Cisco DNA Center for Industrial Automation Design Guide

Executive Summary

The Cisco DNA Center for Industrial Automation Design Guide provides design guidelines to introduce Cisco's Digital Network Architecture (DNA) Center in the Industrial Automation Design as described in the solution brief.

Industrial automation systems have fully adopted standard networking technologies and rely on them for their communications. These networks must have the scale, flexibility, performance, and resiliency needed for these critical systems. This connectivity is the foundation for the industrial IoT and Industry 4.0 evolution–connecting sensors, actuators, and control systems to the machine-learning, digitization innovations in the cloud. IT and Operational Technology (OT) convergence in networking and security technology is not just established but critical to a wave of optimizations and improvements in the ecosystem.

The network management and tools are still far from converged. OT personnel do not have the same access to, and benefit of, the network and security management tools used by IT. And yet they still need to rely on the network to operate the production environment, often without tools that tell them how the network is performing and the ability to maintain that network. If a link fails or a device connects improperly, it takes a sleuth to identify and resolve the problem. Key challenges facing OT personnel are described in the next section.

Note: Software-defined access (SDA) is the industry's first intent-based networking solution for the enterprise built on the principles of the Cisco Digital Network Architecture (DNA). SDA provides automated configuration and end-to-end segmentation to separate user, device, and application traffic without redesigning the network. However, SDA is not yet validated for deployment to support industrial automation and control (the control loop) applications in the Cell/Area Zone in this solution. This guide focuses on non-SDA (non-fabric) design.

Tech Tip: Cisco DNA Center uses the term device to refer to network infrastructure devices such as switches and routers. Client refers to an end device such as a computer, PLC, and HMI. This terminology is used in the document.

Common Network Challenges in Industrial Networks

- Lack of network health visibility prevents network administrators from taking proactive measures to avoid outages. Furthermore, it is difficult to find the root cause of the problem during outages.
- Manual maintenance tasks such software upgrades and configuration changes increase the risk of incomplete or inconsistent changes.
- There can be discrepancies in As-Built versus As-Is network states due to configuration changes over time. Knowledge gaps about communication flows can lead to potential misconfigurations or outages.

Cisco DNA Center Value Proposition in Industrial Networks

The solution described here applies Cisco DNA Center to industrial automation networks and, alongside IT, gives OT a curated view and set of functions to perform key network maintenance tasks, consistently and scalably. The following list describes Cisco DNA Center features that address challenges described in the previous section.

- Network monitoring and analytics for proactive remediation—Cisco DNA Assurance enables every point on the network to become a sensor, sending continuous telemetry on application performance and user connectivity in real time. This, coupled with automatic path-trace visibility and guided remediation, means network issues are resolved in minutes—before they become problems.
- Simplified deployment and automation of network maintenance and configuration tasks—Cisco DNA automation provides Zero-touch device provisioning, software image management, device replacement flows, and network provisioning tasks to facilitate device deployment, configuration, and maintenance at scale. Additionally, compliance checks are provided to guarantee the network is compliant with business intent.
- Consistent security policies for endpoints connecting to the network—The proposed architecture uses Cisco DNA Center, Cisco Identity Services Engine (ISE), and Cisco Cyber Vision to enhance the visibility of assets and interactions and create security policy to segment the network.

Related Documentation

The Cisco DNA Center for Industrial Automation Design Guide builds on top of Industrial Automation and Industrial Security Design and Implementation Guides available at:
https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-industry-solutions/index.html

The following is a list of relevant documentation available at the link above and referenced in this guide.

- Industrial Automation and Security Design Guide:
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/DG/Industrial-AutomationDG.html
- Industrial Automation Implementation Guide:
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/IG/Industrial-AutomationIG.html
- Industrial Security Design Guide:
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/IA_Security/IA_Security_DG.html
- Industrial Security Implementation Guide:
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/IA_Security/IA_Security_IG/IA_Security_IG.html

We have also jointly developed and tested the Converged Plantwide Ethernet set of design and implementation guidelines with Rockwell Automation. The following relevant documents are found on both Cisco and Rockwell Automation's web site:
https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html

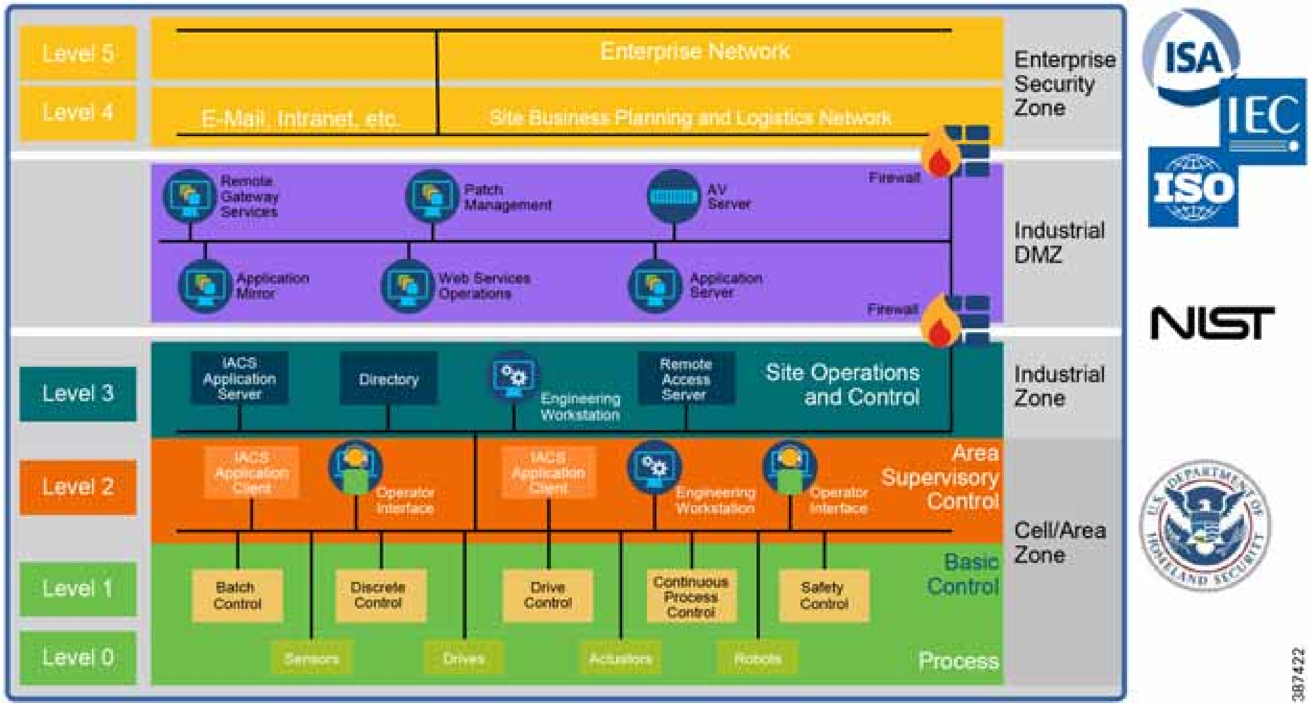
Architecture Considerations

Plant Logical Framework

Industrial Automation architecture uses a logical framework described in detail in the Networking and Security in Industrial Automation Environments Design and Implementation Guide:
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/DG/Industrial-AutomationDG.html

The framework is based on the Purdue Model for Control Hierarchy (reference ISBN 1-55617-265-6) and its objective is to segment devices and equipment into hierarchical functions. This section covers basic concepts on the plant logical framework; for more information refer to the aforementioned guide.

Figure 1 Industrial Plant Reference Architecture with IDMZ



Industrial Zone

The Industrial zone comprises the Cell/Area Zones and site-level area. The Industrial zone is important because all the IACS applications, devices, and controllers critical to monitoring and controlling the plant floor IACS operations are in this zone.

- The Site-level area is where applications related to operating the site reside, specifically the applications and services that are directly driving production. This space is generally “carpeted space”—meaning it has HVAC with typical 19-inch rack-mounted equipment in hot/cold aisles utilizing commercial grade equipment. Devices on this area are known as Level 3 devices.
- The Cell Area/Zone is a functional area within a plant facility and many plants have multiple Cell/Area Zones. Larger plants might have “Zones” designated for fairly broad processes that have smaller subsets of “Cell Areas” within them where the process is broken down into ever smaller subsets. A Cell/Area Zone has devices ranging from Level 0 to 2.
  - Level 0 consists of a wide variety of sensors and actuators involved in the basic industrial process.
  - Level 1 consists of controllers that direct and manipulate the manufacturing process, primarily interfacing with the Level 0 devices.
  - Level 2 represents the applications and functions associated with the Cell/Area Zone runtime supervision and operation such as HMIs and control room workstations.

Enterprise Zone

The Enterprise Zone contains Levels 4 and 5, provides access to the Internet and network applications typically managed by IT, and is non-critical to industrial operations.

- The Site Business Planning and Logistics Network (Level 4) is where the functions and systems that need standard access to services provided by the enterprise network reside. This level is viewed as an extension of the enterprise network.
- The Enterprise Network (Level 5) is where the centralized IT systems and functions exist. Enterprise resource management, business-to-business, and business-to-customer services typically reside at this level.

Although important, these services are not viewed as critical to the IACS and thus the plant floor operations. Because of the more open nature of the systems and applications within the enterprise network, this level is often viewed as a source of threats and disruptions to the IACS network.

Industrial DMZ

To preserve smooth plant operations and functioning of the IACS applications and IACS network in alignment with standards such as IEC 62443, this zone requires clear logical segmentation and protection from Levels 4 and 5. Although not part of the Purdue reference model, the industrial automation solution includes a demilitarized zone (DMZ) between the Industrial and Enterprise zones. The industrial DMZ (IDMZ) is deployed within plant environments to separate the enterprise networks and the operational domain of the plant environment. Downtime in the IACS network can be costly and have a severe impact on revenue, so the operational zone cannot be impacted by any outside influences. Network access is not permitted directly between the enterprise and the plant; however, data and services are required to be shared between the zones, thus the industrial DMZ provides architecture for the secure transport of data. Typical services deployed in the DMZ include remote access servers and mirrored services.

Industrial Automation Requirements

This section covers key requirements on Industrial Automation networks. These requirements and the design to meet them are explained fully in the Networking and Security in Industrial Automation Environments Design and Implementation Guide but are listed in this section to provide context. The main goal of this design guide is to introduce Cisco DNA Center on Industrial Automation while meeting these requirements.

Operational Technology Application Requirements

OT applications at their core are focused on maintaining stability, continuity, and integrity of industrial processes. At the core is a loop of sensors, controllers, and actuators that must be maintained to properly operate the industrial processes. Additionally, several other applications need to gather information to display status, maintain history, and optimize the industrial process operations. From this standpoint, Industrial Automation architecture provides guidance to achieve high availability, low latency, and jitter in the communication.

Ruggedization and Environmental Requirements

Typical enterprise network devices reside in controlled environments, which is a key differentiator of the IACS from typical enterprise applications. The IACS end devices and network infrastructure are located in harsh environments that require compliance to environmental specifications such as IEC 529 (ingress protection) or National Electrical Manufacturers Association (NEMA) specifications. The IACS end devices and network infrastructure may be in physically disparate locations and in non-controlled or even harsh environmental conditions such as temperature, humidity, vibration, noise, explosiveness, or electronic interference.

Due to these environmental considerations the IACS devices and network infrastructure must support and withstand these harsh conditions. Also DIN rail compliant form factor is ideal for industrial environments when compared to enterprise which typically reside in 19-inch rack mounts.

Security Requirements

When discussing industrial network security, customers are concerned with how to keep the environment safe and operational. It is recommended to follow an architectural approach to securing the control system and process domain. Besides the segmentation provided by the logical plant framework, key security requirements in the Cell/Area Zone include device and IACS asset visibility, secure access to the network, traffic segmentation, group-based security policy, malware detection and intrusion detection and Layer 2 hardening (control plane and data plane) to protect the infrastructure.

Information Technology and Operational Technology Convergence

Historically, production environments and the IACS in them have been the sole responsibility of the operational organizations within enterprises. Enterprise applications and networks have been the sole responsibility of IT organizations. But as OT has started adopting standard networking, there has been a need to not only interconnect these environments, but to converge organizational capabilities and drive collaboration between vendors and suppliers.

Decisions impacting IACS networks are typically driven by plant managers and control engineers, rather than the IT department. Additionally, the IACS vendor and support supply chain are different than those typically used by the IT department. OT teams require an easy-to-use and intelligent platform that presents network information in the context of automation equipment. Key functions at this layer will include plug-and-play, easy switch replacement, and ease of use to maintain the network infrastructure. However, IT departments of manufacturers are increasingly engaging with plant managers and control engineers to leverage the knowledge and expertise in standard networking technologies for the benefit of plant operations.

Integrating Cisco DNA Center into the Industrial Automation Architecture

This section explains how to introduce Cisco DNA Center on the Industrial Automation architecture while meeting the requirements listed in IIndustrial Automation Requirements.

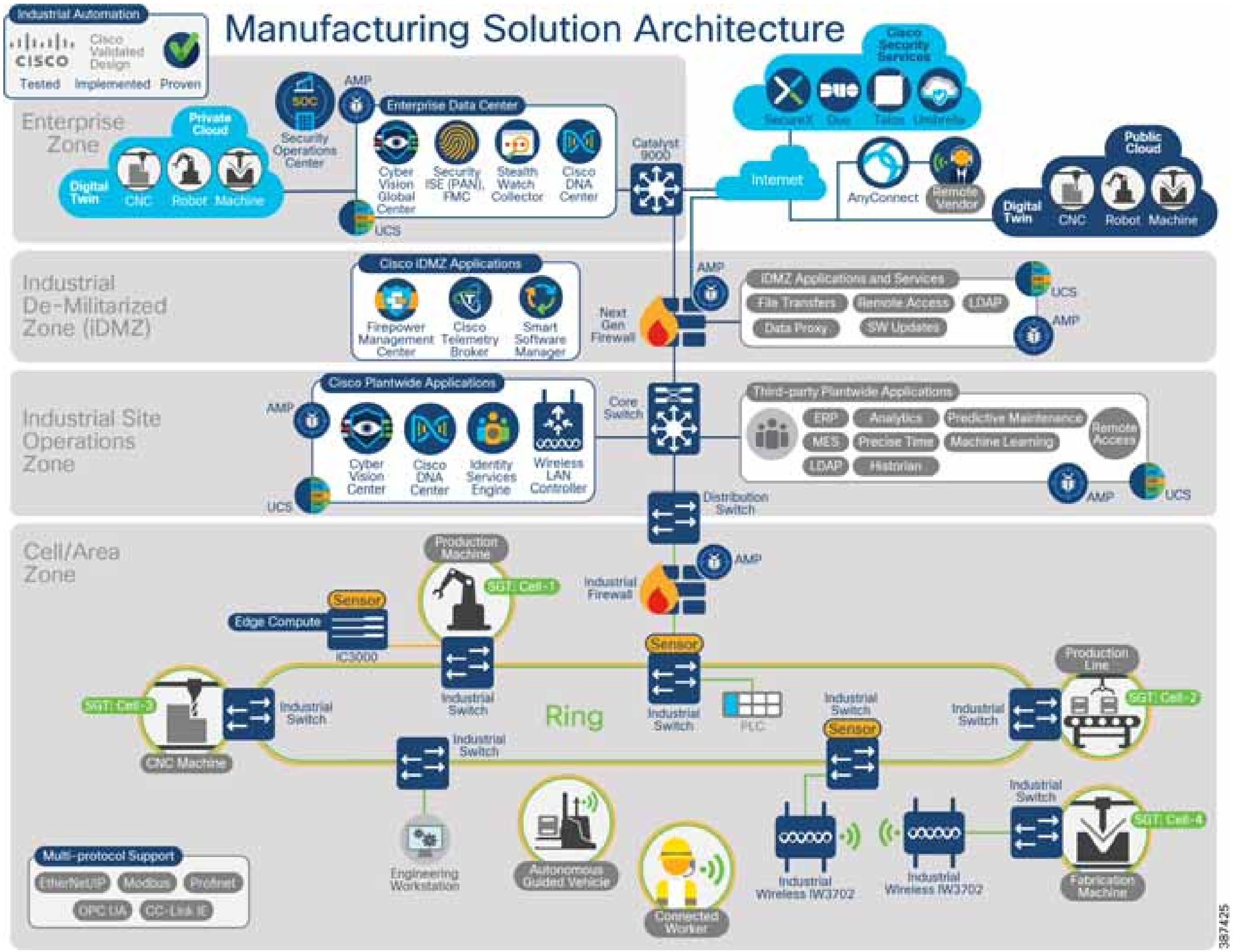
At a high level, key deliverables in this guide include:

- Architecture and design overview
- A list of system components as well as design recommendations for their placement and deployment
- Cisco DNA Center design options relevant to Industrial Automation
- Deep dive on automation capabilities from Cisco DNA Center applicable to the management of Industrial network on a non-SDA deployment
- Description of assurance capabilities applied to this design and requirements for assurance
- A security workflow that integrates Cisco DNA Center, Cisco Identity Services Engine (ISE) and Cisco Cyber Vision sensor to provide secure access to the network based on a Zero-Trust model.

Design Overview

Figure 2 shows the new components in the industrial automation architecture and highlights the position in the architecture of the Cisco DNA Center. Figure 2 provides a logical view of the Industrial Automation architecture, a simplified design that needs to be customized for specific customer application and connectivity requirements.

Figure 2 Manufacturing Solution Architecture



The key additions represented in the above include:

- Deploying a Cisco DNA Center on-premises appliance as part of the industrial zone.
- Interfacing Cisco DNA Center with Cisco cloud services via IDMZ based data proxy service and on-premises Smart Software manager (SSM) for license information.
- Interfacing Cisco DNA Center with an Identify Services Engine (ISE) deployment.
- Monitoring and managing Cisco Industrial Ethernet (IE 2000 Series, Catalyst® IE3x00 Rugged Series, Catalyst IE3400 Heavy Duty Series, and IE 4000 and IE 5000 Series) and Catalyst 9300 and 9500 Series switches. Although not all capabilities of Catalyst 9300 and 9500 are reflected in this guide.
- Integrating IACS device information discovered by Cyber Vision and interfaced into ISE.
- Deploying Cisco Telemetry Broker to scalably convey network and security telemetry data beyond the industrial zone.
- Updating the industrial DMZ firewalls to the Cisco Firepower® 2110 Series supporting Cisco SecureX Threat Response and Secure Firewall Management Center (FMC).

DNA Center is also widely used to manage wireless (WiFi) networks in the Enterprise. Enterprise wireless deployments are often extended into production environments and may be used to support Industrial Automation and Control applications. Another key benefit of deploying DNA Center may be to manage wireless networks in the production environment. Other Industrial Automation and CPwE design and implementation guidance covers wireless networking for production environments. However, this design guidance does not specifically consider DNA Center for production wireless deployments.

Key Design Considerations for DNA Center

We recommend Cisco DNA Center is added as an application in the industrial Site Operations Zone. The rationale behind this decision is threefold:

- DNA Center performs critical functions to maintain the operational status of the production environment, a key design guide for establishing which applications are part of the Industrial Zone. Those critical functions include Assurance and monitoring of the production network, guided remediation of identified problems and device replacement.
- A separate instance for production environments helps ensure operational requirements are maintained. Production environments have significantly higher and different operational requirements than Enterprise system. A DNA Center instance that supports both Enterprise and Production networks may lead to inadvertent changes or updates impacting the production system that could lead to downtime.
- DNA Center in the industrial zone simplifies Performance requirements and keeps communication flows between Cisco DNA Center and Cell/Area Zone switches in one network, below the IDMZ, thus making it easier to meet design recommendations covered on Networking and Security in Industrial Automation Environments Design and Implementation Guide.

Note: Adding Cisco DNA Center to the industrial zone is recommended in this design for the reasons stated above but ultimate decision on location should be made considering the specific customer requirements. If DNA Center is deployed outside the IDMZ to support multiple production environments, we still strongly recommend a separate deployment for Production than Enterprise network management. In any case, it is important to understand operational impacts, scale requirements, latency consideration and communication flows as explained later in this document.

A key IA IDMZ design principle restricts communication directly from industrial zone to the Internet. Therefore, Cisco DNA Center must not communicate directly with cloud-based services. To achieve this, two elements are introduced on the IDMZ:

- It is recommended to use an IDMZ-based proxy service to provide external communication to Cisco DNA Center. Cisco DNA Center is configured to access the Internet to download software updates, licenses, and device software, as well as provide up-to-date map information, user feedback, and so on. Providing internet connections for these purposes is a mandatory requirement. However, access can be provided securely through an HTTPS proxy server deployed in the IDMZ.
- It is recommended to install Cisco Smart Software Manager On-Prem on the IDMZ. This will allow for SSM to synchronize directly with Cisco cloud. Cisco DNA Center will connect to SSM to check license compliance.

Cisco DNA Center is tightly integrated with ISE to provide access control and security policy. Cisco Identity Services Engine provides details and considerations.

Figure 2 shows Cisco Cyber Vision components placement in the network. If Cisco Cyber Vision Global Center is used, it is placed in the Enterprise Zone; Cisco Cyber Vision Center is deployed in the Industrial zone and communicates with the sensors in the Cell/Area Zone as well with the ISE in the Industrial zone. Finally, sensors are deployed in Cell/Area Zones. For details on Cisco Cyber Vision design recommendations in Industrial environments refer to the Industrial Security Design Guide.

Note: Cisco DNA Center assists with deployment at scale, policy conformance and minimization of human errors, and “assurance and analytics” to continually monitor and alert service failure. Nevertheless, it is important to understand considerations and limitations as listed below.

The following is a list of other key considerations when adding Cisco DNA Center:

- Cisco DNA Center requires connectivity to all network devices it manages. That means that all devices that need to be discovered and monitored should have an IP address assigned that is routable and able to reach the Cisco DNA Center.

- As mentioned, Cisco DNA Center requires Internet connectivity and it is recommended to use a proxy. It is also recommended that you allow secure access via the proxy service only to URLs and fully qualified domain names required by Cisco DNA Center. For more details refer to: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/hardening_guide/b_dnac_security_best_practices_guide.html.

- If there is an industrial firewall between Cisco DNA Center and managed devices, make sure required ports are allowed on the firewall. Refer to Communication Flows for information on required ports.

Cell/Area Zone design as defined in the Networking and Security in Industrial Automation Environments Design and Implementation Guide should be preserved to provide operational requirements such as quality of service, resiliency, and low latency. For this reason, Cisco DNA Center is introduced on a traditional Industrial Automation network, or non-SDA (also referred as non-fabric in this guide).

- Latency should be equal to or less than 100 milliseconds to achieve optimal performance for all solutions provided by Cisco DNA Center. The maximum supported latency is 200ms RTT. Latency between 100ms and 200ms is supported, although longer execution times could be experienced for certain functions including Inventory Collection, SWIM, and other processes that involve interactions with the managed devices.

- Cisco ISE must be deployed with a version compatible with Cisco DNA Center. Refer the following link for compatibility information: https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-device-support-tables-list.html

- Cisco DNA Center is supported in single-node and three-node clusters. Scaling does not change based on the number of nodes in a cluster; three-node clusters simply provide high availability (HA). If the Cisco DNA Center node is deployed as a single-node cluster, wiring, IP addresses, and connectivity should be planned and configured with future three-node clustering in mind. In a single-node cluster, if the Cisco DNA Center appliance becomes unavailable, an SD-Access network provisioned by the node still functions. However, automated provisioning capabilities and Assurance insights are lost until the single node availability is restored.

- Cisco DNA Center scale depends on number of managed devices and number of concurrent endpoints among others. For scale limits refer to https://cs.co/sda-resources.

Known Limitations

- At this point Cisco DNA Center does not support managing network devices with management IP address behind a Network Address Translation (NAT) boundary.

- Firewalls running Firepower Threat Defense (FTD) software are not supported on Cisco DNA Center, nevertheless devices connected behind an industrial firewall can be provisioned and managed by Cisco DNA Center.

- Cisco DNA Center does not support automated workflows or assurance for resiliency protocols such as PRP, HSR, REP, DLR. Switches can be still discovered by Cisco DNA Center and benefit from features such as software upgrades, compliance, and device assurance.

- Cisco DNA Center is not suitable to manage products by third party vendors. For a hardware support matrix refer to:

  https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-device-support-tables-list.html

Features Supported

This section provides an overview of some of the key Cisco DNA Center features that will be covered in this document:

- Existing switch discovery

- New switch onboarding
- Device Replacement
- Software Upgrades for network infrastructure
- Software, configuration and security compliance for network infrastructure
- Switch configuration via Cisco DNA Center
- Monitoring of network devices and endpoint network status, including IACS devices
- Troubleshooting and remediation tools provided by Cisco DNA Center
- Network insights
- Security analytics

Products Supported

The following link contains information on devices supported by Cisco DNA Center.

Compatibility Matrix:
https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-device-support-tables-list.html

System Components

The following section introduces the system components listed below. It also provides an overview on TrustSec and Netflow concepts that are used during this guide. Integrating Cisco DNA Center into the Industrial Automation Architecture provides guidance and recommendations on where and how to add the components to the Industrial Automation Architecture.

System components:

- Cisco DNA Center for management of network devices
- ISE for AAA and policy management
- Cisco Cyber Vision for endpoint visibility and to provide context for endpoint authorization
- Cisco Smart Software Manager On-Prem for smart licensing
- HTTPS Proxy for secure connectivity to the cloud

Cisco DNA Center

Cisco DNA Center is a powerful network controller and management dashboard that lets you take charge of your network, optimize your Cisco investment, secure your network, and lower your IT spending. Full automation capabilities for provisioning and change management are enhanced with AI/ ML enhanced analytics that pull telemetry from everywhere in the network.

Cisco DNA Center components:

- Cisco DNA Center hardware appliance—Cisco DNA Center software runs on Cisco DNA Center hardware appliance. The appliance is available in form factors sized to support different size deployments.

- Cisco DNA Center Software—Cisco DNA Center is the centralized manager running a collection of applications and services powering the Cisco Digital Network Architecture. Cisco DNA begins with the foundation of a digital-ready infrastructure that includes routers, switches, access-points, and Wireless LAN controllers. Automation, Analytics, Visibility, and management of the Cisco DNA network is enabled through Cisco DNA Center Software.

Cisco DNA Center centrally manages major configuration and operations workflow areas.

- Design-Configures device global settings, network site profiles for physical device inventory, DNS, DHCP, IP addressing, software image management (SWIM) repository, device templates, and telemetry configurations such as Syslog, SNMP, and NetFlow.
- Policy-Defines business intent including creation of virtual networks, assignment of endpoints to virtual networks, policy contract definitions for groups, and configures application policies (for example, QoS).
- Provision-Provisions devices and adds them to inventory for management, supports Cisco Plug and Play, provisioning flows, and other automation flows.
- Assurance-Enables proactive monitoring and insights to confirm user experience meets configured intent, using network, client, and application health dashboards and issue management.
- Platform-Allows programmatic access to the network and system integration with third-party systems via APIs by using feature set bundles, configurations, a runtime dashboard, and a developer toolkit.

Cisco DNA Center appliance has four interfaces to provide network access:

- Enterprise port (Required)—The purpose of this port is to enable Cisco DNA Center to communicate with and manage your network. In this architecture, the “enterprise interface” connects to the industrial network infrastructure.
- Management Port (Optional)—it provides access to the Cisco DNA Center GUI, allowing users to use the software on the appliance. If you have a separated management network, connect the Cisco DNA Center management and enterprise interfaces to your management and industrial networks, respectively. Doing so ensures network isolation between services used to administer and manage Cisco DNA Center and services used to communicate with and manage your network devices.
- Cluster Port (Required)—The purpose of this port is to enable communications among the primary and add-on nodes in a cluster.
- Cloud Port (Optional)—Use it only if you cannot connect the appliance to the Internet (including to your Internet proxy server) using the enterprise port. This interface is not used on this design since cloud connectivity is achieved via proxy.

Licensing

For a device to be authorized to send data to Cisco DNA Center, that device must be included in your company's Cisco DNA software license subscription. This data provides Cisco DNA Center with the real-time information it needs for the many functions it performs. Cisco encourages customers to purchase complete Cisco DNA Center functionality through a Cisco DNA Advantage license subscription. Limited Cisco DNA Center functionality is also available through a Cisco DNA Essentials license subscription. Cisco DNA Center manages product licenses for managed devices.

Scale Metrics

For current scale metrics, refer to Cisco DNA Center System Scale at: https://cs.co/sda-resources

TrustSec and Enhanced Segmentation

A key component for security implementations and detailed in IEC 62443-3-3 is segmentation of assets into group-based policies. What assets and users need to communicate within a Cell/Area Zone and external to the Cell/Area Zone across an industrial plant needs to be defined. Cisco TrustSec decouples access that is based strictly on IP addresses and VLANs by using logical groupings in a method known as Group-Based Access Control (GBAC). The goal of Cisco TrustSec technology is to assign a Scalable Group Tag (SGT) value to the packet at its ingress point into the network. A GBAC policy determines if communication flows between SGTs is allowed. The policy is enforced based on this tag information. An SGT is a form of metadata and is a 16-bit value assigned by ISE in an authorization policy when user, device, or application connects to the network.

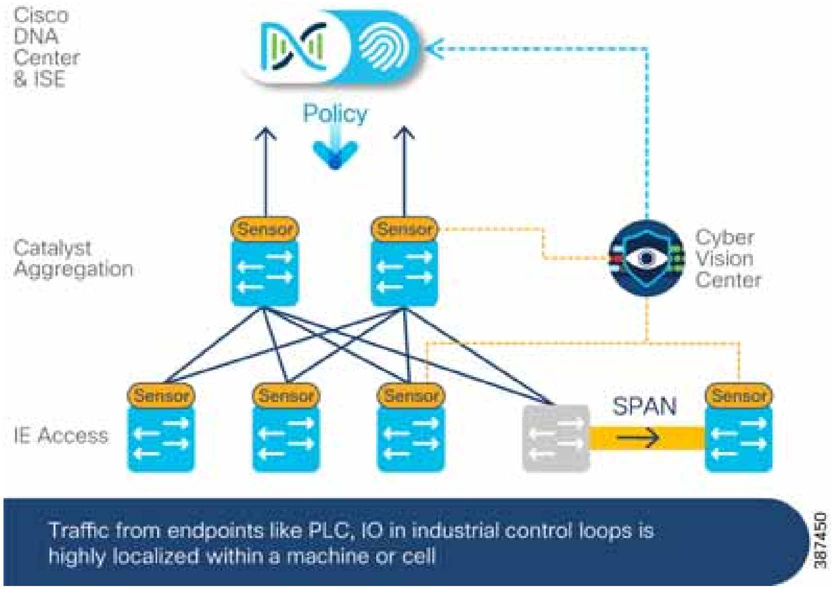
Segmentation using SGTs allows for simple-to-manage group-based policies and enables granular data plane isolation between groups of endpoints within a virtualized network. Using SGTs also enables scalable deployment of policy without having to do cumbersome updates for these policies based on IP addresses.

TrustSec is defined in three phases: classification, propagation, and enforcement. When the endpoint joins the network, an SGT is assigned (classification), the SGT is propagated in the network (propagation) to the enforcement points that control traffic based on tag information and policies (enforcement).

In the Industrial Automation solution, the following components are used to deploy TrustSec:

- Cisco Cyber Vision provides the visibility of the connected assets to Cisco ISE for effective classification.
- Cisco DNA Center is used as the pane of glass to manage and create SGTs and define their policies.
- Cisco ISE administers SGTs and policy.
- Cisco TrustSec-enabled industrial switches provide scalable segmentation across the industrial automation architecture. Different Industrial switches provide different levels of TrustSec support; for TrustSec support on Industrial switches refer to: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/software-platform-capability-matrix.pdf

Figure 3 TrustSec Components in Industrial Automation



Cisco Cyber Vision

Cisco Cyber Vision is an industrial cybersecurity solution specifically designed to ensure continuity, resilience, and safety of industrial operations. It provides asset owners with full visibility into their industrial automation and control systems (IACS) networks so they can ensure operational and process integrity, drive regulatory compliance, and enable easy deployment within the industrial network. Cisco Cyber Vision leverages Cisco industrial network equipment to monitor industrial operations and feeds other Cisco IT security platforms with OT context (for example, IACS device information) to build a unified IT and OT cybersecurity architecture.

Cisco Cyber Vision gives OT engineers real-time insight on the actual industrial process status, such as unexpected variable changes or controller modifications. They can take action to maintain system integrity and production continuity. Cyber experts can easily dive into all this data to analyze attacks and find the source. CISOs have all the information to document their incident reports. Cisco Cyber Vision “understands” the proprietary OT protocols used by automation equipment, so it can track process anomalies, errors, misconfigurations, and unauthorized industrial events. It also records everything and so serves as a kind of “flight recorder” of the industrial infrastructure.

Cisco Cyber Vision has the following components:

- Edge Sensors which are installed in the industrial network. These sensors are dedicated to capture network traffic, decode protocols using the Cisco Deep Packet Inspection engine and send meaningful information to the Cisco Cyber Vision Center.
- Cisco Cyber Vision Center, a central platform gathering data from all the Edge Sensors and acting as the monitoring, detection, and management platform.
- Global Center, an optional component, to which all Centers are connected, for a central view of all Centers deployed within an organization for alerting, reporting, and management functions.

For more information on Cisco Cyber Vision Center and design considerations for an Industrial network refer to Industrial Security Design Guide:
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/IA_Security/IA_Security_DG.html

Cisco Identity Services Engine

Cisco Identity Services Engine (ISE) is a secure network access platform enabling increased management awareness, control, and consistency for users and devices accessing an organization's network. ISE performs policy implementation, enabling dynamic mapping of users and devices to scalable groups, and simplifying end-to-end security policy enforcement. Within ISE, users and devices are shown in a simple and flexible interface. ISE can be installed on Cisco Secure Network Server (SNS) hardware or virtual appliances.

ISE Personas

ISE personas are simply the services and specific feature set provided by a given ISE node. The four primary personas are PAN, MnT, PSN, and pxGrid.

- Policy Administration Node (PAN)—A Cisco ISE node with the Administration persona performs all administrative operations on Cisco ISE.
- Monitor and Troubleshooting Node (MnT)—A Cisco ISE node with the Monitoring persona functions as the log collector and stores log messages from all the administration and Policy Service nodes in the network.
- Policy Service Node (PSN)—A Cisco ISE node with the Policy Service persona provides network access, posture, guest access, client provisioning, and profiling services.
- Platform Exchange Grid (pxGrid)—A Cisco ISE node with pxGrid persona shares the context-sensitive information from Cisco ISE session directory with other network systems such as ISE ecosystem partner systems and Cisco platforms. The pxGrid framework can also be used to exchange policy and configuration data between nodes like sharing tags and policy objects. TrustSec information like tag definition, value, and description can be passed from Cisco ISE to other Cisco management platforms such as Cisco DNA Center and Cisco Stealthwatch.

ISE supports standalone and distributed deployment models. Multiple, distributed nodes can be deployed together to provide failover resiliency and scale. The range of deployment options allows support for hundreds of thousands of endpoint devices. This guide uses the same ISE deployment as referred to in Networking and Security in Industrial Automation Environments Design and Implementation Guide.

Tech Tip: For additional ISE deployment and scale details, see ISE Performance & Scale on Cisco.com Security Community:
https://www.cisco.com/c/en/us/td/docs/security/ise/performance_and_scalability/b_ise_perf_and_scale.html

ISE performs the following functions relevant to this implementation:

- Profiling—Using MAC addresses as the unique identifier, ISE collects various attributes for each network endpoint to build an internal endpoint database. The classification process matches the collected attributes to pre-built or user-defined conditions, which are then correlated to an extensive library of profiles. These profiles include a wide range of device types, including mobile clients, desktop operating systems, and numerous non-user systems such as printers, phones, and cameras. Customized profiles can be created for industrial endpoints such as PLCs. Endpoint attributes are matched to conditions that can then match rules across a library of device types, or profiles. Based on a generic weighting scale, each matching condition can be assigned a different weight, or certainty factor, that expresses the relative value that the condition contributes to classification of the device to a specific profile. Although conditions may match in multiple profiles, the profile for which the endpoint has the highest cumulative certainty factor, or total certainty factor, is the one assigned to the endpoint. This policy is referred to as the Matched Policy, or the Endpoint Profile Policy. Once profiled, the endpoint policy can be directly referenced in Authorization Policy Rule conditions.

- Endpoint authentication and authorization—Authentication policies define the protocols that Cisco ISE uses to communicate with the network devices and the identity sources that it uses for authentication. The authentication method tested in this design guide for industrial endpoints is called MAC Authentication Bypass (MAB). MAB uses the MAC address of a device to determine what kind of network access to provide. This method is used to authenticate end devices that do not support any supplicant software in them, such as 802.1X EAP-TLS, EAP-FAST, and so on.

- Authorization policies are critical for determining what the user should access within the network. Authorization policies are composed of authorization rules and can contain conditional requirements that combine one or more identity groups. The permissions granted to the user are defined in authorization profiles, which act as containers for specific permissions. Authorization profiles group the specific permissions granted to a user or a device and can include attributes such as the SGT.

- SGT and role-based access control policy administration

Cisco DNA Center Integration

ISE integrates with Cisco DNA Center by using pxGrid and REST APIs (Representational State Transfer Application Programming Interfaces) for endpoint event notifications and automation of policy configurations on ISE. pxGrid is used to read all the data, and the REST API is used to write in ISE.

When integrating ISE with Cisco DNA Center the following occurs:

- PSN addresses are learned by Cisco DNA Center, and the Cisco DNA Center administrator associates the network sites to the applicable PSN. The PSN can then be used in the AAA settings when provisioning new network devices. Furthermore, the network device can be inserted and configured in ISE. If the device has TrustSec support, DNA Center will also configure CTS credentials.

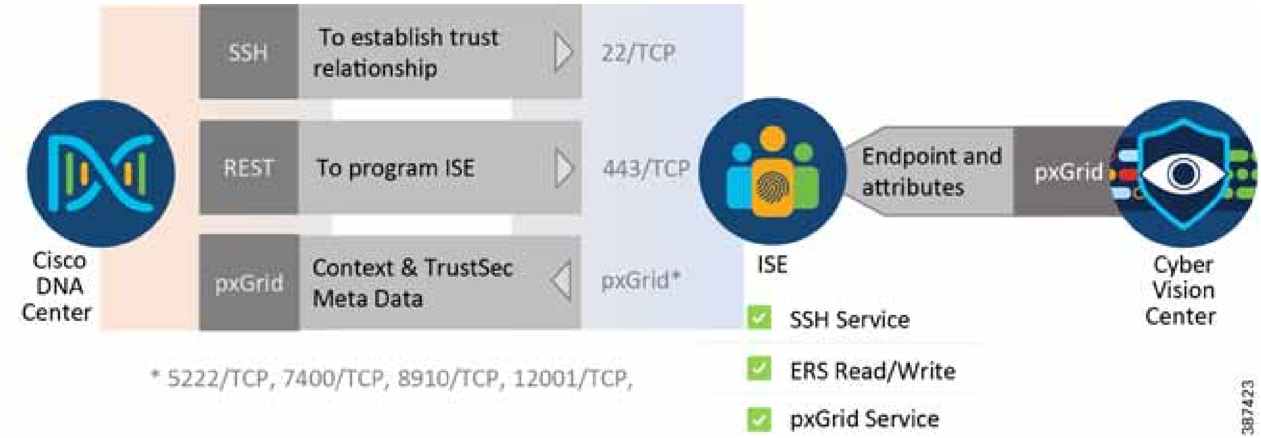
- While SGTs are administered by Cisco ISE through the tightly integrated REST APIs, Cisco DNA Center is used as the pane of glass to manage and create SGTs and define their policies. Group and policy services are driven by ISE and orchestrated by Cisco DNA Center's policy authoring workflows. Policy management with identity services is enabled in using ISE integrated with Cisco DNA Center for dynamic mapping of users and devices to scalable groups. This simplifies end-to-end security policy management and enforcement at a greater scale than traditional network policy implementations relying on IP access-lists.

- ISE provides context for endpoint assurance to provide additional device details.

- ISE provides information for endpoint analytics and policy analytics as described in Phase 4—Policy Analytics and Endpoint Analytics.

Figure 4 shows communication channels for Cisco DNA Center, ISE, and Cisco Cyber Vision Center.

Figure 4 Cisco DNA Center, ISE, and Cisco Cyber Vision Integration



As mentioned in Cisco Identity Services Engine, this guide follows the Networking and Security in Industrial Automation Environments Design and Implementation Guide where ISE is operating on a distributed deployment model as described below:

- One Primary Administration/Secondary Monitoring node
- One Secondary Administration/Primary Monitoring node
- One or several PSN in the Enterprise Zone
- One or several PSN in the Industrial Zone with pxGrid enabled

When integrating an existing ISE to a Cisco DNA Center in the deployment model described, the ISE PAN to Cisco DNA Center communication needs to be explicitly allowed on the IDMZ firewall. For required ports refer to Communication Flows.

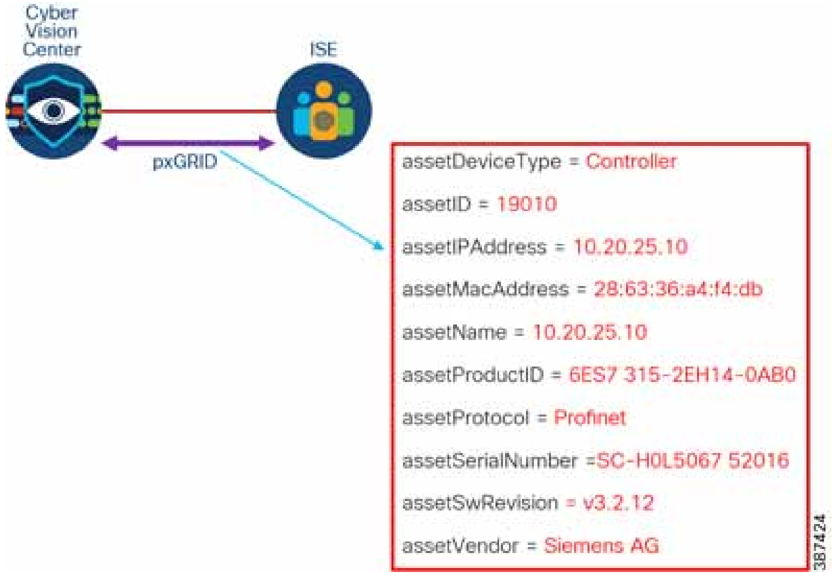
Cisco DNA Center to Cisco ISE latency requirement is maximum 200ms round trip. If meeting this requirement is not possible on a distributed deployment, consider a stand-alone ISE deployment on the industrial zone.

Note that when integrating Cisco DNA Center with ISE, Cisco DNA Center will be the policy administration authority. As a result, the Cisco ISE user interface pages for Scalable Groups, Access Contracts, and Policies will be read-only. The setting can be changed so policies and SGTs are managed from ISE instead. This may be desired when using multiple TrustSec policy matrices. Currently, Cisco DNA Center supports a single matrix.

Cisco Cyber Vision Integration

Cisco Cyber Vision assists ISE in device profiling. In the case of IACS assets, the built-in ISE probes will not be able to get all the information from the IACS asset to create a granular profiling policy because IACS assets may not support some traditional IT protocols that ISE relies on to profile the device. To gain visibility of IACS assets, the Industrial Automation solution uses Cisco Cyber Vision, which provides context of industrial operations and systems. Cisco Cyber Vision Center shares endpoints and attributes with ISE using pxGrid as described in Networking and Security in Industrial Automation Environments Design and Implementation Guide as shown in Figure 5

Figure 5 Cisco Cyber Vision Exporting Attributes to ISE



assetDeviceType = Controller

assetID = 19010

assetIPAddress = 10.20.25.10

assetMacAddress = 28:63:36:a4:f4:db

assetName = 10.20.25.10

assetProductID = 6ES7 315-2EH14-0AB0

assetProtocol = Profinet

assetSerialNumber =SC-H0L5067 52016

assetSwRevision = v3.2.12

assetVendor = Siemens AG

The integration between Cisco Cyber Vision and ISE provides the following benefits:

- Automatically enrolls IACS assets into the ISE endpoint database.
- Enables an OT-IT security administrative team to create granular profiling policies based on the attributes received from Cisco Cyber Vision.
- Allows the OT engineers to leverage the integration between Cisco Cyber Vision and ISE to automatically deploy new security policies in the network.

Cisco Smart Software Manager On-Prem

Cisco DNA Center manages device licenses using Smart Licensing. Cisco Smart Software Manager On-Prem, formerly known as Cisco Smart Software Manager satellite, is a component of Cisco Smart Licensing that works in conjunction with Cisco Smart Software Manager (SSM). It offers near real-time visibility and reporting of the Cisco licenses you purchase and consume while giving security-sensitive organizations a way to access a subset of Cisco SSM functionality without using a direct Internet connection to manage their install base.

Note: On-Prem must synchronize with Cisco SSM periodically to reflect your latest license entitlements. It can be directly connected to Cisco.com or disconnected but synchronized with Cisco SSM via file upload and download.

The following are the required ports:

- User Interface—HTTPS (TCP port 8443)
- Product Registration—HTTPS (TCP port 443), HTTP (TCP port 80)

Note: Currently Cisco DNA Center does not manage licenses on devices without support for smart licensing. The following industrial ethernet switches do not support smart licensing: IE2000, IE4000, IE4010, and IE5000. The default license in those devices is lanbase Right To Use (RTU) permanent license. If ipservices is required, it needs to be activated on the switch. For more information on RTU licenses refer to: https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie4010/software/release/15-2_4_EC/configuration/guide/scg-ie4010_5000/swintro.html

Proxy

By default, Cisco DNA Center is configured to access the Internet to download software updates, licenses, and device software, as well as provide up-to-date map information, user feedback, and so on. Providing internet connections for these purposes is a mandatory requirement.

Using an HTTPS proxy server is a reliable way to access remote URLs securely. We recommend that you use an HTTPS proxy server to provide the appliance with the access it needs to the URLs listed in Required Internet URLs and Fully Qualified Domain Names. Refer to this link for required URLs and FQDN access: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/install_guide/2ndgen/b_cisco_dna_center_install_guide_2_2_3_2ndGen/m_plan_deployment_2_2_3_2ndgen.html?bookSearch=true#concept_z4t_cd3_sfb

Currently, the appliance supports communication with proxy servers over HTTP only. The proxy server communicates with the internet using HTTPS, while the appliance communicates with the proxy server via HTTP.

NetFlow

NetFlow is a protocol for exporting metrics for IP traffic flows. NetFlow data is sent from a flow exporter to a flow collector. Services and applications that serve as NetFlow collectors are designed to receive the NetFlow data sent from exporters, aggregate the information, and provide data visualization and exploration toolsets.

In this design guide, NetFlow is used to provide Group-Based Access Control policy analytics. NetFlow export enabled on industrial switches provides network visibility into the traffic within the Cell/Area Zone. Cisco DNA Center acts as flow collector and correlates flow information by context provided by ISE. NetFlow is available on the Cisco 3400, Cisco IE3300, Cisco IE 4000, Cisco IE 4010, and Cisco IE 5000 switches.

NetFlow Recommendations

It is recommended to enable NetFlow on access ports to provide complete flow visibility. Configuration can be done using templates from Cisco DNA Center.

As network traffic traverses the Cisco device, flows are continuously created and tracked. As the flows expire, they are exported from the NetFlow cache to the flow collector. The NetFlow configuration can include timers to determine when the device exports the flows; a flow is ready for export when it is inactive for a certain time (for example, no new packets are received for the flow) or if the flow is long-lived (active) and lasts greater than the active timer (for example, long FTP download and the standard CIP/IO connections). The device CPU can be impacted by the number of new flows, so it is important to follow these guidelines when configuring NetFlow:

- Active timers should be set based on the number of flows expected to reduce CPU Utilization. The higher the number of new expected flows, the higher the active timer should be, so flows are not removed before all are learned.
- Inactive timers should be set based on the nature of traffic; in other words if a packet matching a particular flow comes only once in 40s and inactive timeout is set to 30s, then the flow will be continuously deleted and re-added, causing high CPU utilization.
- For best performance, NetFlow should be deployed at the Edge where the total number of flows is around 200 to 400. A flow in created when a packet matches unique characteristics defined on the flow record configuration.

The recommended timeout for the Cisco IE 4000, Cisco IE 4010, Cisco IE 5000, and Cisco Catalyst 9300 switches is 60 seconds for the active timeout and 30 seconds for the inactive timeout. For the Cisco IE 3400, the recommendation for active timeout is the default (1800 seconds) and the inactive timeout higher than 600 seconds.

Hardware and Software Components

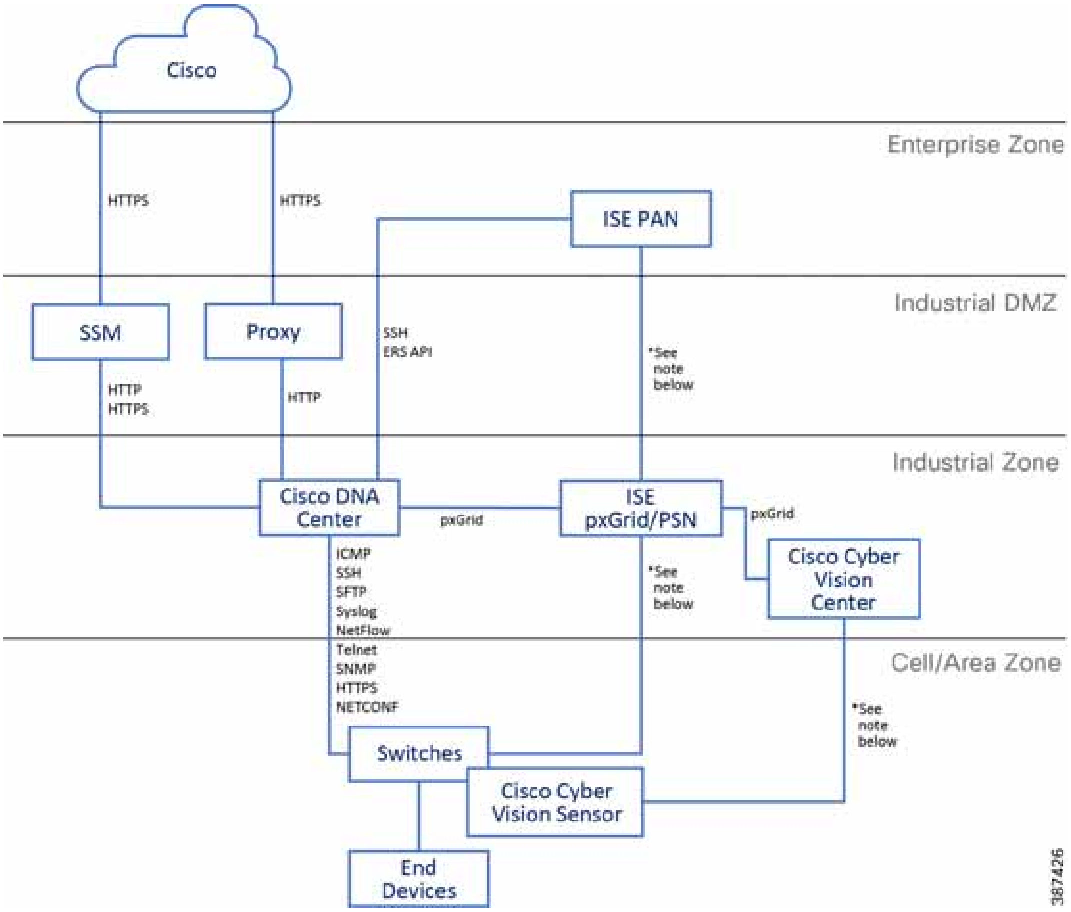
Table 1 Validated Cisco Hardware and Software Components

Product Role	Product	SW Version
Network management and monitoring	Cisco DNA Center Appliance DN2-HW-APL	2.2.3.3
Access Switch	Catalyst IE 3200/3300/3400	17.6.1
Access Switch	IE 4000/ IE2000	15.2(8)E1
Distribution Switch	Cisco IE 5000	15.2(8)E1
Distribution Switch	Cisco Catalyst 9200/9300	17.6.1
Core Switch	Cisco Catalyst 9400, 9500	17.6.1
Policy Management	Cisco ISE	2.7 Patch 1
Network Discovery/Visibility/Anomaly Detection	Cisco Cyber Vision Center/Sensors	4.0
On-Prem License server	Cisco Smart Software Manager On-Prem	8.0
IDMZ Firewall	FPR 2130	FTD 7.0
Firewall Management	FMC	7.0
Industrial Firewall	ISA 3000	FTD 6.7

Communication Flows

Figure 6 illustrates communication flows required for Cisco DNA Center in the Industrial Automation network. This information highlights relevant protocols for flows traversing the IDMZ or industrial firewalls.

Figure 6 Cisco DNA Center Communication Flows–Industrial Automation



Note: Figure 6 does not display ports needed for management access, ISE deployment, or Cisco Cyber Vision deployment. Refer to the following for additional information:

- Cisco ISE Ports Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/2-7/InstallGuide27/b_ise_InstallationGuide27/b_ise_InstallationGuide27_chapter_0110.html
- Industrial Security Design Guide (references Cisco Cyber Vision ports): https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/IA_Security/IA_Security_DG.html
- Cisco DNA Center Security Best Practices Guide (for a complete list of Cisco DNA Center communication ports) https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/hardening_guide/b_dnac_security_best_practices_guide.html

Cisco DNA Center Functions Applied to Industrial Automation Networks

The following section explores Cisco DNA Center components listed below and how they apply to industrial automation networks and industrial ethernet switches.

- Design–Cisco DNA Center Design Activities is used to provide general settings and profiles to the network. These settings are needed to use Cisco DNA Center for automation, assurance and policy.

- Automation–Cisco DNA Automation for Industrial Networks covers tasks that can be automated with Cisco DNA Center to reduce operation workload and apply network changes on a consistent and scalable way. Network automation is a journey to the end goal of achieving complete automation of network tasks based on business intent. On this design we show where we are in this journey and what tasks are completely automated while others need to be supported by customized templates created by the user.
- Assurance–Cisco DNA Assurance for Industrial Networks shows Cisco DNA Center network monitoring and analysis tools.
- Policy–Applying Security Policy to Industrial Automation Networks focuses on applying a consistent security policy to grant access to endpoints based on profile.

Cisco DNA Center Design Activities

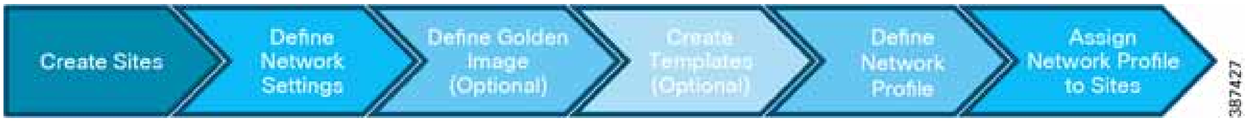
This section covers planning activities that are required in Cisco DNA Center before discovering and provisioning devices or using assurance.

This section assumes the DNA Center appliance has been installed and the software installed. Those topics will be covered in more detail in the DNA Center for Industrial Automation Implementation Guide. This section covers the following design activities:

- Establish the role-based access control in Cisco DNA Center, which is required to create users with right privileges to perform Cisco DNA Center tasks introduced in the guide.
- Define a network hierarchy by creating sites. Sites group devices by physical location and/or function in the network.
- Configure network settings that apply to those sites such as device credentials, DHCP, and NTP servers. These settings may be applied to devices that belong to a site as part of automation workflows. Refer to Adding Network Devices to Inventory.
- Create network profiles. In the case of switches, network profiles link configuration templates to sites.
- Manage software image repository for network infrastructure upgrades.

Figure 7 illustrates the design activities workflow covered in this document.

Figure 7 Design Activities Workflow


Create Sites
Define Network Settings
Define Golden Image (Optional)
Create Templates (Optional)
Define Network Profile
Assign Network Profile to Sites
387427

Role-based Access Control

Cisco DNA Center assigns users to roles that determine what types of operations a user can perform in the system. Cisco DNA Center comes with the following predefined roles:

- Network-Admin-Role–Users with this role have full access to all network-related Cisco DNA Center functions. They do not have access to system-related functions, such as application management, users (except for changing their own passwords), and backup and restore. This is recommended for users that need to perform device provisioning and configuration activities.
- Observer-Role–Users with this role have view-only access to all Cisco DNA Center functions. This is recommended for users that need visibility of inventory and assurance but do not need to apply changes to the network.

- Super-Admin-Role—Users with this role have full access to all Cisco DNA Center functions. They can create other user profiles with various roles, including those with the Super-Admin-Role. This user is for the system administrator. Limit the number of users with this access because they have complete control of the Cisco DNA Center deployment.

We recommend using the predefined roles:

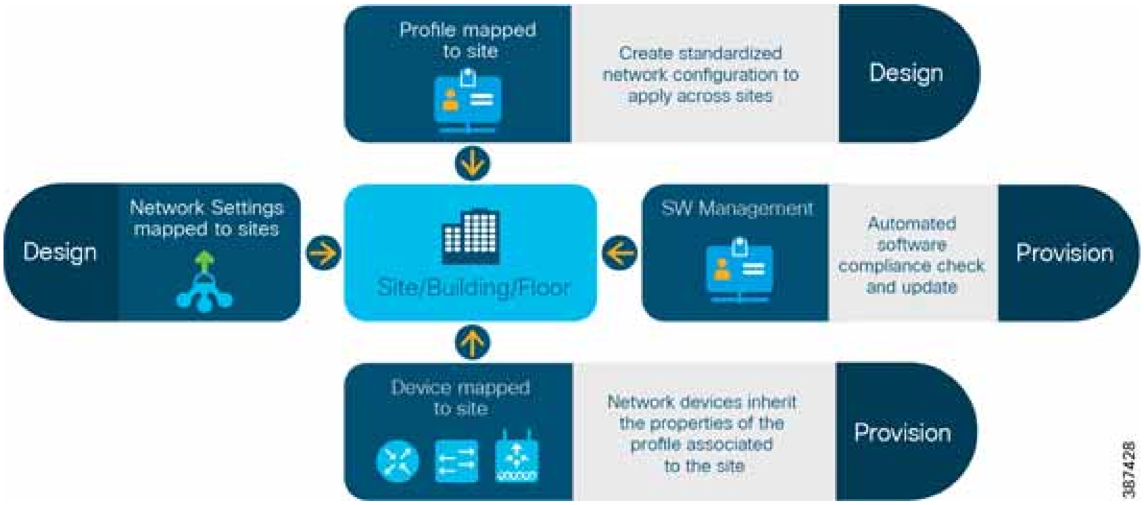
- Users that need to provision the network should use the Network-Admin-Role.
- Users that need assurance and inventory visibility should use the Observer-Role.
- Only Cisco DNA Center system administrators should use the Super-Admin-Role.

If a different role is needed, it is also possible to create customized roles to grant high-level access or granular functionality controls. When denying access to certain features, those features are removed from the user's interface for users in that role. When creating a customized role, make sure you understand the dependencies of the features. For more information refer to: https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-maintenance-guides-list.html

Network Hierarchy

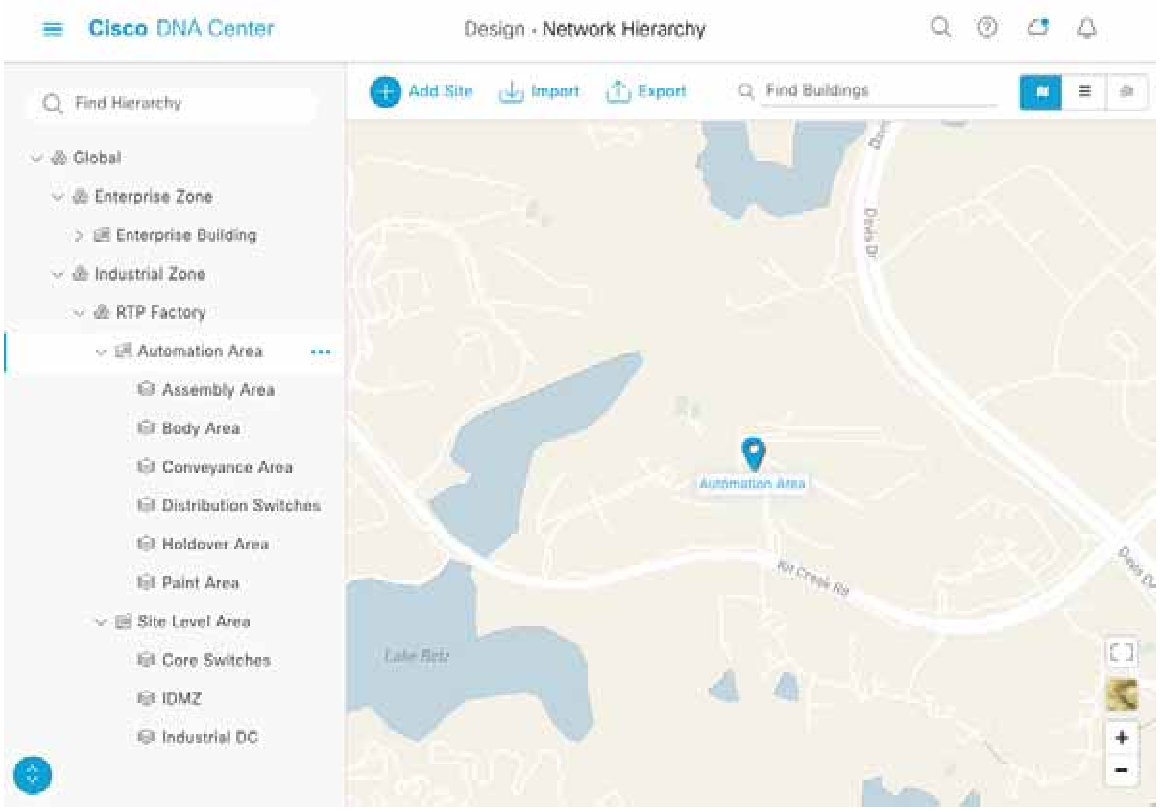
The network hierarchy represents your network's locations. It allows for a hierarchy of sites, which contain areas, which, contain buildings and floors. We refer to areas, buildings, and floors as site information. It is possible to create site information to easily identify where to apply design settings or configurations. A site on Cisco DNA Center determines which network settings, software images, and customized templates are applied to a device as illustrated in Figure 8.

Figure 8 Cisco DNA Center Hierarchy and Site Settings


Profile mapped to site
Create standardized network configuration to apply across sites
Design
Design
Network Settings mapped to sites
Site/Building/Floor
SW Management
Automated software compliance check and update
Provision
Device mapped to site
Network devices inherit the properties of the profile associated to the site
Provision
387428

For a production facility, the site information (area, building, floor) for Enterprise networks may not directly apply. We recommend these to be re-purposed to reflect the production facility. In this validated design a hierarchy is created for the Purdue model logical zones/areas in the production facility framework to guarantee network devices in a production area are configured consistently to perform desired function. When creating a network hierarchy consider creating sites based on physical location as well as logical characteristics (Plant Logical Framework). Devices with the same site information get the same configuration settings and templates, so it may make sense to create “floors” for different production functions, as depicted in Figure 9. The site information can also be used to filter when selecting devices for upgrades, monitoring network health, and displaying topology view, among other functions. Figure 9 illustrates an example for network hierarchy design.

Figure 9 Network Hierarchy



Tech Tip: Additional granularity can be achieved inside a site by using tags. Network devices can be tagged to group devices. This may be useful in case different configurations are needed for devices in the same site, troubleshooting, software activation, and so on. Tags are used to filter on the inventory menu. An example of how to use tags to push configuration to a group of devices is shown in Apply Configuration Changes with Day-N Templates.

Network Settings

Network Settings define common parameters for the site such as DHCP, DNS, AAA, NTP, device credentials, and so on. Settings can be defined globally and overridden per site. The following section describes settings that can be defined for provisioning and managing the industrial automation network. Adding Network Devices to Inventory explains how these settings are configured on the network devices.

Device Credentials

Device credentials refer to the CLI, SNMP, and HTTPS credentials that are configured on network devices. Cisco DNA Center uses these credentials to discover and collect information about the devices in your network. In Cisco DNA Center, you can specify the credentials that most of the devices use so that you do not have to enter them each time you run a discovery job. These credentials are also applied to unconfigured devices when provisioning via Cisco Plug and Play (PnP).

Network

It is possible to define site network services that become the default for the entire site and may be pushed to managed devices as covered in Device Inventory Provisioning. Some available services are DHCP, NTP, DNS, and AAA.

The AAA service can be defined for network and/or client and endpoint authentication. Once Cisco DNA Center is integrated with ISE. An ISE PSN node IP address can be selected from available PSNs on deployment.

Telemetry

The Cisco DNA Center Telemetry function polls network devices and collects telemetry data according to the following telemetry settings: SNMP server, syslog server, NetFlow Collector, or the wired client. With Cisco DNA Center, you can configure telemetry settings on network infrastructure when devices are assigned to a specific site. To understand how these settings are configured on devices refer to Adding Network Devices to Inventory.

Note: Cisco DNA Center is the default SNMP collector. It polls network devices to gather telemetry data.

Table 2 Telemetry Data Setting Options

Setting	Purpose	Configuration Options
SNMP	Defines SNMP trap server for the site	By default, Cisco DNA center is selected. External SNMP trap servers can be added. We recommend using the default setting.
Syslog	Defines syslog server for the site	By default, Cisco DNA center is selected. External syslog server can be added. We recommend using the default setting.
Wired Client Data Collection	Determines if devices on a site should be configured with IP Device Tracking (IPDT) The purpose of IPDT is for the switch to obtain and maintain a list of devices that are connected to the switch via an IP address To do this IPDT sends unicast Address Resolution Protocol (ARP) probes with a default interval of 30 seconds to the connected hosts	Starting 2.1.2.4, Cisco DNA Center introduces flexibility to enable or disable IPDT under Telemetry Settings. When enabled, IPDT is applied to all access interfaces on the switch. We recommend enabling wired client data collection. Additional considerations are explained later in the document.
NetFlow	It is used to create flow collector used for application telemetry and GBAC analytics.	By default, Cisco DNA center is selected but external collectors can be added. Our recommendation is not to configure this setting for sites with industrial switches only. See Tech Tip below.

Tech Tip: The Only NetFlow configuration applied when assigning a device to a site is the NetFlow collector, which is not enough to send NetFlow data. To complete NetFlow configuration, application telemetry needs to be enabled for the device in inventory. Application telemetry is not currently supported on Industrial Switches. For this reason, it is recommended to leave this telemetry setting unconfigured. If GBAC analytics is required, NetFlow configuration should be done via templates. Refer to Apply Configuration Changes with Day-N Templates.

Network Profiles for Switching

Network profiles are a key concept in Cisco DNA Center to standardize configurations for routers, switches, and WLCs in one or multiple sites. In the case of switches, A profile is used to assign configuration templates to devices based on their site information, device product family, and associated tags. For devices that require a similar configuration, a template helps to reduce the configuration time by using variables and logic statements as placeholders for any unique settings.

There are two types of templates that can be associated to a network profile:

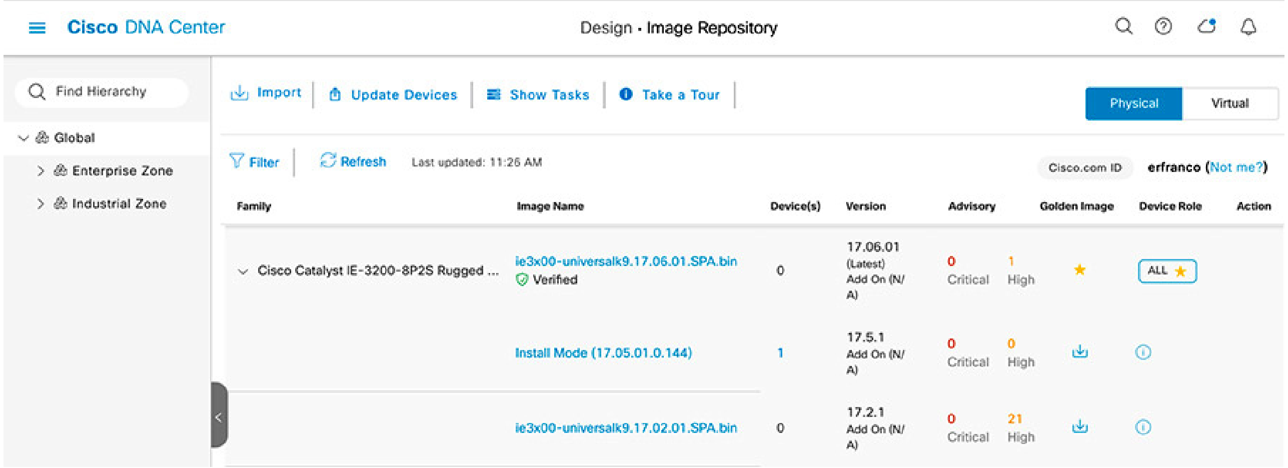
- Onboarding configuration templates must be created with the configuration to be applied to a new device when using PnP provisioning as described on PnP Workflow. Onboarding templates can use variables to define device specific settings.

- Day-N templates are used to push configuration changes to devices already in Cisco DNA Center inventory. Day-N templates can use variables that are bound to inventory settings on the device. This may be useful to select specific settings from the device from a drop-down menu. For example, binding a variable to the interfaces on a device will display all available interfaces.

Image Repository

Cisco DNA Center stores all the unique software images according to image type and version. It is possible to view, import, and delete software images.

Figure 10 Image Repository



Family	Image Name	Device(s)	Version	Advisory		Golden Image	Device Role	Action
Cisco Catalyst IE-3200-8P2S Rugged ...	ie3x00-universalk9.17.06.01.SPA.bin Verified	0	17.06.01 (Latest) Add On (N/A)	0 Critical	1 High	★	ALL ★	
	Install Mode (17.05.01.0.144)	1	17.5.1 Add On (N/A)	0 Critical	0 High			
	ie3x00-universalk9.17.02.01.SPA.bin	0	17.2.1 Add On (N/A)	0 Critical	21 High			

Not Applicable Design Settings

IP address pools, SP Profiles, and Wireless network settings and authentication templates in the Design menu are not covered in this guide because they are not applicable to the design.

DNA Center Design Overview—Summary

In the sections above, a number of concepts and terms were reviewed. Table 3 lists some of the key device variables or characteristics and how they impact various DNA Center functions.

Table 3 Device Characteristics on Cisco DNA Center

Device Characteristic	Required (Y/N)	Defined by	Values/Examples	Impact
Site Information - Area, Building, Floor	Y	User	Area—Production Building Industrial—Cell/Area zone Floor—Paint, Assembly	Device configuration based on associated profiles Network Settings Telemetry Settings Visibility and filtering

Table 3 Device Characteristics on Cisco DNA Center

Product Family	Y	Cisco	Pre-defined, e.g., IE3400	Golden Image Device Configuration
Device Role	Y	Cisco	Core, Distribution, Access	Visibility and filtering
Tags	N	User	e.g. Zone switch	Device Configuration Visibility and filtering

Cisco DNA Automation for Industrial Networks

This section covers automation flows available in Cisco DNA Center that are applicable to Industrial Automation networks, including:

- Adding existing devices to inventory through discovery or PnP
- Enabling telemetry for assurance
- Provisioning switches with site settings
- Applying configuration changes with Day-N templates through inventory provisioning
- Replacing devices
- Upgrading software images
- Checking compliance for network devices
- Visualizing Topology

Adding Network Devices to Inventory

To manage a device using Cisco DNA Center, the device needs to be added to the inventory as described in the following section.

- Existing devices are added via discovery. Brownfield refers to devices that belong to existing sites with pre-existing configuration and are added to Cisco DNA Center through discovery. The Discovery feature scans the devices in the network and sends the list of discovered devices to Inventory.
- New devices are added via PnP. PnP is used for Zero Touch Deployment (ZTD) of new, unconfigured devices in the network. PnP uses the sites network profile to configure devices.
- Offline new switch provisioning. To use PnP for configuration, switches need to be connected to the network. In some cases, this is not always possible in an Industrial Automation environment, and a switch needs to be provisioned before providing network connectivity. For this scenario we describe an offline workflow, where a switch gets basic configuration via CLI or other management tools such as Device Manager and is discovered by Cisco DNA Center when network connectivity is established.

When a network device is added to inventory, it is assigned a default device role, such as access, core, or distribution. The default role may be modified. The role is used to identify and group devices according to their responsibilities and placement within the network.

Tech Tip: Industrial ethernet switches and Catalyst 9300 are assigned an access role by default. Roles can be customized in the case of distribution switches for topology visualization. Note that modifying the role has implications on application policy (which may apply QoS settings) or encrypted traffic analytics configurations. Nevertheless, these two features are not used in this design as explained later in the document.

Before exploring the available workflows in detail, it is important to understand the following Cisco DNA Center concepts:

- Device Controllability
- Device Site Assignment
- Device Inventory Provisioning
- Telemetry Configuration

Note: These concepts are important to understand but do not represent a device onboarding workflow. For specific workflows refer to Discovery Workflow, PnP Workflow, and Offline Provisioning Workflow.

Device Controllability

Device controllability is a system-level process in Cisco DNA Center that enforces state synchronization for some device-layer features. Its purpose is to aid in the deployment of network settings that Cisco DNA Center needs to manage devices. When device controllability is enabled, changes are made on network devices when running discovery, when adding a device to inventory, or when assigning a device to a site. Device controllability is enabled by default but can be disabled. For a list of configurations that are added to the device when controllability is enabled refer to Figure 11.

Note: Device controllability can be enabled and disabled as needed but it is recommended to leave it enabled. When enabled, the telemetry configuration required for assurance is pushed to the devices (syslog messages, SNMP traps, and connected client information). Configuring telemetry settings does not impact the operation of the device or any of its ports. Discovery Workflow contains limitations and recommendations for brownfield devices.

When device controllability is disabled, Cisco DNA Center does not configure any of the credentials or features on devices while running discovery or when the devices are assigned to a site. However, the telemetry settings and related configuration are pushed when the device is “provisioned in inventory” or when Telemetry Settings are updated on the device. For details on operational impact, refer to Device Inventory Provisioning.

A device is added to Cisco DNA Center inventory via PnP or discovery. At this stage, if controllability is enabled and TrustSec is supported on the device, CTS (Cisco TrustSec) credentials are added to the device. CTS credentials are used to specify the Cisco TrustSec device ID and password for the device, which is used in Network Device Admission Control (NDAC) authentication. NDAC is used for authenticating with other Cisco TrustSec devices (such as ISE) and for provisioning the PAC (Protected Access Credentials) with EAP-FAST.

Device Site Assignment

A device is assigned site information to associate specific site settings (network and telemetry settings, credentials, and golden software image), and configurations (templates defined on network profiles). When this happens, controller certificates for Cisco DNA Center are pushed to the device. Also, if device controllability is enabled, telemetry configuration will be added (SNMP trap, Syslog, NetFlow server definitions, and IPDT settings). In the case of IPDT, global configuration as well as per interface specific commands to access interfaces are applied.

Note that these settings are only applied to devices if configured as part of telemetry settings for the site, refer to Telemetry.

Device Inventory Provisioning

Provisioning a device in the inventory is a separate action performed from the Provision/Inventory menu. When provisioning a device that is not yet assigned to a site (e.g., the device was just discovered), site assignment can be done as part of provisioning. When a device is provisioned in the inventory, Cisco DNA Center configures the following settings (providing settings are defined for the site):

- AAA server information, CTS authorization commands, and radius server groups. In addition, Cisco DNA Center configures the device on the ISE PAN and propagates any subsequent updates to the device to ISE PAN.
- DHCP, domain name, and NTP configurations, which are configured as part of site network settings.
- Provisioning workflow also supports any Day-N templates which are created and attached to the site switching profile.

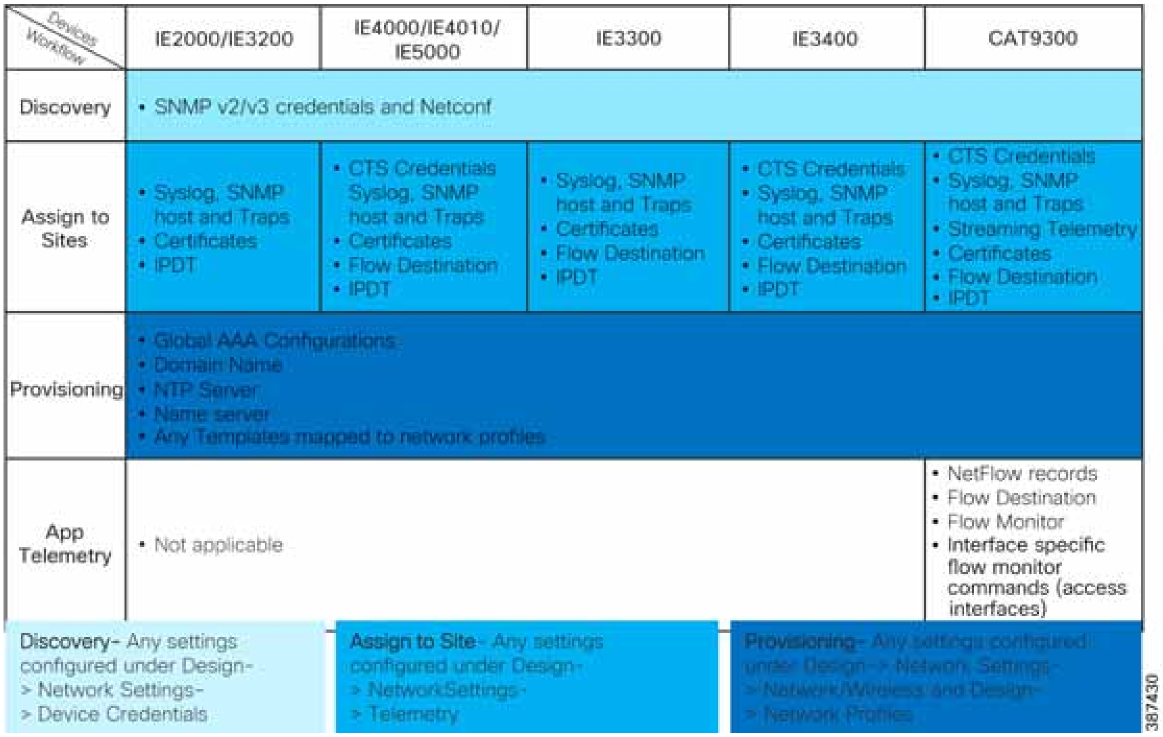
Device inventory provisioning does not cause device reload. Nevertheless, device configuration is changed at this time. For brownfield devices, configuration for AAA, CTS, DHCP, NTP, and DNS will be overwritten with the configuration defined for the site. The configuration may also be overwritten by configuration templates. The user should assess any operational impact and plan accordingly.

Tech Tip: Provisioning always pushes telemetry configuration and site settings to devices, even when device controllability is disabled. Before provisioning a device, a configuration preview is available, which helps verify the configuration before it is pushed to devices; if there are any misconfigurations, the configuration can be ignored.

Putting it all Together

When a device is added to Cisco DNA Center, there are inventory actions that when applied to the device could modify the configuration. Adding a device to a site pushes telemetry settings if controllability is enabled. Provisioning a device will configure site-wide settings and apply customized templates to devices. Figure 11 shows what settings get applied to the devices in the Industrial Zone when device controllability is enabled.

Figure 11 Device Controllability–What Gets Provisioned



Devices / Workflow	IE2000/IE3200	IE4000/IE4010/ IE5000	IE3300	IE3400	CAT9300
Discovery	• SNMP v2/v3 credentials and Netconf				
Assign to Sites	• Syslog, SNMP host and Traps • Certificates • IPDT	• CTS Credentials Syslog, SNMP host and Traps • Certificates • Flow Destination • IPDT	• Syslog, SNMP host and Traps • Certificates • Flow Destination • IPDT	• CTS Credentials • Syslog, SNMP host and Traps • Certificates • Flow Destination • IPDT	• CTS Credentials • Syslog, SNMP host and Traps • Streaming Telemetry • Certificates • Flow Destination • IPDT
Provisioning	• Global AAA Configurations • Domain Name • NTP Server • Name server • Any Templates mapped to network profiles				
App Telemetry	• Not applicable				• NetFlow records • Flow Destination • Flow Monitor • Interface specific flow monitor commands (access interfaces)

Discovery- Any settings configured under Design- > Network Settings- > Device Credentials

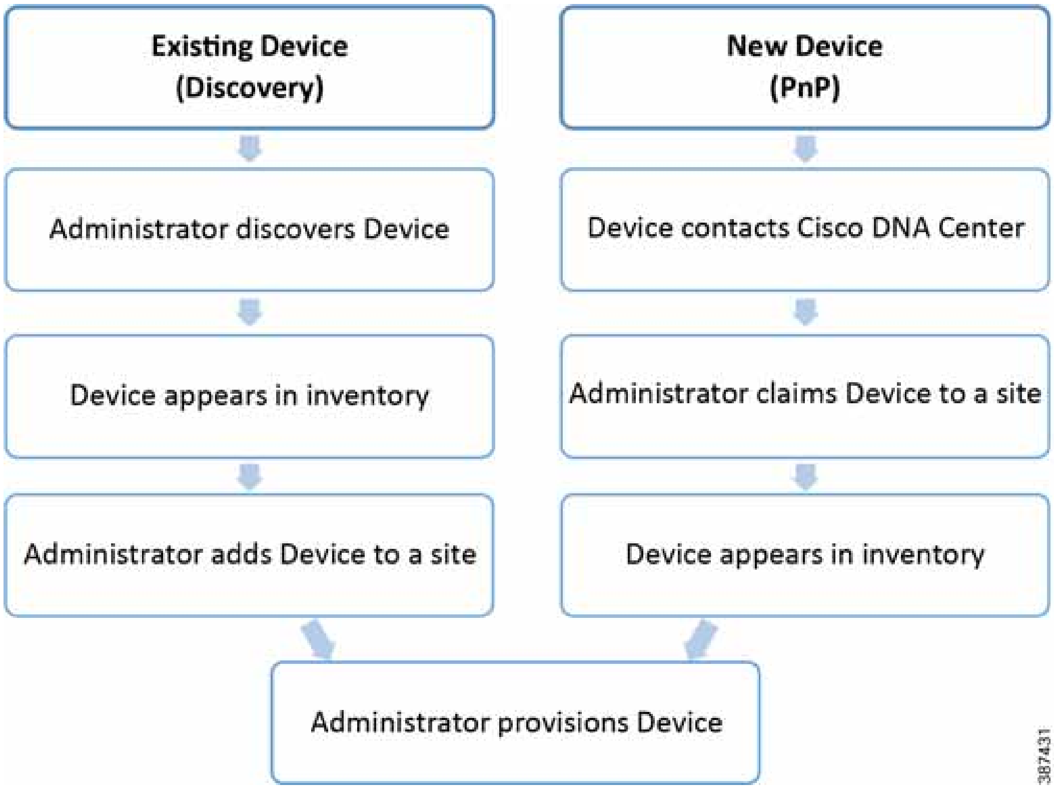
Assign to Site- Any settings configured under Design- > NetworkSettings- > Telemetry

Provisioning- Any settings configured under Design- > Network Settings- > Network/Wireless and Design- > Network Profiles

387430

Figure 12 illustrates the overall process for devices added via PnP or Discovery. Detailed workflows are covered in subsequent sections.

Figure 12 Inventory Actions Sequence


Existing Device (Discovery)
New Device (PnP)
Administrator discovers Device
Device contacts Cisco DNA Center
Device appears in inventory
Administrator claims Device to a site
Administrator adds Device to a site
Device appears in inventory
Administrator provisions Device
387431

Tech Tip: When Cisco DNA Center configures or updates devices, the transactions are captured in the Cisco DNA Center audit logs, which you can use to track changes.

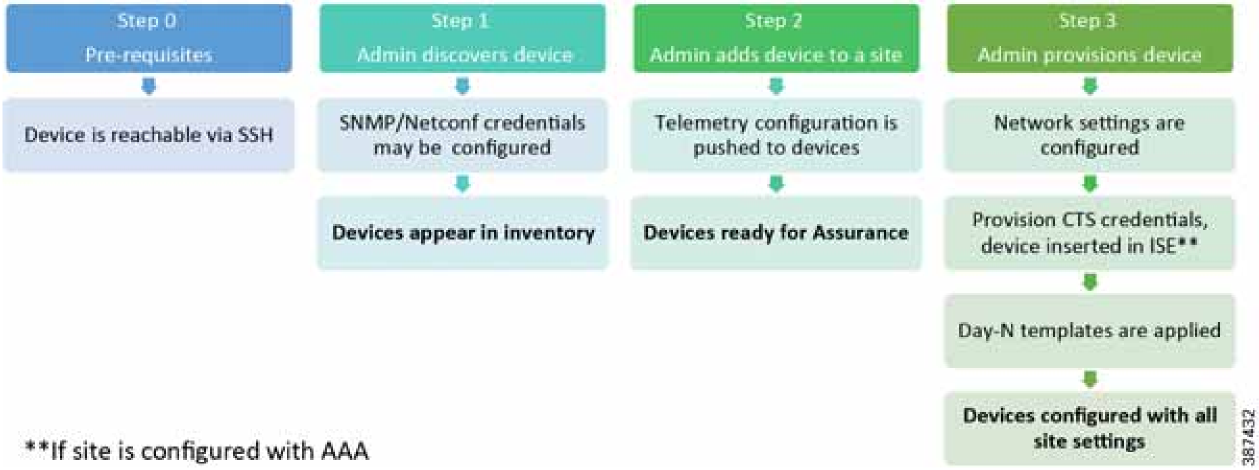
Discovery Workflow

Existing devices can be added in Cisco DNA Center using the Discovery tool. Discovery methods are IP address range, Cisco Discovery Protocol (CDP), or Link Layer Discovery Protocol (LLDP). When running a discovery task, CLI and SNMP read credentials are mandatory. Netconf discovery over SSH is optional. If not present, Cisco DNA Center provisions the respective Netconf and SNMP credentials to make the discovery successful.

Note: SSH and TELNET are supported but SSH is recommended for security.

After a device is discovered, it is assigned to the inventory and a network administrator can assign it to a site and provision it. When provisioning a device that is not yet assigned to a site, site assignment can be done as part of provisioning. See Figure 13 for device discovery workflow.

Figure 13 Device Discovery Workflow


Step 0
Pre-requisites
Device is reachable via SSH
Step 1
Admin discovers device
SNMP/Netconf credentials may be configured
Devices appear in inventory
Step 2
Admin adds device to a site
Telemetry configuration is pushed to devices
Devices ready for Assurance
Step 3
Admin provisions device
Network settings are configured
Provision CTS credentials, device inserted in ISE**
Day-N templates are applied
Devices configured with all site settings
**If site is configured with AAA
387432

Tech Tip: Cisco DNA Center supports discovery of multiple devices in a single discovery task. Site assignment and provisioning activities can be done in bulk.

It is possible to discover a device and add it to a site but skip provisioning to avoid adding configuration to the existing device. This will enable software upgrade, compliance, topology, and assurance features while leaving the switch unchanged. Note that site assignment will still add minimal telemetry configuration to the device when controllability is enabled. Pushing telemetry configuration is recommended since telemetry will provide information for assurance.

Discovery Workflow Caveats and Considerations

- When a device is already configured and new configuration is added by site assignment or inventory provisioning, some issues may arise. The following is a list of possible conflicts.
  - IPDT policy on a device will be overwritten in access ports. If previous configuration is preferred, disable IPDT on telemetry settings for the site so IPDT is not configured. As an alternative, use a template to append commands. Keep in mind that IPDT is required for endpoint assurance and TrustSec capabilities, among others.
  - If AAA configuration exists on the discovered device, provisioning a device into a site with AAA settings configured will generate an error for the AAA portion of provisioning. Either remove AAA settings from site so they are not configured on the discovered device or remove AAA commands from the switch before provisioning. This task can be automated via templates.
  - Provisioning a device that is already in the ISE network devices list could break the CTS trust between the device and ISE. If a device exists in ISE and is provisioned on a site with ISE settings, Cisco DNA Center won't update the device in ISE. Nevertheless, device CTS credentials will be updated in the device. Consequently, CTS trust cannot be established and policies cannot be downloaded. As a workaround, delete device from ISE before inventory provisioning or update CTS credentials manually in ISE (the new credentials are the serial number of the device).
- When IPDT is enabled on IE2000, IE4000, IE4010 and IE5000 switches it is recommended to modify the standard IP address used with the IPDT feature to avoid a known issue where endpoints report a duplicate IP address o 0.0.0.0. Refer to the following link for more details: https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/8021x/116529-problemsolution-product-00.html
- Devices running ring resiliency protocols MRP, REP, or HSR can be discovered and managed by Cisco DNA Center but neighbor information on assurance and topology pages may be incomplete.
- If an industrial switch running Cisco IOS XE that is booting from flash is discovered on Cisco DNA Center, there are additional steps to configure the switch to boot from sdflash before performing a software upgrade from Cisco DNA Center. Refer to Software Image Upgrade for more details.

- If you are using ISE as your AAA server, avoid using admin as the username for device CLI credentials, which can lead to username conflicts with the ISE administrator login, resulting in the inability to log in to devices.
- Devices running MRP, REP or HSR ring resiliency protocols can be discovered and managed by Cisco DNA Center but neighbor information on assurance and topology pages may be incomplete.

PnP Workflow

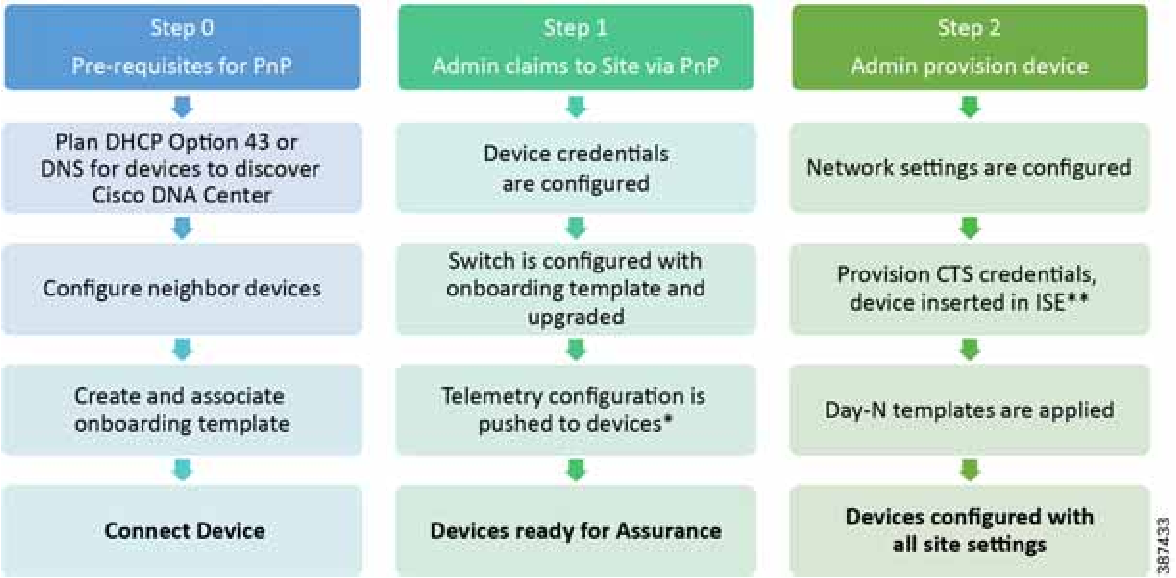
Cisco Plug and Play (PnP) provides a highly secure, scalable, and seamless ZTD experience. Cisco industrial switches that are running IOS or IOS-XE software have an embedded PnP agent that communicates with the PnP deployment server. The PnP agent runs on a device if no startup configuration exists, such as when a device is powered on for the first time or is reset to factory defaults. The PnP agent on the switch attempts to discover the PnP deployment server running on Cisco DNA Center via DHCP or DNS. The switch calls home and downloads the required software and device configuration.

If an unconfigured device is connected to the network and contacts Cisco DNA Center but an administrator has not previously added this device, an entry will be created for the device, but the device will be in an unclaimed state. It will remain in this state until it is claimed.

Alternatively, a device could be added before being connected to the network by adding the serial number and device family to Cisco DNA Center. At that point the device could be claimed to a site. When the device is connected to the network and reaches Cisco DNA Center, software image and configuration will be applied according to site settings.

The device is assigned to the site as part of the PnP workflow, and then the device can be provisioned in inventory. Figure 14 illustrates the PnP workflow from preparation steps to inventory provisioning.

Figure 14 PnP Workflow


Step 0
Pre-requisites for PnP
Plan DHCP Option 43 or DNS for devices to discover Cisco DNA Center
Configure neighbor devices
Create and associate onboarding template
Connect Device
Step 1
Admin claims to Site via PnP
Device credentials are configured
Switch is configured with onboarding template and upgraded
Telemetry configuration is pushed to devices*
Devices ready for Assurance
Step 2
Admin provision device
Network settings are configured
Provision CTS credentials, device inserted in ISE**
Day-N templates are applied
Devices configured with all site settings
387433

Tech Tip: Cisco DNA Center supports PnP of multiple devices at the same time. Claiming and provisioning activities can be done in bulk.

PnP Workflow Caveats and Considerations

- Only switches in linear topologies were validated as part of PnP provisioning workflow. PnP of switches on ring topologies (REP, MRP, and HSR) are not in the scope of this document.
- If a switch will be configured with Cisco Cyber Vision sensor follow steps outlined in Deploying Cisco Cyber Vision Sensor.

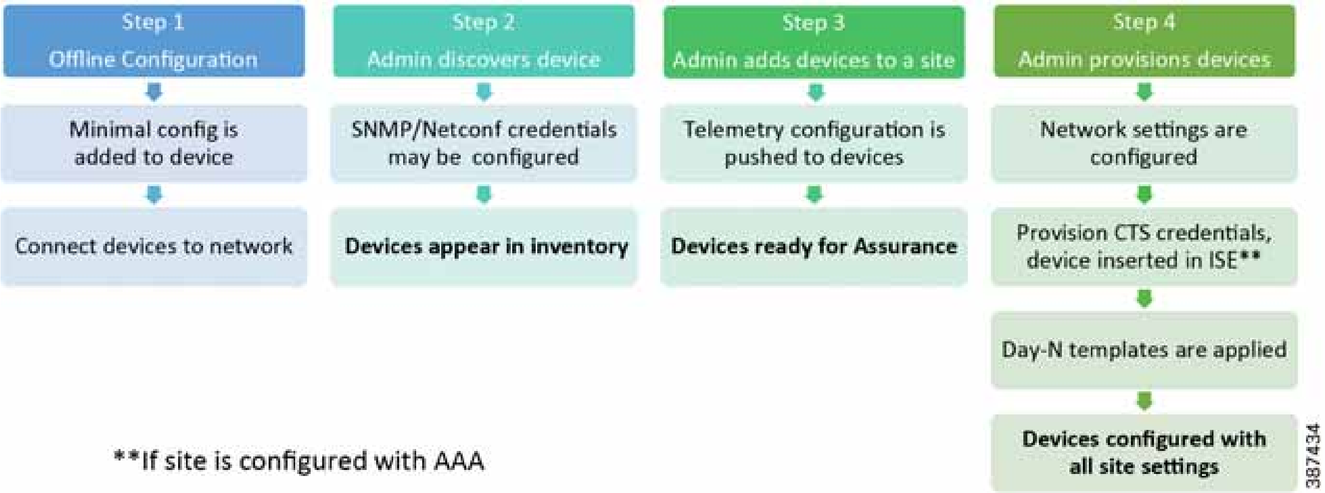
- Similarly to discovery considerations, if you are using ISE as your AAA server, avoid using admin as the username for device CLI credentials, which can lead to username conflicts with the ISE administrator login, resulting in the inability to log in to devices.
- When IPDT is enabled on IE2000, IE4000, IE4010 and IE5000 it is recommended to modify the standard IP address used with the IPDT feature to avoid known issue where endpoints report duplicate ip address 0.0.0.0. Refer to the following link for more details: https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/8021x/116529-problemsolution-product-00.html

Offline Provisioning Workflow

To use PnP for configuration, switches need to be connected to the network. In some cases, this is not always possible in an Industrial Automation environment, and a switch needs to be provisioned before providing network connectivity. In this scenario this design guide proposes an offline workflow, where a switch gets basic configuration via CLI or other management tools such as Device Manager and is discovered by Cisco DNA Center when network connectivity to Cisco DNA Center is established.

Figure 15 illustrates the proposed workflow.

Figure 15 Offline Provisioning Workflow


Step 1
Offline Configuration
Minimal config is added to device
Connect devices to network
Step 2
Admin discovers device
SNMP/Netconf credentials may be configured
Devices appear in inventory
Step 3
Admin adds devices to a site
Telemetry configuration is pushed to devices
Devices ready for Assurance
Step 4
Admin provisions devices
Network settings are configured
Provision CTS credentials, device inserted in ISE**
Day-N templates are applied
Devices configured with all site settings
**If site is configured with AAA
387434

Minimal configuration should provide network connectivity:

- Enable VLAN(s).
- Configure uplink interface, management IP address, and gateway.
- Define local username and password.
- Enable SSH.

Deploying Cisco Cyber Vision Sensor

The Cisco Cyber Vision sensor configuration is stored on an SD card and when an SD card is present, Cisco DNA Center uses it as the default location for software upgrade. Because of this, deploying Cisco Cyber Vision sensor on a switch managed by Cisco DNA Center requires a special process to ensure images can run concurrently with the sensor in SD Flash.

Note: IOS-XE version 17.5 or higher is required for partitioning the SD Flash filesystem into FAT32 for IOS-XE and EXT4 for IOx.

It is required to start from a switch that is booting from Flash. If the switch is not running from Flash, refer to the IE3400 configuration guide to change the boot location. Then, SD Flash needs to be partitioned with a CLI command. After this process is done, the switch configuration needs to be modified to boot from SD Flash. At this point it will be ready to be upgraded using Cisco DNA Center SWIM and to deploy Cisco Cyber Vision Sensor.

Tech Tip: When using PnP to onboard a switch with an SD card present skip the upgrade during the claim process to avoid changing boot location to SD Flash.

The recommended method to deploy Cisco Cyber Vision sensor is:

1. Use a Day-N template to prepare the switch for sensor installation.

2. Deploy the sensor using Cisco Cyber Vision Center management extension.

For additional details refer to:
https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Network_Sensor_Installation_Guide_for_Cisco_IE3400_and_Catalyst_9300_3_1_1.pdf

More information on IE3400 Configuration guide:
https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie3X00/software/17_4/b_system-management-ie3x00/m_1610_swapdrive.html

Device Administration Workflows

Once devices are added to Cisco DNA Center, they can be managed from Inventory. The following section details some of the Inventory capabilities, such as:

- Apply configuration changes with Day-N templates through inventory provisioning.
- Replace devices.
- Perform software image upgrade.
- Check compliance on network devices.
- Visualize Topology.

Apply Configuration Changes with Day-N Templates

Day-N templates can be used to apply configurations to devices after devices have been added to inventory. Templates are associated to a network profile as described in section Network Profiles for Switching. The templates are applied to the devices during Device Inventory Provisioning. A device can be provisioned multiple times. By default, only new configuration is pushed during re-provisioning, but this setting can be overridden. The following table contains a list of common features used in industrial automation and provides guidance for using templates. When using templates:

- Create an onboarding template with minimal config for PnP.
- Create a Day-N global template to be applied during first device provisioning. This template should contain most configuration for the device.
- Create a Day-N template to modify interface configuration. This template can be applied for interface configuration when onboarding endpoints.
- Create Day-N templates for specialized features like preparation steps to install Cisco Cyber Vision Sensor. This template can be associated to a tag, so it is only applicable to some devices as explained at the end of this section.

The companion Implementation Guide provides examples for templates to be used for common features.

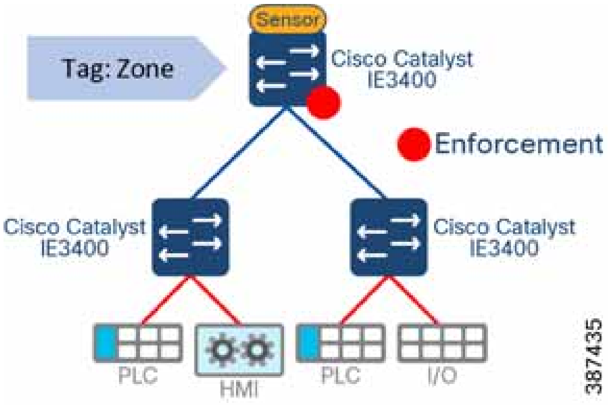
Table 4 Configuration Method for Switch Features for Industrial Automation

Feature	Description	Configuration Method
SSH, credentials, Management IP, Default Gateway	Minimal configuration required to communicate with Cisco DNAC Center	CLI before discovering/Automated by PnP (Onboarding Template)
Telemetry Settings	Syslog, SNMP, IPDT	Automated by Cisco DNA Center during site assignment
Site General Settings	Name server, DHCP, NTP	Automated by Cisco DNA Center during device provisioning
AAA Global Configuration	AAA global configuration and Radius server definition	Automated by Cisco DNA Center during device provisioning
CDP/LLDP	CDP and LLDP are enabled by default.	Use default configuration
AAA Port based authentication	Global commands to create Authentication policy to be applied to interfaces	Day-N template: Global Template
VLANs/SVIs	Additional VLANs and SVIs (besides management)	Day-N template: Global Template
IGMP/PTP	Sets any global parameters for IGMP or PTP	Day-N template: Global Template
Storm Control	Defines global storm control configuration	Day-N template: Global Template
QoS	Define QoS policies to prioritize critical traffic	Day-N Template: Global Template (See note below table)
NetFlow	Define NetFlow record, monitor and exporter	Day-N template: Global Template
Alarms	Defines alarms on the global configuration	Day-N template: Global Template
Interface Configuration	Configuration to define interface type, VLANs, apply policies to interface, TrustSec parameters, authentication, etc.	Day-N template: Port template
TrustSec	Configure SXP or enforcement	Day-N template: Specialized Feature
DHCP Pools	Creates DHCP pools for industrial devices	Day-N template: Specialized Feature
IOx / Cisco Cyber Vision Sensor	Enable IOx and configure ERSPAN destination and AppGi interface	Day-N template: Specialized Feature
L2NAT	Configure L2NAT instance	Day-N template: Specialized Feature
Redundancy	Configuration required to deploy redundancy protocols such as REP	Templates could be used but order of operations will be critical to deployment. This has not been validated using Cisco DNA Center.

Note: Deploying application policy is supported on IE3400 and IE3300. Nevertheless, it is not the chosen method to apply QoS in this design because current implementation is based on Enterprise Medianet Quality of Service Design. This is not suitable for Industrial environments, where priority is given to protocols such as PTP, PROFINET, or CIP instead of voice and video. Furthermore, if default application policy is applied to the access switches, industrial traffic will be put in the default queue.

When provisioning with templates, consider using device tags to group devices that need to be configured with a specific feature set. Device tags are useful to group devices to filter or apply settings to a subset of devices in a site. Consider Figure 16. There are three switches of the same family on the same logical site, but only the top switch needs configuration to enable Cyber Vision sensor and TrustSec enforcement. Tagging the upper-level switch with "zone" tag helps to apply specific configuration templates for the required feature set according to role.

Figure 16 Device Tag Example



RMA Workflow

Replacing devices that fail in the network is a critical part of device lifecycle management. The existing procedure to replace failed devices with new devices is manual and time consuming. The Return Material Authorization (RMA) workflow in Cisco DNA Center provides users the ease of automation to replace failed devices quickly, thus improving productivity and reducing operational expense. RMA provides a common workflow to replace routers, switches, and access points.

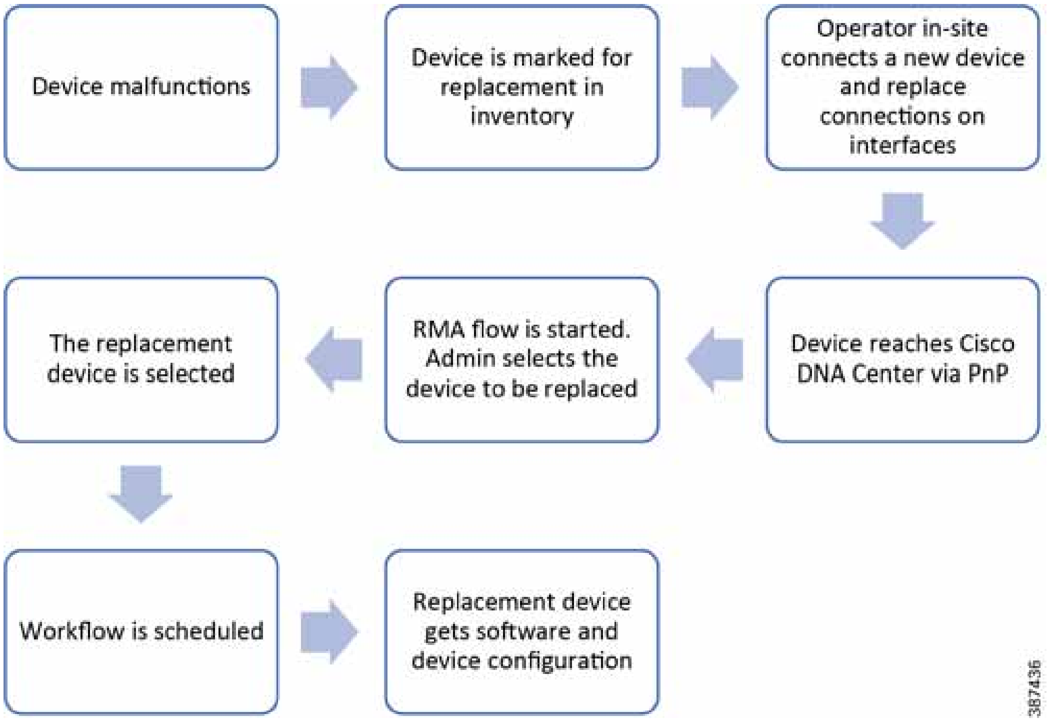
When using the RMA workflow with routers and switches, the software image, configuration, and license are restored from the failed device to the replacement device.

Note: The license is restored only on devices using smart licensing (IE3x00). For IE2000, IE4000 and IE5000, Cisco DNA center does not manage license therefore if the ipservices license is required on these devices it needs to be activated before the RMA workflow.

SD Swap Drive is a feature that has been used to update or restore configuration on a device. This method is still available even if the device is managed by Cisco DNA Center. Nevertheless, the Cisco DNA Center replacement flow has the additional advantage of updating the network device entry in ISE for a seamless experience.

Figure 17 illustrates the replacement workflow.

Figure 17 RMA Workflow


Device malfunctions
Device is marked for replacement in inventory
Operator in-site connects a new device and replace connections on interfaces
Device reaches Cisco DNA Center via PnP
RMA flow is started. Admin selects the device to be replaced
The replacement device is selected
Workflow is scheduled
Replacement device gets software and device configuration
387436

Note about RMA process:

- Before replacing, the faulty device should be unreachable by Cisco DNA Center.
- Replacement devices could be selected from inventory or from a new device that has contacted Cisco DNA Center via PnP. The latter option was depicted in Figure 17.
- The RMA feature only supports exact model replacement and the number of ports in both devices must not vary because of the extension modules.
- The replacement device must have the same uplink interface as the faulty device.
- The Cisco DNA Center repository must have the software image of the faulty device.

Known limitations of RMA Workflow for Industrial Automation:

- The faulty device should be managed by Cisco DNA Center with a static IP address.
- If the replacement device onboards through PnP-DHCP functionality, make sure that the device gets the same IP address after every reload and the lease timeout of DHCP is longer than two hours.
- RMA is not supported for switches deployed with hardware stacking.
- Cisco DNA Center does not support legacy license deployment.
- The RMA workflow is not supported for devices running a .tar software image. Only .bin images are supported.
- If the faulty device was running Cisco Cyber Vision sensor, the sensor needs to be reinstalled after replacement.

Note: If SD Swap Drive is used as replacement method, the network device needs to be deleted from inventory and re-discovered by Cisco DNA Center.

Software Image Upgrade

Cisco DNA Center Software Image Management (SWIM) functionality allows you to push software images to the devices in your network. Prior to pushing the image, Cisco DNA Center checks the device for upgrade readiness, including device management status, SCP and HTTPS file transfer success, and disk space. If any upgrade readiness checks fail, you cannot perform the software image update. After the software image of the device is upgraded, the Cisco DNA Center checks spanning tree, CDP neighbors, and so on, to ensure that the state of the network remains unchanged after the image upgrade. It is possible to create custom checks to gain confidence of network stability before and after the software upgrade. For example, checking the status of the Cyber Vision Sensor application before and after the upgrade to make sure the sensor survives the upgrade.

Figure 18 SWIM Pre and Post Checks

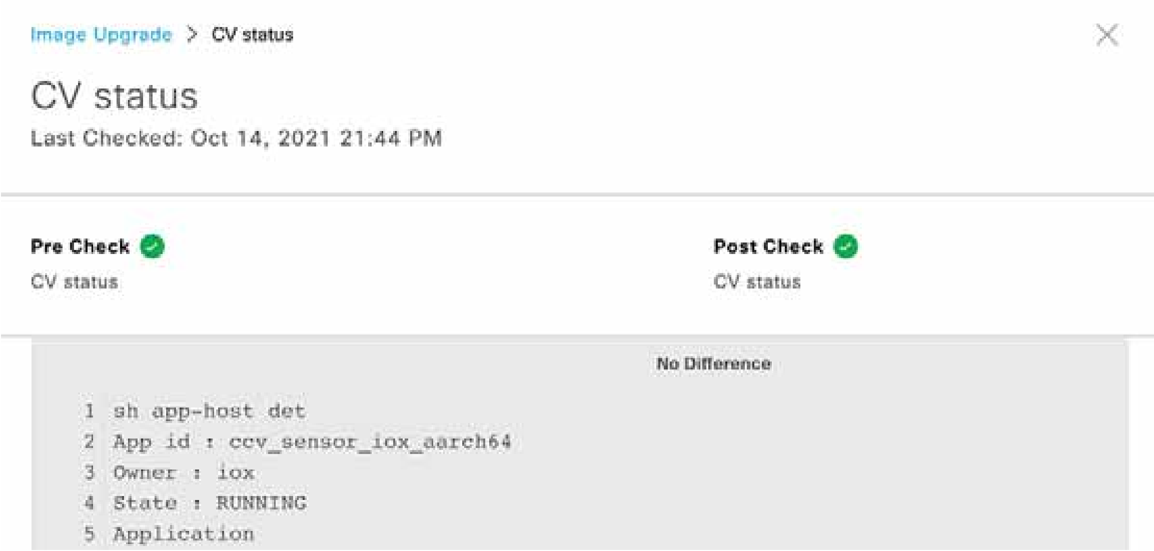


Image Upgrade > CV status

CV status

Last Checked: Oct 14, 2021 21:44 PM

Pre Check ✓

CV status

Post Check ✓

CV status

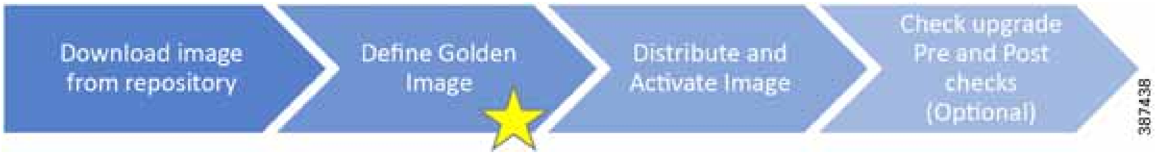
No Difference

```
sh app-host det
App id : ccv_sensor_iox_aarch64
Owner : iox
State : RUNNING
Application
```

The upgrade process is started by defining an image on the repository to be the standard image for a device type in a site, known as the “Golden Image”. Cisco DNA Center compares each device's software image with the image that is designated as golden for that specific device type. If a difference exists between the software image of the device and the golden image, Cisco DNA Center specifies the software image of the device as outdated and triggers readiness pre-checks for those devices. If all the pre-checks are cleared, the image can be distributed and activated. The activation of the new image requires a reboot of the device. This will interrupt the current network activity; if downtime is not feasible, activation can be scheduled to a later time.

SWIM of multiple devices can be scheduled in bulk. Figure 19 shows SWIM workflow.

Figure 19 SWIM Workflow



Download image from repository
Define Golden Image
Distribute and Activate Image
Check upgrade Pre and Post checks (Optional)
387438

SWIM Known Limitation

If a switch has an SD card, SWIM will use it for image installation. If an IE3400 switch is running IOx on an SD card (required for Cisco Cyber Vision sensor), special consideration is required.

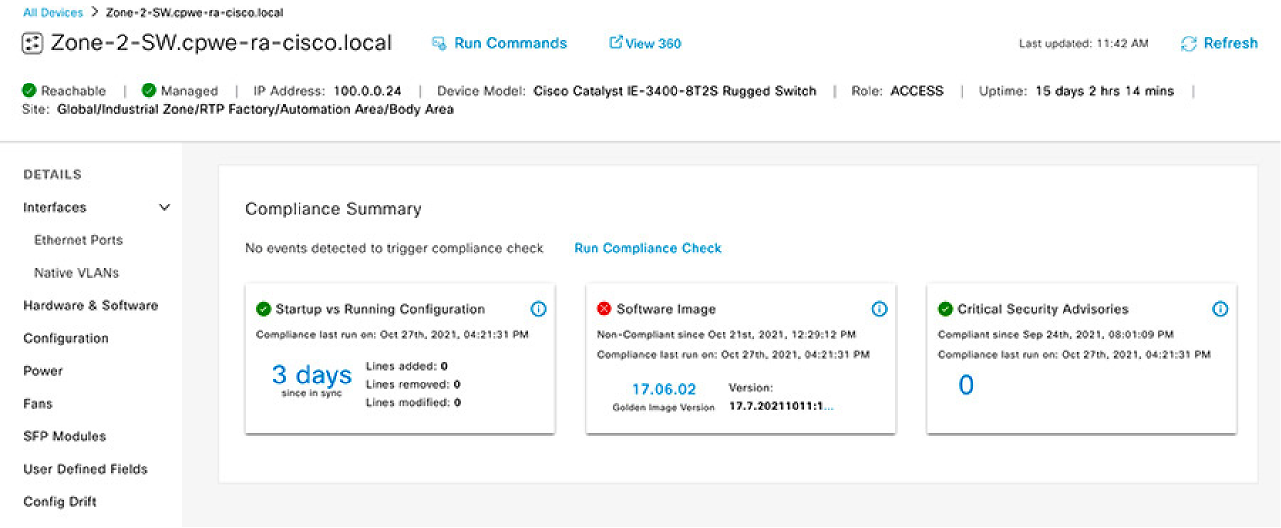
- Booting from SD Flash and running IOx concurrently on the switch is supported starting on IOS XE 17.5.x, when support for partitioning the SD Flash filesystem into FAT32 for IOS-XE and EXT4 for IOx was introduced. If the switch is running a previous version, SWIM is not supported if device is running IOx.
- The process below shows the workflow to support SWIM upgrades and IOx applications concurrently on IE3400. If the SD Flash has not been partitioned, Cisco Cyber Vision Sensor needs to be redeployed.
  - Switch needs to be booting from Flash (if not, sync from SD flash to Flash and change boot variable).
  - SD flash needs to be partitioned (via template or CLI).
  - Sync from Flash to SDFlash and boot from SDFlash.
  - (Optional) Switch is upgraded using SWIM.
  - Cyber Vision Sensor can be installed.

Check Compliance on Network Devices

A network administrator can conveniently identify devices that do not meet compliance requirements for the following areas applicable to industrial switches:

- Startup versus Running Configuration—This compliance check helps identify whether the startup and running configurations of a device are in sync. If the startup and running configurations of a device are out of sync, then compliance is triggered and a detailed report of the out of band changes is displayed. The compliance for startup versus running configurations is triggered within five minutes of any out of band changes. A device will be marked as non-compliant if the Startup and Running configuration are not the same. In the detail view, the system shows the difference between configurations.
- Software Image—This compliance highlights if a device is not running the golden image. When there is a change in the software image, the compliance check is triggered immediately without any delay. If the device is not running the tagged golden image of the device family, it will be identified as non-compliant.
- Critical Security (PSIRT)—PSIRT Compliance checks whether the network devices are running with any critical security vulnerabilities. A device is identified as non-compliant if the device has critical advisories.

Figure 20 Network Device Compliance



Zone-2-SW.cpwe-ra-cisco.local

Last updated: 11:42 AM

✓ Reachable | ✓ Managed | IP Address: 100.0.0.24 | Device Model: Cisco Catalyst IE-3400-8T2S Rugged Switch | Role: ACCESS | Uptime: 15 days 2 hrs 14 mins |
Site: Global/Industrial Zone/RTP Factory/Automation Area/Body Area

Compliance Summary

No events detected to trigger compliance check

✓ Startup vs Running Configuration
Compliance last run on: Oct 27th, 2021, 04:21:31 PM
3 days since in sync
Lines added: 0
Lines removed: 0
Lines modified: 0

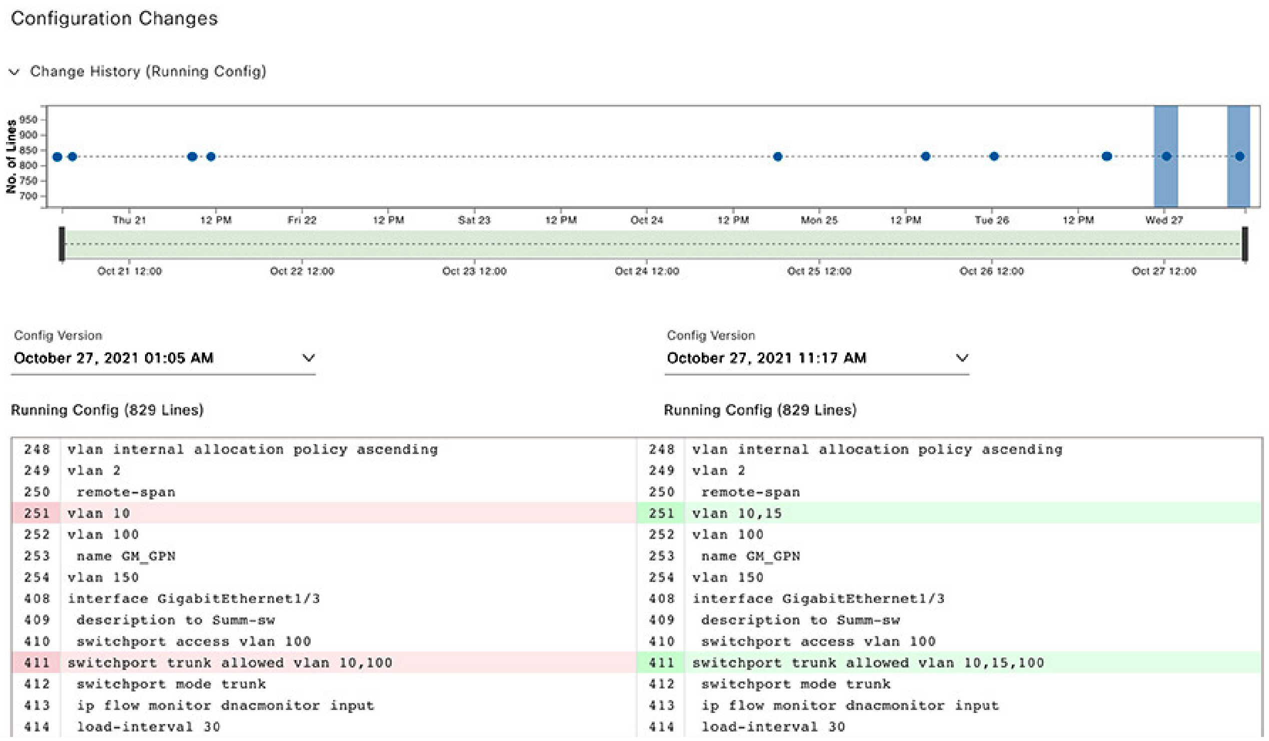
✗ Software Image
Non-Compliant since Oct 21st, 2021, 12:29:12 PM
Compliance last run on: Oct 27th, 2021, 04:21:31 PM
17.06.02 Golden Image Version
Version: 17.7.20211011:1...

✓ Critical Security Advisories
Compliant since Sep 24th, 2021, 08:01:09 PM
Compliance last run on: Oct 27th, 2021, 04:21:31 PM
0

Configuration Drift

Configuration Drift is a tool available on the inventory details for a device. The Configuration Drift page displays configuration changes and allows you to pick any two versions of the device's configuration to compare.

Figure 21 Configuration Drift



Config Version: October 27, 2021 01:05 AM

Running Config (829 Lines)

```
vlan internal allocation policy ascending
vlan 2
 remote-span
vlan 10
vlan 100
 name GM_GPN
vlan 150
interface GigabitEthernet1/3
 description to Summ-sw
 switchport access vlan 100
switchport trunk allowed vlan 10,100
 switchport mode trunk
 ip flow monitor dnacmonitor input
 load-interval 30
```

Config Version: October 27, 2021 11:17 AM

Running Config (829 Lines)

```
vlan internal allocation policy ascending
vlan 2
 remote-span
vlan 10,15
vlan 100
 name GM_GPN
vlan 150
interface GigabitEthernet1/3
 description to Summ-sw
 switchport access vlan 100
switchport trunk allowed vlan 10,15,100
 switchport mode trunk
 ip flow monitor dnacmonitor input
 load-interval 30
```

Topology

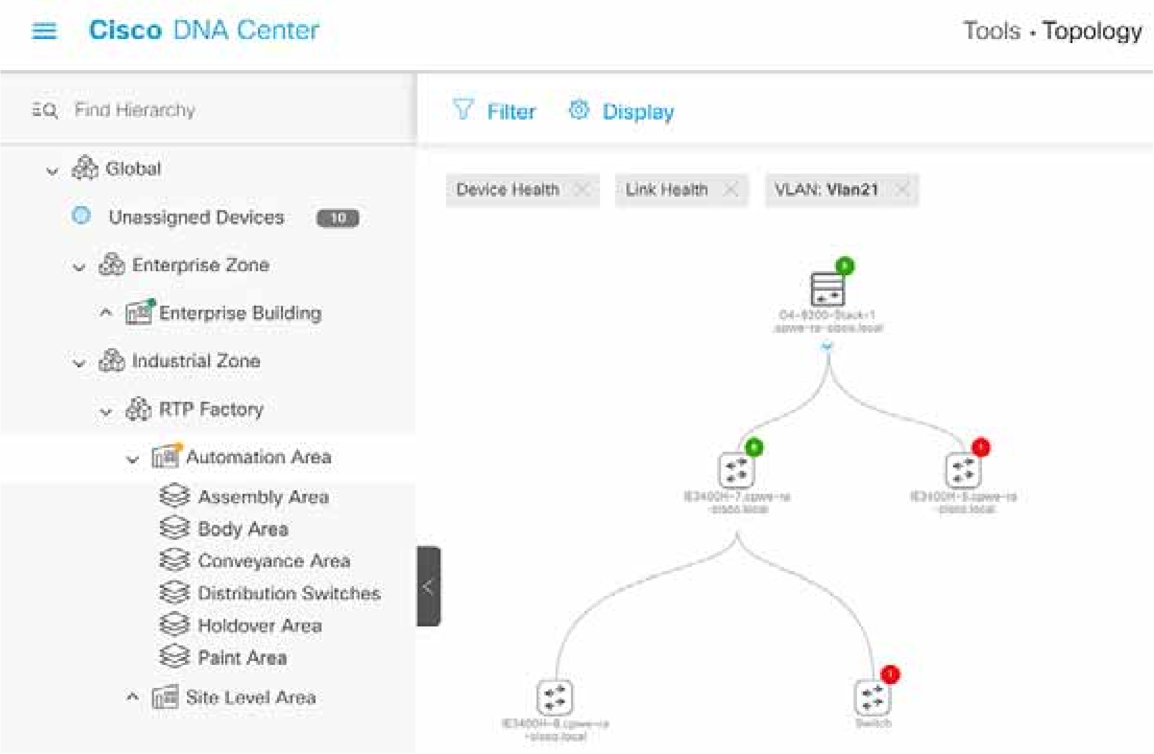
The Topology page displays a graphical view of your network. Based on the device role assigned during discovery (or changed in Device Inventory), Cisco DNA Center creates a physical topology map with detailed device-level data. Using the topology map, you can display the topology of a selected area, site, building, or floor and display detailed link information and filter devices based on a specific Layer 2 VLAN or tag.

Topology Known Limitations:

- Topology view does not display industrial endpoints.
- Topology view does not show resiliency protocol (for example, REP, HSR, STP, or MRP).
- Physical links are displayed but not EtherChannel configurations.
- Devices running MRP, REP or HSR ring resiliency protocols can be discovered and managed by Cisco DNA Center but neighbor information on assurance and topology pages may be incomplete.

Figure 22 shows an example of the topology view; it shows devices with specific VLAN and displays link and device health.

Figure 22 Topology



Interaction With Industrial Network Management Tools

Industrial Ethernet switches support CIP and PROFINET and protocol functionality can be configured with Rockwell Automation Factory Talk Network Manager (FTNM) or PROFINET software such as Siemens TIA portal, respectively.

Cisco DNA Center and industrial management software can co-exist in the same network. It is recommended to have a clear delineation of management responsibilities so as not to have competing operational control of the network features and functions.

Cisco DNA Assurance for Industrial Networks

This section covers available assurance features for the Industrial Automation architecture as well as configuration requirements for assurance to work.

Requirements for Assurance

Network devices must be added to the inventory and be in a managed state before the performance metrics of devices and clients can be viewed. At this point Cisco DNA Center becomes an SNMP collector, polling network devices to gather telemetry data. This is a setting on Cisco DNA Center independent of device controllability, and it does not cause any configuration on devices. Cisco DNA Center gathers the following information:

- Device health—Includes CPU, Memory, Environment Temperature and Device Availability metrics.
- Interface health—Includes Interface Availability and Ethernet metrics.
- TCAM

When a device is added to a site with Controllability enabled, telemetry profiles are configured on the device.

- SNMP trap server—Appendix B—SMP Traps Configured showcases an example of SNMP traps added by Cisco DNA Center to IE3400 running IOS-XE Release 17.6
- Syslog server—Syslog messages with severity of Critical and above (Emergency and Alert) will be displayed on the event viewer for the device. Only a selected list of syslog messages that are less severe than Critical level (Error, Warning, Notice, and Info) are also displayed. For the list of selected syslog messages that are displayed, see: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-assurance/2-2-3/b_cisco_dna_assurance_2_2_3_ug/b_cisco_dna_assurance_2_2_2_ug_chapter_0110.html?bookSearch=true
- IPDT is used to gather information on client devices and provide client assurance.
- Optionally, when ISE is integrated with Cisco DNA Center and used for AAA on the site, Assurance can integrate with ISE to provide more detail about connected clients such as username.

Assurance General Concepts

This section introduces some concepts that are referred in this document when explaining assurance functionality.

Guided Remediation

When an issue is identified by Assurance, actions are suggested to troubleshoot or fix the issue. Some of the suggestions are actionable from the Issue Details.

Time Travel

Network time travel shows the health of the network or device and values for key performance indicators (KPIs) in a timeline. The operator can look backwards to understand the exact conditions of the network at a given time and to determine the root cause of an issue or to identify patterns. A time window at the top of assurance dashboards can be adjusted to intervals of 3 hours, 24 hours, or 7 days, and keeps 30 days of data. Modifying the time window will have effect on all assurance data displayed, so information is applicable to the time in question.

Health Score

A health score is assigned to clients, devices, and networks to easily identify potential issues. The following shows the health score scale and meaning. The next sections explain what factors are considered when assigning a score to switches and clients.

🔴	Poor. Health score range is 1 to 3.
🟠	Fair. Health score range is 4 to 7.
🟢	Good. Health score range is 8 to 10.
●	No Health data. Health score is 0.

Switch Health Score

The Individual Device Health score for a non-fabric switch is the minimum score of the KPI metric health scores in Table 5.

Table 5 Switch Health Score (non-Fabric)

Parameter	Score Calculation
CPU Utilization	If CPU utilization is 95 percent or less, the score is 10. If CPU utilization is more than 95 percent, the score is 1.
Memory Utilization	If memory utilization is 95 percent or less, the score is 10. If memory utilization is more than 95 percent, the score is 1.
Link Errors (Rx and Tx)	Only infrastructure links are considered for link errors. Infrastructure links are topological links between network devices, such as switches, routers, wireless controllers, and APs. If a physical infrastructure interface has errors, the score is 8, if all links are down, it is 1, otherwise it is 10.
Link Discards	Only infrastructure links are considered for link discards. If a physical infra link has packet drops (discards), the score is 8, if all links encounter discards, it is 1, otherwise it is 10.
Link Status	Only infrastructure links are considered for link status UP/DOWN. If a physical infrastructure interface is down, the score is 8, if all interfaces are down, it is 1, otherwise it is 10.

It is possible to customize the health score calculation for network devices by changing the KPI thresholds and specifying the KPIs that are included for the calculation.

Client Health Score

The Individual Client Health score is the sum of the Client Onboarding score and the Client Connectivity score.

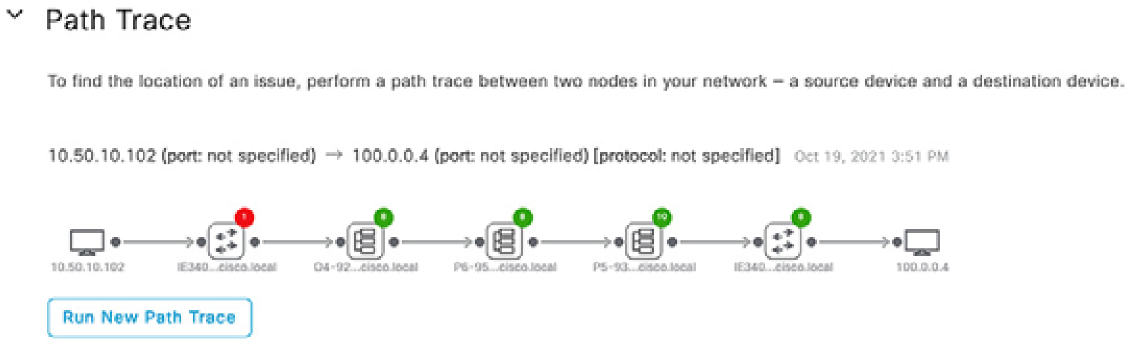
- The Client Onboarding score indicates the experience of a client device while connecting to the network. The score is calculated as follows:
  - If a client connects to the network successfully, the score is 4.
  - If a client failed to connect to the network, the score is 1.
  - If a client is idle, the score is 0.
- The Client Connectivity score indicates the experience of the client device after the device is connected to the network. Connectivity score can be 2 or 6. Link errors determine the Connectivity score and the resulting Overall Health score, as shown below:
  - If a client onboards successfully but has link errors, the Connectivity score is 2 and the Overall Health score is 6.
  - If the client onboards successfully and there are no link errors between the client and the first-hop switch, the Connectivity score is 6 and the Overall Health score is 10.

Path Trace

You can perform a path trace between two nodes in your network-a specified source device and a specified destination device. The two nodes can be a combination of wired or wireless hosts or Layer 3 interfaces, or both. In addition, you can specify the protocol that the Cisco DNA Center controller should use to establish the path trace connection, either TCP or UDP.

When you initiate a path trace, the Cisco DNA Center controller reviews and collects network topology and routing data from the discovered devices. It then uses this data to calculate a path between the two hosts or Layer 3 interfaces, and displays the path in a path trace topology. The topology includes the path direction and the devices along the path, including their IP addresses. The display also shows the protocol of the devices along the path (Switched, STP, ECMP, Routed, Trace Route) or other source type. Figure 23 shows an example of path trace output between two clients.

Figure 23 Path Trace



Path Trace

To find the location of an issue, perform a path trace between two nodes in your network – a source device and a destination device.

10.50.10.102 (port: not specified) → 100.0.0.4 (port: not specified) [protocol: not specified] Oct 19, 2021 3:51 PM

Path trace has the following limitations and restrictions:

- Overlapping IP addresses are not supported.
- CDP is required on network devices.
- Path trace in Cisco Adaptive Security Appliances (ASA) is not supported because Cisco ASA does not support CDP. It is not possible to identify the path through the Cisco ASA appliance.
- Path trace is not supported on devices with NAT or firewall.
- Port-channel Port Aggregation Protocol (PAgP) mode is not supported. Only LACP mode is supported.
- Path trace from a Layer 2 switch is not supported.
- Path trace does not work when the network device is part of a REP, MRP or HSR ring.

Issues

Cisco DNA Center can detect basic issues as well as correlate multiple pieces of information to determine issues. Assurance provides a system-guided approach, where multiple Key Performance Indicators (KPIs) are correlated, and the results from tests and sensors are used to determine the root cause of the problem, and then possible actions are provided to resolve the problem. The focus is on highlighting an issue rather than monitoring data. It is possible to configure REST or email notifications when an issue is triggered.

Issues are assigned a priority as described below:

- P1—A critical issue that needs immediate attention which can result in wider impact on network operations.
- P2—A major issue that can potentially impact multiple devices or clients.
- P3—A minor issue that has a localized or minimal impact.
- P4—A warning issue that may not be an immediate problem but addressing it can optimize the network performance.

Note: Issues allow for customization by enabling or disabling specific issues, changing the priority, or changing the threshold for when an issue is triggered.

Table 6 and Table 7 contain examples of issues that are shown for access switches and clients. For a list of all available issues refer to:
https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-assurance/2-2-3/b_cisco_dna_assurance_2_2_3_ug/b_cisco_dna_assurance_2_2_3_ug_chapter_01001.html?bookSearch=true#id_107179

Table 6 Switch Issues Detected by Assurance

Category	Issue Name	Summary
Connectivity	Interface connecting network devices is down	Interface connecting network devices is down.
Connectivity	Layer 2 loop symptoms	Host MAC address flapping seen on a network device.
Connected	Unable to download SGT access policy from the policy server	Failure to download the source list for access policy for SGT.
Device	Device reboot crash	Device has rebooted due to a hardware or software crash.
Device	Interface is flapping on network device	A port interface is flapping on a switch.
Device	Issues based on syslog events - High temperature	Issues created by single occurrence of syslog event related to high temperature.
Availability	Switch unreachable	Device is unreachable.

Table 7 Endpoint Issues Detected by Assurance

Category	Issue Name	Summary
Onboarding	Wired client authentication failures - Dot1.x failure	Wired client authentication failed. User device authentication with Dot1.x failure. Note This issue is applicable only for single wired clients.
Onboarding	Wired client authentication failures - MAB failure	Wired client authentication failed. User device authentication failed with MAC authentication bypass issues. Note This issue is applicable only for single wired clients.

Assurance Dashboards

Network Health

It is used to monitor and troubleshoot the health of the network. A network consists of one or more devices, including routers, switches, wireless controllers, and access points. Note that clients are not a part of this dashboard. This dashboard shows global location by default but can be filtered to focus on a specific site.

The network health dashboard displays:

- Graph illustrating health score over time. The Network Health score is a percentage of the number of healthy network devices (a health score from 8 to 10) divided by the total number of network devices and is calculated periodically. The network health score exists only in the context of a location; a device needs to be added to the relevant site for it to contribute to the network health score of that site.
- Color-coded chart shows the information about the reachability status of routers, switches, and wireless controllers, with option to see “latest” or “trend”. The Latest tab provides a 5-minute snapshot view. The trend tab shows the performance of devices over selected time range. Hovering the cursor over the chart will display the total number of devices and their health over time.

- The bottom of the page shows a list of network devices and provides filters based on health score, device type or inventory settings.
- Network Devices Reachability depicts latest and trend reachability status of network devices.

Device 360

Device 360 is used to view details about a specific device and determine if there are potential issues that must be addressed. Device 360 displays:

- Graph illustrating device health score over time and device events. Green vertical bars indicate successful events and red vertical bars indicate events that failed. Hovering over the graph will show device KPIs over time and event description.
- Device's health score and Device Details
- Physical neighbor topology displays client and neighbor network devices. Clicking on a link or device will provide additional information.
- Event viewer shows events on selected time frame. Events can be filtered and exported. All syslogs that have a severity of Critical and above (Emergency and Alert), events for any links that are up or down, and events for devices that are reachable or unreachable are recorded in the Event Viewer. Only a selected list of syslogs that are less severe than Critical level (Error, Warning, Notice, and Info) are also displayed.
- Issues for the switch that have occurred on the selected time range.
- Path Trace to display a network topology between a specified source device and a destination device.
- Detail Device information, such as CPU, memory, uptime, and temperature
- Interface information, such as the name, description, operational status, link speed, and so on is displayed. When selecting an interface utilization, errors and discards charts are displayed.

Client Health

Client health displays health of all clients to determine if there are potential issues that must be addressed. A client is an end device (computer, PLC, HMI, etc.) that is connected to a network device (access point or switch). Cisco DNA Center supports both wired and wireless clients. The following list describes available dashlets that provide information for wired clients:

- Graph illustrating aggregated client health percentage over time. Hovering the cursor within the timeline displays the wireless and wired client health score percentage at a specific time. The dotted horizontal line represents the threshold value for healthy clients, which by default is set to 40% but can be customized.
- Breakdown of wireless and wired clients showing connectivity and onboarded status. For the clients that failed to onboard, the breakdown of the reason for the onboarding failure is provided. For example, AAA, DHCP, Other, and so on. The Latest tab provides a 5-minute snapshot view. Trend tab shows client count and health of clients over selected time range.
- Connectivity Physical Link displays distribution of wired client device by link state: physical links up, down, and had errors.
- Client device list provides filters based on device attributes, health score, wired vs wireless and onboarding times (i.e., Authentication >= 5s). Client identifier is client's user ID, hostname, or MAC address based on availability.

Client 360

Client 360 is used to view details about a specific endpoint and determine if there are potential issues that must be addressed. Client 360 displays:

- Graph illustrating client health score over time and events.

- Issues detected on device on the specified time range
- Onboarding shows details on the onboarding process such as authentication state or IP address assignment. It also displays physical connectivity to the network device.
- Event viewer for client events on the specified time range. For wired clients lists ISE server events, access switch system level syslogs, switch port or interface specific events, and client specific events. For the list of messages under each event category, see Messages Displayed in the Event Viewer for Wired Clients: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-assurance/2-2-3/b_cisco_dna_assurance_2_2_3_ug/b_cisco_dna_assurance_2_2_3_ug_chapter_0111.html#reference_fm3_gsz_hjb
- Events can be filtered and exported.
- Path Trace displays a network topology between a specified source device and a destination device.
- Detail Information for wired clients provides information about the client device such as its MAC address, IPv4 and IPv6 address, connected VLAN ID, connection status, link utilization, and connected interface errors.

Overall Health

Overall health can be used to monitor overall health of the deployment including devices and clients. It summarizes network and client health and shows top 10 issues for the network, if any, that must be addressed. The issues are color coded and sorted by their preassigned priority level from P1 to P4, starting with P1. Clicking an issue will open a slide-in pane with additional details about the issue type.

Issues Dashboard

Issues dashboard identifies problems that need to be addressed on the deployment by priority. Provides a graph illustrating issues over time and providing color code to show priority and significance. Intensity of the color indicates if more or fewer issues have occurred for that priority level.

A list with issues is provided, organized by priority. It shows number of times this type of issue occurred, number of sites impacted, number of devices that were impacted by it and most recent date and time this issue was seen.

Machine Reasoning Engine

The Machine Reasoning Engine (MRE) is a network automation engine that uses artificial intelligence (AI) to automate complex network operation workflows. It encapsulates human knowledge and expertise into a fully automated inference engine to perform complex root cause analysis, detect issues and vulnerabilities, and either manually or automatically perform corrective actions. MRE is powered by a cloud-hosted knowledge base, built by Cisco networking experts.

Machine Reasoning knowledge packs are step-by-step workflows that are used by MRE. These knowledge packs are continuously updated as more information is received. The Machine Reasoning Knowledge Base is a repository of these knowledge packs (workflows). To have access to the latest knowledge packs, you can either configure Cisco DNA Center to automatically update the Machine Reasoning Knowledge Base daily, or you can perform a manual update.

Tech Tip: Machine Reasoning package needs to be installed. For more information, see the Cisco DNA Center Administrator Guide.

MRE could be used to troubleshoot issues or to run network reasoner workflows as explained in the following section.

Troubleshoot Issues with MRE

MRE can be used to troubleshoot some of the issues that show on the issues dashboard or health pages. The following issues can be troubleshooted with MRE and are applicable to the Industrial Automation network.

- Layer 2 loop issue (forwarding loop forms in the path of one or more VLANs). Note that MRE does not perform root cause analysis on Layer 2 loops that occur because of unmanaged network devices, virtual machines, or other entities that are not part of the topology known to the Cisco DNA Center.

- CPU high utilization troubleshoots causes of high CPU utilization for a device.

Network Reasoner

The Network Reasoner dashboard provides workflows that can be used to proactively troubleshoot network issues. The dashboard provides a brief description about the workflows, the number of affected devices in the last 24 hours, and impact of running a workflow on a network.

The following tools are applicable to industrial switches:

- CPU utilization–Troubleshoots causes of high CPU utilization for a device.
- Ping Device–Provides ping functionality from the GUI to check network connectivity.

System-wide tools:

- Client count–Checks number of clients is withing Cisco DNA Center limits.
- Device count–Checks number of network devices is within Cisco DNA Center limits.
- Network Bug Identifier–Identifies bugs in the network.

Inventory Insights

Inventory Insights is a feature that uses machine reasoning (MRE) to scan all device inventory and locate incorrect and inconsistent device configurations with other directly connected devices. Inventory insights is located on the Provision menu. Currently Cisco DNA Center supports the following insights:

- Speed/Duplex settings mismatch–Cisco DNA Center displays connected devices that are configured with different speed and duplex values at the two ends of the device link. Insight is only available for inter-switch links.
- VLAN Mismatch–Cisco DNA Center displays connected devices that are configured with different VLANs at the two ends of device link. Insight is only available for inter-switch links.

Not Supported Assurance Features

The following assurance features are not covered in this document as they are not applicable to the non-fabric Industrial Automation design:

- Application Health is currently not available for Industrial Ethernet switches.
- Network services Health (AAA and DHCP)–Wireless-only functionality
- Cisco AI Network Analytics applies to wireless only. AI Network Analytics is used to export network event data from wireless controllers as well as the site hierarchy to the Cisco DNA Center.
- Sensors, Wi-Fi 6, Rogue and aWIPs are for wireless deployments.
- PoE assurance is currently not available for Industrial Ethernet switches.

In addition, the following is a list of assurance limitations applicable to industrial networks:

- Assurance of resiliency protocols is not implemented in the current version.
- Assurance of PTP, IGMP, CIP, and PROFINET is not implemented in the current version.
- If a client auto-negotiates a link as half-duplex, no alarm or issue is generated. Nevertheless, link details are available in inventory details for the device.

Other Troubleshooting and Maintenance Tools

Command Runner

Command Runner tool allows you to send diagnostic CLI commands to selected devices. Read-only commands such as show are currently permitted.

Reports

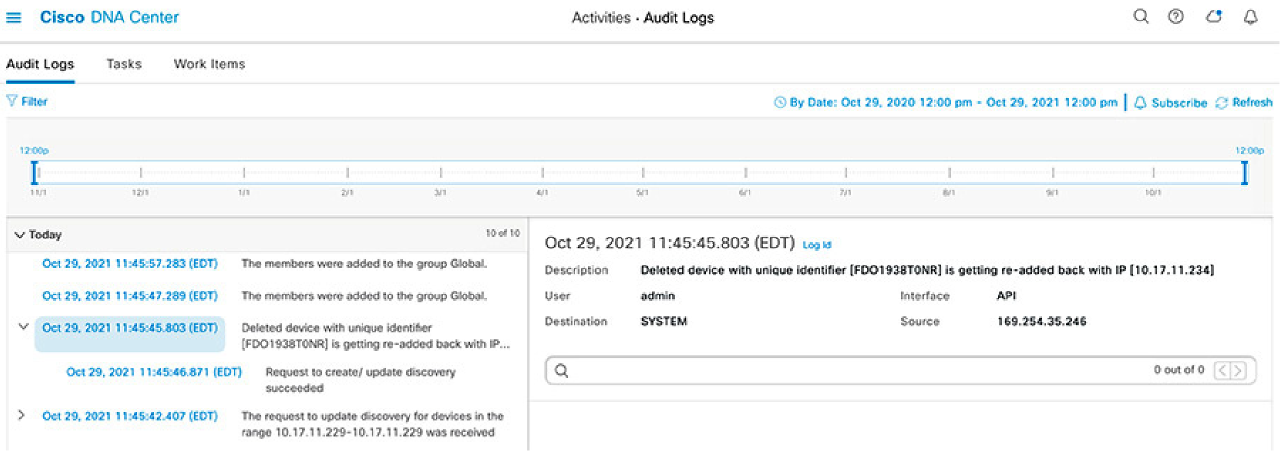
You can utilize data from the Reports feature to derive insights into your network and its operation. By reporting this data in several formats and providing flexible scheduling and configuration options, both data and reports are easily customized to meet your operational needs.

Audit Logs

Audit logs are created to capture critical activities, such as when configuration changes were requested, when the configuration changes were executed, and if there were errors that occurred during the configuration. Audit logs also record system events that occurred, when and where they occurred, and which users initiated them. With audit logging, configuration changes to the system get logged in separate log files for auditing.

Audit logs can be exported from Cisco DNA Center to multiple syslog servers by subscribing to them.

Figure 24 Audit Logs



By Date: Oct 29, 2020 12:00 pm - Oct 29, 2021 12:00 pm

Oct 29, 2021 11:45:57.283 (EDT) The members were added to the group Global.

Oct 29, 2021 11:45:47.289 (EDT) The members were added to the group Global.

Oct 29, 2021 11:45:45.803 (EDT) Deleted device with unique identifier [FDO1938T0NR] is getting re-added back with IP...

Oct 29, 2021 11:45:46.871 (EDT) Request to create/ update discovery succeeded

Oct 29, 2021 11:45:42.407 (EDT) The request to update discovery for devices in the range 10.17.11.229-10.17.11.229 was received

Oct 29, 2021 11:45:45.803 (EDT)

Description Deleted device with unique identifier [FDO1938T0NR] is getting re-added back with IP [10.17.11.234]

User admin Interface API

Destination SYSTEM Source 169.254.35.246

Applying Security Policy to Industrial Automation Networks

Intent-based security gives the administrator the ability to express operational intent and automatically have the system select the appropriate IT-defined security policies without requiring network or security skills.

Cisco DNA Center, when integrated with ISE, provides intent-based security using TrustSec; this is also known as micro-segmentation. Micro-segmentation uses scalable group tags to apply policy to groups of users or device profiles. Micro-segmentation policies are customized for an organization's deployment. The following example shows a security policy that can be used to limit communication between Cell/Area Zones.

Security Policy Example

The scope of this design guide is not to discuss design for the TrustSec deployment on an Industrial Automation network. However, the guide will explain the network configuration workflow, endpoint onboarding, and role of Cisco DNA Center in configuring and monitoring security design. To showcase this, we select a single network design as described below.

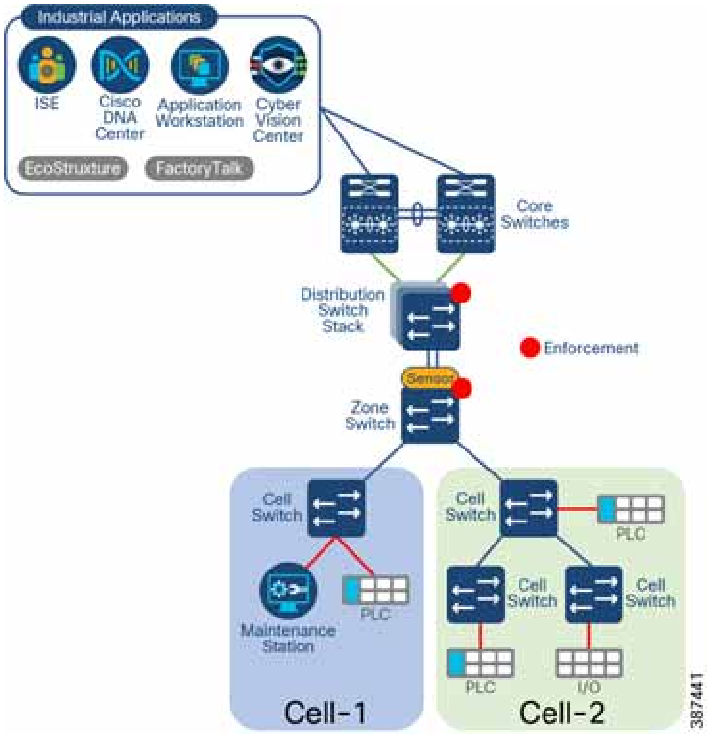
For more information on security design, refer to:
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/DG/Industrial-AutomationDG.html

Note: The example provided below is not a TrustSec design recommendation. It is to be used only as example to understand TrustSec implementation when using Cisco DNA Center. More information on TrustSec design can be found at:
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/DG/Industrial-AutomationDG.html

Figure 25 shows an industrial zone with a linear topology consisting of a zone switch with two cells connected to it. Most endpoints are industrial devices that don't support 802.1x authentication, nevertheless, it is expected that the devices are allowed access to the network. The communication requirements are as follows:

- All communications between industrial devices should be allowed in the cell area.
- Inter-zone communications are restricted to interlocking PLCs.
- Super-user can communicate to all devices in the zone.
- Application station at the site data center can communicate with all devices.

Figure 25 Segmentation Example on Cell Area Zone



To meet those requirements, we can create the following SGTs: Cell-1, Cell-2, Interlock, Application WS, and Super User.

Note: Group Based Access Control Policy matrix provided above is only an example to showcase TrustSec configuration when using Cisco DNA Center. Designing a policy matrix is not in the scope of this document. It needs to be defined based on communication needs and scale considerations.

Security Policy Elements

The following section explains what components and configurations are required to successfully deploy the example security policy.

Classification Elements and Requirements

When an endpoint joins the network, it needs to get the SGT that determines what access is granted to the device. The following is required to classify endpoints:

- SGTs need to be created by a security administrator on Cisco DNA Center - Policy Group-Based Access Control.

  Note: A “default SGT” tag can be created to be assigned to all devices that don't match a classification rule based on known attributes. Further analysis on devices on this category is needed to make any adjustments on process or rules.

- Switch needs to be configured for authentication with ISE; this is automated by Cisco DNA Center as part of inventory provisioning.
- Port-based authentication needs to be configured on the switch. This can be done using Day-N templates applied during inventory provisioning.
- Profiling rules need to be created in ISE (to assign an endpoint profile).
- Authentication and Authorization policies need to be created in ISE (to authorize endpoint based on profile).
- Cisco Cyber Vision could be used to provide additional information on endpoints for profiling.

Propagation Elements and Requirements

Propagation of tags could be done on the control plane using SGT Exchange Protocol (SXP) tunnels or by the data plane adding the tag to the data packet. Propagation methods are not part of the scope of this document. Both propagation methods can be configured via Day-N templates.

Enforcement Elements and Requirements

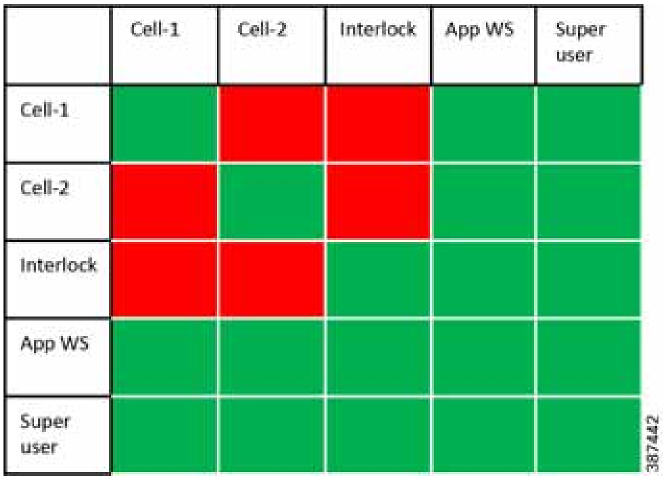
- A group-based access control policy needs to be defined in Cisco DNA Center. A policy could permit or deny all communication between SGTs. If more granularity is desired, custom contracts can be created to allow specific ports. Policy should consider what privileges are granted to devices falling on “default SGT”.
- Enforcement Switch and ISE need to be configured with CTS credentials. This is automated by Cisco DNA Center when device is added to inventory.
- IPDT is required for TrustSec to operate properly; this configuration is automated when adding device to a site.
- Enforcement needs to be enabled on enforcement device; this task can be accomplished via Day-N templates applied during inventory provisioning.

Security Workflow

The following section proposes a workflow to deploy security in the Industrial Automation network. It assumes Cisco DNA Center and Cisco Cyber Vision Center have been integrated with ISE. Before proceeding with the workflow, it is important to define security design such as tag propagation methods and enforcement points. Also, if using Cisco Cyber Vision Center, sensor placement for effective visibility should be decided beforehand. For information on design refer to: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/IA_Security/IA_Security_DG.html

The following policy matrix reflects segmentation requirements when enforcement is located at the zone level switch. Because traffic on cell area zone is not enforced, all cell area communications are allowed and only traffic traversing the zone switch is enforced. The next sections explain what is required to implement this security policy.

Figure 26 Example of Group Bases Access Control Policy



	Cell-1	Cell-2	Interlock	App WS	Super user
Cell-1	🟩	🟥	🟥	🟩	🟩
Cell-2	🟥	🟩	🟥	🟩	🟩
Interlock	🟥	🟥	🟩	🟩	🟩
App WS	🟩	🟩	🟩	🟩	🟩
Super user	🟩	🟩	🟩	🟩	🟩

Note: Group Based Access Control Policy matrix provided above is only an example to showcase TrustSec configuration when using Cisco DNA Center. Designing a policy matrix is not in the scope of this document. It needs to be defined based on communication needs and scale considerations.

Security Policy Elements

The following section explains what components and configurations are required to successfully deploy the example security policy.

Classification Elements and Requirements

When an endpoint joins the network, it needs to get the SGT that determines what access is granted to the device. The following is required to classify endpoints:

- SGTs need to be created by a security administrator on Cisco DNA Center - Policy Group-Based Access Control.

  Note: A “default SGT” tag can be created to be assigned to all devices that don't match a classification rule based on known attributes. Further analysis on devices on this category is needed to make any adjustments on process or rules.

- Switch needs to be configured for authentication with ISE; this is automated by Cisco DNA Center as part of inventory provisioning
- Port-based authentication needs to be configured on the switch. This can be done using Day-N templates applied during inventory provisioning.
- Profiling rules need to be created in ISE (to assign an endpoint profile).
- Authentication and Authorization policies need to be created in ISE (to authorize endpoint based. on profile).
- Cisco Cyber Vision could be used to provide additional information on endpoints for profiling

Propagation Elements and Requirements

Propagation of tags could be done on the control plane using SGT Exchange Protocol (SXP) tunnels or by the data plane adding the tag to the data packet. Propagation methods are not part of the scope of this document. Both propagation methods can be configured via Day-N templates.

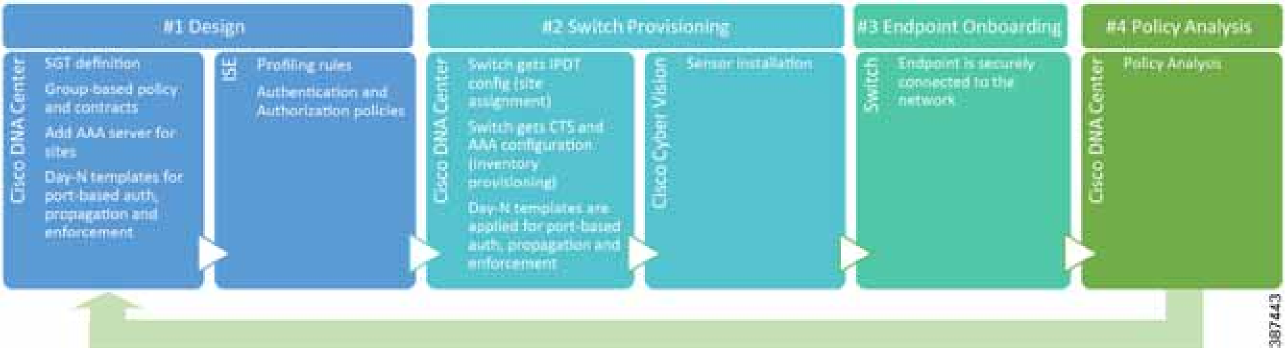
Enforcement Elements and Requirements

- A group-based access control policy needs to be defined in Cisco DNA Center. A policy could permit or deny all communication between SGTs. If more granularity is desired, custom contracts can be created to allow specific ports. Policy should consider what privileges are granted to devices falling on “default SGT”.
- Enforcement Switch and ISE need to be configured with CTS credentials. This is automated by Cisco DNA Center when device is added to inventory.
- IPDT is required for TrustSec to operate properly, this configuration is automated when adding device to a site.
- Enforcement needs to be enabled on enforcement device; this task can be accomplished via Day-N templates applied during inventory provisioning.

Security Workflow

The following section proposes a workflow to deploy security in the Industrial Automation network. It assumes Cisco DNA Center and Cisco Cyber Vision Center have been integrated with ISE. Before proceeding with the workflow, it is important to define security design such as tag propagation methods and enforcement points. Also, if using Cisco Cyber Vision Center, sensor placement for effective visibility should be decided beforehand. For information on design refer to: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/IA_Security/IA_Security_DG.html

Figure 27 Security Workflow


#1 Design
Cisco DNA 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 DNA Center
Switch gets IPDT config (site assignment)
Switch gets CTS and AAA configuration (inventory provisioning)
Day-N templates are applied for port-based auth, propagation and enforcement
Cisco Cyber Vision
Sensor installation
#3 Endpoint Onboarding
Switch
Endpoint is securely connected to the network
#4 Policy Analysis
Cisco DNA Center
Policy Analysis
387443

Phase 1—Design Activities

- Cisco DNA Center
  - Define and create SGTs.
  - Define ISE as AAA server on network settings.
  - Enable wired data collection (IPDT) on telemetry settings.
  - Create Day-N templates to configure the following features on a switch:

    – Port-based Authentication

    – Propagation (SXP or inline tagging)

    – Enable enforcement
- ISE
  - Profiling should be enabled and profiling rules should be configured in ISE.

- Authentication and authorization policies should be defined in ISE.

Phase 2—Switch Provisioning

When a switch joins the network, settings should be pushed to the device. AAA server definition and CTS credentials are configured according to site settings when a switch is provisioned in inventory. Day-N templates are used to configure remaining settings (port-based authentication policy, enforcement, and propagation configuration).

If Cyber Vision sensor will be installed on the switch, it needs to be provisioned; see Deploying Cisco Cyber Vision Sensor for sensor deployment flow.

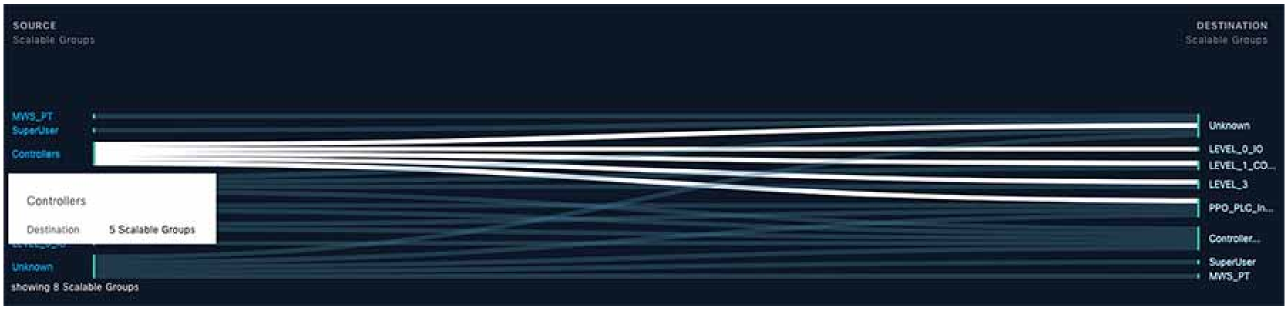
Phase 3—Endpoint Onboarding

Endpoint can be securely connected to the network

Phase 4—Policy Analytics

Active policy analytics should be done to understand communication patterns and refine policy. Policy Analytics is a feature on Cisco DNA Center that discovers activities between endpoints, groups, and applications. This better equips IT teams to test and model segmentation policies. Figure 28 shows policy analytics for scalable groups, highlighting flows initiated on devices with the controller tag. Clicking the tag will provide additional details.

Figure 28 Policy Analytics



Policy Analytics works by correlating NetFlow information from access switches with endpoint information from ISE. NetFlow needs to be configured using Cisco DNA Center as collector and applied to access interfaces on the switches. The companion Implementation guide provides an example of a Day-N template to configure NetFlow.

Known Limitations and Recommendations

- NetFlow is supported on IE3300, IE3400, IE4000 and IE5000.
- NetFlow needs to be configured following the recommendations in NetFlow Recommendations.
- Policy Analytics support on IE switches displays traffic flows for Scalable Groups, ISE Profiles, or Stealthwatch host groups but it does not provide information on most and least active policies. This feature is not supported on industrial switches at this point.

What happens when the endpoint connects?

Consider an endpoint in the example, for example a PLC that connects to Cell-1. When the endpoint connects to the network, it is authenticated and authorized by ISE based on the network profile and it gets an SGT. Endpoints that do not match any profile can be assigned a default SGT so they can communicate and Cisco Cyber Vision Sensor can capture communication flows. Metadata from these flows is sent from the Cisco Cyber Vision Sensor to the Cisco Cyber Vision Center, which processes the data and sends endpoint attributes to ISE via pxGrid. After learning the new attributes, ISE triggers a Change of Authorization to the switch for that port. The endpoint gets authorized again with the appropriate profile and gets a new SGT (note that there is no interruption for endpoint connectivity during CoA).

Assuming SXP from access switch to zone switch is the chosen design for propagation, when the PLC is assigned an SGT, the access switch sends that information to the zone switch via SXP. An IP-to-SGT entry will be created in the zone switch for this PLC and the switch downloads the policies from ISE needed to protect this endpoint. A similar process happens when an end device is connected to Cell-2.

A communication flow from an endpoint in Cell-1 to an endpoint in Cell-2 can be enforced because the zone switch knows the tagging for both endpoints and has the right policies associated to them. Communication may be allowed or denied based on policy.

If the endpoint is not able to connect, you can use the Assurance Client Health page to diagnose issues. Another tool that could be used for troubleshooting is Endpoint Analytics, as described in the following section, because it displays SGT, ISE profiling, AAA information and other endpoint attributes.

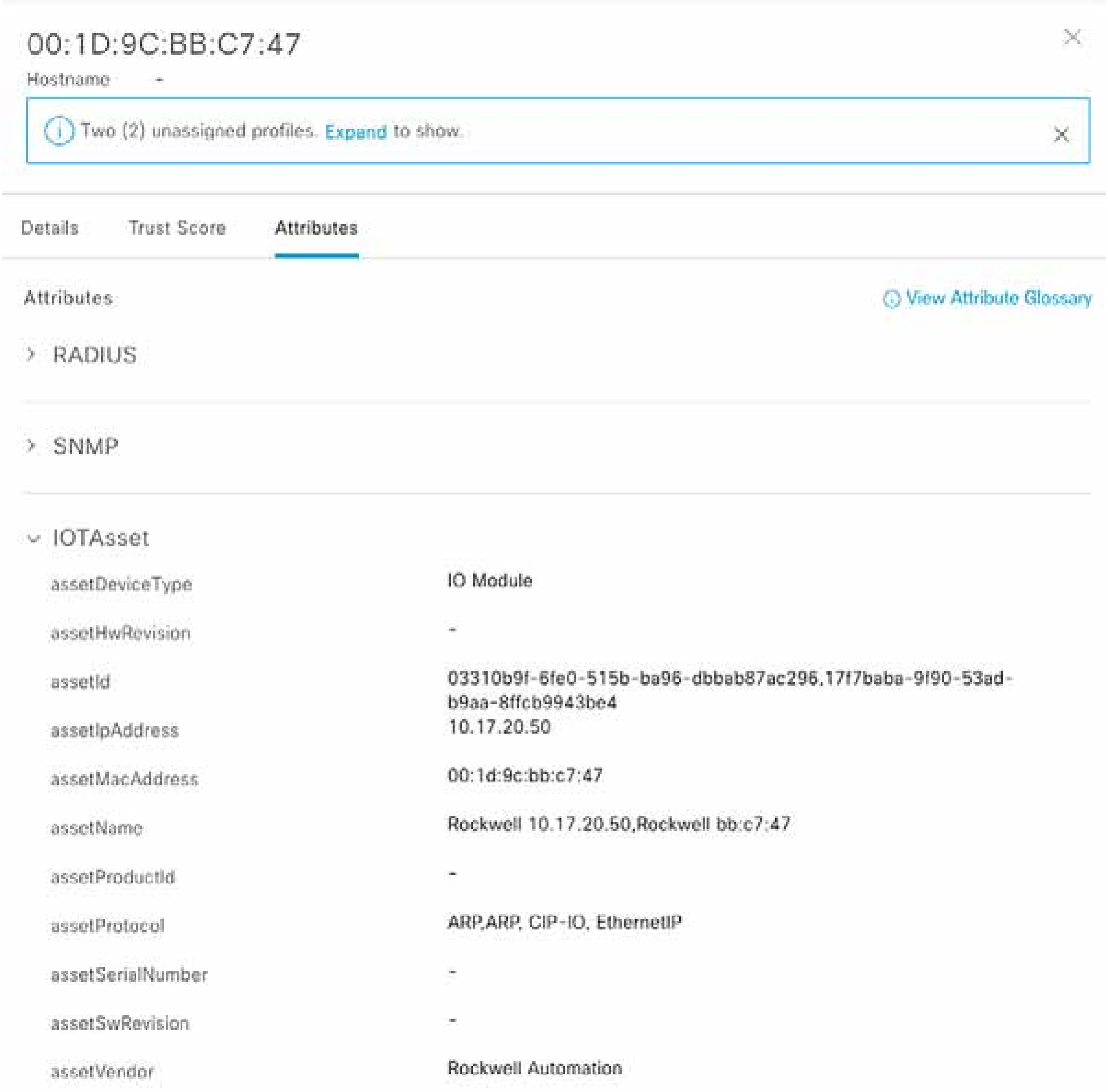
Endpoint Analytics

Cisco AI endpoint analytics is a feature in Cisco DNA Center that can identify new endpoint clients (cameras, machines, and other IoT devices) as they are connected to the network to determine (1) if they are authorized, (2) what profile they should have, and (3) what policies should be applied to this profile.

Endpoint Analytics uses different sources of data to get endpoint information. In the Industrial Automation solution, endpoint information comes from ISE, which uses pxGrid to send information about current sessions. If those endpoints are connected to a switch managed by Cisco DNA Center, the endpoint will be visible in Endpoint Analytics.

Figure 29 shows details for an endpoint as seen in Endpoint Analytics, highlighting IOTAsset attributes (learned via Cisco Cyber Vision Center).

Figure 29 Endpoint Analytics for Industrial Endpoint



00:1D:9C:BB:C7:47

Hostname -

Two (2) unassigned profiles. Expand to show.

Attributes

IOTAsset

assetDeviceType	IO Module
assetHwRevision	-
assetId	03310b9f-6fe0-515b-ba96-dbbab87ac296,17f7baba-9f90-53ad-b9aa-8ffcb9943be4
assetIpAddress	10.17.20.50
assetMacAddress	00:1d:9c:bb:c7:47
assetName	Rockwell 10.17.20.50,Rockwell bb:c7:47
assetProductId	-
assetProtocol	ARP,ARP, CIP-IO, EthernetIP
assetSerialNumber	-
assetSwRevision	-
assetVendor	Rockwell Automation

Note: Endpoint Analytics can be used to profile endpoints by creating profiling rules on Cisco DNA Center instead of ISE. Nevertheless, this is not applicable to Industrial Automation design because attributes learned from Cisco Cyber Vision (IOTasset) are required to profile industrial assets. Currently, IOTAsset attributes are not available for profiling rules. Because of that, this design uses ISE for profiling rules.

Appendix A—Cisco DNA Center Related Documentation

Refer to the following links for relevant Cisco DNA Center Documentation:

- Cisco DNA Center High Availability:
https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/ha_guide/b_cisco_dna_center_ha_guide_2_2_3.html

- Compatibility Matrix: https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-device-support-tables-list.html
- Cisco DNA Center Release Notes: https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-release-notes-list.html
- Cisco DNA Center & ISE Management Infrastructure Deployment Guide: https://cs.co/sda-infra-pdg
- Cisco DNA Center Install and Upgrade Guides: https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-installation-guides-list.html
- Cisco DNA Center Security Best Practices Guide: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/hardening_guide/b_dnac_security_best_practices_guide.html
- Cisco DNA Center End-User Guides: https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-user-guide-list.html

Appendix B–SMP Traps Configured

```
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flowmon
snmp-server enable traps call-home message-send-fail server-fail
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps power-ethernet police
snmp-server enable traps rep
snmp-server enable traps fru-ctrl
snmp-server enable traps entity
snmp-server enable traps envmon
snmp-server enable traps cpu threshold
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal lowspace
snmp-server enable traps port-security
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps license
snmp-server enable traps smart-license
snmp-server enable traps event-manager
snmp-server enable traps ipsla
snmp-server enable traps transceiver all
snmp-server enable traps ike policy add
snmp-server enable traps ike policy delete
snmp-server enable traps ike tunnel start
snmp-server enable traps ike tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
```

```
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps bfd
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps syslog
snmp-server enable traps bgp cbgp2
snmp-server enable traps dhcp
snmp-server enable traps hsrp
snmp-server enable traps ipmulticast
snmp-server enable traps isis
snmp-server enable traps msdp
snmp-server enable traps ospfv3 state-change
snmp-server enable traps ospfv3 errors
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps entity-diag boot-up-fail hm-test-recover hm-thresh-reached scheduled-test-fail
snmp-server enable traps cef resource-failure peer-state-change peer-fib-state-change inconsistency
snmp-server enable traps pimstdmib neighbor-loss invalid-register invalid-join-prune rp-mapping-change
interface-election
snmp-server enable traps errdisable
snmp-server enable traps vlan-membership
snmp-server enable traps alarms informational
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-trunk-down
snmp-server enable traps bulkstat collection transfer
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps rf
```