Feature Deprecation and Removal Details

The following list of features and protocols are planned for eventual removal from Cisco products. The list indicates which features are currently supported by each operating system. The expected release numbers for warnings and feature restrictions are outlined in the feature deprecation and removal strategy. Final feature removal dates will be updated in this document when the release number becomes available.

Some features will not transition through a “restriction” phase and will go directly from warnings to removal. For these features, you will see a release number for the “warning” phase, but N/A for the “restriction.”

Insecure Feature Warnings

Devices will generate security warnings if any of the following features or protocols are enabled when the device is upgraded to the following versions. These warnings are displayed at the time of configuration along with periodic logging events if the insecure feature is still enabled. Please note that releases are subject to change, and this data will be updated as needed.

Feature / Protocol	Operating System / Platform Release				
	IOS XE	IOS XR	NXOS	ISE	ASA/FTD
Plain-text and weak credential storage: Type 0 (plain text), 5 (MD5), or 7 (Vigenère cipher) in configuration files	17.18.2	25.4.1	10.7.1	N/A **	N/A
SSH Version 1	17.18.2	25.4.1	N/A	N/A **	N/A
SNMPv1 / SNMPv2c	17.18.2	25.4.1	10.7.1	3.6	10.5/9.25
SNMPv3 without authentication and encryption (noAuthNoPriv or authNoPriv)	17.18.2	25.4.1	10.7.1	3.6	10.5/9.25
MD5 for authentication and 3DES for encryption of SNMPv3 traffic	17.18.2	25.4.1	N/A	3.6	10.5/9.25
IP source routing based on IP header options	17.18.2	N/A	10.7.1	N/A	N/A
TLS 1.0 / TLS 1.1	17.18.2	25.4.1	10.7.1	3.6	10.5/9.25
TLS ciphers using SHA1 for digital signatures	N/A	N/A	N/A	N/A	Yes
Telnet	17.18.2	25.4.1	10.7.1	N/A **	N/A
FTP	17.18.2	25.4.1	10.7.1	3.6	10.5/9.25

TFTP	17.18.2	25.4.1	10.7.1	3.6	10.5/9.25
HTTP (with some exceptions like OCSP and SCEP)	17.18.2	25.4.1	10.7.1	3.6	N/A
On-Demand Routing (ODR)	17.18.2	N/A	N/A	N/A	N/A
BootP server	17.18.2	N/A	N/A	N/A	N/A
TCP and UDP small servers (echo, chargen, discard, daytime)	17.18.2	N/A	N/A	N/A **	N/A
IP Finger	17.18.2	N/A	N/A	N/A	N/A
NTP control messages	TBA	N/A	N/A	N/A	N/A
TACACS+ using pre-shared keys and MD5	17.18.2	25.4.1	10.7.1	N/A	10.5/9.25
RADIUS using pre-shared keys and MD5 (not using RadSec)	26.1.1	25.4.1	10.7.1	3.6	11.0

Insecure Feature Restrictions

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.

Some platforms (IOS XE, NXOS, and ASA/FTD) 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. More details of the operation of “insecure mode” will be available here as we approach the release dates for each platform.

The continued usage of these features or protocols is highly discouraged and expose customers to additional risk. Cisco recommends using secure alternatives as outlined in the Feature removal and suggested alternatives document. Also note that release numbers are subject to change, and this data will be updated as needed.

Feature / Protocol	Operating System / Platform Release				
	IOS XE	IOS XR	NX OS	ISE	ASA/FTD
Plain-text and weak credential storage: Type 0 (plain text), 5 (MD5), or 7 (Vigenère cipher) in configuration files	26.2.1 *	N/A	10.7.3	N/A **	N/A
SSH Version 1	26.1.1	26.3.1	N/A	N/A **	N/A
SNMPv1 / SNMPv2c	26.1.1	N/A	10.7.2	3.6	11.0
SNMPv3 without authentication and encryption (noAuthNoPriv or authNoPriv)	26.1.1	N/A	10.7.2	3.6	11.0
MD5 for authentication and 3DES for encryption of SNMPv3 traffic	26.1.1	N/A	10.7.2	N/A	11.0
IP source routing based on IP header options	26.1.1	N/A	10.7.2	N/A	N/A
TLS 1.0 / TLS 1.1	26.1.1	26.3.1	10.7.2	3.6	11.0
TLS ciphers using SHA1 for digital signatures	26.1.1	N/A	N/A	N/A	N/A
Telnet	26.1.1	26.3.1	10.7.2	N/A **	N/A
FTP	26.1.1	26.2.1	10.7.2	3.6	11.0
TFTP	26.1.1	26.2.1	10.7.2	3.6	11.0
HTTP (with some exceptions like OCSP and SCEP)	26.1.1	N/A	10.7.2	3.6	N/A
On-Demand Routing (ODR)	26.1.1	N/A	N/A	N/A	N/A
BootP server	26.1.1	N/A	N/A	N/A	N/A
TCP and UDP small servers (echo, chargen, discard, daytime)	26.1.1	N/A	N/A	N/A **	N/A
IP Finger	26.1.1	N/A	N/A	N/A	N/A
NTP control messages	TBA	N/A	N/A	N/A	N/A
TACACS+ using pre-shared keys and MD5	26.1.1	N/A	10.7.2	N/A	11.0
RADIUS using pre-shared keys and MD5 (not using RadSec)	N/A	N/A	N/A	N/A	N/A

* IOS XE 26.2.1 will introduce auto-conversion of type 0 and type 7 credentials to type 6 credentials. Please refer to the Type 6 Key Auto Generation and Conversion document for more details on this feature.

** Feature removed as of ISE 3.5