Validated Profile: Manufacturing (Nonfabric) Vertical

December 19, 2024

Solution Overview

This guide describes Cisco's preferred deployment profile for a manufacturing production network. It offers guidance for a typical nonfabric deployment using Cisco Catalyst Center and serves as a validation resource for deployment engineers. It blends theoretical and practical information to equip engineers with essential service insights, assisting them in making informed decisions during deployment and configuration. This guide is aligned with and generally follows design and implementation guidance in our Industrial Automation and Converged Plant-wide Ethernet (CPwE) Cisco-validated designs (CVDs).

The audience for this guide is IT and operational technology (OT) professionals who deploy or manage manufacturing production networks. This guide serves as a validation reference for vendors, partners, system implementers, customers, and service providers involved in designing, deploying, or operating production systems.

Production environments have evolved significantly over the past 15 years, moving away from proprietary and niche networking technologies towards standard networking technologies and practices. Production networks are typically deployed and managed with a mix of IT and OT teams. These production environments have a unique set of requirements, including the need for network automation to consistently deploy large networks, enhanced network security for environments with little cybersecurity, highly available resilient network infrastructure to support critical operations, simplified monitoring for non-IT operators, and efficient troubleshooting to get operations up and running. The following sections delve into these critical areas, which are fundamental to the development of modern factories, production facilities, and warehouses.

High Availability

Manufacturing operations often run continuously and any disruption in the network can result in production downtime leading to significant financial loss. High availability (HA) ensures that the network is operational in the event of hardware failures, software issues, connectivity issues, or other disruptions, reducing the production downtime to a minimum. Ensuring the uptime of industrial automation and control systems within the manufacturing network requires a robust and resilient network.

The network architecture employed in this guide enhances reliability and fault tolerance of the network, management, and access control systems. The architecture reduces single points of hardware failure through the implementation of switch stacking (physical or virtual) on the supported Cisco Catalyst switches across the OT network, wherever relevant. Network resiliency is accomplished by incorporating multiple network paths, along with the necessary Layer 3 routing protocols and resiliency protocols designed to provide fast recovery within the Layer 2 network. The network setup is engineered for rapid convergence, which is crucial given the stringent latency and minimal packet loss requirements in the manufacturing networks. In addition to the network infrastructure, the systems managing and configuring the network devices are deployed in a redundant mode. Catalyst Center includes a HA configuration with three nodes. Furthermore, Cisco ISE controlling the network policy is deployed as a multi-node cluster with redundancy such as the Policy Administration Node (PAN), Policy Service Nodes (PSN), Platform Exchange Grid (pxGrid), and Monitoring and Troubleshooting Node (MnT).

Network Automation

Manufacturing facilities often have large, complex networks with numerous devices and configurations. Automation streamlines network provisioning, configuration changes, and maintenance tasks reducing downtime, workloads, and the risk of human errors. Scalability is an essential factor for automating a manufacturing network with large number of network devices. Catalyst Center enables seamless onboarding of network devices at a scale for the initial configurations (day-zero configurations) using the plug and play approach, which makes it a crucial tool for automating a complex manufacturing network. Moreover, it supports automated provisioning of configuration changes (day-n configurations) ensuring consistent configuration across all network devices. Software upgrades can be difficult and time-consuming, particularly when dealing with numerous network devices running different images and versions. The Software Image Management (SWIM) feature on Catalyst Center simplifies the software upgrade process and reduces the time taken for upgrades. By centralizing the network automation functions, Catalyst Center addresses the networking requirements for both IT and OT, comprising wired and wireless connectivity while integrating with various security platforms available in the Cisco product portfolio.

Network Security

Network security is a critical requirement for manufacturing networks. Manufacturing networks play an important role in providing connectivity for controlling and overseeing critical processes and machinery. When security is compromised, it can lead to disruption in production resulting in financial loss and potential safety risks. Network security breaches, malware infiltrations, or cyber attacks can lead to significant production downtime causing delayed deliveries, unmet production targets, and revenue setbacks. Unauthorized access or data breaches can expose manufacturers to intellectual property theft and industrial espionage.

The security architecture described in this document integrates the full spectrum of security measures as detailed in the Industrial Automation Security Design Guide, which includes:

- Secure network infrastructure with Cisco Trustworthy technology.
- Next-generation firewalls to establish the Industrial Demilitarized Zone (IDMZ) for protecting the production systems.
- Enhanced view of various assets on the manufacturing plant floor using Cisco Cyber Vision.
- Security policy deployment and segmentation using Cisco TrustSec with Cisco ISE.
- Improved detection and response to issues with Cisco Extended Detection and Response (Cisco XDR).
- Identification of anomalies and malware threats using Cisco Secure Network Analytics and Cisco Cyber Vision.

Network Monitoring and Troubleshooting

As manufacturing processes become increasingly reliant on networked systems, effective network management becomes indispensable. Network management ensures operational continuity, resource efficiency, and security, contributing to the success and competitiveness of the manufacturing facilities. Immediate fault detection is crucial to identify issues such as network congestion, hardware failures, security breaches, and so on. Network management tools can quickly identify problems, reducing the time it takes to resolve them. Network management tools can provide valuable insights into network performance and traffic patterns, which can be used for process optimization, predictive maintenance, and making informed decisions.

Catalyst Center provides an all-inclusive network management platform, excelling in the domains of network monitoring and troubleshooting. It enables network visibility, facilitating the monitoring of devices, applications, service status, and performance. Catalyst Center helps in tracking the health of various network devices such as switches, routers, access points, and endpoints, providing valuable insights into their operational status. The platform also provides tools for traffic analysis, enabling the characterization of network traffic patterns, anomaly detection, and alerts on potential issues that may impact network performance. Additionally, Catalyst Center can provide alerts and notifications based on predefined criteria or network events, allowing the network administrators to respond to issues immediately. Catalyst Center displays network topology maps showing the device interconnections, which helps to understand the network architecture and identify any potential points of failure.

When network issues occur, Catalyst Center helps to identify the root cause by providing detailed insights into the device and traffic behavior. Catalyst Center provides path analysis tools to trace network paths and identify blockage or connectivity issues that may affect application performance. The platform also retains the historical data, enabling administrators to review past network events and performance trends to identify recurring issues.

Hardware and Software Specifications

The solution is validated with the hardware and software listed in the following table.

Role	Model Name	Hardware Platform	Software Version
Catalyst Center Controller	DN2-HW-APL-XL	Catalyst Center Appliance 3-Node Cluster	2.3.7.7
Identity Management, RADIUS Server	ISE-VM-K9	Cisco Identity Services Engine Virtual Appliance	3.3 Patch 4
Network Discovery, Visibility, Anomaly Detection	CV-A-250	Cisco Cyber Vision	4.2.2, 5.0.1
Security Monitoring, Anomaly and Threat Detection	L-ST-SMC-VE-K9 L-ST-FC-VE-K9	Cisco Secure Network Analytics Manager, Cisco Secure Network Analytics Flow Collector	7.4.2
Firewall Manager	FMCv25	Cisco Secure Firewall Management Center	7.2.8
Firewall IDMZ	FPR-2140	Cisco Firepower	7.2.8
Cisco Access Switch	IE3100-18T2C IE3105-18T2C IE3200-8P2S IE3200-8T2S IE3300-8P2S IE3300-8T2S IE3300-8T2X IE3300-8U2X IE-3400-8P2S IE3400-8T2S IE3400H-24FT	Cisco Catalyst IE3100, 3200, 3300, 3400, 9320	17.9.5, 17.12.4
Cisco Distribution Switch	C9300-24T C9300-48T C9300X-24Y C9300X-12Y	Cisco Catalyst 9300 Series Switches	17.9.5,17.12.4
Cisco Core Switch	C9500-12Q C9500-24Q	Cisco Catalyst 9500 Series Switches	17.9.5, 17.12.4
Cisco Wireless Controller	C9800-40-K9	Cisco Catalyst 9800 Wireless	17.9.6, 17.12.4

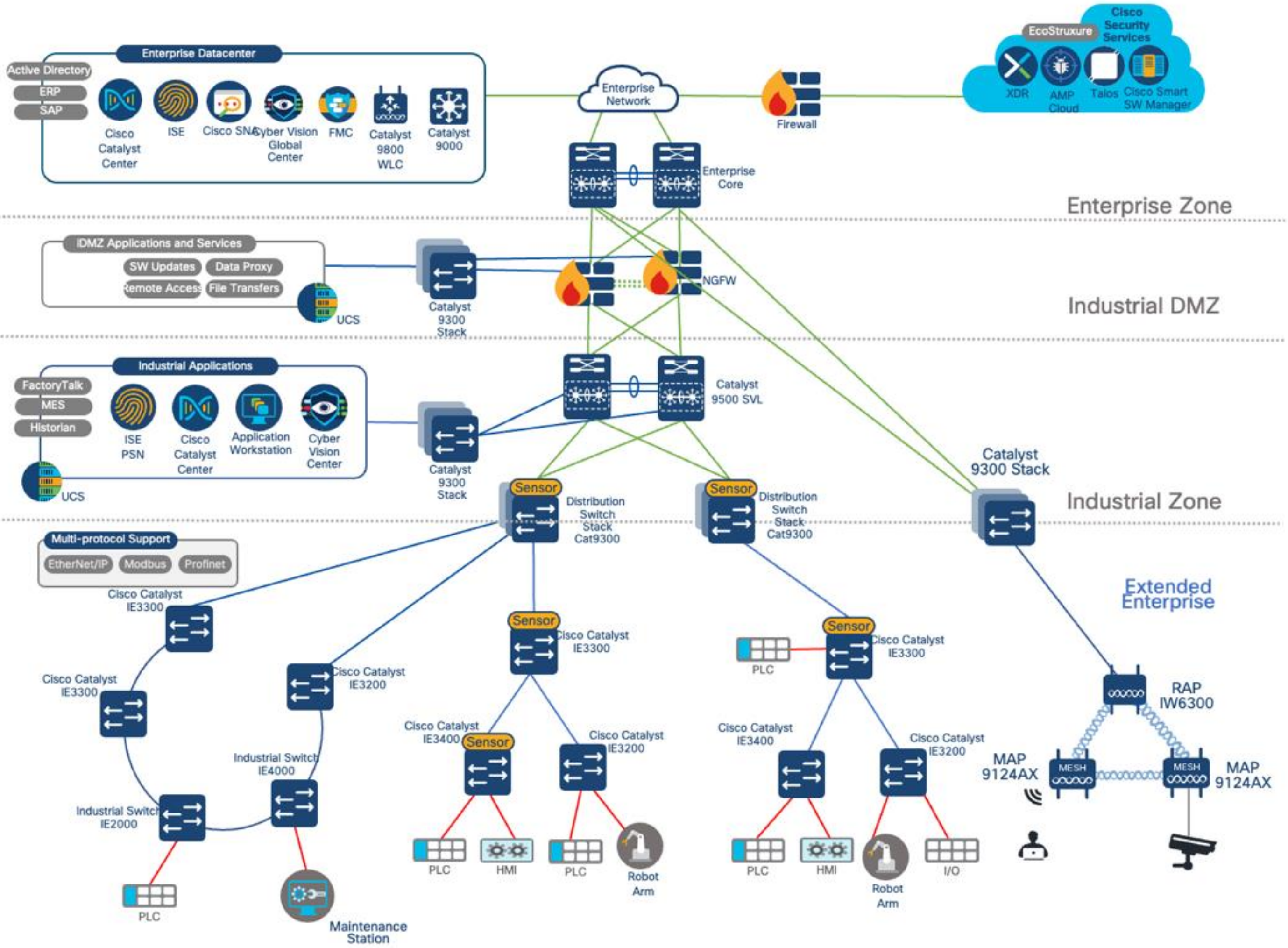
Role	Model Name	Hardware Platform	Software Version
		Controller	
Cisco Access Points	IW-6300H-AC-X-K9 9124AXI	Cisco Catalyst Access Points	17.12.4

The test topology includes the following Industrial Automation and Control Systems (IACS) devices.

Manufacturer	Role	Model
Rockwell Automation	Controller	LOGIX5318ER LOGIX5336ER LOGIX5336ER M LOGIX 5573 Safety LOGIX 5575
	I/O Device	A-B 1791ES-IB8XOBV4 IP20 8/
	Management Software	FactoryTalk Application
Siemens	Controller	S7 300 S7 1500 S7 414F-3 S7 400
	I/O Device	ET200M
	Hardware Module Interface (HMI)	TP 1200
	Management Software	TIA Engineering Workstation
Schneider Electric	Controller	BMEP583020 BMEP582020
	I/O Device	STBNIC2212 BMECRA31210
	Management Software	EcoStruxure Control Expert

Solution Topology

Figure 1.   Solution Topology



Solution Use Cases

Category	Function	Use Case
Network Automation	Day-zero and Day-n Provisioning	• Day-zero onboarding of IE switches using the Catalyst Center Plug and Play (PnP) feature. • Day-n provisioning of Cisco Catalyst switches in the distribution zone and the Cisco Catalyst IE devices in the cell or area zone.
	Resilient Ethernet Protocol (REP) Provisioning	• Nonfabric REP ring provisioning using Catalyst Center. • Day-n IE device additions or removal to the REP ring using Catalyst Center. • REP ring provisioning and segmentation using REP-ZTP with Catalyst Center as PnP server.
	Inventory Management	• Network device discovery by IP address using Catalyst Center. • OT and IT network device software upgrades using Catalyst Center. • Device replacement of IE switches using Catalyst Center. • Topological view of the OT network.
	Extended Enterprise (Wireless)	• Manage and provision wireless networks using Catalyst Center. • Perform day-n changes in the wireless network. • Bring up the wireless mesh network on the plant floor using Catalyst Center. • Deploy CLI templates using Catalyst Center to extend the wireless mesh to noncritical wired devices like IP cameras.
Security	Foundational Security (Industrial DMZ)	• IT and OT segregation using industrial DMZ with the help of Cisco NGFW Firepower devices.
	Cisco Cyber Vision	• Industrial visibility with the help of Cisco Cyber Vision and sensors. • Anomaly and threat detection using Cisco Cyber Vision. • Flow-based anomaly detection using Cisco Secure Network Analytics with hostgroup information enriched from Cisco Cyber Vision.
	Cisco TrustSec	• Segmentation with the help of Cisco TrustSec and policy control orchestrated from Catalyst Center. • Quarantine an industrial device on the plant floor using Cisco Cyber Vision and Cisco TrustSec.
Network Monitoring and Troubleshooting	Group-Based Policy Analytics	• Monitor the traffic flows between various security groups and refine the policy based on the traffic pattern.
	Assurance	• Monitor device, client, and network health using Catalyst Center Assurance. • Troubleshoot issues using guided steps provided by Catalyst Center. • Customize Assurance alerts for interesting events.
	AI Endpoint Analytics	• Unified view of IT and OT endpoints with industrial context enriched through Cisco Cyber Vision.
	Compliance	• Track the compliance of network devices and take appropriate actions to remediate the compliance issues.
	Audit Logs	• Track unauthorized access attempts and provisioning changes to Catalyst Center using the Audit Logs feature.

Category	Function	Use Case
High Availability	Network and Device Resiliency	• Device-level SSO with Cisco Catalyst stack switches and StackWise Virtual Link (SVL)-supported switches. • Layer 2 and Layer 3 redundant link failovers. • Catalyst Center 3-node HA failover along with Cisco ISE PAN or PSN failovers.

Scale Matrix

The solution is verified with the scale numbers listed in the following table. To view the scale numbers for the Catalyst Center appliance, see the Cisco Catalyst Center Data Sheet.

Variable	Scale
Controller device inventory	2000
Network devices per site	500
Zones(Area)	1000
VLANs	2000
Security Group Tag (SGT)	1000
Security Group ACL (SGACL)	500
Security	20,000 (15,000 wired, 5000 wireless)

The following table lists the validated scale profile for a cell/area zone.

Variable	Scale
Endpoints	500
Multicast Groups	200
REP ring size	18
Cisco Cyber Vision flows on Cisco Catalyst IE3400/IE3300 Switches	9600 pps
Cisco Cyber Vision flows on Cisco Catalyst 9300 Switches	12,000 pps

Solution Key Notes

The following sections describe technical notes that are useful for deploying the solution.

Network Automation

The following sections provide information on implementing features related to network automation.

Onboarding of New Switches Using Cisco Plug and Play

In a manufacturing plant, swift onboarding of new switches is important for seamless operations. The onboarding process must have the following key qualities:

- Fast: New switches should be onboarded quickly, ensuring operational readiness within minutes.
- Simple: Operators without a networking background should be able to execute the onboarding process.
- Scalable: The process can be replicated across hundreds of switches.
- Consistent: The process should adhere to the prescribed workflow and ensure uniform configuration and prevent human errors.

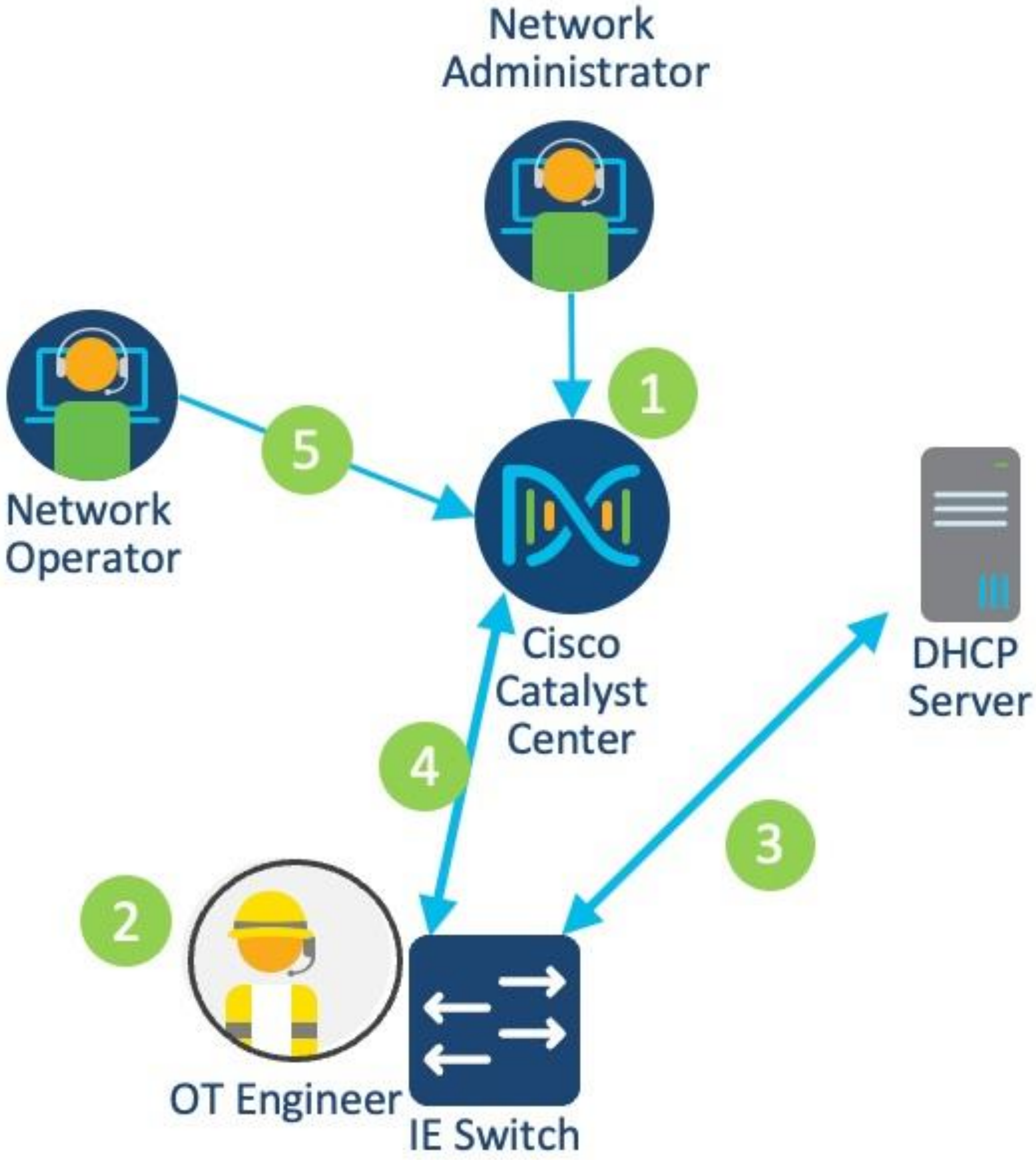
The Catalyst Center onboarding process uses zero-touch deployment through PnP. PnP facilitates the automated configuration of new, unconfigured devices within the network, using the network profile of the site. Sites group the devices based on physical location or function or both in a network.

For Cisco industrial switches running IOS or IOS-XE software, an embedded PnP agent communicates with the PnP deployment server. This PnP agent operates on devices without a startup configuration, such as those that are newly powered up or reset to factory defaults. It discovers the PnP deployment server through DHCP or DNS on Catalyst Center. The PnP agent initiates communication with the PnP server, downloading essential software and device configurations.

When an unconfigured device connects to the network and contacts Catalyst Center, Catalyst Center creates an entry for the device and places it in an unclaimed state until claimed by an administrator. Alternatively, you can add devices to Catalyst Center before installation by entering serial numbers and device families. After connecting these devices, they can be claimed to a designated site and configured with the predetermined software image and configuration based on the site settings.

The following figure shows the PnP provisioning workflow.

Figure 2. **PnP Provisioning Workflow**



The workflow includes the following key steps:

1. The network administrator creates a site hierarchy in Catalyst Center, configures site properties, adds provisioning templates, and defines golden images.
2. The OT engineer connects the industrial switch to the network and powers up the device.
3. The switch uses DHCP to obtain an IP address and discover the PnP server IP address (Catalyst Center).
4. The switch connects with Catalyst Center.

5. The operator claims the device on Catalyst Center. During the claiming process, Catalyst Center performs the following actions:
    - Installs the golden image.
    - Issues configuration, including licensing.
    - Adds the device to the Cisco ISE and Catalyst Center inventory.

Adding Configured Devices to Catalyst Center

While the PnP process offers an efficient approach to switch onboarding, certain scenarios may require alternative methods. For example:

- Offline new switch provisioning: In specific situations, switches require provisioning before they can connect to the network. This is especially relevant in industrial automation environments, where switches may need configuration before gaining network connectivity. As the PnP process relies on network connectivity for configuration, a different approach is needed for switches that are provisioned offline.
- Switch configured outside the manufacturing facility: In certain cases, system integrators configure switches before their arrival at the manufacturing facility. This practice streamlines the onboarding process, as switches arrive preconfigured and ready for immediate deployment.
- Brownfield deployment: *Brownfield* refers to devices integrated into existing sites with established configurations. When dealing with brownfield deployments, network devices are added to Catalyst Center using the Discovery feature.

Discovery Process

For the scenarios mentioned in the previous section, Catalyst Center uses the Discovery feature to add the network devices. The Discovery feature performs a scan of devices within the network and sends a list of discovered devices that is then seamlessly integrated into the device inventory.

Various methods can be employed for discovery, including IP address range, Cisco Discovery Protocol (CDP), or Link Layer Discovery Protocol (LLDP). For this CVP, IP address range was used. During a discovery task, you need to configure the CLI and SNMP Read credentials on Catalyst Center.

Site Assignment and Network Assurance

During device discovery, Catalyst Center provides an option to assign the device to a specific site. When you assign the device to a site, Catalyst Center pushes the telemetry configurations to provide network assurance to the newly added device.

Provisioning an REP Ring

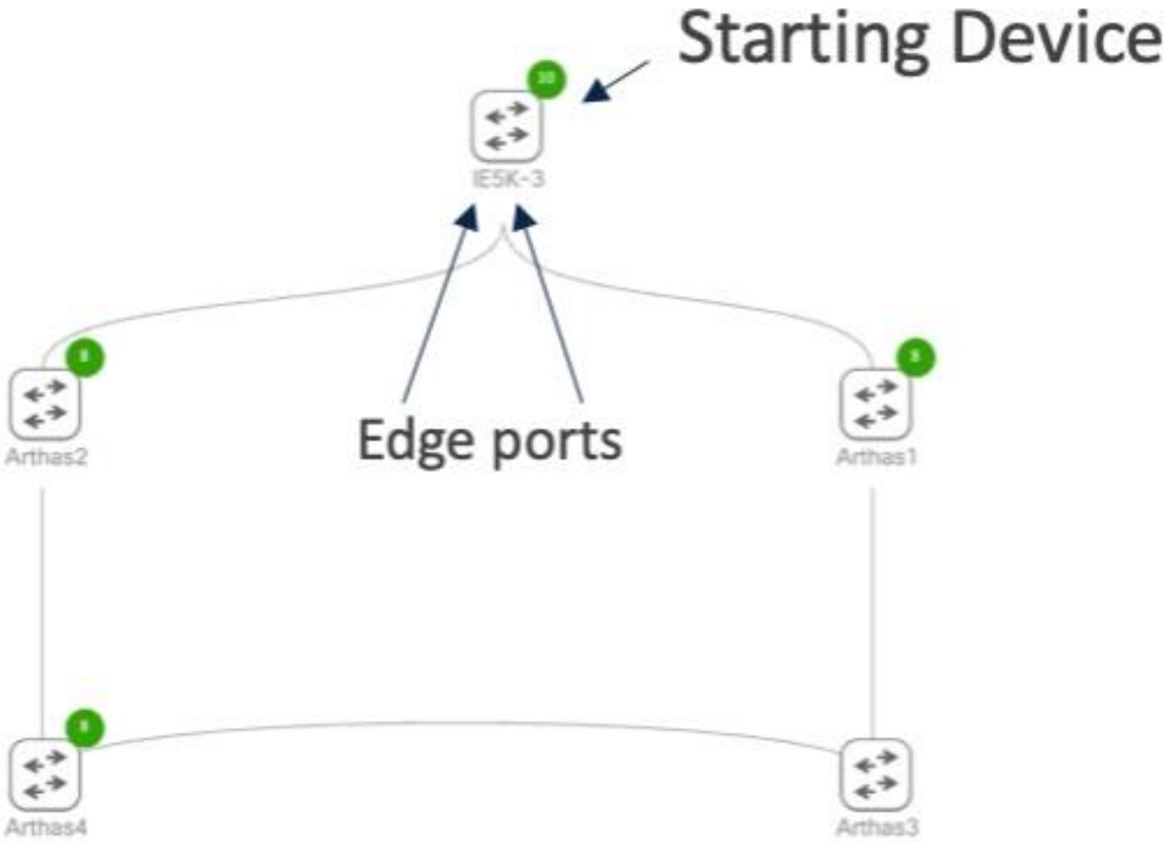
Industrial automation processes heavily rely on the availability and uptime of the IACS applications. To ensure the continuity of these systems, a resilient and robust network design is crucial. By implementing a LAN architecture that enhances the resilience and hardening of standard Ethernet and IP-converged IACS networking technologies, the Overall Equipment Effectiveness (OEE) can be improved, minimizing the impact of failures, and reducing the mean time to repair (MTTR).

A resilient design provides alternative paths in the event of equipment or link failure. Within the cell/area zone, network redundancy is achieved by using a star or ring topology for uplinks from the edge switching platforms. To prevent loops within redundant links, a resiliency protocol needs to be deployed. Resilient Ethernet Protocol (REP) is an example protocol that prevents looping within a ring topology.

REP is a Cisco proprietary protocol that offers an alternative to Spanning Tree Protocol (STP) for controlling network loops, handling link or node failures, and avoiding convergence time. It operates a single redundancy instance per segment or physical ring. A REP segment consists of ports connected to each other with a unique segment ID. Each segment includes standard segment ports and two user-configured edge ports. The network segment terminates at a neighboring Cisco IE access switch or distribution switch, with the terminating port referred to as the edge port. Loop prevention within the ring is maintained by blocking one port in the segment, known as the alternate port. In the event of a segment failure, the alternate port transitions to a forwarding state, allowing traffic to flow through the alternate path, bypassing the network failure.

To learn more about resiliency protocols in industrial automation, see Networking and Security in Industrial Automation Environments Design and Implementation Guide.

Figure 3. Catalyst Center Topology View



Note: This workflow causes an outage during STP to REP conversion.

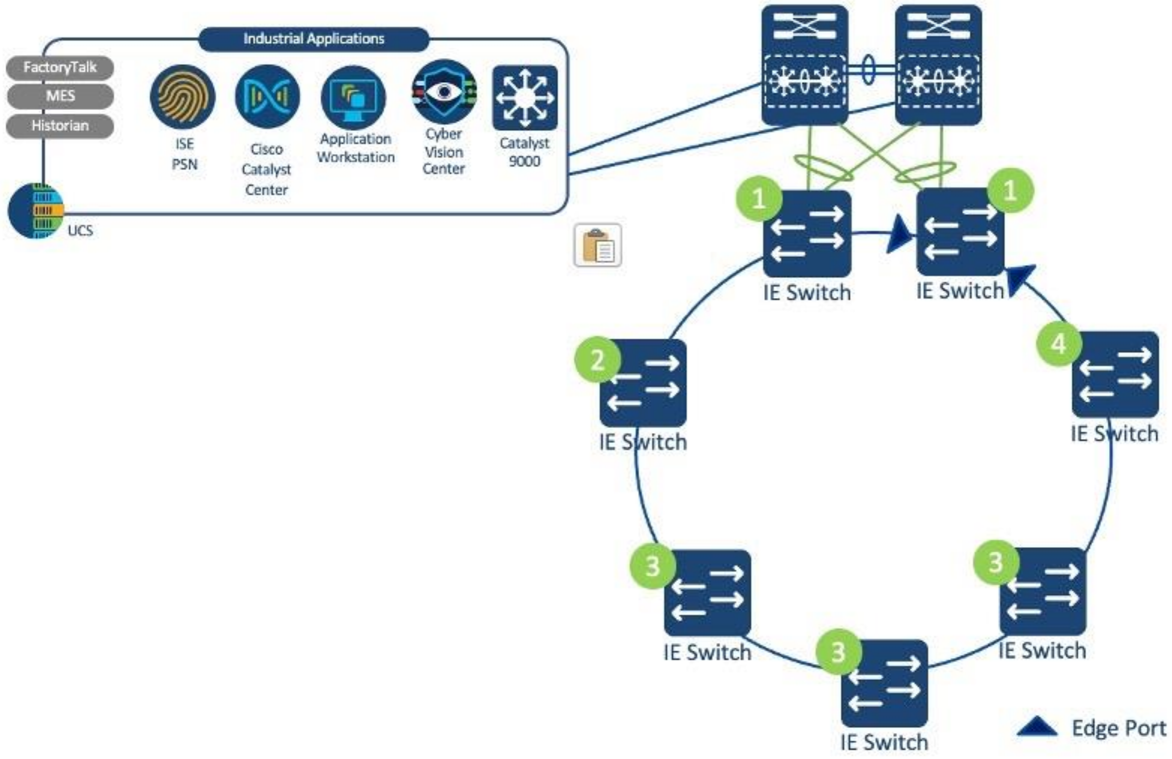
The Catalyst Center REP automation workflow creates a complete REP ring and does support configuration of open REP segments. Before starting the workflow, the links on the ring need to be configured as trunks. By default, the REP ring workflow supports up to 18 devices. Dynamic addition and removal of REP nodes is also supported. The following steps show how to add an additional node to the ring using an unconfigured switch after creating an REP ring using the workflow. For REP ring provisioning, see the Cisco Catalyst Center User Guide.

1. Manually configure or use Catalyst Center templates to push the PnP startup VLAN and DHCP pool configuration to the ring switches.
2. Shut the adjacent interfaces where the new node will be inserted, and ensure that the rep segment <#> command is applied to the interfaces to enable REP and assign segment ID to the interfaces.
3. Configure the rep ztp-enable command on the adjacent interfaces to enable REP ZTP.
4. Connect the new device and unshut the adjacent interfaces. The new node undergoes the PnP process.
5. Claim the new device, ensuring it is added to the same site as the existing REP ring. Catalyst Center automatically adds REP to the relevant interfaces on the new node.

REP ZTP

The Catalyst Center REP workflow mandates the presence of an STP ring comprising switches that are provisioned and managed by Catalyst Center before initiating the workflow. Alternatively, the industrial switches offer an REP ZTP feature as an option. REP ZTP facilitates the provisioning of switches directly into the REP ring through the PnP process. In standard operational scenarios, an REP interface remains traffic-inactive until establishing a REP adjacency with a neighboring switch. REP ZTP, however, deviates from this norm, enabling PnP messages to traverse an REP interface connected to an unconfigured switch. This allows the unconfigured switch to receive its complete configuration, including REP settings on the port. The PnP process enables the switch to seamlessly join an REP segment and transition into regular operational mode.

Figure 4. REP ZTP Provisioning Workflow



The REP ZTP provisioning workflow progresses as follows:

1. The first switch or switches in the ring are provisioned, and these switches have uplinks that are not part of the REP ring. The ring interfaces need to be configured with the REP segment. REP ZTP should be enabled globally and configured on the ring interfaces.
2. A new industrial switch is connected to an REP interface. The upstream switch allows DHCP and PnP flows so the new switch can be configured. The onboarding template pushed to the device contains the REP configuration. After the PnP process is completed, the switch participates in regular REP operation.
3. Additional switches are connected downstream, one at a time. Step 2 is repeated for every new switch.
4. When the last switch is connected, it starts the PnP process on only one of its interfaces. The switch gets provisioned as described in Step 2 and the REP ring is now operational.

For more information on the REP ZTP feature, including hardware and software support, see Redundancy Protocol Configuration Guide.

REP ZTP Versus REP Ring (Nonfabric) Workflow

The following table compares the two REP automation options.

Catalyst Center REP Workflow	REP ZTP
Requires an existing STP ring and switches managed by Catalyst Center and is suitable for existing rings that need to be converted.	Requires new or unconfigured switches and is suitable for new REP segments.
Supports wizard-based approach and doesn't require templates for REP configuration.	Requires templates.
Supports REP rings only (closed segments).	Supports open REP segments.
Supports addition and deletion of nodes.	Supports addition and deletion of nodes.
Causes an outage when migrating from STP to REP.	Doesn't cause any outage after the devices are onboarded.
Catalyst Center displays REP topology in the **Inventory** > **Device Details** window	Catalyst Center does not display REP topology in the **Inventory** > **Device Details** window. It is available through the CLI only.

Software Image Management (SWIM)

The Catalyst Center SWIM functionality offers centralized control over software management for network devices, for both IT and OT domains.

The following features make SWIM a valuable tool for efficient and reliable software image management in manufacturing deployments:

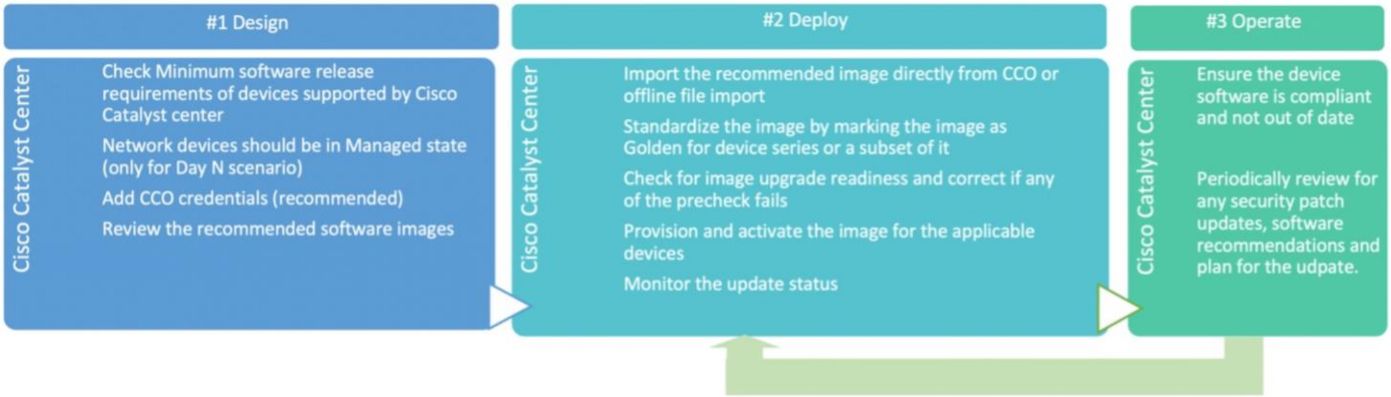
- Compliance: SWIM ensures image compliance by verifying that all devices are operating on the correct version as identified by administrators, who can designate a specific version as the golden image. Catalyst Center flags the devices that are not running the preferred version. In addition to ensuring image compliance, SWIM also aids in the identification of security advisories associated with the software version that are in use and an option to address these security advisories, helping to enhance network security and mitigate potential vulnerabilities.
- Upgrade at scale: A crucial capability when dealing with the extensive array of network devices typically found in a manufacturing deployment.

- Prechecks and post checks: The software upgrade process incorporates a predefined set of prechecks and post checks to assess device health before and after the upgrade. These checks can be customized and used to fit the manufacturing network, to ensure that there is no adverse impact post upgrade. For instance, a customized post check validating the Cyber Vision Sensor status.
- Flexible upgrades: In a manufacturing deployment it's imperative to schedule updates during nonpeak hours to minimize disruption. SWIM provides the flexibility to plan and execute updates at a user-defined date and time. Furthermore, SWIM provides the flexibility to segregate the distribution and activation of the software image into two separate time periods. This approach allows for the staging of the golden image on devices before the actual activation, resulting in a significant reduction in the overall upgrade duration.

For more information on how to use the SWIM features with Catalyst Center, see the Cisco Catalyst Center User Guide.

The following figure outlines a typical Catalyst Center SWIM workflow.

Figure 5. **SWIM Workflow**



Check Minimum software release requirements of devices supported by Cisco Catalyst center

Network devices should be in Managed state (only for Day N scenario)

Add CCO credentials (recommended)

Review the recommended software images

Import the recommended image directly from CCO or offline file import

Standardize the image by marking the image as Golden for device series or a subset of it

Check for image upgrade readiness and correct if any of the precheck fails

Provision and activate the image for the applicable devices

Monitor the update status

Ensure the device software is compliant and not out of date

Periodically review for any security patch updates, software recommendations and plan for the udpate.

Note: SWIM uses internal flash memory for upgrades. To use SWIM to upgrade a switch running from an SD card, reconfigure to boot from internal flash.

For Cisco Industrial Ethernet (IE) switches running Cisco IOS XE Release 17.9.x or earlier, if an SD flash memory module (SD card) is present, ensure that there are no images on the card. Otherwise, software maintenance updates (SMUs) and SWIM will not work. In this scenario, configure the switch to use internal flash memory as the primary boot device.

Wireless Mesh Network

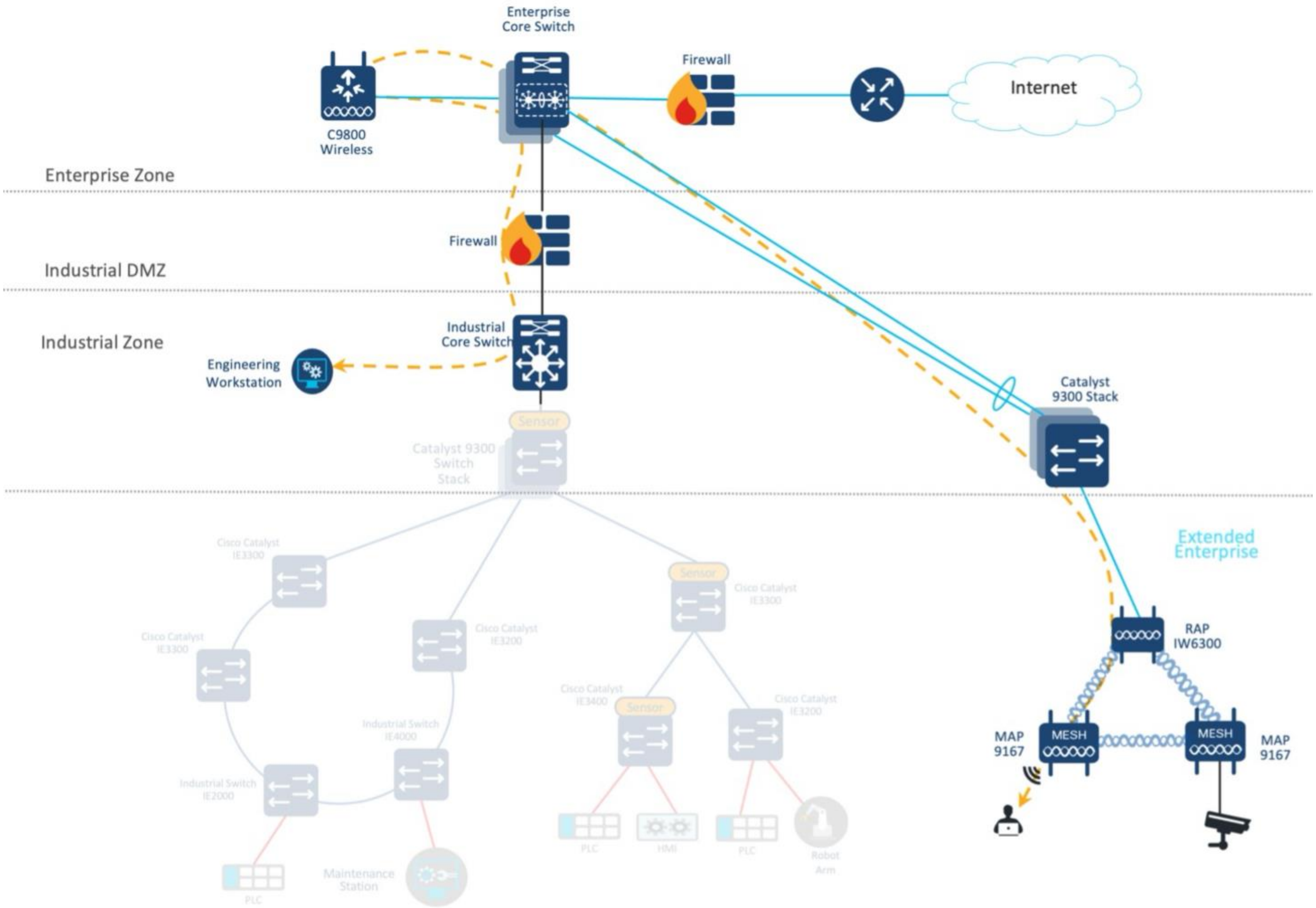
Manufacturing facilities often include expansive spaces characterized by intricate layouts. Wireless mesh networks expand coverage through the interconnection of access points, providing a robust wireless signal strength in remote corners of the establishment. Installing Ethernet cables throughout a manufacturing plant can be challenging due to the physical barriers, machinery, and other logistical limitations. In this context, wireless mesh networks avoid extensive cabling, resulting in expedited and more economical deployment. Mesh networks also provide redundancy by affording multiple data transmission pathways. If one route becomes inaccessible due to interference or device malfunction, the network adeptly redirects traffic through alternative pathways, thus upholding consistent and dependable connectivity.

The Cisco wireless mesh network solution facilitates the cost-effective and scalable deployment of secure wireless LAN. This provides access to both fixed and mobile applications, resulting in heightened safety, efficiency, productivity, and responsiveness. Its seamless integration within the Cisco Unified Wireless Network architecture establishes it as the natural choice for customers aiming to extend their enterprise WLAN coverage to manufacturing plant floors.

The network automation capabilities of Catalyst Center plays a crucial role in enabling the full functionality of the wireless mesh network. Moreover, the network performance can be efficiently tracked using the advanced monitoring feature offered by Cisco Catalyst Assurance. The Mesh Access Points (MAP) undergo secure onboarding facilitated by using a MAC address list. This list can be integrated effortlessly into the AP authorization list within Catalyst Center, through a CSV upload process. For more information on how to bring up a mesh network using Catalyst Center, see the Cisco Catalyst Center User Guide.

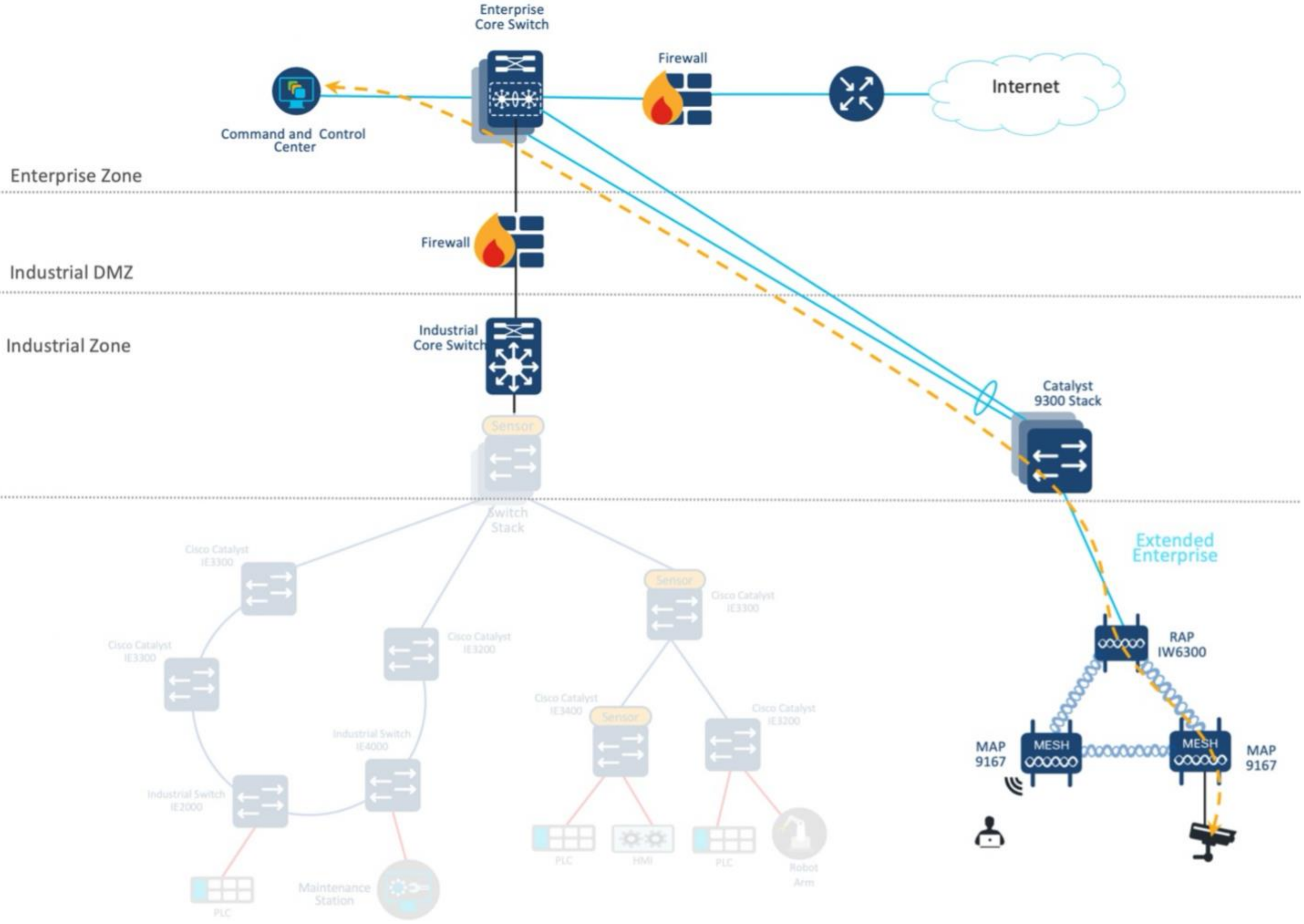
The following figure shows how the floor operations manager accesses the engineering workstation within the industrial zone through the extended enterprise Wi-Fi network.

Figure 6. Extended Enterprise Wi-Fi Network



Wireless mesh network can be extended to other multiservices supporting the plant operations and communications. Within the plant floor, there could exist devices falling into the category of noncritical, multiservice units. Despite their noncritical nature, these units such as security badge access, video surveillance, and telephony require wired network connectivity. Fortunately, these devices can smoothly become part of the wireless mesh network using an Ethernet bridging solution for integration. The following figure shows how the IP cameras are connected to the wired Ethernet port of the mesh AP sending the feed to the command and control center in the industrial zone.

Figure 7. **Extended Enterprise Wi-Fi Network Support for Multiservices**



Catalyst Center does not yet support intent-based network automation to enable the Ethernet bridging solution. For this profile validation, Catalyst Center CLI templates are used to enable the required configurations. For enabling the Ethernet bridging solution in Cisco Catalyst 9800 Wireless Controllers, see Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide.

Security

The following sections provide information on implementing features related to network security.

Operational Technology Network Visibility with Cisco Cyber Vision

Lack of visibility is a common challenge on industrial networks. As these networks can be quite old, widely dispersed, and involve many contractors, operators often do not have an accurate inventory of what is on the network.

Without this, they have limited ability to build a secure communications architecture. A lack of visibility also means that operators are often unaware of which devices are communicating with each other or even of communications reaching industrial devices from the outside. The lack of visibility ultimately leads to a lack of segmentation or control.

OT visibility is a technology that all personas in OT environments can use. OT operators gain the benefit of process level visibility to identify and troubleshoot assets residing on the plant floor. IT operators gain insight into device communication patterns to improve network efficiency. Security teams gain insight into device vulnerabilities and deviations from normal device behaviors. Visibility is important to:

- Identify all assets and group them into zones.
- Visualize data that flows through the conduits between zones.
- Give a clear view of which source data is coming in through external networks.

Cisco Cyber Vision addresses the visibility needs of industrial networks. It is built on a unique edge architecture comprising multiple sensor devices that perform deep packet inspection, protocol analysis, and intrusion detection within the industrial network. The Cyber Vision Center serves as an aggregation platform, storing data from the sensors and offering a user interface, analytics, behavioral analysis, reporting, APIs, and more. For more information on Cisco Cyber Vision in industrial automation networks, see Industrial Automation Security Design Guide 2.0.

Cisco Cyber Vision Sensors are deployed in switches managed by Catalyst Center. It is possible to use templates to prepare the industrial switch for sensor installation via Catalyst Center.

Segmentation Using Cisco TrustSec

Segmentation plays a crucial role in creating zones of trust to protect IACS networks and processes. IEC 62443 provides recommendations on restricted data flow to segment the control system into zones and conduits, limiting the unnecessary flow of data between process networks or services. This helps prevent unintentional or accidental cross-pollination of traffic between untrusted entities. The industrial security solution offers basic guidance on logical isolation for segmenting cell/area zone traffic.

The security journey in the industrial automation architecture begins by segmenting the enterprise network and the OT network, which can be achieved through the implementation of an IDMZ. IDMZ provides a secure boundary between the enterprise and OT networks, ensuring controlled access and protecting critical assets. For more information on IDMZ, see Securely Traversing IACS Data across the IDMZ Using Cisco Firepower Threat Defense.

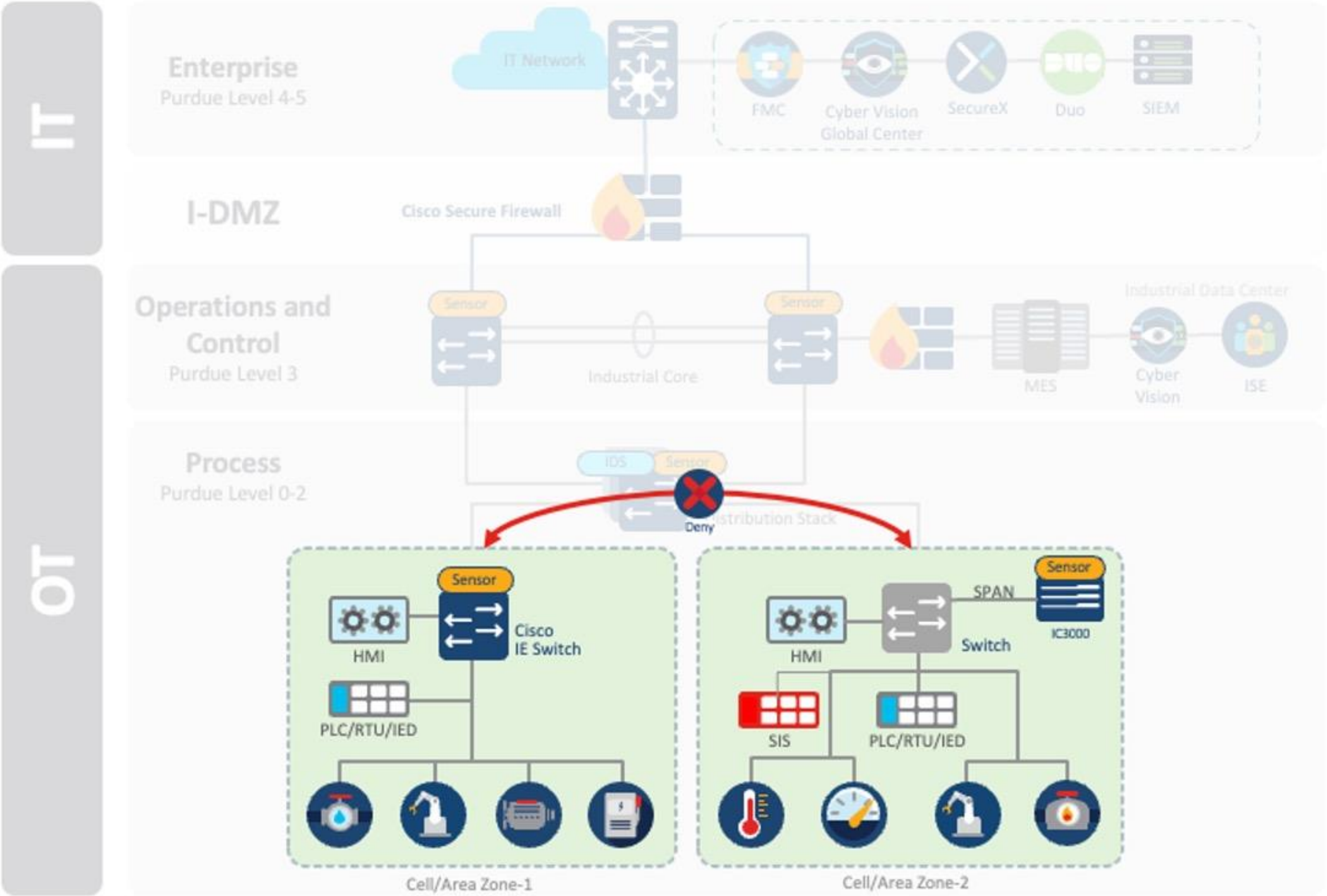
Intent-based security empowers administrators to express their operational intent and automatically select the appropriate security policies defined by IT, without the need for specialized network or security skills.

When Catalyst Center is integrated with Cisco ISE, it enables intent-based security using Cisco TrustSec. Cisco TrustSec uses SGTs to apply policies to groups of users or device profiles. These policies are customized for each organization's deployment.

In an industrial network, there are various common use cases and personas that require secure access, including:

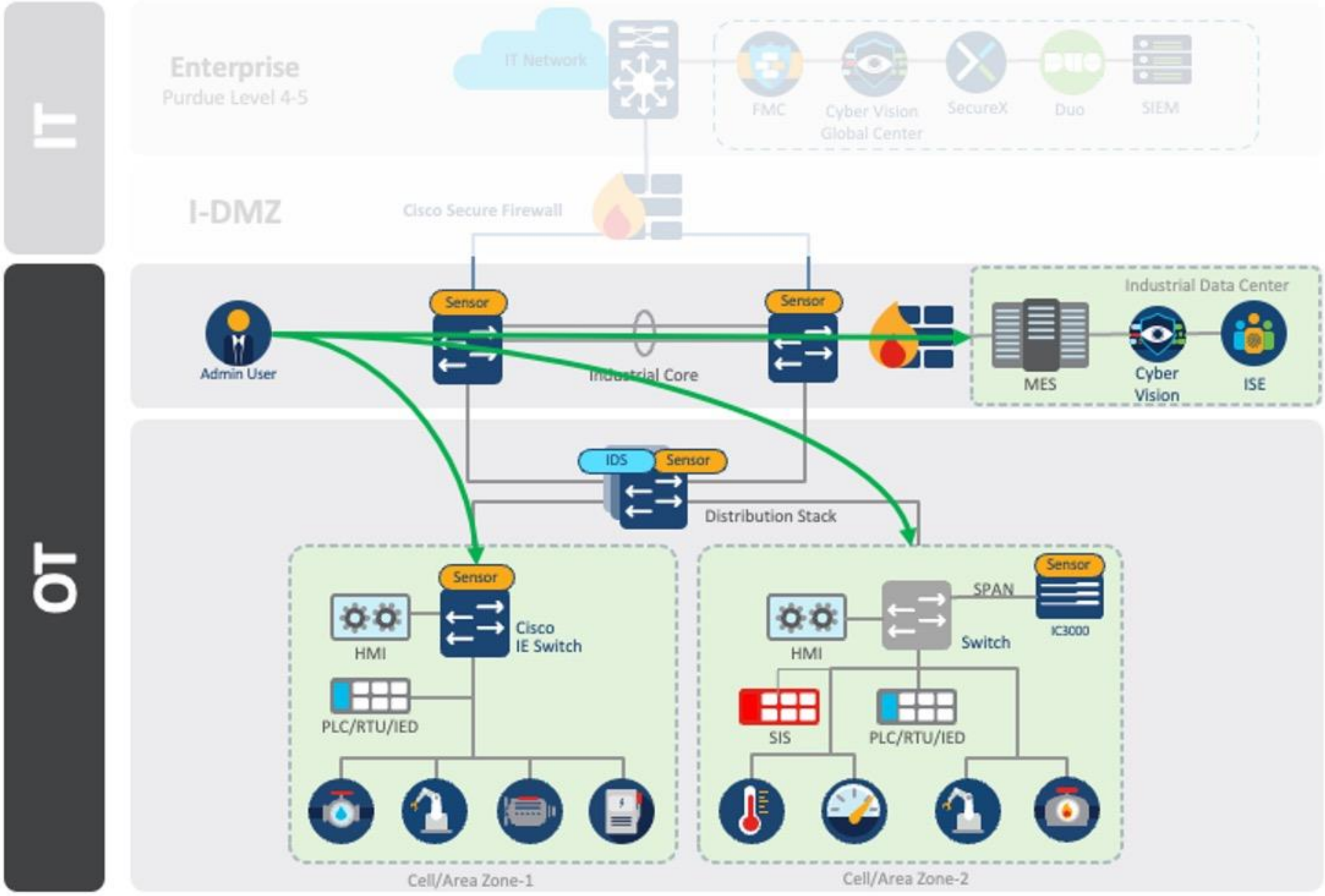
- Cell/Area Zone: This zone consists of multiple cell/area zones where devices within the same zone should have unrestricted communication. However, communication between different zones should be denied by default unless explicitly allowed.

Figure 8. Inter-Cell/Area Zone Segmentation - Denied by Default



- Administrative Users: These users need access to all zones within the network for tasks such as network infrastructure configuration or control logic application. While these user's access should not be limited, their data should be protected.

Figure 9. Administrative Access Permitted with Segmentation



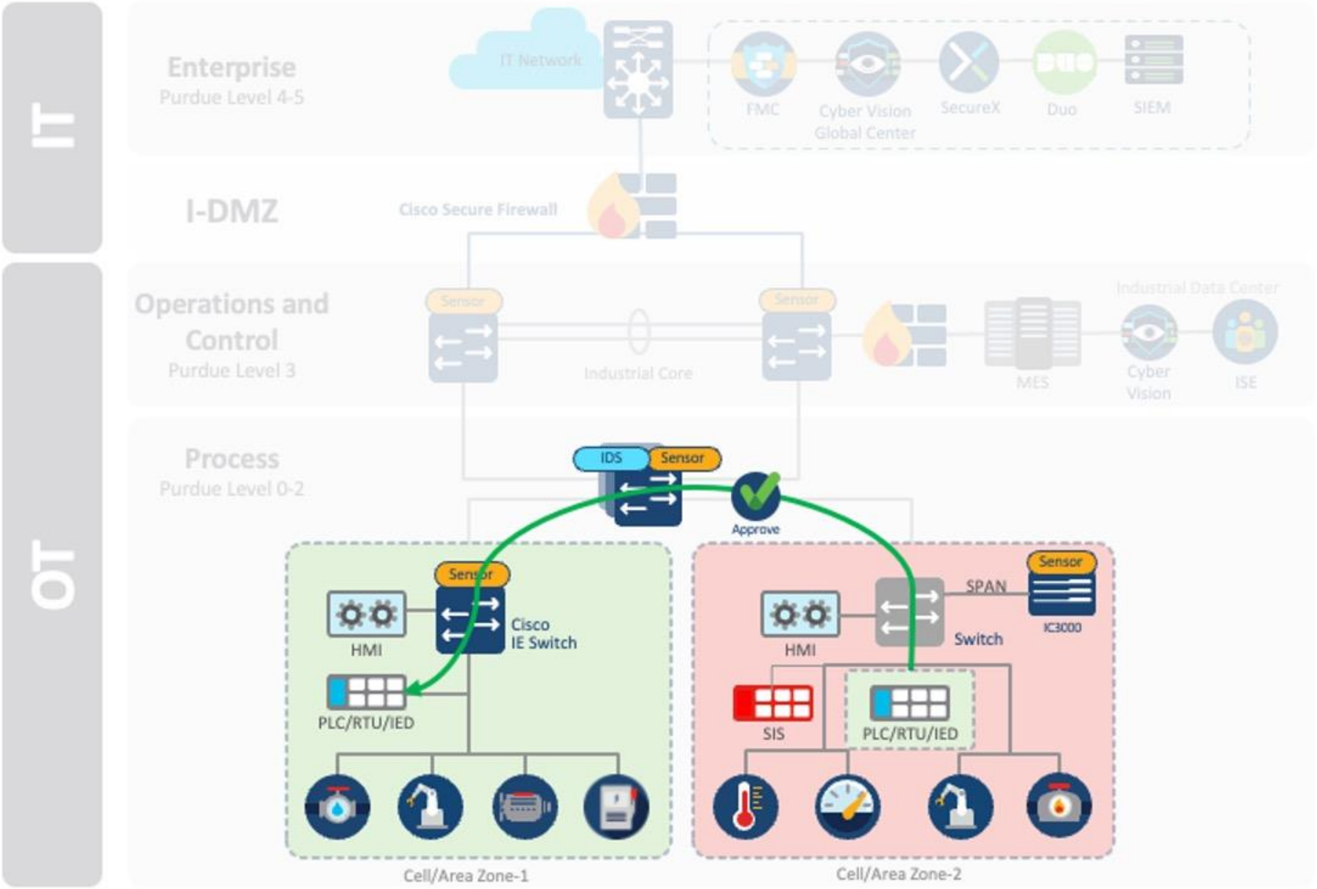
- Infrastructure Services: Endpoints that do not have user presence but require access to a significant portion of the plant, such as DHCP, NTP, or LDAP services.

- Plantwide Applications: Applications within the industrial data center (IDC) with specific access requirements, such as analytics platforms or vendor tools, used for monitoring and maintaining plant floor equipment.

- Maintenance Workstations: These workstations may reside either outside the cell/area zone and act as the maintenance machine for select zones or within the cell/area zone itself but require more privileges when leaving the zone.

- Interlocking Programmable Logic Controllers (PLC) or Interzone Communication: Some industrial communications may need to traverse zones for distributed automation functions. However, strict privilege policies should be applied to ensure that only valid communication is permitted to prevent the spread of malware.

Figure 10. Inter-Cell/Area Zone Communication Permitted for Interlocking PLCs



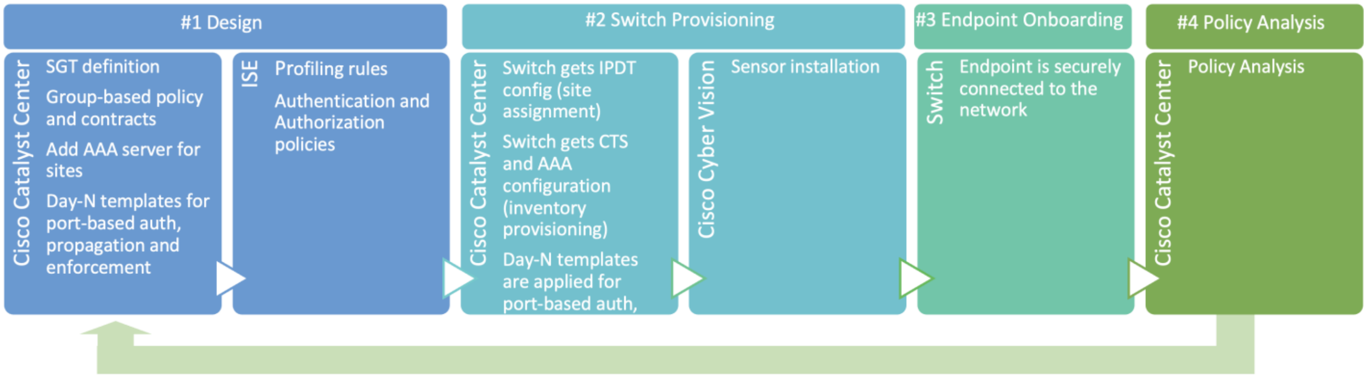
- Convenience Port: Operators who directly plug into the infrastructure may bypass security checks implemented in higher architectural layers. Ensure that only authorized users with authorized device posture can connect to the network helps secure this use case.
- Safety Networks: Safety Instrumented Systems (SIS) are critical to the control network and should either be air-gapped or logically segmented to prevent data leakage into this zone.
- Remote Users: Remote access is commonly granted to employees, partners, and vendors for maintenance, process optimization, and troubleshooting. Access should be restricted to select devices on the plant floor for a limited time.

The first step in deploying segmentation with Cisco TrustSec is to define security design such as tag propagation methods and enforcement points. Also, if you are using Cisco Cyber Vision Center, sensor placement for effective visibility should be decided beforehand.

For information on design, see Industrial Automation Security Design Guide 2.0. Catalyst Center supports the application of policies by providing the necessary tools and functionalities.

The security workflow shown in the following figure showcases how Catalyst Center plays an important role when deploying Cisco TrustSec.

Figure 11. Security Workflow


#1 Design
Cisco Catalyst Center
SGT definition
Group-based policy and contracts
Add AAA server for sites
Day-N templates for port-based auth, propagation and enforcement
ISE
Profiling rules
Authentication and Authorization policies
#2 Switch Provisioning
Cisco Catalyst Center
Switch gets IPDT config (site assignment)
Switch gets CTS and AAA configuration (inventory provisioning)
Day-N templates are applied for port-based auth,
Cisco Cyber Vision
Sensor installation
#3 Endpoint Onboarding
Switch
Endpoint is securely connected to the network
#4 Policy Analysis
Cisco Catalyst Center
Policy Analysis

The security workflow shows the following stages:

Step 1. Design activities refers to configurations based on security design. These configurations can be done before any network device or endpoints are onboarded. Catalyst Center is used to define Cisco TrustSec policy, settings, and templates that will be pushed into network devices.

Step 2. Switch provisioning refers to the action of onboarding a switch into the network. In this stage, settings are pushed to the device as defined in Phase 1.

Step 3. Endpoints can be securely connected to the network and start communicating as allowed by policy.

Step 4. Policy Analysis is done to understand communication patterns and refine policy. Policy Analytics is a feature on Catalyst Center that discovers activities between endpoints, groups, and applications. Policy analysis is discussed in the Group-Based Policy Analytics section.

Cisco Cyber Vision Usage to Quarantine Device to a Zone using Cisco TrustSec

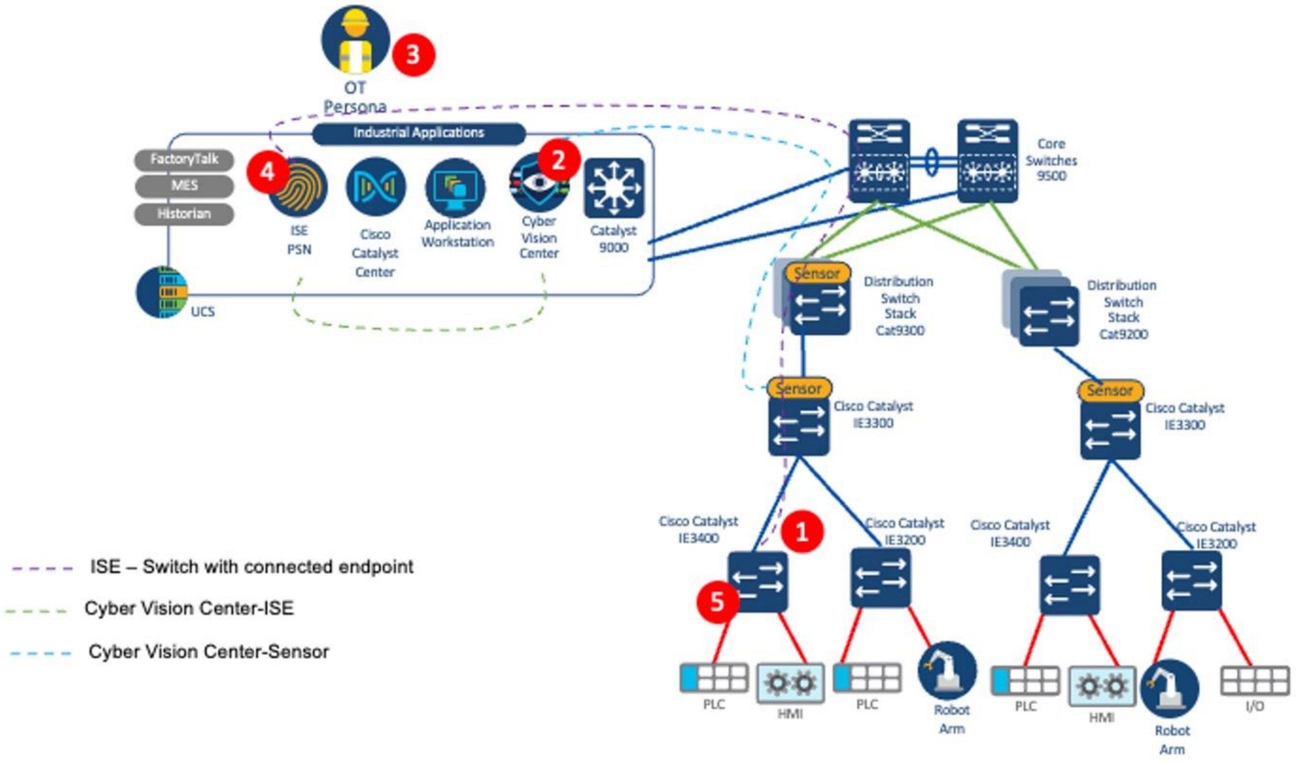
In Cisco Cyber Vision, vulnerabilities are detected using rules stored in a Cyber Vision Knowledge Database (DB). These rules are sourced from various reputable entities such as CERTs (Computer Emergency Response Teams), manufacturers, and partner manufacturers. The detection of vulnerabilities is achieved through the correlation of these Knowledge DB rules with normalized device and component properties. When a device or component matches a rule within the Knowledge DB, a vulnerability is identified. If a device is found to have a critical vulnerability or is compromised in any way, the operator has the ability to assign that device to a quarantine group in Cisco Cyber Vision. Later, this information is communicated to Cisco ISE, which then assigns a new SGT to the device. This new SGT restricts the device's communication until the necessary patches or remediation measures are applied.

The workflow is as follows:

1. A device is connected to the network. The Cisco Cyber Vision Sensor discovers the device and sends information to Cisco Cyber Vision Center.
2. If the device characteristics match a rule, Cisco Cyber Vision Knowledge DB raises a vulnerability alert on the device.
3. The OT engineer reviews the recommended action, but it cannot be deployed immediately because it can cause downtime. The OT engineer assigns the device to a quarantine group on Cisco Cyber Vision Center.
4. Cisco Cyber Vision Center sends this information to Cisco ISE via pxGrid. Cisco ISE profiles the device with the new context.

5. Cisco ISE sends a change of authorization to the switch connected to the device which results in a new SGT assignment.

Figure 12. Cyber Vision to Cisco ISE TrustSec Workflow



Unified Security Operations Center Empowered by Insights from the Industrial Network

Given the increased interconnectedness of operational networks and their vulnerability to cyber threats, administrators of industrial networks can tap into the expertise of their organization's information security teams. By establishing collaborative workflows, they can effectively counter these attacks. In this context, you can explore a scenario involving the identification of anomalies within the Site Operations Center (SOC) on the plant floor. This is achieved through the Cisco Secure Network Analytics flow-based anomaly detection capability, complemented by the contextual insights provided by Cisco Cyber Vision Center about the manufacturing network. This collaborative endeavor facilitates a comprehensive perspective on security incidents, streamlining the process of investigation and remediation.

The following steps describe the workflow for detection of malware in cell/area zone and Level 3 operations:

1. East-West communication between PLCs across the zones, and North-South communication between the Engineering workstation in Site operations center and a PLC in a cell area are the allowed flows.

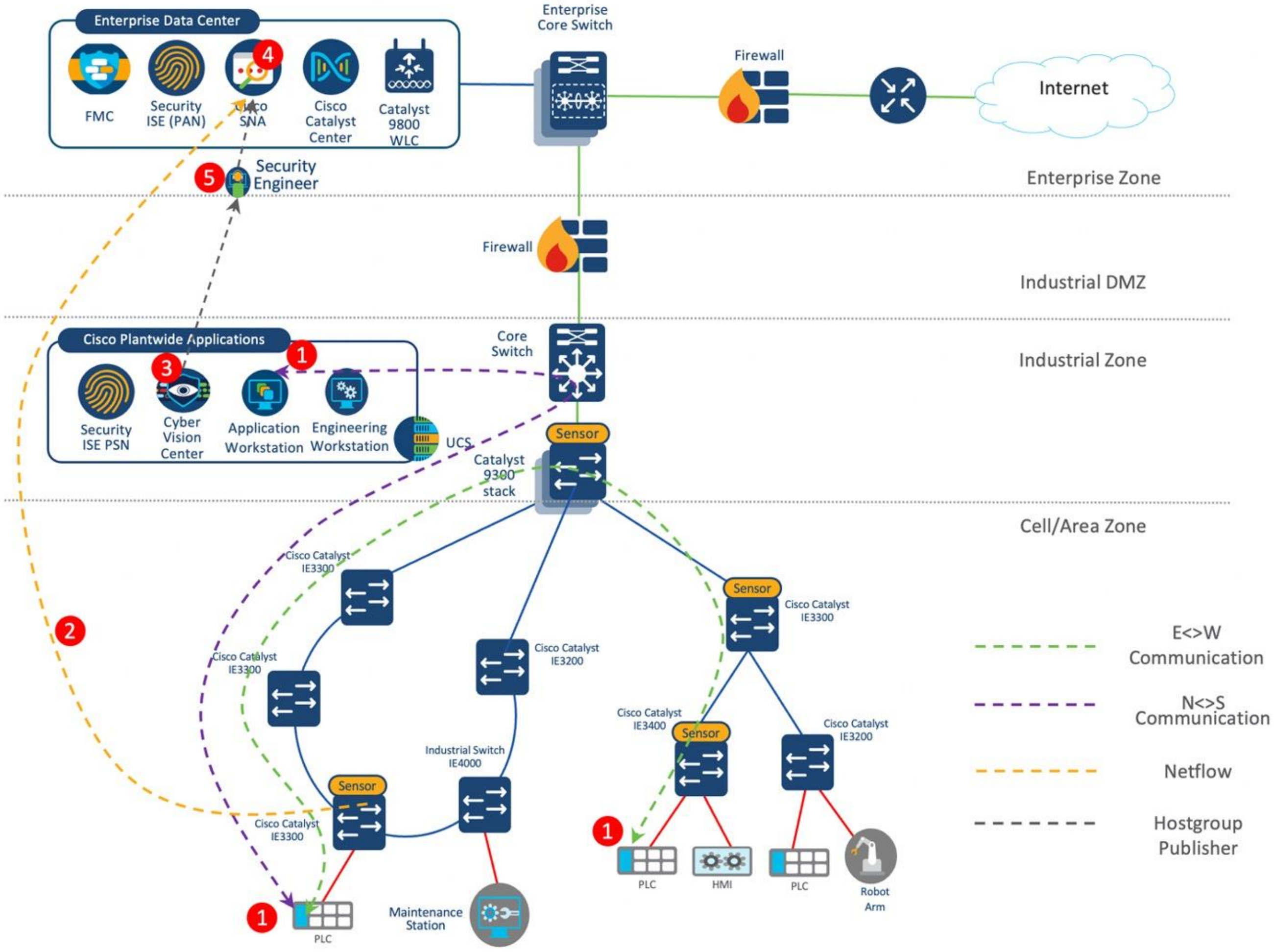
2. The IE switches are enabled with NetFlow to send NetFlow records to the Secure Network Analytics Flow Collector.

3. Cisco Cyber Vision in the industrial zone does a deep packet inspection (DPI) of industrial protocols based on passive monitoring using the Cisco Cyber Vision sensor deployed at various IE devices. These insights from Cisco Cyber Vision add context to the network flows that Cisco Secure Network Analytics monitors.

4. The Secure Network Analytics Manager runs its pre-built algorithms based on the data from the flow collector and reports an alarm indicating the malicious activity occurring in the network flows identified above.

5. The IT security architect reacts to the alert by strategizing the subsequent steps of remediation, which could include conducting more investigation, imposing limitations on the access of the IACS asset, and similar measures.

Figure 13. Cisco Cyber Vision to Secure Network Analytics Malware Detection Workflow



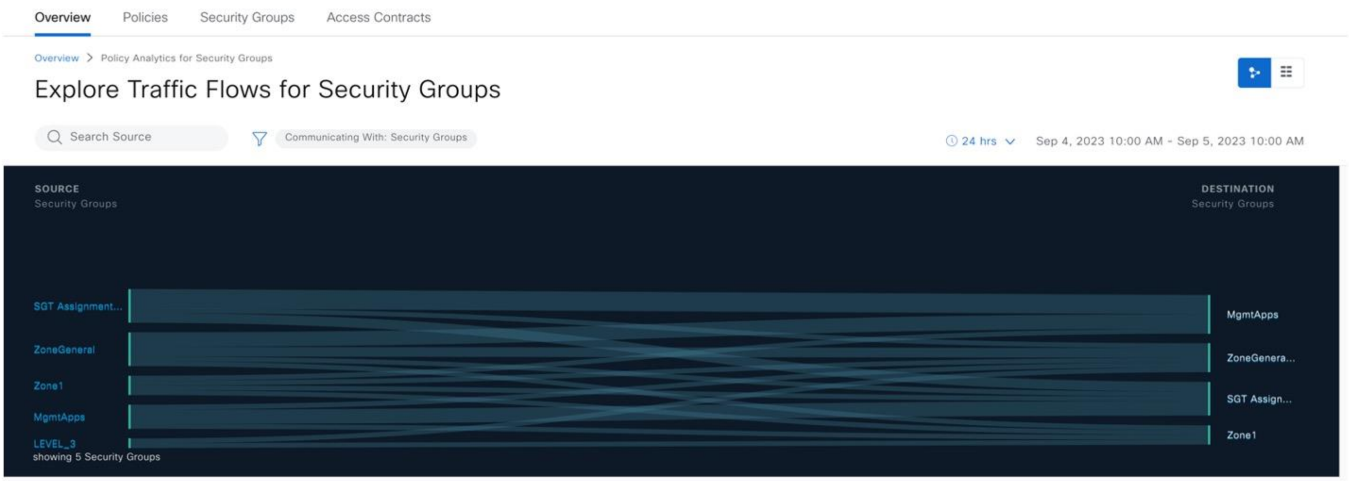
Network Monitoring and Troubleshooting

The following sections provide information on implementing features related to network monitoring and troubleshooting.

Group-Based Policy Analytics

Segmentation plays a vital role in establishing trust zones, thereby enhancing the safeguarding of IACS networks and operations. Employing controlled data movement to divide the control system into distinct zones and pathways is a widely accepted practice. This division minimizes the superfluous exchange of data among various process networks or services. It's imperative to curtail any inadvertent or deliberate exchange of information between untrusted entities. The Group-Based Policy Analytics feature in Catalyst Center aids visibility into communication patterns among different security groups within the cell/zone area of the plant floor. This improved visibility proves valuable in refining the enforcement rules that govern these SGTs. Specifically, the Group-based policy analytics can provide precise insights into the communication details at the protocol and port levels among these groups. This functionality serves as an initial alert mechanism, aiding in the early identification of unintended communications occurring between these groups.

Figure 14. Security Group Policy Analytics



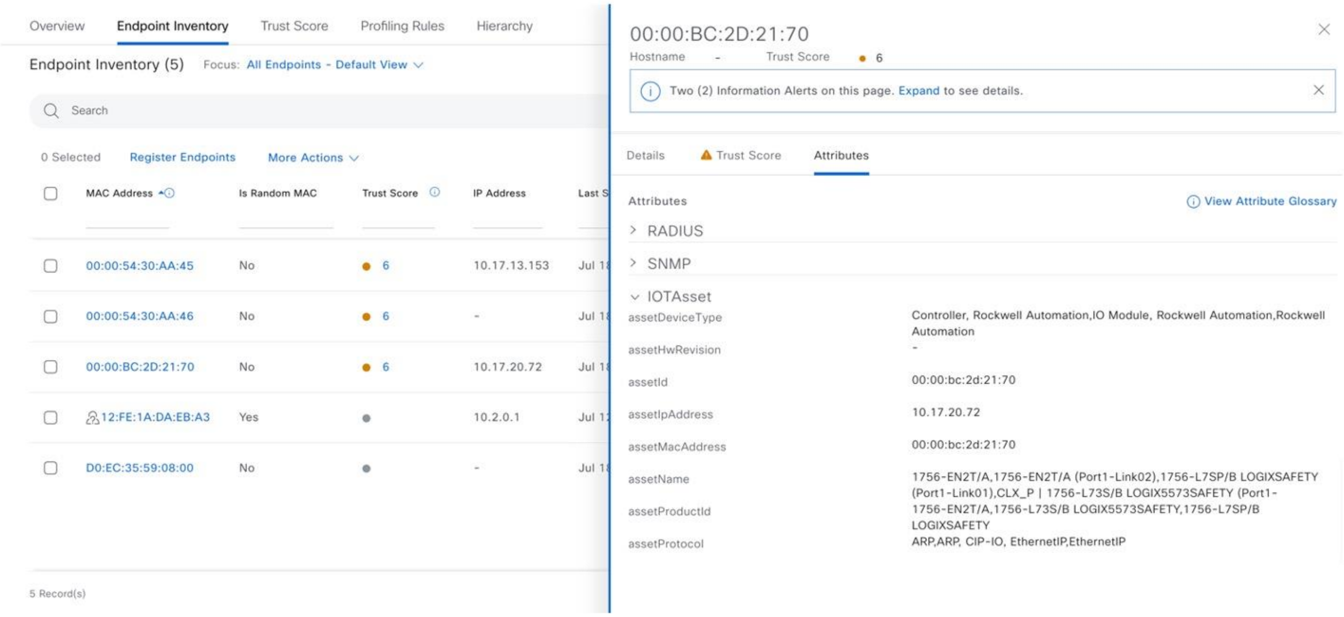
AI Endpoint Analytics

Gaining visibility stands as the initial stride in fortifying endpoint security. Delving profoundly into the endpoint and categorizing it through a multitude of factors becomes pivotal. This process aids in grouping the endpoints and then formulating precise security policies that are constructed upon the amassed visibility.

Cisco AI Endpoint Analytics represents an application within Catalyst Center, designed to identify and categorize endpoints through the assignment of distinct labels. This approach is referred to as Multi-Factor Classification (MFC), involving the allocation of multiple labels to individual endpoints. The AI-driven endpoint analytics engine acquires endpoint metadata from various origins, including sources such as Cisco ISE and deep packet inspection conducted by Cisco Catalyst 9000 Series Switches. This inspection is facilitated by Network-Based Application Recognition (NBAR) technology.

Given the dependence on IE switches within manufacturing plant access networks, the primary data source for AI endpoint analytics is Cisco ISE. This information is then augmented by endpoint metadata originating from Cisco Cyber Vision. The latter involves conducting DPI on industrial protocols and then assigning pertinent labels to the endpoints. These enriched details are later transmitted from Cisco ISE to the Cisco AI endpoint analytics engine. This process leads to the creation of a cohesive viewpoint that encompasses both IT and OT endpoints within Catalyst Center.

Figure 15. AI Endpoint Analytics



Endpoint Inventory (5) Focus: All Endpoints - Default View

0 Selected

□	MAC Address	Is Random MAC	Trust Score	IP Address	Last S
□	00:00:54:30:AA:45	No	● 6	10.17.13.153	Jul 1
□	00:00:54:30:AA:46	No	● 6	-	Jul 1
□	00:00:BC:2D:21:70	No	● 6	10.17.20.72	Jul 1
□	12:FE:1A:DA:EB:A3	Yes	●	10.2.0.1	Jul 1
□	D0:EC:35:59:08:00	No	●	-	Jul 1

5 Record(s)

00:00:BC:2D:21:70

Hostname - Trust Score ● 6

Two (2) Information Alerts on this page. Expand to see details.

Attributes

> RADIUS

> SNMP

IOTAsset

assetDeviceType	Controller, Rockwell Automation,IO Module, Rockwell Automation,Rockwell Automation
assetHwRevision	-
assetId	00:00:bc:2d:21:70
assetIpAddress	10.17.20.72
assetMacAddress	00:00:bc:2d:21:70
assetName	1756-EN2T/A,1756-EN2T/A (Port1-Link02),1756-L7SP/B LOGIXSAFETY (Port1-Link01),CLX_P | 1756-L73S/B LOGIX5573SAFETY (Port1-
assetProductId	1756-EN2T/A,1756-L73S/B LOGIX5573SAFETY,1756-L7SP/B LOGIXSAFETY
assetProtocol	ARP,ARP, CIP-IO, EthernetIP,EthernetIP

Note: In general, endpoint analytics can be used to profile endpoints by creating profiling rules on Catalyst Center instead of Cisco ISE, but the profiling rules in Catalyst Center does not yet support the IOT asset attributes for profiling.

Network Assurance

Troubleshoot Network Issues

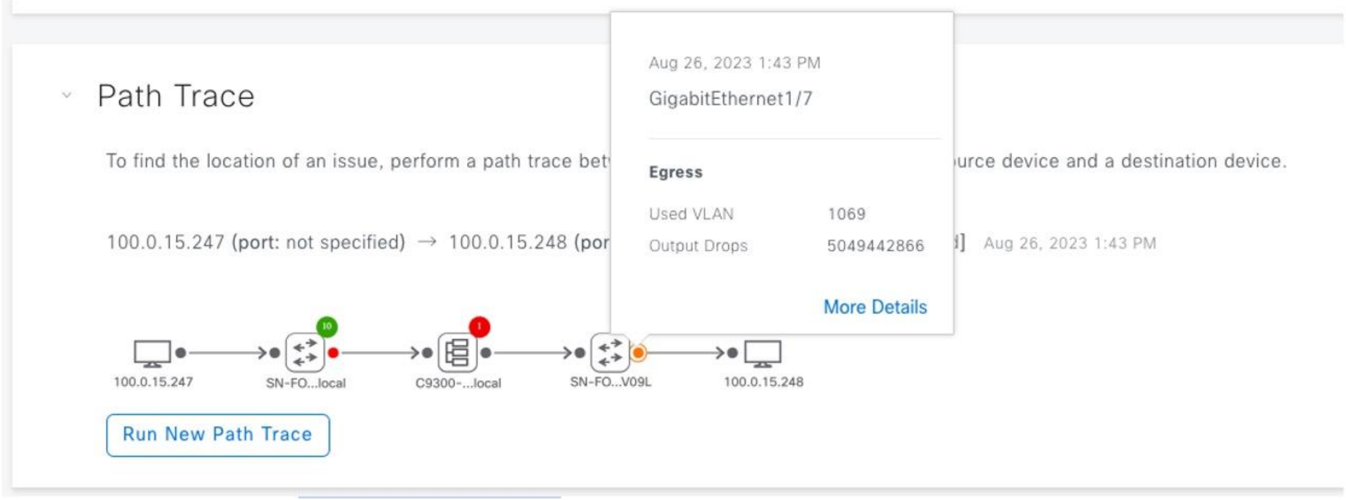
Network Device 360 is a valuable tool in troubleshooting network issues when problems are reported. It allows operators to analyze and diagnose network connectivity problems using Catalyst Center.

To start the troubleshooting process, the operator logs into Catalyst Center and uses the Path Trace feature. The Path Trace feature provides a comprehensive view of end-to-end network connectivity, allowing operators to identify any potential issues along the communication path.

Path trace not only confirms the availability of the communication path but also evaluates the health score of devices along the path. This health score is assigned to clients, devices, and networks, enabling operators to quickly identify any potential issues and prioritize troubleshooting efforts.

The following figure shows the output of path trace, with health score of devices in the path and highlights interfaces with packet drops. Operators can navigate from any of the switches in the network path presented in the path trace output and open the corresponding Device 360 window. This capability facilitates a deeper dive into the specific details of each device along the communication path.

Figure 16. Assurance Path Trace



Path Trace

To find the location of an issue, perform a path trace bet urce device and a destination device.

100.0.15.247 (port: not specified) → 100.0.15.248 (por] Aug 26, 2023 1:43 PM

Aug 26, 2023 1:43 PM

GigabitEthernet1/7

Egress

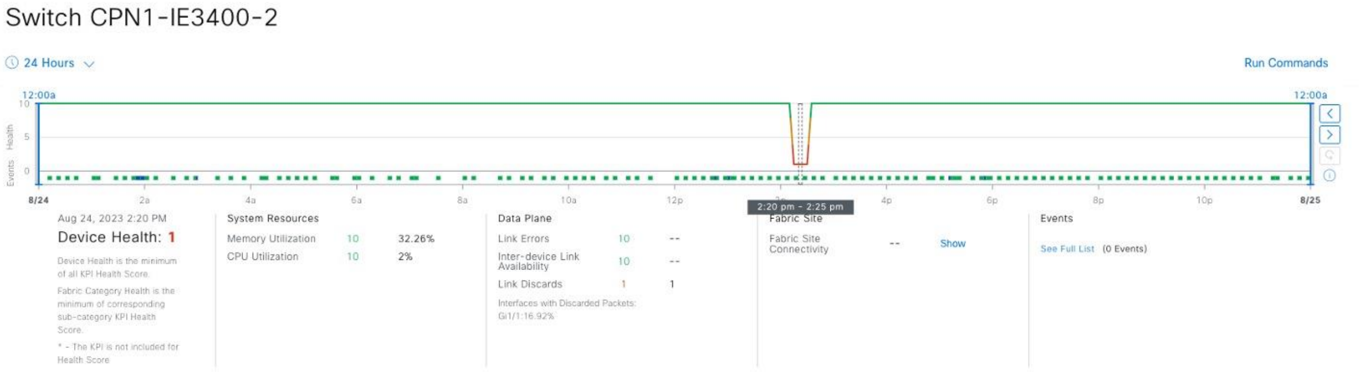
Used VLAN	1069
Output Drops	5049442866

More Details

The Device 360 page displays detailed information about each device, enabling the user to determine if there are any potential issues that need to be addressed. Within the Device 360 page and other assurance pages in Catalyst Center, operators can explore graphs that illustrate past and current key performance indicators (KPIs) over a timeline. These KPI graphs offer a historical perspective on network conditions, allowing operators to understand the exact state of the network at any given time. This information is invaluable for determining the root cause of an issue or identifying recurring patterns.

The following figure shows an example in which a link discards on a particular interface causing temporary decline in the health score.

Figure 17. Assurance Health Score



Switch CPN1-IE3400-2

Aug 24, 2023 2:20 PM

Device Health: 1

Device Health is the minimum of all KPI Health Score.

Fabric Category Health is the minimum of corresponding sub-category KPI Health Score.

* - The KPI is not included for Health Score

System Resources

Memory Utilization	10	32.26%
CPU Utilization	10	2%

Data Plane

Link Errors	10	--
Inter-device Link Availability	10	--
Link Discards	1	1

Interfaces with Discarded Packets: Gi1/1:16.92%

Fabric Site

Fabric Site Connectivity	--	Show

Events

See Full List (0 Events)

Device 360 in Catalyst Center also provides the following information:

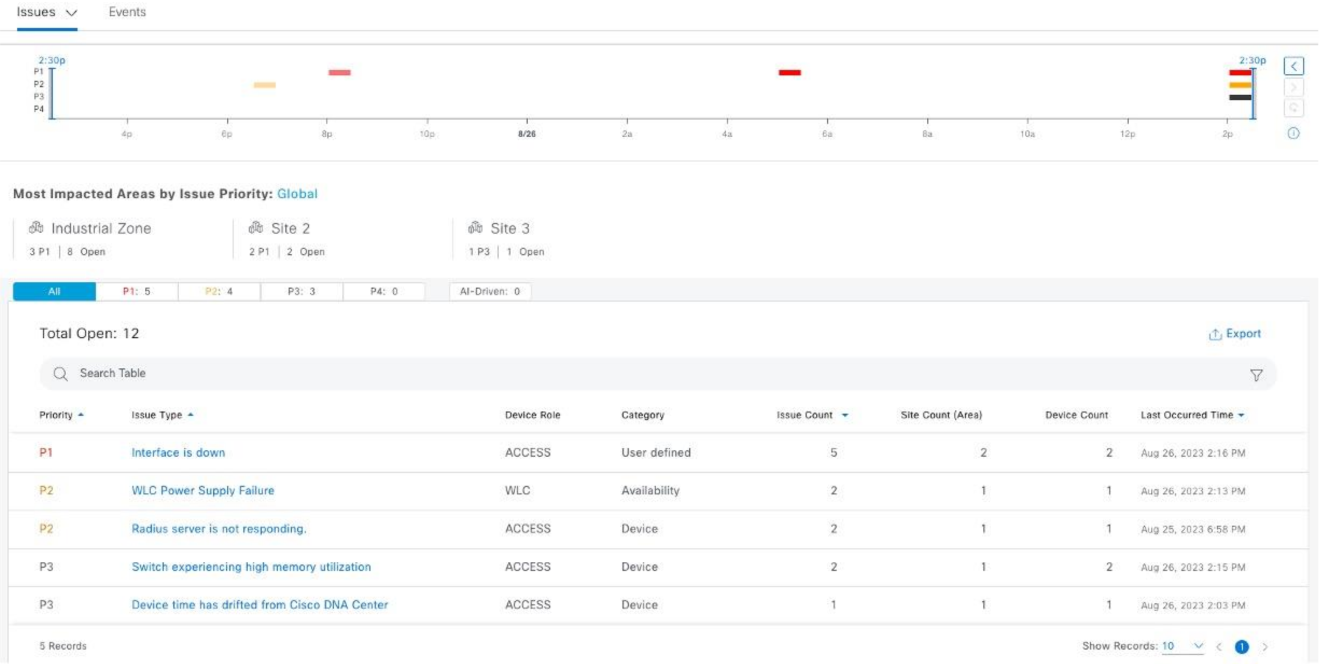
- Visibility into any reported issues and events on a device. Users can easily access and investigate specific issues for further analysis.
- Physical neighbour topology displays client and neighbour network devices. Clicking on a link or device provides additional information.
- Detailed device information, such as CPU, memory, uptime, and temperature.
- Interface information, such as the name, description, operational status, link speed, and so on.
- Interface utilization, errors, and discarding charts.

Address High Priority Issues

The Catalyst Center Issues dashboard identifies problems that need to be addressed in the network by priority. It provides a graph illustrating issues over time, using a color code to show priority and significance. The intensity of the color indicates if more or fewer issues have occurred for that priority level.

The dashboard provides a list of issues organized by priority, as shown in the following figure. It shows the number of times this type of issue occurred, number of sites impacted, number of devices that were impacted by it, and the most recent date and time this issue was seen.

Figure 18. Assurance Issues and Events Dashboard



Most Impacted Areas by Issue Priority: Global

Industrial Zone
3 P1 | 8 Open

Site 2
2 P1 | 2 Open

Site 3
1 P3 | 1 Open

Total Open: 12

Priority	Issue Type	Device Role	Category	Issue Count	Site Count (Area)	Device Count	Last Occurred Time
P1	Interface is down	ACCESS	User defined	5	2	2	Aug 26, 2023 2:16 PM
P2	WLC Power Supply Failure	WLC	Availability	2	1	1	Aug 26, 2023 2:13 PM
P2	Radius server is not responding.	ACCESS	Device	2	1	1	Aug 25, 2023 6:58 PM
P3	Switch experiencing high memory utilization	ACCESS	Device	2	1	2	Aug 26, 2023 2:15 PM
P3	Device time has drifted from Cisco DNA Center	ACCESS	Device	1	1	1	Aug 26, 2023 2:03 PM

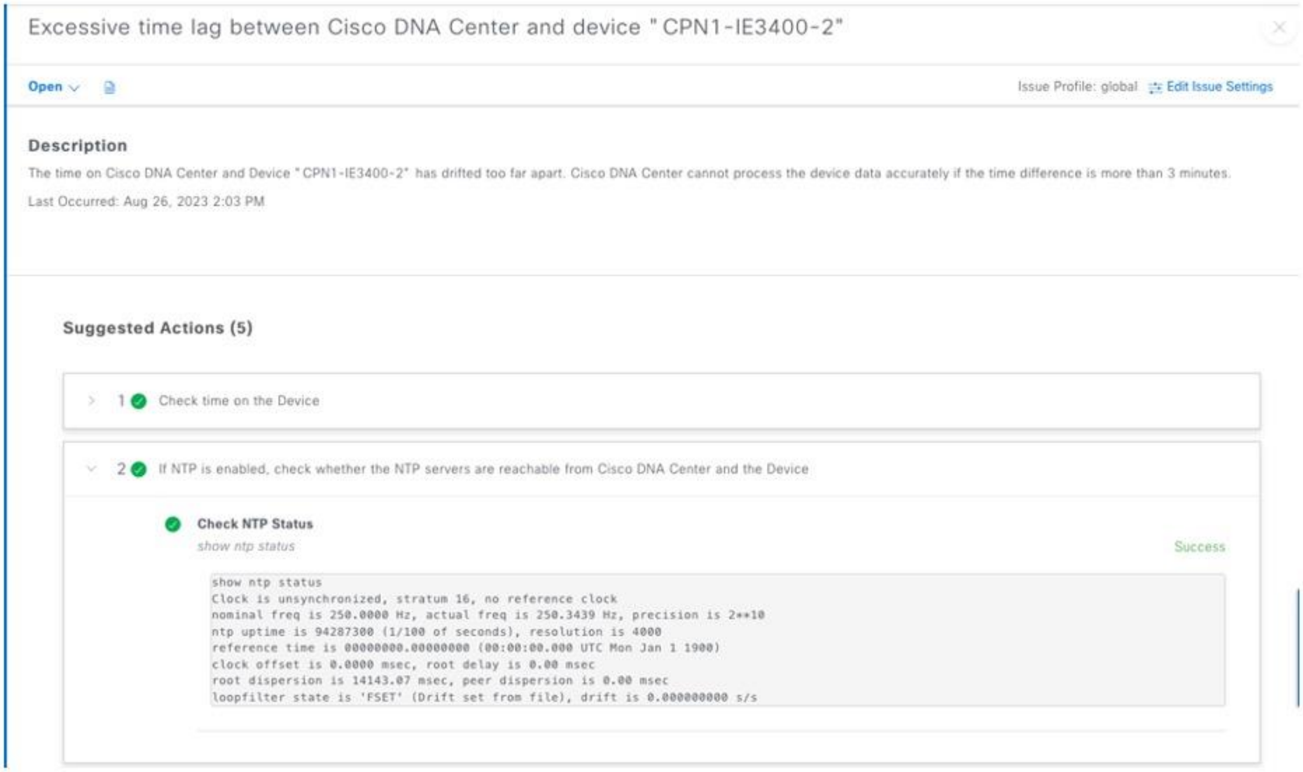
5 Records

Show Records: 10

Furthermore, the Catalyst Center Assurance feature offers a system-guided approach to troubleshooting. It correlates information from various sources, such as device logs, network telemetry, and user reports, to determine the root cause of a problem. Once the root cause is identified, Assurance provides users with possible actions to resolve the problem effectively.

The following figure shows some Catalyst Center suggested actions to investigate a time drift issue. If needed, Catalyst Center runs commands on the device. All this information can be used by the operator to take corrective action.

Figure 19. Issue Remediation



Excessive time lag between Cisco DNA Center and device " CPN1-IE3400-2"

Description

The time on Cisco DNA Center and Device " CPN1-IE3400-2" has drifted too far apart. Cisco DNA Center cannot process the device data accurately if the time difference is more than 3 minutes.

Last Occurred: Aug 26, 2023 2:03 PM

Suggested Actions (5)

1 Check time on the Device

2 If NTP is enabled, check whether the NTP servers are reachable from Cisco DNA Center and the Device

Check NTP Status

show ntp status

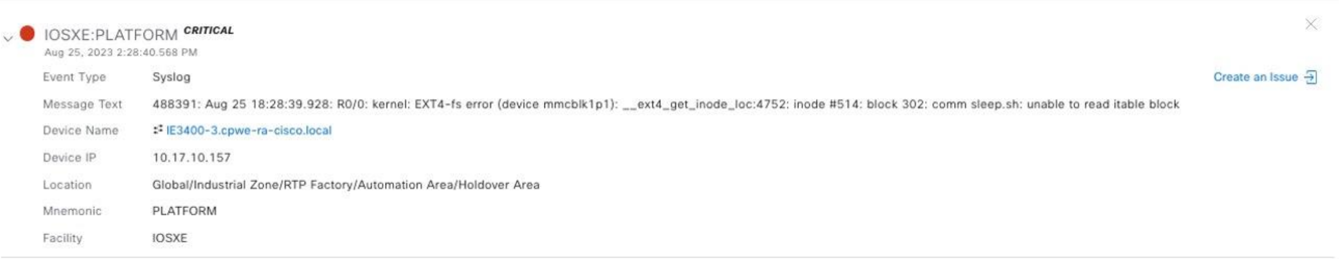
Success

```
show ntp status
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 250.0000 Hz, actual freq is 250.3439 Hz, precision is 2**10
ntp uptime is 94287300 (1/100 of seconds), resolution is 4000
reference time is 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 14143.07 msec, peer dispersion is 0.00 msec
loopfilter state is 'FSET' (Drift set from file), drift is 0.000000000 s/s
```

Customize Assurance to Alert on Interesting Events

You can create customized issues based on events received by Assurance. The following example shows Cisco IOS XE event on an industrial switch received by Catalyst Center. You can create an issue for this type of event to show up on the issues dashboard.

Figure 20. Syslog Event



IOSXE:PLATFORM CRITICAL

Aug 25, 2023 2:28:40.568 PM

Event Type	Syslog
Message Text	488391: Aug 25 18:28:39.928: R0/0: kernel: EXT4-fs error (device mmcblk1p1): __ext4_get_inode_loc:4752: inode #514: block 302: comm sleep.sh: unable to read itable block
Device Name	IE3400-3.cpwe-ra-cisco.local
Device IP	10.17.10.157
Location	Global/Industrial Zone/RTP Factory/Automation Area/Holdover Area
Mnemonic	PLATFORM
Facility	IOSXE

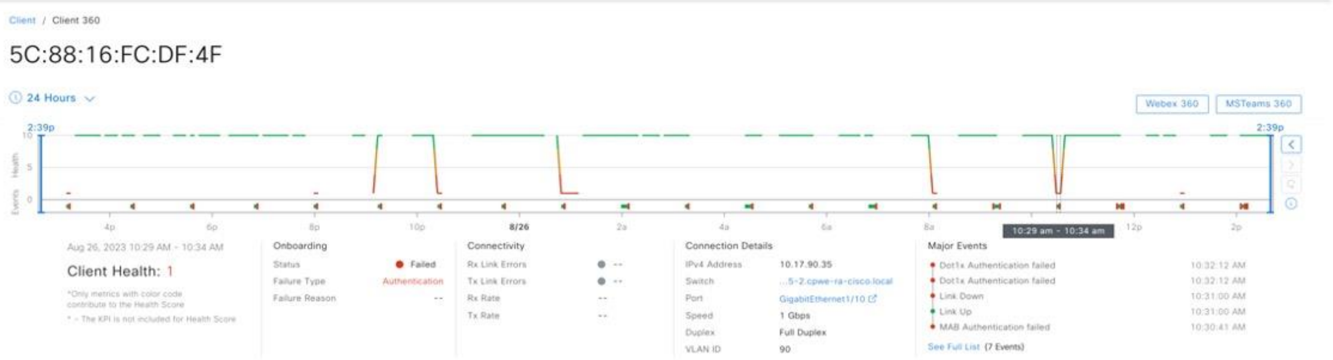
Detecting a Wired Client Issue

The Client Health Dashboard presents an aggregated view of all clients connected to the network. This dashboard displays information such as the connected state, health score, and connected link status for each client. Operators can also apply filters to the dashboard, allowing them to sort and view clients based on criteria such as area, utilization, and health score.

The Event Dashboard within Assurance is another valuable tool for monitoring network events related to wired clients. Operators can easily track events such as link down, link up, and authentication events, providing a comprehensive view of network activity.

For a more detailed analysis of a specific device, operators can zoom in by accessing the Client 360 window. This page offers a graphical representation of the device's health score and events over time, allowing operators to identify patterns and potential issues, as shown in the following figure. Also, Client 360 provides information about related issues and events, offering a comprehensive view of the device's performance.

Figure 21. Client 360 Health Timeline



5C:88:16:FC:DF:4F

Aug 26, 2023 10:29 AM - 10:34 AM

Client Health: 1

*Only metrics with color code contribute to the Health Score

* - The KPI is not included for Health Score

Onboarding

Status	● Failed
Failure Type	Authentication
Failure Reason	--

Connectivity

Rx Link Errors	● --
Tx Link Errors	● --
Rx Rate	--
Tx Rate	--

Connection Details

IPv4 Address	10.17.90.35
Switch	...5-2.cpwe-ra-cisco.local
Port	GigabitEthernet1/10
Speed	1 Gbps
Duplex	Full Duplex
VLAN ID	90

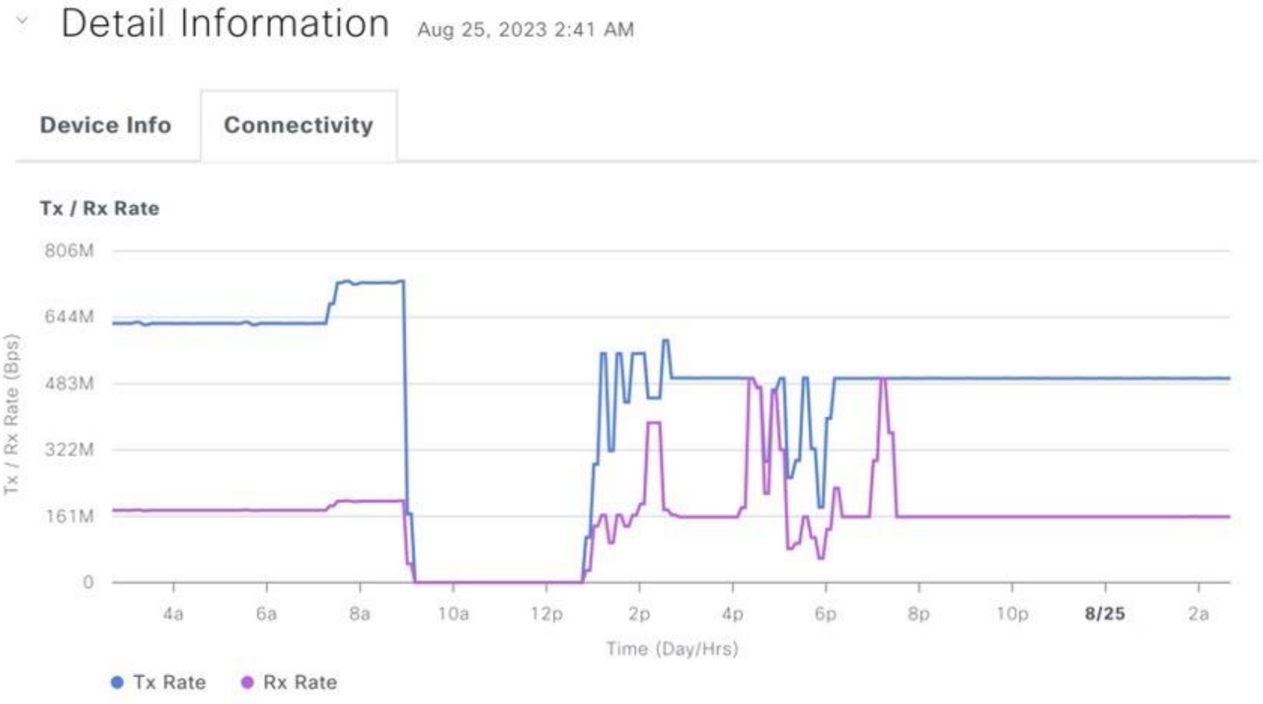
Major Events

● Dot1x Authentication failed	10:32:12 AM
● Dot1x Authentication failed	10:32:12 AM
● Link Down	10:31:00 AM
● Link Up	10:31:00 AM
● MAB Authentication failed	10:30:41 AM

See Full List (7 Events)

Client 360 also provides operators with insights into the neighbor switch information, link status, and utilization of a specific endpoint. The following figure shows link utilization of an endpoint on a selected time frame, aiding in network capacity planning and optimization.

Figure 22. Client 360 Connectivity Timeline



Compliance and Configuration Drift

Compliance management is a critical aspect of network security and governance in the context of industrial automation. It ensures that switches within the industrial network adhere to industry standards, regulatory requirements, and internal policies.

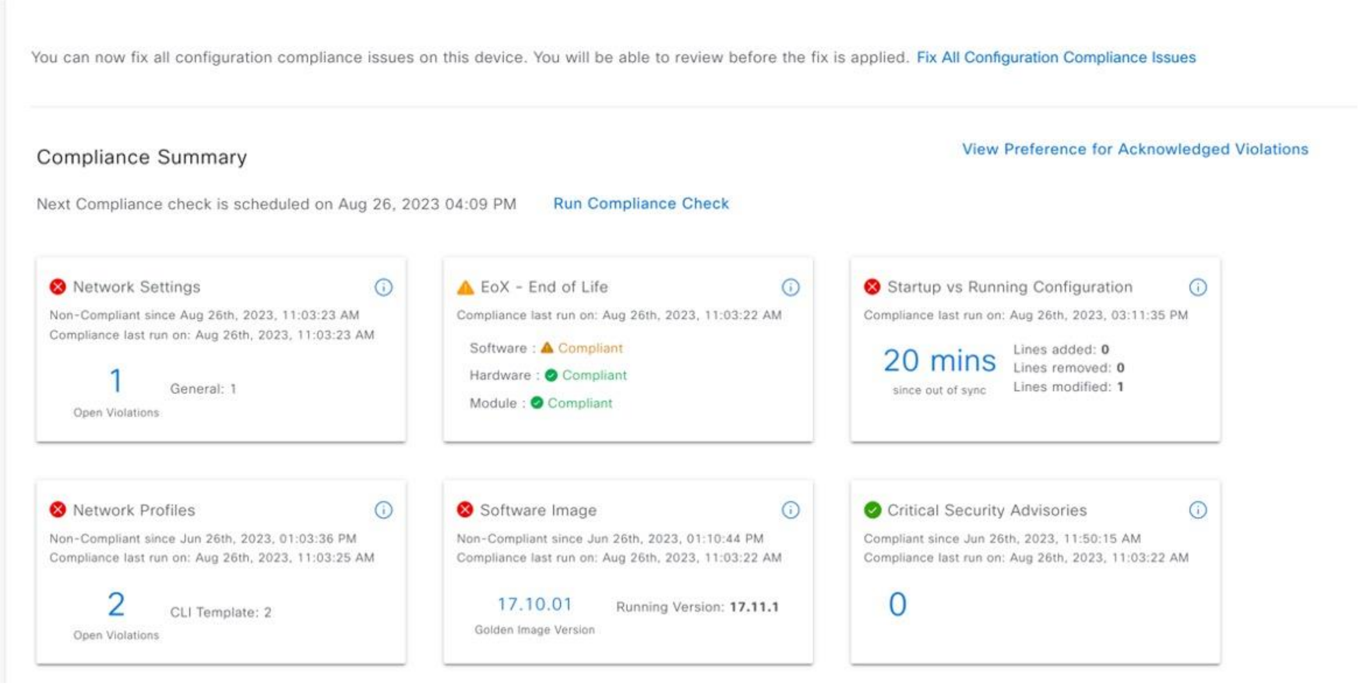
With the Catalyst Center Compliance feature, network administrators in the industrial automation sector gain a centralized and automated approach to monitor, assess, and enforce compliance across their switch infrastructure. This capability allows for consistent and efficient management of compliance policies, reducing the risk of security breaches and ensuring the reliability of the industrial network.

Furthermore, the compliance feature provides continuous monitoring and reporting capabilities, allowing administrators to stay informed about the compliance status of their industrial switches. To ensure the security and integrity of the industrial network, the administrators can easily:

- Track and analyze compliance violations.
- Identify areas of noncompliance.
- Take appropriate actions to remediate any issues.

Automated compliance checks and assessments streamline the compliance management process, significantly reducing manual effort and potential human error. The following figure shows the Compliance Summary window for an industrial switch.

Figure 23. Compliance Summary



You can now fix all configuration compliance issues on this device. You will be able to review before the fix is applied. Fix All Configuration Compliance Issues

Compliance Summary

View Preference for Acknowledged Violations

Next Compliance check is scheduled on Aug 26, 2023 04:09 PM Run Compliance Check

Network Settings
Non-Compliant since Aug 26th, 2023, 11:03:23 AM
Compliance last run on: Aug 26th, 2023, 11:03:23 AM
1 Open Violations General: 1

EoX - End of Life
Compliance last run on: Aug 26th, 2023, 11:03:22 AM
Software : Compliant
Hardware : Compliant
Module : Compliant

Startup vs Running Configuration
Compliance last run on: Aug 26th, 2023, 03:11:35 PM
20 mins since out of sync
Lines added: **0**
Lines removed: **0**
Lines modified: **1**

Network Profiles
Non-Compliant since Jun 26th, 2023, 01:03:36 PM
Compliance last run on: Aug 26th, 2023, 11:03:25 AM
2 Open Violations CLI Template: 2

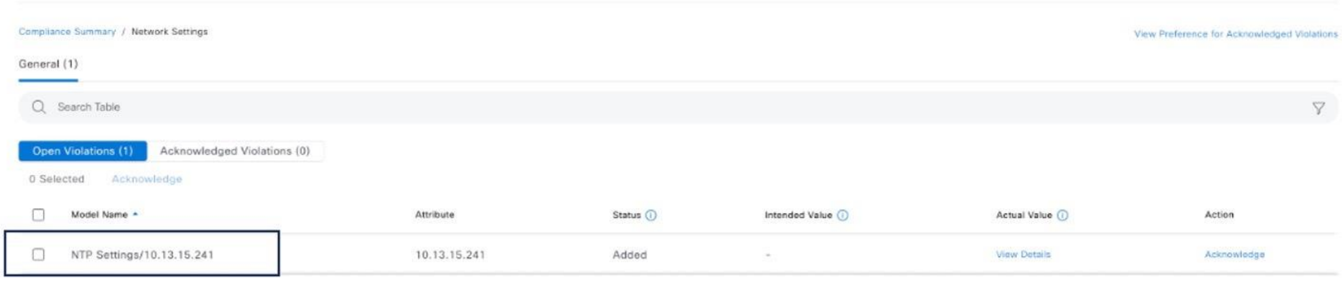
Software Image
Non-Compliant since Jun 26th, 2023, 01:10:44 PM
Compliance last run on: Aug 26th, 2023, 11:03:22 AM
17.10.01 Golden Image Version Running Version: **17.11.1**

Critical Security Advisories
Compliant since Jun 26th, 2023, 11:50:15 AM
Compliance last run on: Aug 26th, 2023, 11:03:22 AM
0

The Compliance Summary window for an industrial switch allows administrators to perform compliance checks in the following areas:

- **Network Settings**: Catalyst Center enables administrators to define configuration settings for a site and push them to switches in that zone. Examples of this are NTP, AAA, and DNS settings. The compliance check identifies and flags any violations that may occur due to out-of-band changes or other factors.

Figure 24. Compliance Network Settings



Compliance Summary / Network Settings

View Preference for Acknowledged Violations

General (1)

Search Table

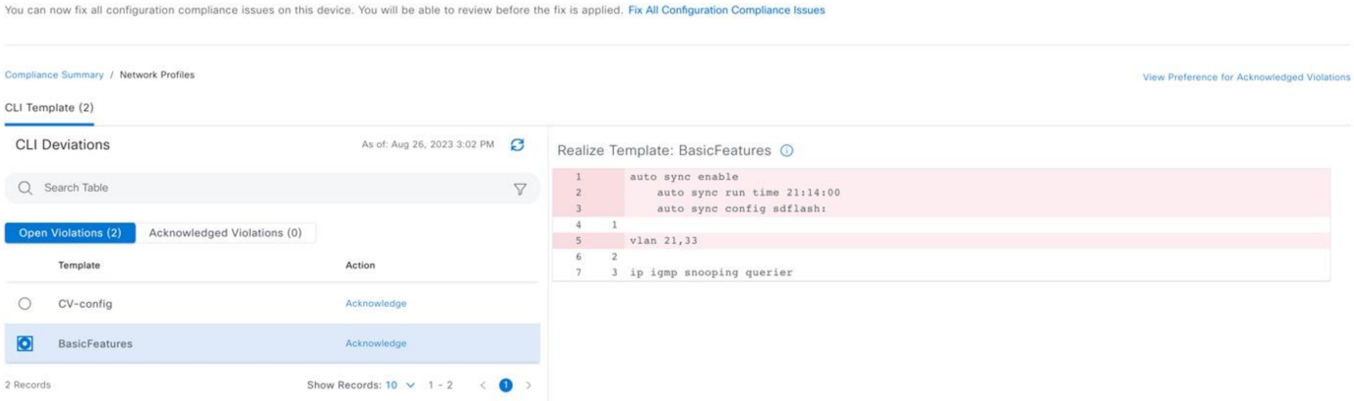
Open Violations (1) | Acknowledged Violations (0)

0 Selected Acknowledge

□	Model Name	Attribute	Status	Intended Value	Actual Value	Action
□	NTP Settings/10.13.15.241	10.13.15.241	Added	-	View Details	Acknowledge

- **Network Profiles**: Administrators can define intent configurations using network profiles and apply them to the device. For industrial switches, this section flags any deviations from the day-n template applied to the device. To assist with remediation, Catalyst Center provides capabilities for making configuration changes to make the devices compliant.

Figure 25. Compliance Network Profiles



You can now fix all configuration compliance issues on this device. You will be able to review before the fix is applied. Fix All Configuration Compliance Issues

Compliance Summary / Network Profiles

View Preference for Acknowledged Violations

CLI Template (2)

CLI Deviations

As of: Aug 26, 2023 3:02 PM

Search Table

Open Violations (2) | Acknowledged Violations (0)

	Template	Action
○	CV-config	Acknowledge
●	BasicFeatures	Acknowledge

2 Records Show Records: 10 1 - 2 1

Realize Template: BasicFeatures

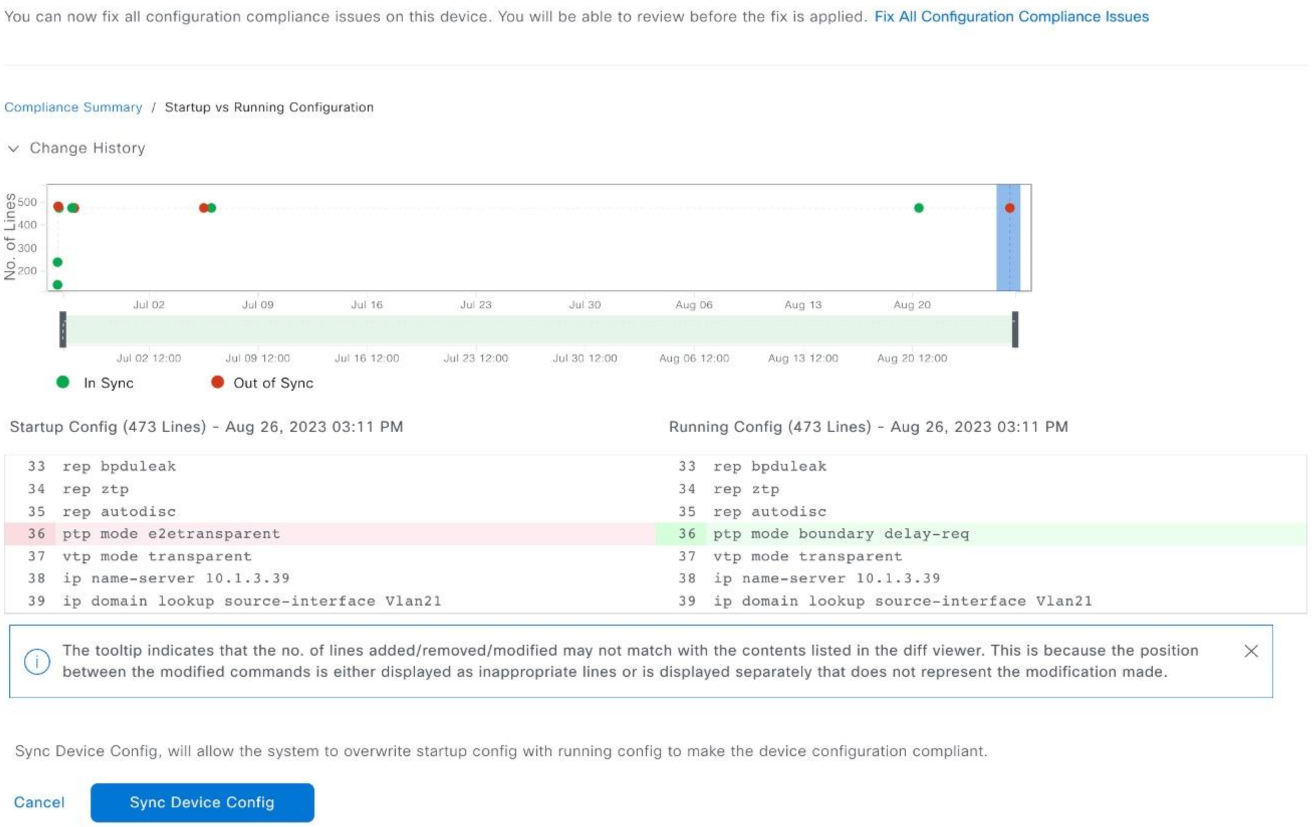
```
auto sync enable
    auto sync run time 21:14:00
    auto sync config sdflash:

vlan 21,33

ip igmp snooping querier
```

- **EoX - End of Life**: This compliance check allows administrators to check the compliance status of hardware and software modules for devices approaching end-of-life.

- **Software Image**: This compliance check allows administrators to compare the tagged golden image in Catalyst Center with the running image on the device. It highlights any differences between the two, enabling administrators to ensure consistency.

- **Startup vs. Running Configuration**: This compliance check helps to identify whether the device's startup and running configurations are synchronized. Any discrepancies between the two configurations are flagged for attention. It is crucial to remediate any changes to ensure that the switch retains the same configuration after a reload or reboot.

Figure 26. Compliance Configuration Comparison



You can now fix all configuration compliance issues on this device. You will be able to review before the fix is applied. Fix All Configuration Compliance Issues

Compliance Summary / Startup vs Running Configuration

Change History

Startup Config (473 Lines) - Aug 26, 2023 03:11 PM

Running Config (473 Lines) - Aug 26, 2023 03:11 PM

```
rep bpduleak                                     rep bpduleak
rep ztp                                          rep ztp
rep autodisc                                     rep autodisc
ptp mode e2etransparent                          ptp mode boundary delay-req
vtp mode transparent                             vtp mode transparent
ip name-server 10.1.3.39                         ip name-server 10.1.3.39
ip domain lookup source-interface Vlan21         ip domain lookup source-interface Vlan21
```

The tooltip indicates that the no. of lines added/removed/modified may not match with the contents listed in the diff viewer. This is because the position between the modified commands is either displayed as inappropriate lines or is displayed separately that does not represent the modification made.

Sync Device Config, will allow the system to overwrite startup config with running config to make the device configuration compliant.

- **Critical Security Advisories**: This compliance check enables administrators to verify if network devices are free from critical security vulnerabilities.

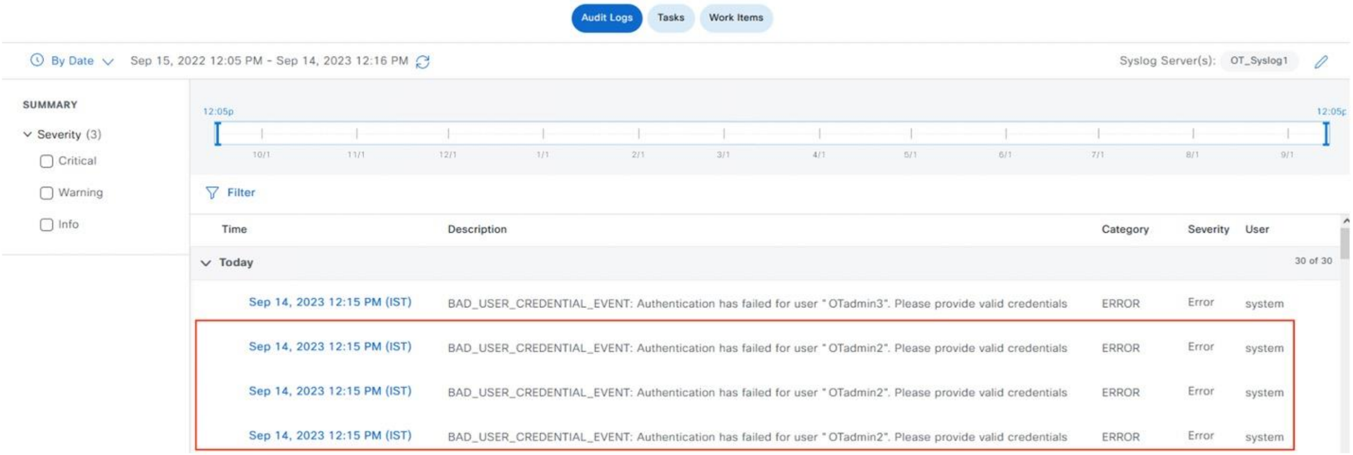
Audit Logs

Audit logs serve the purpose of capturing critical activities, including the timing of requested configuration changes, the execution of these changes, and the detection of any associated errors. They also document system events, their timestamps, locations, and the associated users. Catalyst Center audit logging provides a convenient means to monitor login attempts, access to network resources, and configuration changes, thereby enabling the detection and response to unauthorized or suspicious activities within the manufacturing network. This plays a pivotal role in safeguarding sensitive data and intellectual property.

When network problems arise, especially those potentially caused by misconfigurations, audit logs become indispensable for identifying the underlying cause. They enable the tracing of changes or actions that might have played a role in the issue, facilitating the diagnosis and resolution of network-related problems. Furthermore, Catalyst Center's Audit Log feature facilitates regular review and analysis of these logs to identify trends, anomalies, or patterns that may signify security threats, operational challenges, or opportunities for optimization. To enhance accessibility and centralized management, these audit logs can be conveniently exported to a syslog server, allowing for a consolidated view from multiple systems within the network.

The following figure shows a scenario where a super admin possesses the capability to oversee a series of unsuccessful login attempts made by the user OTadmin2. If these repeated failures suggest a potential intrusion or security breach, the super administrator has the authority to take proactive measures, such as blocking the user's access to the system, as a security precaution with the help of insights from Catalyst Center audit logs.

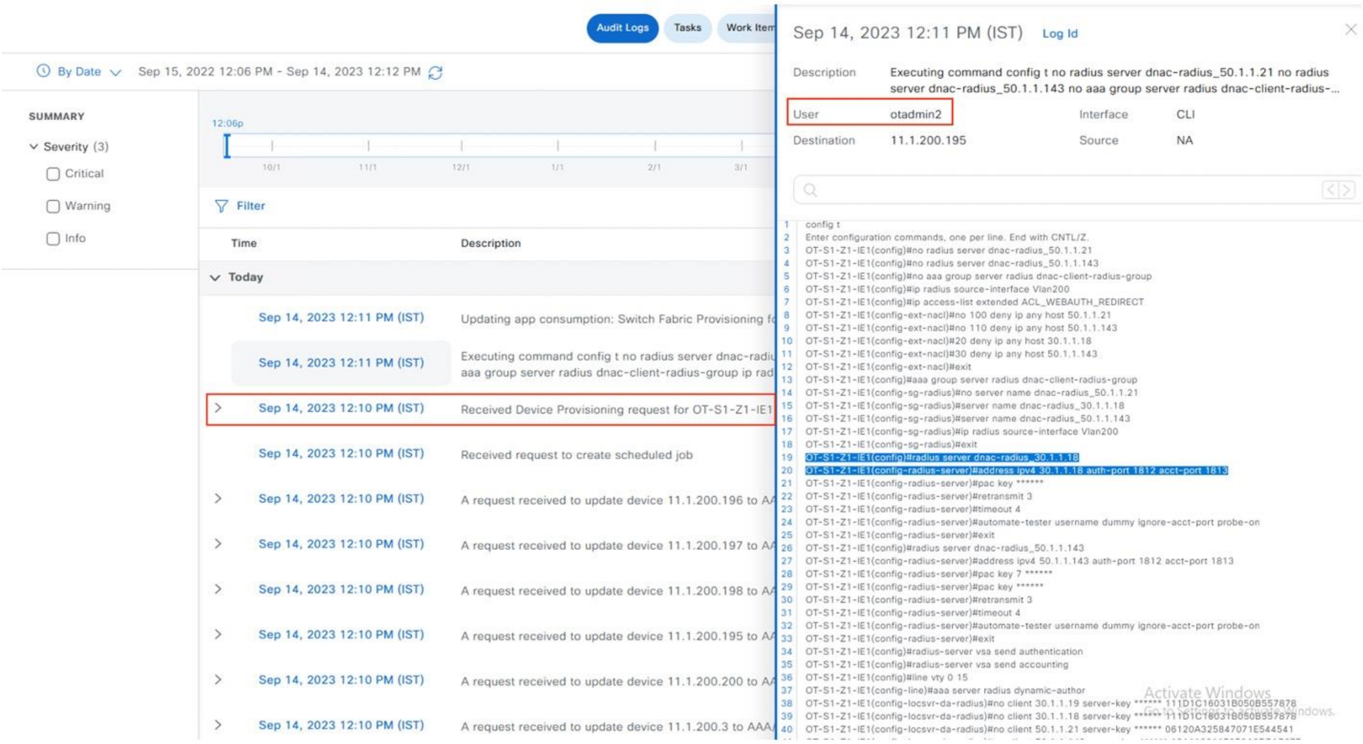
Figure 27. Audit Logs



Time	Description	Category	Severity	User
Sep 14, 2023 12:15 PM (IST)	BAD_USER_CREDENTIAL_EVENT: Authentication has failed for user " OTadmin3". Please provide valid credentials	ERROR	Error	system
Sep 14, 2023 12:15 PM (IST)	BAD_USER_CREDENTIAL_EVENT: Authentication has failed for user " OTadmin2". Please provide valid credentials	ERROR	Error	system
Sep 14, 2023 12:15 PM (IST)	BAD_USER_CREDENTIAL_EVENT: Authentication has failed for user " OTadmin2". Please provide valid credentials	ERROR	Error	system
Sep 14, 2023 12:15 PM (IST)	BAD_USER_CREDENTIAL_EVENT: Authentication has failed for user " OTadmin2". Please provide valid credentials	ERROR	Error	system

In a different scenario, if the OT admin identifies problems with endpoint authentication on the plant floor linked to a specific device named OT-S1-Z1-IE1, the admin can efficiently filter the audit logs to focus on this particular device name and to trace any configuration changes. Through this process, admin is able to pinpoint the change in the Authentication, Authorization, and Accounting (AAA) server configuration, which was provisioned by the user otadmin2, as the root cause of the issue. Later, the administrator can take remedial actions to address and rectify the problem.

Figure 28. Audit Log Details



Time	Description
Sep 14, 2023 12:11 PM (IST)	Updating app consumption: Switch Fabric Provisioning fo
Sep 14, 2023 12:11 PM (IST)	Executing command config t no radius server dnac-radiu aaa group server radius dnac-client-radius-group ip rad
Sep 14, 2023 12:10 PM (IST)	Received Device Provisioning request for OT-S1-Z1-IE1
Sep 14, 2023 12:10 PM (IST)	Received request to create scheduled job
Sep 14, 2023 12:10 PM (IST)	A request received to update device 11.1.200.196 to AA
Sep 14, 2023 12:10 PM (IST)	A request received to update device 11.1.200.197 to AA
Sep 14, 2023 12:10 PM (IST)	A request received to update device 11.1.200.198 to AA
Sep 14, 2023 12:10 PM (IST)	A request received to update device 11.1.200.195 to AA
Sep 14, 2023 12:10 PM (IST)	A request received to update device 11.1.200.200 to AA
Sep 14, 2023 12:10 PM (IST)	A request received to update device 11.1.200.3 to AAA

Sep 14, 2023 12:11 PM (IST)

Description Executing command config t no radius server dnac-radius_50.1.1.21 no radius server dnac-radius_50.1.1.143 no aaa group server radius dnac-client-radius-...

User otadmin2 Interface CLI

Destination 11.1.200.195 Source NA

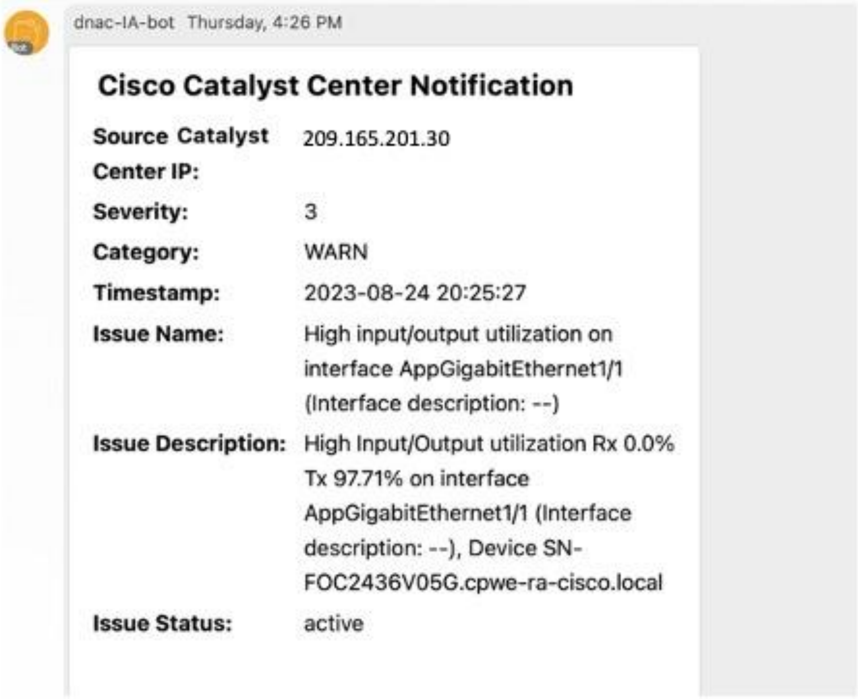
```
config t
Enter configuration commands, one per line. End with CNTL/Z.
OT-S1-Z1-IE1(config)#no radius server dnac-radius_50.1.1.21
OT-S1-Z1-IE1(config)#no radius server dnac-radius_50.1.1.143
OT-S1-Z1-IE1(config)#no aaa group server radius dnac-client-radius-group
OT-S1-Z1-IE1(config)#ip radius source-interface Vlan200
OT-S1-Z1-IE1(config)#ip access-list extended ACL_WEBAUTH_REDIRECT
OT-S1-Z1-IE1(config-ext-nacl)#no 100 deny ip any host 50.1.1.21
OT-S1-Z1-IE1(config-ext-nacl)#no 110 deny ip any host 50.1.1.143
OT-S1-Z1-IE1(config-ext-nacl)#20 deny ip any host 30.1.1.18
OT-S1-Z1-IE1(config-ext-nacl)#30 deny ip any host 50.1.1.143
OT-S1-Z1-IE1(config-ext-nacl)#exit
OT-S1-Z1-IE1(config)#aaa group server radius dnac-client-radius-group
OT-S1-Z1-IE1(config-sg-radius)#no server name dnac-radius_50.1.1.21
OT-S1-Z1-IE1(config-sg-radius)#server name dnac-radius_30.1.1.18
OT-S1-Z1-IE1(config-sg-radius)#server name dnac-radius_50.1.1.143
OT-S1-Z1-IE1(config-sg-radius)#ip radius source-interface Vlan200
OT-S1-Z1-IE1(config-sg-radius)#exit
OT-S1-Z1-IE1(config)#radius server dnac-radius_30.1.1.18
OT-S1-Z1-IE1(config-radius-server)#address ipv4 30.1.1.18 auth-port 1812 acct-port 1813
OT-S1-Z1-IE1(config-radius-server)#pac key ******
OT-S1-Z1-IE1(config-radius-server)#retransmit 3
OT-S1-Z1-IE1(config-radius-server)#timeout 4
OT-S1-Z1-IE1(config-radius-server)#automate-tester username dummy ignore-acct-port probe-on
OT-S1-Z1-IE1(config-radius-server)#exit
OT-S1-Z1-IE1(config)#radius server dnac-radius_50.1.1.143
OT-S1-Z1-IE1(config-radius-server)#address ipv4 50.1.1.143 auth-port 1812 acct-port 1813
OT-S1-Z1-IE1(config-radius-server)#pac key 7 ******
OT-S1-Z1-IE1(config-radius-server)#pac key ******
OT-S1-Z1-IE1(config-radius-server)#retransmit 3
OT-S1-Z1-IE1(config-radius-server)#timeout 4
OT-S1-Z1-IE1(config-radius-server)#automate-tester username dummy ignore-acct-port probe-on
OT-S1-Z1-IE1(config-radius-server)#exit
OT-S1-Z1-IE1(config)#radius-server vsa send authentication
OT-S1-Z1-IE1(config)#radius-server vsa send accounting
OT-S1-Z1-IE1(config)#line vty 0 15
OT-S1-Z1-IE1(config-line)#aaa server radius dynamic-author
OT-S1-Z1-IE1(config-locsvr-da-radius)#no client 30.1.1.19 server-key ****** 111D1C16031B050B557878
OT-S1-Z1-IE1(config-locsvr-da-radius)#no client 30.1.1.18 server-key ****** 111D1C16031B050B557878
OT-S1-Z1-IE1(config-locsvr-da-radius)#no client 50.1.1.21 server-key ****** 06120A325847071E544541
```

Notifications

Operators on the manufacturing floor are constantly on the move, often without access to a stationary dashboard. Therefore, notifications play a crucial role in keeping them informed. With Catalyst Center notifications, administrators and operators can receive real-time updates on any assurance issues or events that may impact the performance or availability of the automation network. This enables them to promptly address any potential problems, minimize downtime, and ensure uninterrupted operations. By using Catalyst Center notifications, industrial automation networks can benefit from improved visibility, proactive monitoring, and efficient troubleshooting, ultimately enhancing the overall reliability and productivity of the network. Supported assurance channels for notifications are REST, PagerDuty, Syslog, Webex, and email.

The following figure shows a Webex notification for high utilization on a network interface. Upon receipt, the operator could take necessary actions to correct the issue.

Figure 29. Webex Notification



dnac-IA-bot Thursday, 4:26 PM

Cisco Catalyst Center Notification

Source Catalyst Center IP:	209.165.201.30
Severity:	3
Category:	WARN
Timestamp:	2023-08-24 20:25:27
Issue Name:	High input/output utilization on interface AppGigabitEthernet1/1 (Interface description: --)
Issue Description:	High Input/Output utilization Rx 0.0% Tx 97.71% on interface AppGigabitEthernet1/1 (Interface description: --), Device SN-FOC2436V05G.cpwe-ra-cisco.local
Issue Status:	active

Technical References

Cisco Catalyst Center User Guide

Cisco Validated Designs for Digital Manufacturing

Cisco Catalyst Center for Industrial Automation Design Guide

Cisco Catalyst Center for Industrial Automation Implementation Guide

Networking and Security in Industrial Automation Environments Design and Implementation Guide

Cisco Catalyst Center User Guide for Nonfabric REP Provision

REP Zero Touch Provisioning

Industrial Automation Security Design Guide 2.0

Securely Traversing IACS Data across the IDMZ Using Cisco Firepower Threat Defense

Cisco Catalyst Center User Guide for Wireless Mesh Network

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide for Ethernet Bridging