Cisco Industrial IoT Portfolio

www.cisco.com/go/iiot

Contents

Bring Cisco scale and security to Industrial IoT	3
Cisco Catalyst Industrial Ethernet (IE) switching portfolio	5
Cisco Industrial Router (IR) portfolio	12
Industrial Wireless (IW) access points and clients	16
Cisco Industrial IoT embedded networks portfolio	20
Industrial cybersecurity	22
Management	25
Edge computing	31
Cisco IoT Validated Designs	33
Cisco Industrial IoT solutions	34

Bring Cisco scale and security to Industrial IoT

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.

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

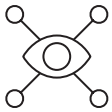
Unparalleled visibility and control

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

Trusted expertise

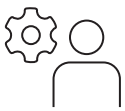
Partner with a trusted leader who offers continuous innovation, market-leading products, an extensive developer program, and resources like deployment blueprints to make you successful

Industrial IoT enables transformative use cases



Remote monitoring

Asset tracking



Worker safety

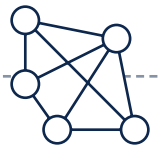
Operational agility

Industrial automation

Predictive maintenance

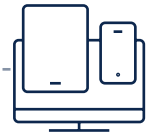
Cisco offers an unparalleled end-to-end Industrial IoT architecture

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

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.

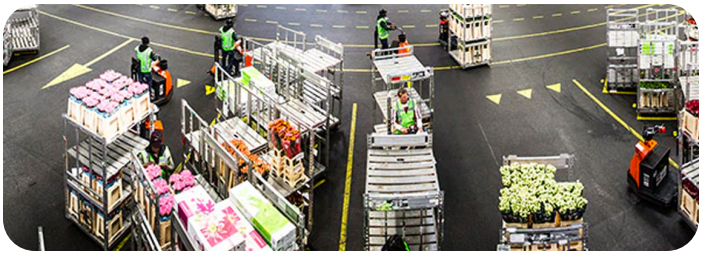
Next step

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

Featured design guides

Extended enterprise

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

Cisco Catalyst Industrial Ethernet (IE) switching portfolio

The Cisco® Industrial Ethernet (IE) switching portfolio includes ruggedized, secure, easy-to-use switches built for extending enterprise networks to outdoor and 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.

Visibility and security

Cisco Catalyst IE switches are available with robust visibility and security features. Select IE switch models incorporate Cisco Cyber Vision, which provides granular visibility into connected assets and traffic flows to monitor your security posture and helps you define rules for network segmentation. IE switches are compatible with Cisco Software-Defined Access (SD-Access), which can be used for easy segmentation, threat isolation, and building a zero-trust industrial network. Select IE switch models can also run Cisco Secure Equipment Access to enable Zero-Trust Network Access (ZTNA) and secure remote access to industrial assets. Your staff and vendors can use SEA for remote configuration, monitoring, or troubleshooting, to increase operational efficiency and reduce costs.

Cisco Catalyst 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 is certified against ISA/IEC 62443- 4-1 as well as ISA/IEC 62443-4-2 which provides assurance that the switches are themselves protected against cyberthreats and contribute to the overall security and resilience of industrial operations. Catalyst IE switches also contain several embedded security features that provide additional layers of protection.

Easy 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.

Multiple 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 PoE needs.
- **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 ones. Some Cisco IP67-rated switch models also provide PoE.
- **Embedded switches:** These switches are ultra-compact and built for secure, high-bandwidth, mission-critical mobile networks. They enable integrators to build custom solutions for specialized use cases.

Built-in OT security and services

Select models of the IE switch portfolio with the open Cisco IOx edge-compute capabilities run a number of essential services. This differentiating feature of the switches eliminates the need for span networks and additional servers and equipment to run these applications. By hosting the services within the switch, this differentiating feature eliminates the need for multiple single-function point solutions, providing a close integration between networking and security and making the architecture simpler, scalable, and more secure.

These services include:

- Cyber Vision sensor to gain granular visibility into connected assets, their vulnerabilities and your security posture, increase operational efficiencies, and help define segmentation policies.
- Dynamic segmentation of operations into zones and conduits to restrict communications between unrelated assets to keep attacks from spreading.
- Secure Equipment Access gateway, which enables Zero-Trust Network Access (ZTNA) features for secure remote access to industrial assets using least privilege policies and strong security controls.
- Edge Intelligence to collect process data in real-time to help improve governance and make better business decisions.

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 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
- Edge compute supporting application hosting
- Cisco Cyber Vision for Industrial Control System (ICS) visibility
- Cisco Secure Equipment Access for scalable, simple, and secure zero-trust remote access to industrial assets
- Cisco Edge Intelligence for real-time data extraction

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 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

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
- Edge compute supporting application hosting
- Cisco Cyber Vision for Industrial Control System (ICS) visibility
- Cisco Secure Equipment Access gateway for scalable, simple, and secure zero-trust remote access to industrial assets
- Cisco Edge Intelligence for real-time data extraction

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.

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

Cisco Catalyst IE3100 Rugged Series

- Ultra-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+ (power budget up to 240W)
- Conformal coating (on select model)
- Cisco IOS XE operating software
- Cisco Catalyst Center for management
- Cisco Secure Equipment Access gateway for scalable, simple, and secure 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

Rack-mount switches

Cisco Catalyst IE9300 Rugged Series Switches

- 19-inch rack-mount switch
- Based on the Cisco UADP ASIC
- All Gigabit Ethernet platform, Layer 2 or Layer 3
- 26 fiber ports, 2 combo Gigabit Ethernet ports (on select models)
- 24 copper ports with PoE/PoE+ (on select models and with power budget up to 720W)
- 4x 10G fiber uplinks (on select models)
- Multigigabit copper ports with 90W/port 4-pair PoE (on select model and with power budget up to 720W)
- GNSS/GPS antenna interface and conformal coating (on select model)
- Cisco IOS XE operating software
- Vertical stacking up to 8 members
- Advanced industrial and redundancy protocols
- Edge compute supporting application hosting
- Cisco Cyber Vision for Industrial Control System (ICS) visibility
- Cisco Catalyst Center for management
- SD-Access fabric edge node

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

Heavy-duty IP67 switches

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
- Edge compute supporting application hosting
- Cisco Cyber Vision for Industrial Control System (ICS) visibility
- Cisco Secure Equipment Access gateway for scalable, simple, and secure zero-trust remote access to industrial assets
- Cisco Edge Intelligence for real-time data extraction

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.

Cisco Industrial Router (IR) portfolio

The 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 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 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.

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.

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 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.

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
- Cisco Cyber Vision for Industrial Control System (ICS) visibility
- Cisco Secure Equipment Access for remote asset access
- 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

Cisco Catalyst IR1800 Rugged Series Routers – FirstNet Capable

- Highly secure, high-performance, modular routers with 5G and Wi-Fi 6 for both mobile and fixed locations
- Next-Generation Firewall capabilities built-in
- Automotive certification and CAN-bus support
- SD-WAN with comprehensive threat protection and security features
- Cisco IOS XE operating software
- Edge compute supporting Cisco Edge Application Hosting
- Cisco Cyber Vision for Industrial Control System (ICS) visibility
- Cisco Secure Equipment Access for remote asset access
- Cisco Edge 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

Expansion modules for the Catalyst IR1101

Enjoy the very small form factor of the Catalyst IR1101, or expand with one or two modules to add more connectivity options:

- IR1101 serial expansion module adds 4 asynchronous serial ports and 2 Gigabit Ethernet LAN ports
- IR1101 cellular expansion module adds one slot for a pluggable network module and one SFP Gigabit Ethernet port as well as an optional 4 GPIO ports and one mSATA slot for data storage

Cisco Catalyst IR8100 Heavy Duty Series Routers – FirstNet Capable

- Heavy duty, IP67-certified, fully modular industrial router designed for harsh outdoor environments
- 5G, public and private LTE, and more
- Advanced cybersecurity and hardware security
- Built-in edge compute and SD-WAN-enabled
- 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
- Cisco Cyber Vision sensor with Snort IDS for Industrial Control System (ICS) visibility
- 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 pluggable module, FirstNet Capable
- Cat18 4G LTE Advanced Pro pluggable module with CBRS and private-LTE support, FirstNet Caoable
- 4G LTE 450-MHz pluggable module*
- 5G Standalone (SA) and Non-Standalone (NSA) sub-6-GHz cellular pluggable module
- 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.

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**.

Industrial Wireless (IW) access points and clients

Workers, assets, and resources are becoming increasingly connected in oil and gas, mining, transportation, and manufacturing. 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. For most of our models, the same hardware can run in either Wi-Fi 6E or Cisco Ultra-Reliable Wireless Backhaul mode. This dual-mode capability gives you the flexibility to decide which technology to use depending on the project requirements. The operational mode can be swapped in the field to enable you to adapt the product to the specific use case, facilitating the transition between the two technologies and optimizing the investment. This flexibility allows you to support a wide range of use cases and deployment scenarios offering different form factors for different applications.

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. Cisco URWB is also scalable, is easy to install, and uses free spectrum.

Cisco URWB can be used to create static, nomadic, and seamless roaming wireless backhaul networks for OT applications. These networks have been designed and successfully deployed in rail, mining, smart cities, container terminals, entertainment, smart factories, military, automotive, and video broadcasting industries. The MPLS-based secure wireless protocol that enables this technology can provide a set of benefits that surpasses other standards and industrial solutions.

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, Cisco 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.

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 patented technology, Multipath Operations (MPO), provides uninterrupted wireless connectivity by sending high-priority packets via redundant paths. 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.

Cisco Catalyst IW9167E Heavy Duty Access Point

- Supports Wi-Fi 6/6E, WGB, or URWB
- 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, WGB or URWB
- 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

Cisco Catalyst IW9167E Heavy Duty Access Point for High-density deployments

- Supports Wi-Fi 6/6E
- Tri 802.11ax Wi-Fi 6E radio (2.4 GHz, 5 GHz, 6 GHz), bringing all the benefits of Wi-Fi 6E to the harshest environments: more spectrum, more channels, higher throughput, and improved security
- 4x4 MIMO, 4 spatial streams
- Pre-assembled with integrated 6E outdoor directional panel antenna designed to address challenges of Wi-Fi in high-density environments such as large public venues
- IP67 certified, withstands dust, water and extreme temperature ranges of -40° to +70°C (-40° to 158°F)
- Supports GNSS, BLE and scanning radio for spectrum management minimizing interference
- Can be powered by PoE or DC

Cisco Catalyst IW9167I Heavy Duty Access Point

- Supports Wi-Fi 6/6E
- 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, WGB, or URWB
- 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

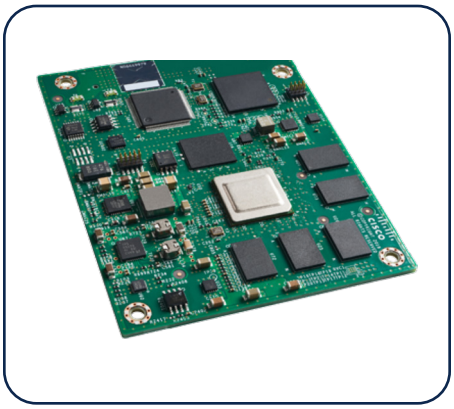
- Supports Wi-Fi 6/6E or URWB
- Dual 802.11ax radio (5 GHz, 5/6 GHz)
- Built-in directional antenna for easy deployments
- Choice of external antennas to quickly extend network to new places when needed (2 N-type)
- 2 Multigigabit RJ-45, optional M12 adapters
- Heavy-duty, IP67-certified enclosure to 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.

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

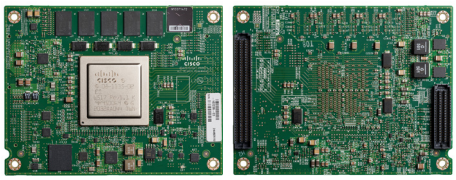
The ESR6300 provides two WAN ports of Gigabit Ethernet that give you a choice of media type and four LAN ports of Gigabit Ethernet with PoE/PoE+ ready options. As your needs evolve, add mSATA storage for Cisco Edge Application Hosting.

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.

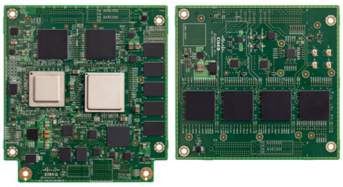
Software-defined WAN on the ESR6300

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.



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
- 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

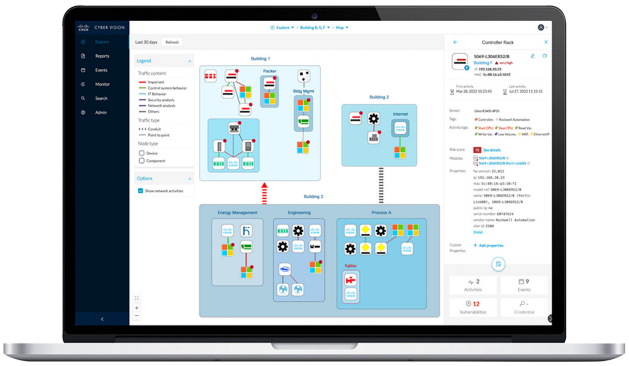
Next steps

Find out more about Cisco's IoT embedded networks.

Industrial cybersecurity

Cisco Cyber Vision

Visibility into your OT/ICS assets and your security posture.



Cisco Cyber Vision provides asset owners full visibility into their Industrial Control System (ICS) and their OT security posture so they have the information they need to reduce the attack surface, segment the industrial network, and enforce cybersecurity policies. Its advanced OT monitoring capabilities also provide insights to improve network efficiency and enable faster troubleshooting of operational issues.

Combining a unique edge architecture that embeds OT security features into your industrial network and deep integration with Cisco's leading security portfolio, Cisco Cyber Vision can be easily deployed at scale to enable IT and OT teams to work together in building innovative industrial operations while securing the global enterprise.

Benefits

Unmatched visibility into all connected assets

Know what to protect. Cisco Cyber Vision automatically builds a detailed inventory of all connected assets, including their communication patterns, vulnerabilities, rack slot configurations, vendor references, serial numbers, and more.

Visibility embedded into your industrial network

Easily deploy at scale. Cisco Cyber Vision embeds visibility capabilities into industrial network equipment. No need to source dedicated appliances or build a dedicated out-of-band network. Network managers will appreciate the unique simplicity and lower costs of Cisco Cyber Vision.

Security posture for IT

Reduce the attack surface. Cisco Cyber Vision calculates risk scores for each part of your operations to help you prioritize what needs to be fixed. Fully integrated with the Cisco security portfolio, it extends the IT Security Operations Center (SOC) to the OT domain.

Operational insights for OT

Improve network performance and reduce downtime. Cisco Cyber Vision provides insights into network issues, device misconfigurations, communication problems, unexpected changes to industrial processes, malicious traffic, and more.

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 environement.

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

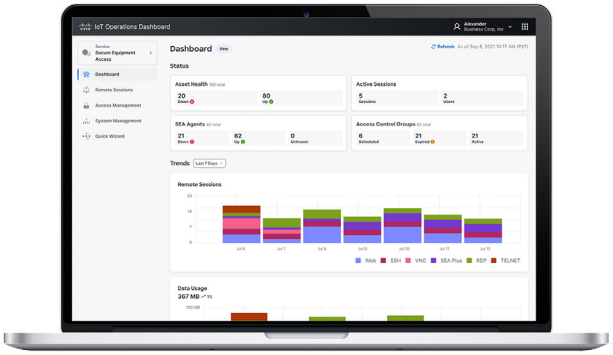
Get comprehensive visibility across both your IT and OT environements. Splunk correlates security information from all your security solutions, including Cyber Vision, so it can detect advanced threats faster, run investigations across the IT and OT domains in a single console, and orchestrate response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

Cisco Secure Equipment Access

Zero-Trust Network Access (ZTNA) for operational environments



Remote access is key to being able to configure, manage, and troubleshoot OT assets without time-consuming and costly site visits. Enabling secure remote access at scale can be a daunting task: Sites might be highly distributed, and assets are often sitting behind Network Address Translation (NAT) boundaries. Configuring firewall rules and deploying dedicated gateway hardware puts an extra burden on IT and OT teams.

With Secure Equipment Access (SEA), Cisco is solving these challenges. It combines all the benefits of a ZTNA solution with a network architecture that makes it simple to deploy at scale in operational environments. There is no dedicated hardware to install and manage. No complex firewall rules to configure and maintain. The Cisco industrial switches or routers that connect your OT assets now also enable remote access to them. And it features comprehensive security capabilities, with advanced cybersecurity controls and easy-to-build policies based on identities and contexts.

Benefits

- **Boosts operational efficiency:** Empower operations teams to easily gain remote access to OT assets, even those behind NAT boundaries
- **Simple to install and scale:** Stop struggling with dedicated appliances and complex firewall setups. Cisco SEA is 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.

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

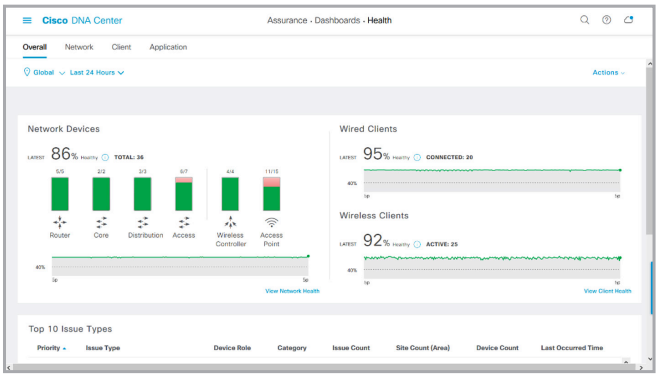
Industrial cybersecurity

- 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

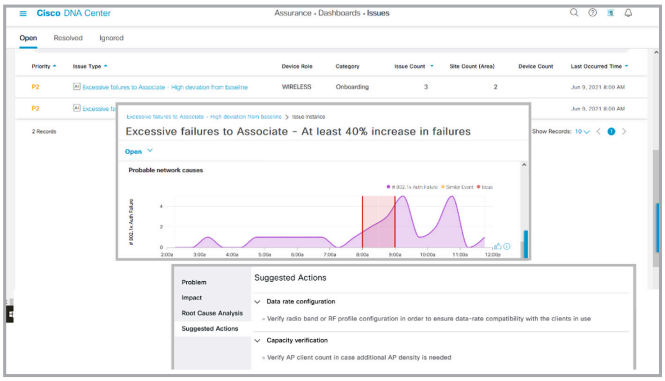
Next steps

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

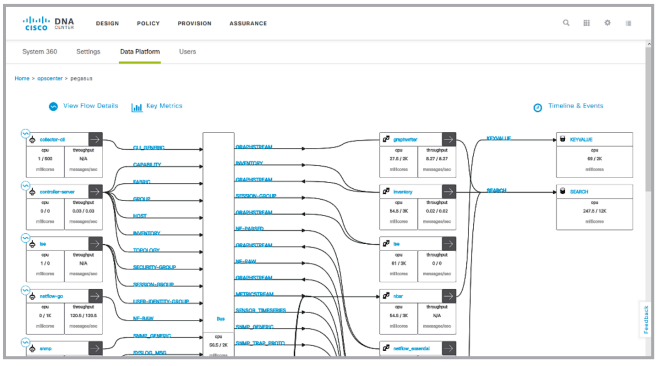
Network health



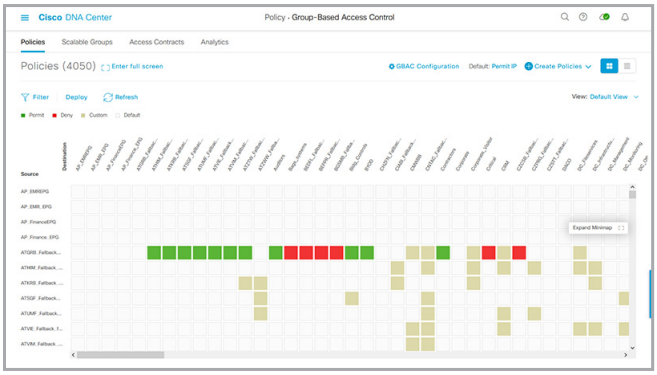
Network issues



Network topology



Access policies for segmentation



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.

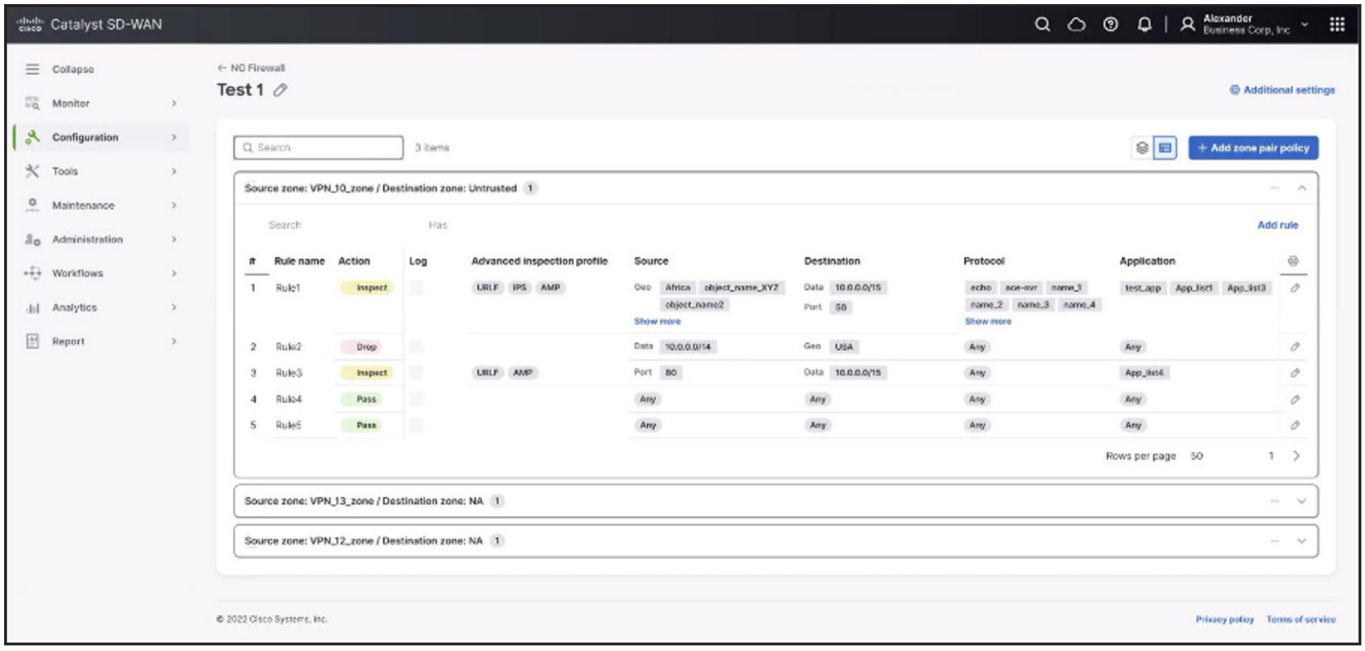
Manage and optimize your industrial fixed and mobile networks using SD-WAN:

- **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

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)

Cisco Catalyst SD-WAN Manager centralizes security policy definition



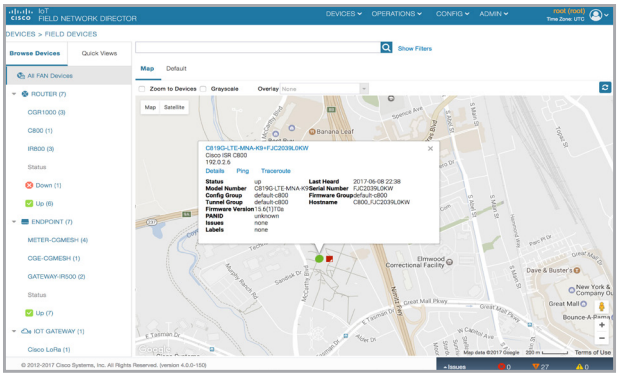
Cisco Catalyst SD-WAN Manager also offers centralized logging and reporting. It collects all events, alarms, and logs from your Cisco industrial routers, giving security teams visibility and understanding of any activity that is occurring within their critical infrastructure and helping them comply with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

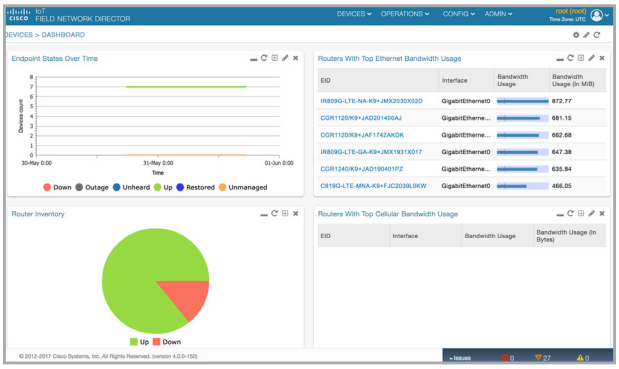
SD-Routing Mode on Catalyst SD-WAN Manager

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.

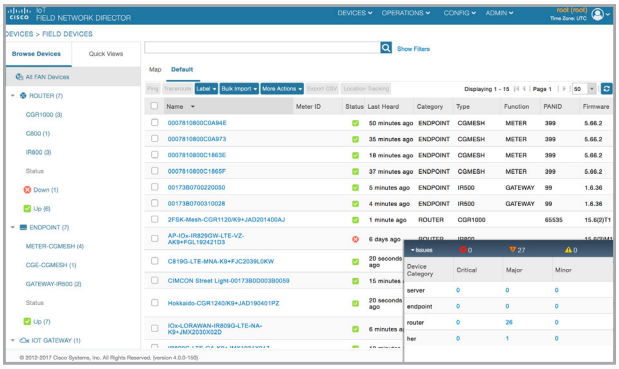
GIS map



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

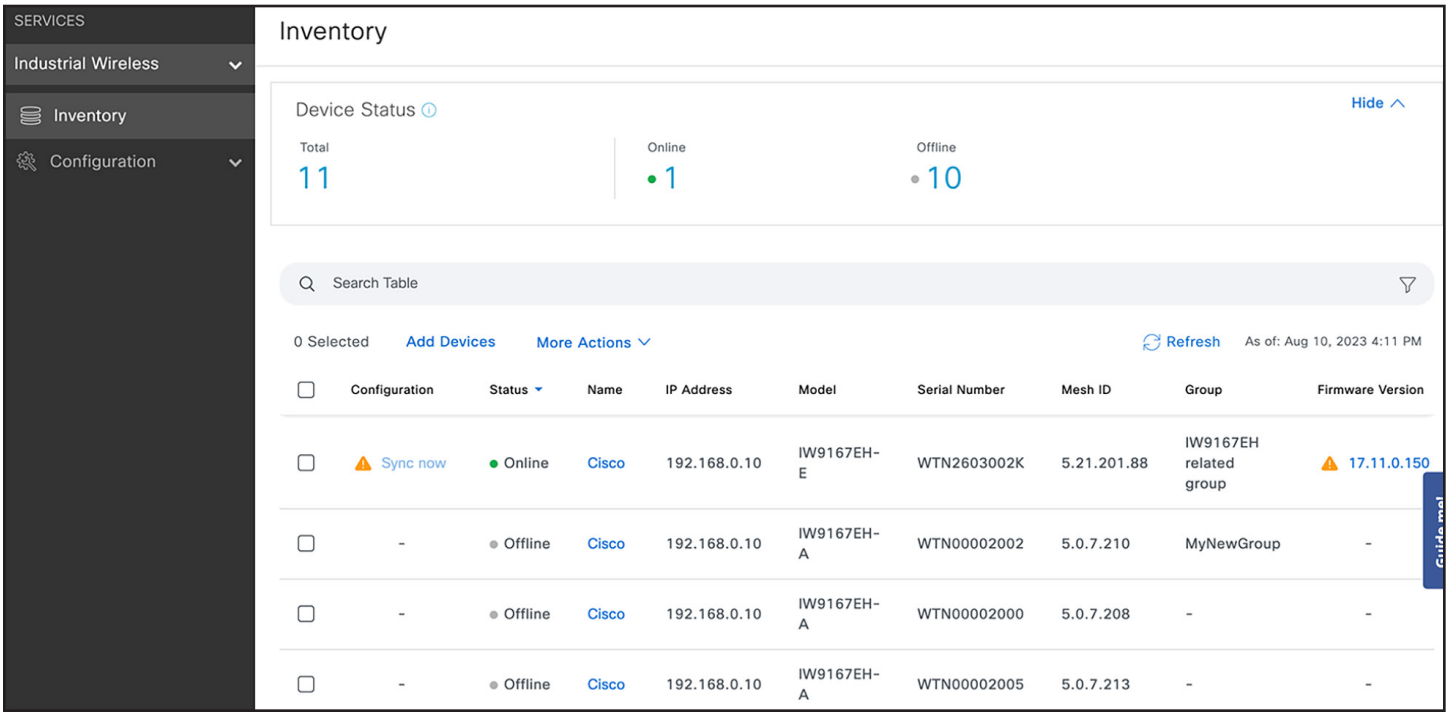
Benefits

- 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

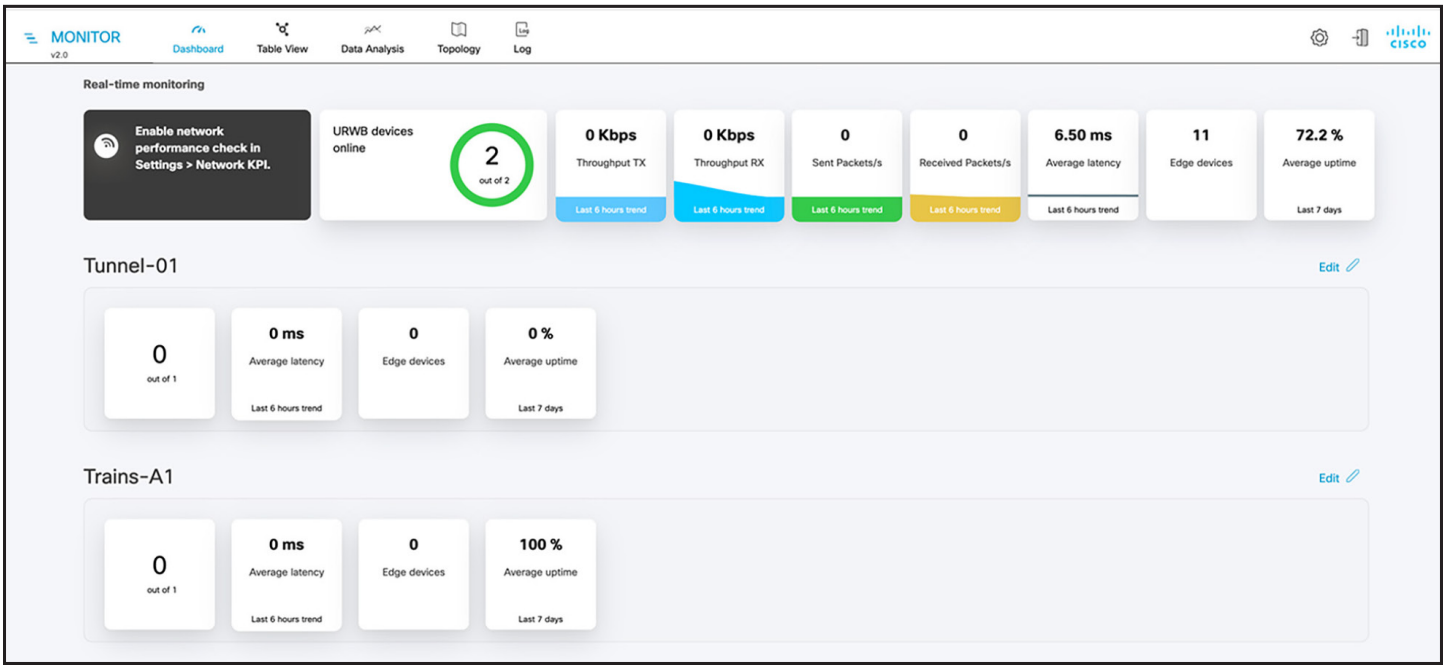
To find out more about Cisco IoT Field Network Director, visit www.cisco.com/go/fnd.

Cisco Industrial Wireless service



Industrial Wireless (IW) service is used to provision and manage 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

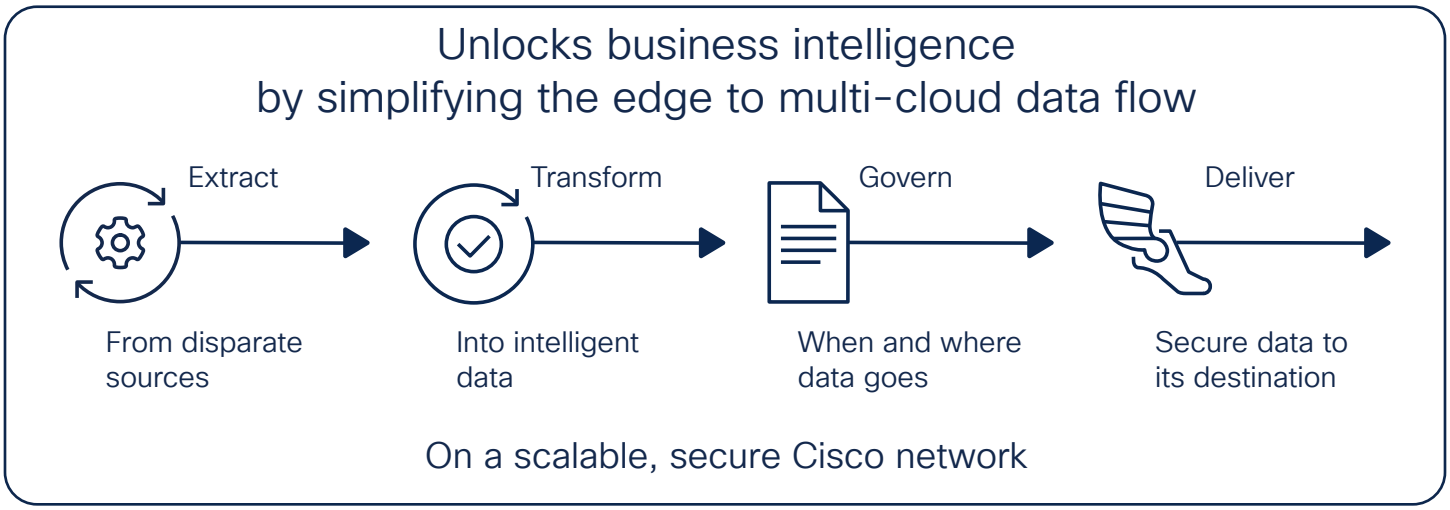


Industrial Wireless (IW) Monitor is a networkwide, on-premises monitoring tool, allowing any URWB user to proactively maintain and monitor one or multiple wireless Operational Technology (OT) networks. IW Monitor displays data and situational alerts from every Cisco URWB device in a network, in real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

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.

Cisco Edge Application Hosting

Edge compute application framework

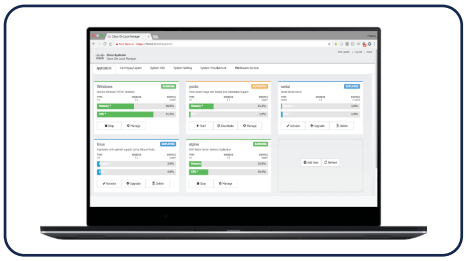
Fast. Simple. Secure. Scalable.

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.

Benefits

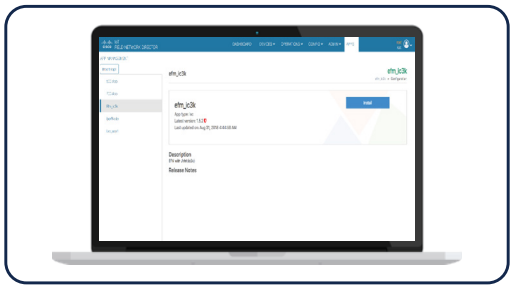
- **Transformation of IoT data into new digital business value:** Build new business with the ability to process high volumes of data at the edge and deliver closed loop system control in real time
- **Rapid time to value:** Achieve business outcomes associated with IoT initiatives more rapidly with 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

Management tool



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

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/.

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

C02-741513-13 11/24