Cisco Industrial IoT Portfolio

www.cisco.com/go/iiot

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

Contents

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

Bring Cisco scale and security foundation to Industrial IoT and AI initiatives

Stop worrying about challenges and start imagining possibilities with Cisco Industrial IoT

Deploying Industrial IoT at scale isn't easy. It requires configuring and managing countless assets and devices and dealing with complex operational and industry requirements. This increase in connected "things" can also create visibility gaps that increase security risks.

Industrial networks also serve as the critical foundation upon which Industrial AI thrives. High-bandwidth, low-latency, and secure networks, required to ensure the swift and reliable transfer of data generated by sensors, machines, and control systems, are crucial for AI algorithms to operate effectively.

Cisco provides the most secure and dependable Industrial IoT portfolio on the market

Cisco IIoT is an end-to-end Industrial IoT architecture that's built on our industry-leading network and security capabilities

Rock-solid infrastructure

Extend the Cisco network you know and trust to scale your Industrial IoT deployment using reliable infrastructure, automation, and familiar management tools

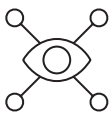
Unparalleled visibility and control

Protect your business with Cisco's industry-leading security and assurance portfolio which gives you complete visibility and control

Trusted expertise

Partner with a trusted leader who offers continuous innovation, market-leading products, an extensive developer program, and resources like deployment blueprints to make you successful

Industrial IoT enables transformative use cases



Remote monitoring

Asset tracking

Worker safety

Operational agility

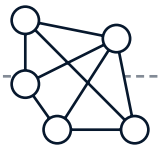
Industrial automation

Industrial AI

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

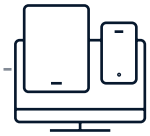
Cisco offers an unparalleled end-to-end Industrial IoT architecture

Interconnect assets, applications and data to uncover transformative business insights



Network connectivity

Extend the network you know and trust to operational environments



Device management

Manage industrial assets and devices at scale with automated solutions

Data control and exchange

Efficiently move the right data to the right place at the right time

Edge computing

Push data processes to the edge to enable fast decision-making in the field

Security

Protect your business from end to end with Cisco's industry-leading security portfolio

Our 67,000 customers are already seeing tremendous results

> "Within a month, we increased our manufacturing floor productivity by over 10 percent.
>
> – Yair Avigdor, COO, Lordan

> "Cyber Vision found more than 20 instances of malware in our substations and identified features and protocols that don't need to be active.
>
> – Emerson Cardoso, Chief Information Security Officer CPFL Energia

Visit http://www.cisco.com/go/iiot to learn more

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

Cisco Industry Validated Designs

We know our products have proven to be the industry's best "ingredients" for Industrial IoT networks. But we also know there can be complexity in designing, deploying, and managing those products into a "meal" – a complete solution to support all courses of a real-world use case.

That's why we have Cisco Validated Designs (CVDs). They are used to validate, architect, and configure next-generation technologies. Each is designed to help you accelerate digital transformation, innovate faster, and stay competitive.

Think of them as blueprints to your successful implementation. For every CVD, our engineers create detailed design and implementation guides that use Cisco and our partners' products to address critical business needs. We then engineer, test, and validate each design for our customers' industry-specific requirements, to guide their own deployments.

Next step

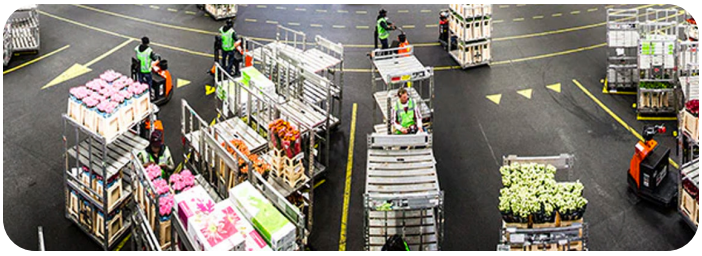
To see how Cisco Validated Designs can help you, visit http://www.cisco.com/go/iiotcvd.

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

Featured design guides

Rugged Enterprise Networking

Securely extend your IT network to rugged and outdoor spaces.



Manufacturing

Improve business operations by digitizing production environments.

Utilities and renewables

Modernize the power grid to improve reliability, security, and distributed renewable resources.

Roadways and intersections

Improve public safety, operational efficiency, and traffic management.

Cisco Industrial IoT solutions

Connected Factory

Factory Wireless

Roadways and Intersections

Substation Automation

Utility WAN

Field Area Network (AMI)

Connected Renewables

Industrial Security

Smart Cities

Site Asset Management

Connected Rail

Distribution Automation

Industrial Automation

Connected Pipeline

Connected Refinery

Cisco IoT accelerates digital transformation, delivering insight and action from your data.
www.cisco.com/go/iiot

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

Cisco Industrial Ethernet (IE) switching portfolio

The Cisco® Industrial Ethernet (IE) switching portfolio offers ruggedized, secure, easy-to-use switches that bring proven IT proficiencies to harsh industrial environments. They provide secure connectivity across challenging operating conditions and industries such as manufacturing, utilities, transportation, oil and gas, mining, roadways, and smart cities. These Cisco switches offer best-in-class Cisco IOS® XE Software with advanced Layer 2 and Layer 3 features, along with industrial protocol support, such as PROFINET and EtherNet/IP to accelerate industries' digital transformation and modernization.

With robust, reliable, secure networking and low-latency high-bandwidth communications, Cisco industrial switches help build the infrastructure necessary to support AI applications and accelerate innovation in demanding environments.

Benefits

- **Enable Industrial AI** by building low-jitter high-bandwidth networks to transport large amounts of real-time data from sensors, machines, and control systems, which is essential for AI algorithms to learn and make informed decisions.
- **Secure operations at scale** by embedding advanced cybersecurity features such as OT visibility, vulnerability assessment, threat detection, zone segmentation, and zero trust remote access, eliminating the need for deploying dedicated security appliances.
- **Boost partnership between IT and OT** with a unified framework for network design and operations, extending IT cybersecurity practices and capabilities to OT environments, and combining monitoring, remote access and automation with unified network management systems.
- **Reduce downtime** with managed Ethernet switches that are more reliable and include high-availability technology to ensure resilient networks, even in extreme industrial environments.
- **Lower operational costs** with zero-touch provisioning that automates connecting thousands of new endpoints as part of Industrial Internet of Things (IIoT) deployments.
- **Assure network performance** in both owned and unowned networks that may exist between industrial sensors and applications in the cloud, enabling organizations to proactively monitor, manage, optimize, and troubleshoot the network to maximize productivity.
- **Protect investments** with modular switches that minimize the need for costly complete replacements and extend the lifespan of your network infrastructure.

Secure by design

Cisco IE switches are developed according to the Cisco Secure Development Lifecycle (SDL), which enforces a secure-by-design philosophy from product planning through end of life and conforms to the requirements of ISA/IEC 62443-4-1 as well as ISA/IEC 62443-4-2. The SDL provides assurance that the switches are themselves protected against cyberthreats and contribute to the overall security and resilience of industrial operations. Cisco IE switches also contain several embedded security features that provide additional layers of protection.

Ready for Industrial AI

Cisco IE switches play a pivotal role in enabling Industrial AI by facilitating high-speed, reliable transfer of real-time data from diverse industrial devices to AI applications in datacenters and cloud. They help build a secure, resilient, and scalable fabric that ensures consistent and deterministic data flows crucial for AI algorithms to perform real-time analysis and control.

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

Select switches offer edge-compute capabilities for local data processing, enabling operations teams to make informed data-driven decisions, right at the source.

Advanced network security

Select models of the Cisco IE switch portfolio with the open Cisco IOx based edge-compute capabilities run a number of essential security functions. This differentiating feature of the switches eliminates the need for deploying dedicated security appliances and avoids security gaps by enabling the switches to protect connected assets. This results in a network architecture that sees more, protects more, and is simpler to deploy at scale.

The built-in advanced security functions include:

- **OT visibility:** The built in Cyber Vision sensor provides comprehensive visibility into Industrial Control Systems (ICS) and OT assets, their vulnerabilities and their communication activities, so you have the insights to reduce your attack surface. It profiles all connected devices to help you build segmentation policies. It detects malicious traffic and abnormal behaviors, so you can defend operations.
- **Microsegmentation:** The Cisco TrustSec® technology, combined with Cyber Vision and/or Cisco Identity Services Engine (ISE) provides identity-based network access control, segmenting networks and enforcing security policies based on user and device roles, enhancing security by limiting lateral movement of threats, and simplifying network management through centralized policy enforcement.
- **Zero trust remote access:** The built in Secure Equipment Access gateway enables Zero-Trust Network Access (ZTNA) capabilities purpose-built for OT workflows. It empowers operations teams with self-service remote access and lets you easily enforce least-privilege access policies so you can control risks from remote users accessing OT assets for remote configuration, monitoring, or troubleshooting.

Centralized network management

Scaling your industrial network and making it more flexible to adapt quickly to changing requirements is easy with intelligent management. You can easily manage your Industrial IoT network with the same tools that manage your IT network, such as Cisco Catalyst™ Center, which allows zero-touch deployments, automates configuration changes, monitors performance, and identifies and helps correct faults, reducing time and cost of deployment. You may also use other management options such as the included web management tool.

Select Cisco IE switches can also be managed by the Meraki dashboard, providing a centralized cloud-based alternative to manage large but highly distributed deployments.

In addition to the management dashboards, Cisco offers a troubleshooting agent for industrial networks, an agentic AI system specifically designed to prevent networking issues from impacting operations in industrial environments, particularly in manufacturing. It acts as a networking expert, gathering data, identifying problems, troubleshooting, and recommending fixes through a conversational interface.

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

Cisco ThousandEyes Assurance

Select Cisco Industrial Ethernet switches can run the embedded ThousandEyes Enterprise Agent that offers a powerful solution for industrial organizations seeking to improve the reliability, security, and performance of both their owned and unowned networks. By providing comprehensive visibility and insights into complex network environments, ThousandEyes Assurance enables proactive problem detection, faster troubleshooting, and enhanced operational continuity, ultimately supporting digital transformation and innovation in industrial sectors.

Comprehensive form factors

Cisco offers its IE switch portfolio in different form factors to suit a range of industries and use cases.

- **DIN rail switches:** These switches can be mounted on standard DIN rails, which are commonly used in industrial control panels. The switches are compact and take up less space in these panels, which is useful in tight spaces where there is limited room for equipment. Cisco IE DIN rail switches are available in both fixed and modular forms that can be expanded with additional ports to keep up with demand. They also offer a choice of power supplies, allowing you to match the right power capacity for your Power over Ethernet (PoE) needs. Select models feature conformal coating for additional resistance against corrosion.
- **Rack-mount switches:** These switches are designed to be mounted in a standard 19-inch equipment rack, which allows for flexibility in deployment – in industrial settings, server rooms, or even in data centers. Some of the Cisco rack-mount industrial switches are conformally coated for additional resistance against corrosion.
- **IP67-rated switches:** These switches are wall mounted and can withstand the harshest conditions, including dust, water, and extreme temperatures, as well as severe shocks and vibrations. Because they are designed to withstand harsh conditions, IP67-rated industrial switches are more reliable and less likely to fail and cause downtime. The switches are equipped with M12 connectors rather than standard RJ-45 connectors. Some Cisco IP67- rated switch models also provide PoE, both fiber and copper ports, and 10GE uplink ports.
- **Embedded switches:** These switches are built for secure, high-bandwidth, mission-critical mobile networks. They enable integrators to build custom solutions for specialized use cases.

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

Modular DIN rail switches

Select models of the Cisco IE switch portfolio are available in a modular form factor. These switches include the base system to which expansion modules may be attached as required. This modularity gives you the freedom to add, remove, or change copper or fiber ports in the future in sync with your evolving needs without having to replace the entire switch.

Cisco IE3500 Rugged Series (New)

- Advanced modular DIN rail switches expandable up to 27 ports
- All Gigabit Ethernet platform, Layer 2 or Layer 3
- Up to 24 ports of PoE/PoE+/4PPoE (power budget up to 480W), and 3 10GE uplinks
- Copper, fiber, and PoE/PoE+/4PPoE expansion modules
- IOS XE operating software
- Microsegmentation based on Cisco TrustSec technology
- Low-jitter switching for time-sensitive critical data
- Choice of management by Catalyst Center or Meraki Dashboard*
- Cisco SD-Access Fabric Edge node
- Cisco IOx application hosting environment
- Cisco Cyber Vision included at no extra cost for visibility of OT assets, activities, and security posture
- Cisco Secure Equipment Access included at no extra cost for zero trust remote access to industrial assets
- ThousandEyes agent for visibility over owned and unowned networks

*** Management by Meraki dashboard available in CY2026**

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

Expansion modules add versatility and flexibility to your industrial network by providing additional ports, functionalities, and features that the base switch units might not have. These modules let you customize the switch to your specific needs, allow you to accommodate future additions and changes, provide built-in scalability, and promote long-term viability and sustainability.

Expansion modules for the Cisco IE3500 Rugged Series allow you to add fiber, copper, or PoE ports. Any expansion module can be attached to any of the base switch models.

The following expansion modules are available for the Cisco IE3500.

6 GE copper and 2 GE fiber ports

8 GE copper ports

8 PoE/PoE+ GE ports

8 GE fiber ports

14 GE copper and 2 GE fiber ports

16 GE copper ports

16 PoE/PoE+ GE ports

4 PoE/PoE+ /4PPoE 2.5GE ports

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

Cisco Catalyst IE3400 Rugged Series

- Advanced modular DIN rail switch expandable up to 26 ports
- All Gigabit Ethernet platform, Layer 2 or Layer 3
- Up to 24 ports of PoE/PoE+ (power budget up to 480W)
- Copper, fiber, and PoE+ expansion modules
- Cisco IOS XE operating software
- Cisco Catalyst Center for management
- SD-Access policy extended node
- Microsegmentation based on Cisco TrustSec technology
- Advanced industrial protocols and additional resiliency and security features
- Cisco IOx application hosting environment
- Optional Cisco Cyber Vision for visibility of OT assets, activities, and security posture
- Optional Cisco Secure Equipment Access for zero-trust remote access to industrial assets

Expansion modules for the Catalyst® IE3400 allow you to add fiber, copper, or PoE ports and include the following. In addition to these, the Catalyst IE3400 can utilize expansion modules for the Catalyst IE3300 with some limitations.

8 fiber ports

8 copper ports

8 PoE+ ports

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

Cisco Catalyst IE3300 Rugged Series

- Modular DIN rail switch expandable up to 26 ports
- All Gigabit Ethernet platform with available 10G uplink option, Layer 2 or Layer 3
- Up to 24 ports of PoE/PoE+ (power budget up to 480W with expansion modules)
- Copper, fiber, and PoE+ expansion modules
- Cisco IOS XE operating software
- Cisco Catalyst Center for management
- SD-Access extended node
- Cisco IOx application hosting environment
- Optional Cisco Cyber Vision for visibility of OT assets, activities, and security posture
- Optional Cisco Secure Equipment Access for zero-trust remote access to industrial assets

Expansion modules for the Catalyst IE3300 allow you to add fiber, copper, or PoE ports to the base system and include the following.

8 copper ports

16 copper ports

8 fiber ports

6 copper, 2 fiber ports

14 copper, 2 fiber ports

8 PoE+ ports*

16 PoE+ ports*

4 1G/2.5G Hi-PoE ports*

* Compatible with select models of the Catalyst IE3300 and IE3400 Rugged Series. Please consult the respective datasheets.

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

Fixed DIN rail switches

Cisco Catalyst IE3200 Rugged Series

- Fixed DIN rail switch, 10 ports
- All Gigabit Ethernet platform, Layer 2
- 8 ports of PoE/PoE+ (power budget up to 240W)
- Cisco IOS XE operating software
- Cisco Catalyst Center for management
- SD-Access extended node

Cisco Catalyst IE3100 Rugged Series

- Compact form-factor fixed DIN rail switch with 6, 10, 12, or 20 ports
- 2 or 4 dual-media or fiber uplink ports
- All Gigabit Ethernet platform, Layer 2
- Up to 8 ports of PoE/PoE+/4PPoE with up to 90W per port
- Total PoE power budget up to 240W
- Conformal coating for added environmental protection (on select model)
- Cisco IOS XE operating software
- Cisco Catalyst Center for management
- SD-Access extended node
- Optional Cisco Secure Equipment Access for zero-trust remote access to industrial assets

Cisco IE1000 Series Switches

- Fixed DIN rail switch, up to 10 ports
- Up to 8 Fast Ethernet (FE) ports, 2x 1G combo uplinks (on select models)
- Lightly managed Layer 2
- Up to 8 ports of PoE/PoE+ (power budget up to 180W)
- Security: Port security, TACACS, 802.1X
- Plug and Play (PnP) for easy deployment

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

Rack-mount switches

Designed to fit into a standard 19-inch rack, Cisco rack-mount switches offer several models with options for 1 Gigabit Ethernet, Multigigabit, and 10 Gigabit Ethernet ports, supporting up to 28 ports for versatile connectivity, up to 90W of PoE per port, and up to 720W per switch. A new model features both 1GE fiber and copper PoE/PoE+ ports.

Cisco Catalyst IE9300 Rugged Series Switches

- 19-inch rack-mount switch
- Based on the Unified Access Data Plane (UADP) Application-Specific Integrated Circuit (ASIC)
- All Gigabit Ethernet platform, Layer 2 or Layer 3
- All-fiber, all-copper, or mixed-media ports with speeds of 1GE, 2.5GE, or 10GE
- PoE/PoE+/4PPoE ports with up to 90W/port
- Up to 720W PoE power budget per switch
- GNSS/GPS antenna interface and conformal coating (on select model)
- Cisco IOS XE operating software
- Vertical stacking up to four members (on select models)
- Advanced industrial and redundancy protocols
- Cisco Catalyst Center for management
- SD-Access fabric edge node
- Cisco IOx application hosting environment
- Cisco Cyber Vision included at no extra cost for visibility of OT assets, activities, and security posture
- Cisco Secure Equipment Access included at no extra cost for zero-trust remote access to industrial assets

Cisco IE4010 Series Switches

- 19-inch rack-mount switch, 28 ports
- All Gigabit Ethernet platform, Layer 2 or Layer 3
- Up to 24 ports of PoE/PoE+ (power budget up to 385W)
- Both copper and fiber ports on a single chassis
- Advanced industrial protocols and additional security features
- Cisco Catalyst Center for management
- SD-Access extended node

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

Heavy-duty IP67 switches

Cisco IP67-rated industrial switches are designed to withstand extreme environments. These switches are certified to protect against dust and water submersion, meeting rigorous standards for temperature, vibration, humidity, and electromagnetic emissions

Cisco Catalyst IE3500 Heavy Duty Series (New)

- Wall-mount IP66/IP67-rated switch with M12 interfaces
- Fast and Gigabit Ethernet platform, Layer 2 or Layer 3
- 8, 16, or 24 copper or fiber ports with speeds of 1GE, 2.5GE or 10GE
- Up to 14 ports of PoE/PoE+/4PPoE up to 60W per port and PoE power budget up to 240W per switch
- IOS XE operating software
- Microsegmentation based on Cisco TrustSec technology
- Low-jitter switching for time-sensitive critical data
- Catalyst Center for management
- Cisco SD-Access Fabric Edge node
- Cisco IOx application hosting environment
- Cisco Cyber Vision included at no extra cost for visibility of OT assets, activities, and security posture
- Cisco Secure Equipment Access included at no extra cost for zero-trust remote access to industrial assets
- ThousandEyes agent for visibility over owned and unowned networks

Cisco Catalyst IE3400 Heavy Duty Series

- Wall-mount IP66/IP67 switch with M12 interfaces
- Up to 24 all Gigabit Ethernet or all Fast Ethernet ports, Layer 2 or Layer 3
- Cisco Catalyst Center for management
- SD-Access policy extended node
- Microsegmentation based on Cisco TrustSec technology
- Advanced industrial protocols and additional security features
- Cisco IOx application hosting environment
- Optional Cisco Cyber Vision for visibility of OT assets, activities, and security posture
- Optional Cisco Secure Equipment Access for zero-trust remote access to industrial assets

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

Cisco Catalyst IE3100 Heavy Duty Series (New)

- Wall-mount IP66/IP67-rated switch with M12 interfaces
- Compact form-factor with 6 FE+2 GE or 8x 1GE ports, Layer 2
- Cisco IOS XE operating software
- Cisco Catalyst Center for management
- SD-Access extended node
- Optional Cisco Secure Equipment Access for zero-trust remote access to industrial assets

Next steps

To learn more about the Cisco Catalyst Industrial Ethernet switching portfolio, visit **www.cisco.com/go/ie** and use the **Cisco Switch Selector** to find the best switch for your particular use case.

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

Cisco Industrial Router (IR) portfolio

Cisco Catalyst industrial routers are a range of ruggedized modular platforms on which you can build a highly secure, reliable and scalable communications infrastructure. They support ThousandEyes Assurance, allowing you to proactively monitor your network with end-to-end visibility all the way to the industrial edge. In addition, they offer built-in advanced OT and IT security capabilities, including Cyber Vision, Secure Equipment Access, and Next-Generation Firewall (NGFW).

All Cisco industrial routers share a core set of common characteristics. They are certified to meet harsh environmental standards – and have modular designs that can help extend product life and lower costs. This flexible design enables WAN redundancy and is ready to handle public and private 4G or 5G – including FirstNet private LTE, and Citizens Broadband Radio Service (CBRS), as well as enhanced data throughputs and differentiated services. They are powered by Cisco IOS XE, and offer a choice of management options, allowing you to extend your network from the enterprise to the industrial edge using common security policies, tools, and management policies.

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

Modular design
Enjoy many pluggable module options, such as public or private 4G and 5G, Wi-Fi 6, and additional storage. The platform can adapt as your connectivity needs grow or technology evolves.

Ruggedized
Designed for industrial deployments, including harsh environments with extreme temperatures.

Scale with choice of management
Scale and simplify operations. Equip IT and operations teams with powerful management tools such as Field Network Director, Cisco Catalyst Center, and Cisco Catalyst SD-WAN Manager.

Enjoy routing and full-stack multilayer security, all in one
There's no need for separate hardware to protect remote operations. Comprehensive enterprise-grade security features and OT threat intelligence are built-in, including next generation firewall capabilities, such as advanced firewalling, URL filtering, intrusion prevention, malware protection, and DNS security.

ThousandEyes Assurance
Proactively monitor OT asset network connectivity health and improve operational resilience with end-to-end network visibility using ThousandEyes Assurance.

Visibility into connected assets
Assess your OT security posture and shrink your attack surface. Cisco Cyber Vision is built in to provide detailed visibility into connected assets, their vulnerabilities, and activities.

Secure access to remote assets
Take control over remote access to OT assets. Cisco Cyber Vision's Secure Equipment Access turns your Cisco industrial routers into Zero-Trust Network Access (ZTNA) gateways to simplify and secure remote access at scale.

Take action right at the edge
Use the platform's built-in edge compute application hosting capabilities, which support building and running your own applications at the edge.

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

Cisco Catalyst IR1100 Rugged Series Routers - FirstNet Capable

- Modular and expandable hardware design to extend product life
- Advanced security capabilities
- Choice of WAN interfaces like Ethernet, dual LTE/5G/ cellular for WAN redundancy
- FirstNet Capable
- Ruggedized and compact with low power consumption
- SD-WAN with enterprise-grade security
- Cisco IOS XE operating software
- Edge compute with application hosting
- ThousandEyes Assurance for proactive monitoring at the industrial edge
- Optional Cisco Cyber Vision for visibility of OT assets, activities, and security posture
- Optional Cisco Secure Equipment Access for zero-trust remote access to industrial assets
- Optional Cisco Edge Intelligence for getting Industrial IoT data to the right applications at the right time
- IEC 61850-3 and IEEE 1613 certified for deployment in utility substations
- 100 GB of additional storage for edge applications

Expansion modules for the Catalyst IR1101

Enjoy thesmall form factor of the Catalyst IR1101, or expand with one or two modules to add more connectivity options. Connect two of any of the four options listed below to each IR1101.

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

IRM-1100-SPMI

Dual active WAN and storage options for flexibility

- 1 x GE fiber port (L2/L3)
- Slot for second PIM
- 4 x digital I/Os for dry/wet contacts
- mSATA slot for additional storage

IRM-1100-SP

Dual active WAN

- 1 x GE fiber port (L2/L3)
- Slot for second PIM

IRM-1100-4A2T

Connectivity to legacy devices on serial ports

- 1 x GE fiber port (L2/L3)
- 4 x asynchronous serial ports

IRM-1100-4S8I (new)

Additional SFP ports for long-distance communications and strong protection against Electromagnetic Interference (EMI)

- 4 x GE SFP ports (L2/L3)
- 8 x digital I/Os for dry/wet contacts

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

Cisco Catalyst IR1800 Rugged Series Routers – FirstNet Capable

- Highly secure, high-performance, modular routers with 5G and Wi-Fi 6
- Next-Generation Firewall capabilities built-in
- Rolling stock EN50155 certified
- SD-WAN with comprehensive threat protection and security features
- Cisco IOS XE operating software
- Edge compute supporting Cisco Edge Application Hosting
- ThousandEyes Assurance for proactive monitoring at the industrial edge
- Optional Cisco Cyber Vision for visibility of OT assets, activities, and security posture
- Optional Cisco Secure Equipment Access for zero-trust remote access to industrial assets
- Optional Cisco Edge Intelligence
- for getting Industrial IoT data to the right applications at the right time
- FirstNet Capable
- 2 cellular slots, 1 Wi-Fi slot
- 8 GB memory
- CAN bus, PoE/PoE+, ADR GNSS slot, SSD slot
- 4 digital I/O ports, advanced security features, 1 RS-232/485 combo port

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

Cisco Catalyst IR8100 Heavy Duty Series Routers – FirstNet Capable

- Heavy duty, IP67-certified, fully modular industrial router designed for harsh outdoor environments
- Wi-SUN Field Area Network 1.1 certified (coming soon)
- 5G, public and private LTE, and more
- Advanced cybersecurity and hardware security
- Built-in edge compute and SD-WAN-enabled
- ThousandEyes Assurance for proactive monitoring at the industrial edge
- 1 Gigabit copper with PoE output
- 1 Gigabit fiber/SFP
- 3 additional I/O slots
- AC powered with built-in battery backup
- 12V DC for external devices

Cisco Catalyst IR8300 Rugged Series Router – FirstNet Capable

- Rugged, 5G, integrated routing and switching platform for many industries and use cases
- Next-Generation Firewall capabilities built-in
- IEC-61850-3 and IEEE 1613 certified for deployment in utility substations
- Hot-swappable, fully redundant power supplies and high-availability design for maximum network uptime and redundancy
- Multiple interface options, including Ethernet switch, T1/E1, and serial (RS-232)
- Enhanced security and advanced QoS for compliance with critical infrastructure protection mandates
- SD-WAN with comprehensive threat protection and security features
- Cisco IOS XE operating software
- Edge compute supporting Cisco Edge Application Hosting
- ThousandEyes Assurance for proactive monitoring at the industrial edge
- Optional Cisco Cyber Vision with Snort IDS for visibility of OT assets, activities, and security posture
- Precision timing source

Pluggable network modules for Catalyst industrial routers

Cisco Catalyst industrial routers provide flexible networking options to meet your constraints and use case requirements. Use the pluggable module that supports the technology you need and replace to adapt to technology changes or as your needs evolve.

- 4G LTE and P-LTE pluggable module, FirstNet Capable
- 4G LTE 450-MHz pluggable module*
- 5G Standalone (SA) and Non-Standalone (NSA) sub-6-GHz cellular pluggable module with P-LTE, FirstNet Capable
- Wi-Fi 6 pluggable module†
- 2-port T1/E1 pluggable module‡
- 8-port RS232 serial pluggable module‡

* Catalyst IR1101 only
† Catalyst IR1800 only
‡ Catalyst IR8300 only

Next steps

To learn more about Cisco Catalyst industrial routers, visit www.cisco.com/go/iot-routers.

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

Cisco Industrial WPAN Routers

Not available for Europe

IR510

IR530

Cisco IR510 WPAN Industrial Router

- High-performance Wi-SUN compliant ruggedized router with 1.2 Mbps data rate
- Provides unlicensed 915 MHz, ISM-band Wireless Personal Area Network (WPAN) communications that enable Industrial IoT applications
- Open RF mesh solution based on the following standards: IEEE 802.15.4 g/e/v, IETF 6LoWPAN, IETF Routing Protocol for Low Power and Lossy Networks (RPL), IETF Mapping of Address and Port – Translation (MAP-T, and IETF Constrained Application Protocol (CoAP)
- Cisco Edge Application Hosting ready

Cisco IR530 Series Resilient Mesh Range Extenders

- Extend the range of the RF wireless mesh network, providing longer reach between WPAN endpoints and other WPAN networks
- Deliver unlicensed 902 to 928 MHz, ISM-band IEEE 802.15.4g/e/v WPAN communications to diverse Industrial IoT applications
- Increases communications network uptime and grid availability, helps ensure message delivery through a rugged industrial hardware design and highly resilient solution architecture
- Lower total cost of ownership by consolidating disparate communications networks used for AMI and distribution automation applications

Next steps

To learn more about
Cisco industrial routers, visit: **cisco.com/go/iot-routers**.

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

Industrial Wireless (IW) access points and clients

Workers, assets, and resources are becoming increasingly connected in manufacturing, transportation, smart cities, oil and gas, mining and beyond. This expansion of Industrial IoT networking and equipment interconnectivity enables new use cases and opportunities, but it also places new demands on your infrastructure. Cisco responds to these demands with range of access point specifically designed for offering extended, high-performance wireless connectivity in these outdoor and harsh industrial environments.

Our access points and clients are all built on the 802.11ax standard. They support Wi-Fi 6/6E and most support Cisco Ultra-Reliable Wireless Backhaul (URWB) enabling you to connect mission-critical applications requiring greater reliability than Wi-Fi alone can provide.

Ultra-Reliable Wireless Backhaul (URWB)

URWB delivers reliable wireless connectivity for moving assets or to extend your network where running fiber isn't feasible or is too costly. It provides high-bandwidth, high-availability, ultra-low-latency, seamless handoffs with zero packet loss, making it ideal for connecting the most demanding applications that need uninterrupted wireless connectivity.

URWB has been successfully deployed in rail, mining, smart cities, container terminals, entertainment, factories, and other industries.

High bandwidth

A multigigabit data rate makes it the ideal choice for demanding applications such as real-time video surveillance, onboard Wi-Fi for edge devices, depot telemetry download, and much more.

Seamless handoff

Handoff is one of the primary challenges in vehicle-to-wayside communications. Unlike other technologies, URWB offers seamless roaming from one base station to the next, helping ensure strong radio signals or no packet loss so moving vehicles are always connected to the application.

Ultra-low latency

When real-time interaction is required, latency must be negligible compared to the reaction time. Thanks to their wireless-aware switching protocol, these radio platforms have incredibly low latency, making them the ideal choice for remote control, machine-level protocols, VoIP, and autonomous and semi-autonomous applications.

Stability and reliability

Mission-critical OT networks cannot allow downtime. Losing connection in OT means stopping machines and processes, often resulting in a huge loss of money.

Thanks to the latest technologies and dedicated network design and deployment, Cisco will help make your wireless data network smooth and seamless.

[1] Wi-Fi 6E availability based on local regulations

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

Fast failover

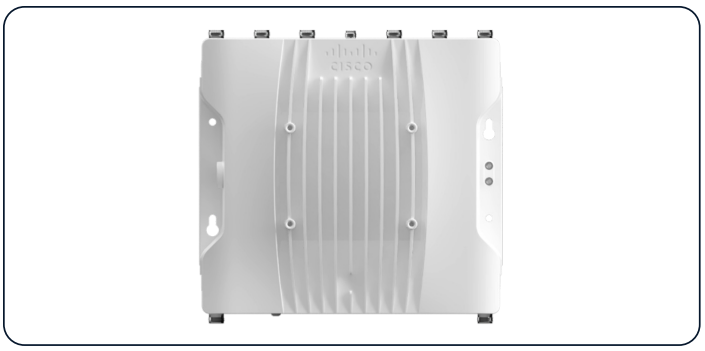
Sometimes stability is not enough. Applications such as Communications-Based Train Control (CBTC) require a failover system in case of communication or hardware default. To accomplish this, Cisco introduced a special algorithm that can reconfigure the network on redundant hardware in less than 500 ms.

High availability

Cisco URWB's innovative technology, Multipath Operations (MPO), provides uninterrupted wireless connectivity by sending high-priority packets via redundant paths. on uncorrelated frequencies at the same time to multiple access points. It lowers the effects of interference and hardware failures, preventing packet loss, lowering latency, and increasing availability.

For more information on URWB, please visit: cisco.com/go/urwb.

Customers can now activate and set up URWB capabilities on their Cisco Wi-Fi access points via the Wireless LAN Controller (WLC), allowing them to manage ultra-reliable networks using Catalyst Center (CC). If needed, URWB can also operate in a dedicated standalone mode on IW Wi-Fi 6E access points. This mode can be configured through IW Service and monitored using IW Monitor.



Cisco Catalyst IW9167E Heavy Duty Access Point

- Supports Wi-Fi 6/6E, URWB and WGB
- Tri 802.11ax radio (2.4 GHz, 5 GHz, 5/6 GHz)
- Suitable for pole installation on wayside/trackside
- 4x4 MIMO, 4 spatial streams, with a wide choice of antennas to better suit each use case
- 8 N-type antenna connectors
- 2 Multigigabit RJ-45, SFP+, optional M12 adapters
- Heavy-duty, IP67 certified enclosure to operate under extreme water, dust, and temperature conditions (-50° to +75°C; -58° to 167°F)
- EN50155 certified for rolling stocks
- Supports GNSS, BLE, and scanning radio for spectrum management, minimizing interference
- Can be powered by PoE or DC

Cisco Catalyst IW9167E Heavy Duty Access Point for hazardous locations

- Supports Wi-Fi 6/6E, URWB and WGB
- Tri 802.11ax radio (2.4 GHz, 5 GHz, 5/6 GHz)
- Suitable for pole installation on wayside/trackside
- 4x4 MIMO, 4 spatial streams, with a wide choice of antennas to better suit each use case
- 8 N-type antenna connectors
- 2 Multigigabit RJ-45, SFP+, HazLoc certified M25 ports
- Heavy-duty, IP67 certified enclosure to operate under extreme water, dust, and temperature conditions (-50°C to +75°C; -58° to 167°F)
- EN50155 certified for rolling stocks
- Class I Division 2, Zone 2/22, ATEX, and IECEx certifications for hazardous locations
- Supports GNSS, BLE, and scanning radio for spectrum management, minimizing interference
- Can be powered by PoE or DC

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

Cisco Catalyst IW9167I Heavy Duty Access Point

- Supports Wi-Fi 6/6E and URWB
- Tri 802.11ax Wi-Fi 6/6E radio (2.4 GHz, 5 GHz, 6 GHz), bringing all the benefits of Wi-Fi 6/6E to the harshest environments: more spectrum, more channels, higher throughput, and improved security
- 4x4 MIMO, 4 spatial streams, with internal omnidirectional antenna 5-6 dBi
- IP67 certified, withstands dust, water and extreme temperature ranges of -50° to +65°C (-58° to 167°F)
- Optional M12 I/O connectors
- Supports GNSS, BLE
- Can be powered by PoE or DC

Cisco Catalyst IW9165E Rugged Access Point and Wireless Client

- Supports Wi-Fi 6/6E, URWB and WGB
- Dual 802.11ax radio (5 GHz, 5/6 GHz)
- DIN rail compact form factor to enable integration in industrial vehicles, robots, cranes, trains, and more
- Wide choice of antennas to better suit each use case (4 RP-SMA)
- 2 Multigigabit RJ-45, optional M12 adapter
- Ruggedized hardware supporting high temperature ranges (-40° to +70°C; -40° to 158°F)
- EN50155 certified for rolling stocks
- Supports GNSS, BLE
- Can be powered by PoE or DC

Cisco Catalyst IW9165D Heavy Duty Access Point

- Supports Wi-Fi 6/6E and URWB
- Dual 802.11ax radio (5 GHz, 5/6 GHz)
- Built-in directional antenna for easy deployments
- Choice of external antennas to quickly extend network to new places when needed (2 N-type)
- 2 Multigigabit RJ-45, optional M12 adapters
- Heavy-duty, IP67-certified enclosure to operate under extreme water, dust, and temperature conditions (-50° to +75°C; 58° to 167°F)
- Supports GNSS, BLE
- Can be powered by PoE or DC

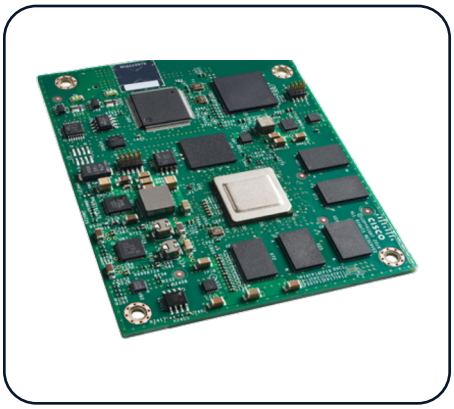
Next steps

To learn more about
Cisco Industrial Wireless access points and clients, visit **cisco.com/go/iw**.

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

Cisco Industrial IoT embedded networks portfolio

The Cisco industrial IoT embedded networks portfolio includes access points, routers, and switches that use Cisco's networking technology packaged into highly ruggedized, low size, weight, and power networking components. Their small form factor coupled with mobile and edge-specific features make these products ideal for applications across industries such as mining, oil and gas, transportation, shipping, and defense, where highly secure, reliable performance is required during extreme conditions.



Cisco ESR6300 Embedded Services Router

Exponentially faster
The ESR6300 offers significantly faster secure throughput than the previous generation of ESRs, to meet increased bandwidth needs arising from the rapid growth of sensor data and video streams.

Cisco trustworthy systems
The onboard Cisco Trust Anchor Module (TAM) plus image signing, secure boot, and runtime defenses help ensure that the code running on the Cisco ESR6300 is authentic, unmodified, and operating as intended.

Simplified integration
At 3 inches by 3.75 inches, the ESR6300 is smaller than its predecessors, making it easier to integrate into compact solutions. It is hardened for extreme temperatures, shock, and vibration to achieve the highest standard of reliability.

Modularity options
The ESR6300 provides two WAN ports of Gigabit Ethernet that give you a choice of media type and four LAN ports of Gigabit Ethernet with PoE/PoE+ ready options. As your needs evolve, add mSATA storage for Cisco Edge Application Hosting.

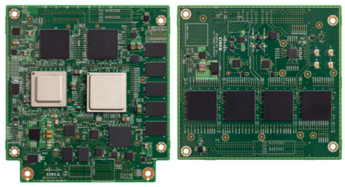
Streamlined management with Cisco IOS XE
Cisco IOS XE is highly programmable, with open and standards-based APIs and next-generation, multilayer security built in. This unified software stack is ideal for process and workflow automation, so you can qualify and deploy new services faster.

Software-defined WAN on the ESR6300
The ESR6300 is hardware ready to support SD-WAN so you can leverage IT expertise to a distributed network, operate at scale, and lower TCO. Cisco SD-WAN architecture delivers scale, simplicity, and unified management for extending the enterprise network to a distributed Industrial IoT deployment.

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

Cisco Catalyst ESS9300 Embedded Series Switch

- High-bandwidth with 10 ports of 10GE Small-Form-Factor Pluggable Plus (SFP+)
- Ruggedized for the harshest conditions, including extreme temperatures (-40° to +85°C), shock, and vibration
- Select model available as a mezzanine card conformant to OpenVPX standards
- FIPS-140 and MIL-STD-810H certifications
- Low power consumption: 35W
- RJ-45 Ethernet management port (optional)
- RJ-45 or USB micro-B console port
- Common +3.3V and 5V power inputs
- Crucial security features including secure boot and zeroization
- Advanced Cisco IOS XE operating system and WEBUI management



Cisco Embedded Service 3300 Series Switches

- High-speed PC 104 compact form-factor switch
- Ruggedized to operate in harsh environments (-40° to +85°C)
- Low power consumption (mainboard 16W, expansion 8W)
- 2x 10G uplink ports, 8x 1G downlink ports on mainboard
- 16x 1G downlink ports on expansion board for high port density
- Modern Cisco IOS XE operating system and WEBUI management
- PoE-ready architecture and software
- Layer 2 Network Essentials feature set

Next steps

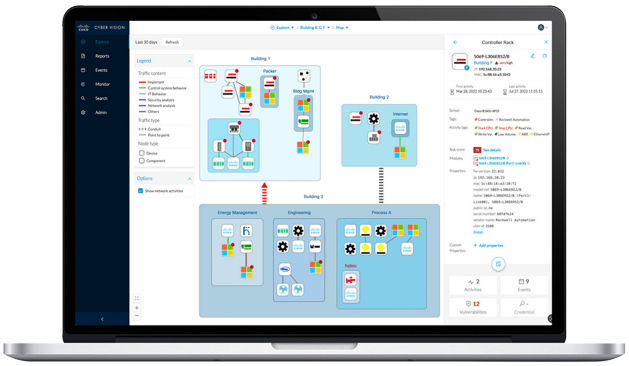
Find out more about Cisco's IoT embedded networks.

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

Cisco Industrial cybersecurity

Cisco Cyber Vision

Visibility, security, and zero-trust remote access for industrial operations.



Cisco Cyber Vision provides continuous visibility into your Industrial Control System (ICS) and your OT security posture so you have the insights to reduce the OT attack surface. Its deep integration with Cisco's leading security portfolio helps protect operations with network segmentation that can be implemented in weeks, not years. Its Zero Trust Network Access (ZTNA) capabilities empower operations teams with self-service remote access to OT assets and let you enforce least privilege policies.

Cyber Vision uses a unique edge architecture that embeds OT security features into your industrial network. The network that connects your assets profiles everything, detects malicious traffic and abnormal activities, enforces IEC 62443 zones and conduits, and controls who can remotely access your assets. That's OT security you can deploy at scale.

Benefits

OT security you can deploy at scale

Cyber Vision embeds visibility capabilities into industrial network equipment. There's no need to deploy dedicated appliances or build out-of-band networks to send network flows to a central security platform. Network managers will appreciate the unique simplicity and lower costs of the Cyber Vision architecture.

Unmatched visibility on your OT cyber risks

Cyber Vision inventories all connected assets, maps their communication activities, and highlights their vulnerabilities so you understand your OT security posture. It detects malicious traffic and abnormal behaviors. All this information is collected by your network equipment, helping ensure 100% visibility.

Adaptive network segmentation to protect OT

Cyber Vision helps implement adaptive segmentation in OT in weeks, not years, so you can protect industrial operations at scale. It lets control engineers group OT assets, creating logical zones and conduits matching their industrial processes. IT can now create access control policies in Cisco Identity Services Engine or Cisco Secure Firewall that will not disrupt production.

Zero trust remote access to OT assets

Cyber Vision's Secure Equipment Access is a comprehensive Zero-Trust Network Access (ZTNA) solution purpose-built for OT workflows. It empowers operations teams with self-service remote access and lets you easily enforce least-privilege access policies so you can control risks from remote users.

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

Macrosegmentation made simple with Cisco Secure Firewall

Automate network segmentation below the IDMZ. Cisco Secure Firewall Management Center (FMC) uses asset groups created by control engineers in Cyber Vision to inform access policies and have Cisco Secure Firewall in the distribution network (IDF) enforced them. Not only this eliminates the need to zone-based firewall, it immediately adapts policies to changes in the OT environment.

Microsegmentation made simple with Cisco ISE

Use your industrial network to enforce ISA/IEC62443 zones and conduits. Cisco Identity Services Engine (ISE) leverages groups created in Cyber Vision to map network access policies to each OT assets and automate micro-segmentation of your industrial network enforced by Cisco networking equipment.

Unify IT and OT security with Splunk

Get comprehensive visibility across both your IT and OT environments. Splunk correlates security information from all your security solutions, including Cyber Vision, so it can detect advanced threats faster, run investigations across the IT and OT domains in a single console, and orchestrate response across your security stack to better protect the global enterprise.

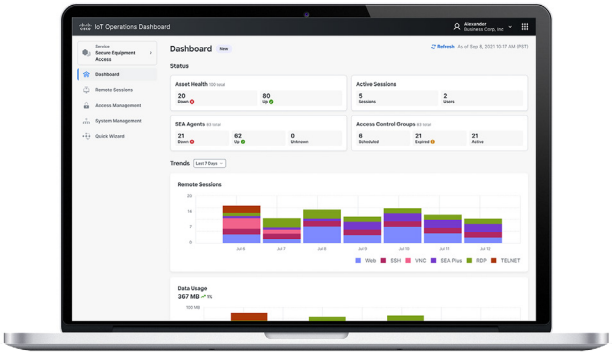
Next steps

To find out more about how Cisco can help you protect your industrial operations from cyber threats, visit www.cisco.com/go/cybervision or www.cisco.com/go/iotsecurity.

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

Cisco Secure Equipment Access

Zero trust remote access, purpose built for OT workflows



Enabling secure remote access to industrial assets can be a daunting task: Sites might be highly distributed, assets are often sitting behind NAT boundaries, and operations teams sometimes need to configure remote access in the middle of the night to keep production going.

With Cyber Vision's Secure Equipment Access, Cisco is solving these challenges. It combines all the benefits of a Zero Trust Network Access (ZTNA) solution with a network architecture that makes it simple to deploy at scale in industrial environments, and a self-service portal to help OT run operations as they need.

There is no dedicated hardware to install and manage. The Cisco switches or routers that connect your OT assets now also enable remote access to them.

And it features comprehensive zero trust security capabilities, enabling IT to enforce advanced remote access controls based on identities and contexts.

Benefits

- **Boosts operational efficiency:** Empower operations teams with a self-service portal that lets them configure remote access when they need it, without compromising on IT security policies
- **Simple to install and scale:** Stop struggling with dedicated appliances and complex VPN setups. Cisco SEA is a zero trust remote access solution embedded in switches and routers
- **Offers least-privilege access:** Allow select users to access only specific devices, using only certain protocols, and only at defined times
- **Enforces strong security controls:** Authenticate users with MFA and SSO. Verify their security posture. Block asset discovery and lateral movement
- **Takes control back:** Record sessions and build audit trails for investigation and compliance. Join and terminate active sessions

Next steps

To find out more about Cisco Secure Equipment Access and ZTNA for OT, visit www.cisco.com/go/sea or www.cisco.com/go/iotsecurity.

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

Network Management

Cisco Catalyst Center

Cisco Catalyst Center is a proven network management system deployed in the world's largest enterprises and most complex networks. Cisco Catalyst Center in industrial automation networks gives OT a curated view and set of functions to perform key network maintenance tasks, consistently and scalably, increasing Overall Equipment Effectiveness (OEE) and uptime, lowering operational costs, enhancing security, and helping ensure network performance.

Benefits

Network automation

- Discover existing network devices and topology
- Use network Plug and Play to provision new infrastructure
- Check for inconsistent configurations
- Deploying new images and patches at scale

Network assurance

- Collecting and analyzing network telemetry information
- Proactively identifying issues and root causes
- Helping step through remediation options

Industrial cybersecurity

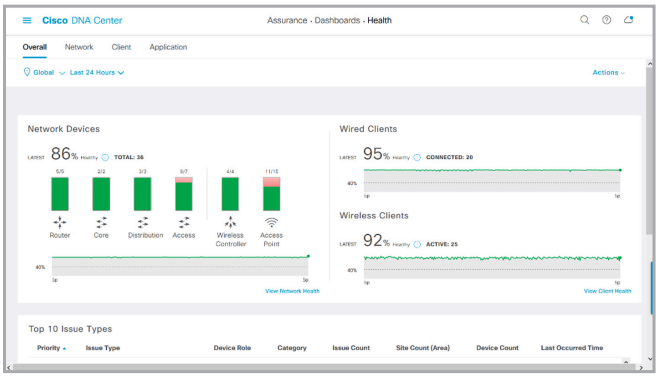
- Detailed visibility into connected industrial assets and applications
- Segment communications
- Monitor and detect abnormal behaviors
- Contain malware and other attacks
- Integrate operational and enterprise security

Next steps

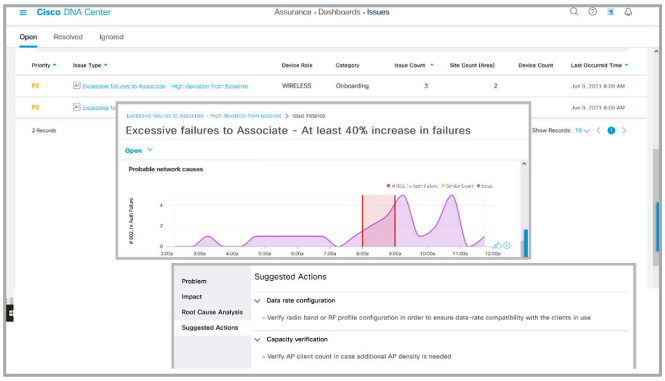
To find out more about Cisco Catalyst Center, visit www.cisco.com/go/iotmanagement.

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

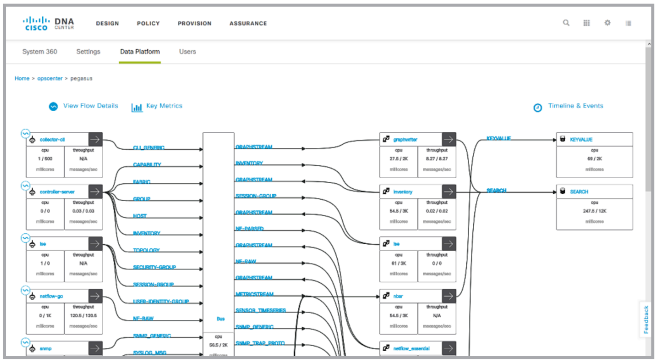
Network health



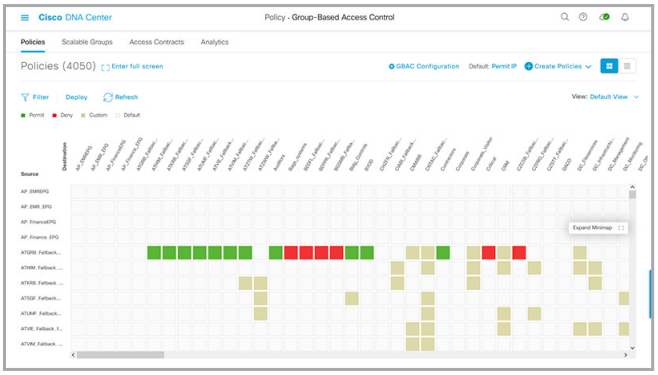
Network issues



Network topology



Access policies for segmentation

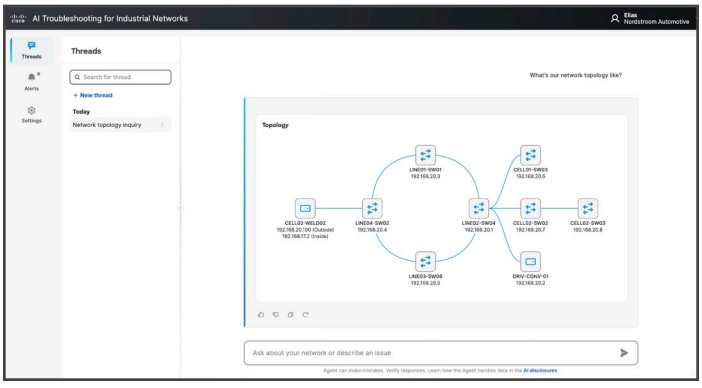


Meraki dashboard

The Meraki dashboard is a powerful cloud-based platform that simplifies network management by providing an intuitive and interactive web interface. It allows users to manage and monitor their network with ease, offering features such as zero-touch deployment, real-time network analytics, and comprehensive visibility into network health and performance. The dashboard supports a wide range of Cisco Meraki and Catalyst products, including wireless access points, switches, and security appliances, enabling seamless integration and management across the entire network. Additionally, the Meraki Dashboard enhances security by providing encrypted data transmission, two-factor authentication, and detailed logging capabilities, ensuring that network operations are secure and reliable. These features make the Meraki Dashboard an ideal solution for organizations looking to streamline their network management processes and improve operational efficiency.

Troubleshooting agent for industrial networks*

Part of Cisco's AgenticOps for industrial networks the troubleshooting agent empowers operational teams by acting as an easy-to-use, AI-powered networking expert specifically designed for industrial environments. It proactively monitors the network for anomalies, instantly diagnoses root causes when issues arise, and provides clear, actionable remediation steps. This streamlined approach significantly reduces Mean Time to Resolution (MTTR), prevents costly downtime, and enables OT teams to confidently maintain operational uptime and boost productivity, regardless of their networking skill level. The agent helps shift operations from reactive troubleshooting to proactive monitoring, thereby maximizing operational uptime and boosting productivity.



This product is currently in alpha stage of development.

Cisco Catalyst SD-WAN

As you connect distributed industrial sites together, it is essential to simplify and automate your WAN infrastructure deployment and management. Cisco Catalyst SD-WAN provides solutions for common challenges for industrial spaces by supporting multiple transports with configurable dynamic routing polices while leveraging the same security features and management tools for both the enterprise and industrial network extensions.

Cisco Catalyst SD-WAN Manager provides centralized policy creation for all Cisco industrial routers deployed in the infrastructure. By creating security policy templates, all existing devices, and any newly connected devices, will be subject to a consistent set of policies curated by the security team.

Manage and optimize your industrial fixed and mobile networks using SD-WAN:

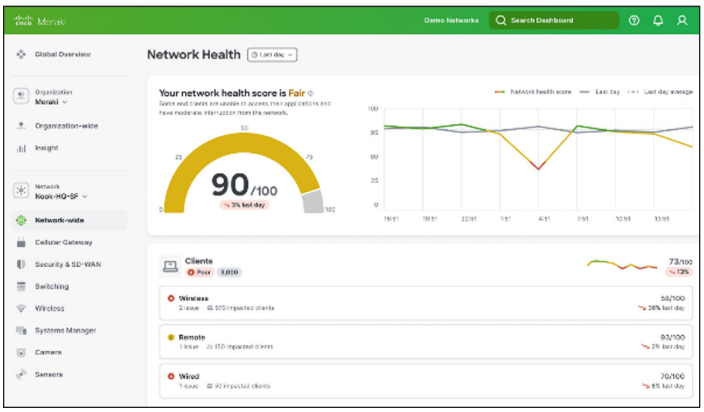
- **Simplified management** using a common management tool for your Enterprise and Industrial devices
- **Multi-WAN support** for always-connected mobile use cases
- **Secure** common policies are extended to the devices at your network edge
- **On-premises** or cloud-hosted architectural flexibility
- **Scalable** solution that allows thousands of assets to operate simultaneously, positioning the customer to meet future requirements

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

Automation benefits

- Zero-touch deployment of field gateways (i.e., no field staff required to configure a gateway)
- Simple provisioning of service VPNs to segregate traffic (such as Supervisory Control and Data Acquisition [SCADA], closed-circuit television [CCTV], Phasor Measurement Unit (PMU), IP Telephony, etc.)
- Templated configurations making it easy to change configuration and push it to gateways
- Application of unified security policies across a diverse range of remote sites and equipment
- Managing multiple backhaul connectivity options at the gateway, including private MPLS for critical SCADA traffic and cellular for backup, and even internet-based connections for non-critical traffic, where appropriate
- Lifecycle management of gateways (e.g., firmware updates, alarm monitoring, and statistics)

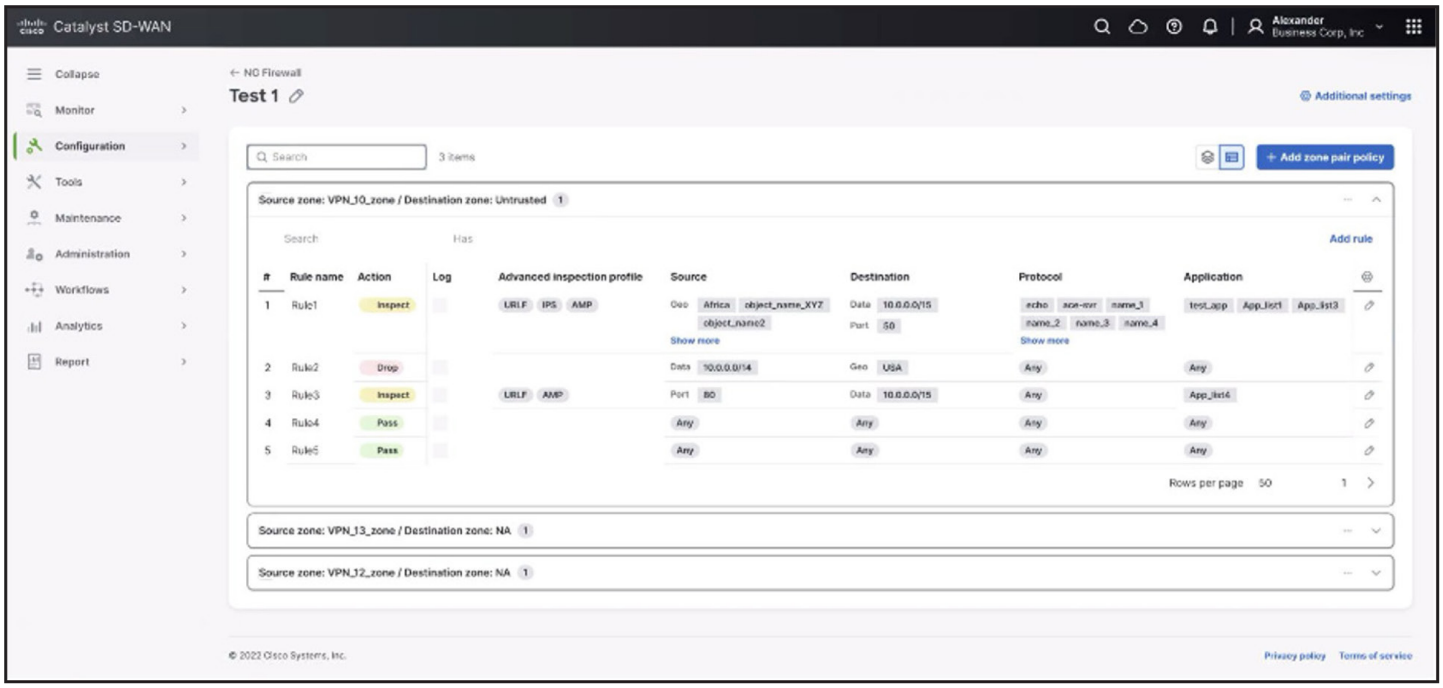
Network health



reliable. These features make the Meraki Dashboard an ideal solution for organizations looking to streamline their network management processes and improve operational efficiency.

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

Cisco Catalyst SD-WAN Manager centralizes security policy definition



Cisco Catalyst SD-WAN Manager also offers centralized logging and reporting. It collects all events, alarms, and logs from your Cisco industrial routers, giving security teams visibility and understanding of any activity that is occurring within their critical infrastructure and helping them comply with cybersecurity mandates like NIS2.

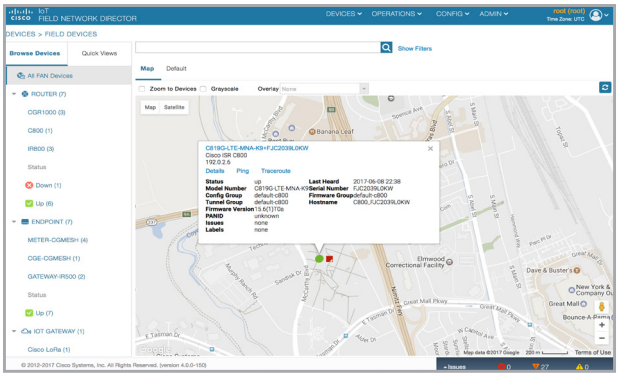
SD-WAN is well suited to industrial deployments because it supports the needed reliable multi-WAN connectivity options, includes configuration templates for replication of consistent configurations across a large geography, and protects devices and connected sensors using end-to-end network security that extends to the edge routers.

SD-Routing Mode on Catalyst SD-WAN Manager

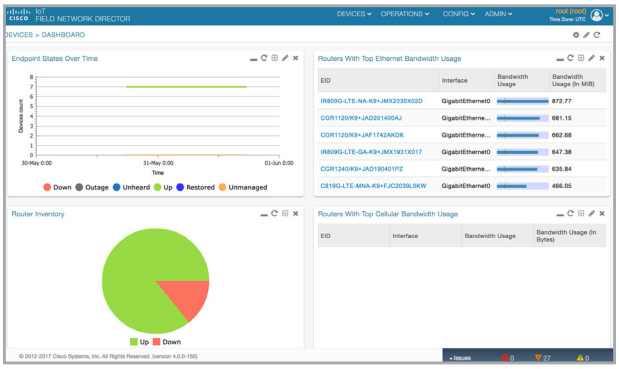
For those who prefer to keep their routers in autonomous mode, SD-WAN Manager supports routing deployments in SD-Routing Mode. Save time and energy managing your routing environment by simplifying monitoring, configuration, and security operations from a single intelligent dashboard. In fact, you can manage multiple deployments in SD-WAN Mode and in SD-Routing Mode all from SD-WAN Manager.

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

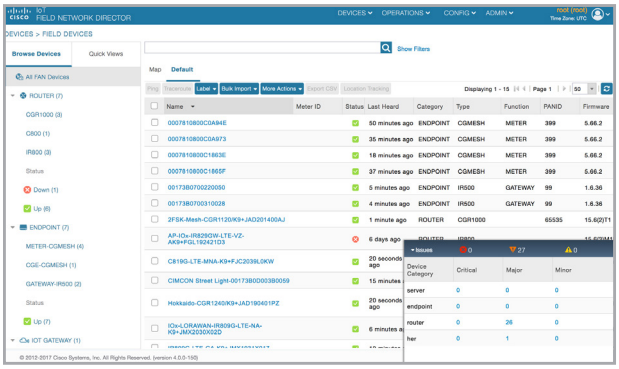
GIS map



Dashboard



Device listing



Device properties

Cisco IoT Field Network Director (FND)

The Cisco IoT Field Network Director (FND), the operating system for the multiservice Field Area Network (FAN), is a software platform that manages multiservice networks of Cisco industrial products, including industrial routers and endpoints for the utilities industry. Features that distinguish the IoT FND include:

- Ease of deployment at scale with Zero-Touch Deployment (ZTD) of gateways and devices
- Secure and scalable end-to-end enrollment and management of these gateways and devices
- Optimized for operation in constrained bandwidth network
- Ease of use with an intuitive web interface and GIS map visualization and monitoring
- Rich set of northbound APIs for third-party integration
- Scales to manage up to tens of thousands of routers and millions of mesh endpoints

Benefits

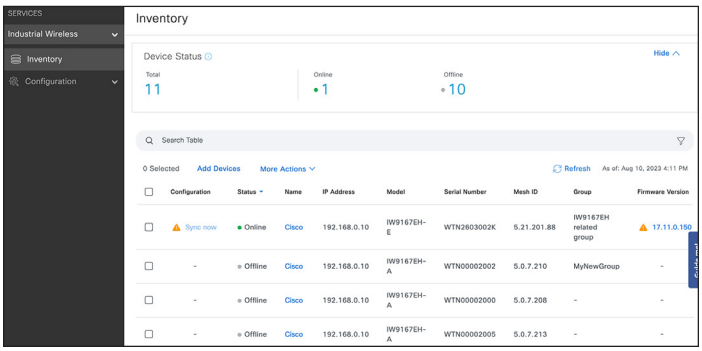
- Comprehensive and customizable dashboard for fast, at-a-glance network health check
- Real-time GIS maps of connected devices for increased asset visibility
- Simplify troubleshooting for operators by providing customizable rules to generate custom events that matter the most
- Integrate with existing automation applications, tools, and processes through open APIs
- Supports Cisco Catalyst IR1100 Rugged Series Routers and Cisco Catalyst IR8100 Heavy Duty Series Routers

Next steps

To find out more about Cisco IoT Field Network Director, visit www.cisco.com/go/fnd.

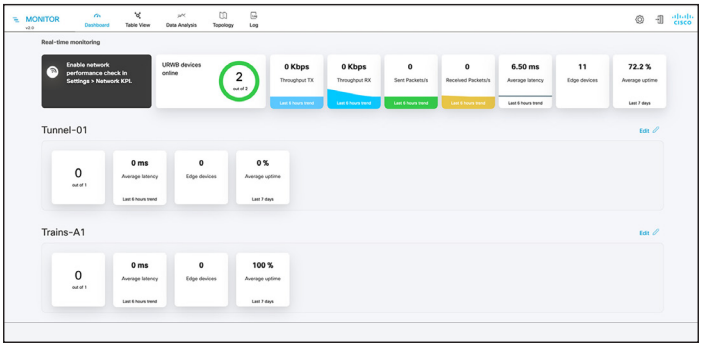
© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Industrial Wireless service



Industrial Wireless (IW) service is used to provision and manage standalone URWB IW devices. It is a secure, cloud-native, scalable service. It also allows you to configure and upgrade the firmware of connected devices remotely. For air-gapped networks, the offline mode still allows for creating templates and configuration files that can be locally uploaded to the device through the WebUI or command-line interface. To learn more about the IW service, see the Cisco Industrial Wireless service At-a-Glance.

Cisco Industrial Wireless Monitor



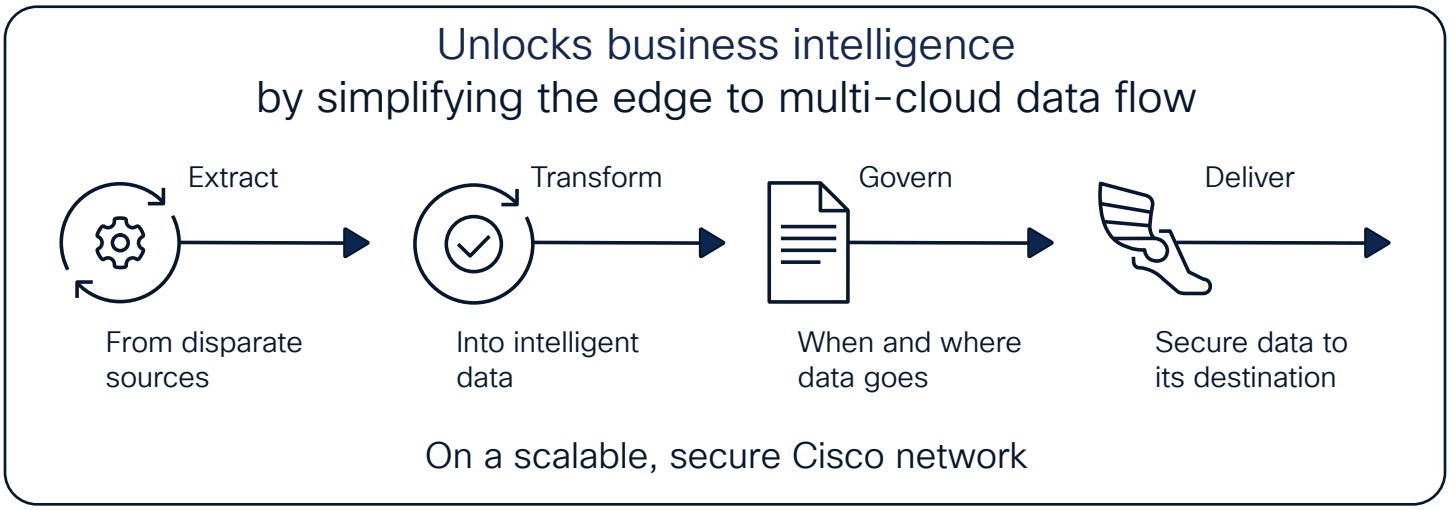
Industrial Wireless (IW) Monitor is a networkwide, on-premises monitoring tool, allowing any standalone URWB user to proactively maintain and monitor one or multiple wireless Operational Technology (OT) networks. IW Monitor displays data and situational alerts from every Cisco URWB device in a network, in real time.

IW Monitor supports fixed and roaming network architectures and allows easier end-to-end troubleshooting of any Cisco URWB system. It can be operated as a standalone system or in parallel with a sitewide Simple Network Management Protocol (SNMP) monitoring tool. It is designed to support network installations used in smart cities, rail, mining, ports and terminals, entertainment, smart factories, and military applications.
Learn more in the IW Monitor solution overview.

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

Edge computing

Cisco Edge Intelligence



Unlock business value by simplifying the edge-to-multicloud data flow

The best decisions are made when the right people have access to the right information at the right time. The IoT has dramatically increased the volume and variety of data produced, opening the door to a wave of new possibilities. The key is to extract the data from its source, transform it so it is usable, and securely deliver the right data to the right applications to put it to work.

But most solutions today are so complicated that organizations often cannot reap the full rewards of their data-gathering projects. The most important data is often at the remote edge of the network, where the core business operates, such as in oil rigs, delivery trucks, and utility substations, and on roads. In addition, organizations lose insight into who has access to what data and often don't have the needed flexibility and simplicity to send the data everywhere it needs to go.

Cisco Edge Intelligence delivers

Cisco Edge Intelligence securely delivers data from connected assets at the network edge to multicloud application destinations. The software is integrated into Cisco's industrial networking and compute devices for an out-of-the box experience to simplify deployment and lower costs. It provides full control over and governance of IoT data, from its extraction to its transformation to its secure delivery. And because Cisco Edge Intelligence has a network- integrated approach with centralized management across the network, applications, and data, it is easy to scale and secure.

Benefits

With Cisco Edge Intelligence, you gain:

- The ability to seamlessly extract, transform, and share data from connected assets at the IoT edge to multicloud environments
- An all-in-one solution for easy deployment out of the box
- Full data ownership, control, and governance
- Cisco security

Next steps

To learn more about Cisco Edge Intelligence, visit www.cisco.com/go/edgeintelligence.

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

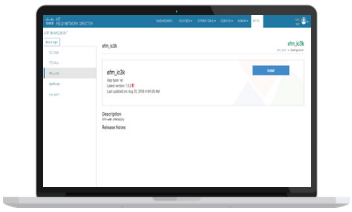
Cisco Edge Application Hosting

Edge compute application framework

Fast. Simple. Secure. Scalable.

Cisco Edge Application Hosting is a simple yet powerful infrastructure framework allowing developers and operators to securely onboard legacy and greenfield applications to their IoT edge infrastructure at massive scale, creating business value from previously untapped data.

Management tool

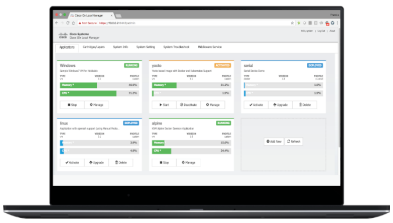


- Zero-touch deployment of devices
- Centralized device and application lifecycle management at scale
- End-to-end security

Benefits

- **Transformation of IoT data into new digital business value:** Build new business with the ability to process high volumes of data at the edge and deliver closed loop system control in real time
- **Rapid time to value:** Achieve business outcomes associated with IoT initiatives more rapidly with application execution at the edge and scale with the Cisco partner ecosystem
- **Broad scope of impact:** Reach production deployment rapidly with edge application management and execution at IoT scale

Docker developer tool EMU



- Execute container or virtual machine concurrently
- Run Windows or Linux applications
- Easily consumable Edge Application Hosting system services

Cisco Edge Application Hosting components

- **Cisco application hosting-enabled edge network devices:** The Cisco edge application framework provides uniform and consistent hosting capabilities for applications across the Cisco IoT network infrastructure. The Cisco Edge Application Hosting environment brings together Cisco IOS XE Software, the industry-leading and highly secure networking operating system, and Linux, the leading open-source platform.
- **Cisco Edge Application Hosting developer tools and documentation:** SDKs, command-line and web-based UI tools, and Cisco DevNet documentation on how to build, package and deploy edge applications to Cisco IOx enabled network devices.
- **Cisco Edge Application Hosting management:** Deploy and manage edge applications at scale from centralized device and edge application management software. Support for both on-premises and cloud-based management. These edge applications may be supplied by an ecosystem partner and Cisco or developed with a range of common programming languages.

Next steps

The Cisco Edge Application Hosting framework offers consistent management and hosting across network infrastructure products. To find out more about Cisco Edge Application Hosting, visit www.cisco.com/go/iox and developer.cisco.com/docs/iox/.

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

Cisco Industrial IoT Portfolio

Deploy. Accelerate. Innovate.

Cisco Industrial IoT is an end-to-end architecture that enables you to digitize your business and drive better business results. It offers rock-solid infrastructure, unprecedented visibility, security, and control, and trusted expertise to help ensure the success of your IoT deployment.

www.cisco.com/go/iiot

© 2026 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

C02-741513-18 02/26