} * {0|7} <community>
Global Config mode	snmp-server host <> version {1|2c} * {0|7} <community> udp-port <0-65535>
Global Config mode	snmp-server host <> vrf <1-65535> version {1|2c} * {0|7} <community> udp-port <0-65535>
Global Config mode	snmp-server host <> vrf <1-65535> version {1|2c} * {0|7} <community>
Global Config mode	snmp context abc user [^]+((credential|access|encrypted))? auth md5 [^]+(access)?
Global Config mode	snmp context abc user [^]+((credential|access|encrypted))? auth sha [^]+ priv des (access)?
Global Config mode	snmp context abc user [^]+((credential|access|encrypted))? auth sha [^]+ priv 3des (access)?
Global Config mode	snmp context abc user [^]+(encrypted))? auth md5 [^]+(access)?
Global Config mode	snmp context abc user [^]+((encrypted))? auth sha [^]+ priv des (access)?
Global Config mode	snmp context abc user [^]+((encrypted))? auth sha [^]+ priv 3des (access)?

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

Global Config mode	snmp context abc user [^]+((credential|access))? auth md5 [^]+(access)?
Global Config mode	snmp context abc user [^]+ auth sha [^]+ priv des <> access <ipv6>
Global Config mode	snmp context abc user [^]+ auth sha [^]+ priv 3des <> access <1-99>
Global Config mode	snmp context abc user [^]+(encrypted))? auth md5 [^]+(access)?
Global Config mode	snmp context abc user [^]+(encrypted))? auth md5 [^]+ priv des (access)?
Global Config mode	snmp context abc user [^]+((encrypted))? auth md5 [^]+ priv 3des (access)?
Global Config mode	Snmp-server community < > <ro|rw>
Global Config mode	snmp mib community-map <> context <> (engineid | security-name|target-list)
Global Config mode	Snmp-server group <> (v1)
Global Config mode	Snmp-server group <> (v2c)

Miscellaneous

Overview

This section covers insecure configurations that cannot be classified into any of the other sections here. Some examples of the features covered in this section are BOOTP server, Network Time Protocol (NTP) authentication, and logging Transport Layer Security (TLS) profile.

Given the diverse nature of the features covered here, we've collected all of the commands and secure alternatives into a table.

What happens if you do not migrate?

Given the diverse nature of the features in this section, it is difficult to describe a general impact.

If you migrate to a later IOS XE release that removes support for these insecure commands, functionality around the specific features will be impacted.

List of affected miscellaneous commands

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

Table 5. Miscellaneous insecure commands

Global config mode	ntp authentication-key <num> md5 <string>	Use cipher <> instead
Global config mode	logging tls-profile <> tls-version TLSv1.1	Use TLS 1.2 or later
Global config mode	logging tls-profile <> ciphersuite <aes-128-cbc-sha | aes-256-cbc-sha>	Use cipher <> instead

Passwords and credentials

Overview

This section covers insecure configurations pertaining to configured passwords and credentials. All types of passwords 0, 5, and 7 passwords are considered insecure, and the recommendation is to use type 6, 8, or 9 passwords instead.

We are taking a different approach with passwords. If you are using passwords of types 0 or 7, the system will automatically attempt to convert that password to a type 6 password. Type 6 passwords use strong AES 128-bit encryption, making them difficult to break. Type 6 passwords have been supported since 2006 onward, and most of the features already support type 6 passwords. However, if there is a feature that doesn't support type 6, insecure mode will be enabled automatically for that feature and deprecation will occur only when type 6 password support is added for that feature.

What happens if you do not migrate?

Ideally, type 0 and 7 passwords should automatically be converted to type 6. Passwords are inherently vital for securing access to the system, and we strongly recommend migrating the device to the newer, more secure alternatives outlined below as soon as possible.

Type 6 password auto-conversion

On upgrade to IOS XE 26.1.1, if a master key is not configured, one will automatically be generated and displayed at boot time. The configured passwords will then be migrated from types 0 and 7 to type 6. The master key is unique per device and is not stored in the configuration file.

However, if a master key was already configured on the box, all auto-converted type 6 passwords will use the same master key.

List of affected password commands

The following table lists the password commands affected by this announcement.

Table 6. Insecure password commands

Global config mode	enable password [1|7] <password>

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

Global config mode	enable secret [1|7] <password>
Global config mode	ip scp password <password>
Global config mode	ip dhcp pool <pool_name> authorization shared-password <password>
Global config mode	group-policy server username <username> password [0 7] <password>
Global config mode	cts policy-server username <username> password [0 7] <password>
Global config mode	cts sxp default password [0 6 7] <password>
Global config mode	group-policy server username <username> password [0 7] <password>
Global config mode	cts credential id <device-id> password <password>
Global config mode	line vty [0 15] username <> password <>
Global config mode	ip wccp web-cache password

Here are some additional warning messages related to wireless on 9800 controllers:

Table 7. Wireless warning messages

Feature	Warning Message	Insecure Command	Secure Recommendation
WLAN	SECURITY WARNING - Module: WLANMGR - Command: security wpa akm dot1x - Reason: dot1x is not a secure authentication key management method	security wpa akm dot1x	Consider using high secure methods like dot1x-sha256 or suite-B-192 for wlan
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	ap dtls-version dtls_1_0	Use stronger tls version to enhance security

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

Feature	Warning Message	Insecure Command	Secure Recommendation
	configured with DTLS 1.0 - deprecated and vulnerable to various attacks		
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 Systems, Inc., and/or its affiliates. All rights reserved.

Conclusion

The first step of security is to clean up the configurations on the device by removing known insecure commands and migrating to secure alternatives. This document covers most of the commands that are now considered insecure. This must not be treated as an exhaustive list. The first source of truth would be the logs generated on 9800 WLC on IOS XE releases 17.18.2 and later.

Complete details on all Insecure Feature Warnings in 26.1.1

This document will be updated as more commands are identified as insecure. Please bookmark this document and review it again closer to the release of IOS XE versions 26.2.x and IOS-XE 27.1.x

While efforts are underway to ensure a smooth migration to secure configurations wherever possible, automatic migrations may not be possible for most of the use cases outlined above. The strong recommendation is to migrate to secure alternatives as soon as possible to enable smooth upgrades to later IOS XE releases. Upgrading to IOS XE 26.2.x and IOS XE 27.1.x and later without migrating the commands as described here will lead to issues and is strongly discouraged.

To learn more about resilient infrastructure, please visit the following webpage:

Resilient Infrastructure

This document is about resilient infrastructure on the C9800 WLCs. For recommendations on migration, please refer to the IOS XE bulletin.

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