Cisco IOS XE Resilient Infrastructure Playbook for Industrial IoT

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

Resilient Infrastructure Overview 3
Infrastructure Resilience Releases and Affected Industrial IoT Commands 3
Customer Readiness Checklist 4
Additional Information 4

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

Resilient Infrastructure Overview

Cisco is improving the security of industrial network environments by updating IOS XE configurations. This initiative replaces legacy, insecure commands with secure alternatives. These changes reduce the attack surface, remove insecure technologies and features, strengthen default settings, and improve product security.

Cisco is introducing these changes in phases. Warnings begin in Cisco IOS XE Release 17.18.2, restrictions begin in Cisco IOS XE Release 26.1.1, and selected insecure features will be removed in future releases. The timing and impact vary by feature, platform, and software release. Customers should migrate to secure alternatives as soon as possible to minimize upgrade risks.

Infrastructure Resilience Releases and Affected Industrial IoT Commands

The following tables summarize the Infrastructure Resilience feature changes by release and list the affected Industrial IoT commands.

Table 1. Infrastructure Resilience Feature Summary

Release	Changes
17.18.2 (Awareness)	• A “warning only” release that identifies risks without affecting operations. • Syslog alerts that are generated when insecure features are configured. • Credential alerts for weak Type 0, Type 5, and Type 7 passwords. • Insecure features targeted for restriction include legacy protocols such as Telnet, HTTP, SNMPv1, and SNMPv2c, and weak cryptographic standards such as DES and MD5. For more details refer to Resilient Infrastructure IOS XE Security Warnings Reference.
26.1.1 (Restriction)	This release introduces a concept called System mode. There are two different modes. Secure and Insecure system modes to control the use of legacy features. You must explicitly configure the **system mode insecure** command to use legacy features. • To support a smooth upgrade and prevent operational disruption, the **system mode insecure** command is automatically applied if insecure configurations are present in the previous release. • The system scans periodically and generates recurring alerts every 24 hours for active insecure configurations. For more details refer to Insecure Feature Restrictions on IOS XE.
Upcoming Release (Secure Defaults & Enhanced Visibility)	• Legacy file transfer protocols, such as FTP and TFTP, are identified as insecure. These configurations trigger administrative warnings in secure and insecure modes. • Standardized security warning reporting and classification. • Guest Shell audit monitoring for security-sensitive operations. • Secure defaults introduced for proxy ARP, NTP control mode, and HTTPS. Express Setup is an exception.
Future Releases (Security Hardening & Legacy Feature Removal)	• Modernized SSH host authentication with support for ECDSA and X.509 certificate-based authentication. • The system generates warnings that prompt users to configure a master key and notify them that future software upgrades might be blocked if a master key is not configured. • YANG-based master key support to improve automation and centralized key administration. • Insecure commands will be deprecated and progressively removed across future releases. • Master keys are generated by default, which allows passwords to be stored with secure Type 6 encryption. • Upgrades to future releases are blocked when obsolete configurations are detected in the source release. • Support for Network Time Security (NTS) to strengthen NTP authentication and integrity. • Deprecation of TLS 1.0, TLS 1.1, and associated weak cryptographic ciphers.

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

Table 2. Industrial IoT Command List

Command mode	Affected command
Global config	**cip security** {**password** <password>| <window timeout value>} **Note**: This Industrial Ethernet command is modified to convert Type 0 and Type 7 passwords to Type 8 when they are added.
Global config	**lte450 profile id** <id> **authentication** <chap | none | pap> **username** <username> **password** <password> **Note:** This Industrial Routing command now supports Type 6 password encryption.

Important Note: Before you upgrade to a later Cisco IOS XE release that removes support for insecure commands, replace those commands with their secure equivalents. Otherwise, the affected features might not work as expected after the upgrade.

Customer Readiness Checklist

- Review the running configuration for insecure features by using the **show system insecure** configuration command, where supported.
- Identify a recommended secure alternative for each affected function and assess the operational impact.
- Test the updated configuration in a lab or during a scheduled maintenance window before deployment.
- Update management tools, automation, and operational procedures as needed.
- Complete the remediation before upgrading to a release that restricts or removes the affected feature.

Additional Information

To learn more about resilient infrastructure, refer https://www.cisco.com/c/en/us/about/trust-center/resilient-infrastructure.html

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