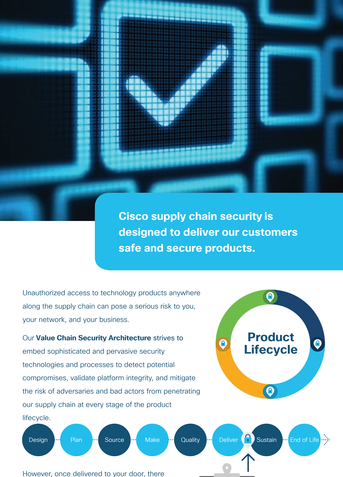
The Cisco Product Integrity Checklist



Cisco supply chain security is designed to deliver our customers safe and secure products.

Unauthorized access to technology products anywhere along the supply chain can pose a serious risk to you, your network, and your business.

Our **Value Chain Security Architecture** strives to embed sophisticated and pervasive security technologies and processes to detect potential compromises, validate platform integrity, and mitigate the risk of adversaries and bad actors from penetrating our supply chain at every stage of the product lifecycle.

Design → Plan → Source → Make → Quality → Deliver → Sustain → End of Life

However, once delivered to your door, there are steps you can and should take to prove the integrity of your Cisco products.

Where Integrity Verification Checklist occurs in the Cisco Value Chain Security lifecycle

Take a **zero trust** approach to your gear!

A zero-trust approach to security prompts you to question your assumptions of trust at every turn, continuously verifying trust before granting only the required access.

Follow our Product Integrity Checklist to protect yourself and your company against harmful products that may be counterfeit or tampered with by verifying the authenticity and integrity of any Cisco products and services you purchase.

1 Buy genuine Cisco products only through authorized sellers

Products sourced from outside Cisco authorized channels may pass through many hands before they reach you. They could contain components that have been tampered with, including the addition of illegal and malicious software.

Counterfeit or compromised Cisco products put you at risk

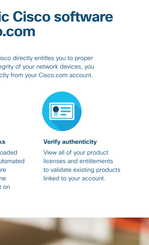
- Cisco cannot guarantee quality or performance.
- You may not have valid software licenses, warranty, and entitlements.
- They may cause serious damage to you, your network, and your business.

TIP Use our **partner locator** to find an authorized Cisco dealer near you.

2 Check the label on the box

Cisco's new **Identity Counterfeit Platform** includes a system of secure labels and label scanners designed to detect counterfeit products and thwart fake product sales.

Look at the **carton security label** and locate the Cisco hologram, usually found overlapping the edge of the carton's white label.



3 Verify the serial number of your new device to validate the authenticity

Complete a serial number health check to verify any new device that you are currently onboarding. If you haven't already, now's a good time to verify the serial numbers of your previously installed Cisco equipment.

4 Physically inspect cards and modules inside your device

Pop open your new Cisco device and look for the genuine Cisco security label on cards and modules.

PCBA security label
Holographic indicators and other security features are found on the printed circuit boards of most Cisco line cards and modules.

Module security label
Holographic security indicators are on most optical transceivers and highspeed cable assemblies.

TIP Visit **Cisco Brand Protection** to learn how to identify counterfeit or pirated products.

5 Verify software chain of custody

Cisco devices must be verified as running authentic and valid software in order to work properly and to ensure security integrity. The Cisco **Integrity Verification (IV) Application** verifies and continually monitors the integrity of any device that can be managed by Cisco DNA Center.

- ✔ Platform (SUDI and secure boot measurements)*
- ✔ Software
- ✔ Hardware
- ✔ Configuration

Cisco provides a Secure Hash Algorithm 512 bits (SHA512) checksum to validate downloaded Cisco images. This newer SHA512 hash value is generated on all software images, creating a unique output that is more secure than the MD5 algorithm.

Secure Unique Device Identity Check* For applicable products, an additional layer of verification may be available here

Check your software against known good values

1. The Cisco IV application compares collected image integrity data against Known Good Values (KGV) for Cisco software.
2. KGVs are available for **download** in standard JSON file format, signed by Cisco.
3. Always verify the signature of the KGV file before using it to assign integrity to your network elements.

TIP **Validate Boot Integrity**
Use the **Cisco Boot Integrity Validator**, a Python module that validates boot integrity visibility output generated by a Cisco IOS-XE device.

6 Download authentic Cisco software directly from Cisco.com

Buying Cisco products through Cisco-approved channels or Cisco directly entitles you to proper Cisco.com account credentials. To ensure the security and integrity of your network devices, you should download all Cisco product software and firmware directly from your Cisco.com account.

Secure access management
Cisco adheres to strict access management policies to ensure your identity before authorizing any software image downloads.

Built-in integrity checks
Software images downloaded from Cisco.com have automated integrity checks to ensure authenticity. Only genuine Cisco software will boot on Cisco platforms.

Verify authenticity
View all of your product licenses and entitlements to validate existing products linked to your account.

Trustworthy solutions are **everyone's responsibility**

In today's hyperconnected world, one organization's security could be everyone's security. It's no longer good enough to ensure safety. We must prove safety. All of us.

For inquiries about the integrity of your device, please contact brandprotection@cisco.com. To learn more about trustworthy solutions, visit the **Trust Center**.