

Cisco IR1000 Rugged Series Secure Routers

- Cisco Catalyst IR1001-G2 Rugged Secure Routers, on page 1
- Prerequisites, on page 2
- Limitations, on page 3

Cisco Catalyst IR1001-G2 Rugged Secure Routers

The Cisco Catalyst IR1001-G2 Rugged Secure Router is a compact, energy-efficient industrial router designed for rugged, modular, and flexible Cisco IIoT edge deployments.

The router is largely based on the Cisco Catalyst IR1101 Rugged Series Router but with a few additional enhancements and capabilities added to it.

Attention This Cisco Catalyst IR1001-G2 Rugged Secure Router guide includes applicable configuration content from the Cisco Catalyst IR1101 Rugged Series Routers guide for features supported on both platforms. It also documents IR1001-G2-specific features introduced in Cisco IOS XE Release 26.2.1.

Benefits of using Cisco Catalyst Rugged Secure IR1001-G2 Router

The Cisco Catalyst IR1001-G2 Rugged Secure Router help in providing:

- Energy efficiency: Operates at very low power, enabling deployment in power-limited environments.
- Flexibility: Software-configurable serial and digital I/O ports allow adaptation to industrial requirements.
- Reliability: Rugged industrial platform for critical infrastructure.
- It supports two 1G Ethernet ports which support Layer 2 and Layer 3 operation.

Table 1: Feature History Table

Feature name	Release information	Feature description

Feature name	Release information	Feature description
Cisco Catalyst IR1001-G2 Rugged Secure Router	Release 26.2.1	The Cisco Catalyst IR1001-G2 Rugged Secure Router is a compact, energy-efficient industrial router for rugged and modular IoT edge deployments. It provides two 1-Gigabit Ethernet ports with Layer 2 and Layer 3 operation, software-configurable serial and digital I/O capabilities, configurable power profiles, scheduled power management, and support for cellular connectivity.
P-5GS6-RC-GL PIM Support	Release 26.2.1	You can use the P-5GS6-RC-GL Pluggable Interface Module to add 5G Standalone Reduced Capability (RedCap) and 4G LTE connectivity to the IR1001-G2. The module supports primary or secondary WAN deployments and provides a migration path to 5G RedCap while retaining existing operational workflows and management interfaces. When 5G RedCap service is unavailable, the module can fall back to 4G LTE
ML-DSA signature for software image authenticity verification	Release 26.2.1	Cisco IOS XE software images and packages can include both RSA and Module-Lattice-Based Digital Signature Algorithm (ML-DSA-87) signatures. The router verifies the ML-DSA-87 signatures in supported image components to provide quantum-resistant software authenticity and integrity validation while retaining RSA signatures for transition and compatibility.

Prerequisites

Before proceeding with the Cisco Catalyst IR1001-G2 Rugged Secure Router configuration, you need to ensure that the router meets all required software prerequisites.

Cisco Catalyst IR1001-G2 Rugged Secure Router has these requirements.

- Basic requirements are:
  - to be connected to a stable power source of 12 to 24 VDC, 1A max.

  - to be able to access the router via the USB Type-C console port,
  - default is high power mode and it must be configured for one of the defined power management profiles as (Option 1: low power, Option 2: high power).

- Cisco Catalyst IR1001-G2 Rugged Secure Router aligns with the Unified Software and Licensing (UNX) Smart Licensing model. Ensure your device is registered with the appropriate Cisco Smart Licensing account to enable full feature sets.
- It supports booting from bootflash: (eMMC) and usb0: (USB flash drive).
- To access the USB contents use `dir usb0:` command.
- For VPN throughput you must consider software crypto performance for secure connectivity.
- If administrative access is lost, press and hold the recessed front-panel button for at least four seconds while powering on the device to reset the configuration.

Limitations

Cisco Catalyst IR1001-G2 Rugged Secure Router has these limitations:

- Crypto: No hardware-based crypto; as only software crypto (AES/SHA/RSA) is available, affecting VPN/IPsec throughput.
- Bootloader: Device does not support TFTP boot; only eMMC and USB boot are supported.
- Digital I/O: Only supports digital signals (0 or 1); there is no support for raw voltage or analog readings.
- TFTP boot: There is no support for TFTP boot.