Deploying Identity and Mobility Services within a Converged Plantwide Ethernet Architecture

Design and Implementation Guide

February 2018

Cisco Validated Design

Document Reference Number: ENET-TD008B-EN-P

Preface

Converged Plantwide Ethernet (CPwE) is a collection of tested and validated architectures that are developed by subject matter authorities at Cisco and Rockwell Automation. The testing and validation follow the Cisco Validated Design (CVD) and Cisco Reference Design (CRD) methodologies. The content of CPwE, which is relevant to both operational technology (OT) and informational technology (IT) disciplines, consists of documented architectures, best practices, guidance and configuration settings to help manufacturers with the design and deployment of a scalable, reliable, secure and future-ready plant-wide industrial network infrastructure. CPwE can also help manufacturers achieve cost reduction benefits using proven designs that can facilitate quicker deployment while helping to minimize risk in deploying new technology.

Industrial IoT (IIoT) offers the promise of business benefits through the use of innovative technology such as mobility, collaboration, analytics, and cloud-based services. The challenge for manufacturers is to develop a balanced security stance to take advantage of IIoT innovation while maintaining the integrity of industrial security best practices. Deploying Identity and Mobility Services within a Converged Plantwide Ethernet Architecture CVD (CPwE Identity and Mobility Services), which is documented in this *Deploying Identity and Mobility Services within a Converged Plantwide Ethernet Architecture Design and Implementation Guide (DIG)*, outlines several security and mobility architecture use cases, with Cisco Identity Services Engine (ISE), for designing and deploying mobile devices, with FactoryTalk® applications, throughout a plant-wide Industrial Automation and Control System (IACS) network infrastructure. CPwE Identity and Mobility Services was tested and validated by Cisco Systems and Rockwell Automation.

Document Organization

This document contains the following chapters and appendices:

Chapter	Description
Chapter 1, “CPwE Identity and Mobility Services Overview”	Presents introduction to CPwE Identity and Mobility Services architecture, Secure Access Control, and Unified Network Access Policy Management for CPwE Identity and Mobility Services.
Chapter 2, “CPwE Identity and Mobility Services Design Considerations”	Presents an overview of CPwE Identity and Mobility Services Technology, wireless and wired access use case overview, design and deployment considerations, and overview of FactoryTalk mobile IACS applications.

Chapter	Description
Chapter 3, “Configuring the Infrastructure”	Describes how to configure CPwE Identity and Mobility Services infrastructure based on the design considerations of the previous chapters, covering the configuration of the wired and wireless network infrastructure, network services, Cisco ISE, and network and application security.
Chapter 4, “Troubleshooting the Infrastructure”	Describes Cisco ISE and wireless infrastructure troubleshooting.
Appendix A, “References”	List of references for CPwE design and implementation guides for network infrastructure services and security.
Appendix B, “Test Hardware and Software”	Hardware and software components used in CPwE Identity and Mobility Services testing.
Appendix C, “Acronyms and Initialisms”	List of acronyms and initialisms used in this document.
Appendix D, “About the Cisco Validated Design (CVD) Program”	Describes the Cisco Validated Design (CVD) process and the distinction between CVDs and Cisco Reference Designs (CRDs.)

For More Information

More information on CPwE Design and Implementation Guides can be found at the following URLs:

- Rockwell Automation site:
  - http://www.rockwellautomation.com/global/products-technologies/network-technology/architectures.page?
- Cisco site:
  - http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html

Note This release of the CPwE architecture focuses on EtherNet/IP™, which uses the ODVA, Inc. Common Industrial Protocol (CIP™) and is ready for the Industrial Internet of Things (IIoT). For more information on EtherNet/IP, see the following URL:

- http://www.odva.org/Technology-Standards/EtherNet-IP/Overview

CHAPTER 1

CPwE Identity and Mobility Services Overview

This chapter includes the following major topics:

Identity and Mobility Services Architecture Introduction

The prevailing trend in Industrial Automation and Control System (IACS) networking is the convergence of technology, specifically IACS operational technology (OT) with information technology (IT). Converged Plantwide Ethernet (CPwE) helps to enable IACS network technology convergence through the use of standard Ethernet, Internet Protocol (IP), network services, security services, and EtherNet/IP. A converged IACS network technology helps to enable the Industrial Internet of Things (IIoT).

IIoT offers the promise of business benefits through the use of innovative technology such as mobility, collaboration, analytics, and cloud-based services. The challenge for manufacturers is to develop a balanced security stance to take advantage of IIoT innovation while maintaining the integrity of industrial security best practices. Business practices, corporate standards, security policies and procedures, application requirements, industry security standards, regulatory compliance, risk management policies, and overall tolerance to risk are all key factors in determining the appropriate security stance.

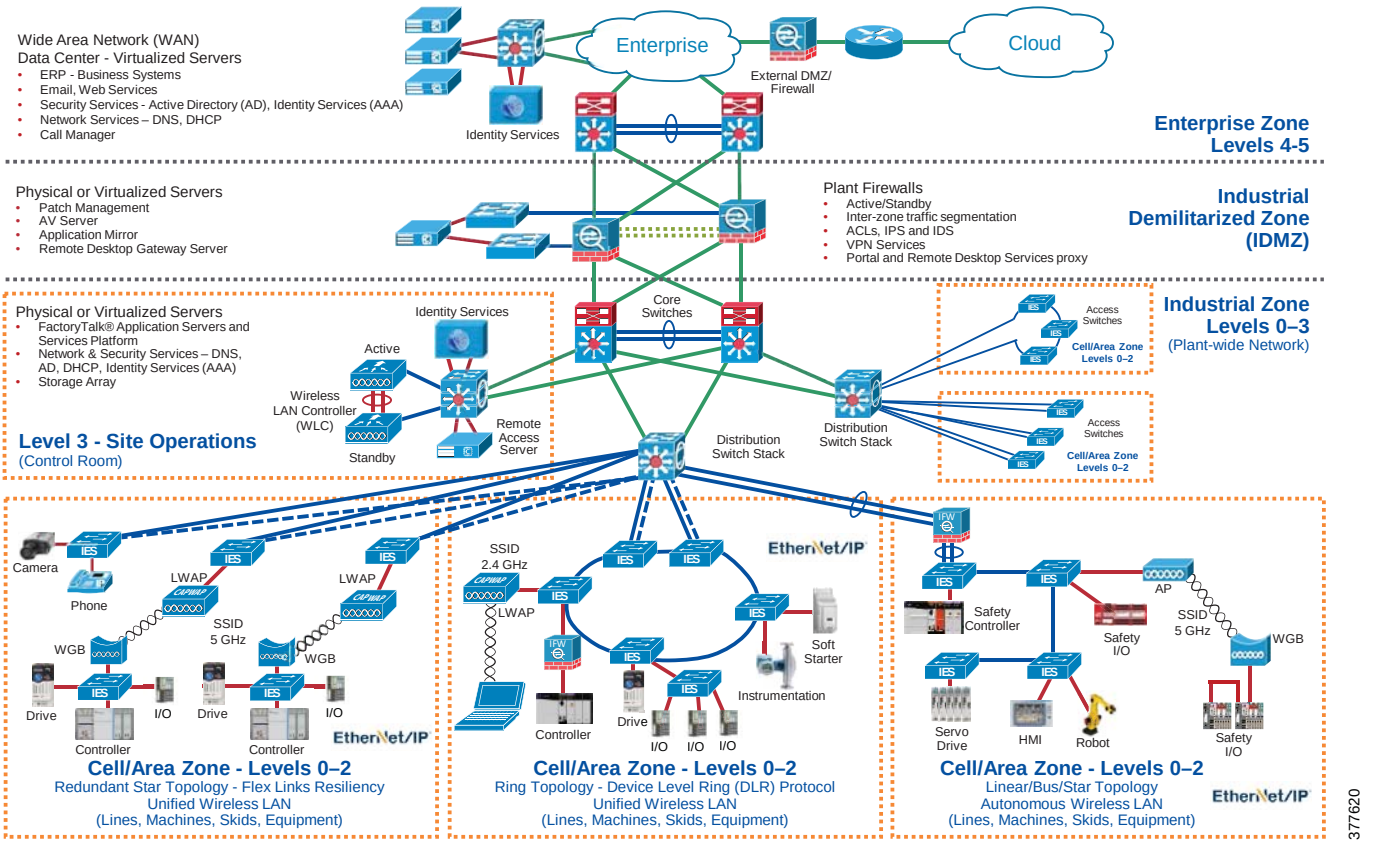
As access methods to the plant-wide industrial network expand, the complexity of managing network access security and controlling unknown risks continues to increase. With a growing demand for in-plant access by trusted industry partners (for example, system integrator, OEM, or vendor), IACS applications within the CPwE architecture (Figure 1-1) face continued security threats. A holistic industrial security stance is necessary in order to help protect the integrity of safety and security best practices while also helping to enable identity and mobility services. No single product, technology, or methodology can fully secure plant-wide architectures. Protecting IACS assets requires a holistic defense-in-depth security approach that addresses internal and external security threats. This approach uses multiple layers of defense (administrative, technical, and physical), using diverse technologies for threat detection and prevention at separate IACS levels, by applying policies and procedures that address different types of threats. The CPwE Industrial Security Framework (Figure 1-2), which applies a holistic defense-in-depth approach, is aligned to industrial

security standards such as IEC-62443 (formerly ISA99) Industrial Automation and Control Systems (IACS) Security and NIST 800-82 Industrial Control System (ICS) Security.

The management and security of the evolving coexistence of technologies within the plant require a different approach. CPwE uses the Cisco Identity Services Engine (ISE) to support centrally managed secure wired computer or wireless mobile device (computer, tablet, smartphone) access to the IACS networks by plant personnel and trusted partners.

This release of CPwE Identity and Mobility Services outlines several security and mobility architecture use cases, with Cisco ISE, for designing and deploying mobile devices, with FactoryTalk® software applications, throughout a plant-wide IACS network infrastructure. CPwE Identity and Mobility Services is brought to market through a strategic alliance between Cisco Systems and Rockwell Automation.

Figure 1-1 CPwE Architecture



Secure Access Control

As the number of known and unknown mobile devices (computer, tablet, smartphone) connecting to the IACS network continues to increase, methods for managing disparate security solutions and mitigating risks continue to mature. Physical security is no longer adequate to prevent attempts to access an IACS network. With the continued proliferation of trusted partner mobile device connectivity and the already constrained plant-wide operational resources, the potential impact of failing to identify and remediate security threats introduces significant risk to plant-wide operations. Protecting IACS assets from mobile devices requires a

centrally manageable defense-in-depth security approach to help with threat detection and prevention. Cisco ISE supports different levels of secure wired and wireless access to the IACS networks by plant personnel and trusted partners.

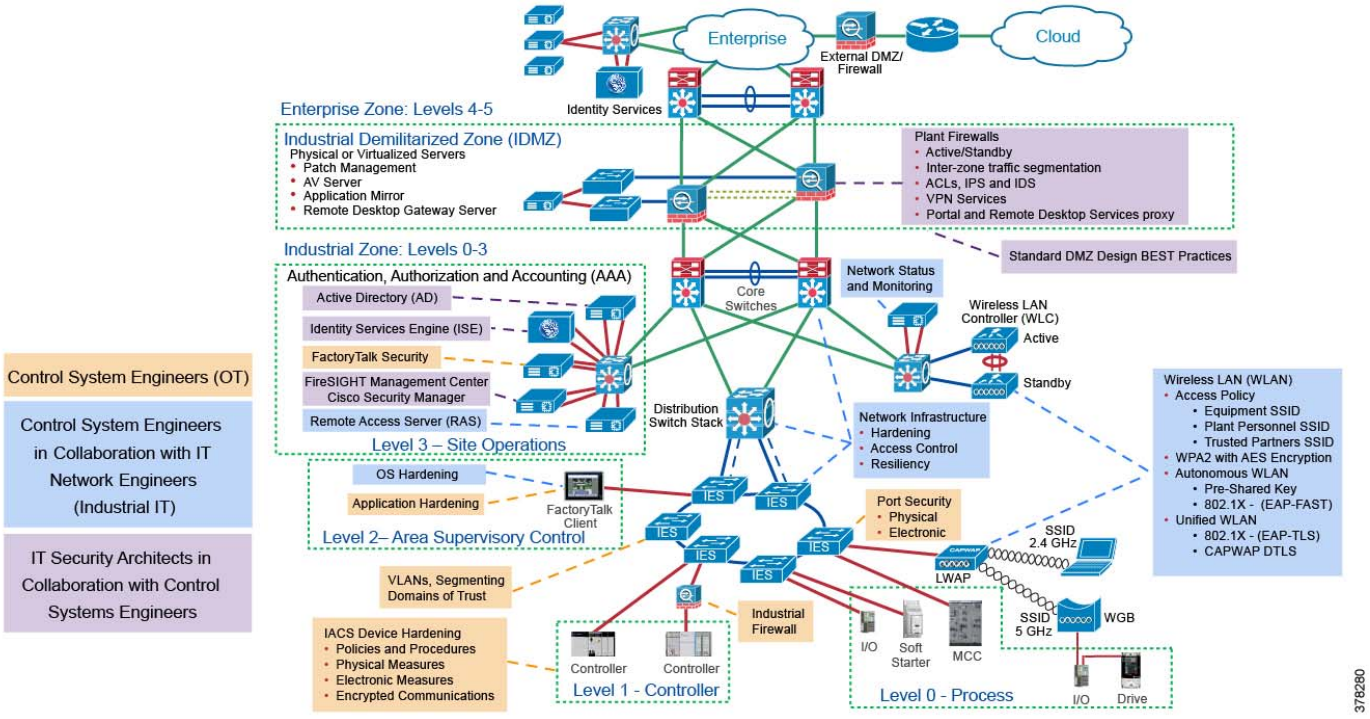
Designing and implementing a comprehensive IACS network access security framework (Figure 1-2) should be a natural extension to the IACS and not implemented as an afterthought. The industrial network access security framework should be pervasive and core to the IACS. However, atop existing IACS deployments, the same defense-in-depth layers can be applied incrementally to help improve the access security stance of the IACS.

One size does not fit all when it comes to risk tolerance. What is acceptable to one manufacturer may be unacceptable to another and vice versa. The CPwE architecture supports scalability, which includes the degree of holistic industrial security (Figure 1-2) applied to a plant-wide security architecture. Scalable security comes in many forms. Choices in multiple layers of diverse technology are available to apply at multiple levels of the IACS application based on risk mitigation requirements to help meet the manufacturer's tolerance to risk.

CPwE holistic defense-in-depth layers (Figure 1-2) include:

- **Control System Engineers** (highlighted in tan)—IACS device hardening (for example, physical and electronic), infrastructure device hardening (for example, port security), network segmentation (trust zoning), industrial firewalls (with inspection) at the IACS application edge, IACS application authentication, authorization, and accounting (AAA).
- **Control System Engineers in collaboration with IT Network Engineers** (highlighted in blue)—Computer hardening (OS patching, application white listing), network device hardening (for example, access control, resiliency), and wired and wireless LAN access policies.
- **IT Security Architects in collaboration with Control Systems Engineers** (highlighted in purple)—Identity and Mobility Services (wired and wireless), Active Directory (AD), Remote Access Servers, plant firewalls, and Industrial Demilitarized Zone (IDMZ) design best practices.

Figure 1-2 CPwE Industrial Network Security Framework



Unified Network Access Policy Management for CPwE

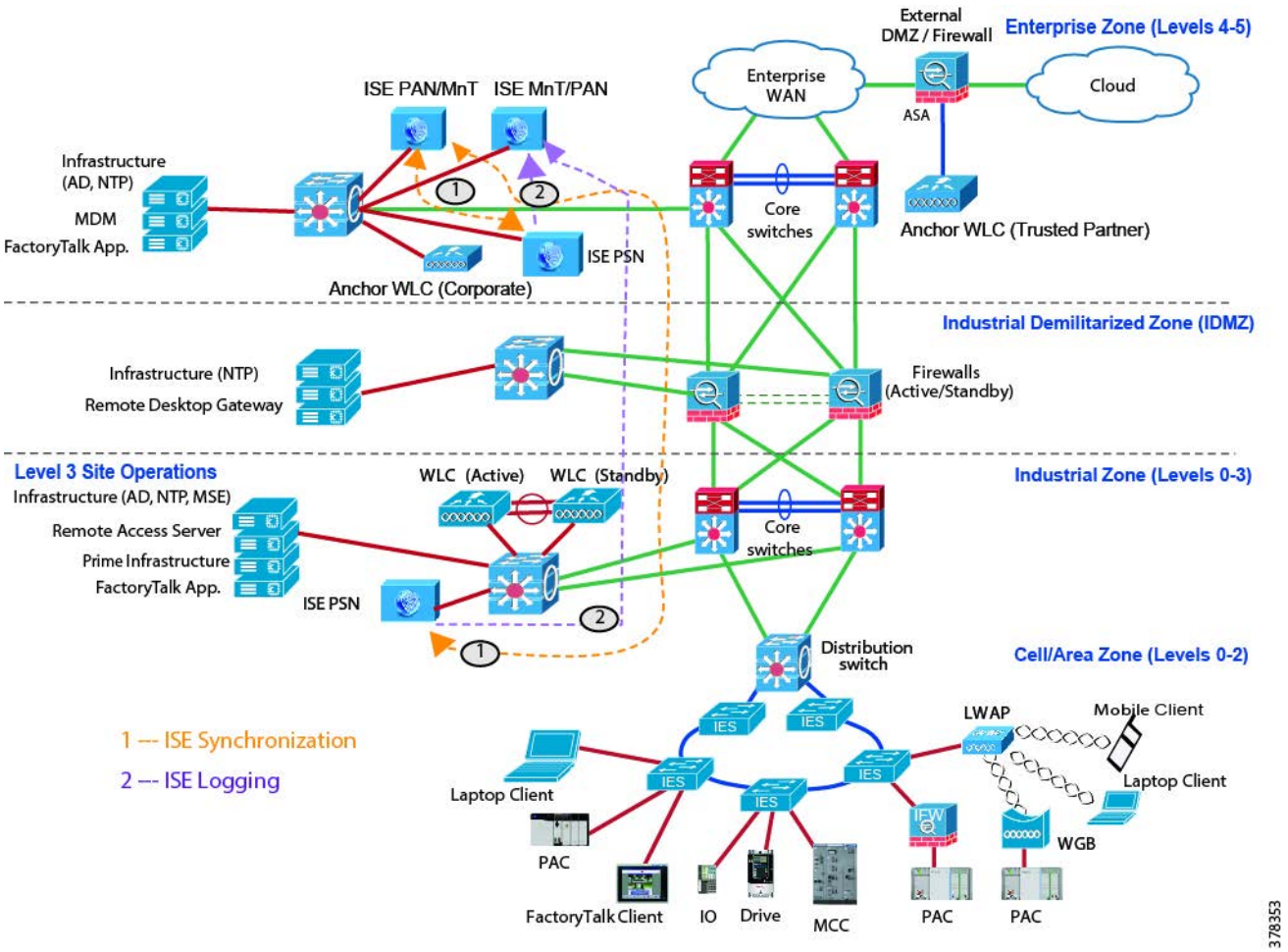
The Cisco Identity Services Engine empowers enterprise IT to help achieve highly secure wired and wireless access within the plant by providing:

- Comprehensive centralized policy management
- Streamlined device onboarding
- Dynamic enforcement
- Mobile device (computer, tablet, smartphone) posturing

A rules-based, attribute-driven policy model is provided to create access control based upon IEEE-802.1X authentication and authorization policies. The 802.1X standard describes authentication protocols and mechanisms for wired and wireless access. Cisco ISE includes the ability to create fine-grained authorization policies that include the association of a user or a mobile device to an associated VLAN or an associated downloadable access control list (DACL). Attributes can also be created dynamically and saved for later use as new mobile devices are introduced to the IACS network.

As shown in Figure 1-3, CPwE Identity and Mobility Services support multiple external identity repositories, including Active Directory for both authentication and authorization. Plant-wide network administrators may centrally configure and manage both wired and wireless access for employees, guests, vendors, and trusted partners based upon authentication and authorization services available from a web-based GUI console. Cisco ISE simplifies administration by providing integrated central management from a single administrative interface for distributed network environments.

Figure 1-3 Unified Identity and Mobility Services for Wired and Wireless



Through the application of Cisco ISE, provision and posture policies are applied across the IACS network in real-time, creating a consistent user access experience to services from wired and wireless connections. Cisco ISE allows IT to define roles such as employees and trusted partners. These roles can be configured to permit and limit access to assets within the Industrial Zone, the Industrial Demilitarized Zone (IDMZ), and the Enterprise Zone.

The Allen-Bradley® Stratix® and Cisco industrial Ethernet switches (IES) work in conjunction with Cisco ISE to apply and enforce the security policies that are configured. For example, if an employee attaches to the IACS network via wired access in the Industrial Zone with a computer, the IES sends the hardware and user information to Cisco ISE. Cisco ISE will send the preconfigured network security policies to the Allen-Bradley Stratix or Cisco IES where the user's access will be limited by the security policy. It is also possible to limit or direct traffic of unknown devices with a Cisco ISE security policy.

Cisco ISE services for wireless access use the Cisco wireless LAN controllers (WLC) to facilitate authentication and authorization of mobile devices (computer, tablet, smartphone) accessing the IACS network. Cisco ISE allows IT to define a set of trusted partners, and for each trusted partner, define a set of authentication and authorization policies across both the wired and wireless environments (see "Unified Wireless Access Overview" section on page 2-19 and "Wired Access Overview" section on page 2-49).

CPwE Identity and Mobility Services CVD

An IACS is deployed in a wide variety of discrete and process manufacturing industries such as automotive, pharmaceuticals, consumer packaged goods, pulp and paper, oil and gas, and mining and energy. IACS applications are made up of multiple control and information disciplines such as continuous process, batch, discrete, and hybrid combinations. One of the challenges facing manufacturers and OEMs is the need to enable secure connectivity from mobile devices to plant-wide IACS applications in order to take advantage of the business benefits associated with the IIoT.

CPwE is the underlying architecture that provides standard network and security services for control and information disciplines, devices, and equipment found in modern IACS applications. Cisco ISE is used in conjunction with the CPwE architecture to provide an additional and dynamic layer of network access control security by identifying the mobile device, IACS application (FactoryTalk), and logged-on user to push security policies to the network infrastructure that the mobile device is accessing. The CPwE architecture (Figure 1-1), through testing and validation by Cisco and Rockwell Automation, provides design and implementation guidance, test results, and documented configuration settings that can help to achieve the real-time communication, reliability, scalability, security, and resiliency requirements of modern IACS applications for manufacturers and OEMs. Cisco ISE builds on top of the defined best practices and network architecture with a centrally managed architectural model where the IT department maintains the management of the Cisco ISE platform that operates in the Industrial Zone.

Device profiling within the Industrial Zone is based upon a device profiler service, which identifies specific mobile devices (computer, tablet, smartphone) connecting to the plant-wide network. The specific mobile devices are profiled based on the endpoint profiling policies configured within Cisco ISE. Based on the user, mobile device, or IACS application identity, Cisco ISE grants permission (via secure access rules) to the specific mobile devices to access the plant-wide network based on the result of the policy evaluation or routes the untrusted mobile device to an administratively defined safe destination.

CPwE Identity and Mobility Services enables centralized plant-wide flexibility in deciding how to implement guest policies. Cisco ISE provides a self-service registration portal for plant personnel, vendors, partners, and guests to register and provision new devices automatically according to the business policies defined by the plant-wide operations. CPwE Identity and Mobility Services enables IT to establish automated plant-wide device provisioning, profiling, and posturing while keeping the process simple for plant personnel to get their mobile devices onto the plant-wide network with limited IT help.

The following is a synopsis for this release of CPwE Identity and Mobility Services CVD:

- Identity Services Engine (ISE) Overview
- Unified and Autonomous Wireless LAN (WLAN) Architecture Overview
- Mobile Device Management (MDM) and Mobile Service Engine (MSE) Overview
- Mobile IACS Applications Overview
  - Tested and validated: FactoryTalk TeamONE™ (diagnostic modules) software and ThinManager® software
  - Referenced: FactoryTalk View, FactoryTalk ViewPoint, FactoryTalk Batch View, FactoryTalk VantagePoint®, FactoryTalk Analytics for Devices software, Studio 5000® software
- Security and Mobility Architecture Use Case Overview
- Design and Implementation Considerations

CHAPTER 2

CPwE Identity and Mobility Services Design Considerations

This chapter includes the following major topics:

CPwE Identity and Mobility Services Technology Overview

With the introduction of secure employee and trusted partner (OEM, system integrator, vendor) access, the use of Cisco ISE as an identity and access control policy platform enables organizations to enforce compliance, enhance infrastructure security, and streamline their service operations. Its architecture allows an organization to gather real-time contextual information from the network, users, and devices to make proactive policy decisions by tying identity into various network elements including industrial Ethernet Switches (IES) and Wireless LAN Controllers (WLC).

This deployment uses Cisco ISE as the authentication and authorization server for the wired and wireless networks using the Remote Authentication Dial-In User Service (RADIUS) protocol. Cisco ISE uses Microsoft Active Directory (AD) as an external identity source to access resources such as users, computers, groups, and attributes. Cisco ISE supports Microsoft AD sites and services when integrated with AD. Cisco ISE needs an identity certificate that is signed by a Certificate Authority (CA) server so that it can be trusted by mobile devices, gateways, and servers.

This section describes the distributed Cisco ISE system, integration of Cisco ISE with Mobile Device Management (MDM), Mobility Service Engine (MSE), Active Directory and Certificate Services, and provides design recommendations for wired and wireless CPwE Identity and Mobility Services for FactoryTalk Industrial Automation and Control System (IACS) applications.

Cisco ISE Distributed Deployment

Within the CPwE architecture, Cisco and Rockwell Automation recommend to deploy the Cisco ISE platform as a distributed system. In this solution, the corporate IT department manages the Cisco ISE platform and is responsible for applying and managing authentication and authorization policies throughout the company.

In the distributed installation, Cisco ISE system is divided into three discrete nodes (personas)—Administration, Policy Service, and Monitoring—which are described as follows:

- **Policy Administration Node (PAN)** allows the Enterprise IT team to perform all administrative operations on the distributed Cisco ISE system. The PAN (located in the Enterprise Zone) handles all system configurations that are related to functionality such as authentication and authorization policies. A distributed Cisco ISE deployment can have one or a maximum of two nodes with the Administration persona that can take on the primary or secondary role for high availability.
- **Policy Service Node (PSN)** provides client authentication, authorization, provisioning, profiling, and posturing services. The PSN (located within the Industrial and the Enterprise Zone) evaluates the policies and provides network access to devices based on the result of the policy evaluation. At least one node in a distributed setup should assume the Policy Service persona and usually more than one PSN exists in a large distributed deployment.
- **Monitoring Node (MnT)** functions as the log collector and stores log messages and statistics from all the Administration and Policy Service Nodes in a network. The MnT (located in the Enterprise Zone) aggregates and correlates the data in meaningful reports for the enterprise IT and OT personnel. A distributed Cisco ISE system can have at least one or a maximum of two nodes with the Monitoring persona that can take on primary or secondary roles for high availability.

For optimal performance and resiliency, Cisco and Rockwell Automation provide these recommendations for the CPwE Identity and Mobility Services architecture:

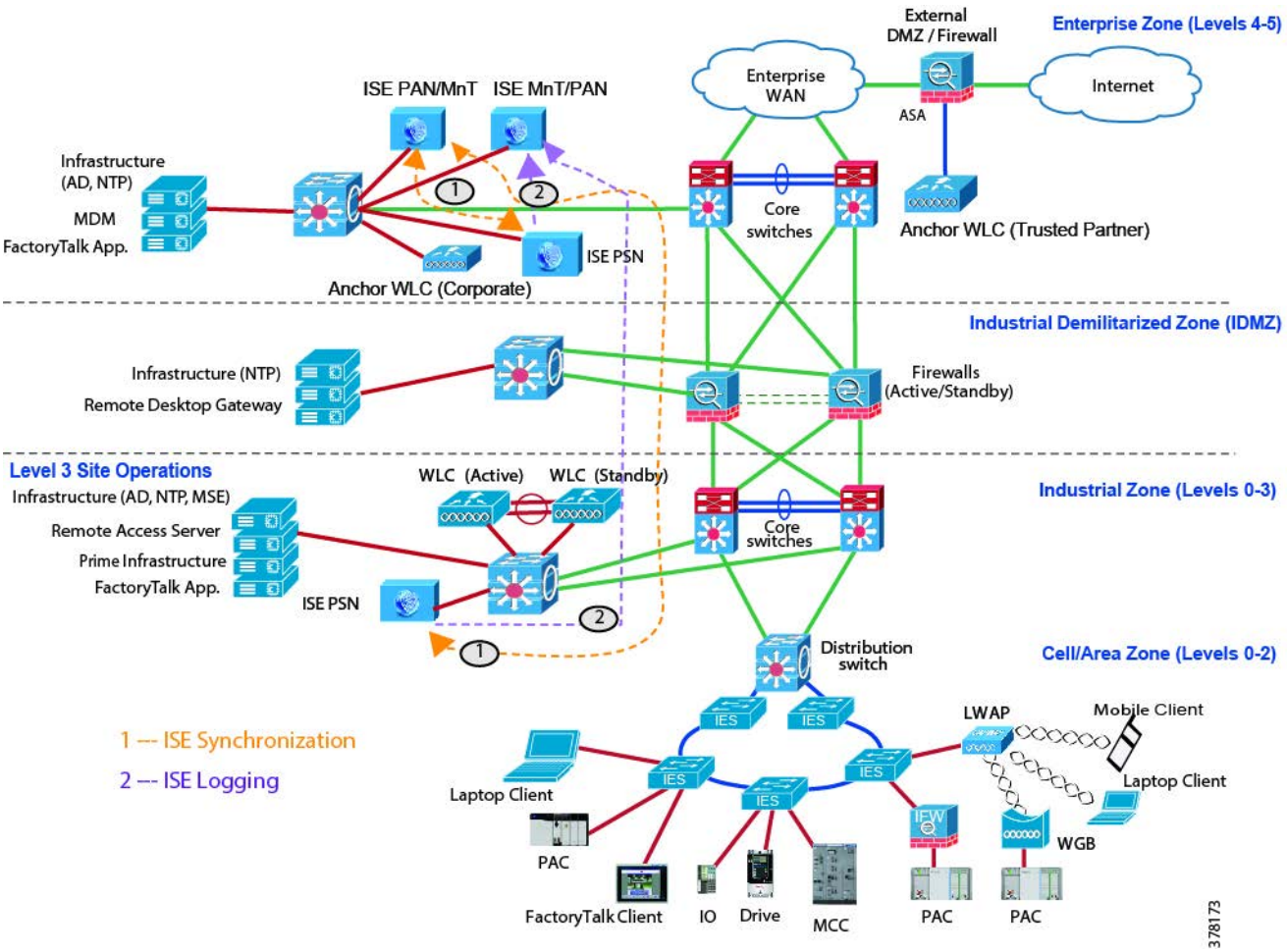
- Administration and Policy Service personas should be configured on different Cisco ISE nodes.
- Monitoring and Policy Service personas should not be enabled on the same Cisco ISE Node. The Monitoring node should be dedicated solely to monitoring for optimum performance.
- A PSN should be placed in the Industrial Zone (Levels 0-3) to provide services for clients in the Industrial Zone. If the Enterprise and Industrial Zones become isolated, any existing clients will still be able to securely access the network.
- A PSN should also be present in the Enterprise Zone to authenticate corporate mobile users who connect to the corporate network through the IDMZ in a secure data tunnel. This scenario is covered in details later in the document.

Based on the recommendations above, a typical distributed Cisco ISE deployment in the CPwE architecture consists of the following nodes (hardware appliances or VMs) as shown in Figure 2-1:

- 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

Note The number of PSN in the Enterprise and Industrial Zones may depend on the company size, the number of active clients, redundancy requirements, and geographical distribution (for example, one PSN per each plant).

Figure 2-1 Distributed CPwE Identity and Mobility Services Architecture



As indicated in Figure 2-1:

1. The Enterprise Zone Primary PAN/Secondary MnT synchronizes its policy configurations with the Industrial and Enterprise Zone PSNs.
2. The Industrial and Enterprise Zone PSNs send the detailed logs to the Enterprise Zone Primary MnT/Secondary PAN node.

High Availability with Cisco ISE

In a high availability configuration, the Primary PAN is in the active state to which all configuration changes are made. The Secondary PAN is in the standby state and will receive all configuration updates from the Primary PAN.

Cisco ISE supports automatic failover for the Administration persona. If the Primary PAN goes down, an automatic promotion of the Secondary PAN is initiated. For this, a non-administration node (a PSN) does periodic health checks for each of the administration nodes. When the failed PAN comes back online, it takes a secondary role until promoted manually.

Cisco ISE also supports redundancy for MnT nodes. Both the primary and secondary MnT collect log messages. In case the primary MnT goes down, the secondary MnT automatically becomes the primary node.

High availability for Policy Services nodes is achieved by placing two or more PSNs into a node group and configuring multiple PSNs as RADIUS servers on the network access devices such as WLCs and IES. The PSNs within a node group exchange heartbeat messages to detect node failures. If a PSN fails, some of its clients may be using the ISE web portal for provisioning or other purposes. In this case, one of the PSNs in the node group can force those clients to reauthenticate to the new PSN.

Note For the recommended installation and deployment of distributed Cisco ISE system within the CPwE architecture, please follow the best practices and deployment guidelines in the following documents:

- Cisco Identity Services Engine Administrator Guide, Release 2.2
  http://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_010.html
- Cisco Identity Services Engine Installation Guide, Release 2.2
  http://www.cisco.com/c/en/us/td/docs/security/ise/2-2/install_guide/b_ise_InstallationGuide22.html

Mobile Device Management (MDM)

Mobile devices such as smartphones provide great convenience and a productivity increase for workers. At the same time, introducing mobile devices in the Industrial Zone network adds security risks that must be addressed. If a mobile device is allowed unrestricted Internet access from the corporate network or outside the corporate network (via cellular or home connection), there is always a risk of compromising the mobile device with malware leading to data theft or operation disruption.

One way to control the risk is to only allow “on premise” mobile devices without cellular access and with no or very limited Internet access. If this is not practical due to operational requirements, security solutions like Mobile Device Management (MDM) with strong mobility and security policies are necessary.

MDM platforms help to secure, monitor, and manage mobile devices, including both corporate-owned mobile devices as well as employee-owned Bring Your Own Devices (BYOD). MDM functionality typically includes Over-the-Air (OTA) distribution of policies and profiles, digital certificates, applications, data and configuration settings for all types of devices.

There are a wide range of third-party MDM solutions that set device policy in the same way that Cisco ISE sets network policy. An MDM can set mobile device use policies such as encrypted storage or pin lock requirements, wipe the devices over the air, and disable the use of features such as the camera and audio recorder. With the addition of MDM client software, the administrator can gather additional information about installed applications and set more comprehensive policies such as alerts when a blacklisted application is active or the device has been rooted or jailbroken.

While Cisco ISE provides critical policy functionality to enable the BYOD solution, it has limited awareness of mobile device posture. On the other hand, MDM solutions have such device posture awareness, but are quite limited as to network policy enforcement capacity.

Therefore, to complement the strengths of both Cisco ISE and MDM platforms, Cisco ISE includes support of an MDM integration API which allows it to do both:

- Pull various informational elements from the MDM server in order to make granular network access policy decisions that include mobile device details and/or posture status.
- Push administrative actions to the managed mobile devices (such as remote wiping) using the MDM server.

Note For information about ISE integration with MDM, please refer to the following URL: https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_01000.html

Location Based Services (LBS)

In the CPwE Identity and Mobility Services architecture, Cisco ISE integration with Mobility Services Engine (MSE) provides access to users based on their specific physical location within the Industrial Zone. This ability adds another level of context by which access is authorized.

Users can be granted access to certain IACS resources while they are in a particular Cell/Area Zone or even in a particular location within the Zone. When an individual leaves the designated area, access to specific information is automatically denied, protecting confidential data and access to resources. For example, within the Industrial Zone, maintaining schedules, processes, and quality control requires that only authorized personnel have access to machines. With location-based network access manufacturers can allow access to IACS applications and changes to IACS devices only when employees are on the plant floor. This level of control mitigates the risk of unauthorized parties hijacking mobile devices to disrupt operations.

The location-based authorization enabled by the integration of MSE with Cisco ISE increases the granular control administrators have and their ability to be more sensitive in their access authorization. MSE will also help enforce location-based policies by periodically checking for location changes and automatically reauthorizing the user if a location change is detected.

The integration of Cisco MSE with Cisco ISE:

- Enables you to configure location hierarchy across all location entities.
- Applies MSE location attributes to access requests to be used in your authorization policy.
- Checks the MSE periodically (every 5 minutes) for location changes.
- Reauthorizes access or updates the policy based on the new location.

Note For information about ISE integration with MSE, please refer to the following URL: https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_010010.html

Active Directory Services

While Cisco ISE can maintain an internal list of users for authentication purposes, most organizations rely on an external directory as the main identity source. By integrating with Microsoft Active Directory (AD), a single source for identity objects, such as AD users and groups, can be used in the authorization process.

Companies need a central repository of information about people and their access rights that applies to both the Industrial and Enterprise Zones. AD services in the Industrial Zone should be designed to allow secure replication of information across the IDMZ while being able to operate independently if necessary.

In addition to providing identity to secure network access, the AD accounts and groups can be linked to the FactoryTalk Security accounts which provide a layer of IACS application security using the same identity for employees.

The following sections describe AD deployment scenarios and provide design recommendations for CPwE Identity and Mobility Services.

Active Directory Overview

Active Directory Domain Services (AD DS) provide a distributed database of information about network resources and application data. AD DS organize network elements, such as users, computers, and other devices, into a hierarchical structure that includes the Active Directory forest, domains in the forest, and organizational units (OUs) in each domain. In addition to logical hierarchy, computers in AD DS can be grouped into site objects which typically represent a physical location. A server that is running AD DS is called a Domain Controller (DC).

- A **forest** acts as a security boundary for an organization and defines the scope of authority for administrators. By default, a forest contains a single domain, which is known as the forest root domain.
- A **domain** is a logical group of network objects (computers, users, devices) that share the same AD database. An AD domain supports a number of core functions including network-wide user identity, authentication, and trust relationships. Additional domains can be created in the forest to provide partitioning of AD DS data. Multiple domain structure is primarily used to create administrative boundaries within the organization.
- **OUs** simplify the management of large numbers of objects by the delegation of full or limited authority to other users or groups. OUs are used more often than domains to provide structure and to simplify the implementation of policies and administration.
- **Sites and Subnets** represent the physical topology of the organization and help to control data replication and to scale globally over a network with limited bandwidth.

AD DS implements security with a logon authentication and access control to resources in the directory. Authorized network users and administrators can use a single network logon to access resources anywhere in the network. Policy-based administration allows simplified management of even the most complex network.

An AD replication service distributes directory data across a network. Any change to directory data is replicated to all DCs in the domain.

Note For information about Active Directory Domain Services, please refer to the following URL: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/ad-ds-getting-started

Active Directory Deployment in the CPwE Architecture

The tested and validated deployment of the AD DS in the CPwE architecture is based on the AD implementation in a single domain with multiple sites. A single AD domain for the Enterprise and Industrial Zones maintains a single identity and access policy repository for all employees in a company.

To deploy the CPwE architecture topology, the addition of an Active Directory Domain Controller (AD DC) in the Industrial Zone is required. The Industrial Zone is placed in its own AD site. Establishing separate sites for the Industrial and Enterprise Zones provides the following benefits:

- Efficient use of bandwidth for replication in case of WAN connectivity.
- Detailed control of replication behavior, for example schedule.
- Industrial assets can authenticate to the local DC.

Note For best practices and deployment guidelines when installing AD DS, refer to the following URL: https://technet.microsoft.com/en-us/library/hh472160.aspx

Active Directory Replication across IDMZ

The CPwE architecture for AD implements bi-directional replication between the Enterprise DC and the Industrial Zone DC. An AD administrator should be able to create, delete and update accounts in the Industrial Zone and the changes will be replicated to the Enterprise Zone and vice versa.

Companies may also choose one-directional replication (Enterprise DC to Industrial DC only) due to security policies and management practices.

Note For information about Active Directory replication, please refer to the following resources:

- How Active Directory Replication Works
  https://technet.microsoft.com/en-us/library/cc772726(v=ws.10).aspx
- Active Directory Replication Technologies
  https://technet.microsoft.com/en-us/library/cc776877%28v=ws.10%29.aspx

For information about configuring AD replication across the IDMZ, please refer to:

- Securely Traversing IACS Data across the Industrial Demilitarized Zone
  http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td009_-en-p.pdf

Multiple AD Domains

Many companies choose to implement a separate AD domain for the Industrial Zone or in some cases multiple AD domains for each plant or even for individual IACS deployments such as process control systems (PCS). These domains may be part of a single AD forest or separate forests with trust relationships between each other or may be completely isolated from the Enterprise AD.

Some reasons for selecting and maintaining the multi-domain architecture might include a manufacturer's security policies and risk assessment, requirements to support legacy systems and maintain separate user databases, separation of administrative duties between IT and OT personnel, and different policies and procedures between zones.

Several possible scenarios exist:

1. Isolated domains—The Industrial Zone or individual IACS deployments have their own AD domain in a forest that is completely isolated from any other domains with no trust relationships.
2. Domain trusts in a single forest—The Industrial Zone or individual IACS deployments have their own domains which are part of a larger forest with trusts established to a corporate domain.

   This setup could be complex to configure and more difficult to troubleshoot.
3. Single corporate domain with multiple sites—The Industrial Zone is part of the corporate domain as a separate site with its own domain controllers.

   This model has been selected for the CPwE Identity and Mobility Services architecture. A single AD domain for the Enterprise and Industrial Zones simplifies configuration and management while maintaining a single identity and access policy repository for all employees in a company.

While only single domain design has been validated for the CPwE Identity and Mobility Services architecture, the same infrastructure can, in principle, support a multiple domains model and provide similar functionality. For example, Cisco ISE supports multi-domain environments if trust relationships are established between domains.

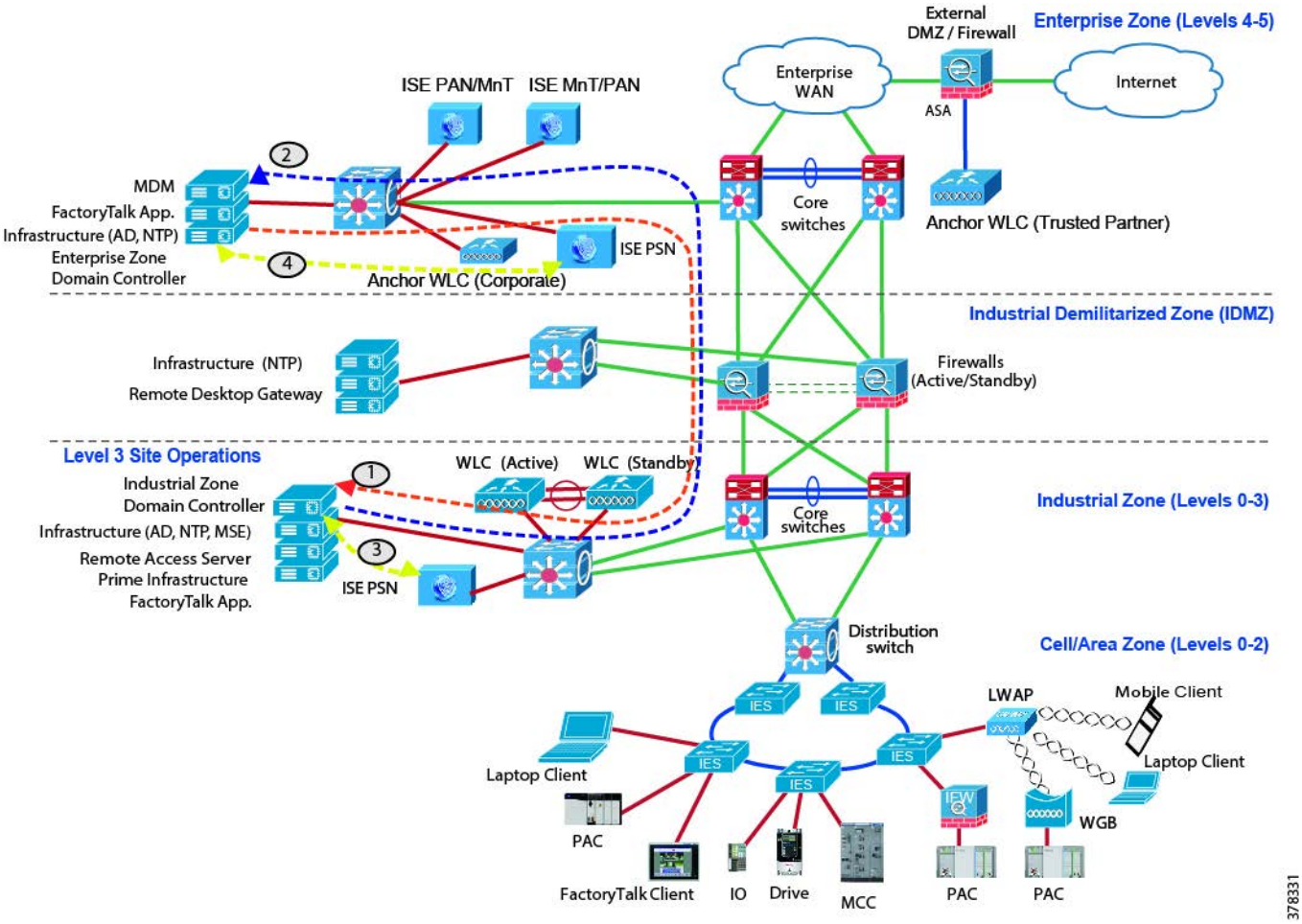
Active Directory and Cisco ISE Integration

Cisco ISE uses Microsoft AD as an external identity source to access resources such as users, computers, groups, and attributes. Cisco ISE retrieves user or computer attributes and groups from AD for use in authorization policy rules.

Cisco ISE also supports certificate retrieval from AD for user and computer authentication that uses the Extensible Authentication Protocol with Transport Layer Security (EAP-TLS) protocol. After Cisco ISE retrieves the certificate, it performs a binary comparison of this certificate with the client certificate(s). When a match is found, the user or computer authentication is passed.

Figure 2-2 illustrates the inter-operation between Cisco ISE and AD DCs as well as AD replication between the DCs in the Industrial and Enterprise Zones.

Figure 2-2 AD Replication and Integration with Cisco ISE



As indicated in Figure 2-2:

1. The Enterprise DC replicates any changes to the Industrial Zone DC.
2. The Industrial DC replicates any changes to the Enterprise Zone DC.
3. Industrial PSN communicates with the Industrial DC to authenticate users in the Industrial Zone.
4. Enterprise PSN communicates with the Enterprise DC to authenticate users in the Enterprise Zone.

Certificate Services

A certificate is an electronic document that identifies an individual, a server, a device, or other entity and associates that entity with a public key. Certificates can be self-signed or digitally signed by an external Certificate Authority (CA). A CA-signed digital certificate is considered industry standard and more secure.

Certificates are used in a network to provide secure access. Cisco ISE uses certificates for internode communication, EAP-TLS authentication of mobile devices, and communication with external servers and all the end-user portals (guest, sponsor, and personal devices portals).

The following sections describe certificate services and provide design recommendations for CPwE Identity and Mobility Services.

Certificate Services Overview

Public Key Infrastructure (PKI) is a system of services and procedures for lifecycle management of public key certificates. Depending on the manufacturer's security policy, PKI and certificate-based authentication methods can be required for:

- User network access, both wired and wireless, using 802.1X authentication.
- Authentication of network devices, for example servers and wireless APs.
- Encryption and/or authentication of e-mail messages and other documents.
- Application authorization with code signing.
- Web server authentication for Transport Layer Security (TLS) communication.
- Authentication between mutually trusted devices for IPsec and SSL VPN.

When PKI is implemented as Active Directory Certificate Services (AD CS) in a domain, the following features are available:

- Manual certificate enrollment of users using the web-based service or the Certificates Microsoft Management Console (MMC) snap-in.
- Automatic certificate enrollment of users via the AD group policy.
- Publishing and automatic distribution of trusted root certificates, issued certificates, and Certificate Revocation Lists (CRL) using AD.

PKI Components and Functions

PKI has multiple operational components that interact with each other during certificate issuance, revocation, validation, and authentication (see Figure 2-3):

- **Certificate Policy and Certificate Practice Statement** are documents that describes the general PKI architecture, practices, and procedures for key generation and storage, certificate issuance, renewal and revocation, operational and technical controls, and related legal matters. Having comprehensive and accurate policies and certificate practices is a critical step in helping to create a reliable PKI which should precede any PKI server deployment.
- **Certification Authority (CA)** is a trusted entity that manages and issues public key certificates for secure network communication. CAs can issue certificates to other CAs in the PKI or directly to end users (PKI subscribers). The CA also provides certificate status to relying parties.
- **Registration Authority (RA)** verifies the information provided by a requester of a digital certificate, interacts with the CA on behalf of the subscriber, and interacts with subscribers for certificate requests, revocation requests, and key compromise and recovery requests.

In smaller deployments, RA functions are often reside on the same server with the CA.

- **PKI Subscribers** are end devices (users, computers, servers, network devices, applications) that request and obtain certificates from the CA. Subscribers present their certificates for authentication purposes to relying parties.

  PKI subscribers can obtain their certificates through auto-enrollment using AD group policy or manually through Certificate Signing Requests (CSR). Certificates can also be distributed to network devices that are not part of the AD (such as routers and switches) through Simple Certificate Enrollment Protocol (SCEP).

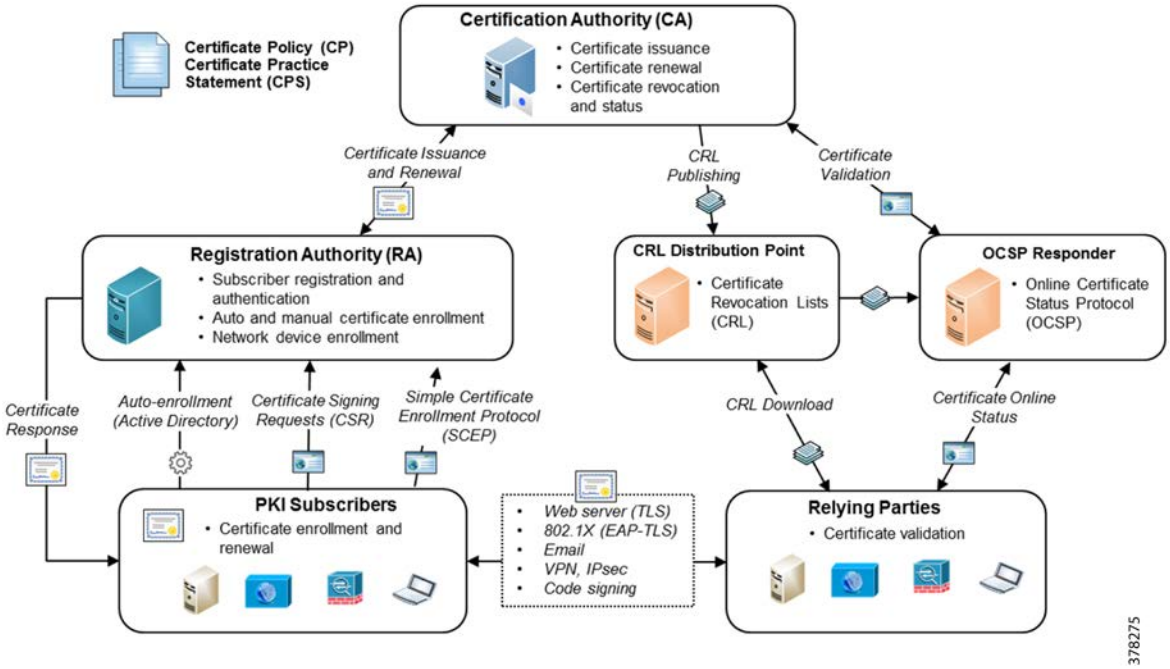
- **Relying Parties** are users or devices that rely on certificates and the PKI to authenticate subscribers. Relying parties should be able to verify that the certificate has not been revoked, has not expired, and has been issued by the trusted CA.

- **CRL Distribution Point** is a place in the network (typically a web server) where CAs publish Certificate Revocation Lists (CRL), which are CA-signed lists of all revoked certificates up to date. Relying parties should download the most recent CRL on a regular basis to check certificate status.

- **OCSP Responder** is a server that provides a real-time validation of a certificate via an Online Certificate Status Protocol (OCSP). Using OCSP responders in the network can reduce network load and improve response time for relying parties.

Note Depending on the system size, administrative boundaries, and security policies, various PKI functions can be combined on the same server or distributed among many servers in the network.

Figure 2-3 PKI Components and Functions



Certification Authority Hierarchy

PKI supports a hierarchical structure with various CA roles in the network, depending on the scale of the system and security policies.

- **Root CA** is the most trusted CA in a CA hierarchy and is the first CA installed in the network. When a root CA remains online, it is used to issue certificates to the intermediate and subordinate CAs. The root CA typically remains offline to protect the private keys. The root CA rarely issues certificates directly to users, computers. or services.
- **Intermediate CAs** are the next in hierarchy after the root CA. The intermediate CA issues certificates only to subordinate CAs. In small scale deployments, an intermediate CA may not be present.
- **Subordinate CAs** are CAs that are not root CAs. Subordinate CAs can be used to issue certificates to users and computers or to issuing CAs.
- **Issuing CA** is used to issue certificates directly to users and computers. In small scale deployments, this role may be assigned to subordinate CAs.

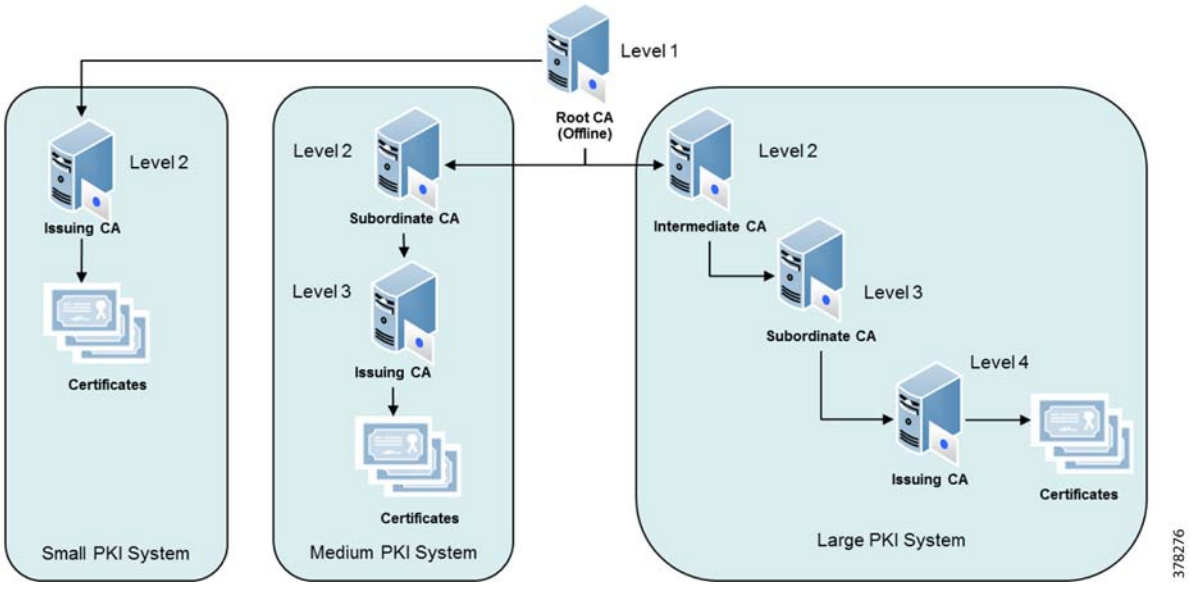
AD Certificate Services can be deployed with CAs in Enterprise CA and stand-alone CA modes depending on the specific requirements:

- **Enterprise CA** is integrated with AD and use domain services for certificate management. Enterprise CAs are typically used for issuing user and computer certificates.
- **Stand-alone CA** is not dependent on AD and not part of a domain. A stand-alone mode is often used to implement a secure offline root CA and is used for issuing certificates to intermediate and subordinate CAs.

Note For more information about planning a CA hierarchy in the AD CS, please refer to the following URL: https://technet.microsoft.com/en-us/library/dn786436(v=ws.11).aspx

Figure 2-4 shows the CA hierarchy and various deployment models depending on the system scale.

Figure 2-4 CA Hierarchy and Deployment Models



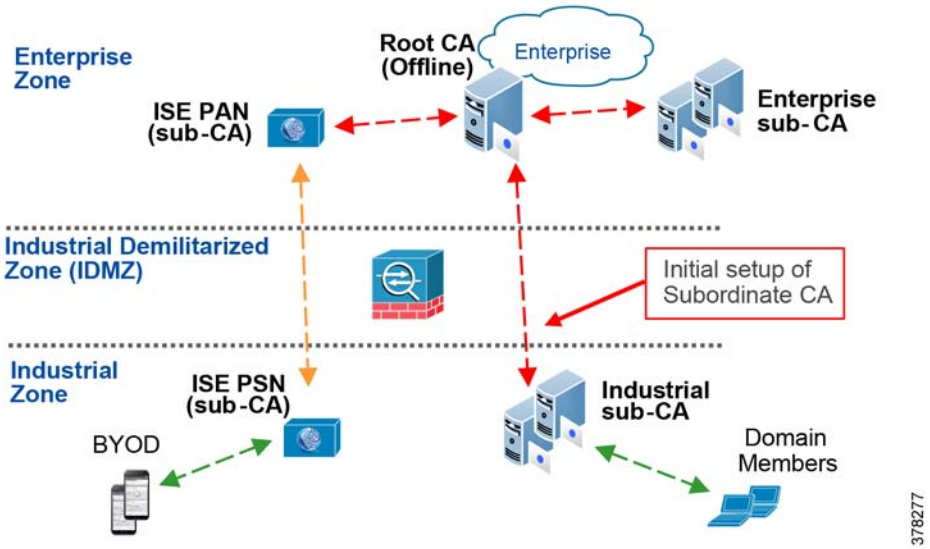
Certificate Services Deployment in the CPwE Architecture

Within a CPwE Identity and Mobility Services architecture, Cisco and Rockwell Automation recommend the implementation of a distributed PKI model with the root CA in the Enterprise Zone and subordinate CAs in the Enterprise and Industrial Zones.

- The root CA in the Enterprise Zone should be configured as a stand-alone server (not part of the domain) and should be used only to issue certificates to intermediate and subordinate CAs. As a best security practice, the root CA should remain offline while not in use.
- The minimum recommended deployment is a two-tier CA hierarchy with multiple subordinate CAs in the Enterprise and Industrial Zones to support different business applications such as web servers, VPN, email, and 802.1X authentication, as well as different geographical and administrative units. This provides for better manageability and flexibility, especially when it is necessary to revoke CA certificates due to a key compromise.
- Large organizations may choose to implement a three-tier CA hierarchy where an intermediate CA in the Enterprise Zone issues certificates to subordinate CAs in the Industrial Zone. This approach adds to the management cost but allows for more flexibility in applying different issuing policies and revoking certificates. This intermediate CA should remain offline as the best practice.
- Subordinate CA in the Industrial Zone is responsible for validating industrial users and devices and issuing certificates automatically through the AD CS and manually with the client's Certificate Signing Request (CSR). This prevents users from sending requests to the issuing CAs in the Enterprise Zone. Multiple subordinate CA may be deployed inside the Industrial Zone for redundancy.
- Cisco ISE can serve as a subordinate CA for issuing certificates to mobile devices that are not part of the domain, either corporate-issued or personal to support a Bring Your Own Device (BYOD) scenario. The Enterprise and Industrial PSNs are subordinate CAs to the PAN. Mobile devices can use SCEP portal on the PSN for certificate provisioning.

The PKI infrastructure in the CPwE architecture is shown in Figure 2-5.

Figure 2-5 CPwE PKI Infrastructure



Note During the initial setup of the subordinate CA in the Industrial Zone, IT administrators have to issue a CSR and copy the issued certificate from the root CA to the sub-CA through the IDMZ. Once this process is completed, there should be no permanent communication between the root and sub-CA.

The subordinate CA in the Industrial Zone should provide the following services to industrial clients:

- **Certification Authority (CA)** to issue and manage certificates via the Active Directory using Group Policy and to publish CRLs that are accessible from the Industrial Zone.
- **Certificate Authority Web Enrollment** to allow users to connect to a CA via HTTPS in order to manually request certificates and retrieve CRLs.

Additional AD CS features may also be deployed on the sub-CA or separate servers depending on the organization's scale and needs:

- **Certificate Enrollment Web Service** to enable users and computers to enroll for and renew certificates using HTTPS when the client computer is not a member of a domain or when a domain member is not connected to the domain.
- **Certificate Enrollment Policy Web Service** to enable non-domain users and computers to obtain certificate enrollment policy information.
- **Online Responder** to accept revocation status requests for specific certificates via OCSP, evaluate the status of these certificates, and send back a signed response containing the requested certificate status information.
- **Network Device Enrollment Service (NDES)** to allow routers and other network devices that do not have domain accounts to obtain certificates via SCEP.

Note For information about AD Certificate Services, please refer to the following URLs:

- https://technet.microsoft.com/library/hh831740.aspx
- https://technet.microsoft.com/en-us/library/cc772192.aspx

Cisco ISE Certificates

Cisco ISE relies on PKI to provide secure communication with mobile devices, with network administrators for Cisco ISE management, as well as between Cisco ISE nodes in a multi-node deployment.

Cisco ISE provides the Admin Portal to manage the following two categories of X.509 certificates:

- System certificates—These are server certificates that identify a Cisco ISE node to client applications. Every Cisco ISE node has its own system certificates, each of which are stored on the node along with the corresponding private key.
- Trusted certificates—These are CA certificates used to establish trust for the public keys received from users and devices. The Trusted Certificates Store also contains certificates that are distributed by the SCEP which enables registration of mobile BYOD into the network. Certificates in the Trusted Certificates Store are managed on the Primary Administration Node (PAN).

Note In a distributed Cisco ISE deployment, you must import the trusted certificate only into the certificate trust list (CTL) of the PAN. The certificate gets replicated to the secondary PAN and to the PSNs.

Certificate Types in Cisco ISE

When you add or import a certificate in to Cisco ISE, you should specify the purpose for which the certificate is to be used:

- Admin—For internode communication and authenticating the Admin portal.
- EAP—For EAP-TLS authentication (802.1X).
- RADIUS DTLS—For RADIUS DTLS server authentication.
- Portal—For communicating with all Cisco ISE end-user portals via HTTPS.
- xGrid—For communicating with the pxGrid controllers (third-party and other Cisco security platforms).

You can associate different certificates from each node for communicating with the Admin portal (Admin), the pxGrid controller (xGrid), and for TLS-based EAP authentication (EAP). However, you can associate only one certificate from each node for each of these purposes.

X.509 certificates are only valid until a specific date. When a system certificate expires, Cisco ISE functionality that depends on the certificate is impacted. Cisco ISE notifies you about the pending expiration of a system certificate when the expiration date is within 90 days.

Enabling PKI in Cisco ISE

By default, a Cisco ISE node is preinstalled with a self-signed certificate that is used for EAP authentication, Admin portal, portals, and pxGrid controller. This certificate must be replaced with server certificates that are signed by a trusted CA.

During the initial Cisco ISE deployment, administrators must populate the Trusted Certificates Store with the trusted corporate CA certificates. If a certificate chain consists of a root CA certificate plus one or more intermediate CA certificates, to validate the authenticity of a user or device certificate you must import the entire chain into the Trusted Certificates Store.

Wireless Access Design

To take advantage of the business benefits of Industrial IoT (IIoT), manufacturers should consider providing onsite wireless access for trusted partners and employees. Wireless Employee/Trusted Partner Access is accomplished for the Industrial Zone using the following methods:

- Plant Personnel access with direct access to Industrial Zone IACS equipment or Level 3 Site Operations (Figure 2-10)
- Plant Personnel or Trusted Partner partial access to the IACS equipment or Level 3 Site Operations limited to specific machines, production areas or servers (Figure 2-10)
- Plant Personnel or Trusted Partner access via the Remote Access Server (RAS) using Remote Desktop Services (RDS) for all IACS applications such as Studio 5000 Logix Designer® software (Figure 2-10)
- Employee (non-Plant Personnel) access to Enterprise Zone resources (Figure 2-11)
- Trusted Partner access to Guest DMZ for limited Internet access or VPN back to the RAS (Figure 2-12)

The access methods mentioned above use IEEE 802.1X authentication for permitting access to the network. Within the CPwE architecture, EAP-TLS is used as the secure authentication method supported with the Active Directory Certificate Services.

Corporate-issued mobile device access (computer, tablet, smartphone) is based on the user group membership and user certificate profiles. These devices are provisioned by the IT department and have correct certificates installed via the AD group policy or secure provisioning network. A mobile device whitelist on the Cisco ISE can also be used to limit access to corporate-issued mobile devices only based on the MAC address.

Personal device (BYOD) access, if permitted by the manufacturer's corporate mobility and security policies, is based first on the user login credentials and group membership and later on the certificate profiles when the device is provisioned using the self-serve portal.

Profiling and posturing using Cisco ISE and third-party MDM solutions confirm that BYOD as well as corporate-issued mobile devices are compliant with the manufacturer's mobility and security policies.

Mobile Device Considerations

Mobile devices within the Industrial Zone give workers access to real-time production information such as Overall Equipment Effectiveness (OEE). Mobile devices can also provide valuable diagnostics data to maintenance personnel when a downtime event occurs so they immediately know where a problem is occurring, what the issue is, and where they can get the tools they need to fix it. Mobile devices also offer a breadth of functionality that simplify tasks and help fewer staff do more in less time.

The CPwE Identity and Mobility Services architecture provides the necessary technology and infrastructure components to securely incorporate mobile devices into a plant-wide network. Key advantages of the CPwE Identity and Mobility Services architecture include:

- Cisco ISE as the centralized policy server that integrates tightly with an organization's Active Directory and PKI infrastructure, as well as third-party MDM solutions.
- Single point of visibility and control of users, devices, location, network, and applications resulting in greater security and ease of management.
- Single wireless infrastructure to support various user roles and access levels.

Table 2-1 provide an overview of security requirements for the mobile workforce and corresponding components of CPwE Identity and Mobility Services.

Table 2-1 Security Requirements of Mobile Workforce

Security Requirements	CPwE Identity and Mobility Services
• Identify users and mobile devices that are accessing the network and allow connectivity only if they are authorized and meet manufacturer's policy. • Provide secure encrypted access optimized for efficient application delivery and capabilities. • Provide granular application access to mobile users based on user's role and other criteria.	Cisco ISE and policy enforcement through wireless and wired infrastructure components that participate with ISE.
• Allow visibility into users, mobile devices, and the mobile applications on the network.	Cisco ISE with comprehensive monitoring, logging, and application visibility capabilities for network administrators and security monitoring platforms.

Table 2-1 Security Requirements of Mobile Workforce

• Confirm that mobile devices are safe and compliant with the company policy, not jail-broken or rooted, and do not have malware or applications that can compromise the network availability, data integrity, or confidentiality. • Enforce device-level security functionality such as remote wipe/lock with integrated Network Access Control (NAC), thus ensuring that an action can be taken on non-compliant devices at any time (not just during access).	MDM solutions that are integrated with Cisco ISE to provide profiling, posturing, and remediating of the mobile devices.
• Provide granular network access based on a mobile user's physical location in the network.	Cisco ISE and integration with Cisco MSE for WLAN Location Based Services.

As part of a defense-in-depth security strategy, authentication and authorization policies on the network level should be complemented with application-level security solutions, for example FactoryTalk Security, ThinManager Relevance, and OS protection software.

Corporate Mobile Devices

The corporate-issued mobile devices for the Industrial Zone must have their MAC addresses already present in the Whitelist of Cisco ISE user groups and also must come with pre-installed user certificates for SSIDs that can be accessed by the devices. The appropriate MDM applications should also be preinstalled if an MDM solution is in place.

In case of Windows-based mobile devices, host protection solutions such as antivirus and malware prevention software should be in place, as well as corporate solutions to monitor and control software installation. In many aspects, this is similar to MDM for iOS and Android devices.

Users must adhere to the corporate mobility and security policies for the Industrial Zone regarding approved applications, mobile device types, Internet access, and types of data that can be stored on the mobile device.

BYOD Mobile Devices

Many companies are starting to allow personal mobile devices (BYOD) in their networks. The goal is to improve users' experience and productivity as well as to help simplify operations and reduce costs. This trend will continue to grow and will be more prevalent in manufacturing and process industries as well.

It is critical to understand the company's tolerance for risk and evaluate the potential dangers of allowing BYOD in the Industrial Zone (malware, unauthorized applications, loss of confidential data) versus the benefits (mobile workforce flexibility and increased productivity). Another consideration is whether the infrastructure, IT resources, and expertise are in place to support, secure, and monitor the BYOD deployment.

BYOD means that devices previously unmanaged by IT enter the network. In order to protect the network, organizations must create different policy levels and authorization rules for BYOD as opposed to corporate-issued mobile devices. In addition, different permissions must be assigned based on who uses the devices.

In the Industrial Zone, as a best practice, BYOD access should be limited to read-only or restricted to certain resources by using authorization rules on Cisco ISE, network security policies, such as firewall rules and ACLs, as well as application-level restrictions.

Cisco ISE provides a BYOD self-service portal so users can register and seamlessly get their new devices onto the network securely. IT staff can benefit from automated device provisioning, profiling, and posturing services available for any level of security compliance requirements.

As for corporate-issued devices, BYOD users must agree and strictly follow the corporate security policy for the Industrial Zone regarding approved applications and data security.

Internet Access Requirements

To align with industrial security standards such as IEC-62443 and NIST 800-82, a traditional security policy for IACS devices within the Industrial Zone is to not allow direct access to the Internet for obvious security reasons. While this will remain true for many secure environments, manufacturers may want to realize the IIoT business benefits by providing limited Internet access to selected users and IACS applications to be able to perform their tasks without impeding productivity.

Mobile devices in the Industrial Zone may need access to the Internet resources for the following reasons:

- IACS application access to cloud services, for example FactoryTalk Cloud services necessary for FactoryTalk TeamONE™ operation.
- Connectivity to the private cloud resources managed by the manufacturer to view production data and analytics.
- VPN access to the trusted vendor’s corporate network as part of the normal workflow during commissioning and maintenance of the vendor's equipment.
- Access to IACS manufacturer’s websites for firmware downloads, documentation, and technical support.
- Access to mobile device OS vendors’ (e.g., Apple, Google) cloud infrastructure servers to enable push notifications, mobile OS updates, as well as part of BYOD and MDM provisioning.

The challenge for manufacturers is to develop a balanced security stance to take advantage of IIoT innovation while maintaining the integrity of industrial security best practices. Business practices, corporate standards, security policies, application requirements, industry security standards, regulatory compliance, risk management policies, and overall tolerance to risk are key factors in determining the appropriate manufacturer’s security stance as to whether limited secure connectivity from an IACS application within the Industrial Zone to a trusted cloud is permitted.

A holistic defense-in-depth industrial security stance is necessary in order to help protect the integrity of safety and security best practices while also helping to enable identity and mobility services. No single vulnerability should be permitted to disrupt operations. Communication to the Internet through the IDMZ, if allowed by manufacturer’s security stance, must be strictly controlled and data must be inspected for malicious content. Multiple layers of defense (administrative, technical, and physical) using diverse technologies for detection and prevention should be used to address different types of threats. The manufacturer should also confirm that the Internet Service Provider (ISP) is trusted and provides network and security services to help protect connectivity and data.

Several Cisco technologies and security platforms exist to achieve these goals—with various levels of complexity and granularity—which can be integrated with Cisco ISE for comprehensive security:

- Access Control Lists (ACL) on the WLC and IDMZ firewalls can be used for basic whitelisting of URL and IP addresses.
- Cisco ASA firewalls with FirePOWER services and next-generation Firepower appliances in the IDMZ provide deep packet inspection (DPI) of web traffic to achieve application control, threat prevention, and advanced malware protection.

  Refer to the Cisco Next-Generation Firewalls page at:
  https://www.cisco.com/c/en/us/products/security/firewalls/index.html

- Cisco Web Security appliance (WSA) provides web proxy services, automated traffic analysis and application visibility, website reputation analysis and blacklisting, TLS proxy to inspect encrypted traffic, Advanced Malware Protection (AMP), and many other features.

  Refer to the Cisco Web Security Appliance page at:
  https://www.cisco.com/c/en/us/products/security/web-security-appliance/index.html

- Cisco Umbrella solution as Secure Internet Gateway (SIG) is a cloud-delivered security platform that can protect managed mobile devices in the network by filtering Domain Name System (DNS) requests and inspecting content from risky domains.

  Refer to the Cisco Umbrella page at:
  https://umbrella.cisco.com/

RF Spectrum Considerations

The proliferation of mobile devices within the Industrial Zone brings new challenges to the task of managing wireless spectrum, especially in places where wireless media is used with critical IACS applications. Even if mobile devices are logically separated from IACS wireless devices by using separate SSIDs and authentication methods, they still may use the same wireless channel and consume the bandwidth. Even simply probing channels for known SSIDs can create issues with latency-sensitive IACS applications when the number of mobile clients starts to grow.

Cisco and Rockwell Automation recommend these steps made for managing RF spectrum:

- Develop a comprehensive RF spectrum policy in collaboration with IT.
- Always perform a detailed site survey to help achieve best performance for all mobile devices. If RF coverage is poor and data rates are low for certain devices, this can create bandwidth utilization issues in the channel that affect every device in it.
- Use 2.4 GHz band or selected 5 GHz channels for non-critical mobile personnel access. Reserve specific channels in the 5 GHz frequency band exclusively for critical IACS applications such as I/O, peer-to-peer, and safety control.
- Do not allow mobile devices to connect to the same SSID as your critical IACS applications for maintenance purposes. Use different wireless SSID in a different channel and VLAN even when communicating with IACS devices mounted on mobile equipment. The main reasons are difficulty to control traffic levels from users' mobile devices and varying QoS schemes that may affect latency sensitive applications.
- To help prevent users' devices from probing the wireless network, it is better to provide the appropriate level of access to all users, including guests and trusted partners, or explicitly prohibit unauthorized Wi-Fi devices within the Industrial Zone.

Note For more information, please refer to the *Deploying 802.11 Wireless LAN Technology within a Converged Plantwide Ethernet Architecture Design and Implementation Guide* at the following URLs:

- Cisco site:
  https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/NovCVD/CPwE_WLAN_CVD.html
- Rockwell Automation site:
  http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td006_-en-p.pdf

WLAN Architecture Considerations

There are two main types of WLAN architectures in the CPwE Identity and Mobility Services that are discussed below, Unified WLAN Architecture and Autonomous WLAN Architecture.

Unified WLAN Architecture

The Unified WLAN architecture is a Cisco solution for large scale plant-wide deployments of wireless infrastructure. In the Unified architecture, the WLAN functionality is split between lightweight access points (LWAP) and wireless LAN controllers (WLC). Most WLAN control and management functions are centralized in the WLC and timing-critical functions of the 802.11 protocol are distributed to lightweight or "thin" APs.

In addition to base functionality provided by LWAP and WLC, the Unified architecture includes comprehensive solutions for:

- WLAN management, end-user connectivity, and application performance visibility
- Advanced spectrum analysis, Location Based Services (LBS), and wireless Intrusion Prevention Services (wIPS)
- Design and implementation of security policy across the entire network
- Advanced integration with Cisco ISE

The Unified WLAN is considered the primary wireless architecture for CPwE Identity and Mobility Services that covers the majority of use cases and applications.

Autonomous WLAN Architecture

The Autonomous WLAN architecture consists of stand-alone access points that implement all of the WLAN functions: management, control, and data transport and client access. An example of an autonomous access point is the Stratix 5100 AP or any Cisco AP running the autonomous Cisco IOS software.

Each autonomous AP is configured and managed individually. Limited coordination of operation exists between autonomous APs, as well as limited capability to implement scalable solutions for configuration and firmware management, client mobility, WLAN security, and resilience.

The following use cases can be considered for mobile devices in the autonomous WLAN:

- Low level of expertise that makes it hard to support more comprehensive solutions such as Cisco Unified WLAN
- Instant connectivity to remote locations, small scale operations, stand-alone/isolated IACS applications for monitoring and preventive diagnostics where necessary infrastructure is not yet available or cost prohibitive
- Temporary WLAN installations for commissioning of vendor equipment

Unified Wireless Access Overview

For a mobile device (corporate-issued or BYOD) to obtain access, the user must be authenticated by Cisco ISE; the result is an authorization profile that is applied to the WLC. The mobile device would pass through the following steps before being allowed to access the network:

1. Authentication
2. Profiling and Posturing

3. Provisioning (BYOD only)
4. Authorization

Authentication

802.1X authentication in the Unified WLAN involves three parties:

- The supplicant—A client device that wishes to attach to the wireless network.
- The authenticator—The WLC that accepts authentication requests from the client and sends it to the RADIUS authentication server.
- The authentication server—Cisco ISE that validates client's identity and sends back the success or failure RADIUS message.

Authentication policies are used to define the protocols used by Cisco ISE to communicate with the mobile devices and the identity sources to be used for authentication. Cisco ISE evaluates the conditions and, based on whether the result is true or false, applies the configured result.

The authentication protocols used in CPwE Identity and Mobility Services are:

- Protected Extensible Authentication Protocol (PEAP)
- Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)

Authorization Policies

Authorization policies are critical to determine what the user is allowed to 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 mobile device and can include attributes such as an associated VLAN and ACL. Cisco Wireless LAN Controllers support named ACLs (known as Airespace ACLs). These ACLs must be preconfigured on the WLC. Using the RADIUS Airespace-ACL Name attribute-value pair, Cisco ISE instructs the WLC to apply the ACL.

An additional identity group may be defined on Cisco ISE for the purpose of uniquely identifying corporate-issued devices. This identity group, named Whitelist, maintains a list of devices owned by the corporation. The Whitelist is manually updated by the IT administrator and contains the MAC addresses that could be granted full access or more permissive access than the personal (guest) devices.

Authorization rules in Cisco ISE can use wide variety of conditions including:

- User group membership
- Authentication method
- Mobile device type and OS
- Posturing and profiling results
- User location and time of access

Note In addition to the local authorization policies within the Industrial Zone, specific access rules may be applied in the IDMZ firewalls for mobile devices in a particular IP subnet or device group. These firewall rules could be used, for example, to grant limited Internet access for certain applications that require cloud connectivity.

The following is CPwE Identity and Mobility Services wireless access example (as displayed in Figure 2-10, Figure 2-11, and Figure 2-12).

1. A corporate-owned or BYOD mobile device connects to the designated Employee or Trusted Partner SSID.
2. Mobile devices authenticate using 802.1X / RADIUS against the Industrial WLC (the authenticator) and either the Industrial PSN or the Enterprise PSN (the authentication server) depending on the SSID.
   a. The RADIUS request flows from the Industrial WLC to the Industrial PSN for the Industrial Employee SSID.
   b. The RADIUS request flows from the Industrial WLC to the Enterprise PSN over an IPsec tunnel for the Corporate Employee or Trusted Partner SSID.
3. The user data flows either through the local WLC (the Industrial Zone) or is tunneled to the anchor WLC (the Enterprise Zone or Guest DMZ) depending on the SSID to which the user is connected.

Differentiated access control for wireless clients is provided by Airespace ACLs applied to the WLC as well as ACLs in the IDMZ firewalls. The different access scenarios for a mobile user are:

- Full access to the entire Industrial Zone
- Limited access to the specific Cell/Area Zone or to specific devices within the Cell/Area Zone
- Limited access to the specific Level 3 Site Operation assets or to the RAS only
- Full or partial access to the Enterprise Zone via the tunnel (corporate users)
- Internet access provided via the tunnel to the Guest DMZ (partners and guests)
- Limited Internet/cloud access for mobile devices in the Industrial Zone

Manufacturers' security policies, risk assessment results, and application requirements determine the appropriate level of access for mobile users in general and to a particular device type or user group.

Mobile Device Use Cases

The following use cases are examples of access requirements for the CPwE Identity and Mobility Services architecture:

- **Limited Access**—This use case enables access exclusively to corporate-issued mobile devices.
- **Enhanced Access**—This use case provides network access for BYOD, as well as corporate-issued mobile devices. It allows policies that enable granular role-based application access and extends the security framework within the Industrial Zone.
- **Advanced Access**—This comprehensive use case also provides network access for BYOD and corporate-issued mobile devices. However, it includes the posture of the mobile device into the network access control decision through integration with third-party MDMs.

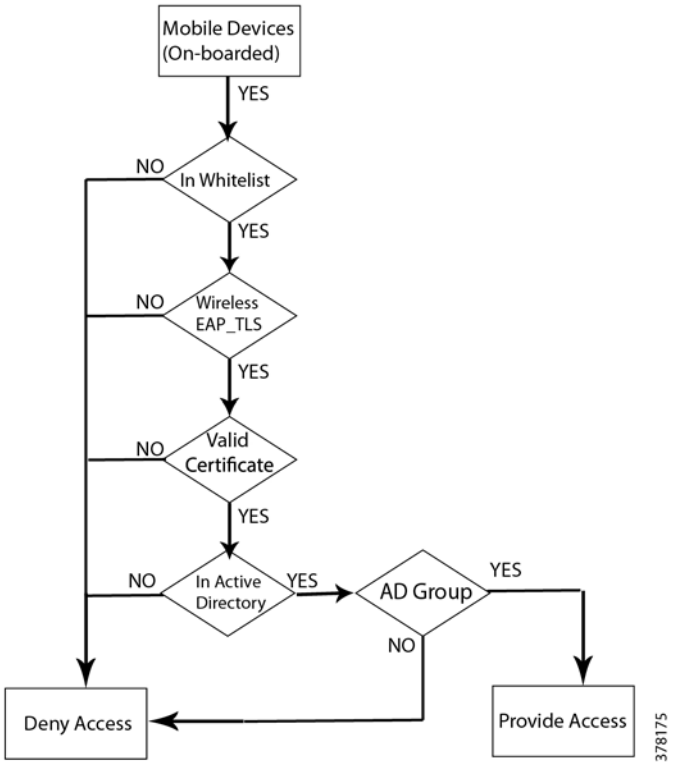
Limited Access—Corporate Mobile Devices

This use case (Figure 2-6) enforces a more restrictive policy that allows only mobile devices owned or managed by the manufacturer to access the network and deny access to employees' BYOD devices.

Cisco ISE grants mobile devices full access to the network based on the mobile device's certificate and inclusion in the Whitelist identity group. This use case introduces the use of a Whitelist, a list of corporate mobile devices maintained by Cisco ISE that is evaluated during the authorization phase.

As an additional security measure, mobile devices can be "on premise" only, with disabled cellular access for data and never leave the Industrial Zone perimeter. This decision depends on the manufacturer's security policy, workflow, and application requirements.

Figure 2-6 Limited Access for Corporate-owned Devices



Note It is important to understand that corporate-issued mobile devices in the whitelist can still be compromised with malware or inappropriate applications if allowed to connect to the Internet (from the manufacturer's network or using a cellular/home connection). Additional security measures such as MDM solutions and web security solutions are recommended to help prevent such risk.

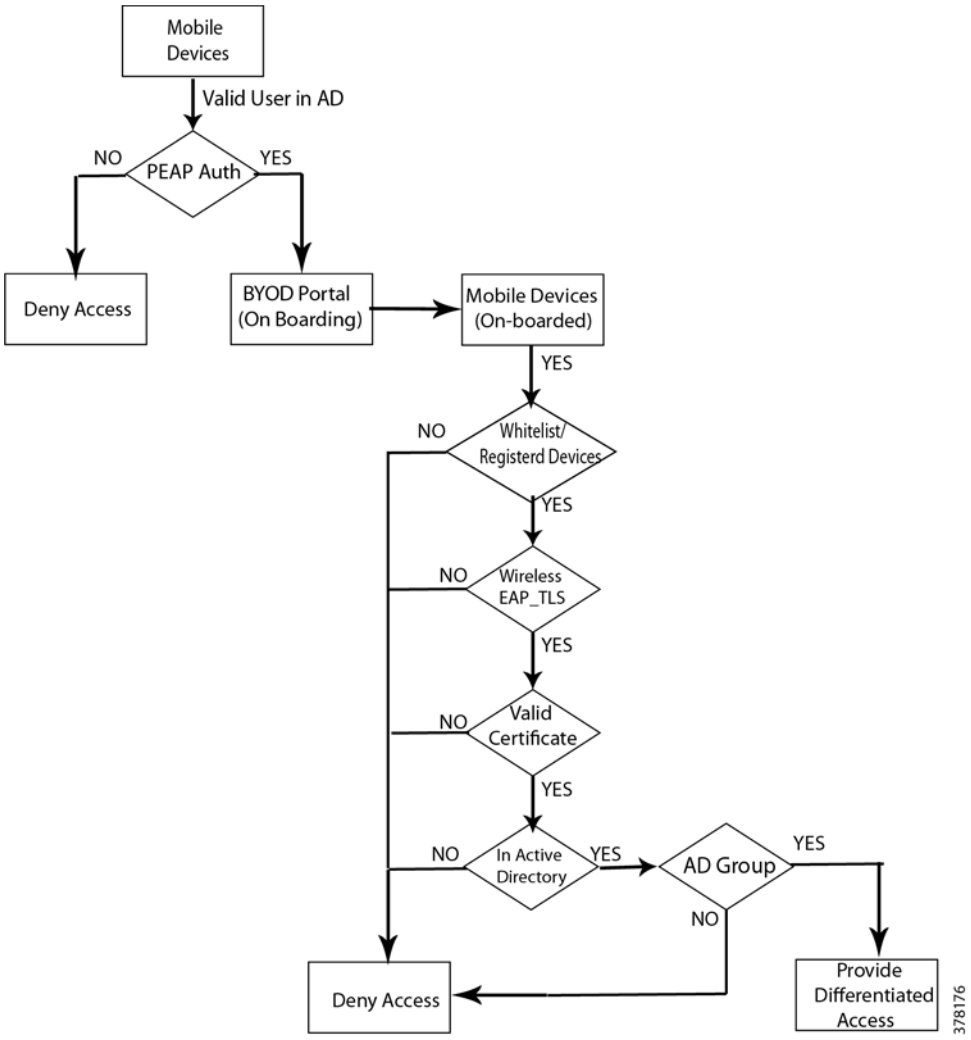
Enhanced Access—BYOD and Corporate Mobile Devices

This use case (Figure 2-7) builds on the Limited Access use case and provides the infrastructure to on-board BYOD onto the network by enrolling digital certificates and provisioning configuration files. The use case focuses on how to provide different access levels to BYOD based on authentication and authorization rules.

Employees that have registered their mobile devices using the Cisco ISE BYOD portal and have received a digital certificate are granted unique access based on their Active Directory group membership.

Cisco ISE also provides the capability of identifying (profiling) the mobile device OS and type and helping prevent certain types of devices from connecting to the network.

Figure 2-7 Enhanced Access for BYOD and Corporate-owned Devices

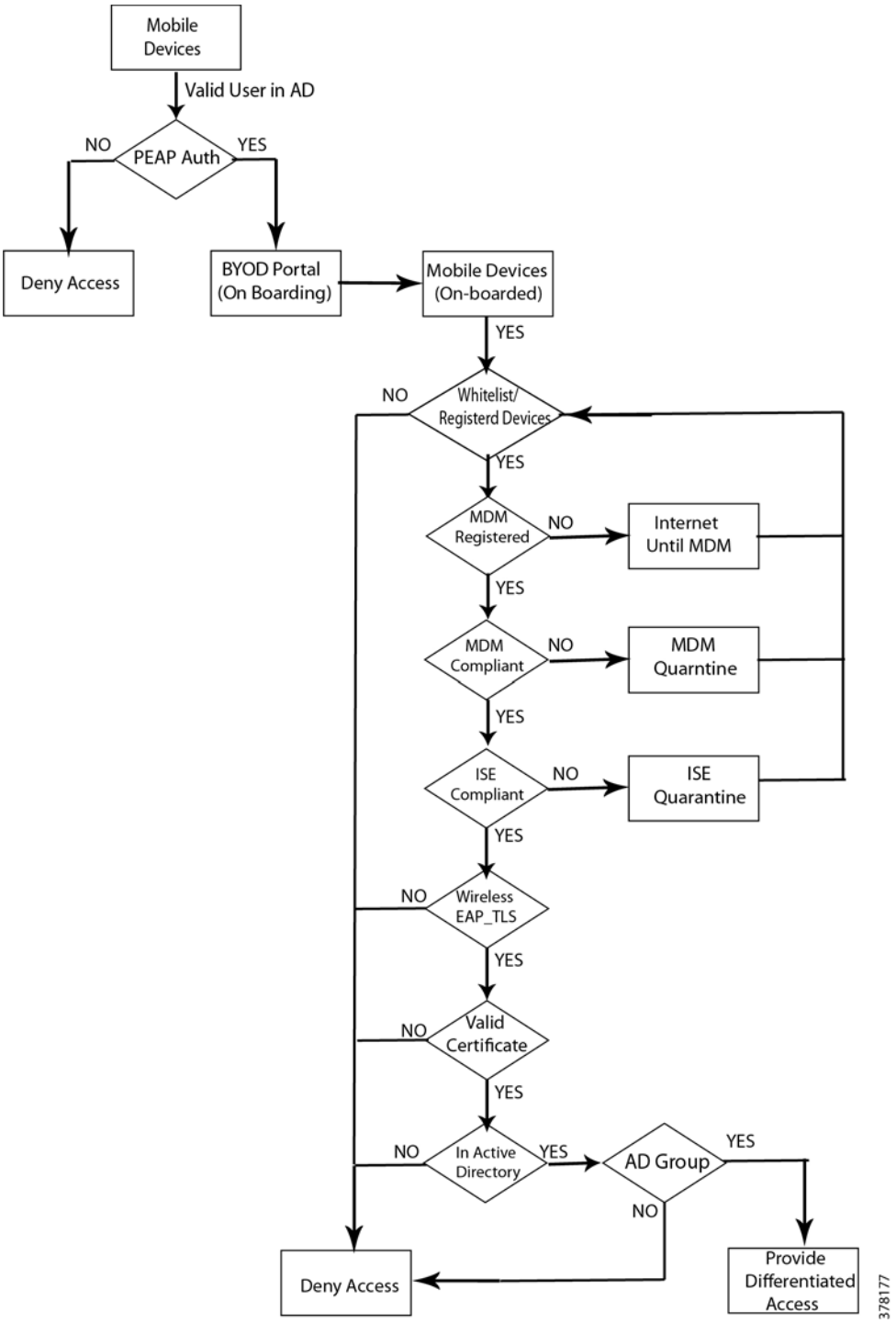


Advanced Access—MDM Posture

This use case (Figure 2-8) uses a MDM to manage and secure mobile devices. While MDM servers are not able to enforce Network Access Control policies, they provide unique mobile device posture information not available on the Cisco ISE. By combining Cisco ISE policies with additional MDM information a robust security policy can be enforced on mobile devices.

The integration between Cisco ISE and MDM is through a REST API, allowing Cisco ISE to query the MDM server for additional compliance and posture attributes.

Figure 2-8 Advanced Access with MDM Posture



BYOD Provisioning

Deploying digital certificates to mobile devices requires a network infrastructure that provides the security and flexibility to enforce different security policies, regardless of where the connection originates. CPwE Identity and Mobility Services focuses on providing digital certificate enrollment and provisioning while enforcing different permission levels. It covers Android™ and Apple® iOS™ mobile devices, in addition to Windows OS devices.

The general steps when a new mobile device connects to the network are:

1. A new device connects to a SSID using the user credentials. This SSID is secured with PEAP. Once the device is authenticated, it redirects the user to a BYOD portal where the certificate enrollment and profile provisioning begins.
2. The provisioning service requests information from the mobile device and provisions the configuration profile, which includes a Wi-Fi profile with the parameters to connect to the same SSID now secured through EAP-TLS and is granted access to network resources based on different Cisco ISE authorization rules.

Note The following sections describe CPwE architecture and steps for BYOD provisioning when a new mobile device connects to the Industrial Zone network. Another scenario may also be considered when a new mobile device is provisioned in the corporate network first, then moved to the Industrial Zone with appropriate certificates and profiles already in place.

Client Provisioning Policy

Cisco ISE looks at various elements when classifying the type of login session through which users access the network, including client's mobile device OS and version, browser type and version, and others. Once Cisco ISE classifies the client mobile device, it uses client provisioning policies to confirm that the client is set up with an appropriate software agent version, up-to-date compliance modules, and correct agent customization packages and profiles, if necessary.

The following are considerations for client provisioning on the mobile devices:

- Based on the mobile device type, push an appropriate Software Provisioning Wizard (SPW) to the mobile device. This Wizard configures the 802.1X settings on the mobile device and configures the endpoint to obtain a digital certificate.
- In certain mobile devices such as iOS devices, there is no need for SPW package because the native operating system on the iOS devices is used to configure the 802.1X settings.
- For Android devices, the SPW package needs to be downloaded from Google Play Store which requires Internet access.
- The SPW packages for other mobile devices such as Windows and MacOS laptops are developed by Cisco and they can be downloaded using the Cisco ISE administration web page

MDM Deployment Options and Considerations

With MDM solutions, there are two main deployment models:

- **On-Premise**—In this model, the MDM software is installed on servers in the Enterprise zone, which is supported and maintained by the enterprise IT staff.

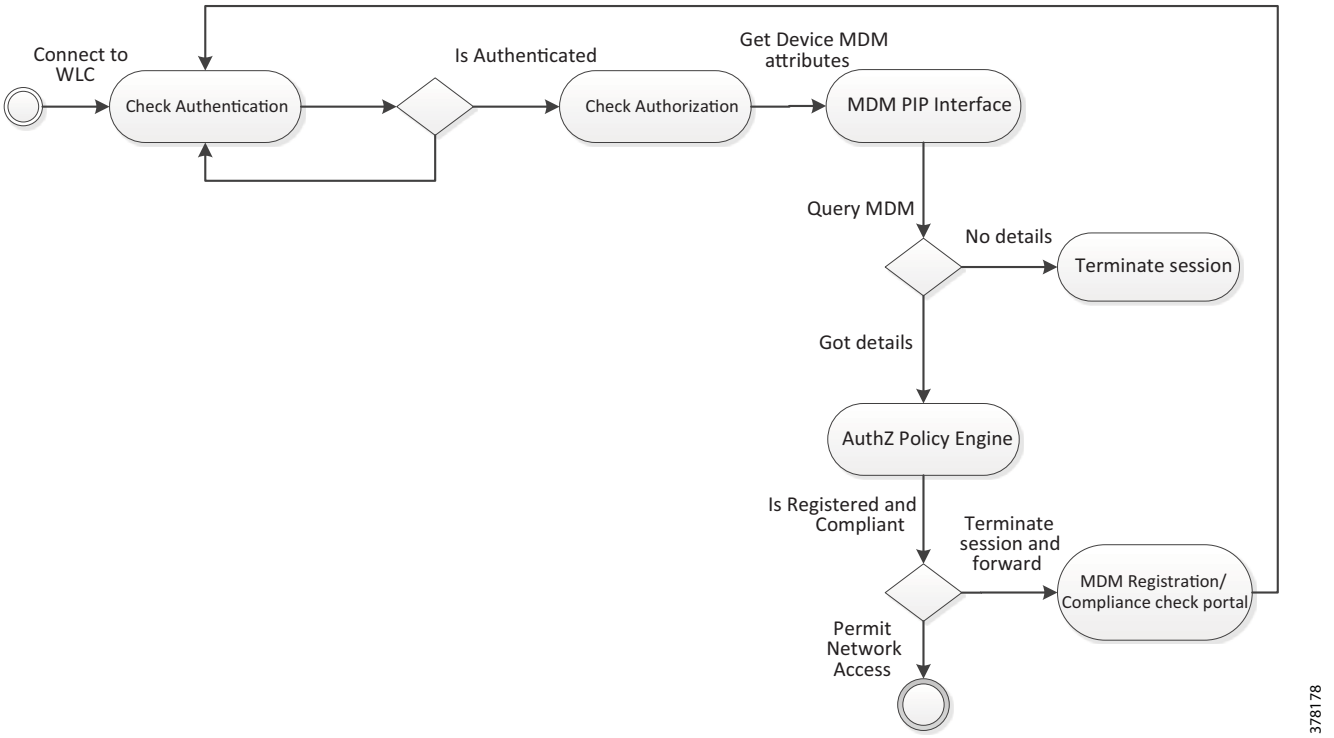
- **Cloud-based**—In this model, also known as an MDM Software-as-a-Service (SaaS) model, the MDM software is hosted, supported, and maintained by a provider at a remote Network Operation Center (NOC). Customers subscribe on a monthly or yearly basis and are granted access to all MDM hardware/software through the Internet.

In the CPwE Identity and Mobility Services architecture, the On-Premise Solution is deployed where the MDM server is installed as a VM in the Enterprise Zone.

The following steps take place when checking for device compliance (Figure 2-9):

1. The user connects to an on-boarding SSID and is guided through the registration and on-boarding process with Cisco ISE.
2. Once the user has been on-boarded with the proper certificate/profiles, the user connects to a secure SSID.
3. Cisco ISE makes an API call to the MDM server. If the mobile device is not registered with the MDM, the user is presented with the appropriate page to proceed to their MDM enrollment page.
4. Once the user completes the enrollment with the MDM server, they return to an enrollment redirect page that includes a continue button. When the user selects the continue option from the page, Cisco ISE will issue a Change of Authorization (CoA), forcing the user to reauthenticate. The API should now indicate the user has enrolled with the MDM. API results are cached by Cisco ISE for the duration of the authorization flow.
5. Cisco ISE uses the cached MDM information for the specific MAC address to verify the device's posture including its MDM compliance status. If the device is not in compliance with the MDM policies, the user is once again informed and is asked to become compliant.
6. Once the mobile device becomes compliant, the user is authorized to access the network based on the assigned permissions (Full, Partial Access, or Internet Access).
7. Cisco ISE can poll the MDM server periodically to get compliance information.

Figure 2-9 MDM Compliance Flow



Unified Wireless Access Use Cases

The following sections describe wireless access implementations for roles such as Industrial Employee, Corporate Employee, and Trusted Partner within CPwE Identity and Mobility Services. This implementation is based on the Cisco Unified WLAN Architecture and design principles described earlier.

Wireless Access to Industrial Zone

This use case (Figure 2-10) describes user access to the Industrial Zone resources from a mobile device. Plant personnel and trusted partners may require this type of access to be able to:

- Commission new equipment faster.
- Monitor parameters of IACS devices for proactive maintenance.
- Collect information, troubleshoot problems, and apply configuration changes to help minimize downtime.
- Access Level 3 Site Operation servers from mobile human-machine interface (HMI) and thin client devices.

Depending on the manufacturer’s security policy and configured authorization rules, different user groups, as well as trusted partners, may get access to different sets of Industrial Zone resources. The access may be further restricted by filtering network protocols that are allowed for the mobile device. The following access policies have been considered:

- Plant Personnel with full access to the Industrial Zone IACS equipment or Level 3 Site Operations

- Plant Personnel or Trusted Partner with partial access to the IACS equipment or Level 3 Site Operations limited to specific machines, production areas, or servers
- Plant Personnel or Trusted Partner access to the Remote Access Server using Remote Desktop Services for all IACS applications

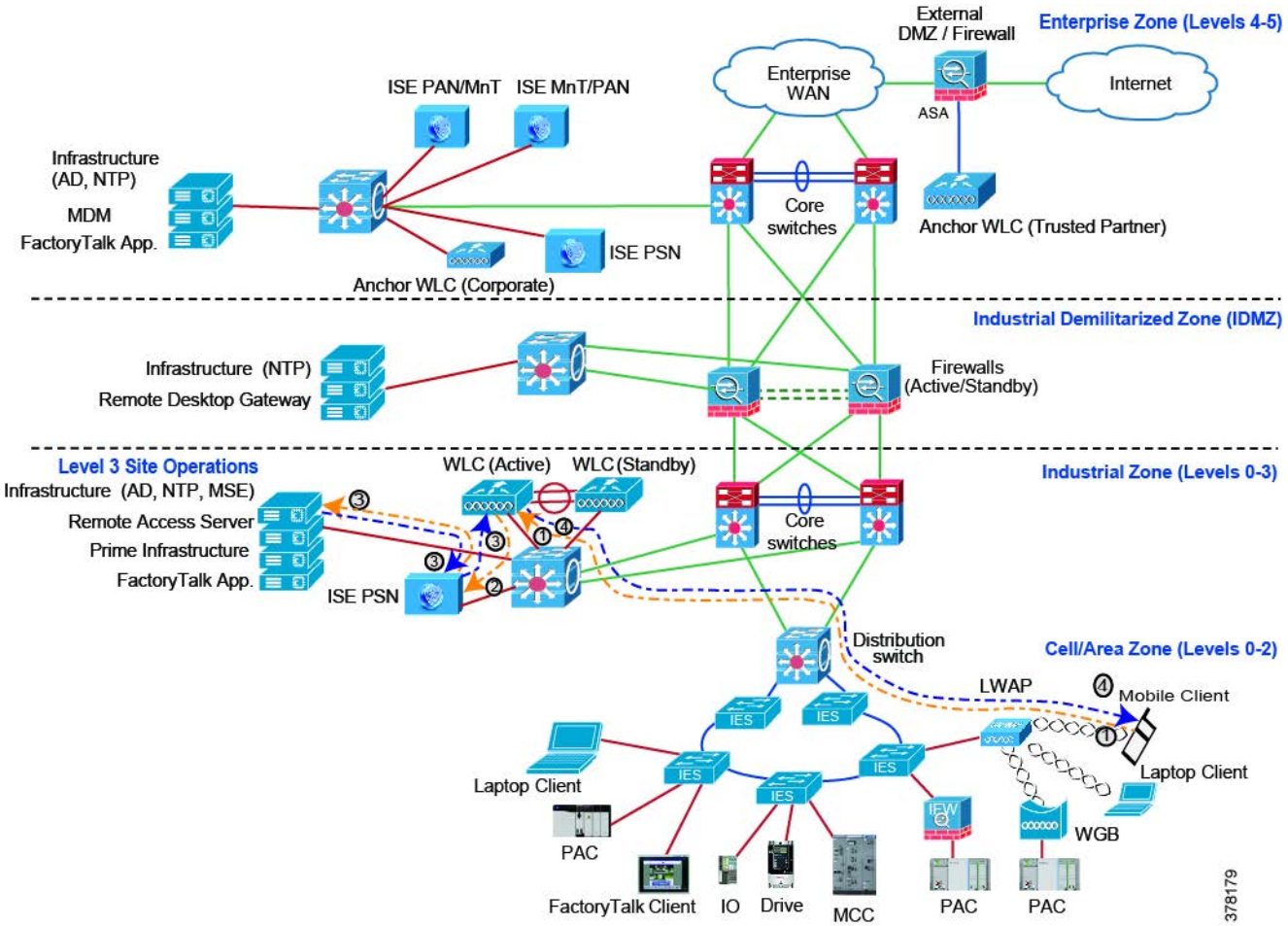
Plant personnel access can be permitted for corporate-issued mobile devices or for BYOD (personal or newly issued devices) if the manufacturer's policy allows BYOD in the network. The architecture should implement profiling and posturing of mobile devices using Cisco ISE and MDM solutions.

Trusted partner access to the Industrial Zone assets should only be allowed from corporate-issued mobile devices that are dedicated for that purpose. Mobile devices owned by trusted partners, vendors and guests should not be given access to the Industrial Zone directly.

A user connecting to the wireless network using the Industrial Employee SSID will be directed by the AP to the Industrial WLC located in the Level 3 Site Operations. The Industrial WLC, using the Cisco ISE Industrial PSN as the authentication server, will validate the user credentials and certificate and will provide appropriate access to the Industrial Zone.

Figure 2-10 is a diagram of the network architecture used in this solution.

Figure 2-10 Wireless Access to Industrial Zone—Plant Personnel or Trusted Partner



As indicated in Figure 2-10:

1. A mobile device connects to the Industrial Employee SSID, logs in, and sends an 802.1X authentication request, which gets tunneled from the AP to the local WLC in the Industrial Zone.
2. The Industrial WLC forwards a RADIUS authentication request on behalf of the mobile device to the Industrial PSN.
3. The next step depends on whether the mobile device is a BYOD (or a corporate-owned device that has not been provisioned) or is a pre-provisioned corporate-issued device.
   a. For a personal (BYOD) mobile device, the Industrial PSN checks AD for the user account. If the account belongs to the correct user group, the Industrial PSN approves the request with a RADIUS response redirecting the user to the BYOD portal to download the user certificate.

      Once the device has the user certificate, it requests network access via the PSN. If the certificate is correct, the PSN approves the request with a RADIUS response that includes the ACL name to be applied at the WLC.
   b. For a corporate-issued mobile device, the user certificate is already present. The Industrial PSN verifies the certificate and whether the mobile device belongs to the whitelist group. If both conditions are met, the PSN approves the request with a RADIUS response that includes the ACL name to be applied at the WLC.
   c. If an MDM solution is implemented, the PSN checks if the mobile device is registered with the MDM server and compliant with the policy. Non-compliant devices are redirected to the MDM portal for remediation or denied access.
4. The traffic flows from the resources in the Industrial Zone through the local WLC to the Plant Personnel or Trusted Partner mobile devices and vice versa. The ACL on the WLC restricts access to certain assets and/or network protocols based on the user group and other criteria.

Wireless Access to Enterprise Zone

This use case (Figure 2-11) describes plant personnel or corporate user access to the Enterprise Zone resources from a mobile device while physically located in the Industrial Zone.

Plant personnel or corporate users may require access to the Enterprise network from the Industrial Zone to be able to:

- Use corporate applications such as email and ERP systems as part of the normal workflow during production.
- Access the Internet and manufacturer’s internal sites for IACS firmware downloads, documentation, and technical support.

The CPwE Identity and Mobility Services architecture provides secure access to the Enterprise Zone for authorized users without compromising the security of the Industrial Zone assets. This type of access removes the requirement for a separate WLAN infrastructure for Enterprise access thus saving cost and maintenance time.

By default, authorization policies defined in the Enterprise Zone apply to the user’s access, including Internet access. Depending on the security policy, the Enterprise access may be further restricted by an ACL on the Industrial WLC and may also restricted to a certain group of users and mobile devices.

The following access policies have been considered:

- Plant Personnel or Corporate User with full access to the Enterprise Zone assets and to the Internet as permitted for a corporate user
- Plant Personnel or Corporate User with partial access to the Enterprise Zone limited to specific application servers

- Corporate User with access to the Remote Desktop Gateway (RDG) in the IDMZ for remote connectivity to the appropriate assets in the Industrial Zone

Plant personnel or corporate users' access to the Enterprise Zone can be allowed for corporate-issued mobile devices or for BYOD (personal or newly issued devices) if the manufacturer's policy allows BYOD in the network. The architecture should implement profiling and posturing of BYOD using Cisco ISE and MDM solutions.

The wireless user's data is placed in a secure EoIP (Ethernet over IP) tunnel between WLCs in both zones. The IDMZ firewall configuration allows the tunnel traffic between WLCs. As a result, the user's traffic is isolated from the Industrial Zone network traffic and terminated in the Enterprise Zone. From a user's perspective, wireless connectivity looks as if a user is attached to the Enterprise wireless network.

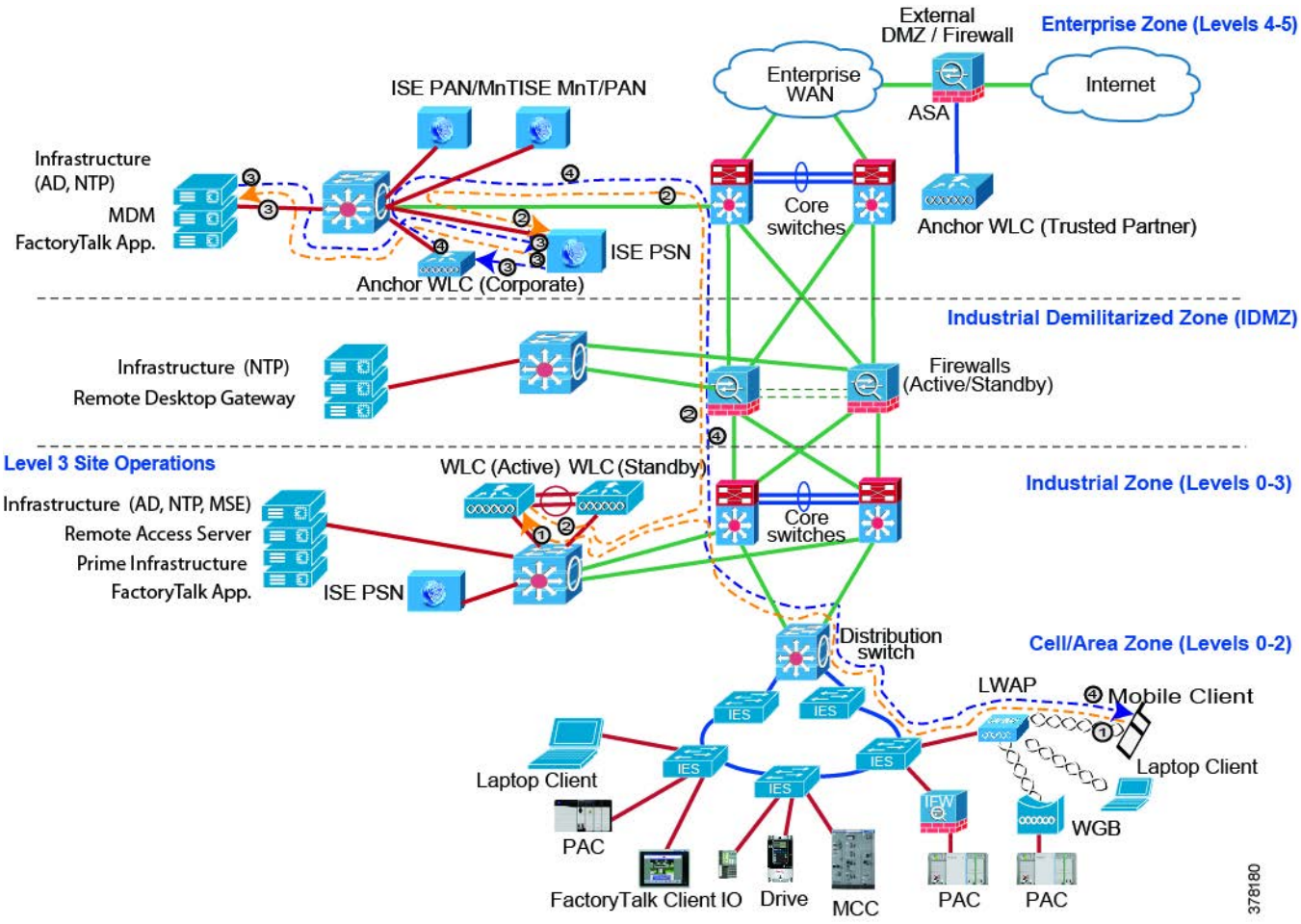
IPsec Tunnel for RADIUS data

In the CPwE Identity and Mobility Services architecture, to secure RADIUS communication between the Wireless LAN controller in the Industrial Zone and the Cisco ISE PSN node in the Enterprise Zone, an IPsec tunnel is created to encrypt and protect RADIUS data as it traverses the IDMZ.

Note For more information about using IPsec with Cisco ISE, refer to the following URL: http://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-22/210519-Configure-ISE-2-2-IPSEC-to-Secure-NAD-I.html

Figure 2-11 is a diagram of the network architecture used in this solution.

Figure 2-11 Wireless Access to Enterprise Zone—Plant Personnel or Corporate User



As indicated in Figure 2-11:

1. A mobile device connects to the Corporate Employee SSID, logs in, and sends an 802.1X authentication request which gets tunneled from the AP to the local WLC in the Industrial Zone.
2. The Industrial WLC forwards a RADIUS authentication request on behalf of the mobile device to the Cisco ISE Enterprise PSN over an IPsec tunnel.
3. The next step depends on whether the mobile device is a BYOD (or a corporate-owned device that has not been provisioned) or is a pre-provisioned corporate-issued device.
   a. For a personal (BYOD) mobile device, the Enterprise PSN checks AD for the user account. If the account belongs to the correct user group, the PSN approves the request with a RADIUS response redirecting the user to the BYOD portal to download the user certificate.

      Once the device has the user certificate, it requests for network access through the PSN. If the certificate is correct, the PSN approves the request with a RADIUS response that includes the ACL name to be applied at the WLC.

   b. For a corporate-issued mobile device, the user certificate is already present. The Enterprise PSN verifies the certificate and whether the device is present in the whitelist group. If both conditions are met, the PSN approves the request with a RADIUS response that includes the ACL name to be applied at the WLC.

c. If MDM solution is implemented, the PSN checks if the mobile device is registered with the MDM server and compliant with the policy. Non-compliant devices are redirected to the MDM portal for remediation or denied access.

4. The traffic flows from the resources in the Enterprise Zone through the EoIP tunnel and the Industrial WLC to the corporate user mobile device and vice versa. The ACL on the WLC restricts access to certain assets and/or network protocols based on the user group and other criteria.

Wireless Access for Trusted Partners and Guests

This use case (Figure 2-12) describes access for mobile devices owned by trusted partners or guests located in the Industrial Zone.

Trusted partners and guests may require access to the Enterprise Guest DMZ and the Internet to be able to:

- Establish VPN access to their company's corporate network as part of the normal workflow during commissioning and maintenance of the vendor's equipment.
- Access the Internet for IACS firmware downloads, documentation, and technical support.
- Establish secure remote access via VPN through IDMZ to the IACS equipment managed by the vendor.

The CPwE Identity and Mobility Services architecture helps to enable secure access to the Enterprise Guest DMZ and the Internet for authorized users without compromising the security of the Industrial Zone assets. This type of access removes the requirement for a separate WLAN infrastructure for guest access thus saving cost and maintenance time.

By default, authorization policies defined for guest users in the Enterprise Guest DMZ apply here, including access to the Internet and VPN portals for trusted partners. However, as opposed to a typical guest access in the Enterprise, trusted partners and guests in the Industrial Zone should have an AD account for authentication.

Depending on the security policy, the partner/guest access may be further restricted by an ACL on the Industrial WLC and may also restricted only to a certain group of devices. The Internet access may also be limited to whitelisted web sites only.

The following access policies have been considered:

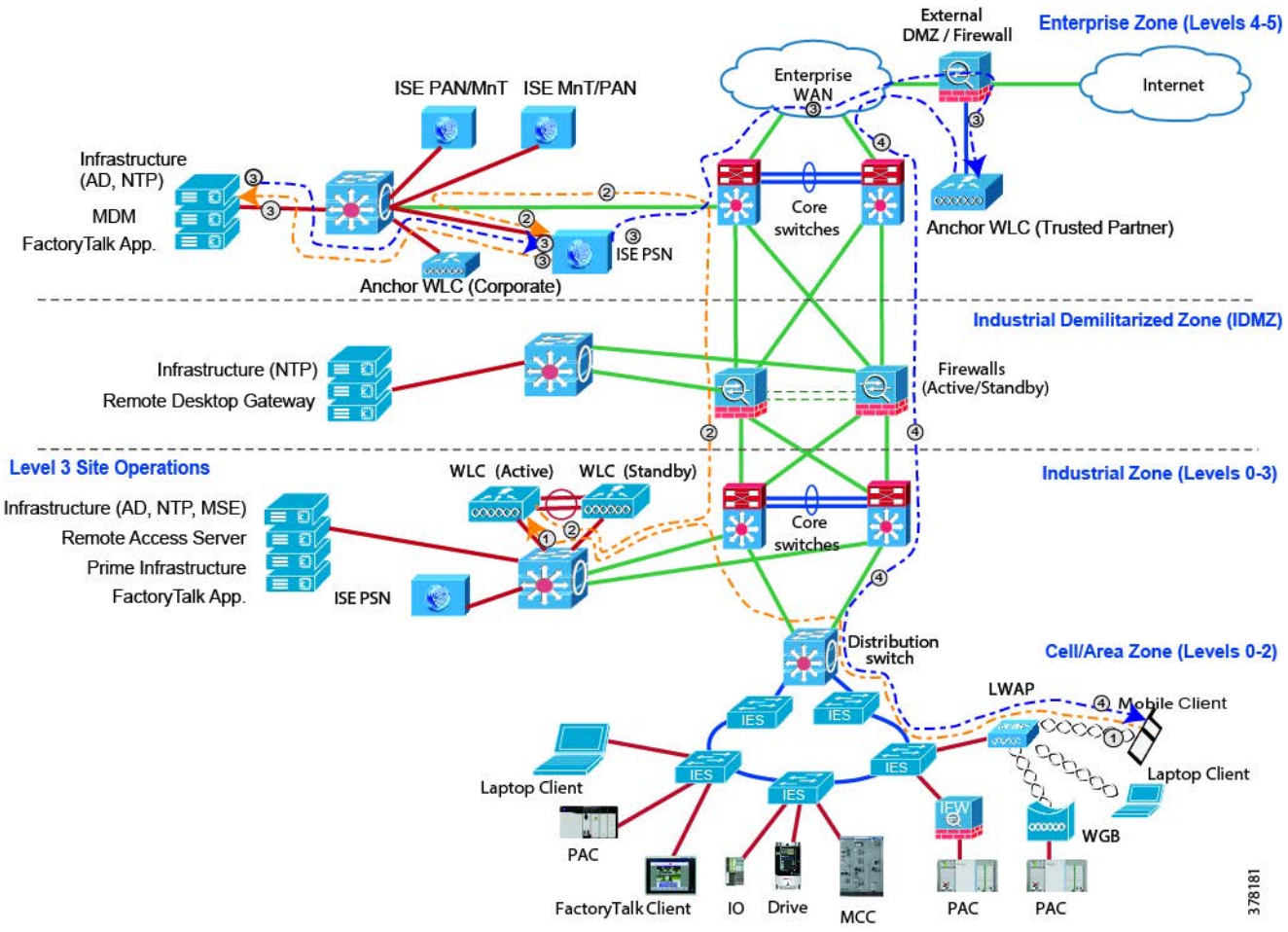
- Trusted partner or guest user with access to the Internet as permitted for a corporate guest user
- Trusted partner access to the VPN portal in the Enterprise DMZ for secure remote access to specific IACS equipment as permitted by manufacturer's security policy

Trusted partner or guest access to the Enterprise Guest DMZ and the Internet can be allowed for corporate-issued mobile devices designated for partner access or for BYOD if the manufacturer's security policy allows BYOD in the network. The architecture should implement profiling and posturing of BYOD using Cisco ISE and MDM solutions.

The implementation for this use case is very similar to the previous case for the Enterprise access. The wireless user's data is placed in a secure EoIP (Ethernet over IP) tunnel between the Industrial WLC and Guest WLC in the Enterprise Guest DMZ. The IDMZ firewall configuration allows the tunnel traffic between WLCs. As a result, users' traffic is isolated from the Industrial Zone network traffic and terminated in the Guest DMZ.

Figure 2-12 is a diagram of the network architecture used in this solution.

Figure 2-12 Wireless Trusted Partner Access



As indicated in Figure 2-12:

1. A mobile device connects to the Trusted Partner SSID, logs in, and sends an 802.1X authentication request, which gets tunneled from the AP to the local WLC in the Industrial Zone.
2. The Industrial WLC forwards RADIUS authentication request on behalf of the mobile device to the Cisco ISE Enterprise PSN over an IPsec tunnel.
3. The next step depends on whether the mobile device is a BYOD owned by the trusted partners or guest or is a pre-provisioned corporate-issued device designated for the trusted partner's use.
   a. For a BYOD mobile device, the Enterprise PSN checks AD for the guest user account. If the account exist and belongs to the correct user group, the PSN approves the request with a RADIUS response that includes the ACL name to be applied at the WLC.
   b. For a corporate-issued mobile device designated for the trusted partner's use, the user certificate is already present. The Enterprise PSN verifies the certificate and whether the device is present in the whitelist group. If both conditions are met, the PSN approves the request with a RADIUS response that includes the ACL name to be applied at the WLC.
4. The traffic flows from the Enterprise Guest DMZ resources and the Internet through the EoIP tunnel and the Industrial WLC to the trusted partner or guest user mobile device and vice versa. User can connect to the partner VPN portal in the DMZ for remote access to IACS equipment.

Centralized Data Switching versus FlexConnect

The CPwE Identity and Mobility Services architecture validates two implementation modes in the Unified WLAN, Centralized Data Switching and FlexConnect Mode.

Centralized Data Switching

In the Unified WLAN design with centralized data switching, all data and control traffic is backhauled from the lightweight access point to the WLC before being terminated and placed on the wired network.

The advantages of this design are centralized access control of all traffic from a single point within the wired network and less complexity for wireless roaming in large scale environments.

The disadvantages of this design are the potential for scalability bottlenecks at the wireless controllers or the network infrastructure connecting to the wireless controllers and inefficient data flow when source and destination are close to each other (in the same Cell/Area Zone). This is especially important for latency sensitive data such as real-time control.

FlexConnect Mode

This mode provides more flexibility in deploying a wireless LAN. For example, the wireless LAN may be configured to authenticate plant personnel using a centralized AAA server, but once the user is authenticated the traffic is switched locally on the IES in the Cell/Area Zone.

FlexConnect mode with local switching functionality eliminates the need for data to go all the way back to the WLC in Level 3 Site Operations when access to local resources within the Cell/Area Zone is a requirement. This reduces the Round Trip Time (RTT) delay for access to IACS applications on plant floor devices, increasing application performance.

The decision to use FlexConnect versus centralized switching model on the LWAP/SSID depends on the application requirements and most prevalent wireless data flows. For example, if mobile users only have to access application servers in Level 3 Site Operations, centralized switching makes more sense.

Autonomous Wireless Access

This section discusses architectures, authentication, and authorization policies for autonomous WLANs in the Industrial Zone.

While Cisco Unified WLAN is the primary architecture for plant-wide wireless deployments, there are cases where an autonomous WLAN is more feasible due to lower cost, lower level of expertise to deploy and maintain, lack of infrastructure, or temporary deployments.

Authentication

Authentication methods in the autonomous WLAN will depend on the existing infrastructure and manufacturer’s security policies. While many companies choose to implement pre-shared key authentication as a quick and easy way to provide wireless connectivity, this approach carries significant risks and should not be used. The CPwE Identity and Mobility Services architecture uses 802.1X authentication for the autonomous WLAN.

Pre-shared Key Authentication

Pre-shared key authentication, such as WPA2-PSK, was designed for home users and small size networks without a centralized authentication server. It relies on a common passphrase that is stored on APs and client devices.

WPA2-PSK method provides strong encryption of users' data as long as the shared key is secure. However there are significant disadvantages and risks associated with pre-shared keys:

- Pre-shared keys cannot be used to limit access only to certain users or user groups. Anyone with the key knowledge can authenticate to the WLAN.
- Once the key is compromised, all mobile devices need to be reconfigured with the new key. This may also apply when a user leaves the company.
- Lost or stolen devices can represent risks since authentication is not tied to the device certificates or user credentials.
- Corporate security policy may not allow pre-shared key authentication.
- Pre-shared key authentication may not support fast roaming methods.

If pre-shared key authentication has to be used when the 802.1X infrastructure is not available, it should be limited to temporary deployments or to limited areas with very strict control of who and from what mobile devices can access the network. In other words, it must not be used for convenience or to bypass existing manufacturer's access rules and security policies.

802.1X Authentication

802.1X authentication in the Autonomous WLAN is similar to the Unified architecture and involves three parties:

- The supplicant—A mobile device that wishes to attach to the wireless network.
- The authenticator—The autonomous AP, for example a Stratix 5100 wireless access point, that accepts authentication requests from the mobile device and sends it to the RADIUS authentication server.
- The authentication server—The RADIUS server, for example Microsoft Network Policy Server (NPS), Cisco ISE, or any other third-party RADIUS server, that validates mobile devices and sends back the success or failure RADIUS message.

The authentication protocols used in the CPwE Identity and Mobility Services with autonomous architecture are:

- Protected Extensible Authentication Protocol (PEAP)
- Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)

Authorization Policies

The authorization policies in the autonomous WLAN architecture with 802.1X are defined using multiple criteria depending on the capabilities of the RADIUS server solution.

- Microsoft NPS can evaluate several conditions: user group, access point name, SSID name, authentication protocol, and date and time. Based on the conditions, a decision is made to allow or deny access to the mobile device.
- Cisco ISE provides enhanced criteria in addition to the standard RADIUS attributes that include mobile device type, OS, profiling, and posturing results.

- Since the Stratix 5100 AP does not support dynamic ACL and VLAN assignment, static ACLs are defined on the AP per SSID. Each user group with a different authorization profile has to connect to an appropriate SSID. If a user tries to connect to the wrong SSID, access will be denied by the RADIUS server.

Autonomous Wireless Architecture

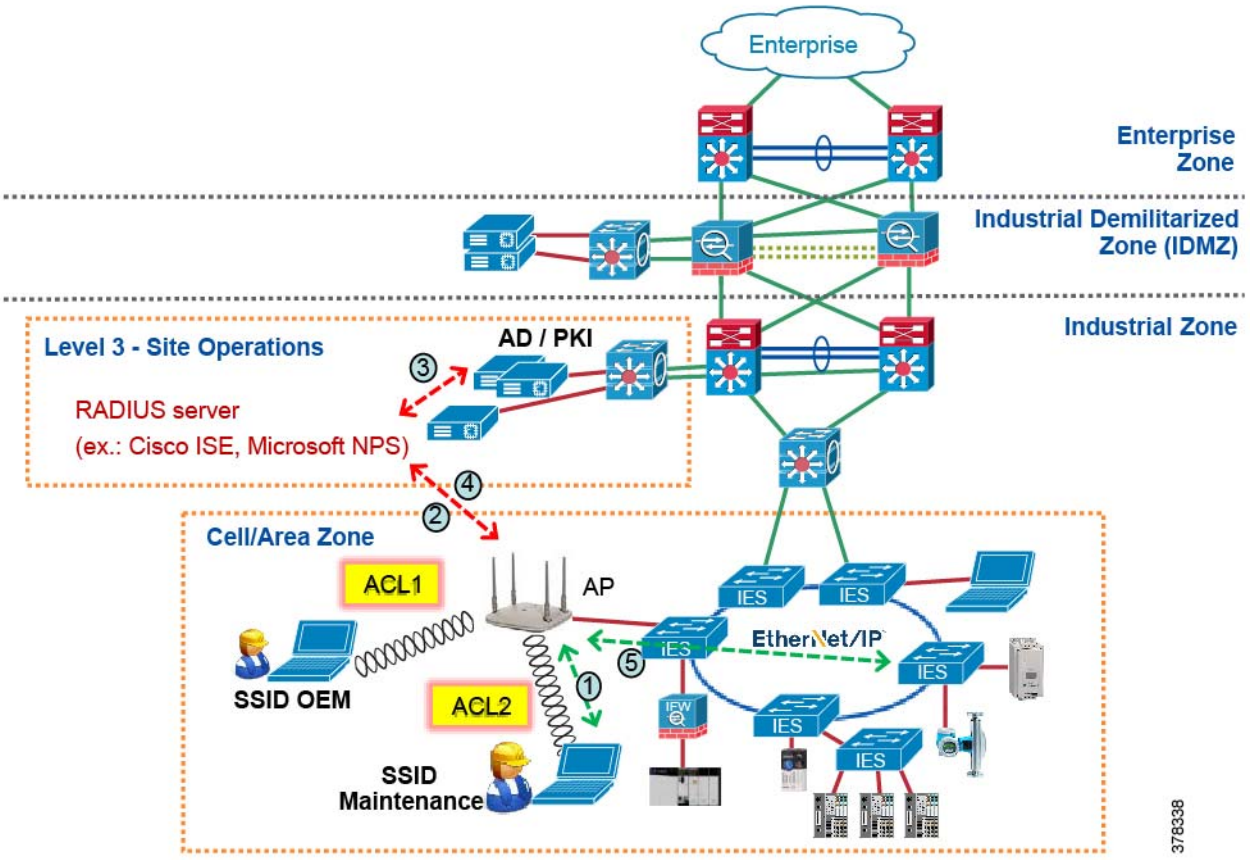
The autonomous WLAN architecture for CPwE Identity and Mobility Services (Figure 2-13) defines user access to the Industrial Zone resources from a mobile device in situations where larger scale plant-wide wireless infrastructure is not available. Plant personnel and trusted partners may require this type of access to be able to:

- Commission new equipment faster.
- Monitor parameters of IACS devices for proactive maintenance.
- Collect information, troubleshoot problems, and apply configuration changes to help minimize downtime.
- Access Level 3 Site Operation servers from mobile HMI and thin client software on mobile devices.

Depending on the manufacturer's security policy and configured authorization rules, different user groups, as well as trusted partners, may get access to different set of Industrial Zone resources. Wireless access in the Autonomous WLAN architecture should only be allowed from corporate-issued mobile devices that are dedicated for that purpose. Mobile devices owned by trusted partners and guests should not be given access to the Industrial Zone directly.

A user connecting to the wireless network using the Maintenance or OEM SSID will be authenticated by the AP using the RADIUS server in the Level 3 Site Operations. If the access is granted to a particular SSID, the static ACL on the AP will control the level of access to the Industrial Zone assets.

Figure 2-13 Autonomous WLAN Architecture



As indicated in Figure 2-13:

1. A mobile device client connects to the Maintenance or OEM SSID, logs in, and sends an 802.1X authentication request to the autonomous AP.
2. The AP forwards RADIUS authentication request on behalf of client to the RADIUS server, for example Microsoft NPS.
3. For a corporate-issued approved mobile device, the user certificate is already present. The RADIUS server verifies the certificate and whether the user is a member of the correct AD group matching the SSID.
4. If these conditions are met, the RADIUS server approves the request with a RADIUS response to the AP.
5. The traffic flows from the resources in the Industrial Zone through the AP to the Plant Personnel or Trusted Partner mobile devices and vice versa. The static ACL on the AP restricts access to certain assets and/or network protocols based on the user group.

Mobile IACS Applications

CPwE Identity and Mobility Services provide framework and design guidelines to develop network and security infrastructure to support mobile IACS applications in the industrial environment.

New mobile applications enable workers to collaborate and share knowledge, view live diagnostics, interact with IACS alarms, and troubleshoot devices from their devices anywhere within the Industrial Zone. This can accelerate worker response times to downtime events and ultimately help reduce mean time to repair (MTTR).

Manufacturers can now pull data from almost any point in their operations and transform it into useful information. That information, known as manufacturing intelligence, can be viewed on mobile devices and shared with other mobile users for quick analysis and decision making.

The following sections provide an overview of mobile IACS applications, their data flows and access requirements, and other considerations.

Mobile HMI and Visualization

FactoryTalk View

FactoryTalk View provides robust and reliable functionality in an HMI solution that scales from a stand-alone, machine-level HMI to a distributed visualization solution.

FactoryTalk View Site Edition (SE) is a supervisory-level HMI software for developing and running distributed applications that can involve multiple users and servers in a network. Mobile users can use FactoryTalk View SE applications on Windows laptops running a client software (“thick clients”) or on mobile devices as “thin clients” via Remote Desktop Protocol (RDP).

FactoryTalk View Machine Edition (ME) is a “stand-alone” HMI solution that runs the application on HMI terminals for machine-level operator interface. Mobile users can view or interact with the HMI terminals using Virtual Network Computing (VNC) client software on their devices.

FactoryTalk ViewPoint

FactoryTalk ViewPoint allows plant personnel to view and interact with the FactoryTalk View SE or ME applications from a web browser on a PC or a mobile device, providing continuous system visibility and improving real-time decision-making. FactoryTalk ViewPoint provides a browser-based client with no additional software to install and configure and is supported on Windows, iOS, and Android devices.

The FactoryTalk ViewPoint SE server is located in the Industrial Zone Level 3 Site Operations. Mobile users can access the ViewPoint web interface directly from the Industrial Zone or using a reverse web proxy server in the IDMZ.

With FactoryTalk ViewPoint ME, mobile users can access HMI terminals in the Cell/Area Zone using the browser.

Note For information about reverse web proxy technology and how to use it with FactoryTalk applications, refer to *Securely Traversing IACS Data across the Industrial Demilitarized Zone*: http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td009_-en-p.pdf

FactoryTalk Batch View

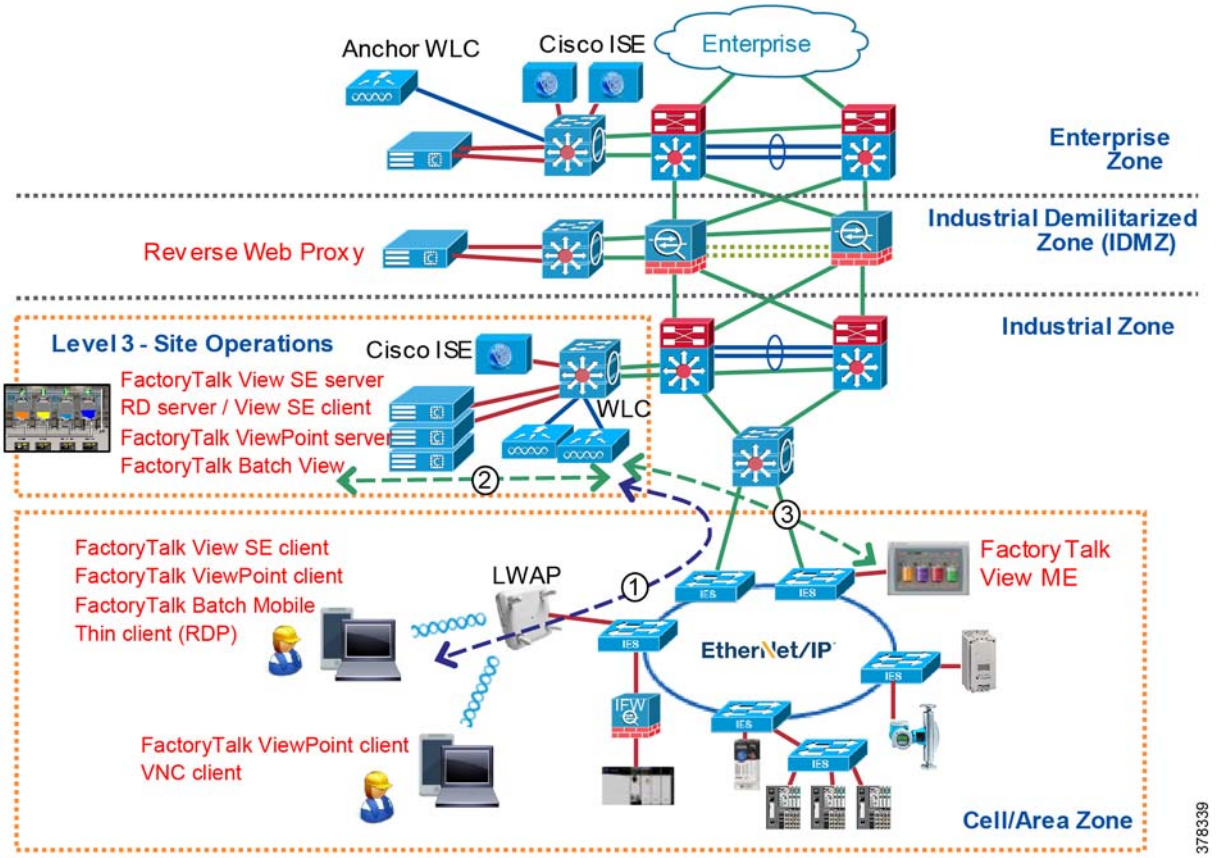
FactoryTalk Batch View is the HMI component of the FactoryTalk Batch solution for process control. It can deliver information to a browser interface or to an HMI control in a FactoryTalk View SE application.

Similar to FactoryTalk ViewPoint, mobile users can access the FactoryTalk Batch View web interface directly from the Industrial Zone using a browser or as thin clients.

Mobile HMI Use Cases

Figure 2-14 illustrate mobile plant personnel access to HMI applications described above in the CPwE architecture.

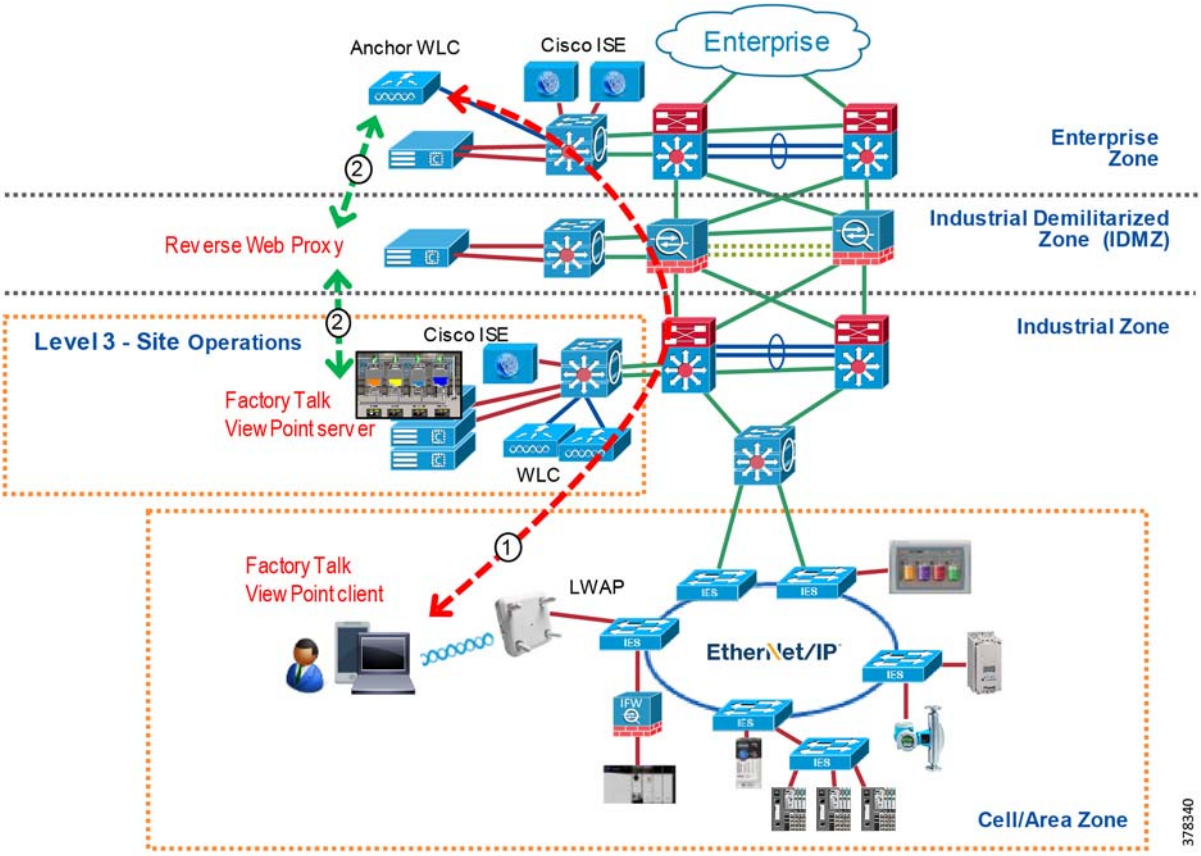
Figure 2-14 Mobile HMI Use Cases - Plant Personnel



1. Wireless connection to the Industrial Zone network through the Industrial WLC
2. Access to FactoryTalk application servers in the Level 3 Site Operations:
   a. FactoryTalk View SE client (Windows laptop) to server via FactoryTalk Live Data
   b. FactoryTalk ViewPoint or Batch Mobile client to server via HTTPS
   c. Thin client to Remote Desktop server running FactoryTalk View SE client
3. Access to FactoryTalk View ME terminals in the Cell/Area Zone:
   a. FactoryTalk ViewPoint client to server on the HMI terminal via HTTP
   b. VNC client to server on the HMI terminal

Another possible scenario is when a reverse web proxy server in the IDMZ provides access to the FactoryTalk ViewPoint server. In such case, mobile corporate users can access the web content on the server (read-only) as illustrated in Figure 2-15.

Figure 2-15 Mobile HMI Use Cases—Corporate User



1. Wireless connection to the Enterprise Zone network through the Enterprise anchor WLC, user data is tunneled between the Industrial and Enterprise WLC
2. Access to the FactoryTalk ViewPoint server (read-only) through reverse web proxy/HTTPS

Analytics and Manufacturing Intelligence

FactoryTalk VantagePoint

FactoryTalk VantagePoint is a powerful web-based Enterprise Manufacturing Intelligence (EMI) solution that integrates all data into a single information management and decision support system. FactoryTalk VantagePoint collects real-time and historical data from different sources such as Logix controllers, OPC data sources, FactoryTalk Historian server, and SQL/Oracle databases.

Mobile users can access manufacturing intelligence data from anywhere in the network on any mobile device for quick analysis and decision making.

FactoryTalk Analytics for Devices

FactoryTalk Analytics for Devices is an IACS appliance that provides a quick look into the health of IACS devices in a Cell/Area Zone, as well as historical diagnostics, dashboards, and action cards. Mobile users can view this data in a browser of a mobile device to identify and solve maintenance issues.

Cloud Analytics

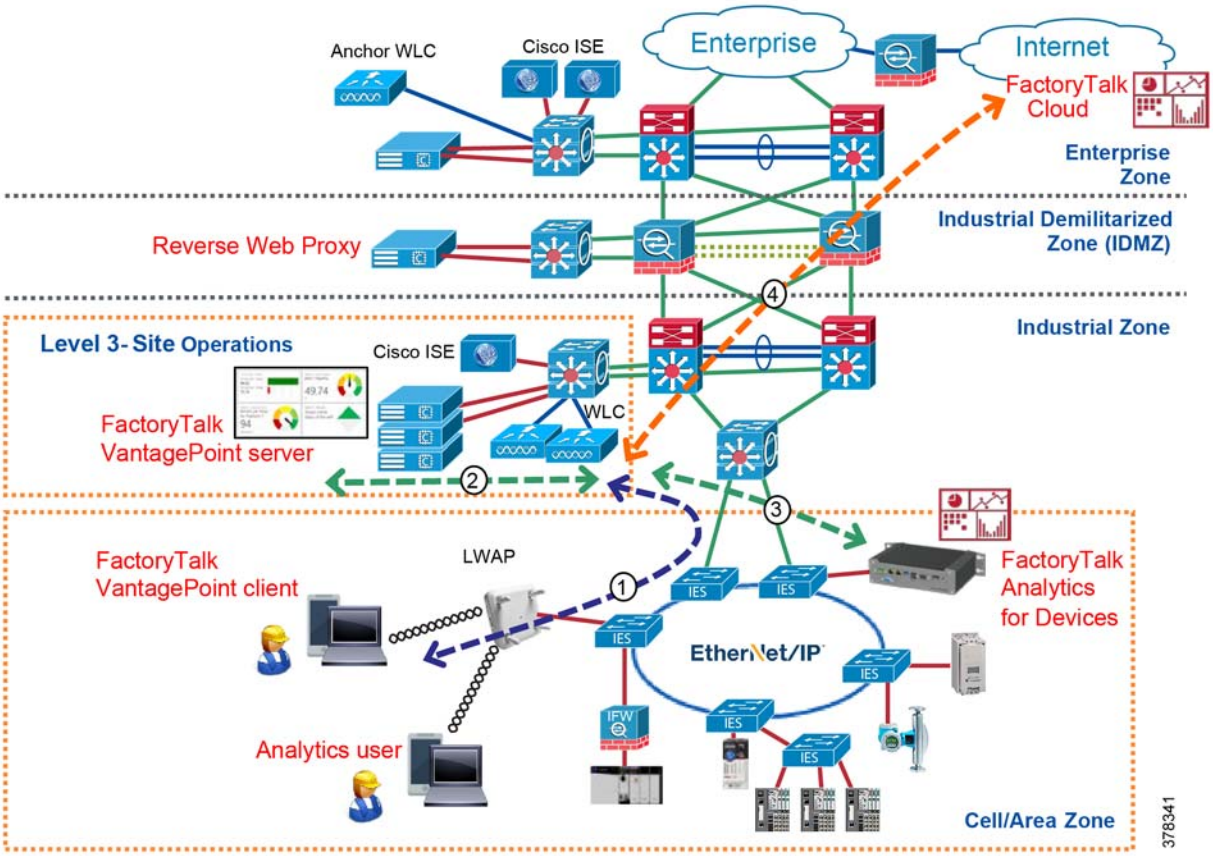
Manufacturers (depending on security stance) increasingly use cloud-based solutions to collect and analyze data from smart IACS assets within the Industrial Zone. Cloud-based data repository can also be used for EMI, Enterprise Resource Planning (ERP), and supply-chain tracking systems. Data can be accessed from a web browser with proper authentication mechanisms.

Rockwell Automation provides FactoryTalk Cloud solution for manufacturing companies and OEMs based on Microsoft® Azure® technology. Mobile plant personnel, corporate users, as well as trusted partners may need access to the FactoryTalk Cloud data from the Industrial Zone. Since data resides on the Internet, architecture and security concerns as well as potential threats and vulnerabilities must be addressed before giving this type of access to mobile users.

Mobile Analytics Use Cases

Figure 2-16 illustrate mobile plant personnel and trusted partner access to EMI and analytics data described above in the CPwE architecture. In this scenario, the mobile user has access to the Industrial Zone directly.

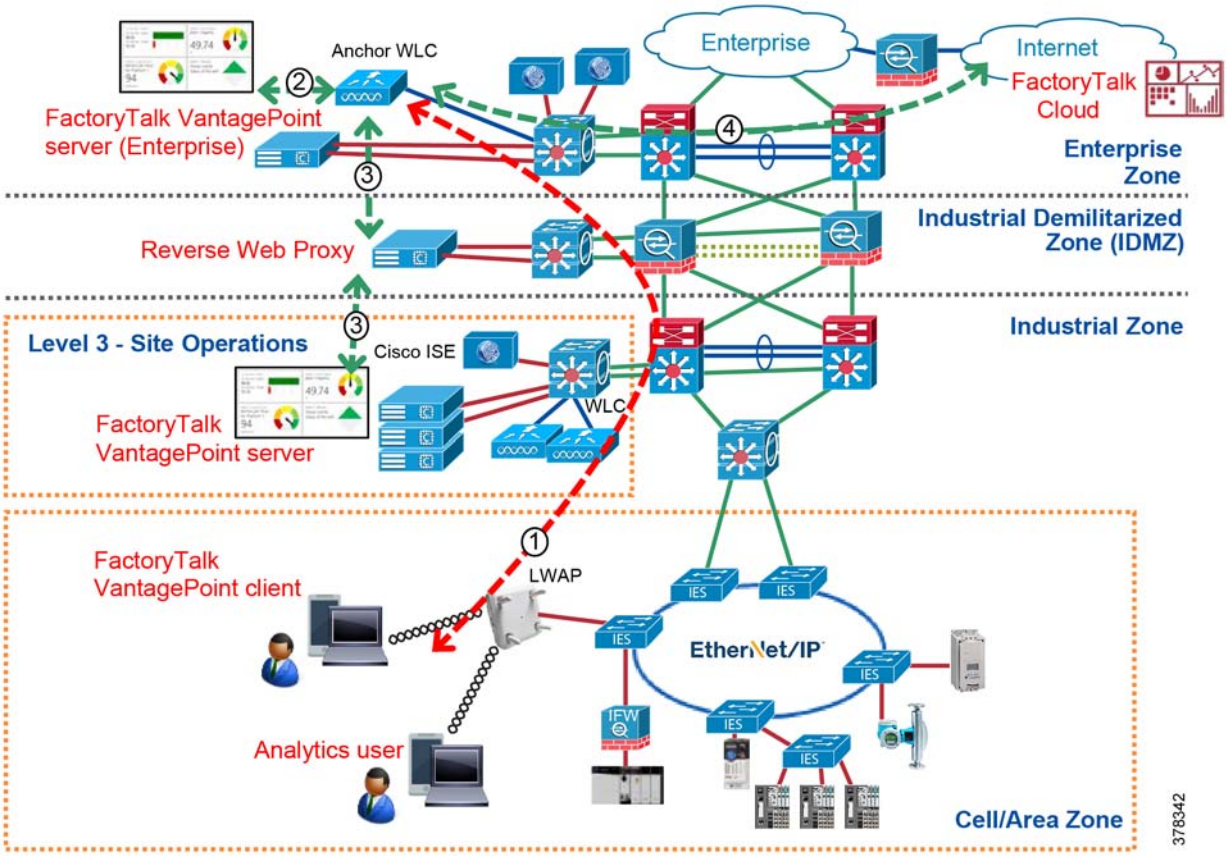
Figure 2-16 Mobile Analytics Use Case—Plant Personnel



1. Wireless connection to the Industrial Zone network through the Industrial WLC
2. Access to the FactoryTalk VantagePoint server in the Level 3 Site Operations via HTTPS
3. Access to the FactoryTalk Analytics for Devices appliance via HTTP or HTTPS
4. Access to the FactoryTalk Cloud web server via HTTPS, traffic is inspected and/or proxied in the IDMZ

In another scenario, a corporate mobile user has access to the Enterprise Zone and can view the FactoryTalk VantagePoint data or FactoryTalk Cloud data (Figure 2-17).

Figure 2-17 Mobile Analytics Use Cases—Corporate User



1. Wireless connection to the Enterprise Zone network through the Enterprise anchor WLC, user data is tunneled between the Industrial and Enterprise WLC
2. Access to the FactoryTalk VantagePoint server in the Enterprise Zone via HTTPS
3. Access to the FactoryTalk VantagePoint server in the Industrial Zone through reverse web proxy/HTTPS
4. Access to the FactoryTalk Cloud web server via HTTPS, traffic is inspected and/or proxied in the Enterprise DMZ

FactoryTalk TeamONE (Diagnostic Modules)

FactoryTalk TeamONE is an iOS and Android application that enables industrial workers to investigate and troubleshoot IACS application issues resulting in increased productivity and reduced MTTR.

FactoryTalk TeamONE consists of multiple modules, with capability to quickly integrate with other Rockwell Automation applications. Diagnostic modules collect real-time information about IACS devices such as device health, status, parameter trends, alarms, and events. This information may come from various sources, for example EtherNet/IP interface of the device, FactoryTalk Alarms and Events server, and FactoryTalk Analytics for Devices.

Connectivity Requirements

FactoryTalk TeamONE functionality depends on the level of access available for a mobile device within the Industrial Zone.

- Diagnostic modules require access to the Industrial Zone assets from a mobile device using a Wi-Fi network
- Diagnostic modules requiring access to Rockwell Automation Knowledgebase articles, image and video attachments, trends, and alarms require connectivity to the FactoryTalk Cloud via a Wi-Fi or cellular network
- Application updates and push notifications require access to Apple or Google servers in the Internet via a Wi-Fi or cellular network

Note Mobile devices by default use the Wi-Fi connection to send and receive data. If the Wi-Fi connection is not available or the signal is very poor, the device falls back to the cellular data connection (if available and enabled). Using both types of connections at the same time (dual-homing), even if technically possible, should not be allowed. As an additional security measure, users may be required to manually disable the cellular data connection or an MDM policy can be applied to restrict the cellular data usage.

A manufacturer's tolerance to risk, security policy and practices, existing network infrastructure, and workflow requirements will determine what type of architecture and access level is appropriate for the FactoryTalk TeamONE deployment. Two main scenarios can be considered for the application:

1. Isolated IACS network (Figure 2-18).
    a. Mobile workers use FactoryTalk TeamONE diagnostic modules while connected to the Industrial Zone WLAN or to an isolated IACS asset with Wi-Fi connectivity. Information is stored locally on the device.
    b. Mobile workers connect to the Enterprise Zone WLAN or use cellular data network to access the Rockwell Automation Knowledgebase via the FactoryTalk Cloud.
2. Converged IACS network (Figure 2-19).
    a. Mobile workers use FactoryTalk TeamONE diagnostic modules while connected to the Industrial Zone WLAN. Cloud connectivity is allowed through the IDMZ with multiple layers of network and application security in place.
    b. Depending on the security requirements, mobile devices could be on-premise only with no cellular access.

Figure 2-18 FactoryTalk TeamONE—Isolated IACS Network

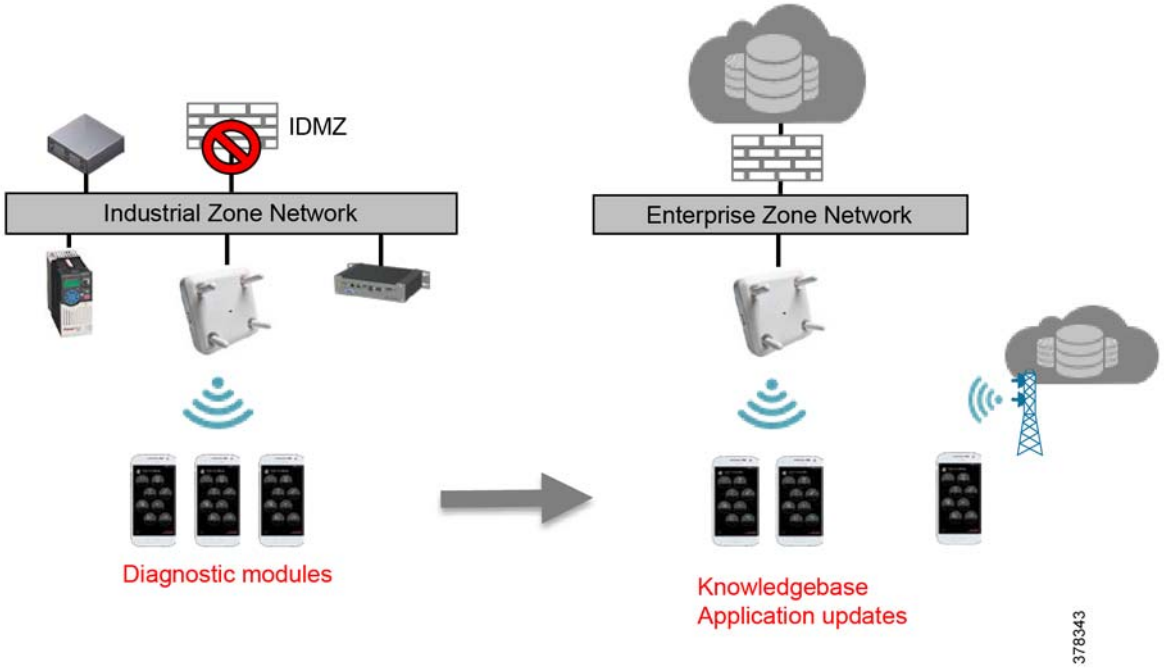
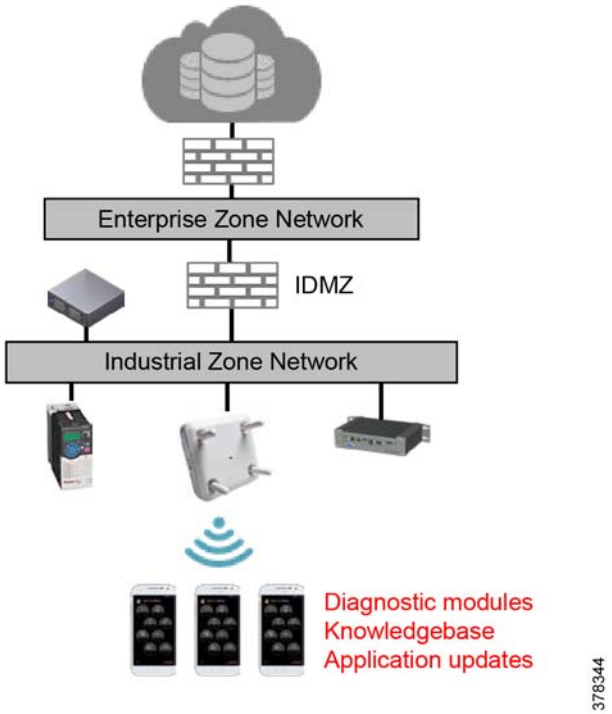


Figure 2-19 FactoryTalk TeamONE—Converged Network

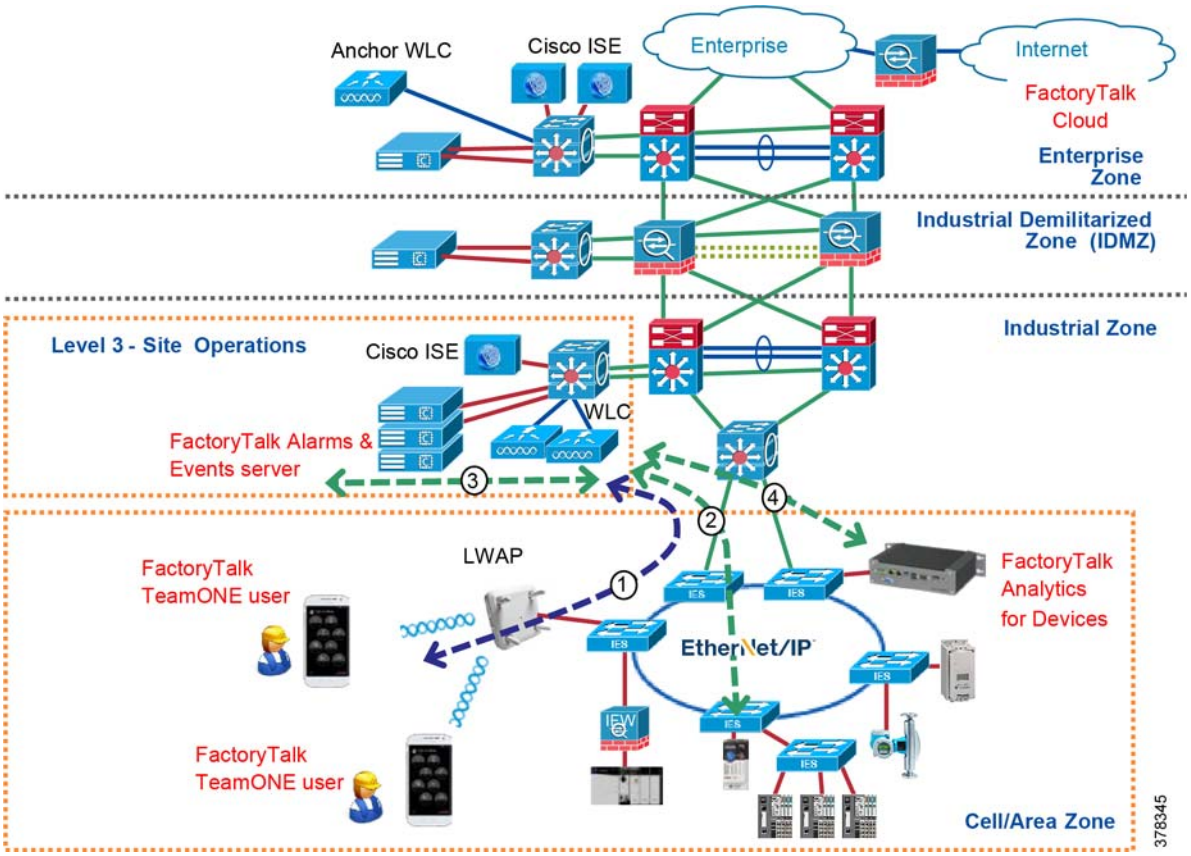


FactoryTalk TeamONE (Diagnostic Modules) Use Cases

Figure 2-20 and Figure 2-21 illustrate FactoryTalk TeamONE in the CPwE Identity and Mobility Services architecture based on scenarios described above.

Figure 2-20 represents FactoryTalk TeamONE access to the Industrial Zone assets (diagnostic modules).

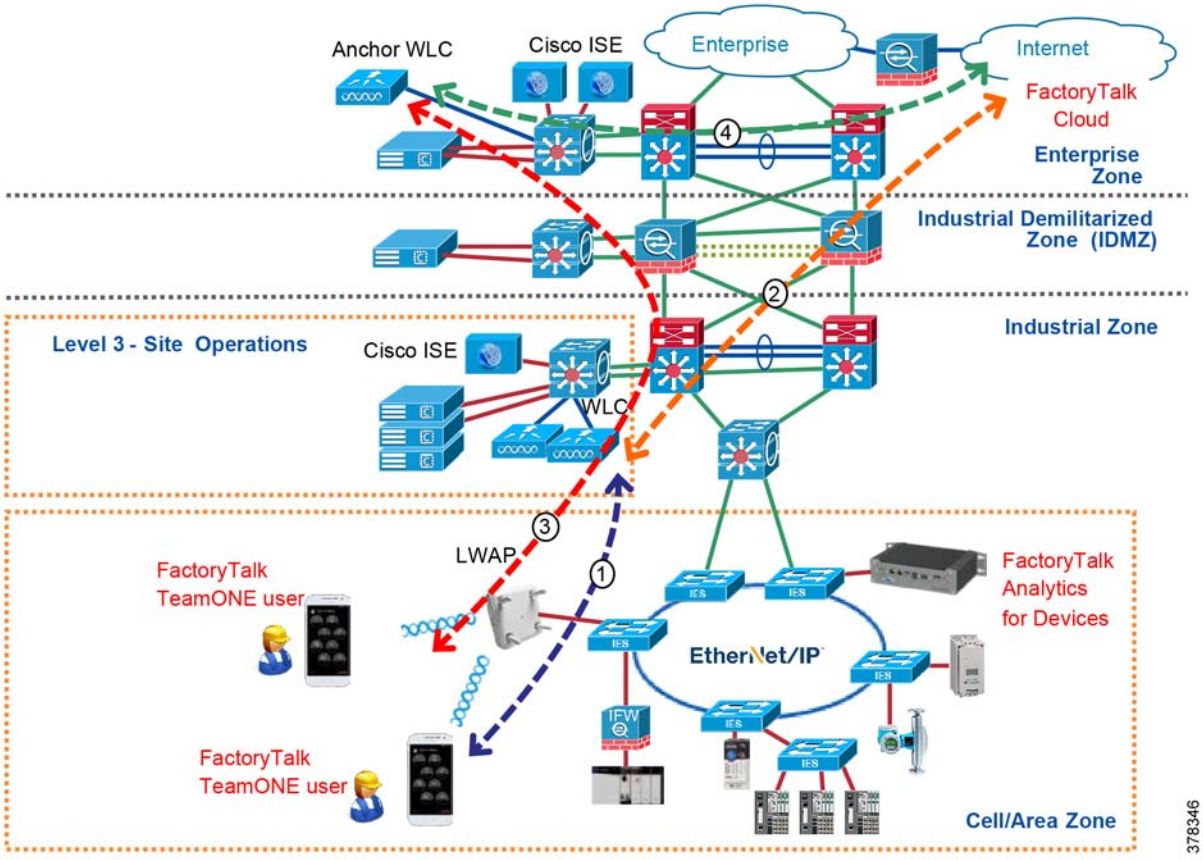
Figure 2-20 FactoryTalk TeamONE Use Cases—Industrial Zone Access



1. Wireless connection to the Industrial Zone network through the Industrial WLC
2. Status and diagnostic data from IACS devices in the Cell/Area Zone via EtherNet/IP
3. Alarm data from the FactoryTalk Alarms and Events server in the Level 3 Site Operations
4. IACS device alerts and diagnostic information from the FactoryTalk Analytics for Devices appliance

Figure 2-21 shows FactoryTalk Cloud access (updates, Knowledgebase) either directly from the Industrial Zone (steps 1-2) or through the tunnel to Enterprise Zone (steps 3-4).

Figure 2-21 FactoryTalk TeamONE Use Cases—Cloud Access



1. Wireless connection to the Industrial Zone network through the Industrial WLC
2. Access to the FactoryTalk Cloud via HTTPS, traffic is inspected and/or proxied in the IDMZ
3. Wireless connection to the Enterprise Zone network through the Enterprise anchor WLC, user data is tunneled between the Industrial and Enterprise WLC
4. Access to the FactoryTalk Cloud via HTTPS, traffic is inspected and/or proxied in the Enterprise DMZ

ThinManager

ThinManager® provides software solutions for IACS networks that enable secure, centralized configuration and deployment of applications and content to every PC, thin client, mobile device, and user.

ThinManager Relevance® is the location-based mobile management platform that allows applications and content to be securely delivered to specific locations within the manufacturer's facility. ThinManager Relevance uses location resolvers and geofences like QR codes, Bluetooth beacons, Wi-Fi, and GPS to confirm that mobile users and devices only receive content in authorized areas. Content specific to a user's role can be delivered based on Relevance user credentials which can be linked to Active Directory accounts.

Within the CPwE Identity and Mobility Services architecture, ThinManager can be used to securely manage content delivery to mobile devices from various applications and data sources in the Industrial Zone: FactoryTalk View SE and ME applications, FactoryTalk VantagePoint data, Studio 5000 Logix Designer,

terminal shadowing, streaming video, and many others. Thin clients can receive content from Microsoft Remote Desktop servers running these applications, as well as VNC servers (for example FactoryTalk View ME terminal) and IP cameras.

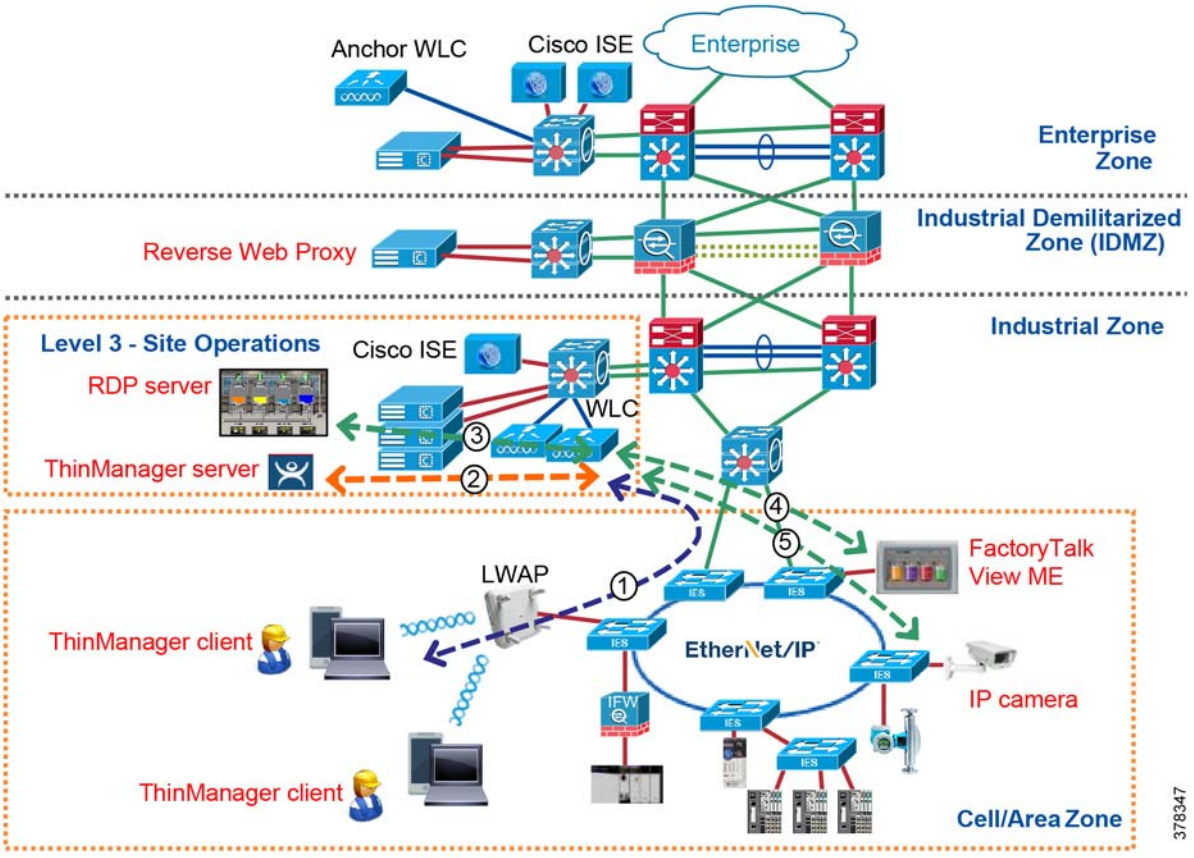
ThinManager solution provides additional security when introducing mobile devices into the industrial environment since no production data is stored locally and content delivery can be authorized by any combination of user, location, and device.

ThinManager Use Cases

A ThinManager service is installed on a server in the Level 3 Site Operations to configure and manage content delivery for thin mobile clients. A client software needs to be installed on Windows, iOS and Android mobile devices to enable ThinManager and Relevance functionality. Redundancy and failover is supported with installation of redundant ThinManager servers and RDP servers.

Figure 2-22 illustrates the ThinManager use cases in the CPwE architecture.

Figure 2-22 ThinManager Use Cases



1. Wireless connection to the Industrial Zone network through the Industrial WLC
2. Communication between the ThinManager server and the ThinManager client application on the mobile device
3. Remote Desktop server content, for example FactoryTalk View SE application screen

4. VNC server content, for example FactoryTalk View ME screen on a HMI terminal
5. Streaming video from an IP camera

Mobile Application Recommendations

Cisco and Rockwell Automation recommend the following security measures when using IACS applications on mobile devices in the Industrial Zone:

- Implement application-level security for user authentication and authorization such as FactoryTalk Security and ThinManager Relevance, in addition to authentication and authorization of mobile devices with Cisco ISE. Application security should be integrated with Active Directory user database.
- Limit read-write access to HMI applications and IACS equipment to dedicated on-premise mobile devices with no cellular connectivity and no Internet access from the Industrial Zone.
- For additional security, use dedicated on-premise mobile devices as thin clients, with location-based authorization and geofence functionality in ThinManager to prevent content delivery outside the authorized area.
- Use provisioning, profiling, and posturing of mobile devices with Cisco ISE and MDM, especially for mobile devices with Internet connectivity outside the Industrial Zone.
- Use 802.1X authentication for Unified and Autonomous WLAN architectures. Avoid using pre-shared key authentication.
- Autonomous WLANs, if necessary, should be restricted to corporate-issued mobile devices only.
- If an application requires access to FactoryTalk Cloud and other web resources directly from the Industrial Zone through the IDMZ:
  - Evaluate corporate standards, security, and risk management policies, industry security standards, and regulatory requirements to determine if this type of access is acceptable.
  - If allowed, limit Internet access from the Industrial Zone to known and corporate-issued devices that stay on premise.
  - Internet access must be secured by methods described in Internet Access Requirements, such as web proxy, TLS proxy, DPI, URL whitelisting or blacklisting, and so on.
  - Confirm that both the cloud provider and the ISP are trusted and provides the necessary network and security services to help protect connectivity and data.

Wired Access Design

In addition to wireless access, manufacturers may need to provide on-site wired access for trusted partners and employees using maintenance ports on IES in the Cell/Area Zone. Wired Employee/Trusted Partner Access is accomplished for the Industrial Zone using the following methods (see Figure 2-23):

- Plant Personnel wired access with direct and full access to Industrial Zone equipment
- Plant Personnel or Trusted Partner partial access to the IACS equipment limited to a specific machine/skid or production area
- Plant Personnel or Trusted Partner access via the Remote Access Server (RAS) using Remote Desktop Services (RDS) for all IACS applications such as Studio 5000 Logix Designer

The access methods mentioned above use IEEE 802.1X authentication for permitting access to the network. Within the CPwE architecture, EAP-TLS is used as the secure authentication method supported with the Active Directory Certificate Services.

Corporate-issued computer access is based on the user group membership and user certificate profiles. These computers are provisioned by IT department and have correct certificates installed using the AD group policy or secure provisioning network. A computer whitelist on Cisco ISE can also be used to limit access to corporate-issued computers only based on the MAC address.

Wired access for contractors and trusted partners should only be allowed via corporate-issued computers designated for this purpose. Wired access for personal or third-party issued computers should not be allowed.

Wired Access Overview

For a user/computer to obtain access, the user must authenticate and present its credentials which are verified by Cisco ISE. The result is an authorization profile that is applied to the IES in the Cell/Area Zone.

To avoid confusion, the ports on the IES should be labeled accordingly within the Cell/Area Zone regarding which ports are open for use as a maintenance port. IES should have MAC port security and physical lock-in and block-outs on the RJ-45 and fiber ports to help prevent users from using the wrong port.

Under normal network operations, the user device would pass through the following steps before being allowed to access the network:

1. Authentication
2. Authorization

Authentication

802.1X authentication for wired access involves three parties:

- The supplicant—A client computer that wishes to attach to the network.
- The authenticator—The Stratix or Cisco IES that send RADIUS request to the authentication server.
- The authentication server—Cisco ISE which validates the user’s identity and sends the RADIUS response back to the IES.

Authentication policies are used to define the protocols used by Cisco ISE to communicate with the mobile devices and the identity sources to be used for authentication. Cisco ISE evaluates the conditions and, based on whether the result is true or false, applies the configured result.

The authentication protocols used in CPwE Identity and Mobility Services are:

- Protected Extensible Authentication Protocol (PEAP)
- Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)

Authorization Policies

Authorization policies for wired access 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 computer and can include tasks such as an associated VLAN and an associated downloadable ACL (DACL).

An additional identity group (whitelist) may be defined on Cisco ISE for the purpose of uniquely identifying corporate-issued devices. The whitelist is manually updated by the IT administrator and contains the MAC addresses of the computers that are allowed on the network.

Authorization rules in Cisco ISE can use wide variety of conditions including:

- User group membership
- Authentication protocol
- Device type and OS
- Posturing and profiling results
- Wired user location based on the IES name
- Time of access

Different access scenarios for a wired user are:

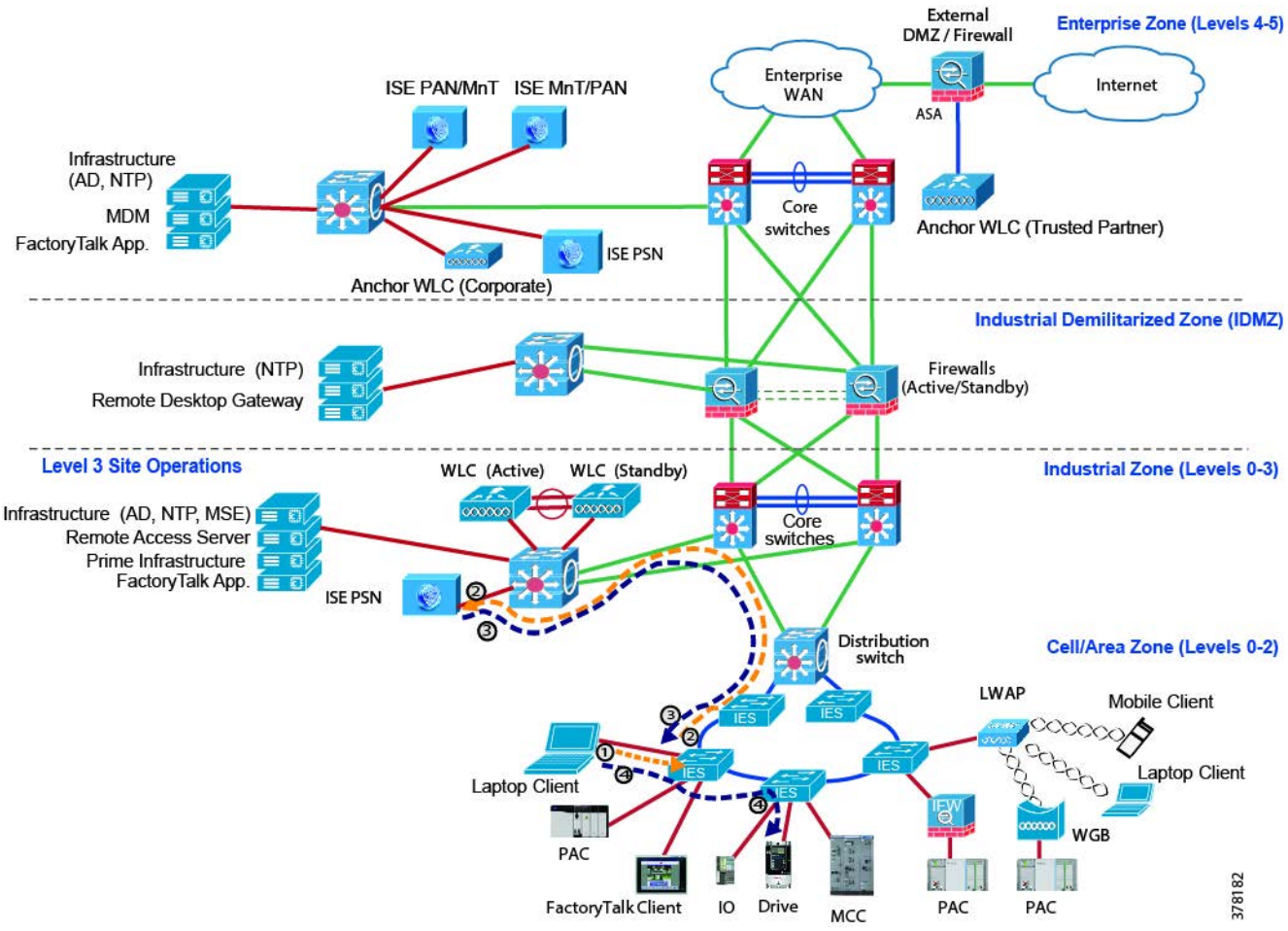
- User is allowed unrestricted access to the Industrial Zone.
- User is allowed limited access to the specific Cell/Area Zone or to specific devices within the Cell/Area Zone.
- User is allowed access only to the RAS in the Level 3 Site Operations.

The computers can be denied wired access if the user is not in the Active Directory or belongs to the wrong group, the certificate has expired or invalid, the device is a part of the Blacklist group, or the device type and OS is not allowed access.

Wired Plant Personnel/Trusted Partner Access

Figure 2-23 illustrates wired access use case implementation for the roles such as Plant Personnel and Trusted Partner for CPwE Identity and Mobility Services.

Figure 2-23 Wired Access to Industrial Zone—Plant Personnel or Trusted Partner



1. Wired user connects to the maintenance port on the IES, logs in, and sends the 802.1X authentication request.
2. The IES forwards RADIUS authentication request on behalf of the user to the ISE PSN in the Industrial Zone.
3. A corporate-issued computer should already be joined to the domain and have the correct user certificate. The Industrial PSN verifies the user credential, group membership, user certificate, and whether the computer is present in the whitelist group. If all conditions are met, the PSN approves the request with a RADIUS response that includes the ACL name and VLAN to be applied at the IES port.
4. The traffic flows from the resources in the Industrial Zone through the IES to the Plant Personnel or Trusted Partner computer and vice versa. The dynamic ACL on the IES restricts access to certain assets and/or network protocols based on the user group and other criteria.

Note Computers connecting to the wired maintenance ports in the Cell/Area Zone should have proper OS protection mechanisms such as antivirus and malware protection software as well group policy restrictions. In addition to the 802.1X authentication, FactoryTalk Security should be used to provide application level security and authorization.

CHAPTER 3

Configuring the Infrastructure

This chapter describes how to configure Cisco ISE infrastructure in the CPwE Identity and Mobility Services architecture based on the design considerations of the previous chapters. It covers the configuration of the network infrastructure, network services, data traversal, web application access, and network and application security, all from an IDMZ perspective. It includes the following major topics:

Network Infrastructure Configuration

This section describes validated configurations for the network infrastructure that is needed to support CPwE Identity and Mobility Services use cases with Cisco ISE.

The following configuration steps are covered in this section:

- Active Directory Configuration
- DNS Configuration
- Dynamic Host Configuration Protocol (DHCP) Configuration
- Certificate Services Configuration
- Network Time Protocol (NTP) Configuration

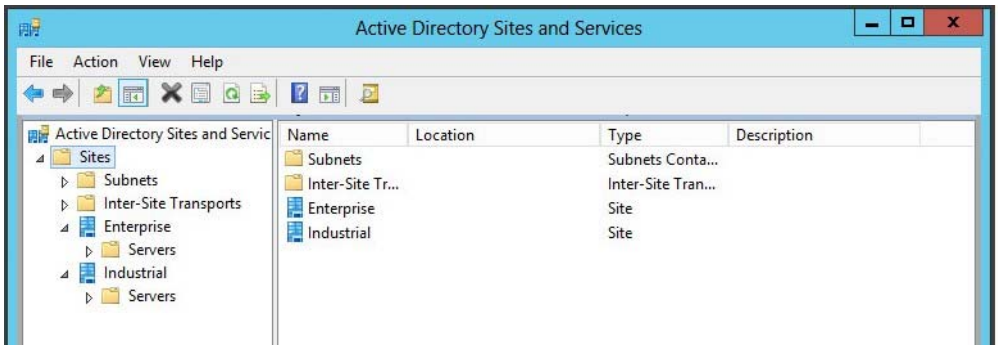
Active Directory Configuration

The following steps describe the configuration required to install and configure AD DS in the Industrial Zone as part of a single corporate domain, including AD replication between the Enterprise and Industrial Zones.

Step 1 Add a new AD site for the Industrial Zone using the **Active Directory Site and Services** console on the Enterprise DC.

Step 2 Create subnets that define IP address ranges for the Industrial Zone AD site.

Figure 3-1 Windows Server 2012 Active Directory Sites and Services Window



Step 3 Configure IDMZ firewall to allow AD replication between DCs in the Enterprise and Industrial Zones.

a. Allow TCP/UDP ports for protocols such as LDAP, Kerberos, SMB, and RPC.

b. Restrict communication to specific IP addresses that belong to DC servers.

c. Configure **DCE RPC inspection** on the IDMZ firewall.

Note Detailed steps for IDMZ firewall configuration are available in *Securely Traversing IACS Data across the Industrial Demilitarized Zone Design and Implementation Guide* at the following URL: http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td009_-en-p.pdf

Step 4 Configure a Domain Controller in the Industrial Zone.

a. Install **Active Directory Services** role on an existing Windows server in the Site Operations environment.

b. Promote the server to a **Domain Controller** and add it to an existing corporate domain using Domain Admin user credentials.

c. Enable **Domain Name System (DNS)** and **Global Catalog** DC options.

d. Select the Industrial Zone site to which this DC belongs and define the **Directory Services Restoration Mode (DSRM)** password for this DC.

e. Select the Enterprise Zone DC from which you want to replicate the AD DS installation data. Alternatively, you can select the option Install from Media to reduce the time and amount of traffic during the installation.

f. Configure additional options as needed, complete the installation, and restart the server.

Step 5 Repeat the previous steps to configure an additional DC in the Industrial Zone for redundancy.

Step 6 Create the necessary users groups for the Industrial Zone.

Note Detailed information on how to install AD DS is available at the following URLs:

https://technet.microsoft.com/en-us/library/hh472162(v=ws.11).aspx

https://technet.microsoft.com/en-us/library/hh831477.aspx

DNS Configuration

The DNS server role is typically installed on the Industrial Zone DC as part of the AD DS installation when joining the existing corporate domain.

After DNS configuration in the domain is completed, the following steps are required as part of the Cisco ISE distributed setup:

Step 1 Add host records and enter IP addresses and fully qualified domain names (FQDNs) of all the Cisco ISE nodes in the DNS server.

Step 2 Configure the forward and reverse DNS lookup for all the Cisco ISE nodes in the DNS server.

DNS-resolvable names are required for node registration by the primary PAN. The FQDN of ISE nodes are also used as subject names when creating security certificates.

Note Refer to the following URL for guidance and procedures on configuring DNS in the AD environment: https://technet.microsoft.com/en-us/library/cc730921.aspx

DHCP Configuration

Dynamic Host Configuration Protocol (DHCP) servers should be installed as part of the Level 3 Site Operations environment to support automatic IP address assignment for wired and wireless clients in the Industrial Zone. The following DHCP configuration is required:

Step 1 Configure redundant DHCP servers in the Industrial Zone. The DHCP role can be installed on the Industrial DCs or stand-alone servers.

Step 2 Create DHCP scopes with address pools for various groups of endpoints (mobile devices) depending on the SSID and VLAN to which they connect.

Step 3 Configure Layer 3 switches and WLCs to relay DHCP requests to the DHCP servers on each VLAN IP interface where mobile clients are attached.

Step 4 For mobile users that connect to the Enterprise Zone or Guest DMZ using the tunnel, DHCP scopes should be created on the servers in those zones.

The CPwE Identity and Mobility Services architecture has been tested using Windows servers running DHCP service role. Many network infrastructure devices, such as IES, autonomous APs, and Cisco WLCs, also have internal DHCP server features. It is recommended to avoid using network devices to assign addresses to mobile clients due to scalability and roaming concerns.

Note Refer to the following URL for guidance and procedures on configuring DHCP on Windows servers: https://technet.microsoft.com/en-us/library/cc755282.aspx

Certificate Services Configuration

This section describes the configuration of certificate services (CS) in the CPwE Identity and Mobility Services architecture using Microsoft Windows server implementation.

This architecture has been validated using common PKI for the Enterprise and Industrial Zones, with the root CA in the Enterprise Zone and the subordinate CA in the Industrial Zone. Large scale PKI may use an intermediate CA to issue certificates to the Industrial subordinate CA.

Note This design guide does not provide in-depth guidance for PKI and AD CS deployment and only outlines important steps to implement CPwE Identity and Mobility Services with PKI. For detailed information on configuring AD CS, please refer to the following URL: https://technet.microsoft.com/en-us/library/hh831740(v=ws.11).aspx

Step 1 Verify that AD CS for the domain is configured to support certificate distribution and certificate status verification.

a. Stand-alone root CA and Enterprise intermediate and subordinate CA should be deployed in the Enterprise Zone as part of the AD Certificate Services.

b. Trusted root CA certificates, including certificates from trusted third-parties, should be added to the Trusted Root Certification Authorities store in the Group Policy and automatically distributed to clients.

c. The domain group policy should be configured to automatically enroll users for certificates. Note that some organizations may choose to do manual certificate enrollment by IT administrators depending on the PKI practice policy.

d. Appropriate certificate templates should be created and configured for different purposes such as user and workstation authentication, web server authentication, IPsec, and so on.

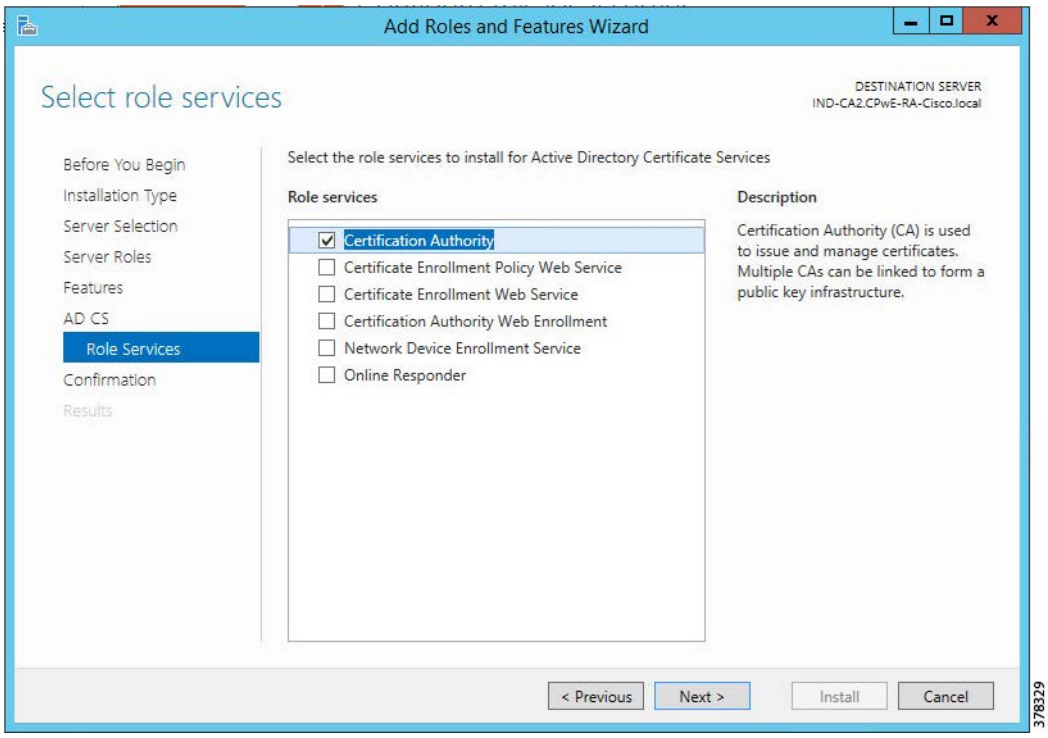
e. Make sure that certificate status and revocation information are updated regularly and made available to relying parties by CRL Distribution Points (by HTTP, LDAP, or file shares) or OCSP Responders (by OCSP).

Step 2 Configure a subordinate CA in the Industrial Zone. Do not use the DC server for this role.

a. To customize default settings for the CA, configure the CAPolicy.inf file and place it in the **C:\Windows** folder. This file allows you to specify CA parameters such as private key length, signature algorithms, validity periods for certificates, and many others. Refer to the Microsoft resources for details.

b. Install **Active Directory Certificate Services** role on the server. Select **Certification Authority** role service.

Figure 3-2 Adding Certificate Authority Service

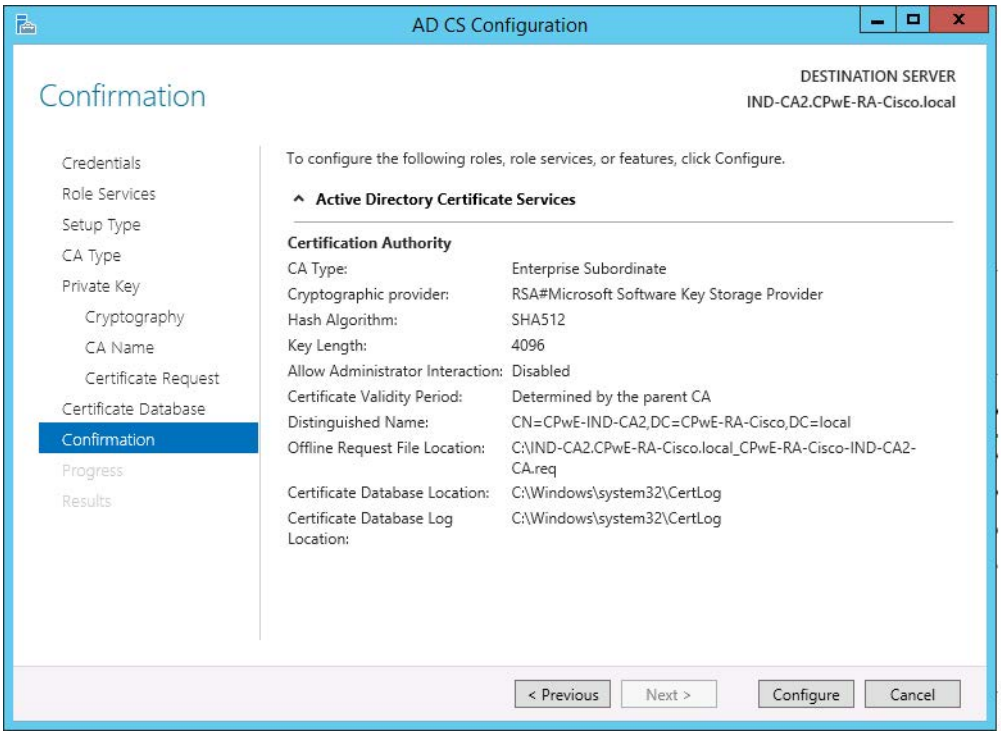


c. In the **AD CS Configuration** wizard, select CA types as **Enterprise CA** and **Subordinate CA**, create a private key, and configure cryptographic options per the manufacturer's PKI policy.

d. Configure **Common Name (CN)** for the CA that will be used in the issued certificates.

e. Save a certificate request to a file on the local server and complete the configuration.

Figure 3-3 CA Configuration Summary



Step 3 Issue the certificate for the Industrial CA on the parent CA.

a. Manually transfer the certificate request file from the Industrial CA to the parent CA in the Enterprise Zone (either root CA or intermediate CA).

b. Submit the request on the parent CA and issue a certificate for the Industrial CA. The details of this process may vary per your company's PKI policy and procedures.

c. Copy the certificate file to the Industrial CA and install the CA Certificate using the **Certification Authority** console. Start the CA service.

Step 4 Configure additional CA properties.

a. In the CA Properties, configure **CRL Distribution Points (CDP)** locations via HTTP or LDAP. These can reside on the local server or on a remote server. Relying parties will use CDP to obtain certificate revocation information.

b. In the CA Properties, configure **Authority Information Access (AIA)** locations where users can obtain the CA certificate by HTTP or LDAP.

c. In the Revoked Certificates properties, configure **CRL publication intervals** as specified by the manufacturer's policy.

Step 5 Select **Certificate Templates to Issue** and add templates from the AD store depending on the manufacturer's needs.

a. Add a certificate template for User Authentication that allows domain users to auto-enroll for certificates.

b. Add a certificate template with the intended purposes of Server and Client Authentication. This template is needed for the Cisco ISE system certificates to function properly.

Note Refer to the following URL for information about certificate templates in AD DS: https://technet.microsoft.com/en-us/library/cc730826(v=ws.10).aspx

Step 6 If required, install **Certificate Authority Web Enrollment** service for web-based certificate request, renewal, and CRL retrieval in the Industrial Zone.

a. It is recommended to install the CA Web Enrollment service and other AD CS services on a separate server(s) in the Industrial Zone.

b. **Web Server (IIS)** role and features will be added automatically. Configure the IIS for HTTPS and provide the SSL certificate from the Industrial CA.

c. Configure Windows Authentication for users connecting to the web server.

Step 7 If required, install **Certificate Enrollment Web Service** and **Certificate Enrollment Policy Web Service** for non-domain users to enroll for and renew certificates. This may not be necessary in the CPwE architecture since the Cisco ISE will be used to issue certificates to BYOD and guest users (if allowed in the network).

Step 8 If required, install **Network Device Enrollment Service (NDES)** to issue and manage certificates for network devices such as IES and routers using SCEP. While this service can be used, in principle, to enroll mobile devices in the BYOD scenario, Cisco ISE will use its internal SCEP service for that purpose.

Note In the CPwE Identity and Mobility Services architecture, Cisco ISE internal CA is used to issue certificates to BYOD and guest users (if allowed in the network) and operates as a SCEP proxy server for mobile devices. Therefore, it may not be necessary to deploy Certificate Enrollment Web Service and NDES for mobile users.

Step 9 If required, install **Online Responder** service to provide real-time certificate status to relying parties via OCSP.

NTP Configuration

The CPwE Identity and Mobility Services architecture requires NTP servers for each zone and time synchronization across the entire infrastructure to support Active Directory, PKI, and distributed Cisco ISE. Time synchronization is necessary in order to avoid problems with certificate validity, user logins, unsynchronized logs, etc.

Detailed NTP configuration in the CPwE architecture is out of scope for this design and implementation guide. In general, these steps should be completed:

Step 1 Configure NTP servers in the network and verify that all clients and infrastructure devices can reach them from the Industrial Zone, Enterprise Zones, and IDMZ.

Step 2 Make sure that NTP servers in the Industrial Zone can synchronize their clock to the Enterprise NTP servers through the IDMZ or synchronize to a common time source such as a GPS time source.

Step 3 Follow Microsoft guidelines for configuring Windows Time Service in the domain.

Note Refer to the following URLs for more information:

- Network Time Protocol: Best Practices White Paper
  http://www.cisco.com/c/en/us/support/docs/availability/high-availability/19643-ntpm.html
- Windows Time Service
  https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/windows-time-service/windows-time-service

Initial Cisco ISE Configuration

This section describes the validated configurations required for the initial Cisco ISE setup. You must perform this initial Cisco ISE setup before configuring authentication and authorization policies for clients.

The following configuration steps are covered in this section:

- Cisco ISE Licensing
- Cisco ISE Certificate Configuration
- Distributed Setup Configuration
- External Identity Source (AD) Configuration
- Whitelist Configuration
- Network Device Configuration

Note It is assumed that all Cisco ISE nodes have been installed as VMs or physical appliances and basic parameters are configured with the initial setup program using the CLI. These steps are covered in the *Cisco Identity Services Engine Installation Guide* at the following URL:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/install_guide/b_ise_InstallationGuide22/b_ise_InstallationGuide22_chapter_010.html

Cisco ISE Licensing

Cisco ISE licensing offers two options to manage your licenses:

- Smart Licensing—Licenses are maintained in a centralized database called the Cisco Smart Software Manager (CSSM). With a single token registration, you can monitor Cisco ISE software licenses and endpoint (mobile device) license consumption easily and efficiently.
- Traditional Licensing—Licenses are purchased and imported individually based on current needs. Application features and access are managed from Cisco ISE, such as the number of concurrent endpoints (mobile devices) that can use Cisco ISE network resources.

Licensing in Cisco ISE is supplied in different packages—Base, Plus, Apex, and Device Administration—for both Traditional and Smart Licensing options. For the CPwE Identity and Mobility Services architecture, Base, Plus, and Apex license packages (Table 3-1) may be required depending on the mobile device use cases described in Chapter 2, “CPwE Identity and Mobility Services Design Considerations.”

Table 3-1 Cisco ISE Licensing

Cisco ISE License Package	Perpetual or Subscription	Cisco ISE Functionality for CPwE	Notes
Base	Perpetual	• Basic network access: AAA, IEEE 802.1X • Guest services	
Plus	Subscription (1, 3, or 5 years)	• Device Registration and BYOD Provisioning • Internal Certificate Authority • Profiling Services • MSE integration for location services	Does not include Base services; a Base license is required to install the Plus license.
Apex	Subscription (1, 3, or 5 years)	• Third Party MDM integration • Posture Compliance	Does not include Base services; a Base license is required to install the Apex license.

Cisco ISE will notify you of license expiration or consumption problems 90, 60, and 30 days in advance.

Step 1 Import the necessary licenses to the Cisco ISE node that will have the primary PAN role.

a. Obtain the license file from Cisco.

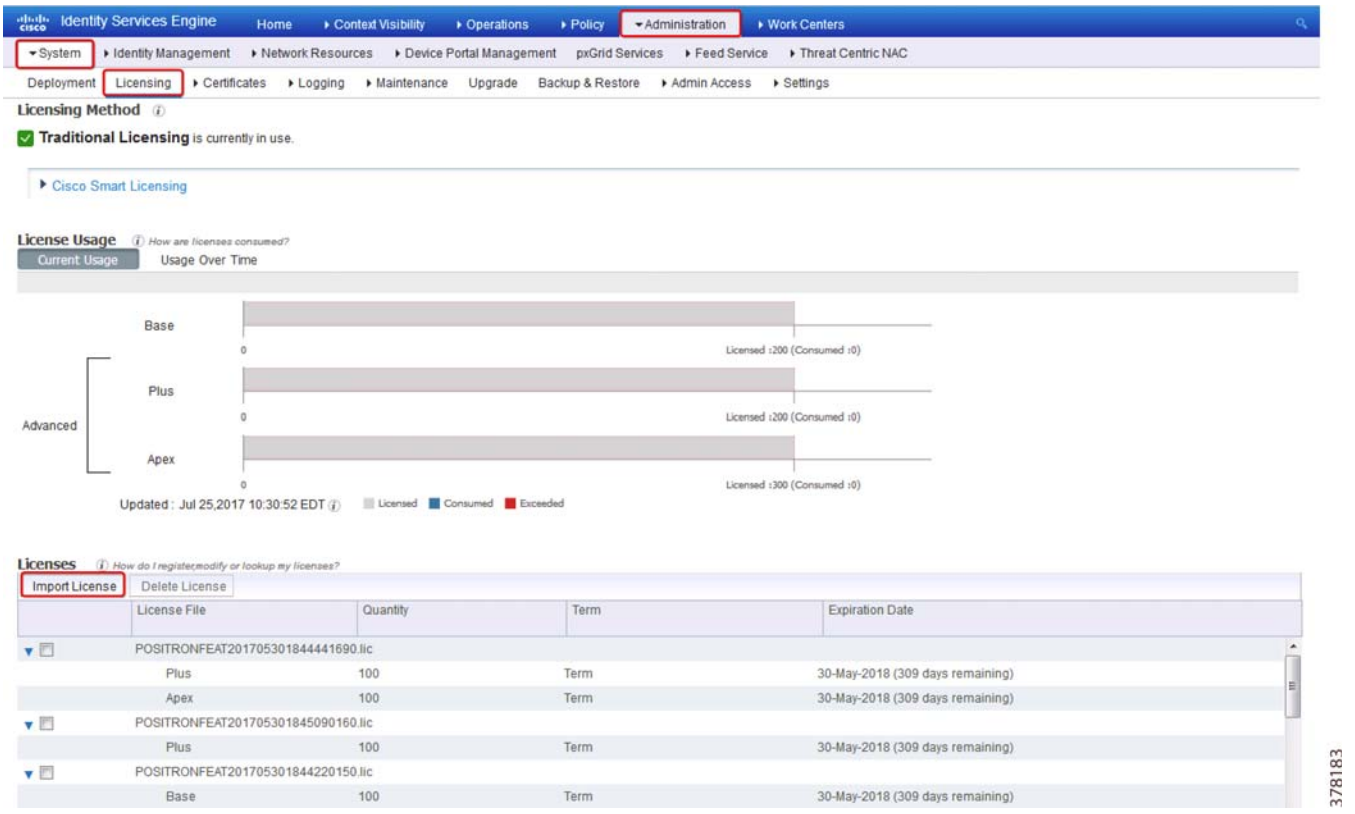
b. From **Administration** > **System** > **Licensing**, scroll to the **License Files** section.

c. Click **Import License**, browse for the license file, and then click **Import**.

d. Confirm that the new license is displayed in the **License Files** section (see Figure 3-4).

Step 2 When the distributed Cisco ISE deployment is completed, licenses on the primary PAN will be propagated to all nodes automatically.

Figure 3-4 Cisco ISE License Import Window



Cisco ISE Certificate Configuration

Before Cisco ISE nodes can be joined in a distributed system, necessary CA-signed certificates must be installed on each node as well as trusted root and subordinate CA certificates must be added to the trust store.

Step 1 Generate a certificate request and obtain the system certificate signed by the subordinate CA for each Cisco ISE node in the network:

a. From **Administration** > **System** > **Certificates**, choose **Certificate Signing Requests** in the left pane.

b. Click **Generate Certificate Signing Requests (CSR)**, fill in the required fields, and then click **Generate** (see Figure 3-5 and Figure 3-6). Use the node FQDN as a CN for the certificate subject.

c. Click **Export** in the window that appears to download the request and save it in an encoded form as a text file.

d. Using CA Web Enrollment service on the subordinate CA, connect to the web page for manual certificate enrollment via HTTPS. Enter the AD user credentials that allow you to perform the enrollment.

e. On the web page, select **Request a certificate** > **Advanced Certificate Request**, and click **Submit a certificate request** using base 64-encoded request.

f. Copy and paste the previously generated CSR, select the correct certificate template, and click **Submit**. Download the certificate chain and save with a .cer file extension.

Note The certificate template selected should be configured previously on the CA as part of the Certificate Services infrastructure configuration with Client and Server Authentication purpose.

Figure 3-5 Cisco ISE Certificate Signing Requests Page

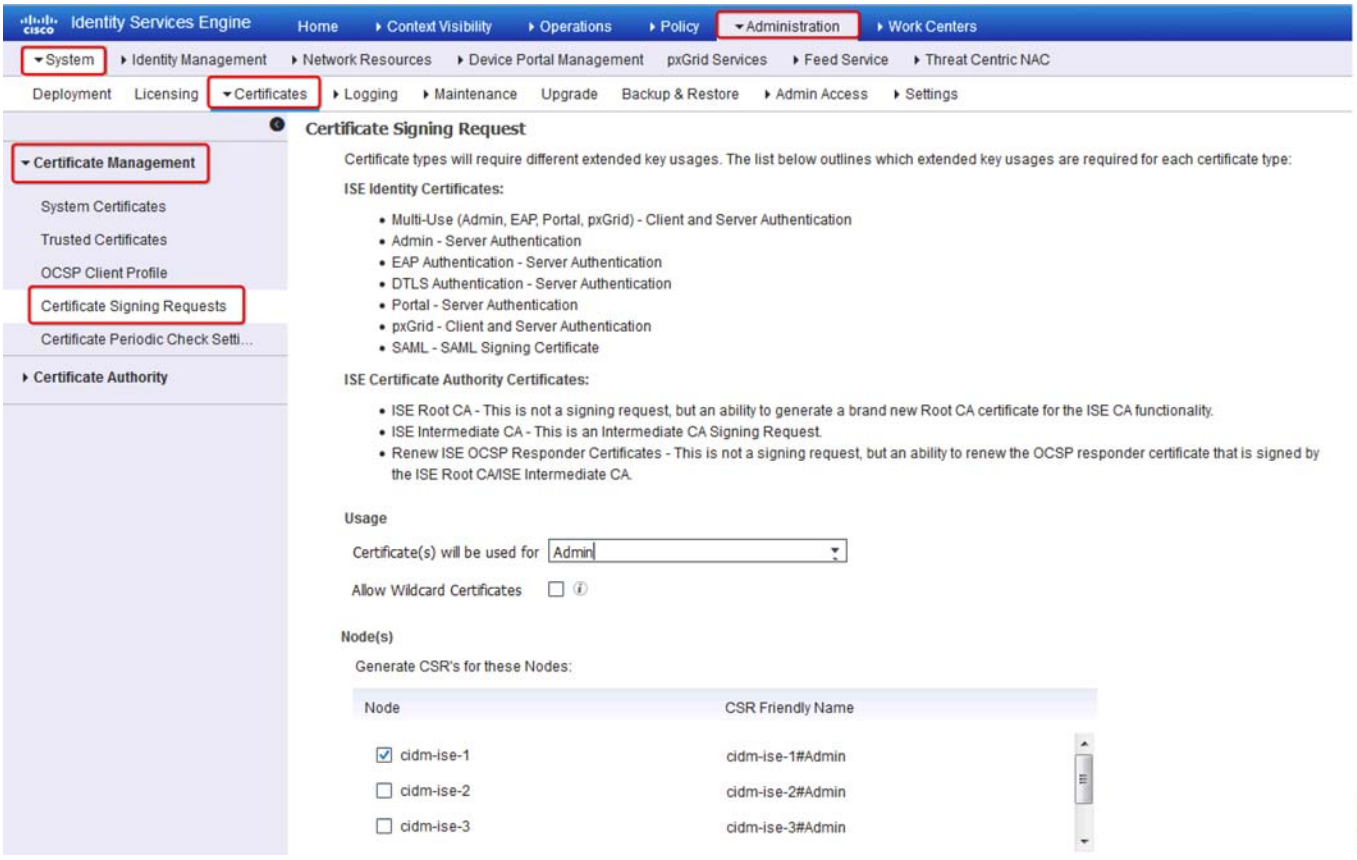
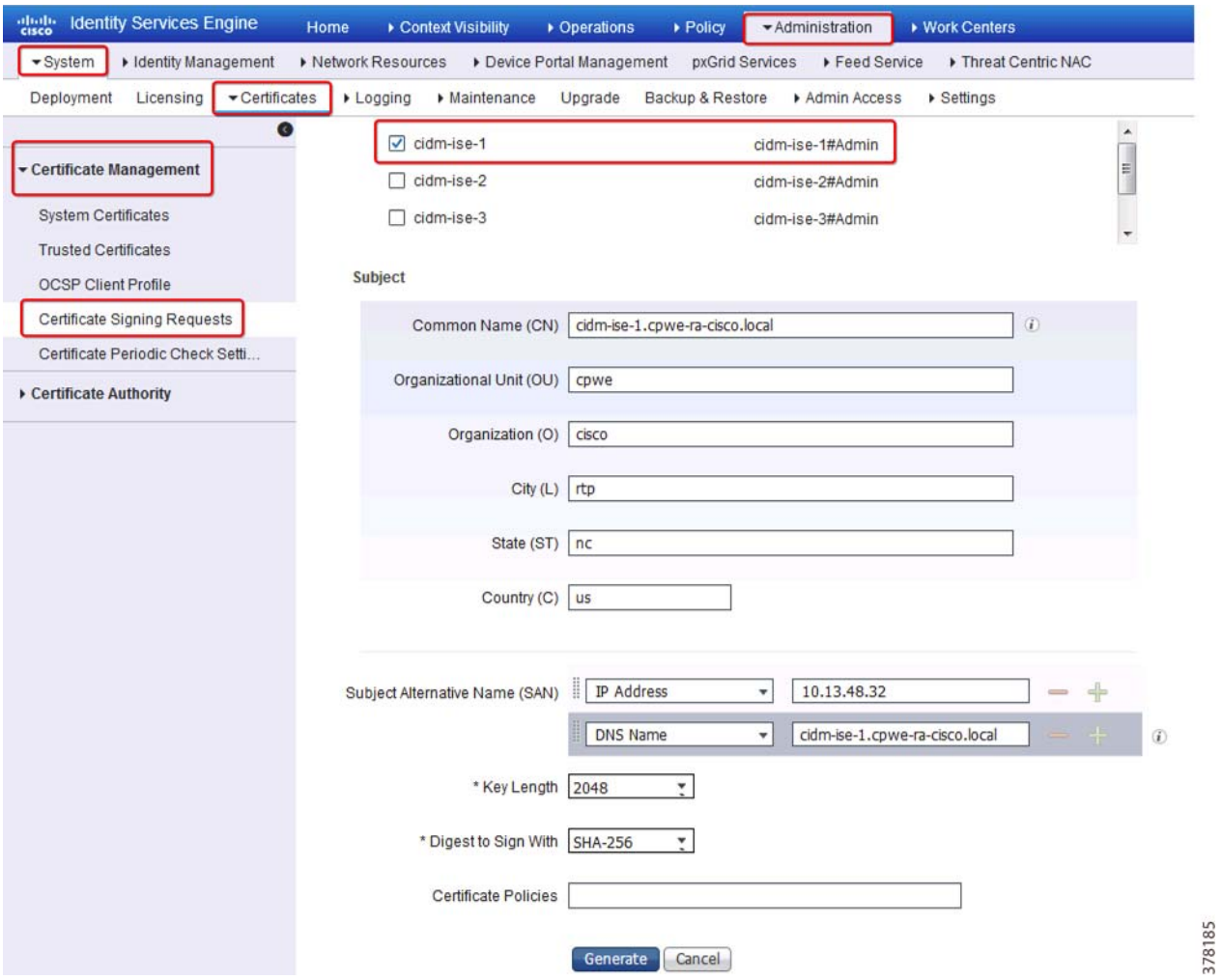


Figure 3-6 Example of a Cisco ISE CSR



Step 2 Install system certificates on every Cisco ISE node.

a. On the **Certificates** page, select the submitted CSR and then click **Bind Certificate** to append the CA-signed certificate.

b. Browse to the certificate file obtained from the CA, fill in the **Friendly Name** field, if desired, and then click **Submit**.

c. Once complete, click **System Certificates** in the left pane and verify that the new system certificate appears there. Select its check box and then click **Edit**.

d. Under **Usage**, check all boxes to allow this certificate to be used by all services. Click **Save**.

Note For disaster recovery, Cisco recommends exporting all system certificates and their private key pairs to a secure and reliable backup location

Step 3 Install trusted certificates for the Root CA, subordinated CA, MDM, and other trusted parties to the Trusted Certificate Store (Figure 3-8).

a. Obtain the CA certificate from the Active Directory store or using the CA Web Enrollment page.

b. Choose **Administration** > **System** > **Certificates** > **Trusted Certificates**. Click **Import**.

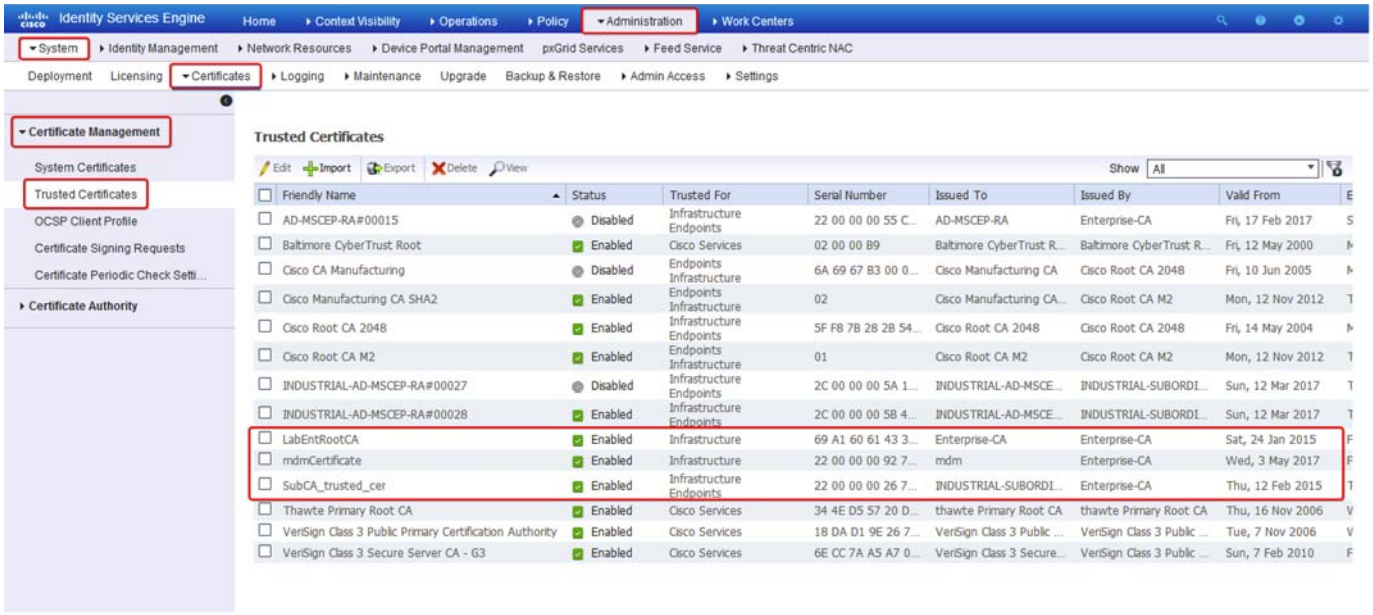
c. Browse to the saved certificate file and configure the **Friendly Name** if desired.

d. Select **Trust for authentication within ISE** checkbox to trust this CA certificate when validating the certificate chain for inter-node communication.

e. If planning to use the CA certificate in the certificate chain for EAP authentication, select the **Trust for client authentication and Syslog** checkbox.

f. Repeat the steps for the CAs higher in the PKI hierarchy up to the root CA.

Figure 3-7 Cisco ISE Trusted Certificates Page



Step 4 Verify that required DNS configuration is completed for each Cisco ISE node.

a. The domain name and DNS servers in the respective zone should be configured as part of the initial CLI setup or later with the following commands:

```
ip domain-name <DOMAIN NAME>
ip name-server <DNS SERVER IP ADDRESS>
```

b. Host records are created with forward and reverse resolution on the DNS servers. The FQDN should match the one in the system certificate subject.

Certificate Template Configuration on Cisco ISE

In the CPwE Identity and Mobility Services architecture, Cisco ISE is acting as a Simple Certificate Enrollment Protocol (SCEP) proxy server for issuing certificates for EAP authentication, thereby allowing mobile clients that are not part of the domain to obtain their digital certificates from the CA.

The internal CA functionality in the Cisco ISE combined with the initial registration process greatly simplifies the provisioning of digital certificates on endpoints.

Step 5 Configure SCEP profile and Certificate Template for EAP Authentication.

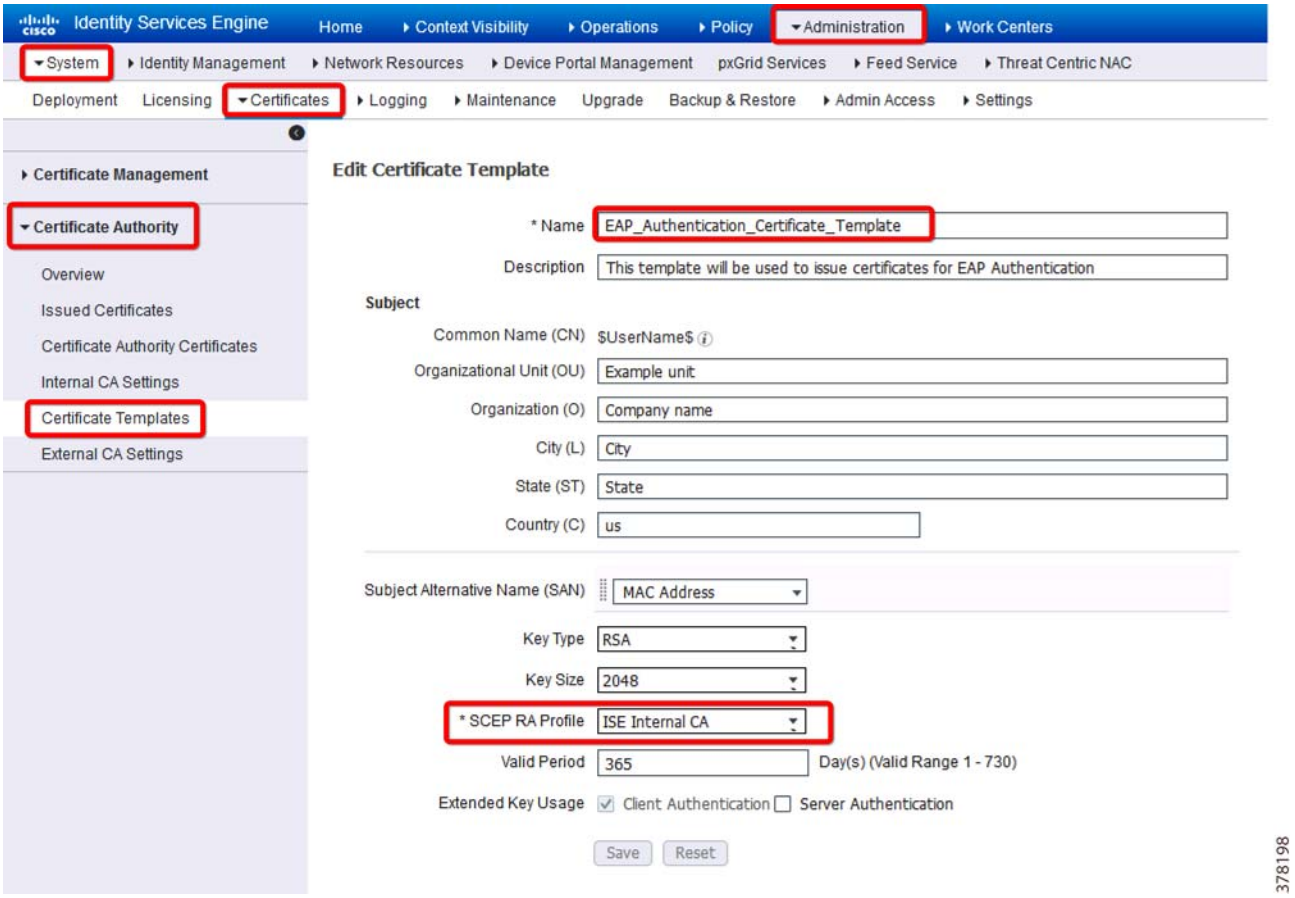
a. From **Administration** > **System** > **Certificates** > **Certificate Authority** > **Internal CA Settings**, verify that the internal CA is enabled.

b. On the **Certificate Template** page, edit the default **EAP Authentication** template and fill the necessary information.

c. The SCEP Profile is set to the ISE Internal CA by default.

Note It is also possible to use an external SCEP server to distribute certificates to mobile clients, for example a subordinate CA in the Industrial Zone. This configuration has not been validated for the CPwE architecture.

Figure 3-8 Certificate Template for EAP Authentication



Distributed Setup Configuration

As discussed in Chapter 2, “CPwE Identity and Mobility Services Design Considerations,” the Cisco ISE distributed setup supports centralized configuration and management. The distributed setup consists of three types of nodes, as described in Table 3-2.

Table 3-2 Cisco ISE Distributed Setup Node Types

Type of Node	Admin Node (PAN)	Policy Node (PSN)	Monitoring Node (MnT)
Location in CPwE	Enterprise Zone	Enterprise Zone Industrial Zone	Enterprise Zone
Feature	All system-related configuration, including authentication and authorization profiles	Evaluates the policies and makes all the decisions	Log collector and store log messages

Note This section provides general steps to configure Cisco ISE nodes in the distributed system. For complete information, please refer to the following URL: https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_010.html

Step 1 Configure a Cisco ISE node with a primary PAN role.

a. On the intended primary PAN, from **Administration** > **System** > **Deployment**, click the node name in the table.

b. Under **Personas** and next to **Administration**, change the role from **STANDALONE** to **PRIMARY** and then click **Save**.

c. Wait for Cisco ISE services to restart, then return to the Deployment page and confirm the primary PAN role.

d. Make sure that all other ISE nodes are in the Standalone mode, reachable using their FQDN, and have all necessary certificates added.

Step 2 Add the secondary PAN to the deployment.

a. From **Administration** > **System** > **Deployment** on the Primary PAN, click **Register ISE Node**.

b. Enter FQDN and admin credentials for the node that is going to be the secondary PAN.

c. After the node is joined and completes the reboot, confirm the status on the Deployment page.

Step 3 Configure monitoring roles on the Primary and Secondary PANs.

a. Click on the Primary PAN name on the Deployment page and configure **Monitoring** role as **SECONDARY**. Remove the **Policy Service** role from the PAN and click **Save**.

b. Click on the Secondary PAN name on the Deployment page and configure **Monitoring** role as **PRIMARY**. Remove the **Policy Service** role from the PAN and click **Save**.

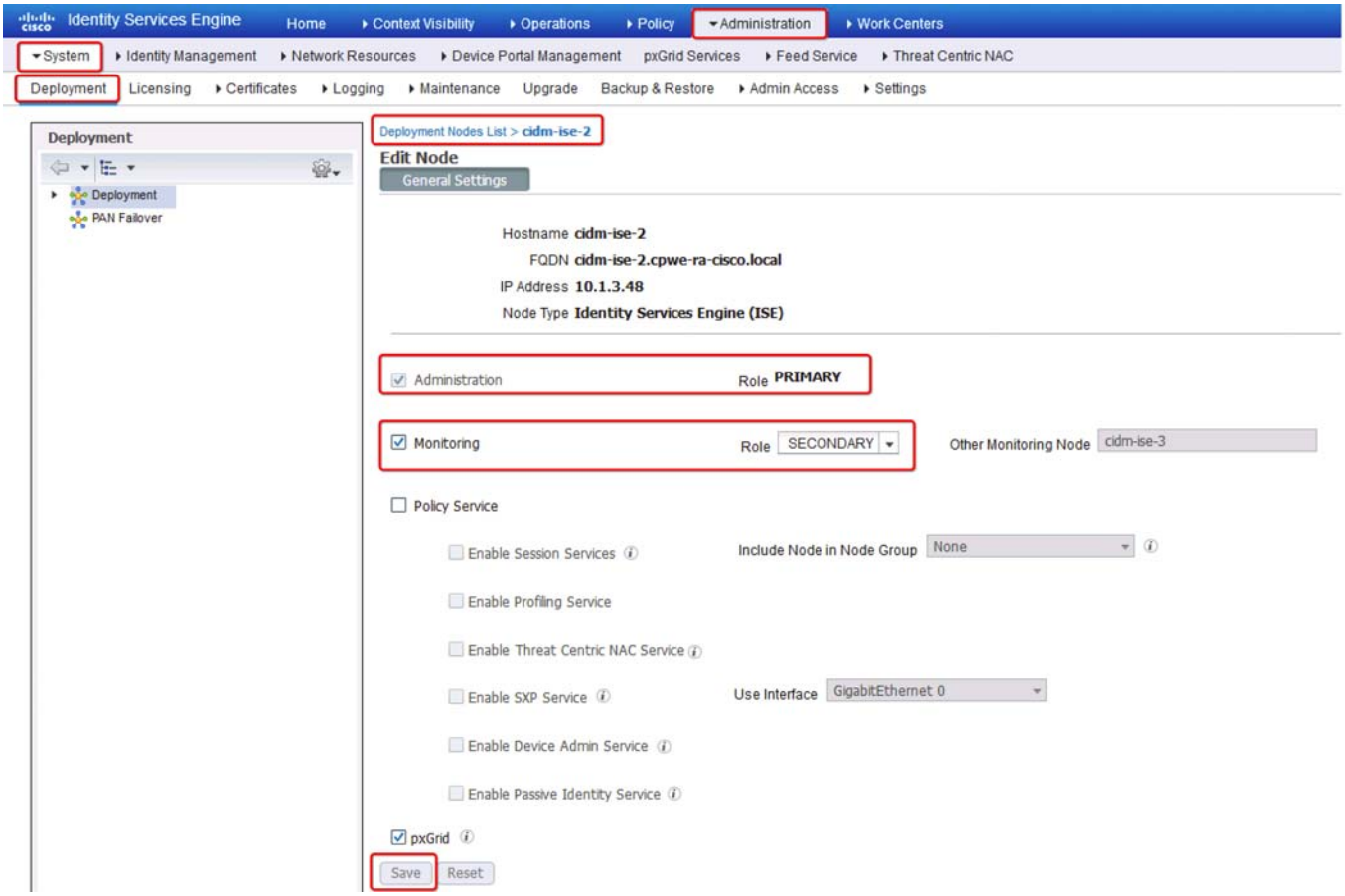
Step 4 Add PSNs to the deployment.

a. Register available Cisco ISE nodes and configure **Policy Service** role. Enable appropriate services such as Session, Profiling, and Device Admin.

b. If applicable, place multiple PSNs in each zone in a node group for load balancing and failover purposes.

Figure 3-9 Cisco ISE Deployment Page

Figure 3-10 Cisco Primary PAN Settings



Note Once the distributed setup has been created, all configurations are performed on the primary PAN which synchronizes changes with the other nodes. The GUI for the other Cisco ISE nodes will have only limited configuration options available such as diagnostic logs and system certificate management.

Identity Source Configuration

The following sections describe the configuration of the AD as the user identity source and certificate authentication profiles for EAP-TLS authentication.

External Identity Source (AD) Configuration

The following steps describe the configuration of AD as an external identity source for Cisco ISE:

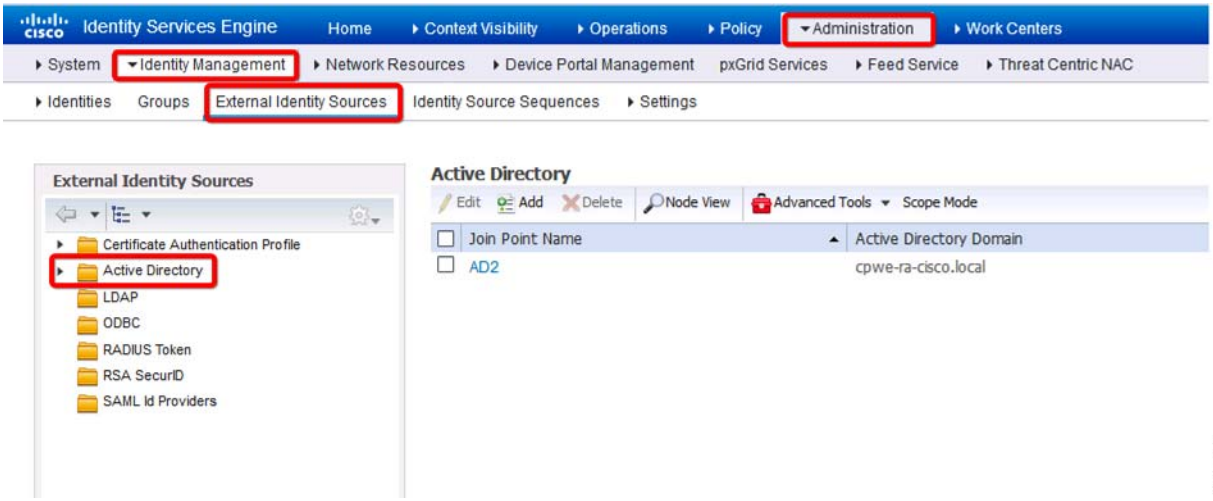
Step 1 Create the AD join point:

a. From **Administration > Identity Management > External Identity Sources**, click **Active Directory** in the left pane.

b. Click **Add** and then type the desired **Join Point Name** and the **Active Directory Domain** to join.

c. Once finished, click **Submit**.

Figure 3-11 AD Join Point

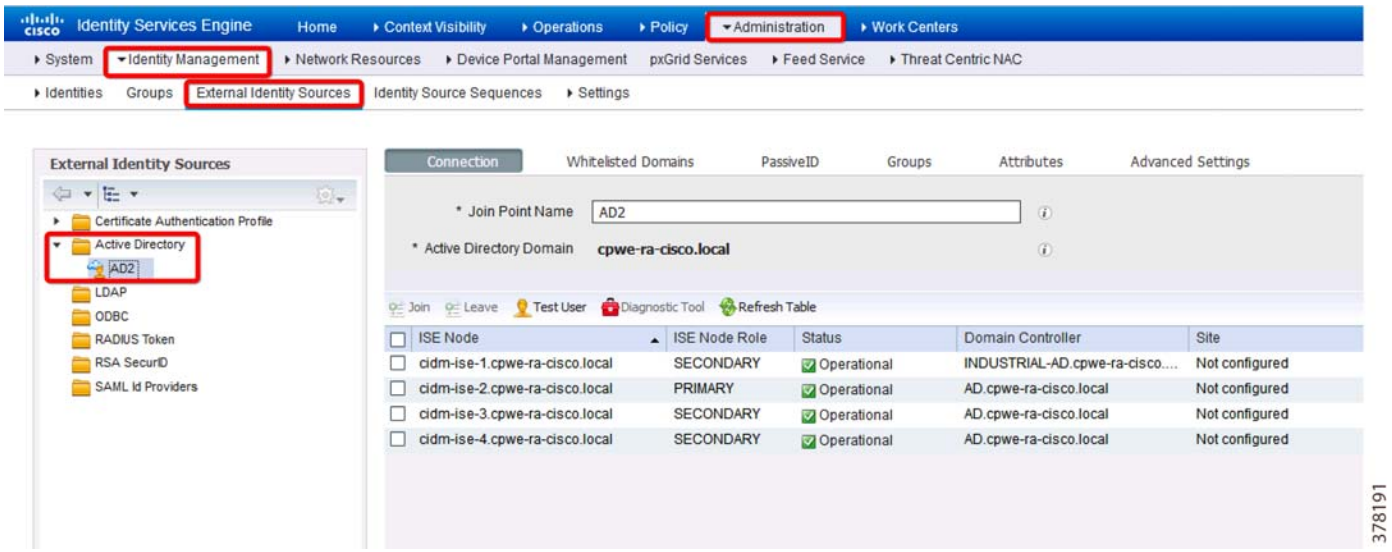


Step 2 Join the AD domain using the join point:

a. Click on the Join Point name in the left pane. All distributed Cisco ISE nodes should be listed and show a status of “Not Joined.” Select each node’s check box and then click **Join**.

b. Specify a **User Name** and **Password** with permissions to join the domain and then click **OK**. If the operation succeeds, the node will show a status of “Operational” and the host name of the local AD server.

Figure 3-12 Cisco ISE Node Status in AD



Step 3 Retrieve all necessary groups from the AD server (as configured in Active Directory Configuration):

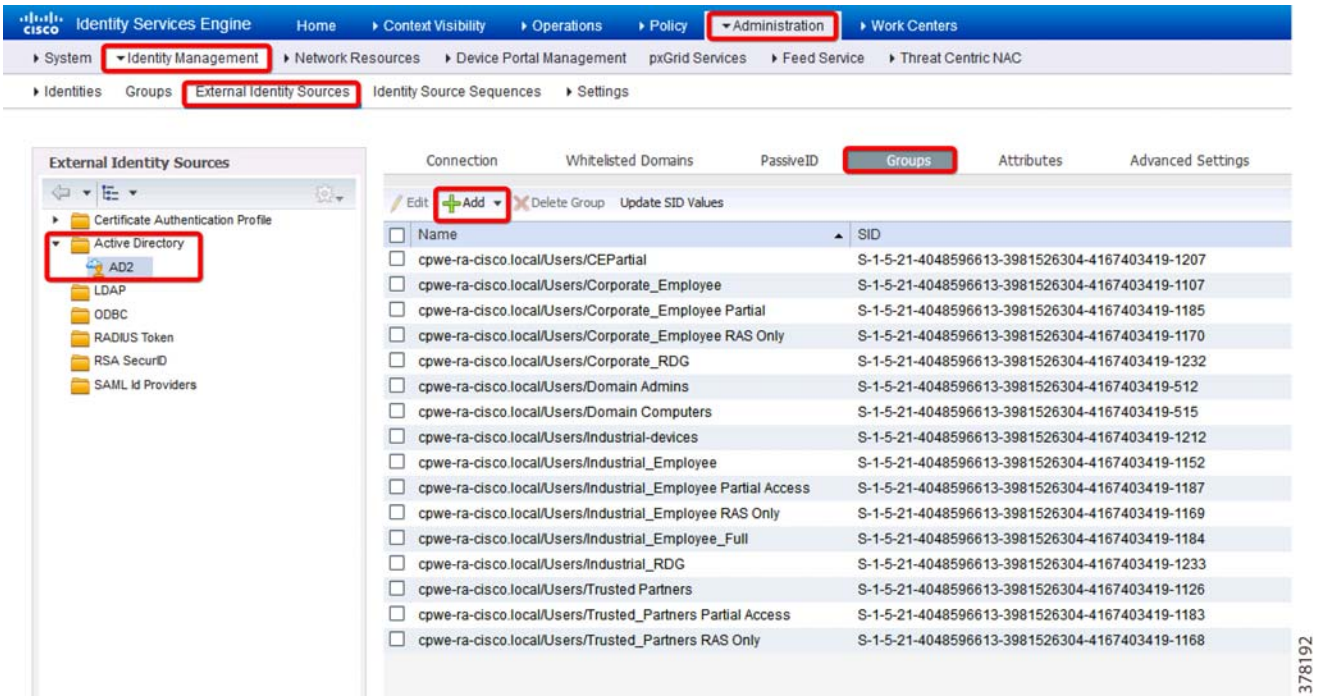
a. From the **Active Directory Join Point** page, click the **Groups** tab.

b. From **Add > Select Groups from Directory**, click **Retrieve Groups.**

c. Select the check boxes for any groups that will be referenced in client policies and then click **OK**.

d. Verify that the groups are now listed in the table and then click **Save**.

Figure 3-13 AD Groups Example



Certificate Authentication Profile Configuration

To use certificates for authenticating endpoints that connect to the network, a certificate authentication profile should be defined in Cisco ISE. The profile includes the certificate field that should be used as the principal user name.

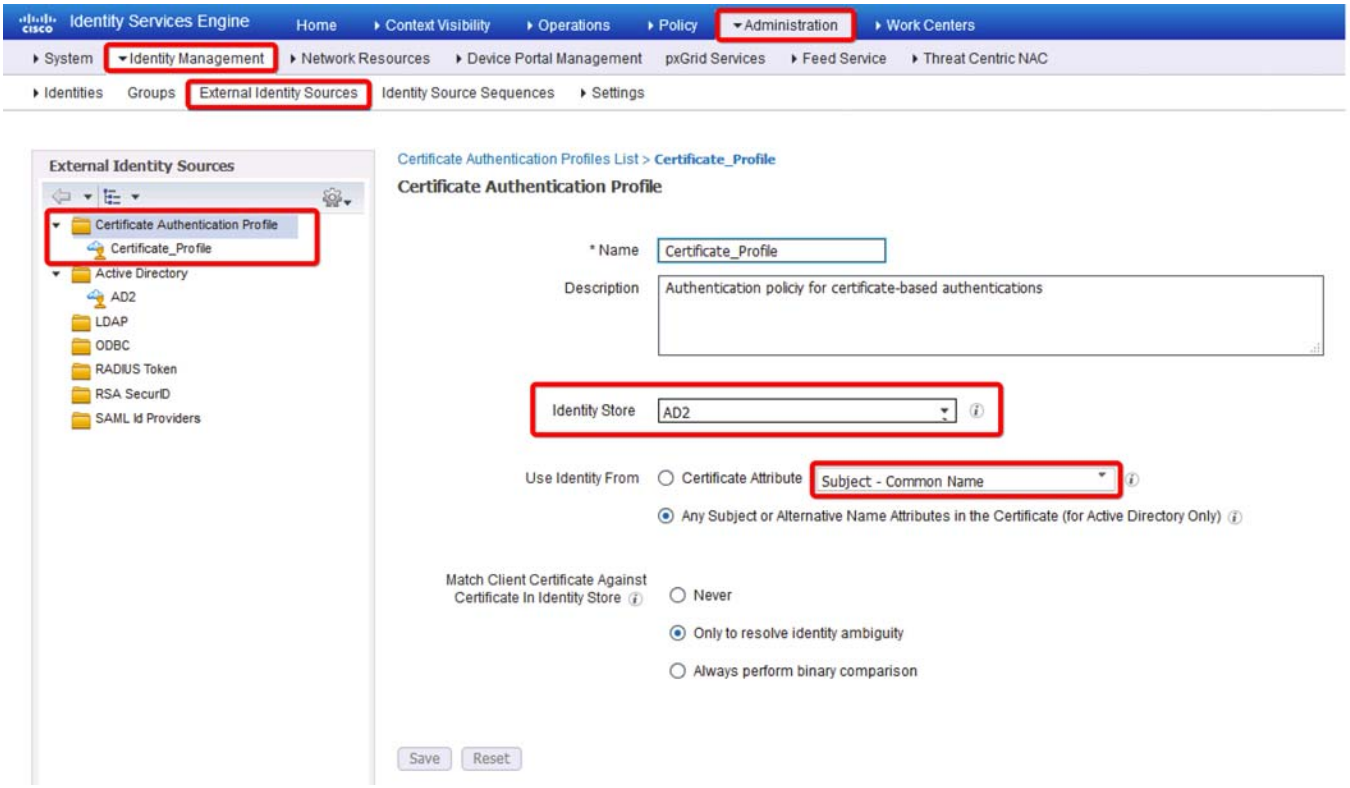
Step 4 Create a certificate authentication profile.

a. From **Administration** > **Identity Management** > **External Identity Sources**, click **Certificate Authentication Profile** in the left pane and then click **Add**.

b. Fill in the **Name** field with any desired name. Select the AD join point from the **Identity Store** drop-down.

c. Select **Any Subject or Alternative Name Attributes in the Certificate** (for Active Directory Only) and click **Submit**.

Figure 3-14 Certificate Authentication Profile



Identity Store Sequence Configuration

After the certificate authentication profile is created, it can be used in the identity source sequence so that Cisco ISE can obtain the attribute from the certificate and match it against the defined identity sources (e.g., AD).

Step 5 Create the identity store sequence.

a. From **Administration** > **Identity Management** > **Identity Source Sequences**, click **Add**.

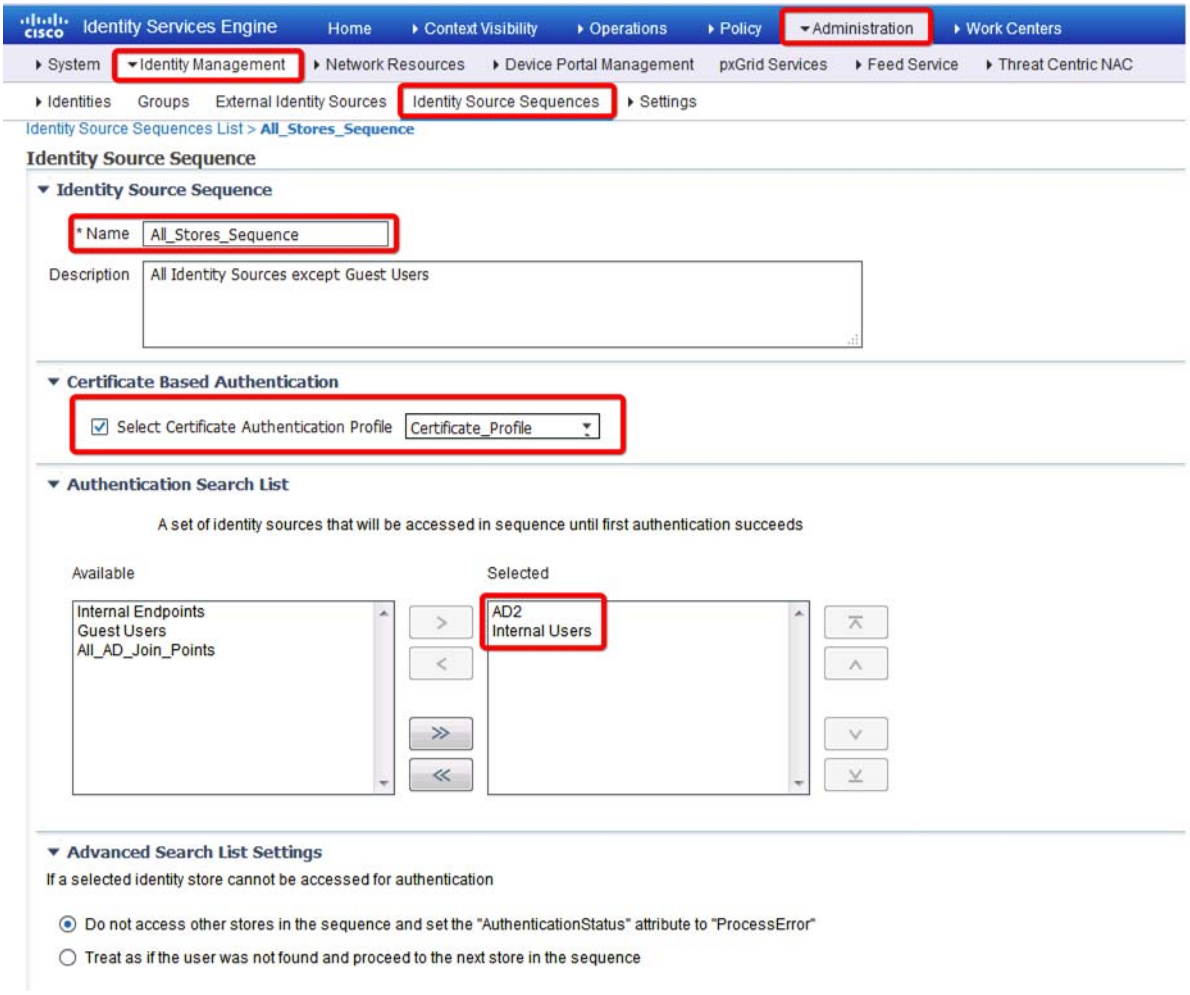
b. Fill in the **Name** field. Select the check box next to **Certificate Based Authentication** and then select the certificate profile created in the previous step.

c. Under **Authentication Search List**, move the AD join point to the list on the right.

d. Under **Advanced Search List Settings**, select **Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"** and click **Save**.

Note If the AD store cannot be accessed for any reason, the authentication status will be Process Error. The default behavior in this case is not to send a response and drop the request.

Figure 3-15 Identity Store Sequence



Whitelist Configuration

The following steps describe the configuration of the Whitelist for approved corporate-issued devices:

Step 1 Create an Endpoint Identity Group for the Whitelist.

a. From **Administration** > **Identity Management** > **Groups** > **Endpoint Identity groups**, click **Add**.

b. Configure the group name and click **Submit**.

Note Cisco ISE also comes with several system-defined endpoint identity groups, for example for blacklisted devices, self-registered devices, and groups based on the device type profiles.

Step 2 Add a corporate device manually to the Whitelist:

a. From **Context Visibility** > **Endpoints**, click **+** (plus sign) to add a new endpoint.

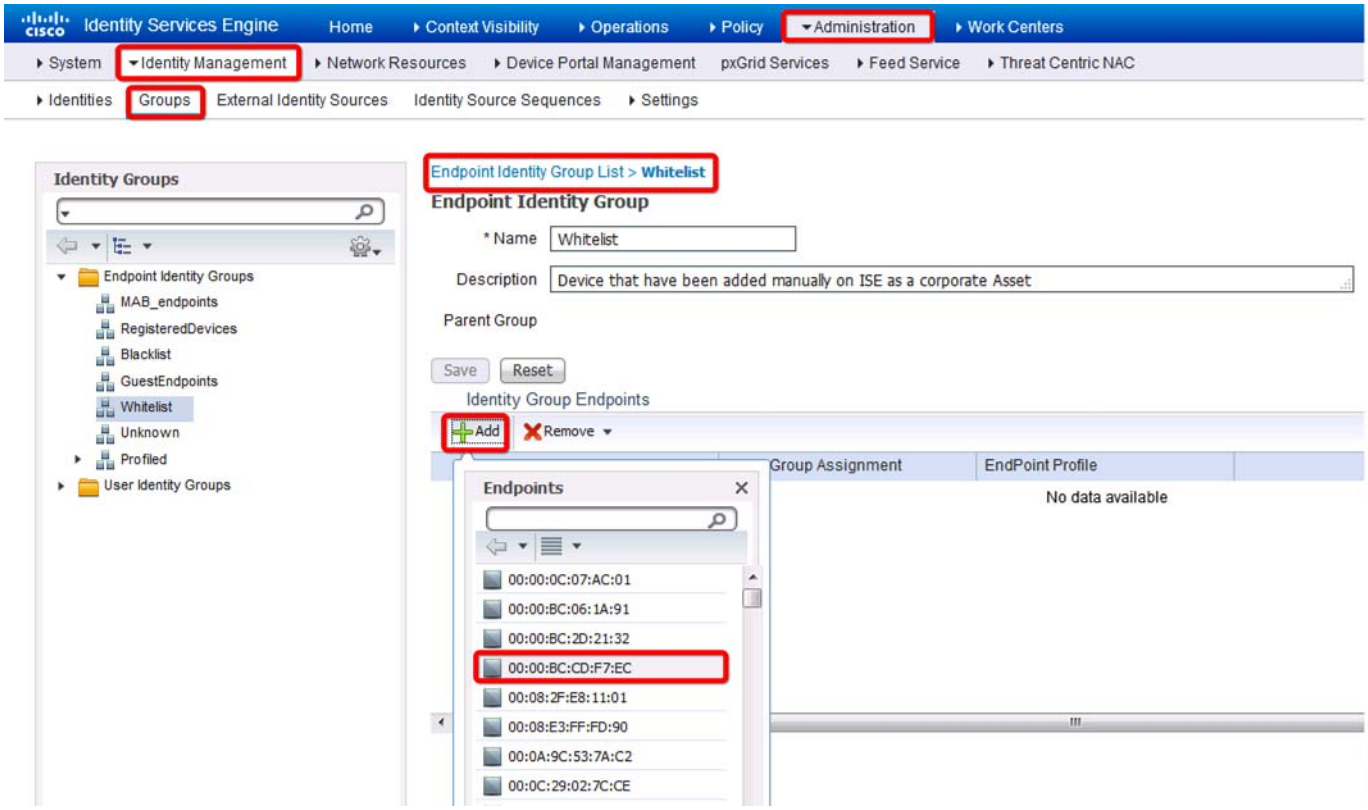
b. Configure the MAC address of the device in the **MAC Address** field.

c. Select the **Static Group Assignment** checkbox, select the previously configured Whitelist group name, and click **Save**.

d. Large number of endpoints can also be imported as a list in CSV format.

Step 3 Endpoints can also be added to the whitelist group from the **Endpoint Identity Groups** page if they have been previously identified by the PSN or imported manually.

Figure 3-16 Adding Endpoints—Identity Groups Page



Network Device Configuration

This section describes how to define network devices (such as a switch, a WLC, or a router) from which RADIUS service requests are sent to the Cisco ISE PSN. You must define network devices and configure mutual authentication before Cisco ISE can interact with them.

Note For complete information on managing network devices with Cisco ISE, refer to: https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_01000.html

Step 1 From **Administration > Network Resources > Network Device Groups**, create network device groups to organize network devices by type and location, if desired.

Step 2 Add any network devices that will send RADIUS requests to Cisco ISE on behalf of clients:

a. From **Administration > Network Resources > Network Devices**, click **Add**.

b. Fill in the hostname and IP address of the device.

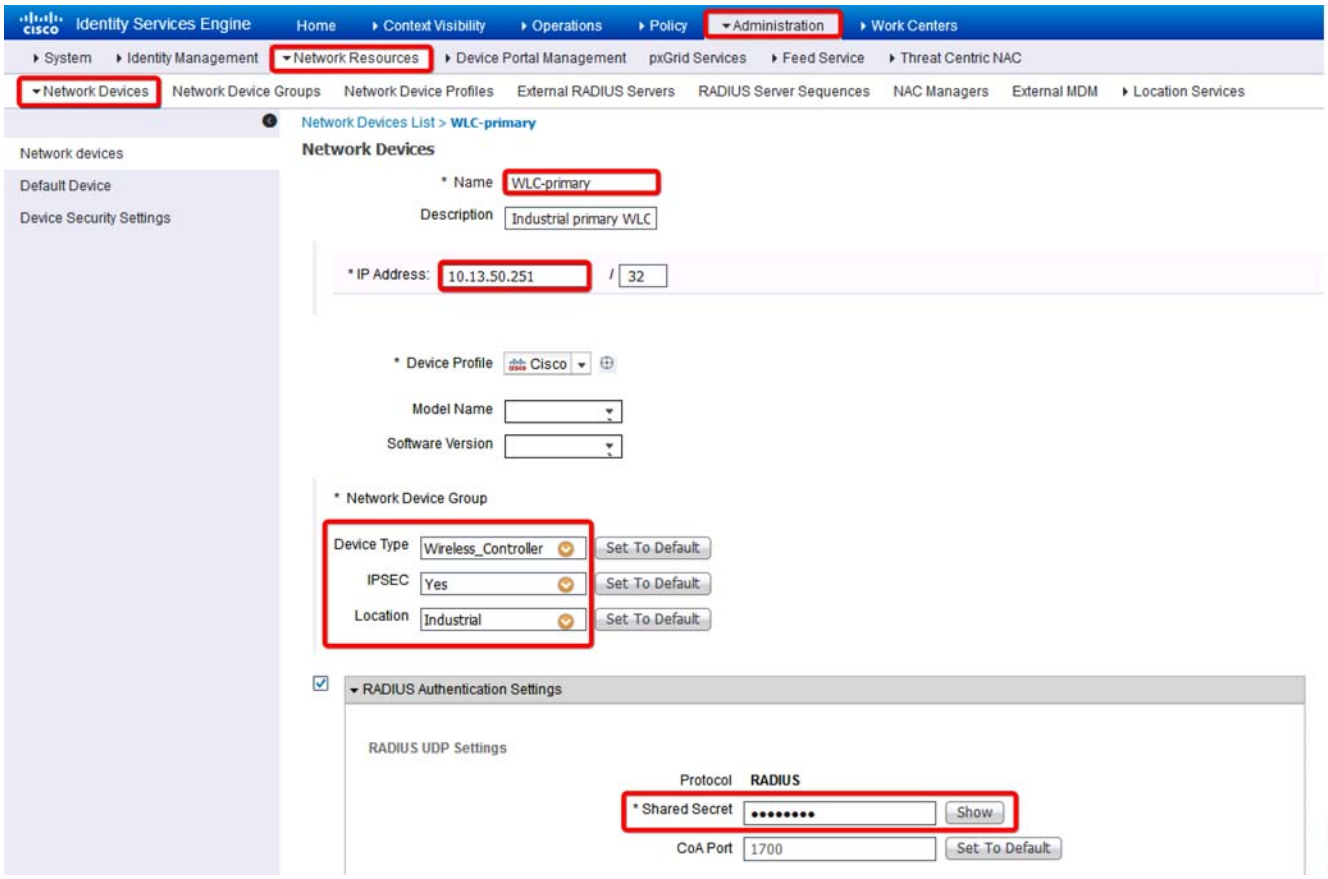
c. Under **Network Device Group**, select either the default location and device type or any specific groups created earlier.

d. Select the check box next to **RADIUS Authentication Settings** and expand it and then enter the shared secret RADIUS password. This password must match the configuration of the network device itself or RADIUS exchanges will fail.

e. If the network device will use IPsec for RADIUS communication, add it to the **IPsec** group. Click **Save**.

f. Network devices can also be imported as a CSV file.

Figure 3-17 Adding Network Device



Step 3 Configure IPsec services on the Cisco ISE using steps described at the following URL: http://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-22/210519-Configure-ISE-2-2-IPSEC-to-Secure-NAD-I.html

Cisco ISE uses Embedded Services Router (ESR) software to create a VPN tunnel.

Wireless Access Configuration

This section describes configuration details for the Cisco ISE, Cisco WLC, and Stratix 5100 as an autonomous AP based on the design recommendations in Chapter 2, “CPwE Identity and Mobility Services Design Considerations.”

The following configuration steps are covered in this section:

- Cisco ISE Configuration
- Industrial WLC Configuration
- Guest Anchor WLC Configuration
- Enterprise Anchor WLC Configuration
- Flex Connect Architecture Configuration
- Autonomous WLAN Configuration

Cisco ISE Configuration for Wireless Access

This section describes how to configure Cisco ISE to properly authenticate and authorize wireless clients and provide the appropriate level of access to the network. The following configuration steps are covered in this section:

- Device Portal Configuration
- Mobile Device Provisioning
- Mobile Device Profiling
- MDM Server Integration
- MSE Integration for Location Based Services
- Policy Element Configuration
- Authentication Policy Configuration
- Authorization Policy Configuration

Device Portal Configuration

Cisco ISE provides default web-based portals for employees to register their personal devices using the various non-guest portals such as the BYOD and MDM. These portals can be customized based on the company's standards and policies.

With multiple Policy Service nodes (PSNs) in a deployment that can service a web portal request, Cisco ISE needs a unique identifier for the portal HTTPS certificate. When you add or import certificates that are designated for portal use, you must define a certificate group tag and associate it with the corresponding certificate on each PSN in your deployment. You must associate this certificate group tag to the corresponding end-user portals (guest, sponsor, and BYOD portals). You can designate one certificate from each node for each of the portals.

Note For complete information on configuring web portals on Cisco ISE, refer to: https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_010000.html

Step 1 Configure the BYOD portal:

a. From **Administration** > **Device Portal Management** > **BYOD**, select the default BYOD Portal.

b. Select **Registered Devices** as the Endpoint Identity group.

c. Select the certificate group tag that points to the PSN certificate to be used to secure HTTPS communication. The tag is defined when adding a systems certificate designated for the portal use.

d. Customize other web page settings if needed. The right side of the window illustrates the BYOD portal flow.

Figure 3-18 BYOD Portal Page

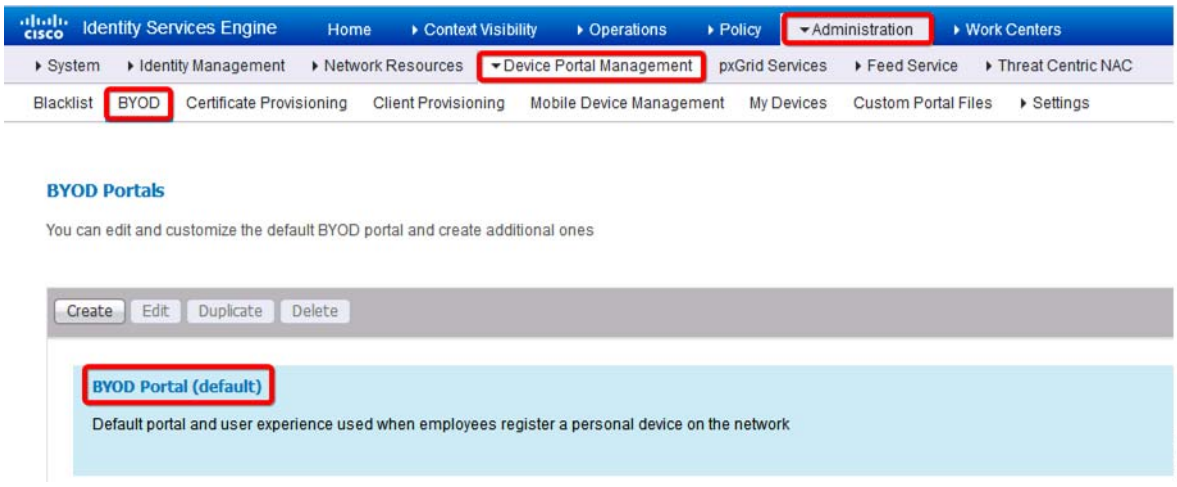
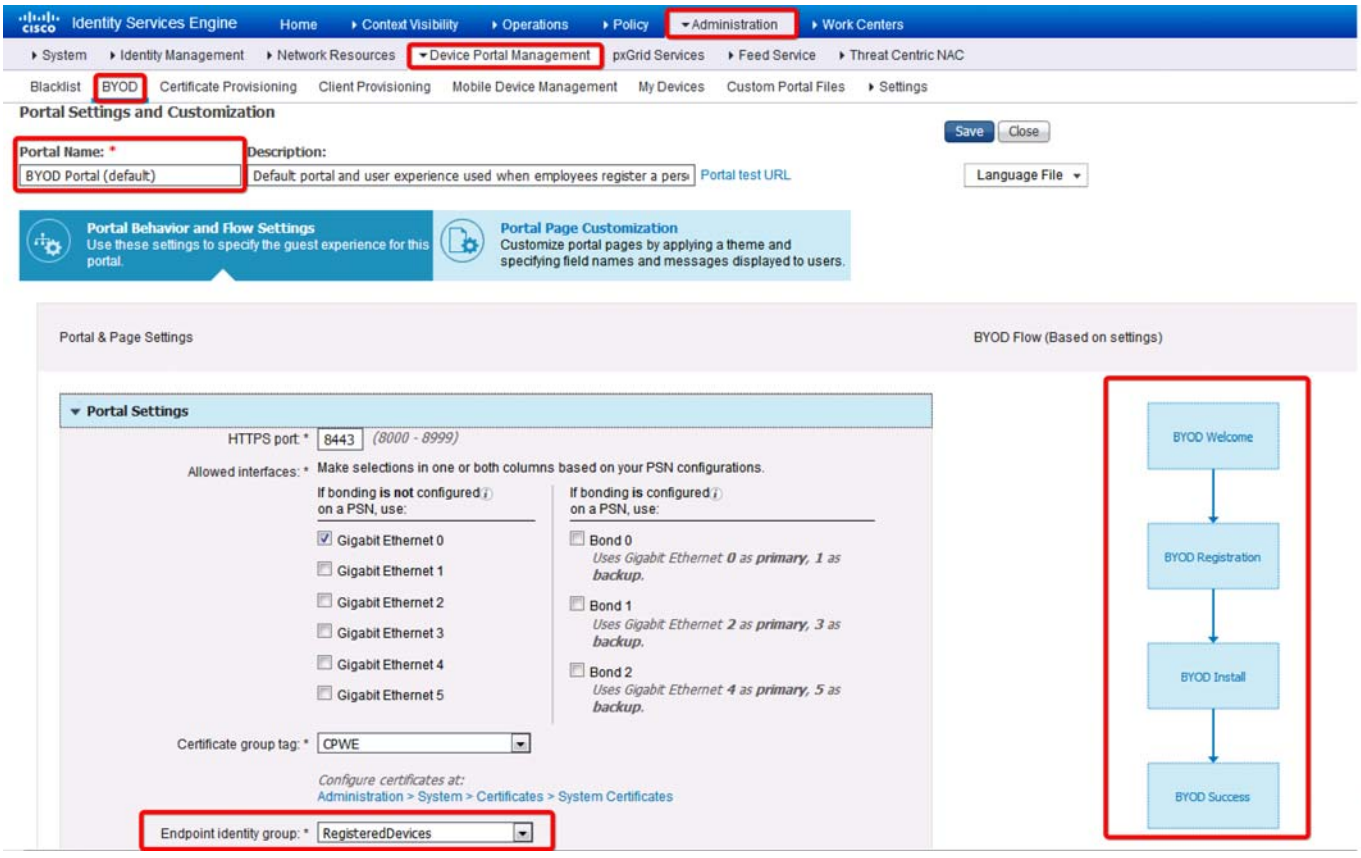


Figure 3-19 BYOD Portal Settings and Flow



Step 2 Configure the MDM Portal:

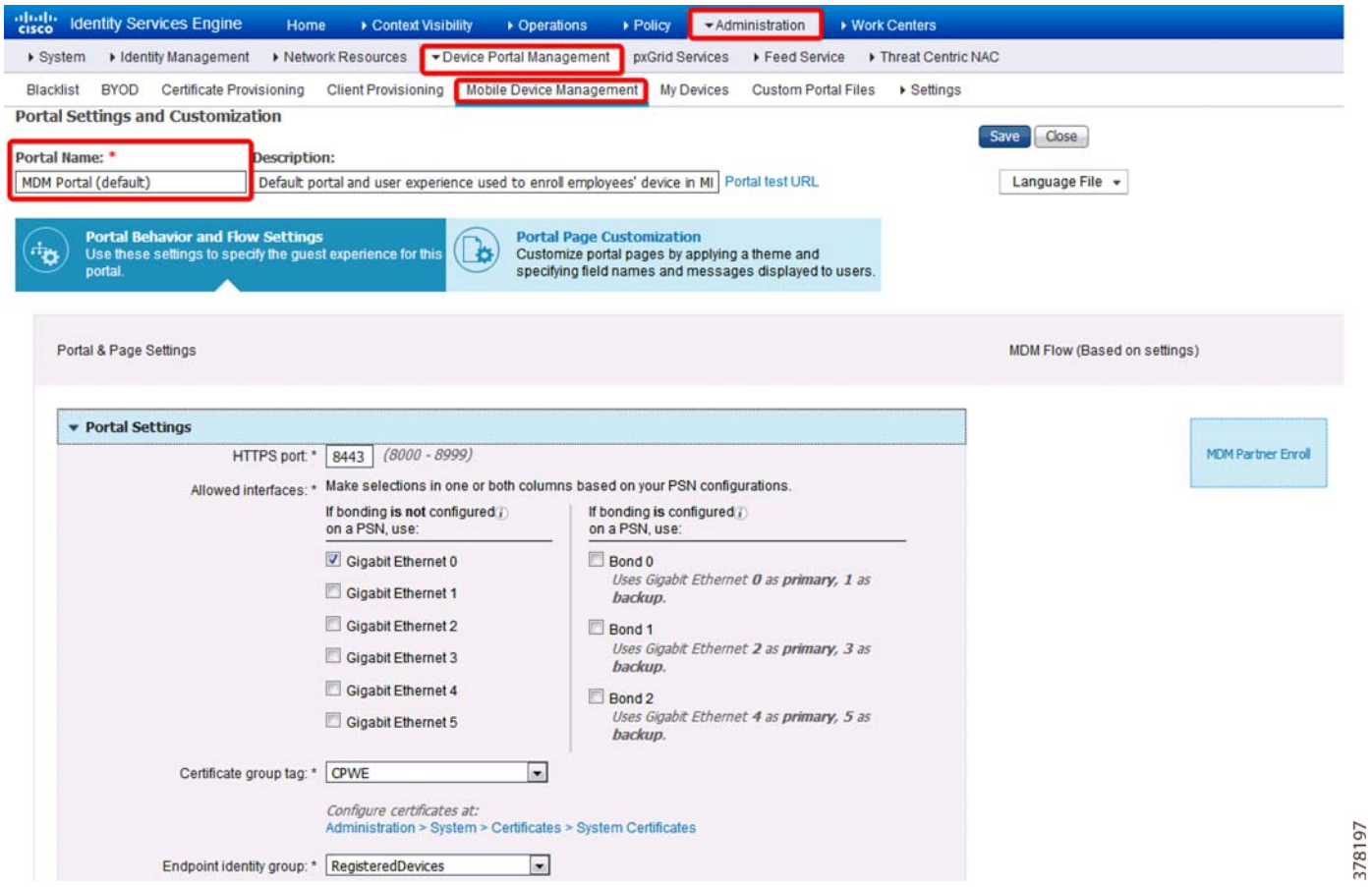
a. From **Administration** > **Device Portal Management** > **Mobile Device Management**, select the default MDM Portal.

b. Select **Registered Devices** as the Endpoint Identity group.

c. Select the certificate group tag to use for the portal.

d. Customize other web page settings if needed.

Figure 3-20 MDM Portal Settings



Mobile Device Provisioning

This section explains the mobile client provisioning process, interaction between the endpoints and the BYOD Registration portal, and the steps required to enroll the digital certificate and configuration profile.

Client Provisioning

Cisco ISE looks at various elements when classifying the type of login session through which users access the network, including the client's device OS and version, browser type and version, and others. Once Cisco ISE classifies the client device, it uses client provisioning resource policies to help confirm that the client is set up with an appropriate agent version, up-to-date compliance modules, and correct agent customization packages and profiles, if necessary.

The following are considerations for client provisioning on the endpoints:

- Based on the endpoint, Cisco ISE pushes an appropriate Software Provisioning Wizard (SPW) to the device. This wizard configures the 802.1X settings on the endpoint and configures the endpoint to obtain a digital certificate.

- In certain endpoints such as iOS devices, there is no need for a SPW package because for iOS devices the native operating system is used to configure the 802.1X settings.
- For Android devices, the SPW package needs to be downloaded from Google Play Store during the provisioning process.
- The other SPW packages are developed by Cisco and they can be downloaded from within the Cisco ISE web interface or from the Cisco website.

The configuration steps to configure mobile client provisioning are described below.

Step 1 Define the Native Supplicant Profile for mobile devices based on the platform and type of access:

a. From **Policy Elements** > **Results** > **Client Provisioning** > **Resources**, click **Add**.

b. Assign a name and specify the device OS (or select **all**).

c. In the **Wireless Profile**, click **Add**. Configure the SSID name that will be provisioned to the device.

d. Specify other wireless profile parameters such as security, certificate template, and platform-specific settings.

e. Multiple wireless profiles with separate SSIDs can be configured and the first profile will be the active profile.

Figure 3-21 Client Provisioning Resources Page

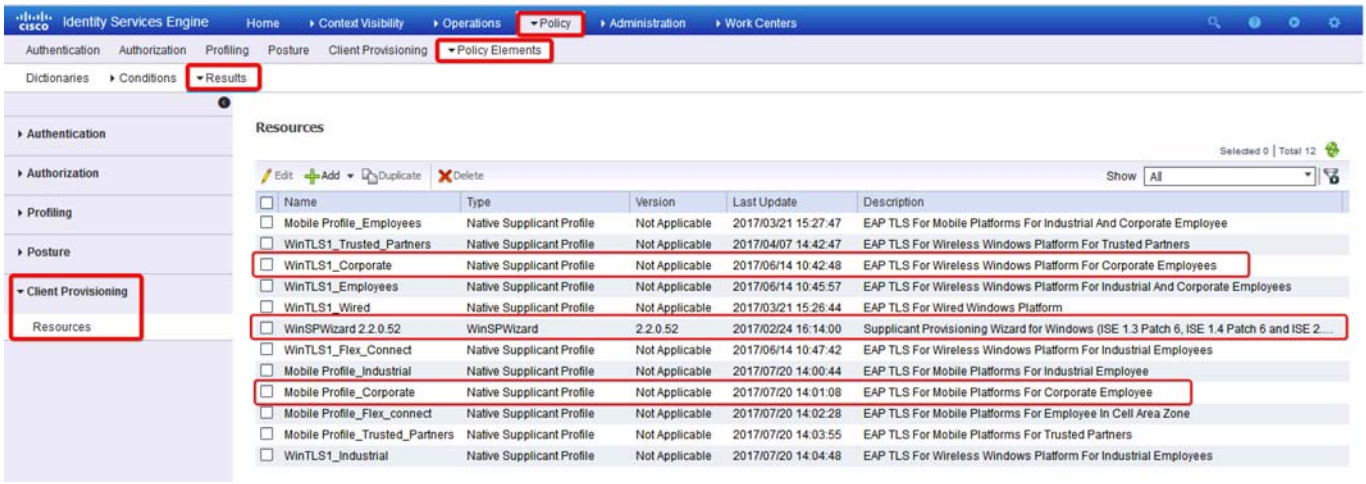
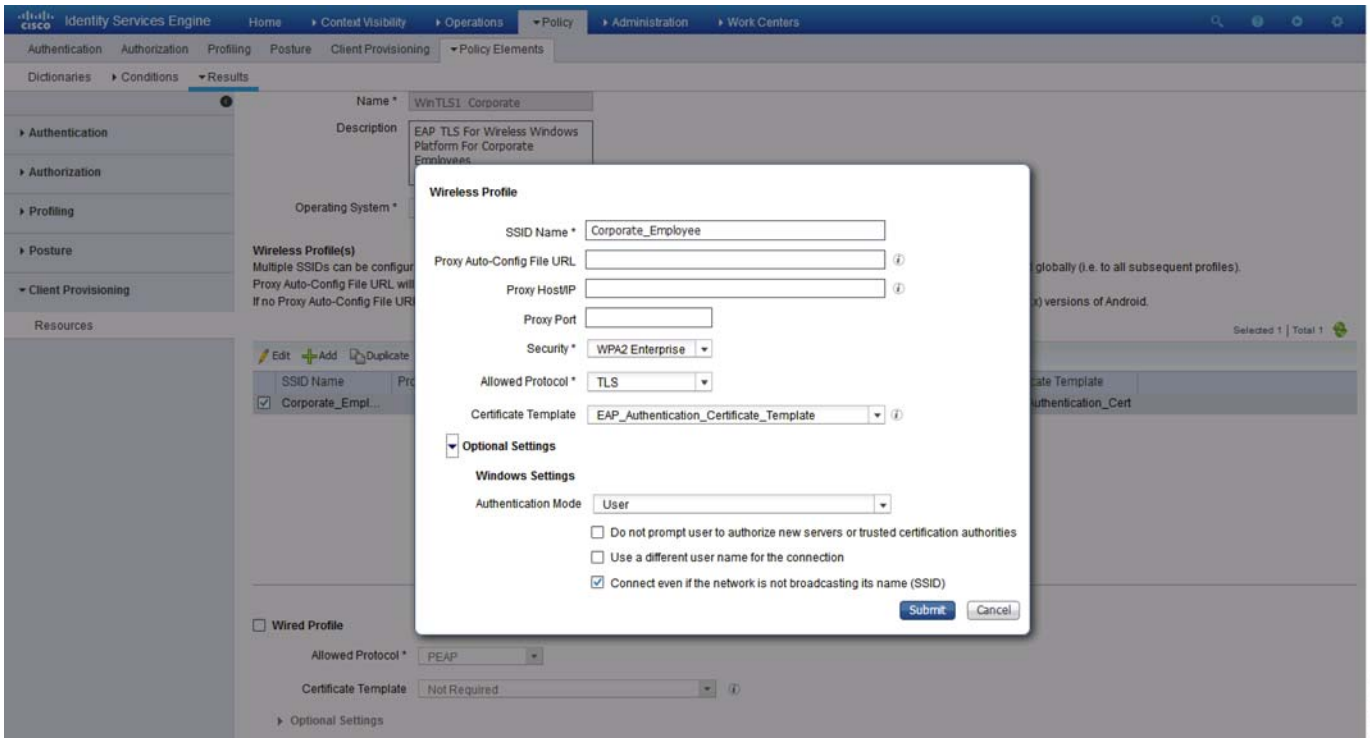


Figure 3-22 Wireless Profile for Native Supplicant



Step 2 Configure Client Provisioning Policies to determine which users receive which version of the provisioning resources.

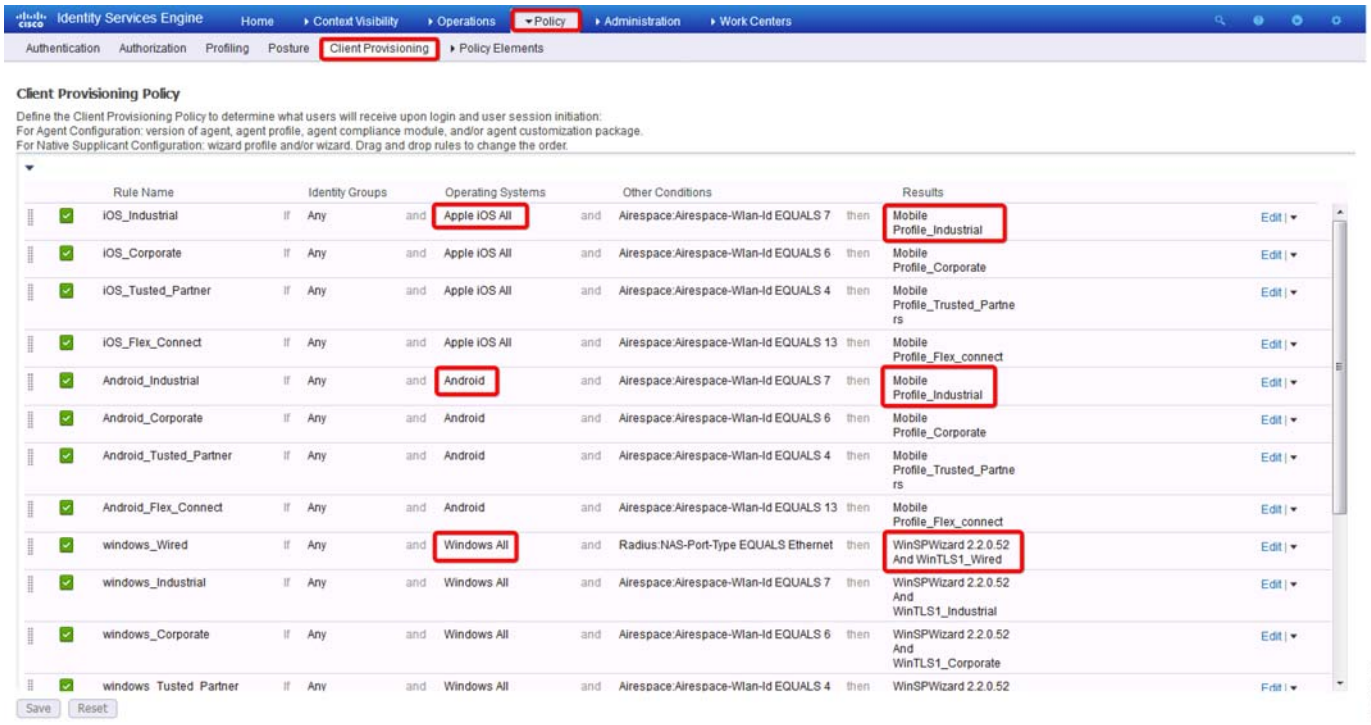
a. From **Policy** > **Client Provisioning**, add or edit existing policies.

b. Specify the rule name and conditions such as AD group, OS, and SSID.

c. Specify the resulting profile to be applied from the list configured in step 1.

In the example below, different provisioning policies are configured based on the OS and the WLAN ID number defined in the Cisco WLC. The WLAN parameter is passed to the PSN during RADIUS authentication.

Figure 3-23 Client Provisioning Policy



Provisioning iOS Devices

The following steps take place while provisioning Apple iOS devices:

1. The device connects to the provisioning SSID using PEAP authentication.
2. The device is redirected to the BYOD Registration Portal.
3. After successful authentication, the Over-The-Air (OTA) enrollment begins.
4. The device sends a unique identifier (such as its MAC address) and other information.
5. Certificate enrollment information is sent to the device.
6. A SCEP request is made to Cisco ISE, which returns a device certificate.
7. The wireless profile for the SSID to which the device is trying to connect is sent to the device.
8. Once the enrollment is complete, the user manually connects to the SSID for which it received the wireless profile using EAP-TLS authentication.

Provisioning Android Devices

The following steps take place while provisioning Android devices:

1. The device connects to the provisioning SSID using PEAP authentication.
2. The device is redirected to the BYOD Registration portal.
3. After successful authentication, the portal page redirects the user to the Google Play Store.
4. The user installs the Supplicant Provisioning Wizard (SPW).
5. The SPW is launched to perform provisioning of the device. The SPW performs the following functions:

a. Discovers Cisco ISE and downloads the profile from Cisco ISE.

b. Creates a certificate/key pair for EAP TLS.

c. Makes a SCEP proxy request to Cisco ISE and gets the device certificate.

d. Applies the wireless profile to allow connectivity to the SSID to which the client was trying to connect.

6. The SPW triggers re-authentication and connects to the SSID for which it received the wireless profile, automatically using EAP-TLS authentication.

Note The Android agent (SPW) must be downloaded from the Google Play Store and is not provisioned by Cisco ISE. Therefore, a BYOD Android device must be able to reach the Google store from the place in the network point where provisioning take place. Two possible scenarios exist for clients in the Industrial Zone:

- Provisioning of Android devices through the enterprise anchor WLC (recommended)
- Direct access to the Google Play store through the IDMZ (if permitted by the company's security policy)

Mobile Device Profiling

Profiling is a key service responsible for identifying, locating, and determining the capabilities of endpoints that attach to the network to deny or enforce specific authorization rules. Two of the main profiling capabilities include:

- Collector is used to collect network packets from network devices and forward attribute values to the analyzer.
- Analyzer is used to determine the device type by using configured policies that match the attributes.

Profiling is done using a large number of probes, including RADIUS, DHCP, DHCP SPAN, HTTP, DNS, etc.

Endpoint profiling policies in Cisco ISE allow it to categorize discovered endpoints on your network and assign them to specific Endpoint Identity Groups.

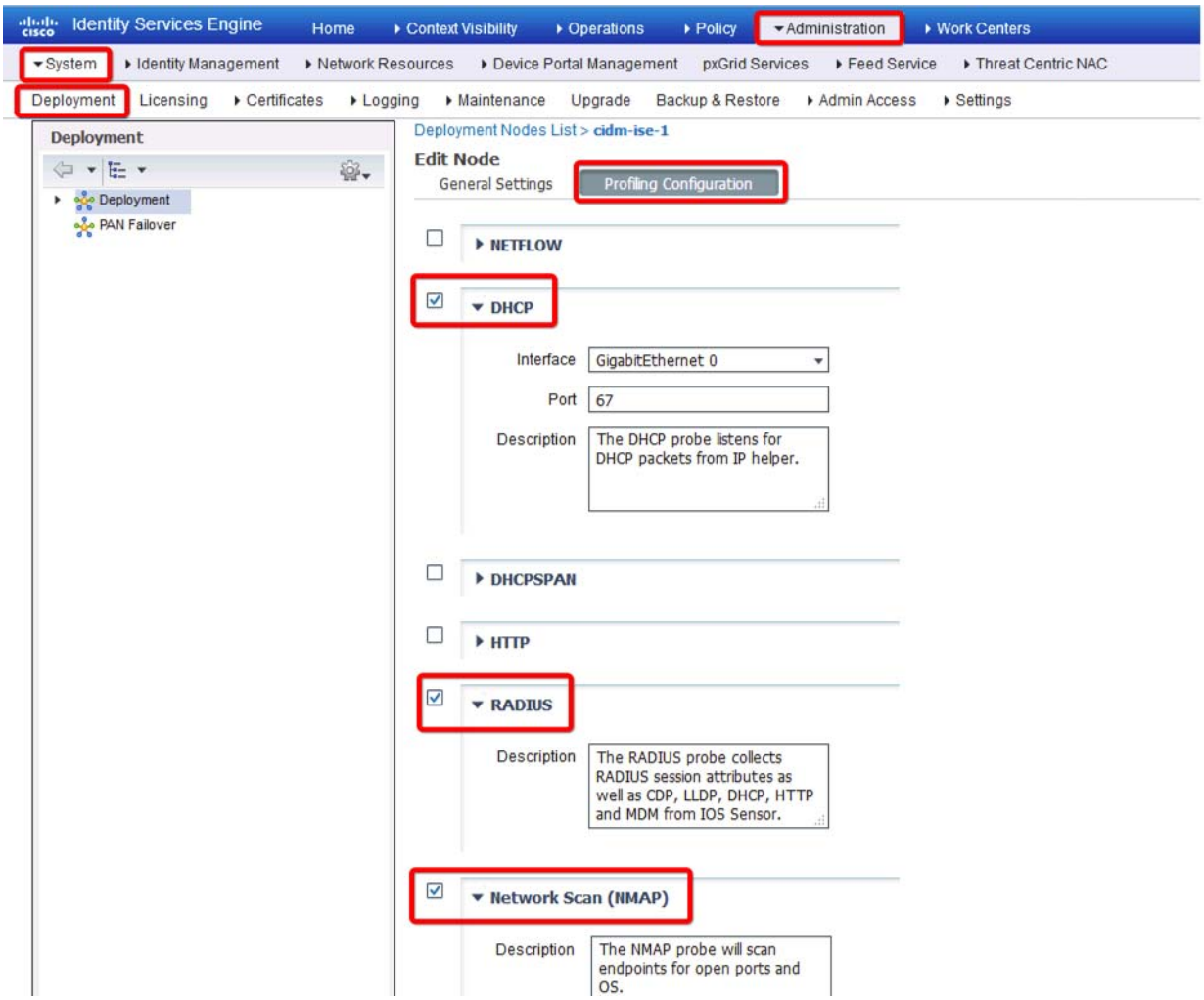
Note For complete information on Cisco ISE profiling services, refer to: https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_010101.html

Step 1 To enable profiling on Cisco ISE:

a. From **Administration** > **System** > **Deployment**, click on the **PSN** hostname and select **Profiling Configuration**.

b. Enable or disable profiling methods as appropriate for the organization.

Figure 3-24 PSN Profiling Configuration

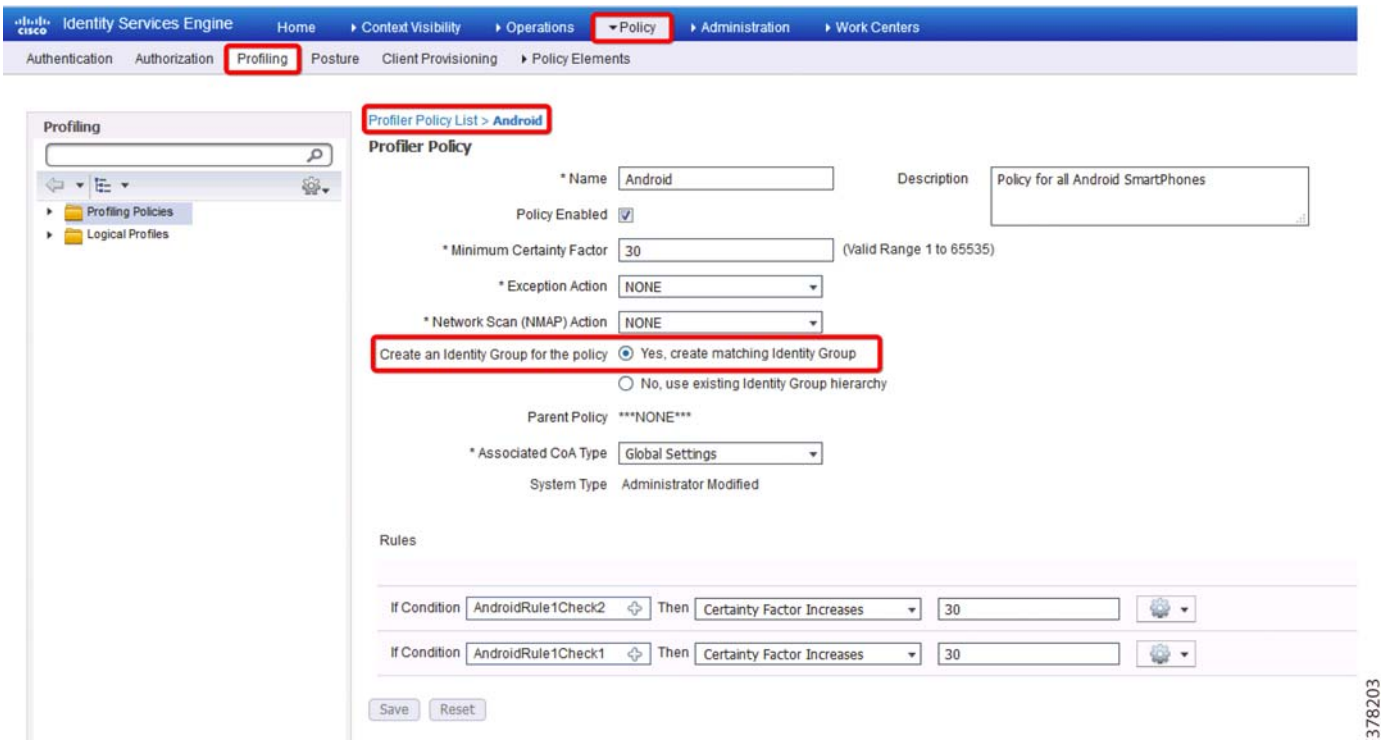


Step 2 To create an identity group based on the profiling results such as the OS of the device:

a. From **Policy** > **Profiling** > **Profiling Policies**, choose the default policy for the device type and click **Edit**. Custom profiling policies can also be created here.

b. Enable the **Create Matching Identity Group**. This group can then be used in the authorization policies.

Figure 3-25 Profiler Policy and Identity Group



Logical Profiles

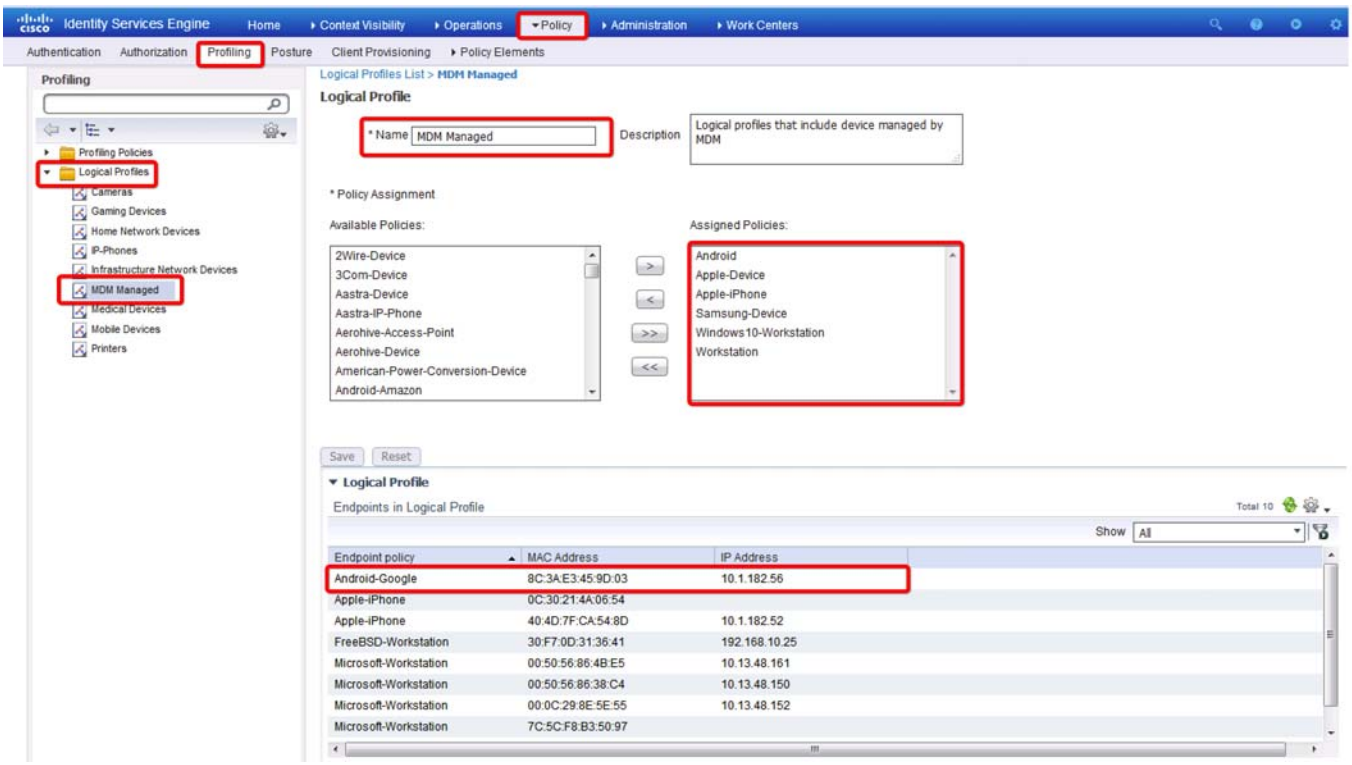
Logical profiles are containers that group different device profiles to create an overall category of profiles. Logical profiles provide additional flexibility to the authorization policies, enhancing the overall network access policy.

With logical profiles, a single entry in the authorization rule is able to include several profiles so there is no need to create a matching identity group for each device type.

For the CPwE Identity and Mobility Services architecture, a logical profile was created to group the mobile device types that are managed by the MDM.

Step 3 To create a logical profile, click **Policy** > **Profiling** > **Logical Profiles**. Click **Add** and select the appropriate profiler policies for the logical profile.

Figure 3-26 Logical Profile Configuration



MDM Server Integration

This section describes only the general steps required to integrate an MDM server with Cisco ISE. The CPwE Identity and Mobility Services architecture uses the on-premise MDM deployment model where the server is located in the Enterprise Zone. Cisco ISE can be integrated with various third-party MDM servers.

Note For more information on MDM integration and vendor-specific steps, refer to: https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_01000.html#ID397

Step 1 Configure Cisco ISE to authenticate the MDM API.

a. Install the MDM's HTTPS certificate in the Cisco ISE Trusted Certificates store.

b. Select the **Trust for Authentication within ISE** option.

Figure 3-27 MDM Certificate Options

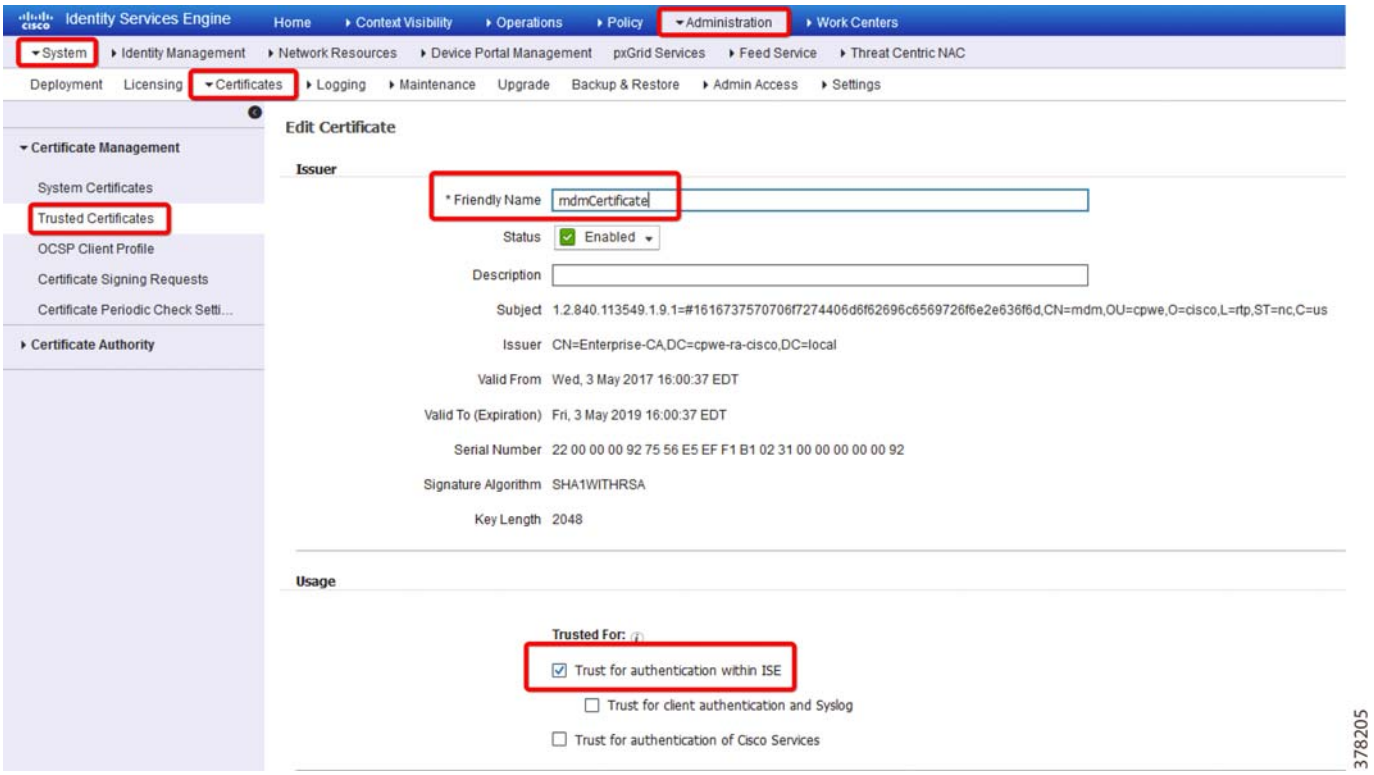
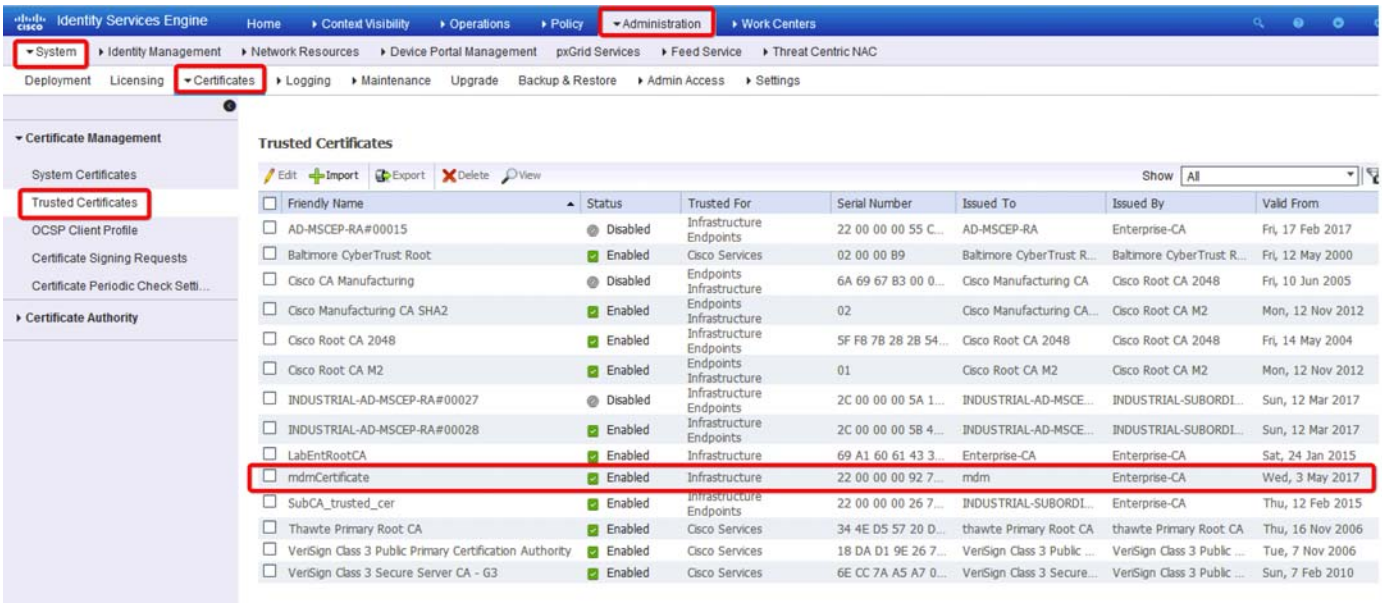


Figure 3-28 Trusted MDM Certificate



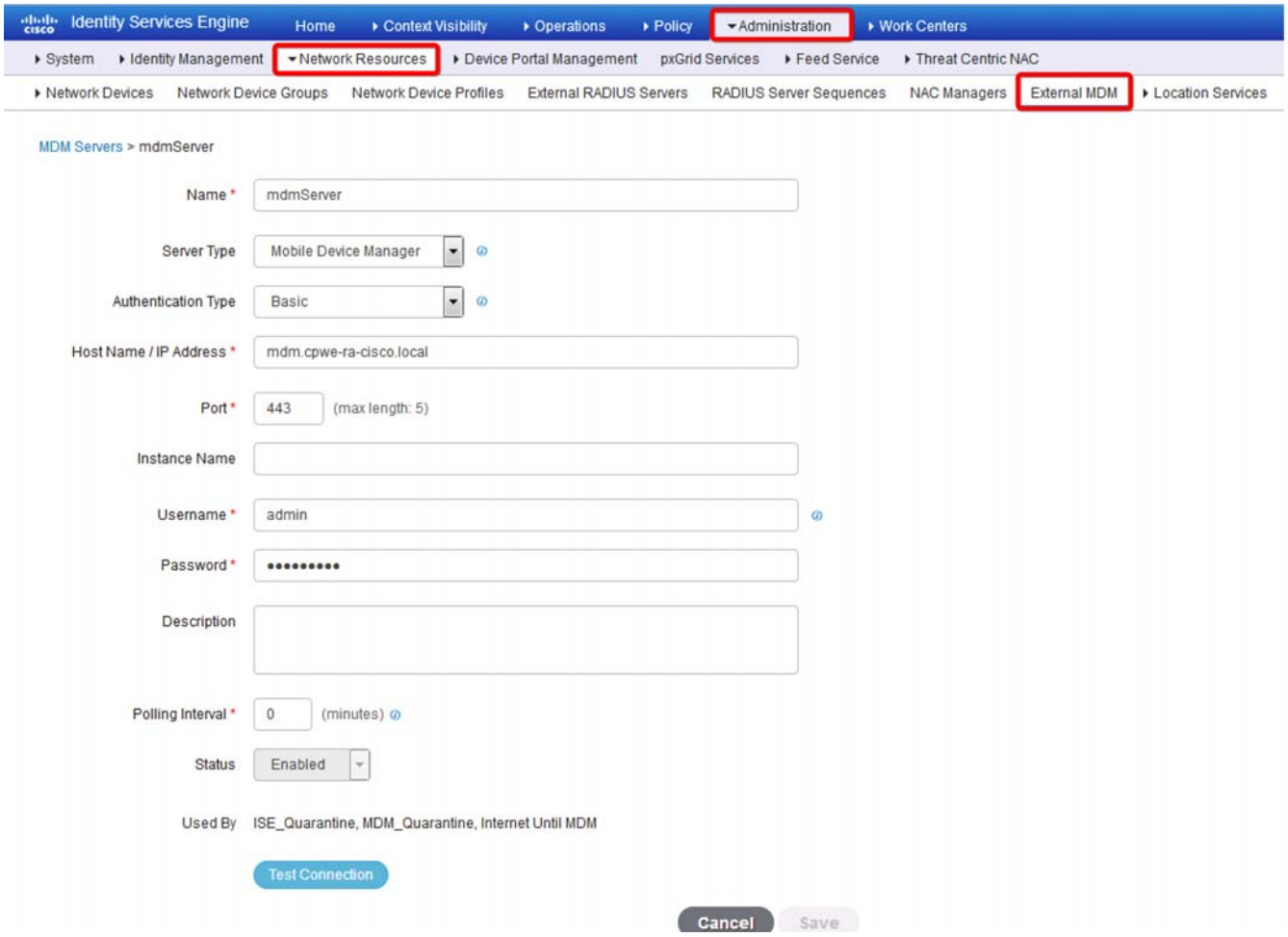
Step 2 Configure the connection parameters for the MDM server.

a. Using **Administration** > **Network Resources** > **External MDM**, configure the server name, the DNS, or the IP address. The TCP port will typically be 443 for HTTPS.

b. Configure the username and password that matches the API account settings on the MDM server.

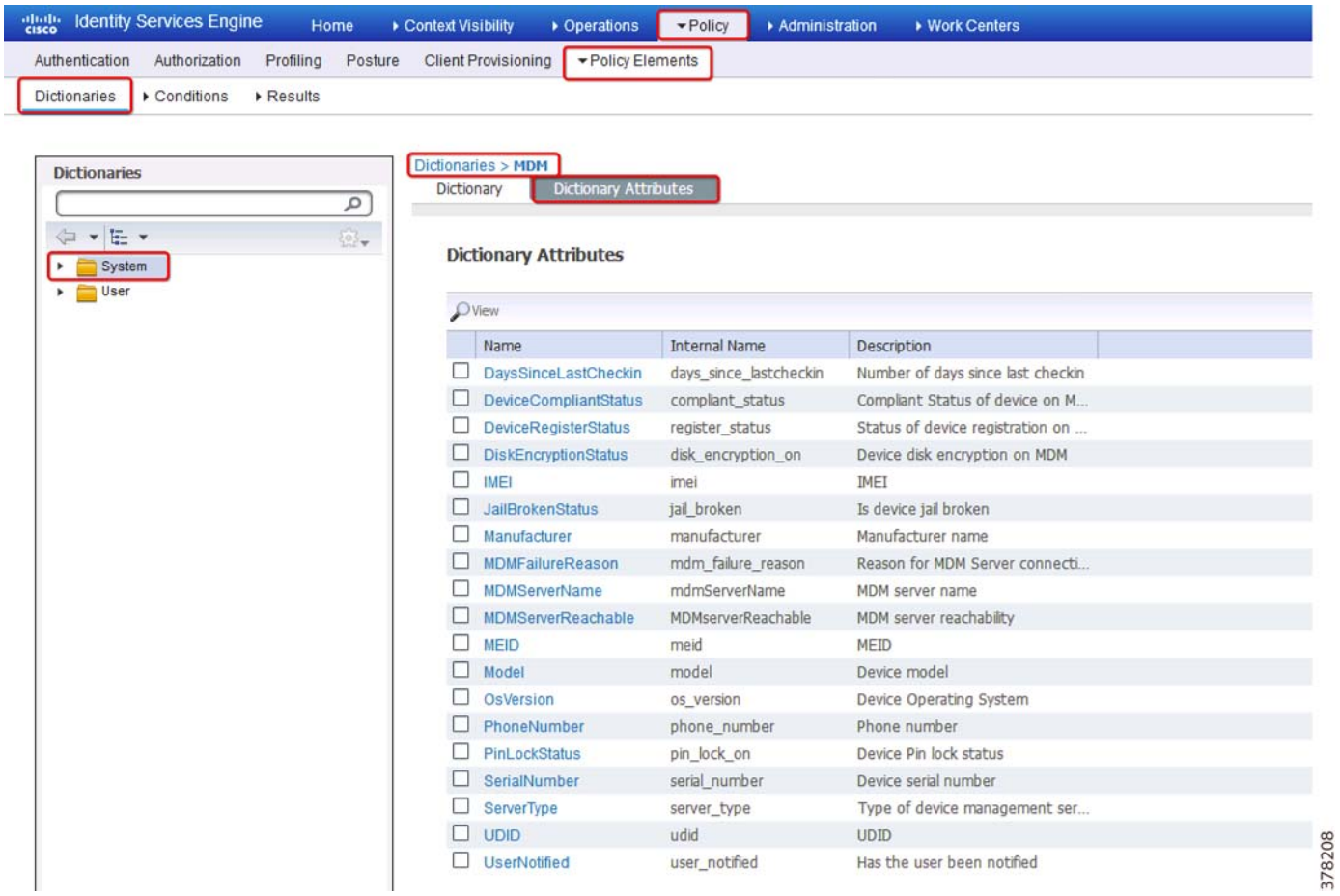
c. Configure the polling interval that specifies how often Cisco ISE will query the MDM for changes to device posture. This value should be the same as the polling interval on the MDM server (usually every few hours). An interval of 0 minutes effectively disables polling.

Figure 3-29 MDM Connection Settings



Step 3 Once the MDM server is connected to Cisco ISE and the connection test is successful, the Cisco ISE dictionary gets updated with MDM attributes. These attributes can be used in authorization policies.

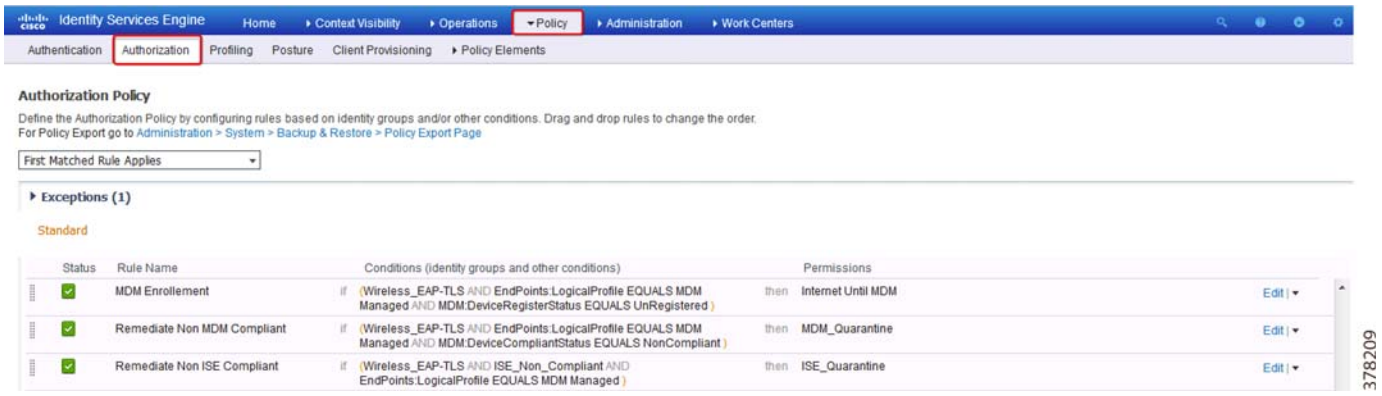
Figure 3-30 MDM Dictionary Attributes



Step 4 Configure authorization policies using mobile device compliance status.

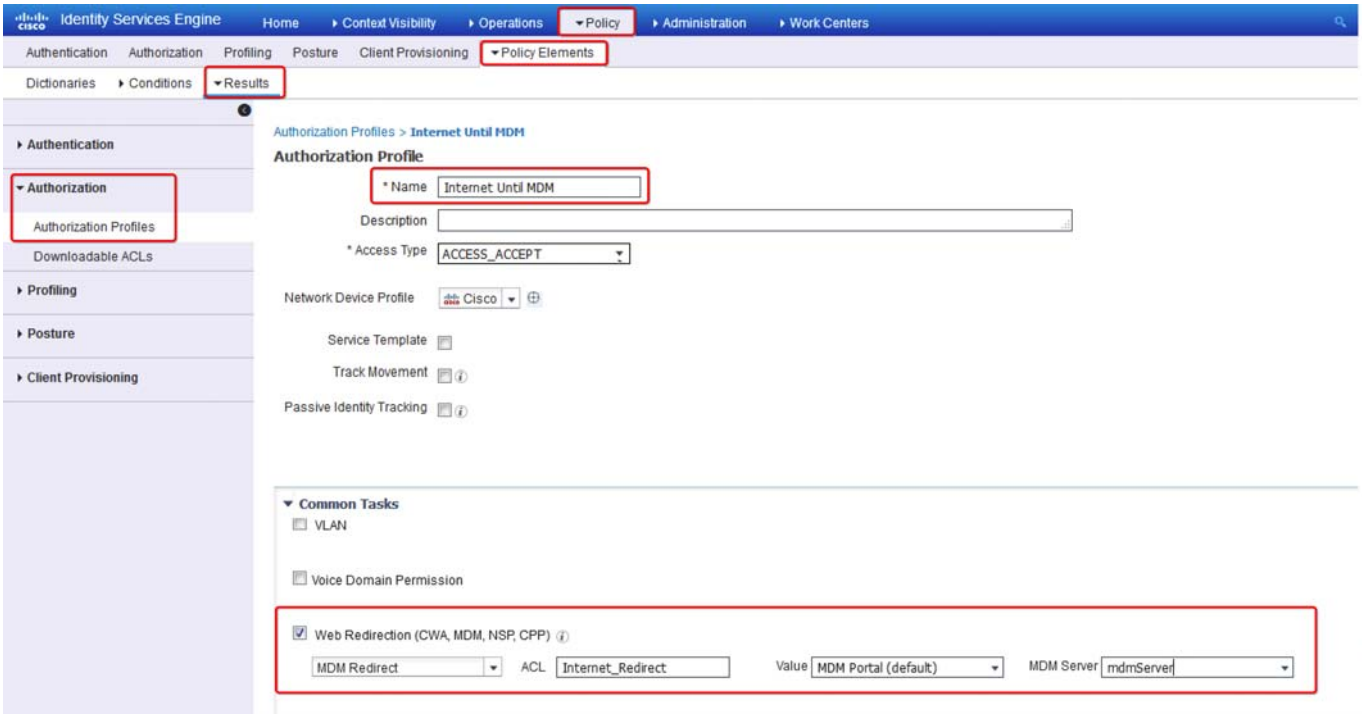
Figure 3-30 shows an example of Cisco ISE authorization rules to enforce mobile device compliance. These authorization rules are executed after the user has on-boarded the mobile device and before additional access (e.g., Full, Partial, Internet) to the network is granted.

Figure 3-31 Authorization Policies using MDM Attributes



a. One of the above authorization profiles (**Internet until MDM**) is configured to redirect nonregistered devices to the redirect URL (the MDM portal page).

Figure 3-32 Web Redirection Profile for MDM



b. Non-compliant devices are placed in quarantine until they become compliant; e.g., until they download the correct OS version or remove the inappropriate applications.

c. As part of the authorization profile, the PSN sends an ACL name to the WLC in the RADIUS response. The WLC applies the ACL to the traffic to and from the wireless user.

MSE Integration for Location Based Services

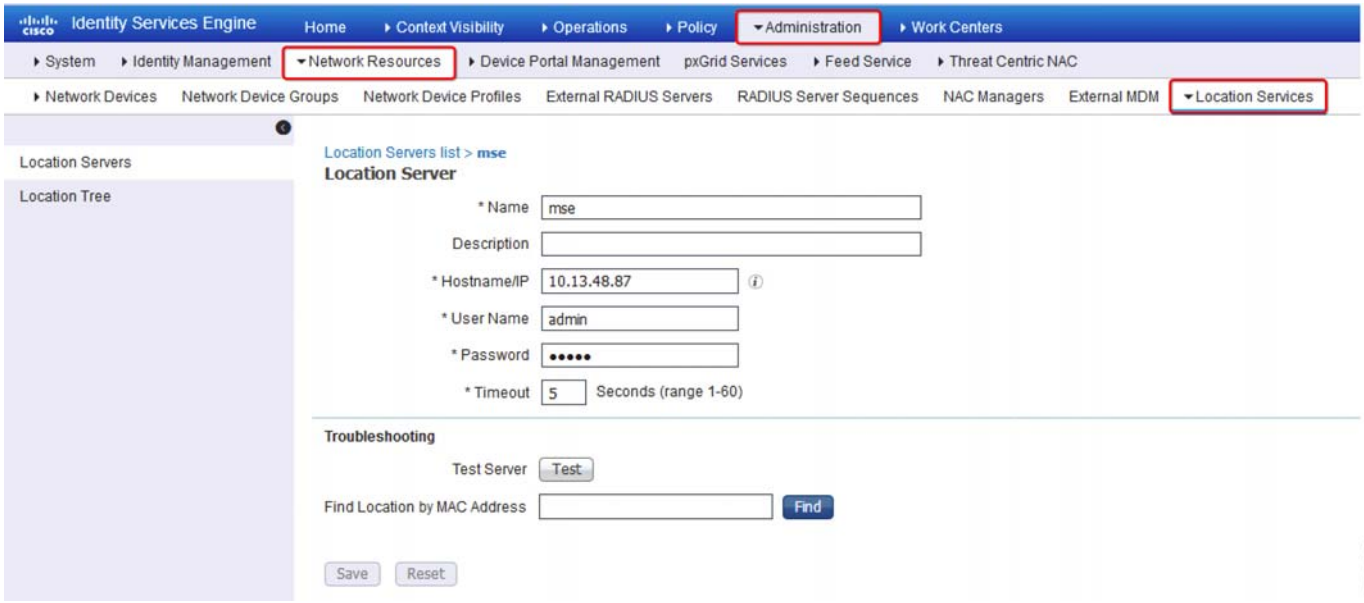
Steps below outline integration of Cisco ISE with the Cisco MSE to use the wireless user's physical location as part of the authorization profile.

Step 1 Configure the location server parameters.

a. In **Administration** > **Network Resources** > **Location Services**, configure the MSE name, DNS hostname or IP address, and login credentials.

b. The same page lets you test the connection and perform client location lookup by MAC address.

Figure 3-33 Location Server Parameters



Step 2 Once the server is connected to Cisco ISE and the test is successful, the location tree gets updated with the location map attributes and the Cisco ISE dictionary gets updated with MSE attributes. These attributes can be used in the authorization profiles.

Figure 3-34 MSE Location Tree

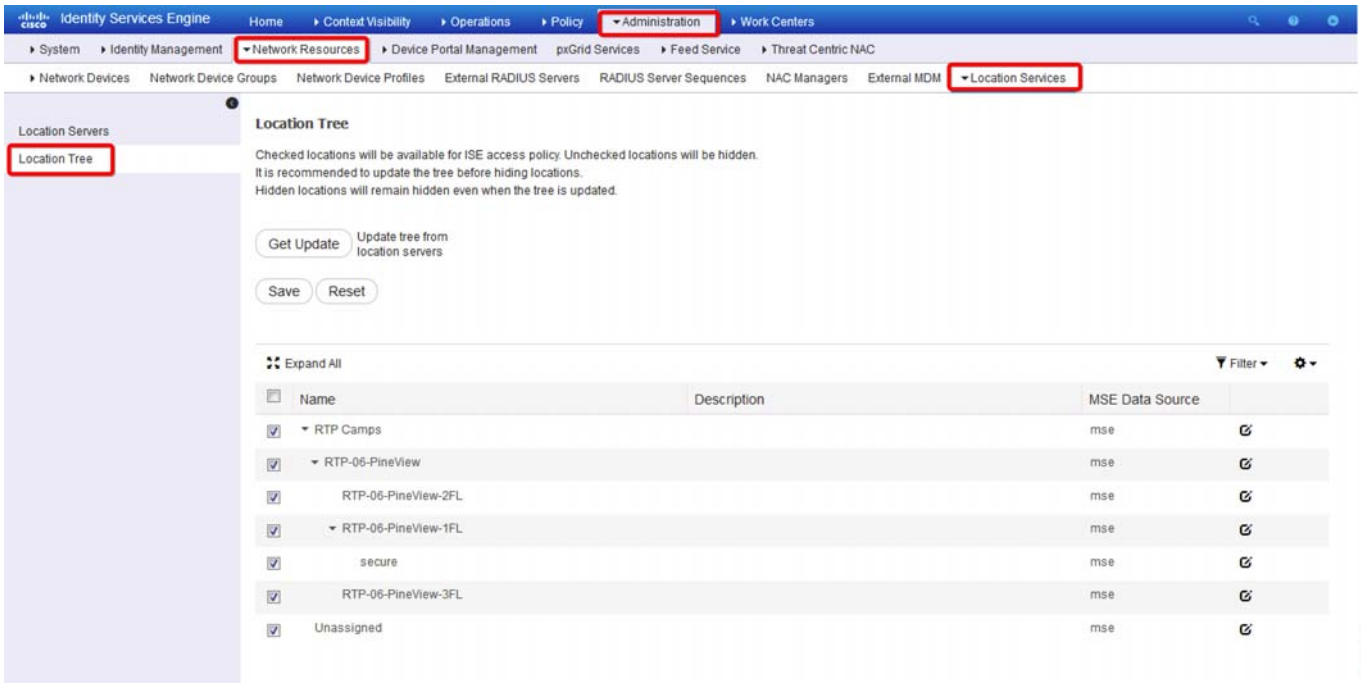
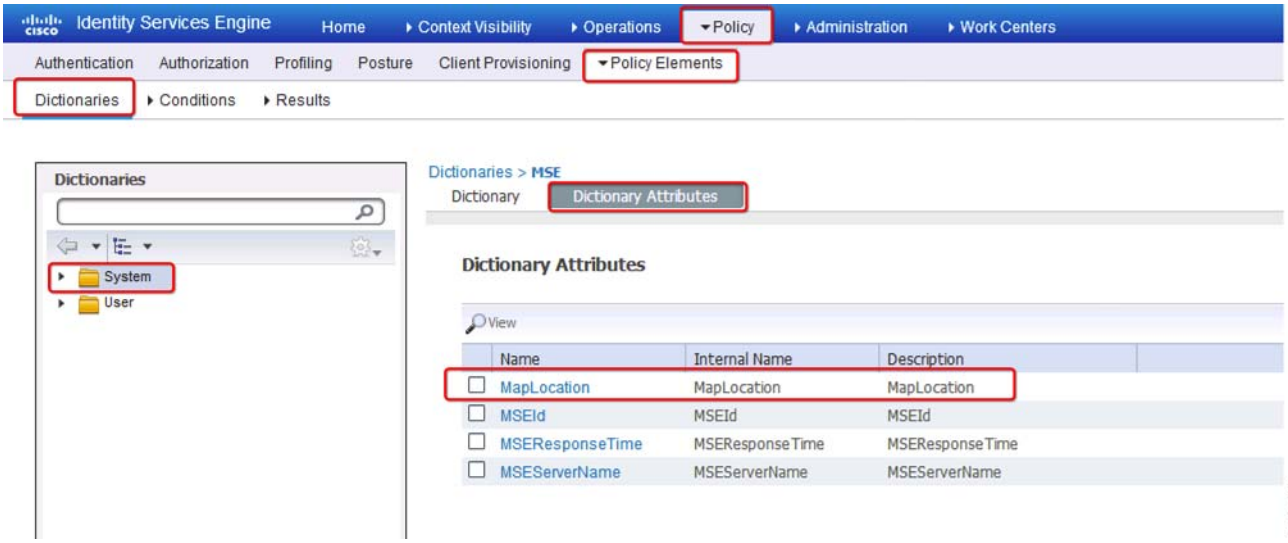
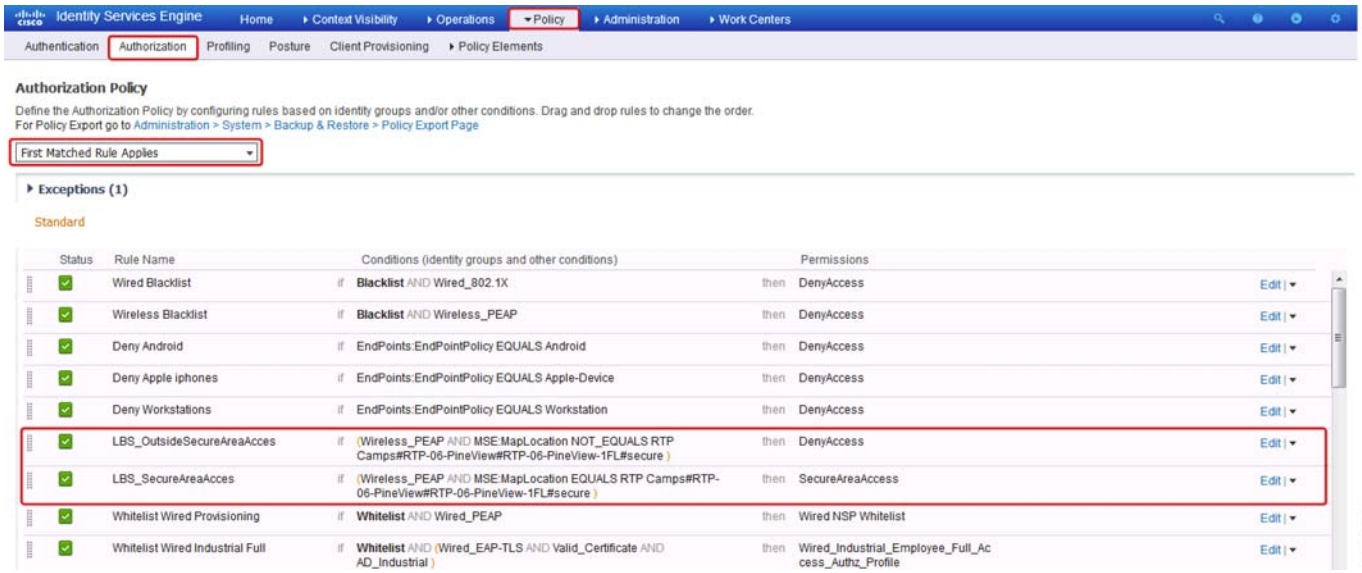


Figure 3-35 MSE Dictionary Attributes



Step 3 An example of the authorization profile using location information is shown below. In the example, the access is denied if a wireless user is outside the defined area.

Figure 3-36 Authorization Profile using LBS



Policy Element Configuration

This section describes the configuration of policy elements such as simple and compound conditions, as well as a list of allowed protocols. The conditions can be used to build authentication and authorization policies.

Note For more information about Cisco ISE policy elements, refer to: https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_010001.html

Step 1 Specify the list of allowed authentication protocols.

a. In **Policy Elements** > **Results** > **Authentication protocols** > **Allowed protocols**, edit **Default Network Access** list or add a new list.

b. Configure the protocol services allowed in the network, for example EAP-TLS and PEAP. Most of the time, default Cisco ISE settings are sufficient.

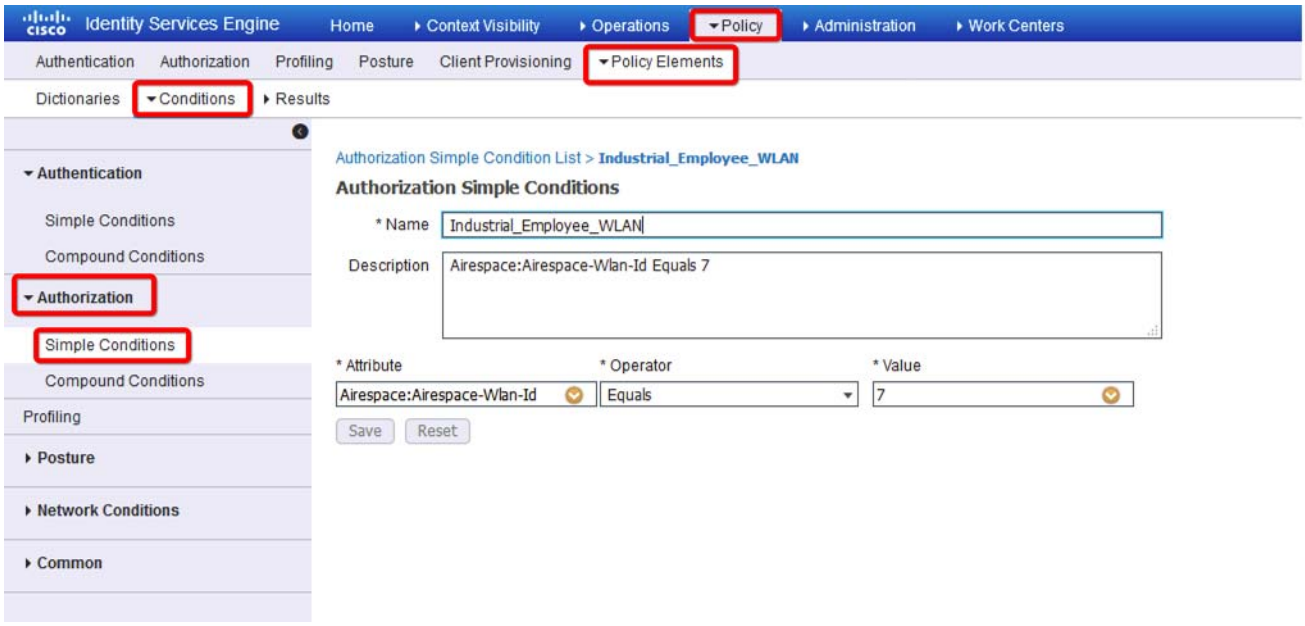
Step 2 Create simple conditions for authorization based on the SSID.

a. In **Policy** > **Policy Elements** > **Conditions** > **Authorization** > **Simple Conditions**, click **Add**.

b. Create a rule as shown based on the WLAN ID attribute that should match the WLC WLAN ID number. In the example below, the Industrial Employee WLAN ID is shown.

c. Create simple conditions for all other SSIDs in the architecture.

Figure 3-37 Simple Condition for Authorization



Step 3 Create compound conditions for authorization.

The following steps show an example for the Industrial Employee authentication and authorization. Configuration for other use cases, such as Corporate Employee and Trusted Partner access, should be similar. Depending on the company's security policies and procedures for wireless access, other criteria may be used in the conditions, such as device OS, physical location, posture status, and so on.

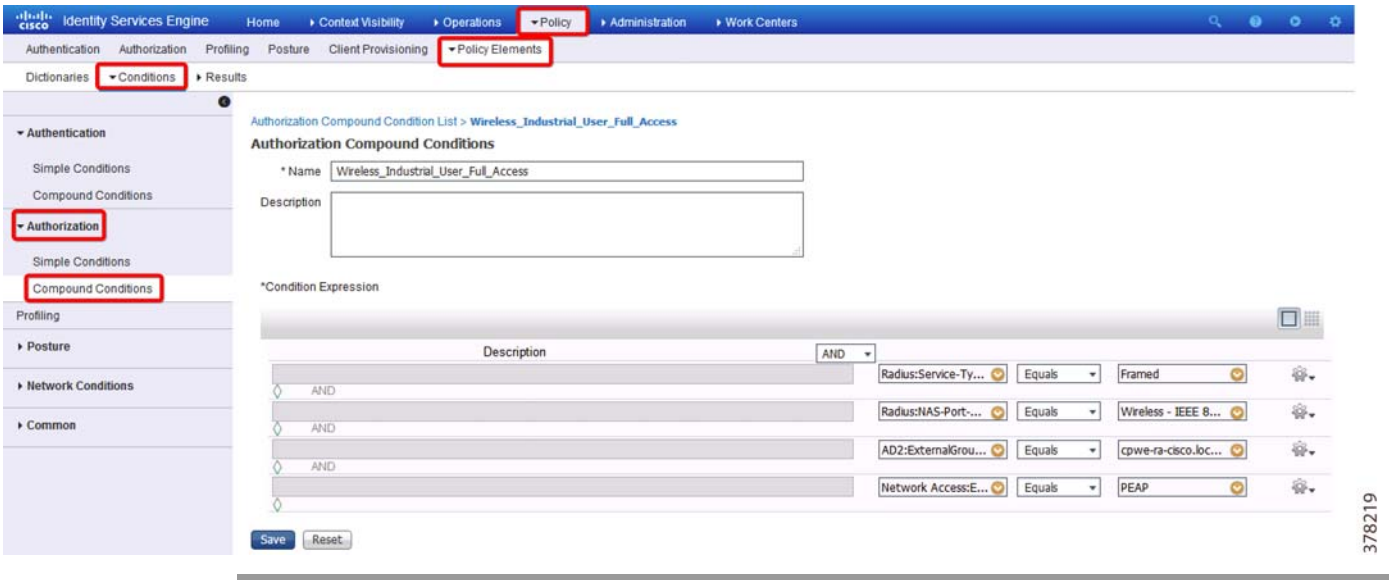
a. In **Policy** > **Policy Elements** > **Conditions** > **Authorization** > **Compound Conditions**, click **Add**.

b. Select attributes for wireless 802.1X access as shown (RADIUS Service Type and NAS-Port).

c. Add a condition for the user's AD group (in this case, the group for plant floor workers with full access).

d. Add a condition for the authentication protocol, for example EAP-TLS or PEAP.

Figure 3-38 Example of Authorization Compound Condition



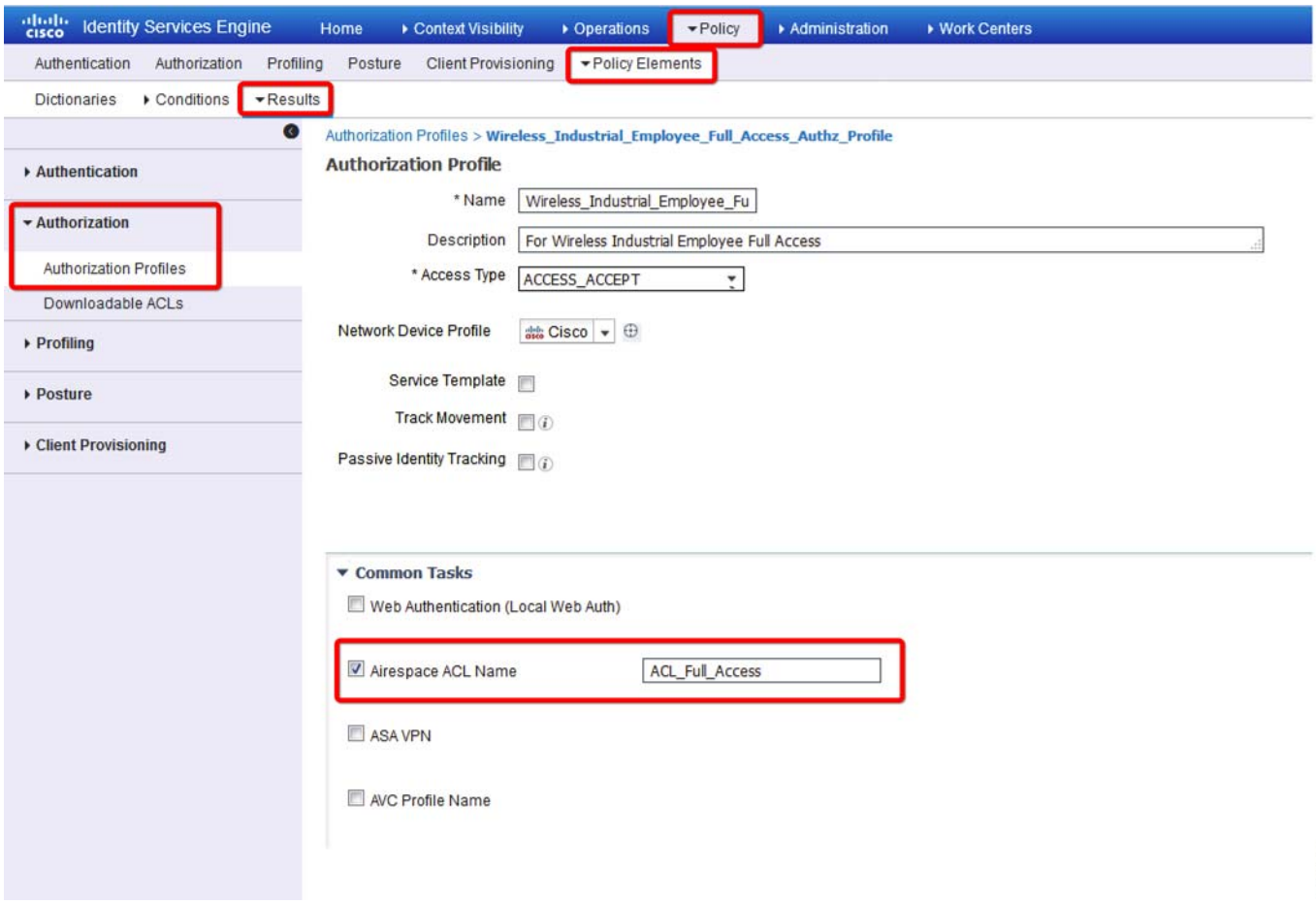
Authorization Profiles

An authorization profile for wireless access acts as a container for a number of specific permissions to be granted and can include:

- An associated VLAN.
- Wireless LAN Controller attributes such as the use of a Named ACL (Airespace ACL).
- An associated downloadable ACL (DACL) for wired 802.1X access.

An example of the authorization profile for the **Industrial Employee with Full Access** is shown below. The profile defines an ACL name that the WLC must apply to the user's traffic.

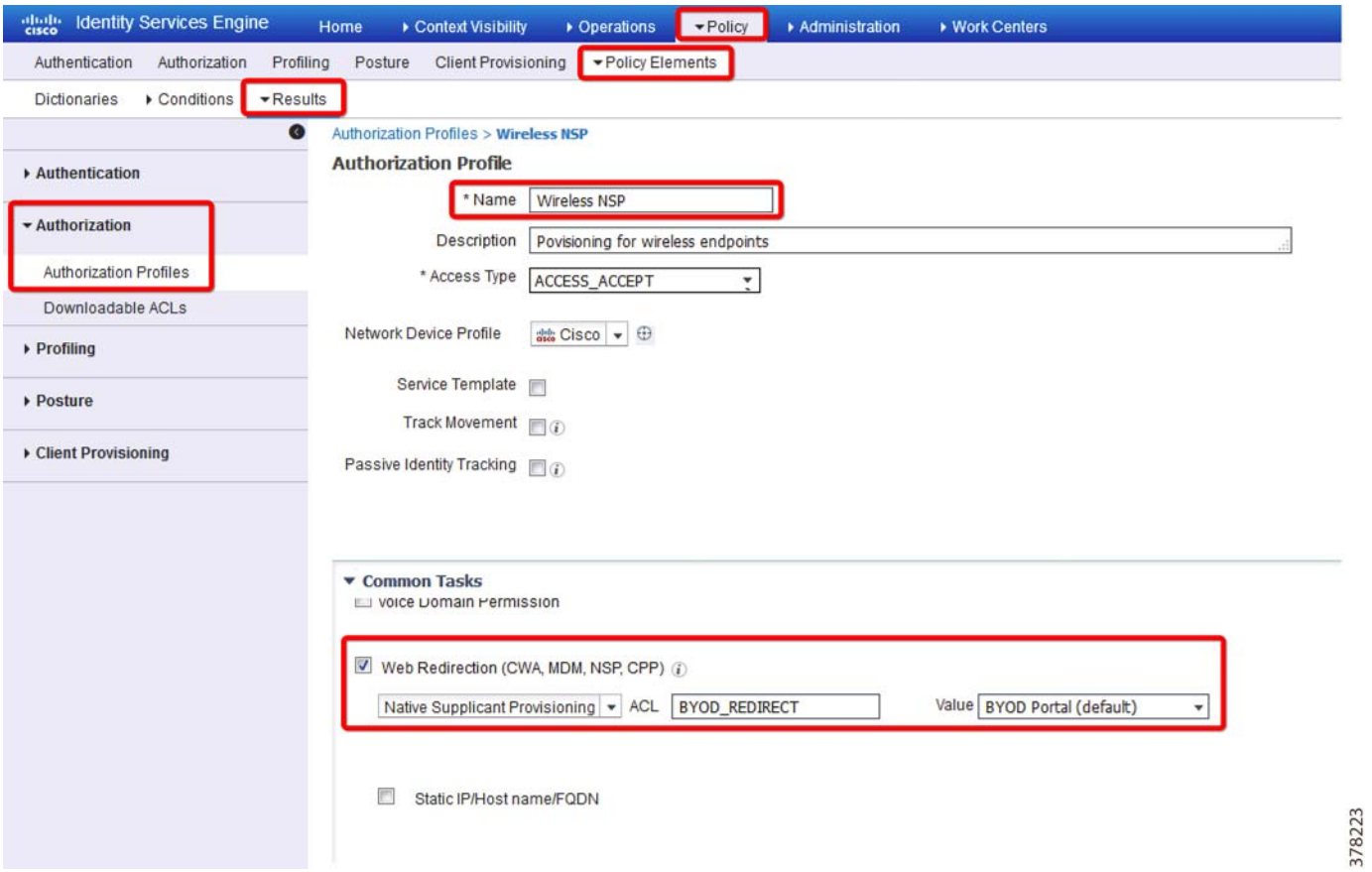
Figure 3-39 Industrial Employee Authorization Profile Example



In addition to the standard Permit Full Access, Permit Partial Access and Deny Access authorization profiles, wired and wireless **Native Supplicant Profiles (NSP)** have been defined in the CPwE architecture. The NSPs are used to redirect wireless users to the BYOD registration portal when they access the network using a non-provisioned device.

The Wireless NSP specifies the ACL name and the BYOD portal URL for web redirection. The WLC will find these parameters in the RADIUS response.

Figure 3-40 NSP Authorization Profile Example



Authentication Policy Configuration

Authentication policies are used to define the protocols used by Cisco ISE to communicate with the endpoints and the identity sources to be used for authentication. In a normal deployment scenario, the endpoints would primarily use the 802.1X protocol to communicate with Cisco ISE. Cisco ISE authenticates these endpoints against the AD or authenticates them using digital certificates.

Cisco ISE evaluates the conditions and based on whether the result is true or false, it applies the configured result. An authentication policy includes:

- An allowed authentication protocol, such as PEAP, EAP-TLS, etc.
- An identity source used for authentication, such as the AD.

Similar to the way access lists are processed, authentication rules are processed from the top down. When the first condition is met, processing stops and the assigned identity rule is used.

The rules are evaluated using “If, then, else” logic, for example:

```
IF Wireless_802.1X then Allow EAP-TLS and PEAP
Else if next condition then <Action>
<…>
Else Use Default Rule
```

Note For more information about Cisco ISE authentication policies, refer to: https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_010010.html

The following steps describe the configuration of authentication policies for wireless clients:

Step 1 Configure authentication policy.

a. From **Policy** > **Policy Sets**, select the **Default Policy Set**.

b. In the **Authentication Policy**, either customize the default Dot1x policy or insert a new policy above/below any existing policy.

c. Assign a Rule name (such as Wireless Dot1x AuthC).

d. Add an existing **Wireless_802.1X** authentication compound condition from the library. Select **Default Network Access** as a default Allowed Protocol Service list (or select a custom list).

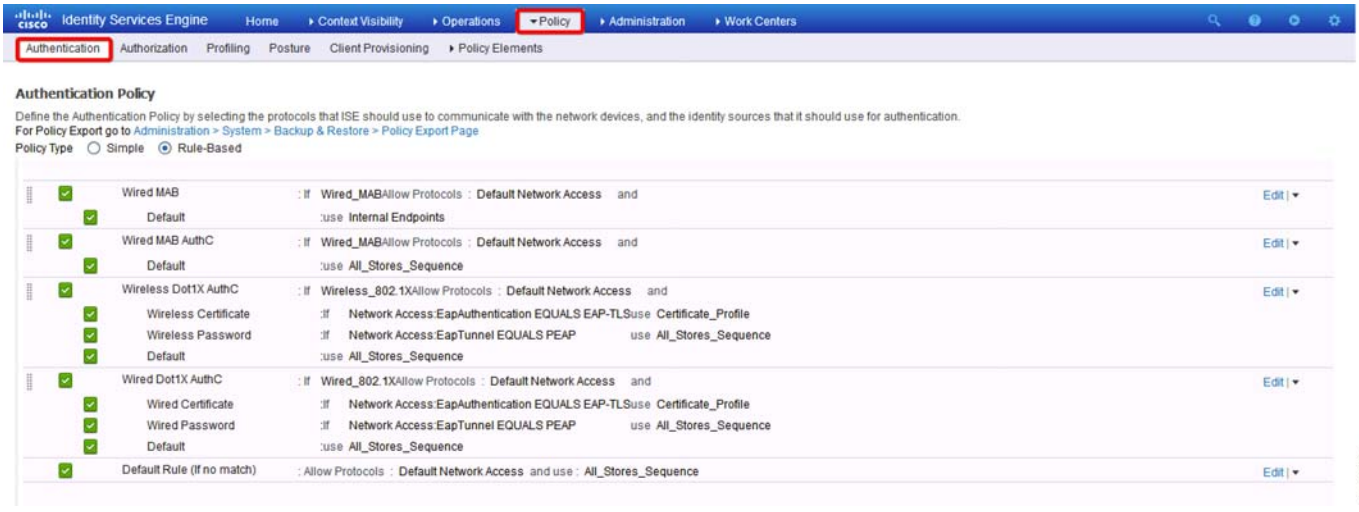
e. For the Default condition, set the Identity Source to **All_Stores_Sequence**.

f. Insert a new row above and create a new condition for the EAP-TLS method as shown below.

g. In the **Use** section, change the Identity Source to the previously configured certificate authentication profile.

h. Insert a new row to create a rule for the PEAP method as shown below. Set the Identity Source to **All_Stores_Sequence**.

Figure 3-41 Authentication Policy Example



Authorization Policy Configuration

Authorization policies define the overall security policy to access the network. Network authorization controls user access to the network and its resources and what each device can do on the system with those resources. An authorization policy is composed of multiple rules which are defined by three main elements:

- Names

- Conditions
- Permissions

Similar to the authentication rules, authorization rules are processed from the top down. When conditions are met in a rule, processing stops and the assigned permission dictates what authorization policy to use. Based on the requirements, the conditions can be individual simple conditions, combined together in one compound condition, or a combination of both.

Authorization rules are created similar to the authentication rules described in the previous section. An example of rules used to validate the CPwE Identity and Mobility Services architecture is shown below. The specific set of conditions and permissions for a particular deployment may differ based on a specific security policy and environment.

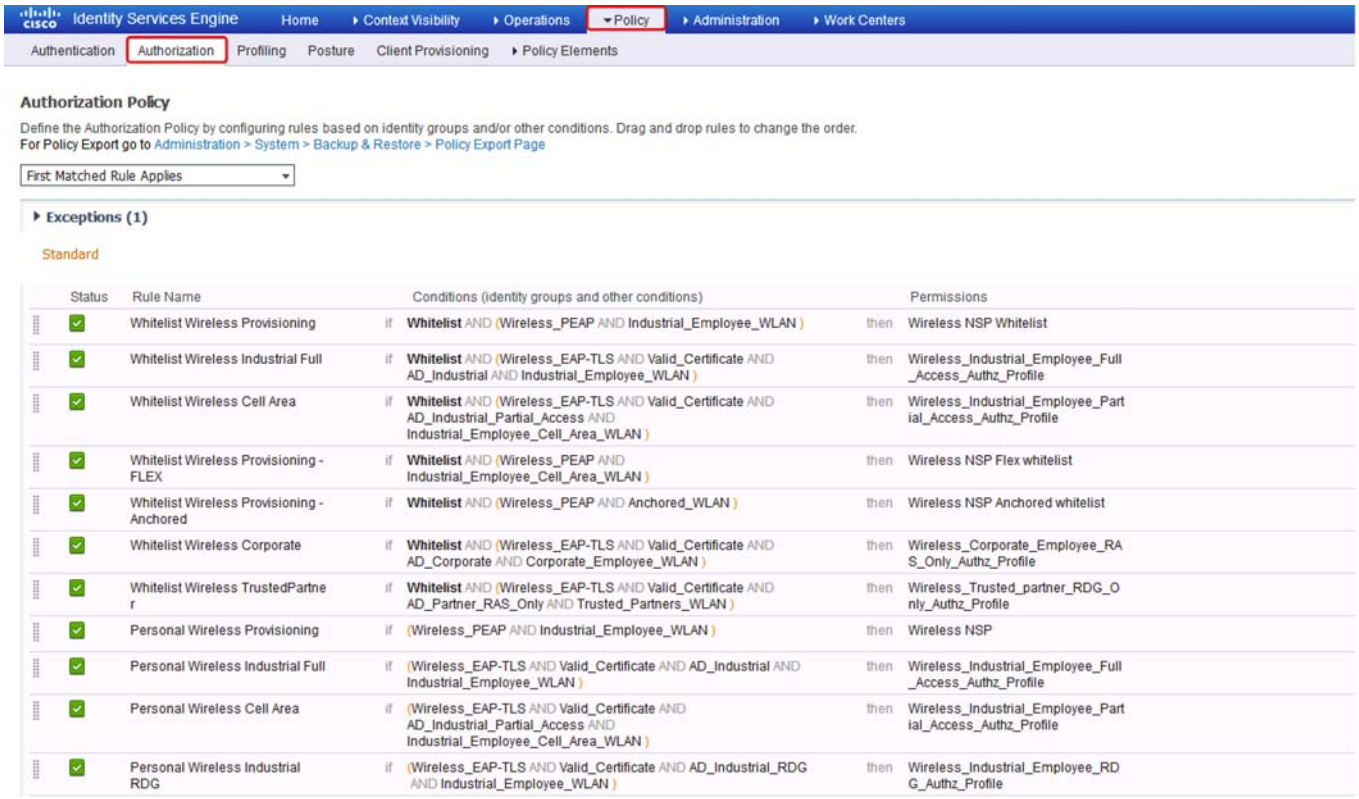
In the example below, a rule for corporate-issued wireless devices is matched when all following conditions are met:

- The device is in the Whitelist of MAC addresses.
- The EAP-TLS protocol is used for authentication.
- The certificate is valid (issued by the trusted authority and not expired or revoked).
- The user belongs to the correct AD group.
- The device is associated to the correct WLAN SSID.

When a particular rule is matched, permissions are enforced by the authorization profiles associated with the rule. The profiles may specify attributes to be sent to the WLC such as an ACL name or VLAN to apply.

Conditions and permissions for BYOD as well as non-provisioned devices may be different, for example to redirect the user to the provisioning portal. In this case, the device has to use PEAP for authentication since the certificate has not yet been installed.

Figure 3-42 Authorization Policy Example



Industrial WLC Configuration

This section describes how to configure the Industrial WLC to implement wireless user access scenarios described in Chapter 2, "CPwE Identity and Mobility Services Design Considerations." The following configuration steps are covered in this section:

- RADIUS Configuration
- Interface Configuration
- WLAN Configuration
- ACL Configuration
- Anchor Mobility Configuration

Note Configuration of the Unified WLAN infrastructure for the Industrial Zone, including wireless connectivity to IACS devices, is covered in the *Deploying 802.11 Wireless LAN Technology within a Converged Plantwide Ethernet Architecture Design and Implementation Guide* at the following URLs:

- Cisco site: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/NovCVD/CPwE_WLAN_CVD.html
- Rockwell Automation site: http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td006_-en-p.pdf

It is assumed that the Industrial Zone WLC has already been installed and configured with the initial parameters. Refer to the specific product guide on the Cisco website for details.

Note Complete configuration guide for the Cisco WLC software can be found here: https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-4/config-guide/b_cg84.html

RADIUS Configuration

RADIUS is a client/server protocol that provides centralized security for users attempting to gain access to a network. The CPwE Mobility and Identity Services architecture uses Cisco ISE PSNs as a RADIUS servers for user traffic.

Industrial PSN is used for mobile clients connecting to the Industrial Zone resources. Enterprise PSN is used for Corporate Users and Trusted partners (Guests) that are connecting to the Enterprise Zone through the EoIP tunnel. RADIUS over IPsec will be used to secure communication through the IDMZ.

The following steps describe the RADIUS configuration on the industrial WLC.

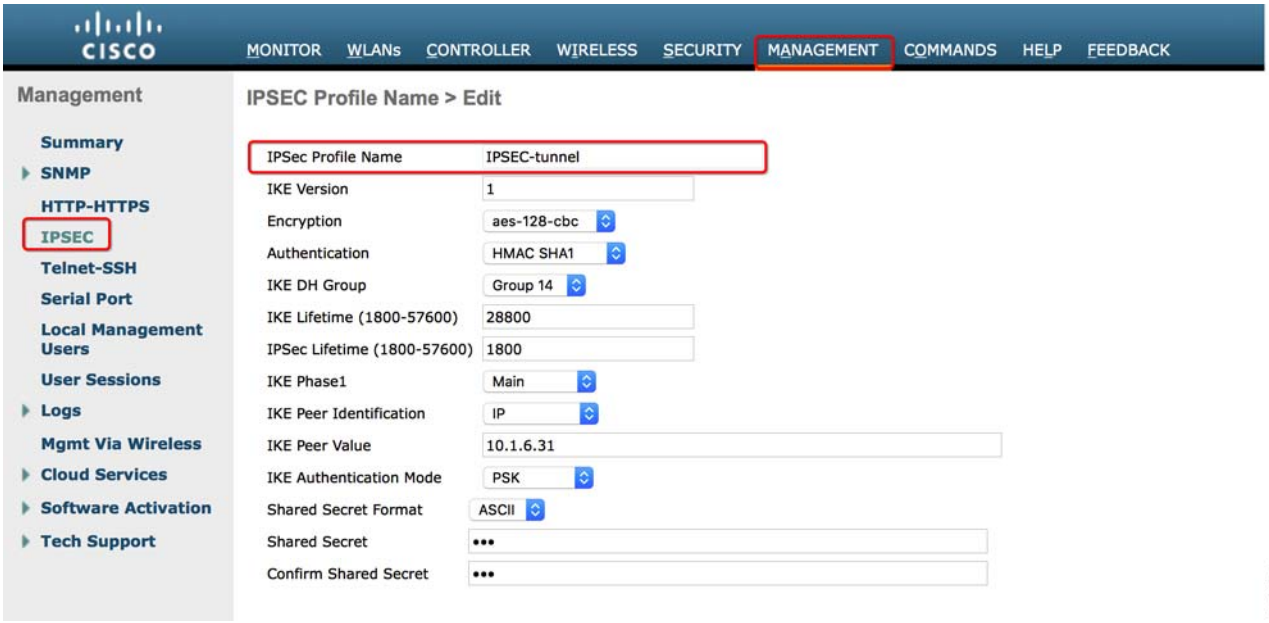
Step 1 Create an IPsec profile to be used for the Enterprise PSN.

a. From **Management** > **IPsec**, create a new IPsec profile.

b. Configure the Enterprise PSN IP address and the shared secret to authenticate IPsec peers.

c. Fill in the other parameters as shown below. The profile settings should match the IPsec parameters supported by Cisco ISE.

Figure 3-43 IPsec Profile



Note For additional security, instead of a shared secret, certificates can be used for mutual authentication between the WLC and the PSN. This method has not been validated for this CVD release.

Step 2 Configure the Industrial PSN as a RADIUS server.

a. From **Security** > **RADIUS** > **Authentication**, click **New**.

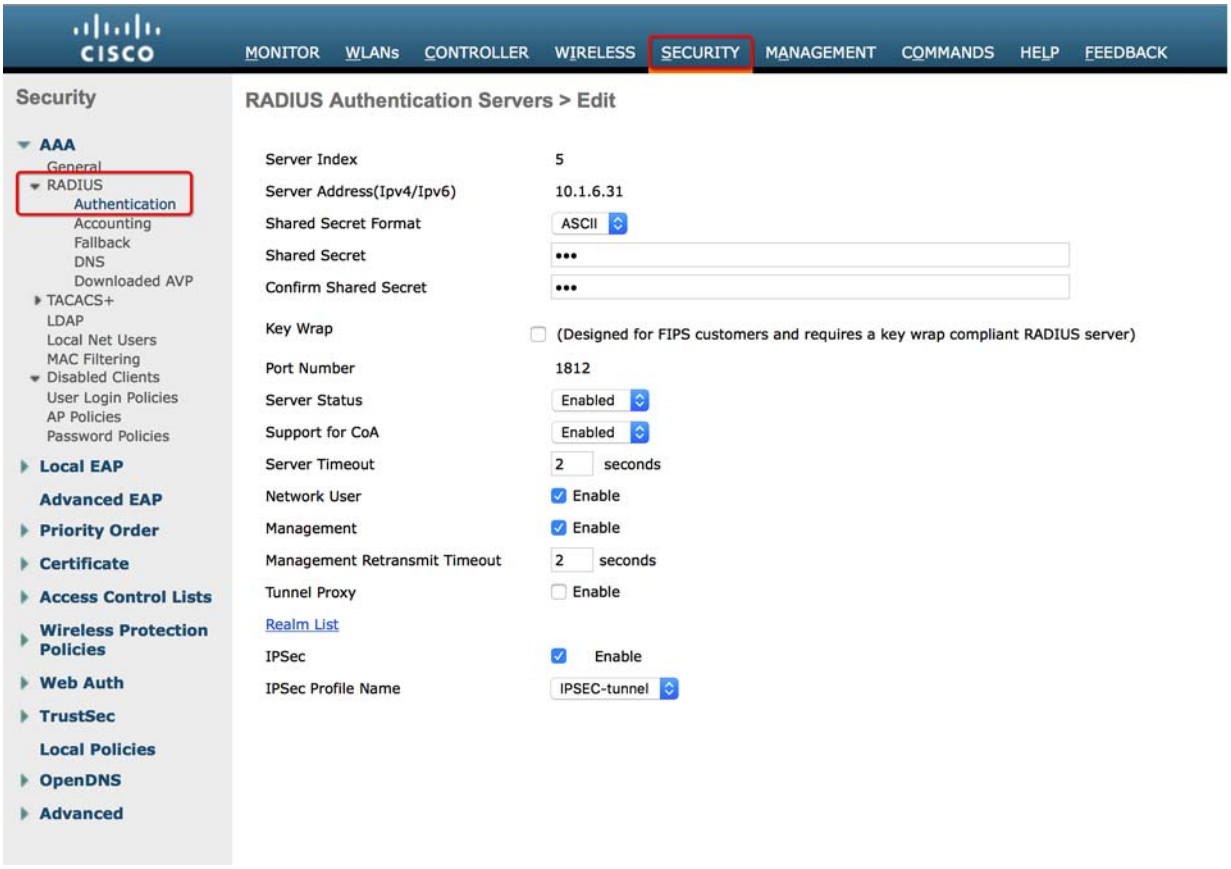
b. Fill in **Server IP address** and **Shared Secret**. The other parameters can be left as default.

c. Click **Apply** and **Save Configuration**.

Step 3 Repeat the above steps for any redundant PSNs in the Industrial Zone.

Step 4 Configure the Enterprise PSN as a RADIUS server. Select the previously configured **IPsec Profile Name**.

Figure 3-44 RADIUS Authentication Server with IPsec



Interface Configuration

The CPwE Identity and Mobility Services architecture uses VLAN segmentation in the Industrial Zone to logically segment wireless users in a VLAN and IP subnet which makes it easier to apply security policies. The WLC should be configured with an IP interface to forward the user's traffic to the appropriate VLAN. The IP interface is associated with the WLAN SSID.

The validated architecture uses a single IP interface and WLAN SSID for all mobile users accessing the Industrial Zone. After the user is authenticated, an ACL is applied to the WLAN based on the authorization profile. This approach reduces the complexity and the number of SSIDs that need to be broadcasted.

Note Depending on the security policy, mobile users can also be grouped into several VLANs per their authorization profile (e.g., a separate VLAN for Trusted Partners to access the Industrial Zone). In this case, the WLC should have IP interfaces that are mapped to those VLANs.

The PSN can send the VLAN ID in the RADIUS response and the WLC associates the appropriate interface with the Industrial WLAN dynamically using the AAA Override feature.

The following steps describe the interface configuration on the industrial WLC.

Step 1 Configure an IP interface for Industrial Employees.

a. Choose **Controller** > **Interfaces** and click **New** to add an IP interface.

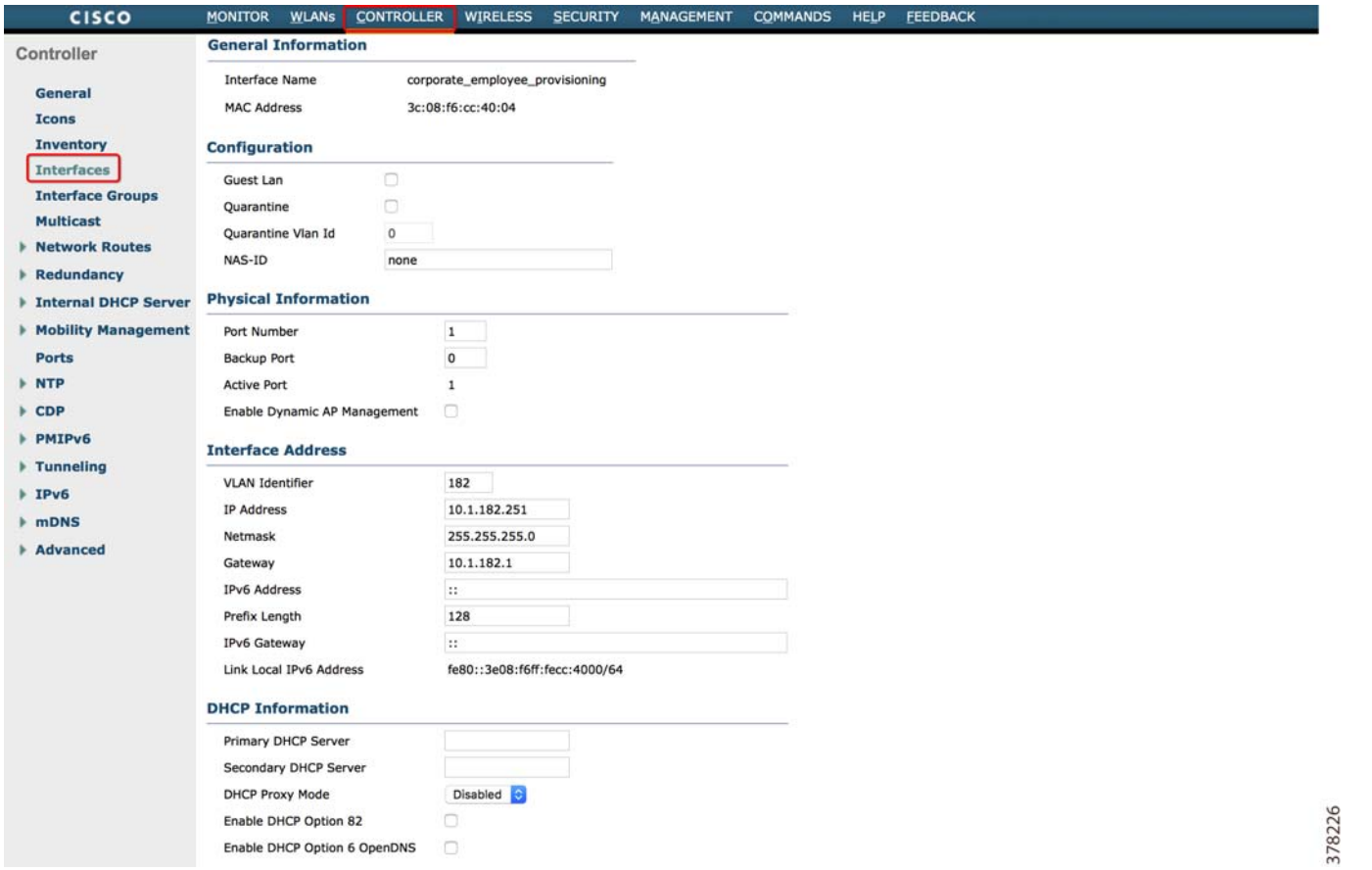
b. Enter the associated VLAN, IP address, network mask, and the gateway.

c. If the DHCP servers are on the different subnet (which is most likely), enter the DHCP server's IP addresses and enable the Global DHCP proxy mode.

d. Click **Apply** to commit your changes.

Note In case of a Corporate User or a Trusted Partner accessing the Enterprise Zone or the Guest DMZ through the tunnel, the necessary IP interfaces should be created on the anchor WLC. The user's data will be forwarded through the EoIP tunnel and mapped to a VLAN/IP subnet in the corresponding Zone.

Figure 3-45 WLC Interface Configuration Example



WLAN Configuration

The CPwE Identity and Mobility Services architecture applies logical segmentation to the wireless network similar to VLAN segmentation in the wired infrastructure. Cisco WLC is configured with several WLANs to provide separate SSIDs for different user access scenarios, each with its own authentication and authorization policies.

The following steps describe the WLAN configuration on the Industrial WLC.

Step 1 Create a WLAN for Industrial Employees.

a. Select **WLANs** page and create a new WLAN by choosing **Create New** from the drop-down list. The WLANs > New page appears.

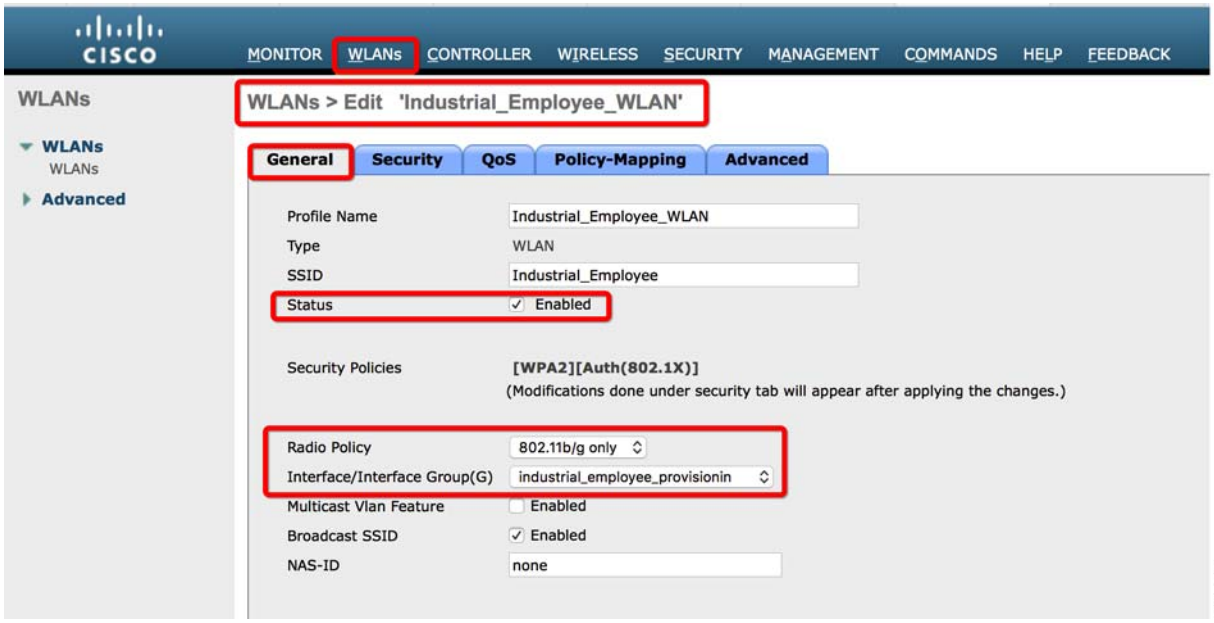
b. Choose **WLAN** from the **Type** drop-down list, assign **Profile Name**, **SSID**, and **WLAN ID**.

c. On the **General** tab, configure **Radio Policy** as defined in the company's RF policy. For example, select 802.11g only to restrict the WLAN to the 2.4 GHz radio or **802.11a/g** to allow both 2.4 GHz and 5 GHz radios.

d. Select the **Interface** in the Industrial Zone where the wireless data will be forwarded in the wired network.

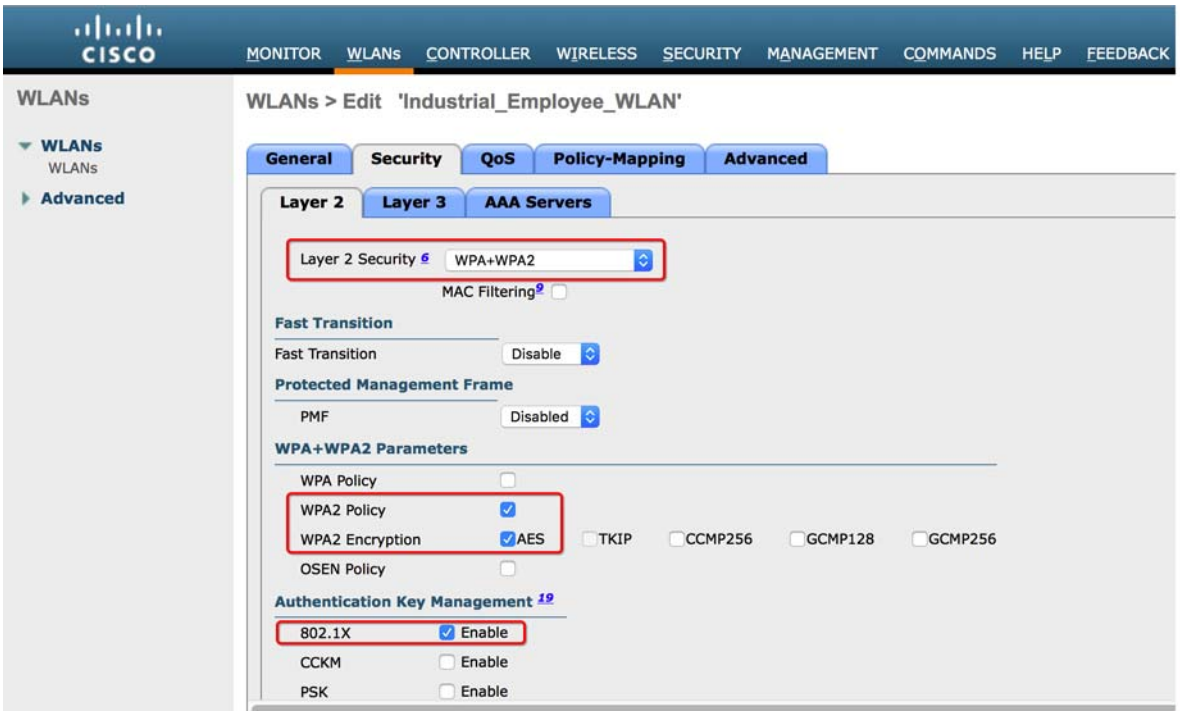
e. Disable or enable **Broadcast SSID** as defined in the company's policy. If all mobile devices are corporate-issued and provisioned ahead of time, the SSID may be hidden. BYOD deployments typically broadcast the SSIDs for provisioning purposes.

Figure 3-46 WLAN General Parameters



f. On the **Security** > **Layer 2** page, configure authentication parameters as shown: **WPA2 Encryption AES** and **802.1X** key management.

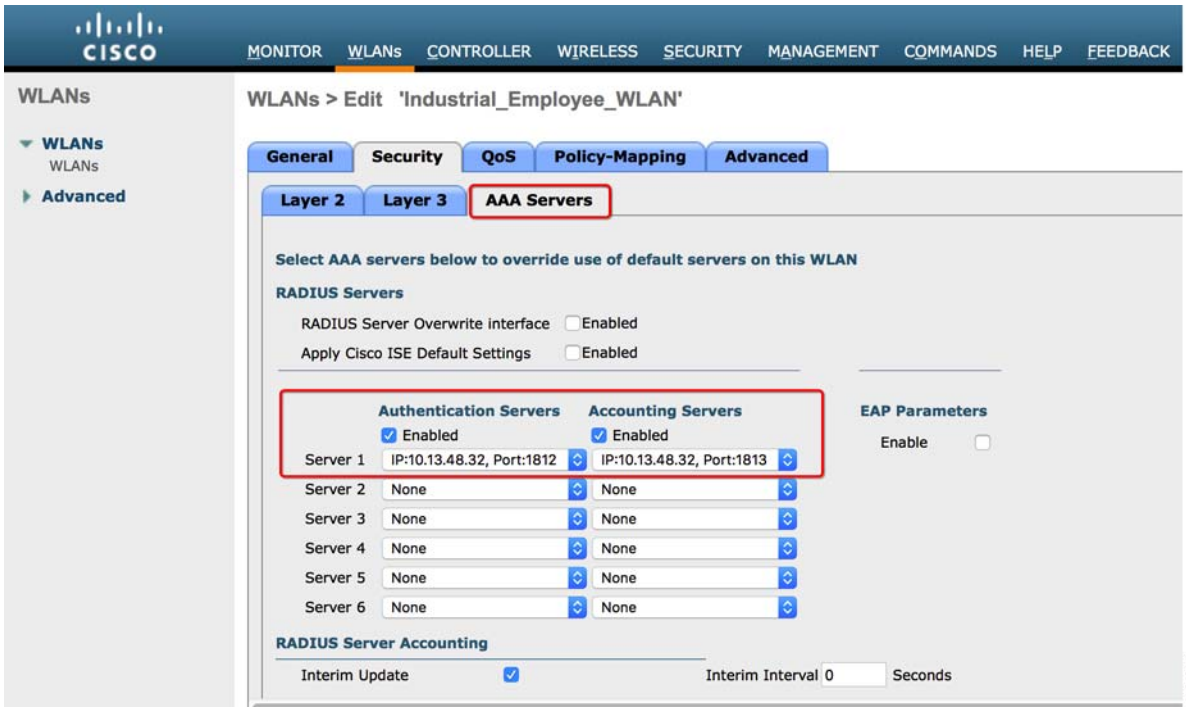
Figure 3-47 WLAN Layer 2 Security



g. On the **Security** > **AAA Servers** page, select the previously configured primary RADIUS server (the Industrial PSN) for both authentication and accounting.

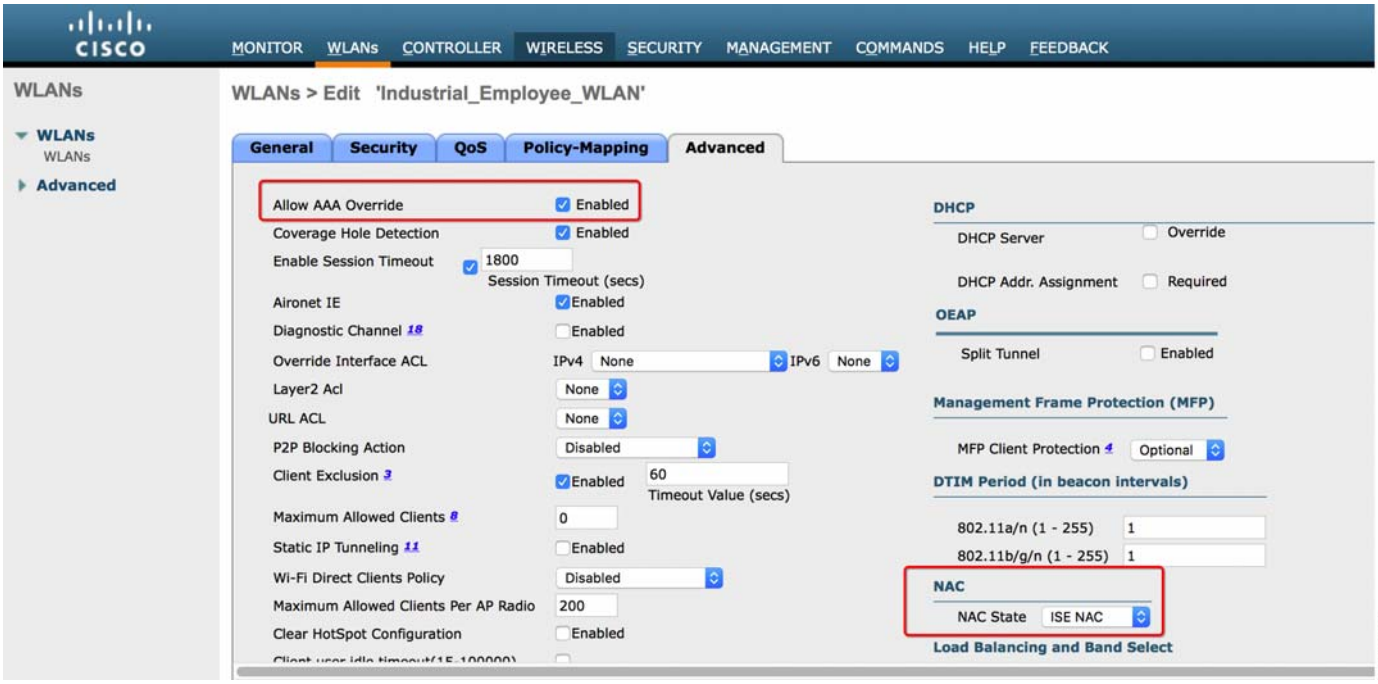
h. Add redundant RADIUS servers (redundant PSNs) if available.

Figure 3-48 WLAN AAA Servers



i. On the **Advanced** page, check **Allow AAA Override** and select **ISE NAC** as the NAC state.

Figure 3-49 WLAN Advanced Parameters



j. Enable the WLAN on the General page. Click **Apply** to commit your changes.

Note The WLAN ID should match the parameter configured in the condition for the Cisco ISE authorization policy. The SSID name should match the name in the Client Provisioning profile for BYOD provisioning (if allowed).

Step 2 Configure WLANs for the Corporate Employee and Trusted Partner (Guest) access.

a. Select the WLC **Management** Interface for the WLAN. The Industrial WLC will establish the EoIP tunnel to the anchor WLC in the Enterprise Zone or Guest DMZ. The user's data will be forwarded to the appropriate IP interface on the anchor WLC.

b. Select the Enterprise PSN as a RADIUS server for these WLANs.

c. Other parameters should remain the same as for Step 1.

ACL Configuration

As part of the authorization policy, an ACL can be applied to the mobile client's data flow. These name-based ACLs are defined on the Industrial WLC and are being using by Cisco ISE in the authorization profiles (called as Airespace ACL).

If the data is forwarded to the anchor WLC, matching ACLs have to be created on both the Industrial and the anchor WLC.

Particular ACL parameters, such as allowed IP addresses and protocols, are specific to the deployment and may vary greatly. The following steps only describe the general steps for the ACL configuration and give an example of a configured ACL on the industrial WLC.

Step 1 Configure an ACL for the restricted access to the Industrial Zone.

a. From **Security** > **Access Control Lists** > **Access Control Lists**, click **New**.

b. Assign the ACL name and click **Apply**.

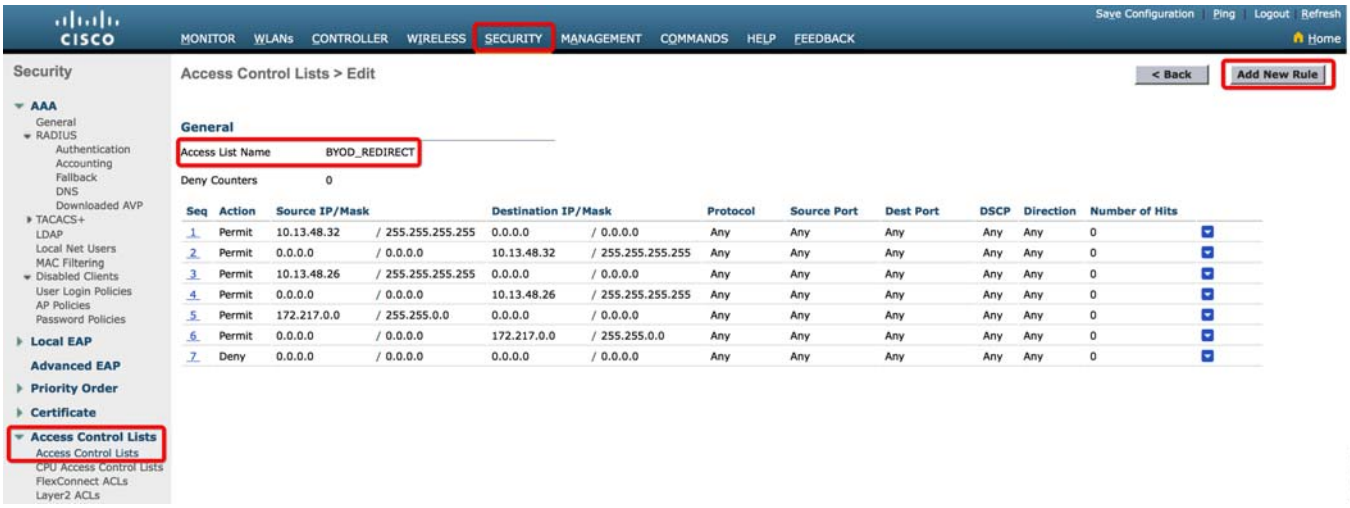
c. Click the newly created ACL name and click **Add new rule**.

d. Configure the rules as needed. Rules must be created for both directions (i.e., with a mobile client as the source and as the destination).

e. Click **Apply** and save the configuration.

Step 2 Configure ACLs for the BYOD redirection to the provisioning portal. An example is shown below. In this case, the user is allowed to access the Industrial PSN, the DHCP server, and the Google Play servers. The actual ACL in a production environment may be more granular and depends on the environment.

Figure 3-50 BYOD Redirect ACL Example



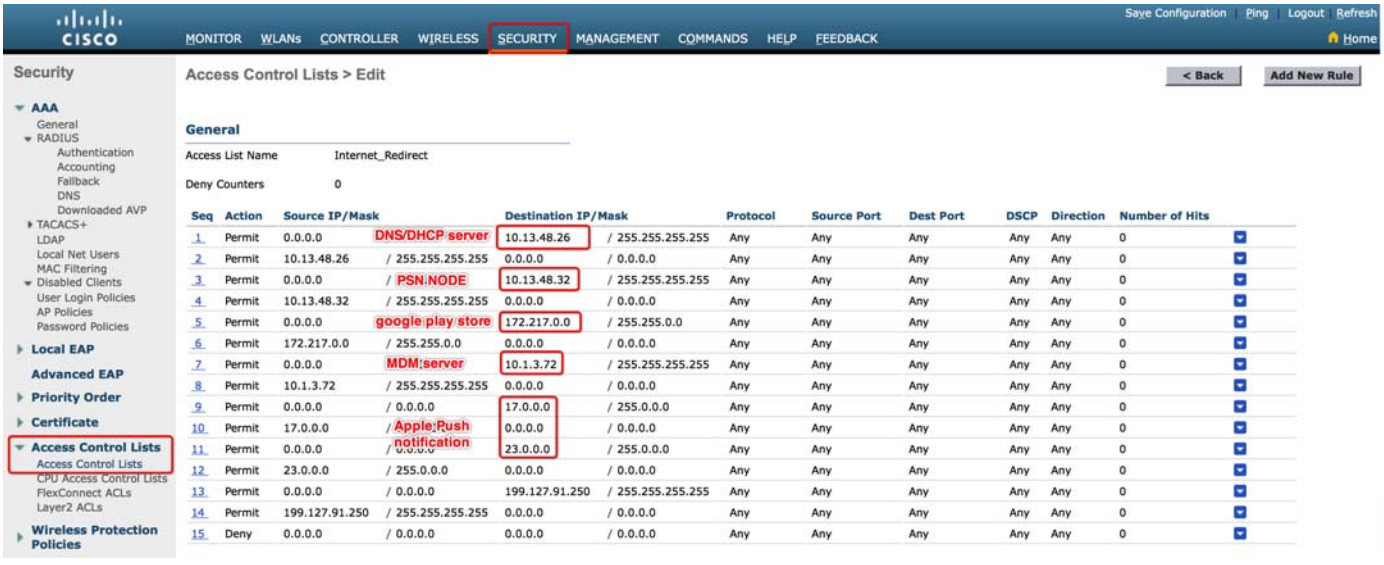
Step 3 Configure ACLs for corporate User access. For example, an ACL may allow access to the Enterprise Zone resources, to the RDG in the IDMZ, and to the reverse web proxies in the IDMZ. The ACL should match exactly the ones configured on the Enterprise anchor WLC.

Step 4 Configure ACLs for trusted partner and guest access. For example, an ACL may allow access to the Internet and to the RDG in the IDMZ. The ACL should match exactly the ones configured on the Guest anchor WLC.

Step 5 If an MDM is deployed in the network, configure an ACL for non-registered devices that allows access to the MDM portal and other necessary resources.

The ACL in the example below allows access to the PSN, the MDM server, Google Play store, Apple and Google servers, as well as DHCP.

Figure 3-51 MDM Redirection ACL Example



Anchor Mobility Configuration

With the auto-anchor mobility feature of Cisco WLC, packets from the wireless client are encapsulated through a mobility tunnel between the Industrial WLC (known as the foreign controller) to the Enterprise or Guest DMZ WLC (known as the anchor controller), where they are de-capsulated and delivered to the wired network.

The following steps describe the mobility configuration on the industrial WLC:

Step 1 Configure the mobility group and its members.

a. From **Controller** > **General**, configure the **Default Mobility Domain Name**. The name of the group may be different from the mobility group name on the anchor WLCs.

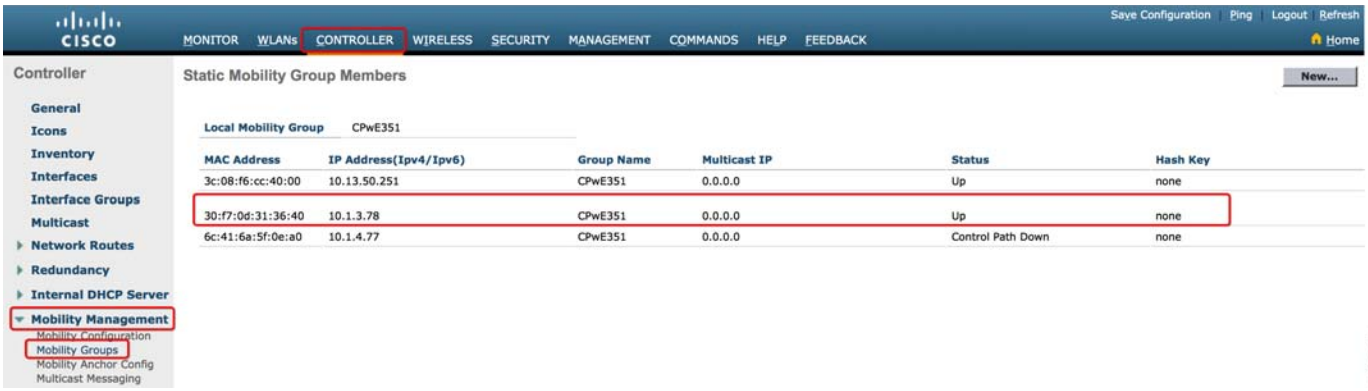
b. From **Controller** > **Mobility Management** > **Mobility Groups**, click **New**.

c. Configure the mobility group name of the Enterprise anchor WLC and the IP and MAC addresses of its management interface.

d. Repeat the steps for the Guest DMZ anchor WLC.

e. Apply the configuration and verify that the status of the mobility members is up. In case of communication issues, verify the IDMZ firewall configuration. The firewall should allow EoIP traffic (IP protocol 97) and CAPWAP traffic (UDP ports 16666, 16667) between the WLCs.

Figure 3-52 Mobility Group Configuration



Step 2 Configure mobility anchor for the WLANs.

a. From **WLAN** page, select the Trusted Partner WLAN, hover your mouse on the **down arrow**, and click **Mobility Anchors**.

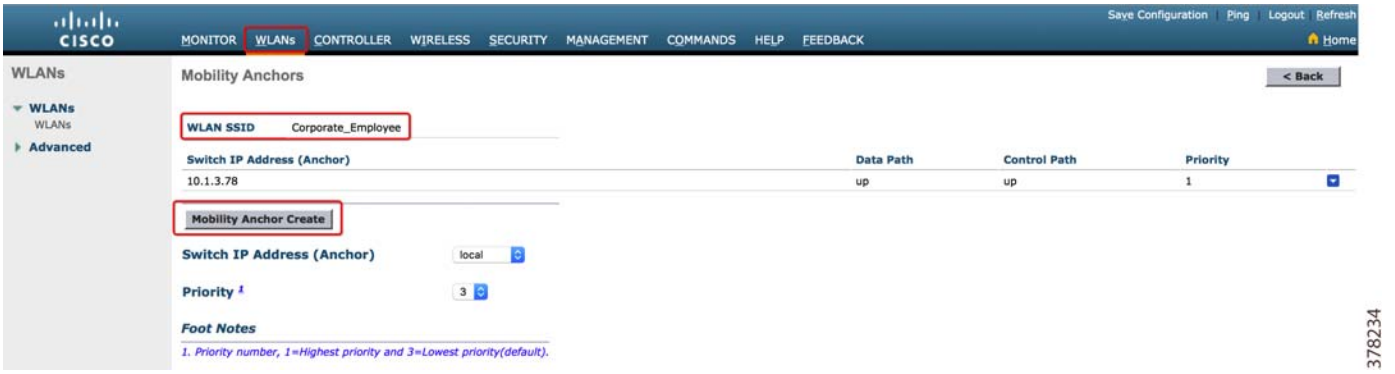
b. Select the IP address of the Guest DMZ WLC as the Switch IP address (Anchor).

c. Click **Mobility Anchor Create**. Click **OK** when a warning appears.

d. Repeat the steps to assign the Enterprise anchor WLC to the Corporate Employee WLAN.

Figure 3-53 Adding Mobility Anchors to WLAN

Figure 3-54 Mobility Anchor Configuration



Guest Anchor WLC Configuration

The CPwE architecture specifies the use of a controller dedicated to wireless traffic from trusted partners and guests to access the Internet. This controller, known as the Guest anchor WLC, is usually located in the Enterprise External DMZ network (the Guest DMZ). The traffic originates on the WLC in the Industrial Zone and is forwarded to the Guest WLC in a secure tunnel.

An EoIP tunnel is established between the Industrial WLC and the anchor WLC in order to help achieve path isolation of trusted partner and guest traffic from the Industrial Zone traffic. Path isolation is a critical security management feature for trusted partner access. It helps to apply separate security policies while maintaining a single WLAN infrastructure in the Industrial Zone for all types of users.

One or more provisioned WLANs (that is, SSIDs) can be mapped to a specific anchor controller within the network. All traffic (both to and from a mapped WLAN) traverses the EoIP tunnel that is established between the Industrial WLC and the anchor WLC.

Configuration steps for the Guest Anchor WLC are similar to the steps described above for the Industrial WLC.

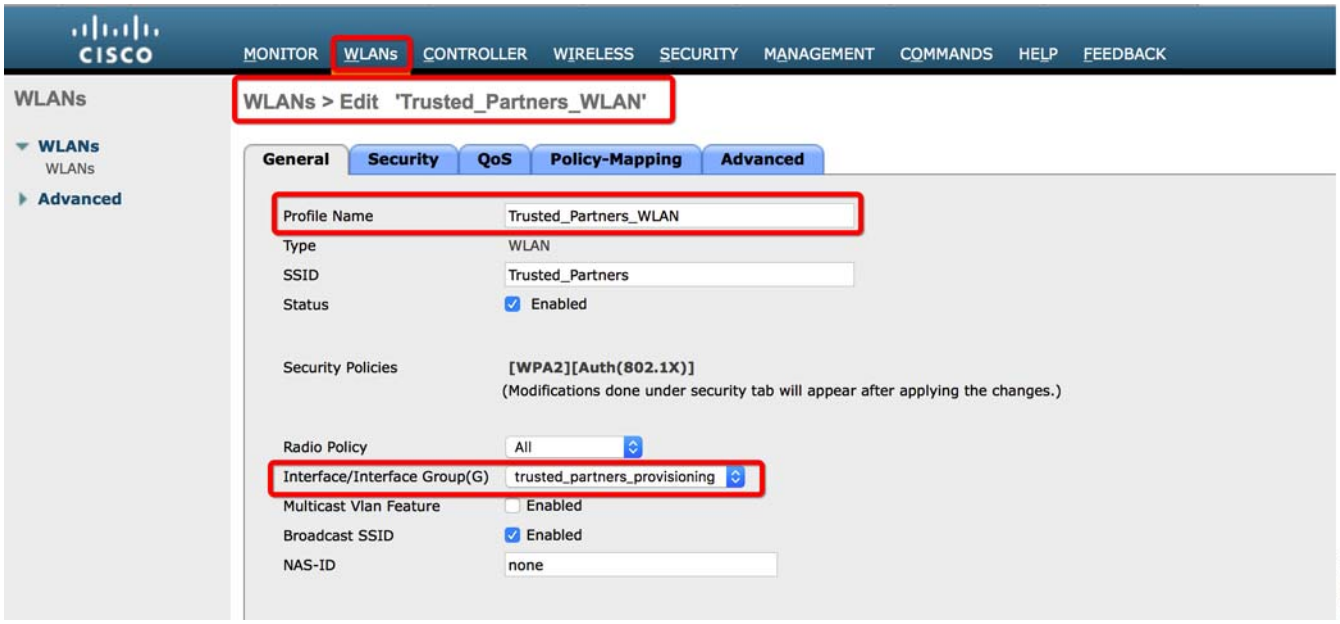
Step 1 Configure the IP interface for the Trusted Partner VLAN in the Guest DMZ.

Step 2 Add Enterprise PSNs to the RADIUS server configuration.

Step 3 Configure the WLAN for the Trusted Partner access that matches the WLAN configured on the Industrial WLC. Assign the interface configured in step 1.

Note Make sure that the WLAN ID matches the number of the Trusted Partners WLAN on the Industrial WLC.

Figure 3-55 Trusted Partner WLAN on the Guest WLC\



Step 4 Configure RADIUS servers for the WLAN as Enterprise PSNs.

Step 5 Configure the mobility group and add the Industrial WLC as a mobility member.

Step 6 Configure the ACL for trusted partner and guest access that matches the one configured on the Industrial WLC for the same purpose.

Step 7 Configure the IDMZ firewalls and the Enterprise DMZ firewalls to allow mobility traffic between WLCs: IP protocol 97 (EoIP) and UDP ports 16666, 16667 (CAPWAP). Make sure to restrict the traffic to the management IP addresses of the WLCs.

Note One of the possible scenarios is to allow trusted partners to access the Remote Desktop Gateway (RDG) in the IDMZ. In this case, both the Enterprise DMZ firewall and the IDMZ firewall should be configured to allow inbound traffic (HTTPS) from the Trusted Partner VLAN to the RDG.

Enterprise Anchor WLC Configuration

The CPwE Identity and Mobility Services architecture allows mobile corporate users to access the Enterprise Zone resources from the plant floor. This is achieved through a dedicated WLC, known as the Enterprise anchor WLC. This WLC may be already deployed by corporate IT for enterprise users and needs to be configured as a mobility anchor to the Industrial Zone. Alternatively, a new WLC may be installed just for this purpose.

Similar to the Guest anchor WLC scenario, the wireless traffic originates on the WLC in the Industrial Zone and is forwarded to the Enterprise WLC in a secure EoIP tunnel.

Configuration steps for the Enterprise Anchor WLC are similar to the steps for the Guest Anchor WLC.

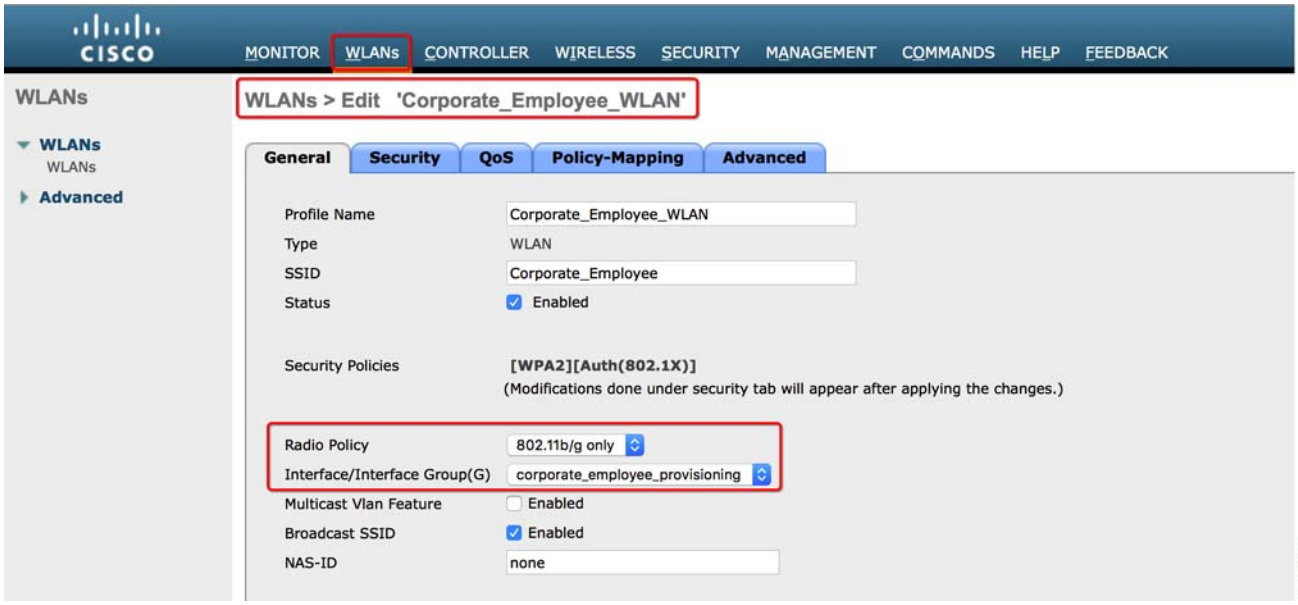
Step 1 Configure the IP interface for the mobile corporate users in the Enterprise Zone.

Step 2 Add Enterprise PSNs to the RADIUS server configuration.

Step 3 Configure the WLAN for corporate user access that matches the WLAN configured on the Industrial WLC. Assign the interface configured in step 1.

Note Make sure that the WLAN ID matches the number of the Corporate User WLAN on the Industrial WLC.

Figure 3-56 Corporate User WLAN on Enterprise Anchor WLC



Step 4 Configure RADIUS servers for the WLAN as Enterprise PSNs.

Step 5 Configure the mobility group and add the Industrial WLC as a mobility member.

Step 6 Configure the ACL for corporate user access that matches the one configured on the Industrial WLC for the same purpose. For example, an ACL may allow access to the Enterprise Zone resources, to the RDG in the IDMZ, and to the reverse web proxies in the IDMZ.

Step 7 Configure the IDMZ firewalls to allow mobility traffic between WLCs: IP protocol 97 (EoIP) and UDP ports 16666, 16667 (CAPWAP). Make sure to restrict the traffic to the management IP addresses of the WLCs.

Note One of the possible scenarios is to allow corporate users to access the Remote Desktop Gateway (RDG) in the IDMZ. In this case, the IDMZ firewall should be configured to allow inbound traffic (HTTPS) from the mobile corporate user VLAN to the RDG.

FlexConnect Architecture Configuration

The CPwE Identity and Mobility Services architecture provides an option to use the FlexConnect WLAN design. Using FlexConnect mode, access points can switch client data traffic locally and perform client authentication locally when their connection to the WLC is lost.

When an endpoint associates to a FlexConnect access point, the access point sends all authentication messages and control data to the WLC. With respect to data packet flows, the WLAN can be in any one of the following modes:

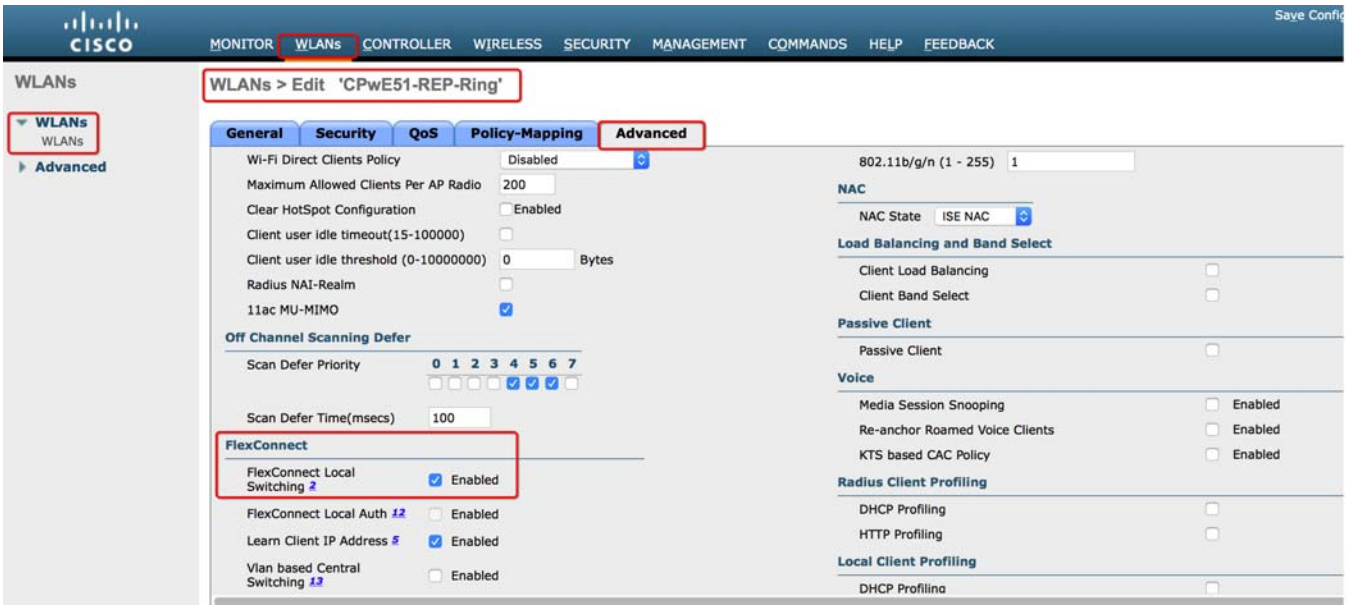
- Central switching—Both the wireless user traffic and the control traffic is sent in the CAPWAP tunnel to the WLC, where the user traffic is mapped to a VLAN interface and forwarded to the switch.
- Local switching—The FlexConnect AP switches data packets locally at the wired interface using VLAN trunking to the access switch.

FlexConnect with local switching can be used for the Industrial Zone wireless access when most of the data flows are directed to the local IACS assets in the Cell/Area Zone. This may be useful in situations when wireless access is provided in remote locations with WAN connectivity to the WLC.

FlexConnect WLAN Configuration

The FlexConnect WLAN configuration is very similar to the Industrial Employee WLAN configuration. The difference is that FlexConnect Local Switching should be configured in the **WLAN** > **Advanced** settings.

Figure 3-57 FlexConnect WLAN with Local Switching



Flex Connect AP Configuration

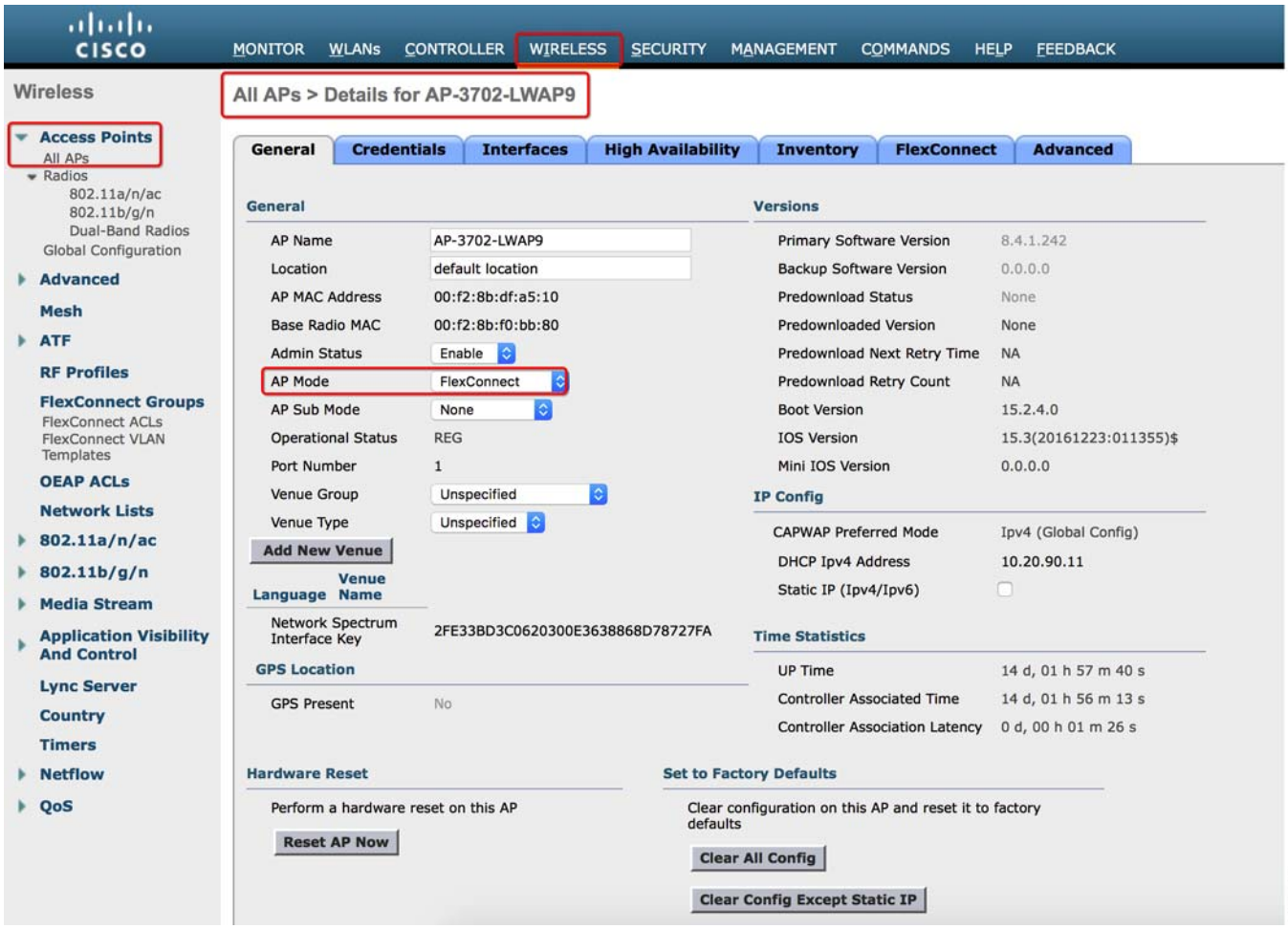
The following steps describe configuration of an AP for FlexConnect mode.

Step 1 Change the AP Mode to FlexConnect.

a. From **Wireless** > **Access Points** > **All APs**, select the AP name.

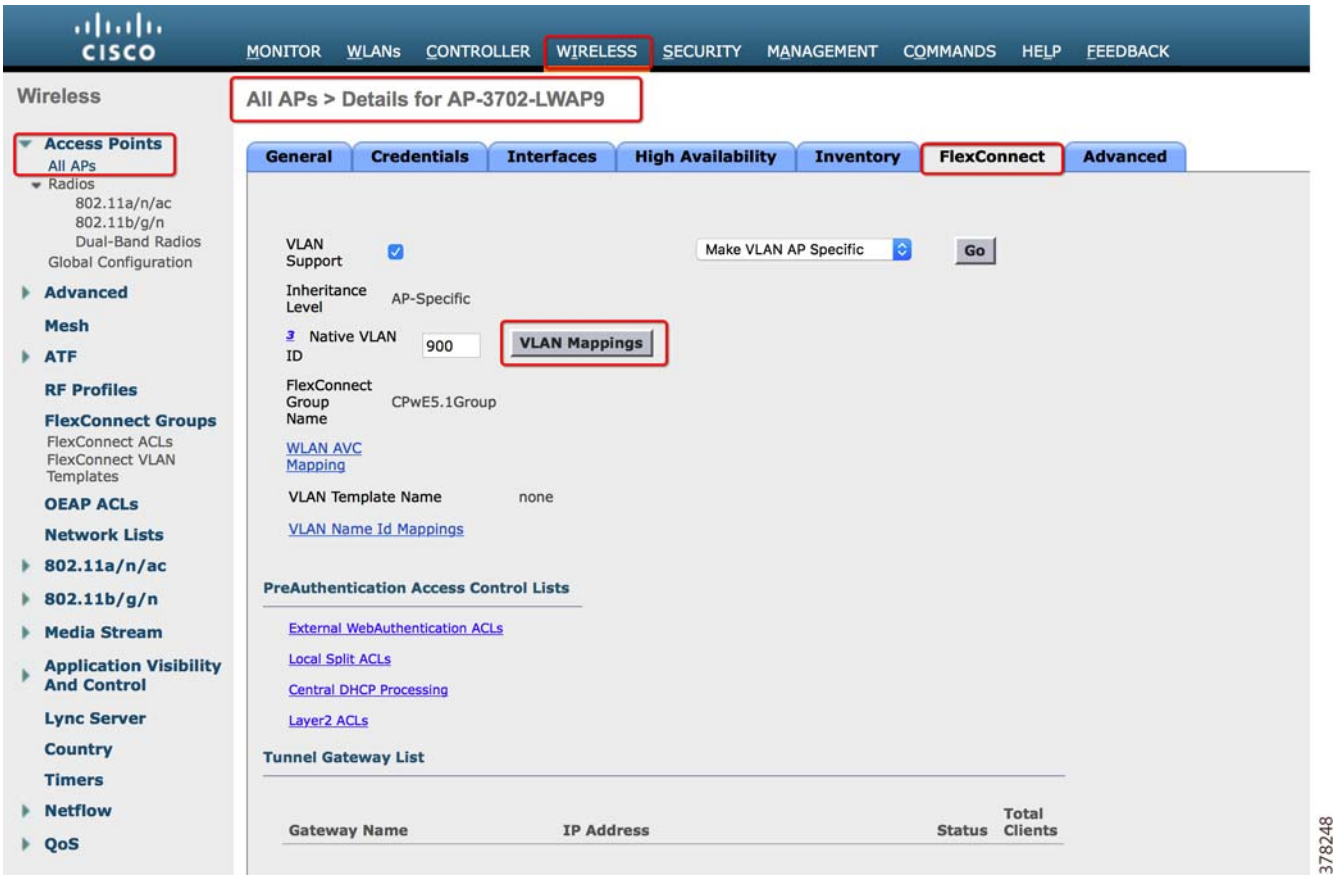
b. Change the AP Mode to **FlexConnect**.

Figure 3-58 FlexConnect AP Mode



Step 2 From the **FlexConnect** tab, specify the Native VLAN for the FlexConnect mode.

Figure 3-59 Native VLAN for FlexConnect

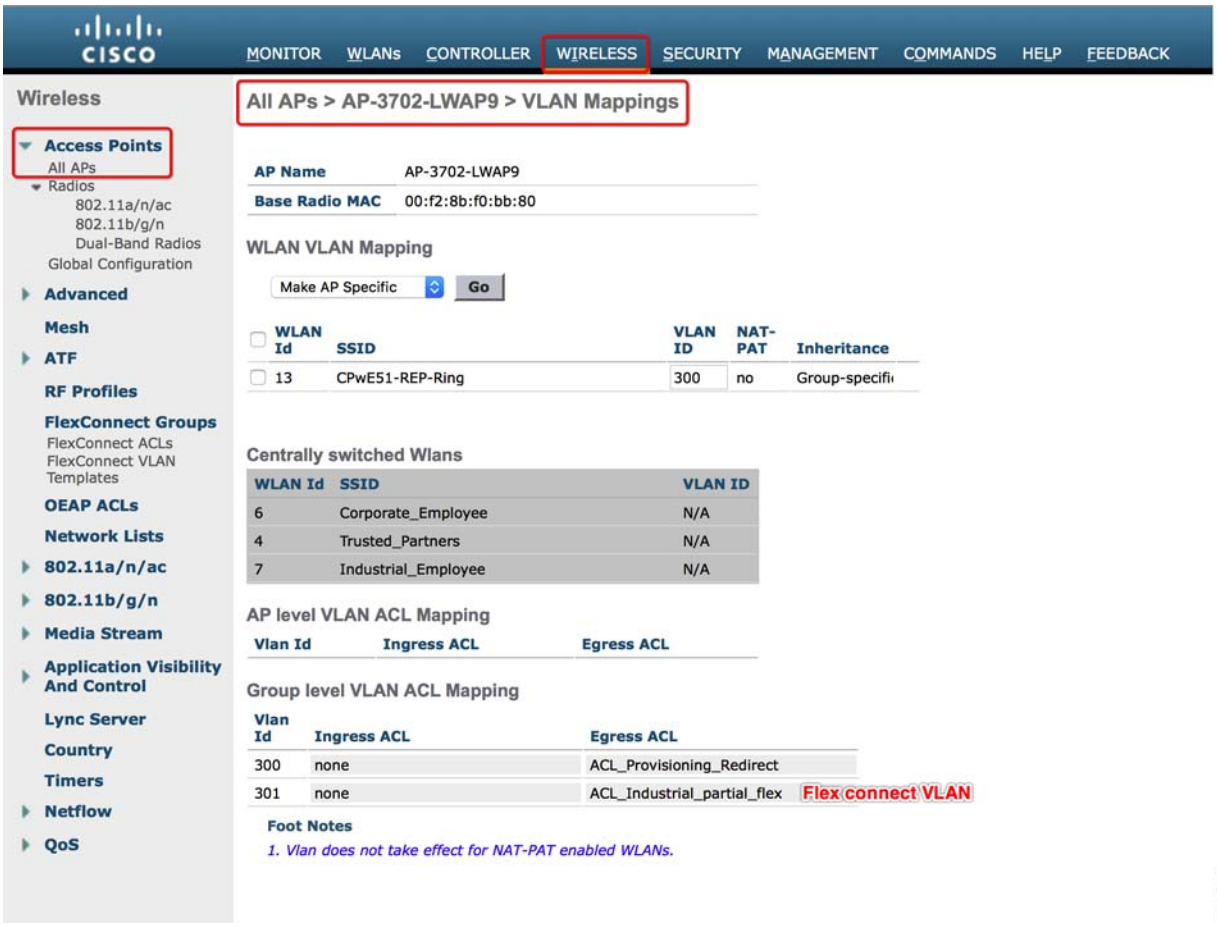


Step 3 Click **VLAN Mapping** and define the VLAN ID to be used for local switching.

In the example below, clients obtain an IP address from VLAN 300 (Provisioning) when doing local switching. When using the AAA Override feature with FlexConnect, the client is moved to a different VLAN dynamically (VLAN 301) based on the matched authorization profile and will obtain an IP address from that VLAN.

The VLAN Mapping settings can be configured at the AP level or the AP can inherit the settings from the FlexConnect Group.

Figure 3-60 FlexConnect VLAN Mapping



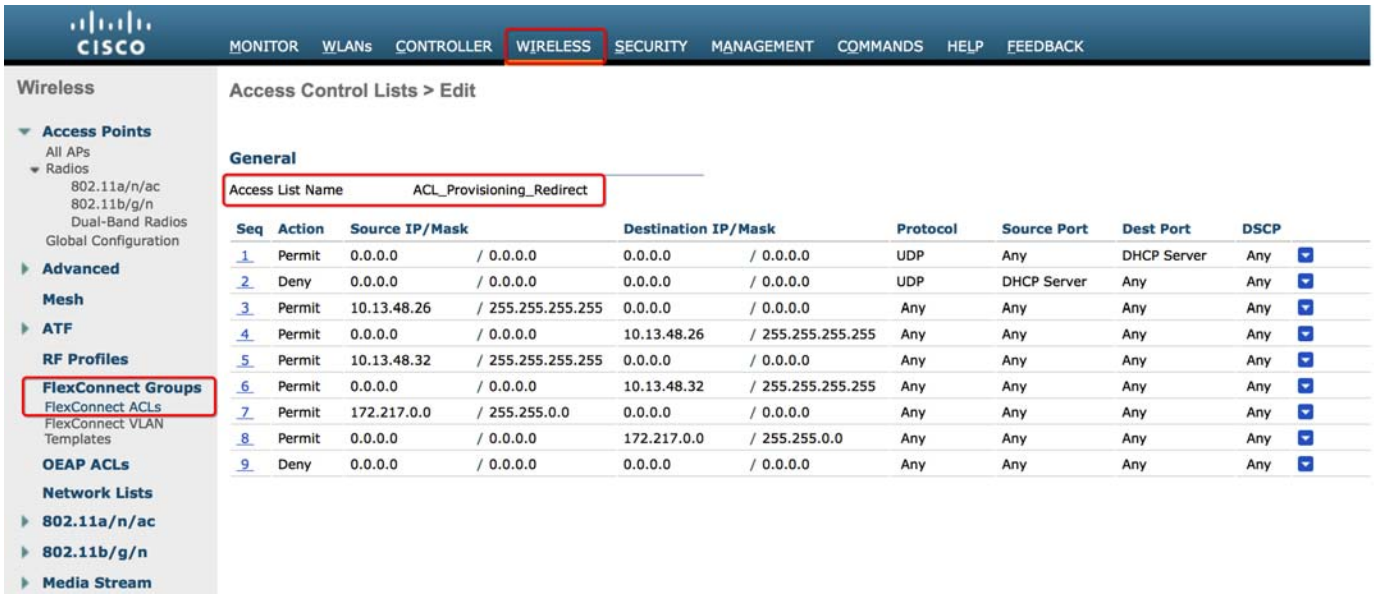
Flex Connect ACL Configuration

ACLs in the FlexConnect mode are applied on the AP level to the ingress and egress traffic. These ACLs are configured similar to the use cases for the centralized mode switching.

Step 1 From **Wireless** > **FlexConnect ACLs**, configure the ACL to enforce the redirection to the BYOD provisioning portal.

In the example below, the ACL allows access to the DHCP server, the Industrial PSN, and to the Google Play servers. The actual ACL in the production environment may be more granular and complex.

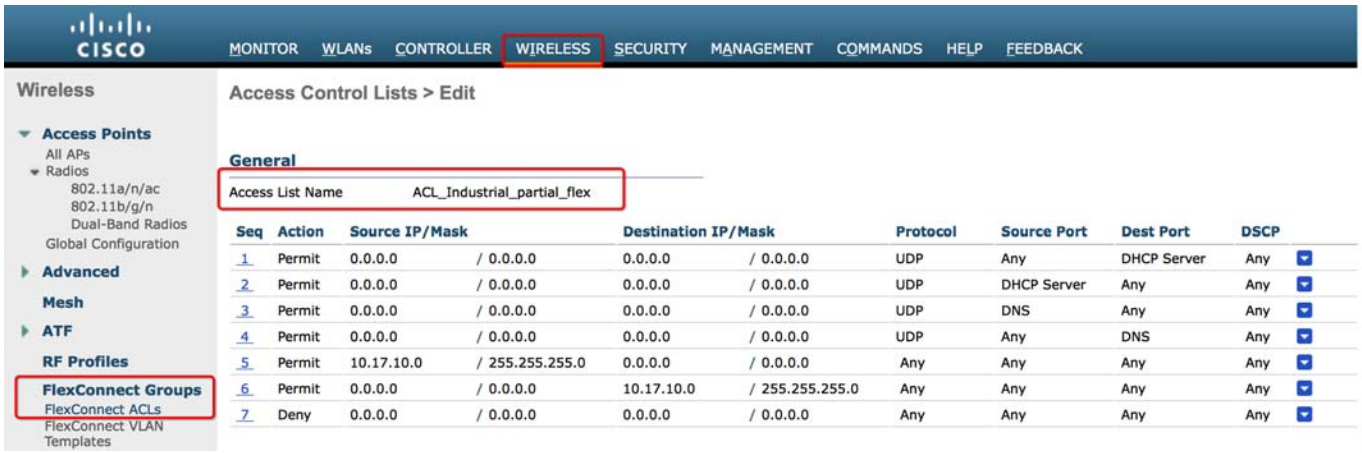
Figure 3-61 FlexConnect ACL Example for BYOD Provisioning



Step 2 Configure the ACL for restricted access to the Industrial Zone (if necessary).

In the example below, access is only allowed to the RAS in Site Operations and to the DHCP and DNS servers.

Figure 3-62 FlexConnect ACL Example for Restricted Access to the Industrial Zone



Autonomous WLAN Configuration

This section describes configuration of the autonomous WLAN within the CPwE Identity and Mobility Services architecture using Allen-Bradley Stratix 5100 APs. To provide security for mobile users, the architecture includes 802.1X authentication with EAP-TLS or PEAP. Cisco ISE authentication and

authorization policies can be developed for small-scale autonomous WLANs. If Cisco ISE infrastructure is not available within the manufacturer's network (or not cost effective to implement), Microsoft NPS can be used as an AAA server to authenticate users.

Autonomous AP Configuration

The autonomous WLAN architecture described in Chapter 2, "CPwE Identity and Mobility Services Design Considerations" provides two SSIDs configured for different level of access, e.g., full access for employees and restricted access for trusted partners. Depending on the requirements, this access model can be extended further.

The Stratix 5100 uses Microsoft NPS or Cisco ISE as a RADIUS server to authenticate the user. Based on the user group and the SSID, the access is granted or denied. In the case of the trusted partner SSID, a static ACL is applied to the radio interface.

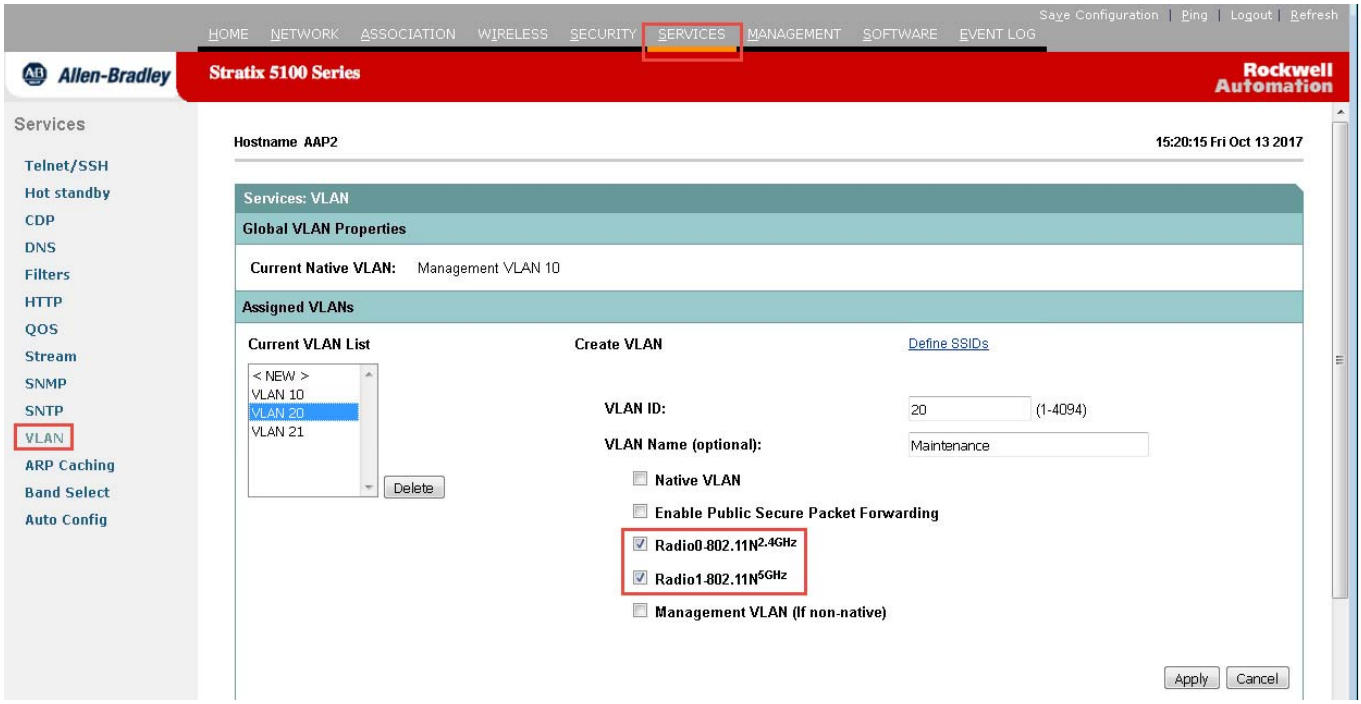
The main steps to configure the Stratix 5100 AP in this scenario are provided below. It is assumed that initial installation steps have been completed for the AP.

Note The complete configuration guide for the Stratix 5100 can be found here: http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um006_-en-p.pdf

Step 1 Configure VLANs on the AP.

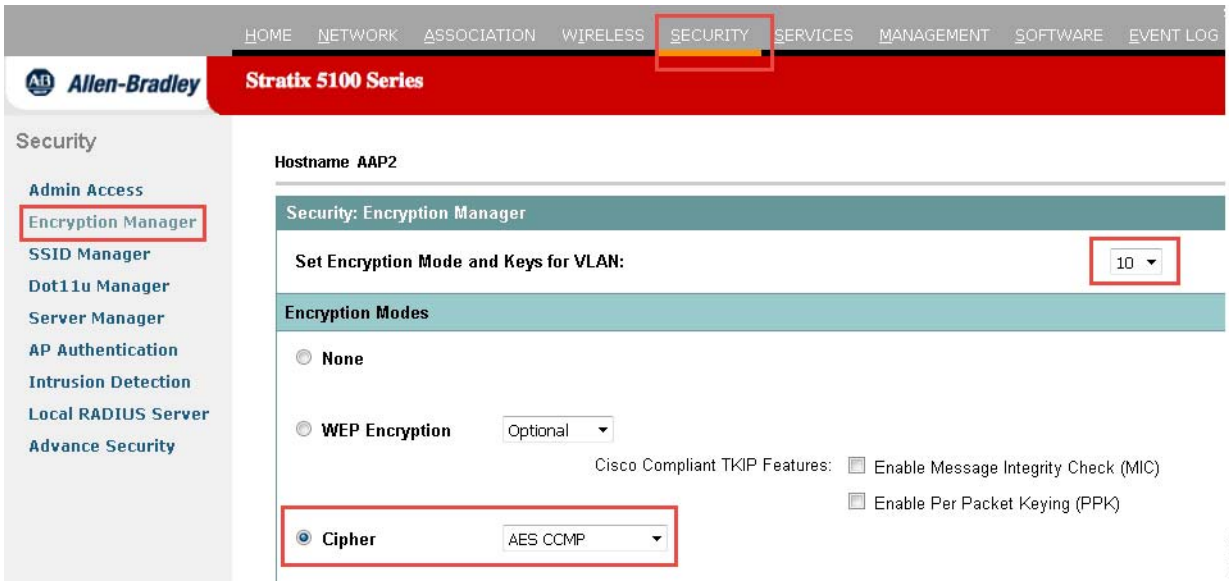
a. From **Services** > **VLAN**, create necessary VLANs for different groups of users, for example Engineers and OEM VLAN. Assign VLANs to the 2.4 GHz or 5 GHz radios or both depending on the RF policy.

Figure 3-63 Allen-Bradley Stratix 5100 VLAN Configuration



b. From **Security** > **Encryption Manager**, configure encryption for each user VLAN as **AES CCMP**. Do **NOT** configure any other parameters.

Figure 3-64 Allen-Bradley Stratix 5100 Encryption Configuration

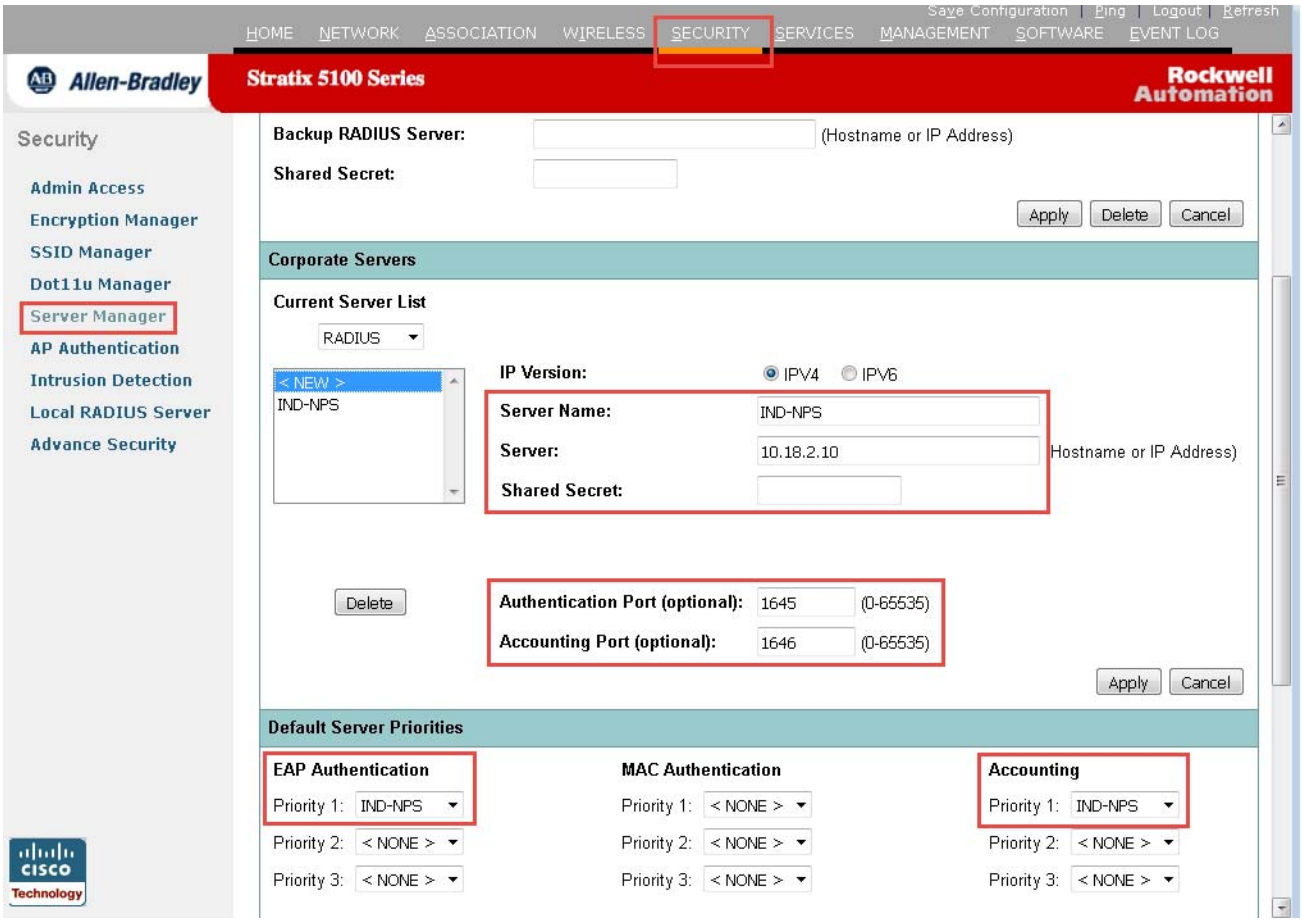


Step 2 Configure RADIUS parameters.

a. From **Security** > **Server Manager**, add the primary RADIUS server name and IP address. Make sure that TCP ports for RADIUS communication match what is configured on the server (Cisco ISE or Microsoft NPS).

b. In the **Default Server Priorities**, assign the server name as first priority for **EAP Authentication and Accounting**.

Figure 3-65 Allen-Bradley Stratix 5100 RADIUS Configuration



c. Repeat the steps above to add redundant RADIUS servers (if available).

d. If the Stratix 5100 AP name is to be used as a condition by the RADIUS server (for example, to use the AP location in the authorization rule), apply this CLI command:

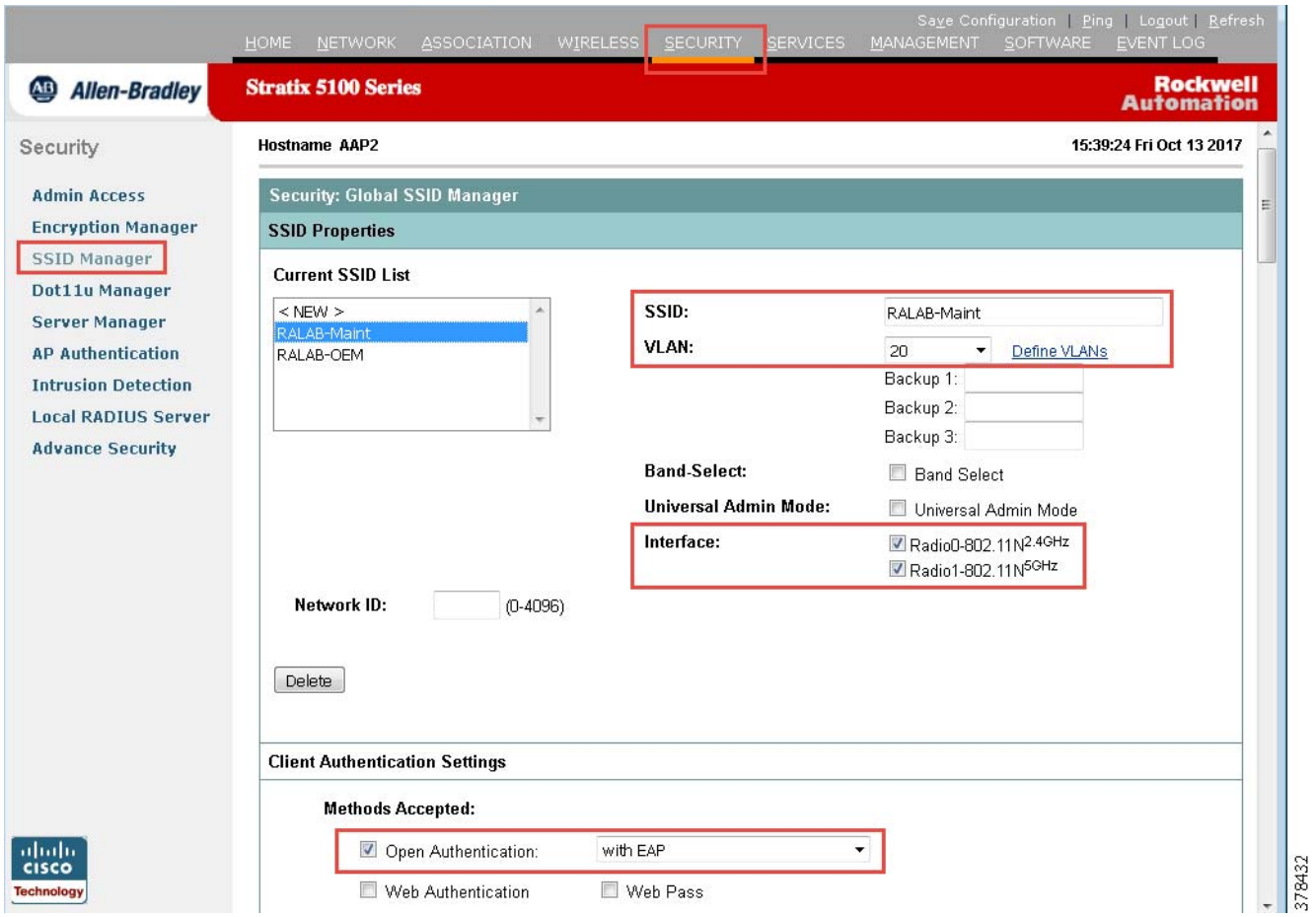
```
radius-server attribute 32 include-in-access-req format %h
```

Step 3 Configure SSIDs for each user group.

a. From **Security** > **SSID Manager**, create an SSID matching each user VLAN. Assign to radio interfaces as defined by the RF policy.

b. In the **Client Authentication Settings**, select **Open Authentication with EAP**.

Figure 3-66 Allen-Bradley Stratix 5100 SSID Configuration

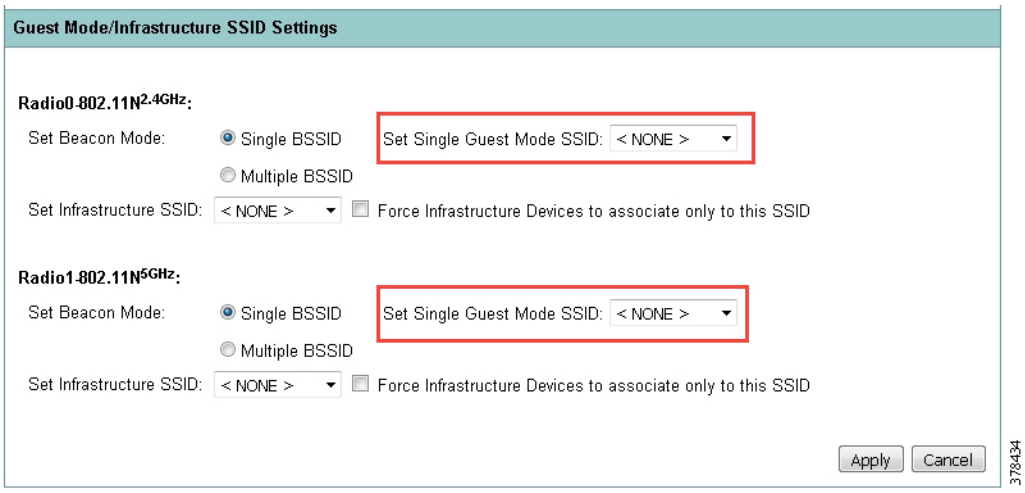


c. Configure **Key Management** as **Mandatory** with **WPAv2**.

Figure 3-67 Allen-Bradley Stratix 5100 Key Management

d. For additional security, disable SSID broadcast in the **Guest Mode Settings**.

Figure 3-68 Allen-Bradley Stratix 5100 Guest Mode



Step 4 Using the CLI or web interface (**Services** > **Filters** > **IP Filters**), configure the ACL for the restricted user VLAN (if applicable). Apply the ACL to corresponding radio interfaces. An example of an ACL is shown below.

In this example, an OEM user is allowed to access a specific IP subnet in the Industrial Zone, as well as DHCP and DNS servers. The actual ACL in the production environment may be more complex.

```
ip access-list extended OEM_In
permit icmp 10.20.21.0 0.0.0.255 any
permit udp any any eq bootps
permit udp 10.20.21.0 0.0.0.255 host 10.18.2.10 eq domain
permit udp 10.20.21.0 0.0.0.255 host 10.18.2.11 eq domain
deny   ip any host 10.20.30.1
permit ip 10.20.21.0 0.0.0.255 10.20.30.0 0.0.0.255
deny   ip any any
!
interface Dot11Radio1.21
ip access-group OEM_In in
```

Cisco ISE Configuration for Autonomous WLAN

Cisco ISE authentication and authorization policies for autonomous WLAN are similar to those for the Unified WLAN with the following considerations:

- The Stratix 5100 AP is not able to dynamically assign a VLAN or DACL to the radio.
- The authorization policy, in addition to user credentials or certificate, can be based on the SSID name that the Stratix 5100 AP sends in the RADIUS request.
- The authorization profile can be Permit Access or Deny Access.

An example of authorization rules for users connecting to the Stratix 5100 is:

- If the AD Group = "*Engineers*"

  AND the endpoint is in the *Whitelist* group

  AND SSID name = "*SSID-Engineers*"

  Then Permit Access

- If the AD Group = "*OEM*"

  AND the endpoint is in the *Whitelist* group

  AND SSID name = "*SSID-OEM*"

  Then Permit Access

- Else Deny Access

The SSID name can be passed to the PSN and used in a rule as a Cisco vendor-defined attribute **cisco-av-pair** with the value **ssid=**<*SSID*>.

Microsoft NPS Configuration for Autonomous WLAN

Most manufacturing environments, including medium and small scale companies, already have Microsoft Windows servers deployed in the Industrial Zone as part of the Active Directory services or to support IACS applications. One of the Windows server roles could be the Network Policy Server (NPS) which is the Microsoft implementation of a RADIUS server.

Using Microsoft NPS for 802.1X authentication can be a cost-effective solution for small scale networks where the Cisco ISE platform is not available.

The general steps for configuring Microsoft NPS are provided below.

Note For complete information on the Microsoft NPS, refer to the following URL: https://technet.microsoft.com/en-us/library/cc771347(v=ws.10).aspx

Step 1 Install the NPS role on a Windows server (either on the Industrial DC or a stand-alone server).

Step 2 Create a **Connection Request Policy** for the autonomous WLAN access based on the following conditions and settings.

a. NAS Port Type: **Wireless - IEEE 802.11**

b. Client Friendly Name (optional): <*AP name*> or name pattern expression

c. Authentication methods: use settings in the Network Policy

d. Other conditions as needed by the security policy and procedures

Step 3 Create a **Network Policy** for each user group and SSID.

a. NAS Port Type: **Wireless - IEEE 802.11**

b. Client Friendly Name (optional): <*AP name*> or name pattern expression

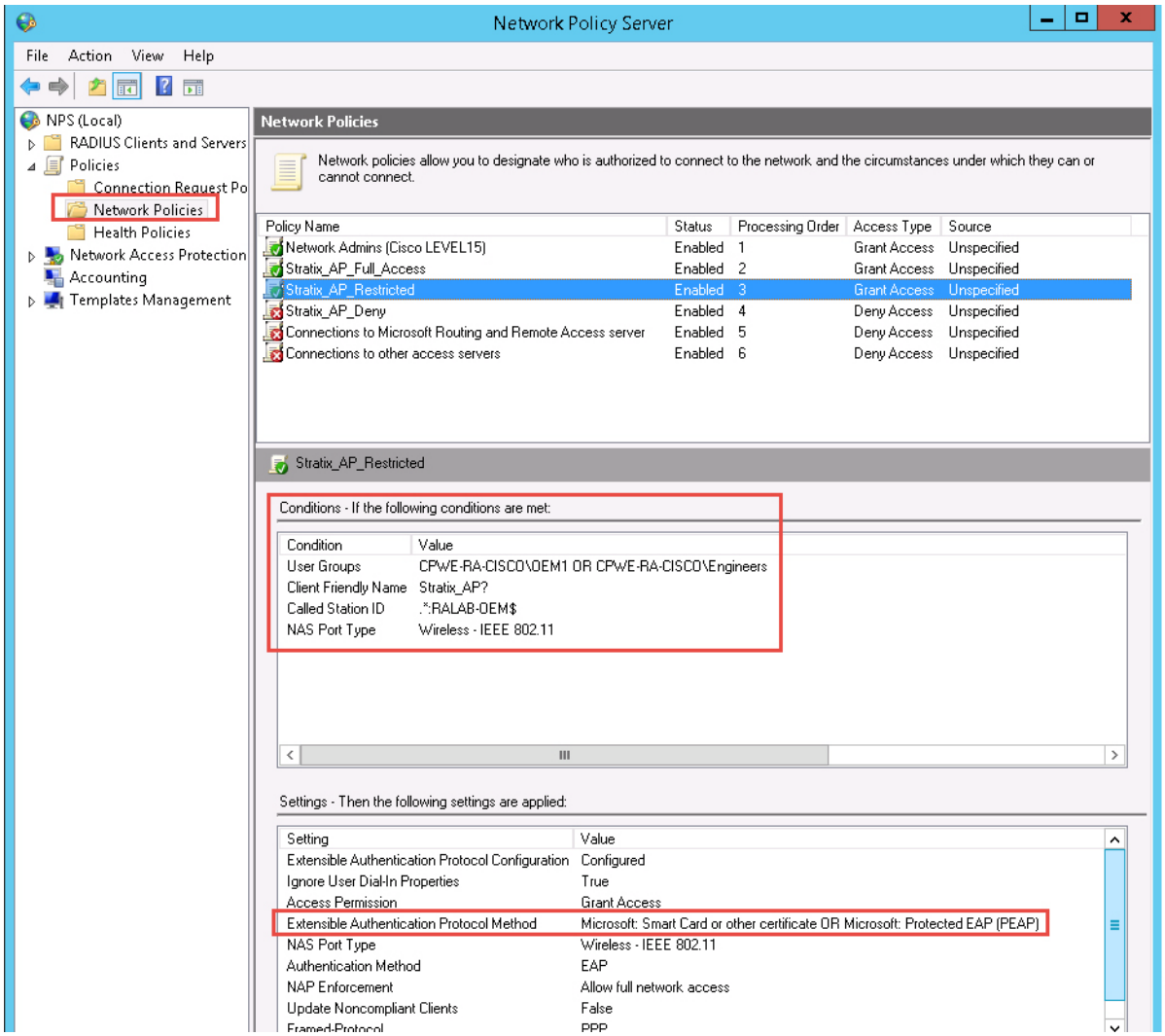
c. User Groups: <*AD Group*>

d. Called Station ID: ***.*:**<*SSID name*>**$**

e. Authentication methods: Certificate or PEAP

f. Other conditions as needed by the security policy and procedures

Figure 3-69 NPS Policy Example



Wired Access Configuration

This section describes the configuration for wired access in the Industrial Zone using 802.1X authentication with Cisco ISE and the IES. The following configuration steps are covered in this section:

- Cisco ISE Configuration
- IES Configuration
- Wired Client Configuration

Cisco ISE Configuration for Wired Access

This section describes how to configure Cisco ISE to properly authenticate and authorize wired computers and limit their access to the network.

The following configuration steps are covered in this section:

- Policy Element Configuration
- Authentication Policy Configuration
- Authorization Policy Configuration
- MAC Authentication Bypass (MAB) Configuration

Policy Element Configuration

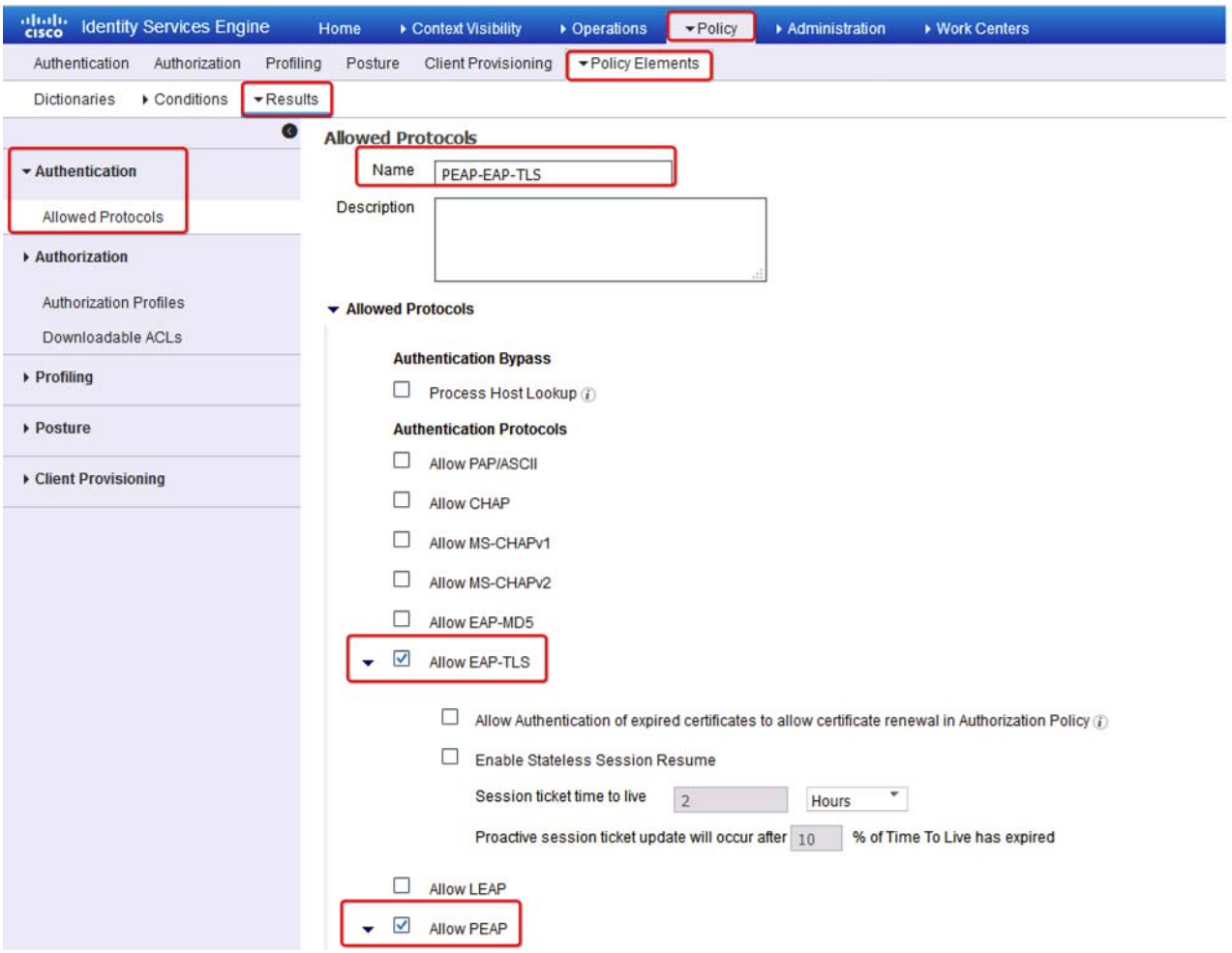
The following steps describe the configuration of authentication and authorization policy elements for wired access.

Step 1 Create the list of allowed authentication protocol services.

a. From **Policy > Policy Elements > Results**, expand **Authentication** in the left pane and select **Allowed Protocols**. Click **Add** to create a separate list for wired access.

b. Fill in the **Name** field and select the check boxes for only the authentication protocols that will be used by wired clients, for example EAP-TLS and PEAP.

Figure 3-70 Allowed Protocols for Wired Access



Step 2 Create the downloadable ACLs (DACL) to be applied to the IES port.

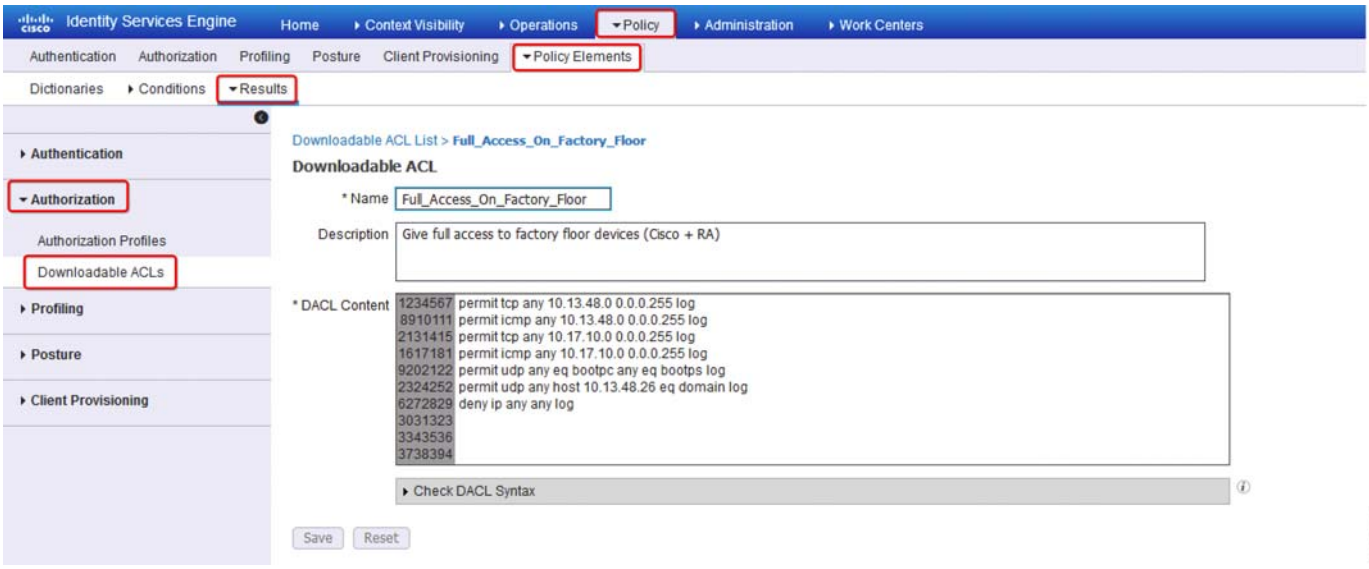
a. From **Policy > Policy Elements > Results**, expand **Authorization** in the left pane and select **Downloadable ACLs.** Click **Add**.

b. Fill in the **Name** field and then add the desired ACL entries in the **DACL Content** area. These ACL entries are defined in the same fashion as in Cisco IOS for switches.

c. To validate the ACL, expand **Check DACL Syntax** and click **Recheck**. Confirm that the returned text is “DACL is valid” and then click **Submit**.

d. Repeat the steps to create multiple DACLs if necessary, for example to restrict an OEM vendor access on the plant floor. Typically a DACL would allow access to the DHCP and DNS servers and the PSN, in addition to the list of approved IACS assets. Domain-joined PCs may need access to the Industrial DC as well.

Figure 3-71 Downloadable ACL Configuration



Step 3 Create an authorization profile to apply to the user session.

a. From **Policy > Policy Elements > Results**, expand **Authorization** and select **Authorization profiles.** Click **Add** to add a profile.

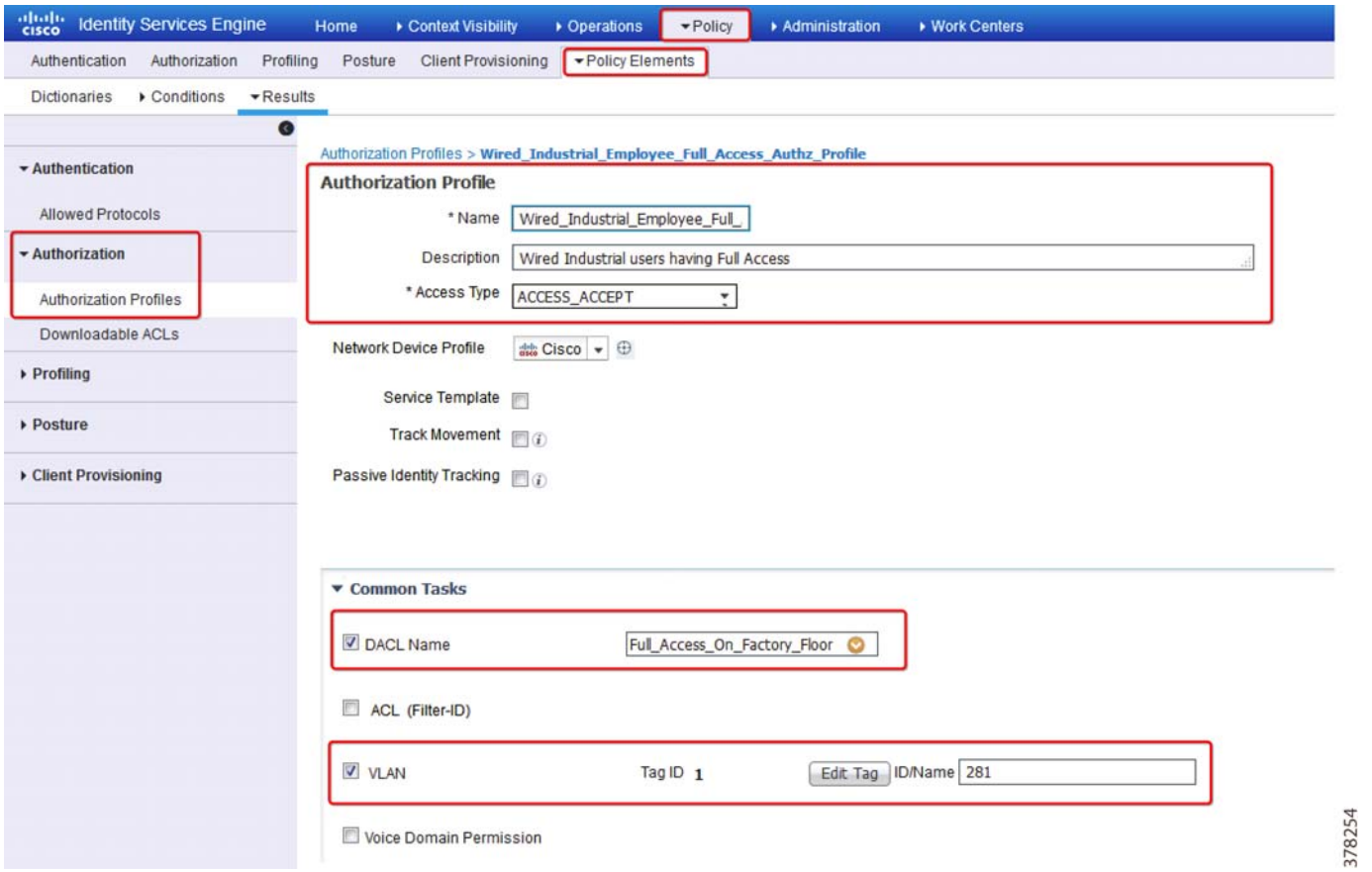
b. Fill in the **Name** field. Choose **ACCESS_ACCEPT** from the **Access Type** menu.

c. Check the **DACL Name** check box to choose a DACL from the drop-down menu.

d. Check the **VLAN** check box and enter the dynamic VLAN number to be applied to the IES port in the RADIUS response. Click **Save**.

e. Repeat the steps to create the necessary profiles for different types of users, for example partial access and trusted partner access.

Figure 3-72 Wired Access Authorization Profile



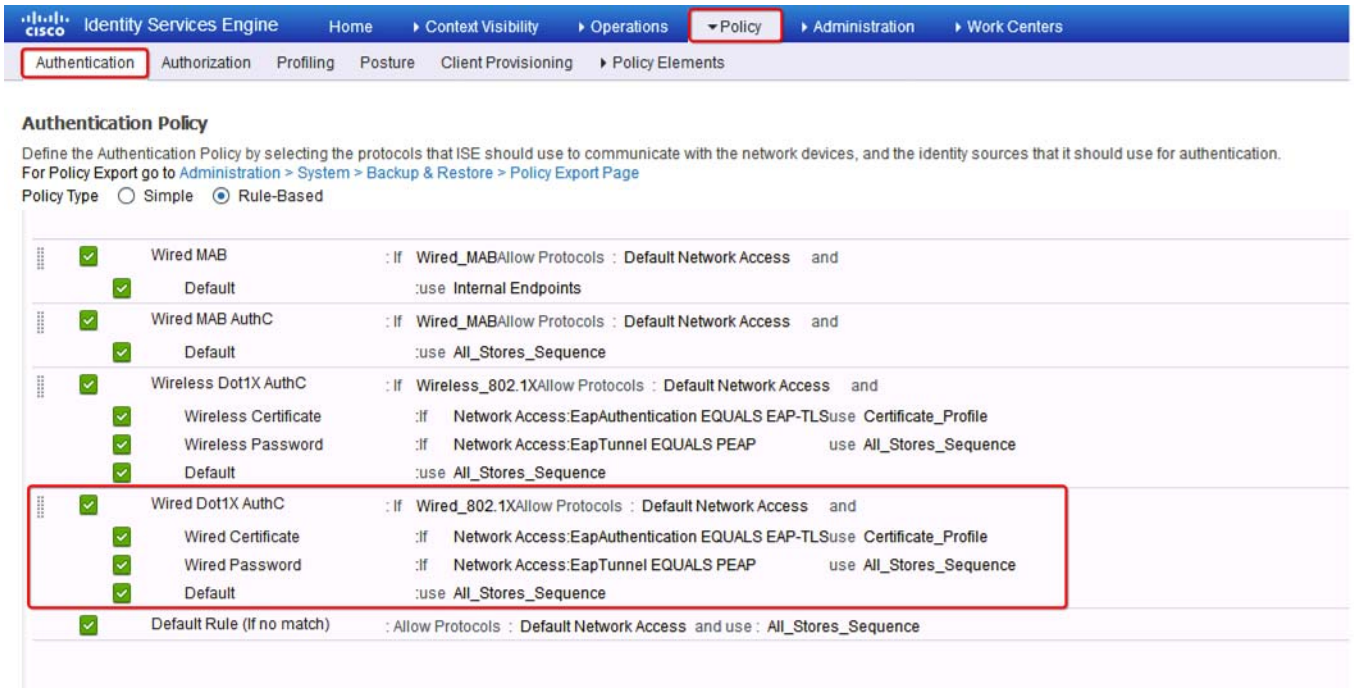
Authentication Policy Configuration

The configuration of authentication policies for wired clients is similar to wireless access.

The example below shows conditions and the resulting identity store parameters:

- If a user access method is wired 802.1X and matches the allowed protocol list, then:
  - For EAP-TLS access (**Wired_Certificate** condition), use the defined certificate profile as the identity source.
  - For PEAP access (**Wired_Password** condition), use the defined AD store.

Figure 3-73 Wired Access Authentication Policy



Authorization Policy Configuration

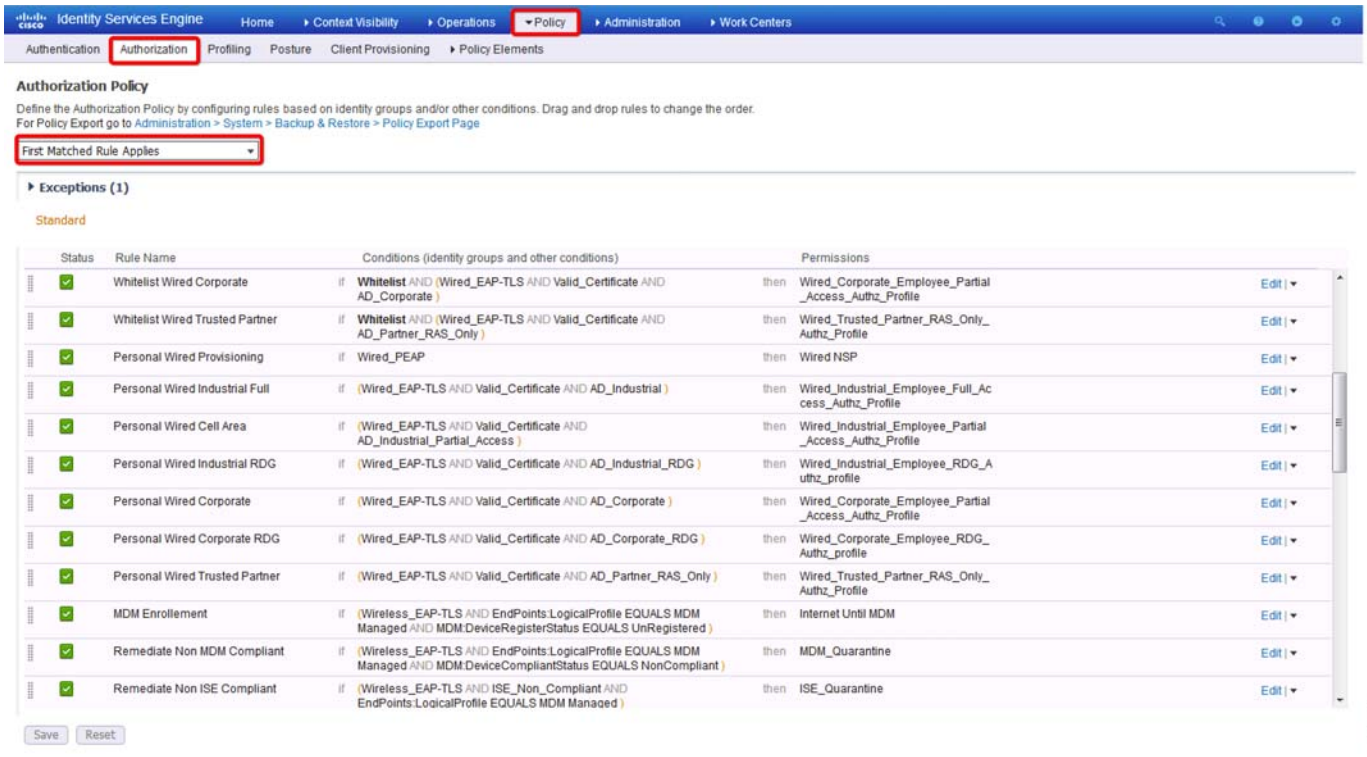
The configuration of authorization policies for wired clients is similar to wireless access. For example, a rule for wired access using a corporate-issued PC can be created to match all of the following conditions:

- The device is in the Whitelist of MAC addresses.
- EAP-TLS protocol is used for authentication.
- The certificate is valid (issued by the trusted authority and not expired or revoked).
- The user belongs to the correct AD group.
- The device is associated to the correct WLAN SSID.

If all conditions in the rule match, the selected authorization profile for wired access will be applied to the user's session.

Below is the example of the authorization policies for wired access that were used to validate the architecture. The actual implementation may vary based on the company's security policy and procedures.

Figure 3-74 Wired Access Authorization Policies



MAC Authentication Bypass (MAB) Configuration

Cisco ISE provides a method to authenticate wired devices in the network by using preconfigured MAC address lists. This is useful to track devices that do not support 802.1X authentication such as most IACS devices as well as printers, phones, and similar assets.

MAB offers the following benefits on wired networks:

- Network visibility for IACS devices since the authentication process provides a way to link a device's IP address, MAC address, switch, and port. This visibility is useful for security audits, network forensics, network use statistics, and troubleshooting.
- Identity-based services based on an endpoint's MAC address, for example, dynamic VLAN assignment and ACL provisioning.
- Fallback or standalone authentication as a complementary method to IEEE 802.1X.

It is critical to understand MAB limitations and security considerations:

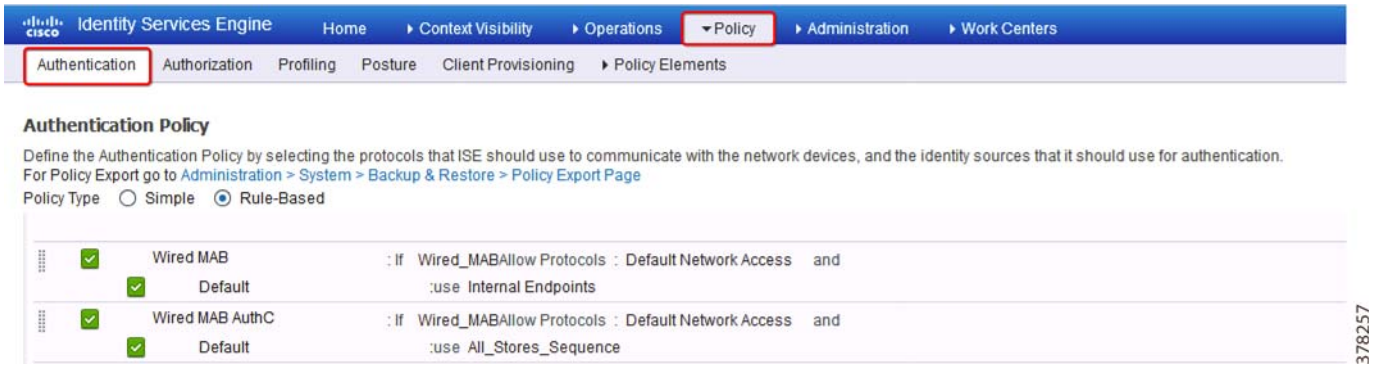
- Creating and maintaining an up-to-date MAC address database can be a challenge in large networks.
- IACS devices may experience a delay when MAB is used as a fallback mechanism to 802.1X since MAB waits for IEEE 802.1X to time out before validating the MAC address.
- MAB can be used to authenticate only devices, not users. Different users logged into the same device will have the same network access.
- Unlike IEEE 802.1X, MAB is not a strong authentication method. MAB can be defeated by spoofing the MAC address of a valid device.

Caution When using MAB with dACL, IP Device Tracking (IPDT) must be enabled on the IES ports. IPDT uses ARP probes to determine the IP addresses of hosts on different ports; this behavior may disrupt IACS devices and applications. The IPDT operation should be configured according to Cisco and Rockwell Automation recommendations and tested with IACS devices and applications. Please refer to IES Configuration for Wired 802.1X for details.

MAB Authentication Profile

An example of the MAB authentication profile is shown below. The Default Network Access list allows authentication bypass for MAB. Cisco ISE will use the internal endpoint list as an identity store.

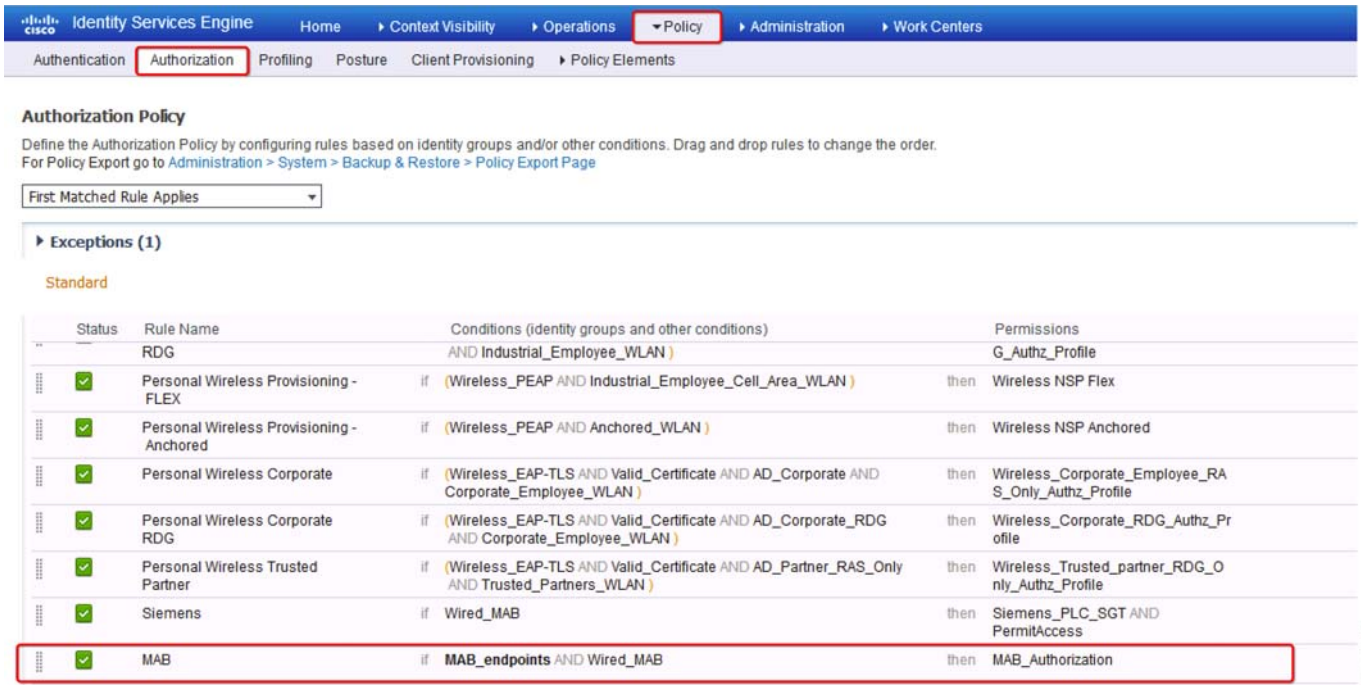
Figure 3-75 Wired MAB Authentication Policy



MAB Authorization Profile

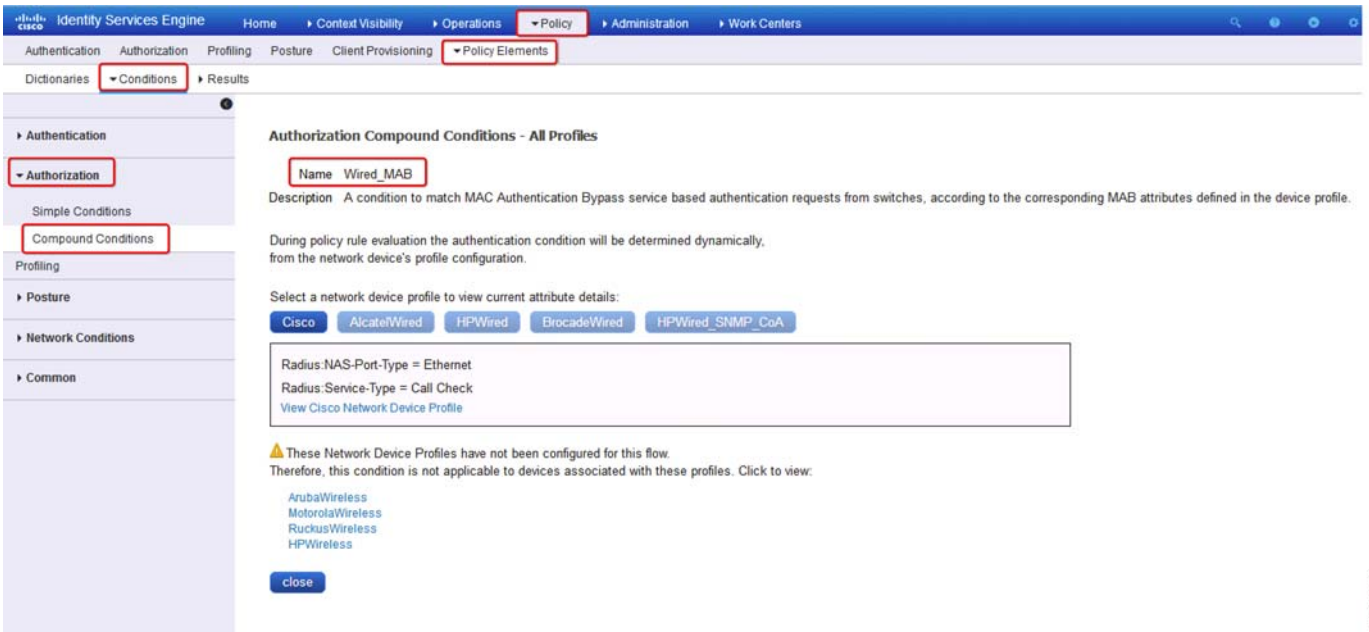
The authorization policy for MAB uses the preconfigured MAC address list (**MAB_Endpoints**) as the condition for the rule and the **Wired_MAB** compound condition.

Figure 3-76 Wired MAB Authorization Policy



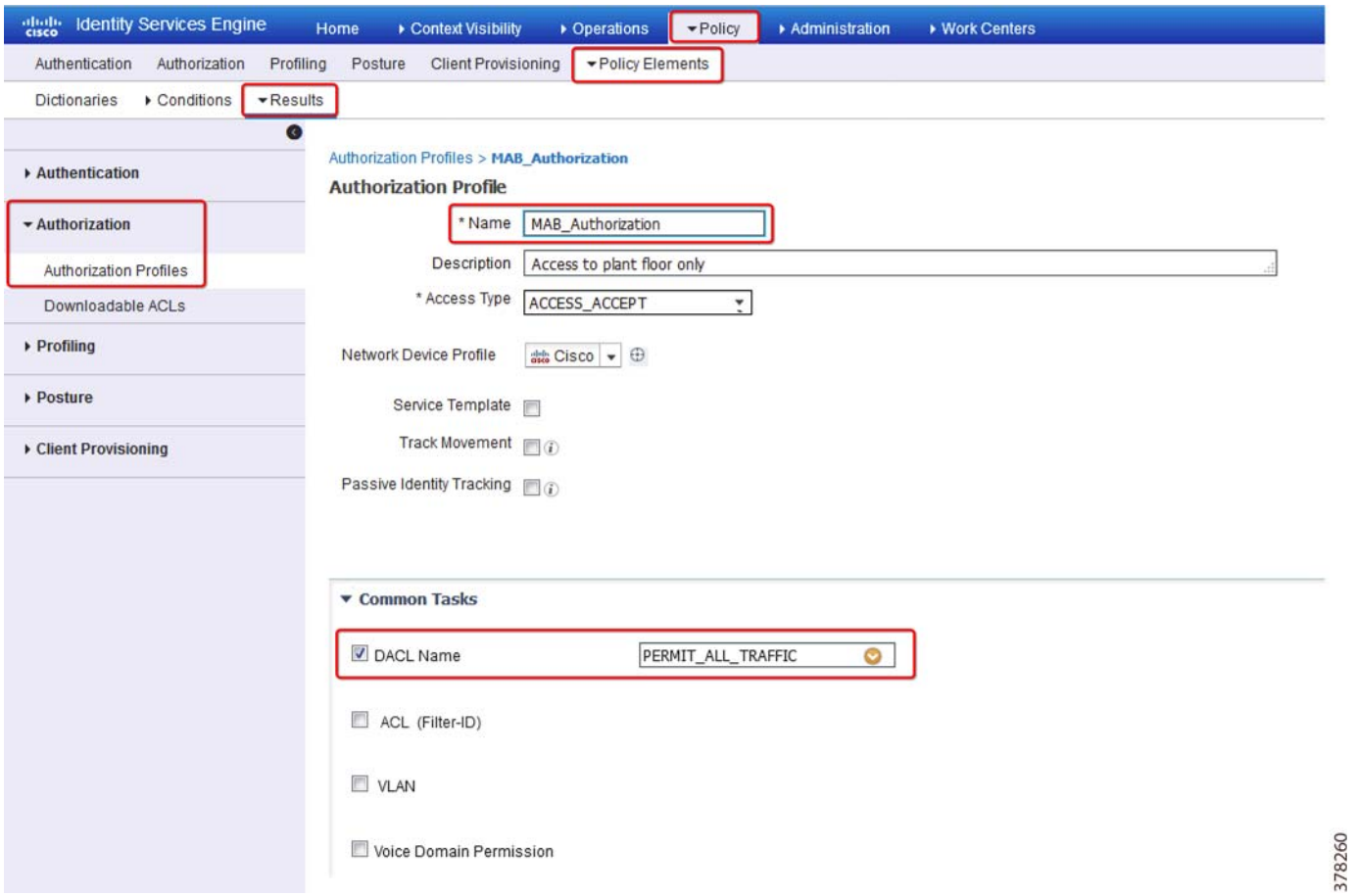
The default **Wired_MAB** compound condition in Cisco ISE is shown below.

Figure 3-77 Wired MAB Condition



The **MAB_Authorization** profile in the example below applies a DACL that permits full access to the Industrial Zone. This DACL can also be used to restrict access for MAB devices based on the company's requirements.

Figure 3-78 MAB Authorization Profile



IES Configuration for Wired 802.1X

This section describes how to configure the IES for 802.1X authentication on the maintenance ports to control and limit wired user access to the network.

The following configuration steps are covered in this section:

- VLAN Configuration
- AAA and RADIUS Configuration
- ACL Configuration
- 802.1X Configuration

The CLI configuration examples are provided for reference only and may have to be modified to match the production environment.

VLAN Configuration

In order to support dynamic VLAN assignment on the switch ports, appropriate VLANs have to be created on the IES. The VLAN numbers must match the ones that are defined in the authorization profiles in Cisco ISE.

Step 1 Using the Device Manager or the global configuration mode in CLI, create the VLANs as defined in the Cisco ISE authorization profiles for wired access, for example:

- VLAN for full access to the Industrial Zone.
- VLAN for partial access to the Industrial Zone (trusted partner access).

Step 2 It is recommended to place RADIUS traffic in a VLAN that is different from the user's data (typically the switch management VLAN) or to create a dedicated VLAN for that purpose.

Step 3 Make sure that newly created VLANs are allowed on the trunks between all switches in the Cell/Area Zone.

Step 4 Add necessary VLANs to the distribution switches in the Cell/Area Zone and create the IP interfaces for the VLANs.

Step 5 Create DHCP scopes on the DHCP servers to assign IP addresses to the users.

AAA and RADIUS Configuration

The following steps describe the AAA and RADIUS configuration on the IES using CLI.

Step 1 Configure the IES for AAA.

a. Enable Authentication, Authorization, and Accounting (AAA) services:

```
aaa new-model
```

b. Configure the server group name to be used for the 802.1X authentication and authorization:

```
aaa authentication dot1x default group <RADIUS_GROUP>
aaa authorization network default group <RADIUS_GROUP>
```

c. Create an accounting method for 802.1X (provides additional information about sessions to Cisco ISE):

```
aaa accounting dot1x default start-stop group <RADIUS_GROUP>
```

d. After enabling AAA services, it is also recommended to configure an authentication and authorization methods for management login to the switch CLI or Device Manager. Several methods may be chosen depending on the requirements:

```
aaa authentication login default {enable|local|group <NAME>}
```

- enable—Authentication using the local enable password on the switch.
- local—Authentication using the local username and password on the switch.
- group—Authentication using RADIUS or TACACS+ server group.

Note For more information on switch-based authentication and AAA services, refer to the following URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie4010/software/release/15-2_4_EC/configuration/guide/scg-ie4010_5000/swauthen.html

Step 2 Configure the Cisco ISE Industrial PSN as the server in the RADIUS group.

```
aaa group server radius <RADIUS_GROUP>
server name <ISE_PSN>
!
radius server <ISE_PSN>
address ipv4 <PSN_IP_ADDRESS> auth-port 1812 acct-port 1813
```

```
key <SHARED_KEY>
!
aaa server radius dynamic-author
client <PSN_IP_ADDRESS> server-key <SHARED_KEY>
!
```

In this example, default UDP ports 1812 and 1813 are used for RADIUS communication. The shared key specifies the authentication and encryption key used between the switch and the RADIUS server. The key is a text string that must match the key used on the PSN for the network device profile.

Step 3 If redundant PSNs are deployed in the Industrial Zone, repeat the above steps for each one of them.

Step 4 Configure other global RADIUS parameters.

a. Configure the RADIUS server retries and timeouts (default is 3 retries with 5 second timeout each).

```
radius-server dead-criteria time 5 tries 3
```

b. Configure the IES to send predefined and Cisco vendor-specific attributes to the RADIUS server:

```
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server dead-criteria time 5 tries 3
radius-server vsa send accounting
radius-server vsa send authentication
```

Step 5 Configure the IP interface to be used as a source of RADIUS messages (typically the switch management VLAN):

```
ip radius source-interface vlan <RADIUS_VLAN>
```

ACL Configuration

The following describes the configuration of the default ACL on the 802.1X-enabled port. Its purpose is to help prevent unauthorized access in certain scenarios.

After the computer is authenticated and authorized by Cisco ISE, if a mistake exists in the syntax of the DACL, the IES rejects the DACL sent by the Cisco ISE. Another situation is when no DACL is sent in the RADIUS response. In this case, the default ACL will be used on the IES to prevent unauthorized access (so called fail closed security mode).

In the example below, the ACL-DEFAULT access list allows DHCP, DNS, and ping traffic. The default ACL may be modified to fit the company's security needs.

```
ip access-list extended ACL-DEFAULT
    permit udp any eq bootpc any eq bootps
    permit udp any any eq domain
    permit icmp any any
    deny ip any any
```

After the user is authorized and a valid DACL is received, the DACL will replace the default ACL on the port for the duration of the wired connection.

802.1X Configuration

The following describes 802.1x configuration on the IES:

Note For complete information on 802.1X port-based authentication, refer to the following URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie4010/software/release/15-2_4_EC/configuration/guide/scg-ie4010_5000/sw8021x.html

Step 1 Enable 802.1X globally on the switch.

```
dot1x system-auth-control
```

Step 2 Apply 802.1X configuration for the desired maintenance port.

a. Enter the interface configuration mode.

```
interface <PORT NUMBER>
```

b. Enable IP device tracking (IPDT) on the port which is required for DACL.

```
ip device tracking maximum 2
```

c. Configure the authentication method priority, order, fail action, and timers.

```
authentication priority dot1x
authentication order dot1x
authentication event fail action next-method
```

d. Configure the violation action (restrict access for additional devices that may fail authentication).

```
authentication violation restrict
```

e. Enable port for 802.1X.

```
dot1x pae authenticator
authentication port-control auto
```

f. Apply the default ACL to the port (required for DACL).

```
ip access-group ACL-DEFAULT in
```

g. Configure the default VLAN on the port for unauthenticated clients.

```
switchport mode access
switchport access vlan <DEFAULT-VLAN>
```

Step 3 In the global configuration mode, configure the IPDT parameters as shown below.

```
ip device tracking probe delay 10
ip device tracking probe auto-source fallback 169.254.26.64 0.0.0.0 override
```

These commands apply workarounds that help to avoid potential issues with IACS applications.

Caution IP Device Tracking (IPDT), which operates in accordance with RFC 5227, must be enabled on the IES to implement RADIUS downloadable ACL. IPDT uses ARP probes to determine the IP addresses of hosts on different ports; this behavior may disrupt IACS devices and applications.
IPDT should **only** be enabled in the following situations on IES ports with 802.1X authentication:
—Maintenance ports and/or designated non-IACS equipment ports
—IACS ports with MAC Authentication Bypass if DACL is required by the security policy, with proper IPDT workaround applied and tested with IACS devices and applications
By default, IPDT should **not** be enabled on ports connected to IACS devices and applications if DACL functionality is not required.
Please refer to the URLs below for more details and IPDT workarounds:

—https://rockwellautomation.custhelp.com/app/answers/detail/a_id/568750
—http://www.cisco.com/c/en/us/support/docs/ip/address-resolution-protocol-arp/118630-technote-ipdt-00.html

Wired Client Configuration

Wired clients such as Windows PCs must be preconfigured to use the proper authentication method before they can be authenticated and authorized through a maintenance port with 802.1X.

The general steps for Windows clients are.

Step 1 Configure the PC for the domain and verify that the necessary group policy is applied and security certificates are installed (if EAP-TLS is used in the network).

Step 2 Start the **Wired AutoConfig** service on the PC and change the startup type to **Automatic**.

Step 3 Open the network adapter properties and enable 802.1X authentication mode.

Step 4 Configure 802.1X parameters such as a network authentication mode (certificates or PEAP), whether to validate the RADIUS server certificate, and what trusted CAs to use for validation.

Step 5 Enable single sign-on for authentication to use users' Windows credentials automatically.

Note For guidance on configuring Windows clients for wired 802.1X authentication, refer to the following URL: https://documentation.meraki.com/MS/Access_Control/Configuring_802.1X_Wired_Authentication_on_a_Windows_7_Client

CHAPTER 4

Troubleshooting the Infrastructure

This chapter includes the following major topics:

Cisco ISE Troubleshooting Tips

The following section provides high level troubleshooting information to assist in identifying and resolving problems you may encounter when you use the Cisco Identity Services Engine (ISE).

Note For complete information on Cisco ISE monitoring and troubleshooting tips, refer to the following URL: https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_011001.html

Cisco ISE Processes Check

If the web interface of Cisco ISE cannot be reached or certain services are not working, it may be necessary to check whether Cisco ISE application processes are running properly. In order to do that, log into the CLI using SSH and run the following command:

```
show application status ise
```

An example of the output from the primary PAN is shown below. The output can be compared with the normal operation output and forwarded to Cisco TAC for support. In particular, database processes, AD connector, and the application server should be running.

```
ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          5741
Database Server                        running          96 PROCESSES
Application Server                     running          14541
Profiler Database                      running          7036
ISE Indexing Engine                    running          6828
AD Connector                           running          13502
M&T Session Database                   running          3701
```

```
M&T Log Collector                       running         10544
M&T Log Processor                       running         10453
Certificate Authority Service           disabled
EST Service                             disabled
SXP Engine Service                      disabled
Docker Daemon                           running         666
TC-NAC Service                          disabled
Wifi Setup Helper Container             running         22963
 Wifi Setup Helper Vault                running         35
 Wifi Setup Helper MongoDB              running         14
 Wifi Setup Helper Web Server           running         285
 Wifi Setup Helper Auth Service         running         136
 Wifi Setup Helper Main Service         running         179
 Wifi Setup Helper WLC Service          running         247
pxGrid Infrastructure Service           disabled
pxGrid Publisher Subscriber Service     disabled
pxGrid Connection Manager               disabled
pxGrid Controller                       disabled
PassiveID WMI Service                   disabled
PassiveID Syslog Service                disabled
PassiveID API Service                   disabled
PassiveID Agent Service                 disabled
PassiveID Endpoint Service              disabled
PassiveID SPAN Service                  disabled
DHCP Server (dhcpd)                     disabled
DNS Server (named)                      disabled
```

Troubleshooting User Authentication

This section describes steps to troubleshoot issues with user authentication.

Testing Users for Active Directory Authentication

Testing authentication is useful to troubleshoot authentication and authorization issues for end users. You can use the Test User feature to test Active Directory authentications. The test returns the results along with group and attribute details (authorization information) that can be viewed on the Admin Portal.

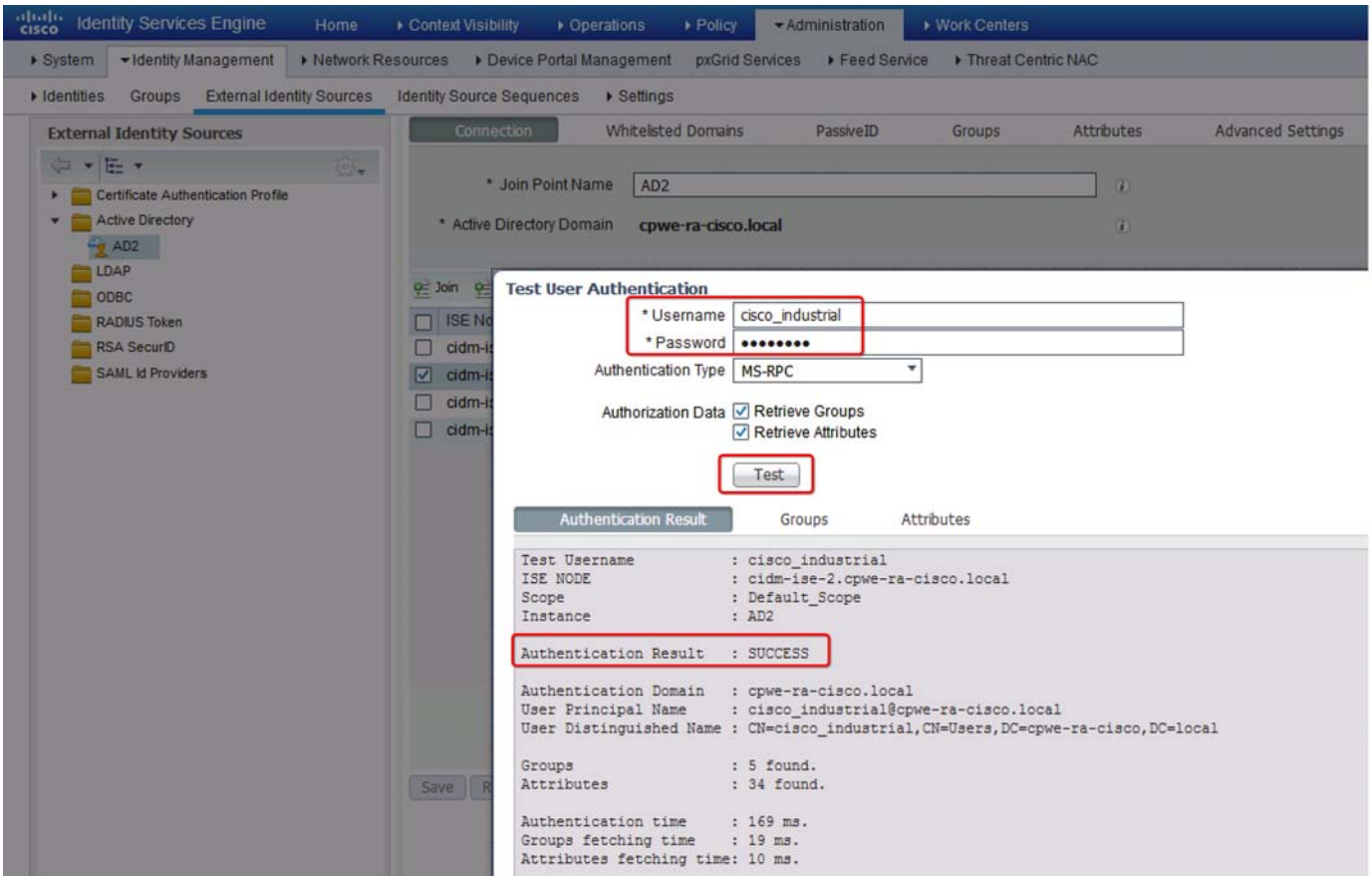
Follow these steps to test users:

Step 1 From **Administrator** > **Identity Management** > **External Identity Stores** > **Active Directory**, click on the AD join point name.

Step 2 Select the Cisco ISE PSN you want to test. Click **Test User**.

Step 3 Enter credentials and click **Test**. Verify the results, the user group, and other details.

Figure 4-1 Test User Authentication



Monitoring Live Authentications

You can monitor recent RADIUS authentications as they happen from the Live Authentications page. The page displays the top ten RADIUS authentications in the last 24 hours. This section explains the functions of the Live Authentications page.

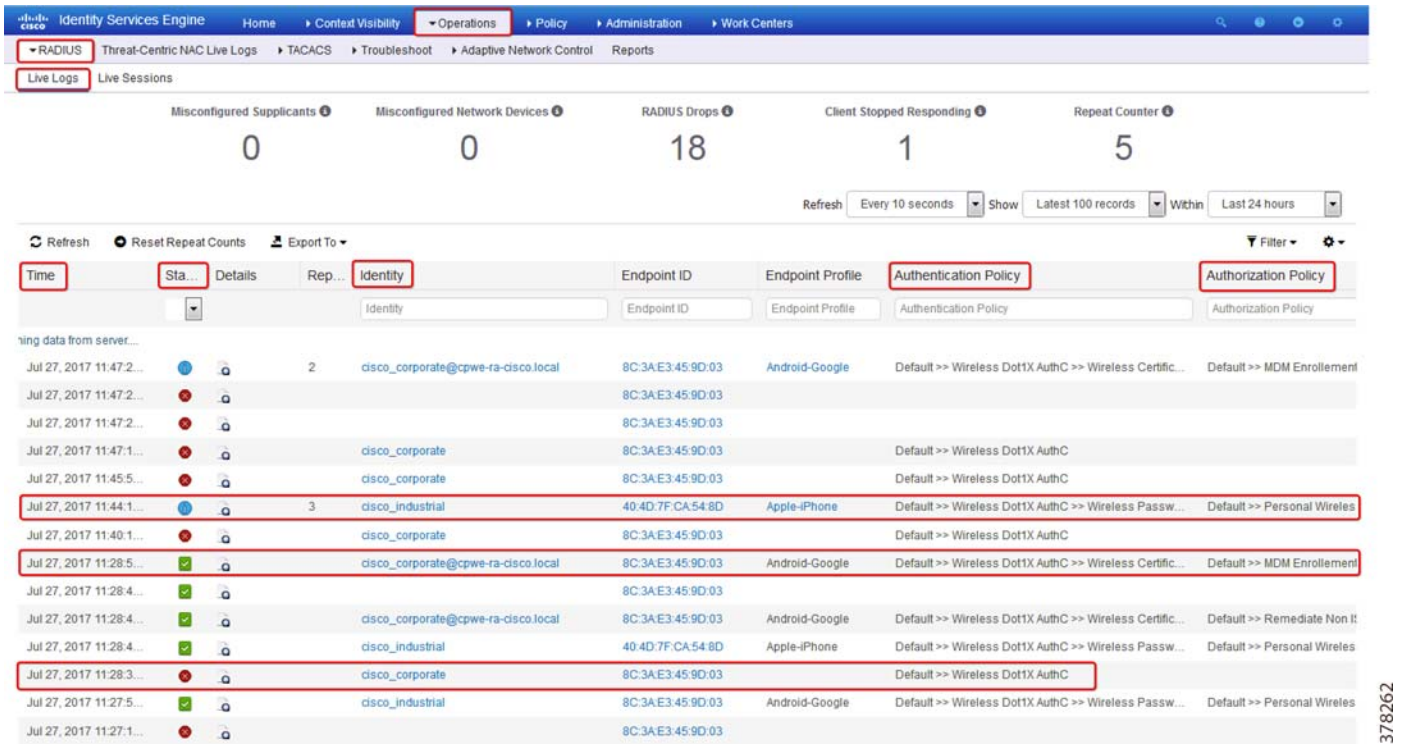
When a single endpoint authenticates successfully, two entries appear in the Live Authentications page: one corresponding to the authentication record and another corresponding to the session record (pulled from session live view).

Subsequently, when the device performs another successful authentication, the repeat counter corresponding to the session record is incremented. The Repeat Counter that appears in the Live Authentications page shows the number of duplicate radius authentication success messages that are suppressed.

To monitor authentication logs in real time, choose **Operations** > **RADIUS Live Logs**.

The logs show details such as user identity, endpoint MAC address and profile (OS type), matching authentication and authorization policy, and many others. Clicking on the **Details** icon provides very detailed information about the current user session and RADIUS steps, as well as reasons for rejected access.

Figure 4-2 Live RADIUS Logs



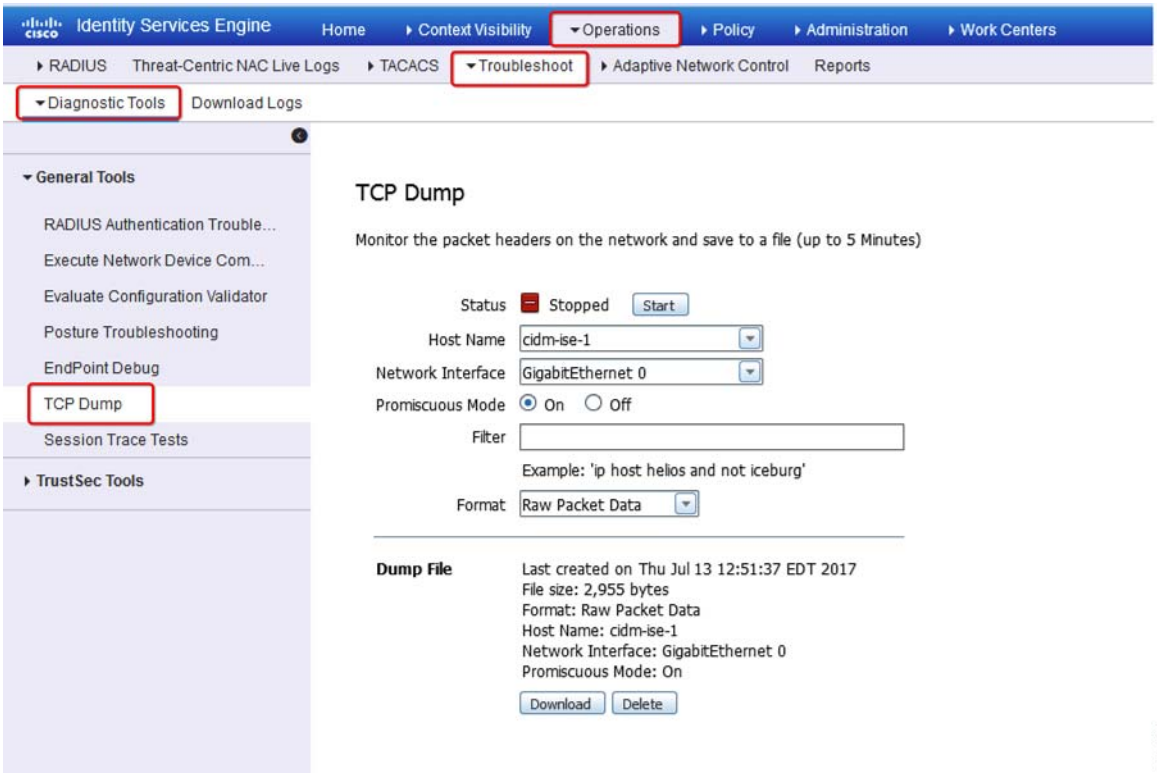
Using TCP Dump Utility

The TCP Dump Utility is a tool to validate the incoming traffic when you want to examine whether the expected packet actually reached a node. For example, when there is no incoming authentication or log indicated in the report, you may suspect that there is no incoming traffic or that the incoming traffic cannot reach Cisco ISE. In such cases, you can run this tool to sniff the traffic and verify.

From **Operations** > **Troubleshoot** > **Diagnostic Tools** > **TCP Dump**, you can configure the options and then collect data from the network traffic to help you troubleshooting a network issue.

The **Raw Packet Data** option creates a PCAP file for Wireshark. The **Human Readable** option creates a text file with headers and protocol information.

Figure 4-3 TCP Dump Utility



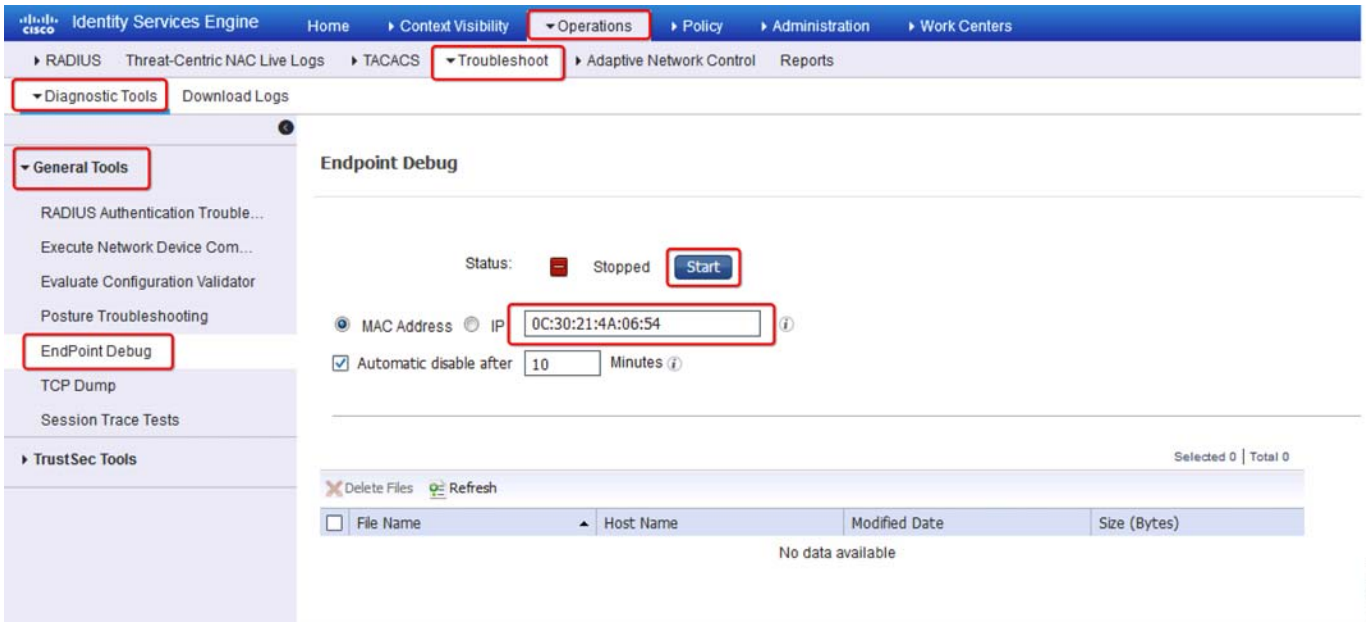
Troubleshooting Endpoints

This section provides information about tools and reports to troubleshoot wired and wireless endpoints (mobile devices) in the network.

Debugging Endpoints

The Endpoint Debug tool can be used to get the logs of all the control plane traffic between the endpoint and Cisco ISE nodes.

Figure 4-4 Endpoint Debug Tool



Troubleshooting BYOD and MDM Endpoints

Once the endpoint (mobile device) is registered with the MDM server, the MDM report can be used to see if the device is in compliance with the Cisco ISE and MDM server.

From **Operations** > **Reports** > **Endpoints and Users**, click **External Mobile Device Management**.

Figure 4-5 MDM Report

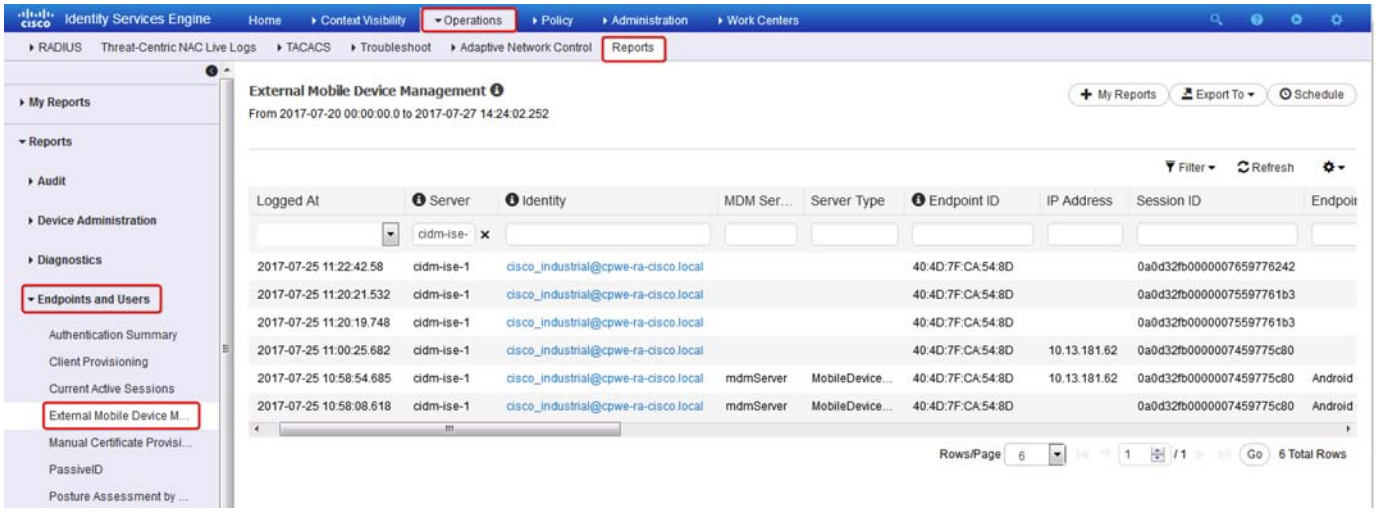
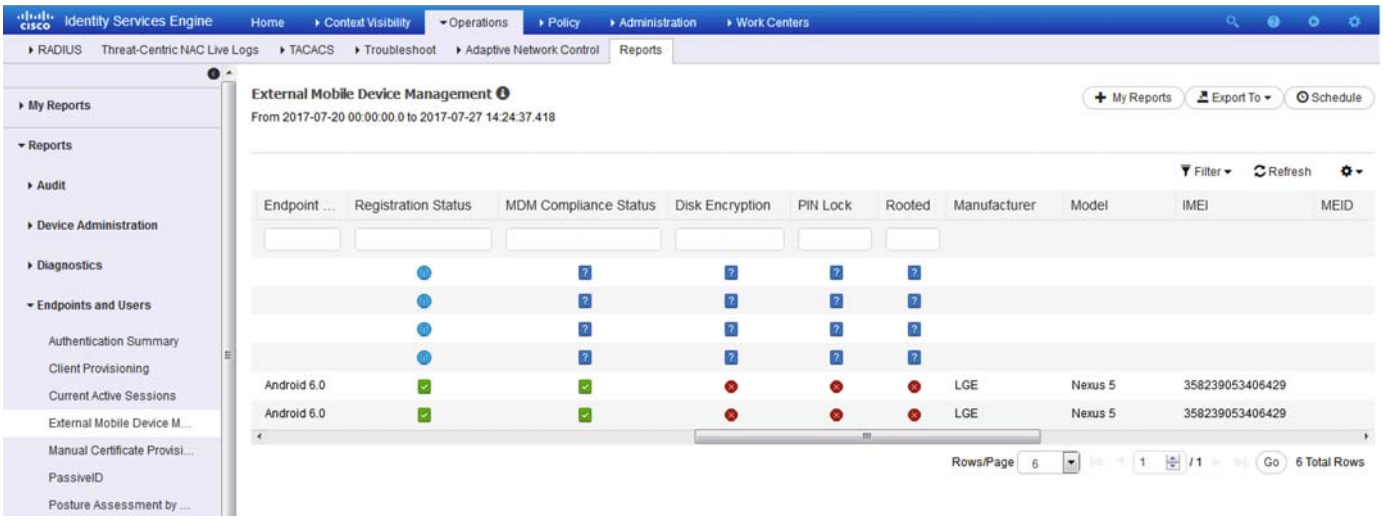


Figure 4-6 MDM Report (Continued)



The **Endpoints** tab under **Context Visibility** provides good information about the endpoint properties, including BYOD endpoints and compliance status.

Figure 4-7 Endpoints—BYOD

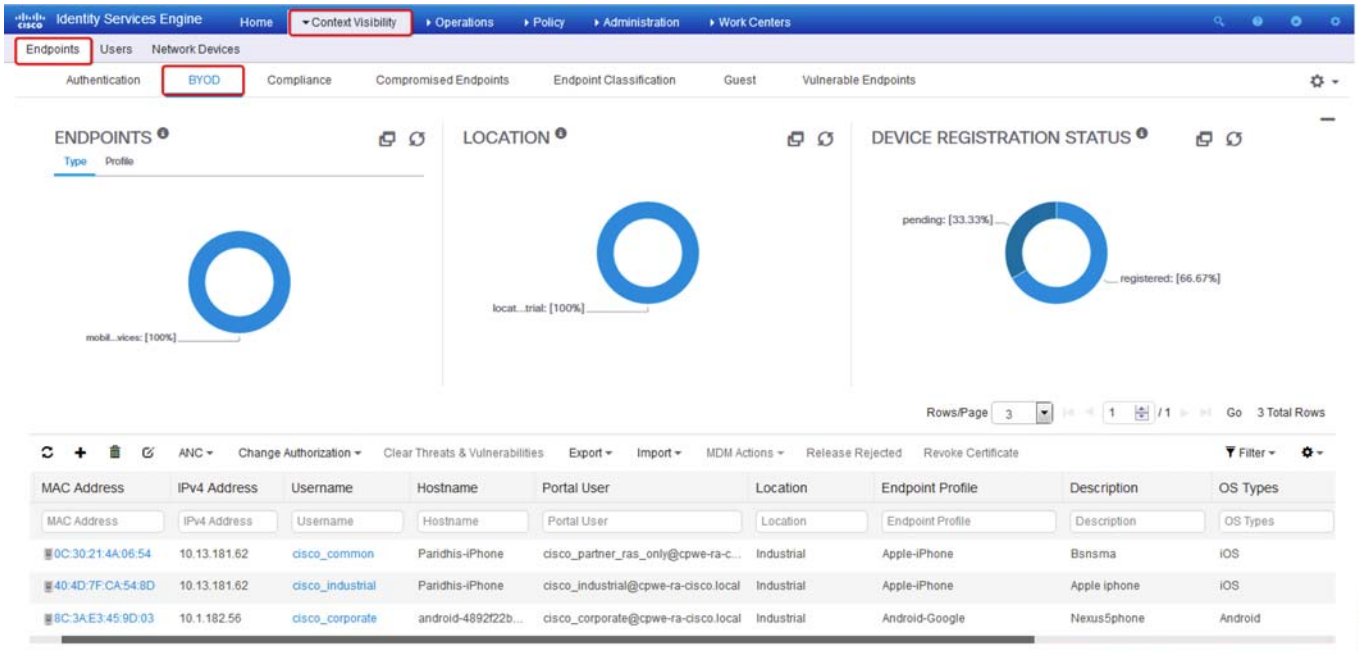
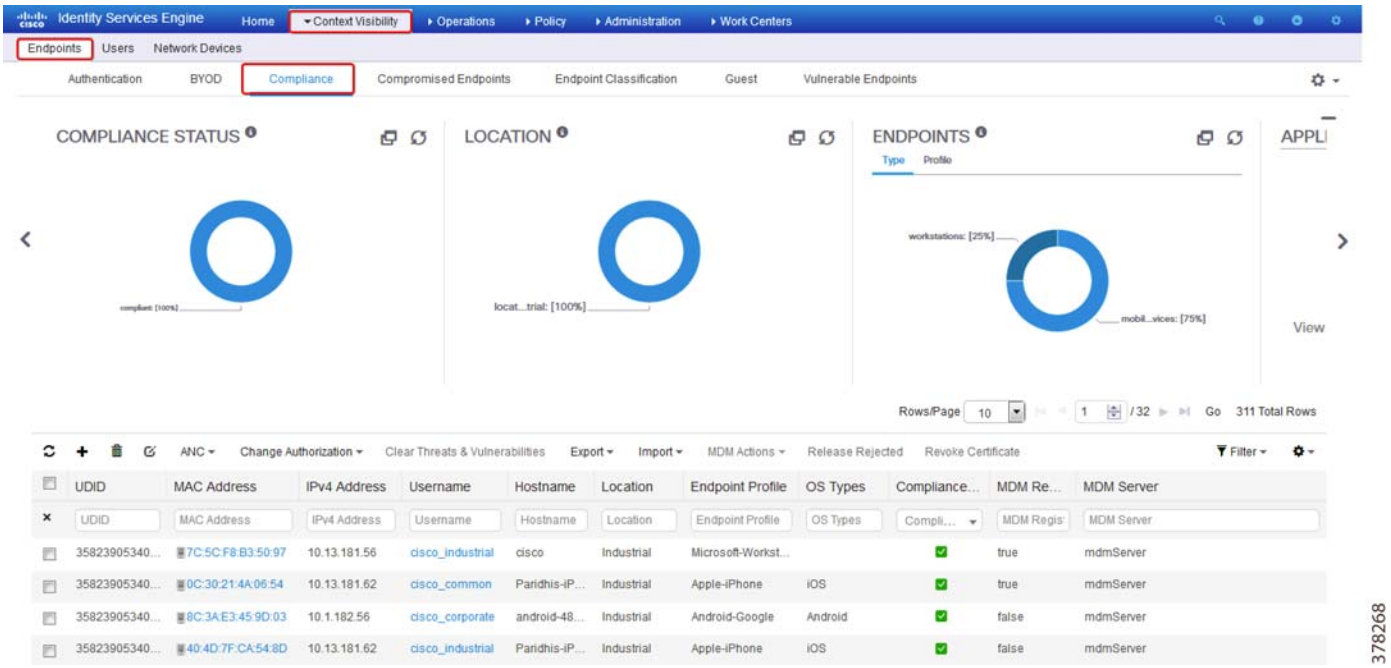


Figure 4-8 Endpoints—Compliance



WLC Troubleshooting Tips

The following section provides high level troubleshooting information to assist in identifying and resolving problems you may encounter when you use the Cisco Wireless LAN Controller (WLC).

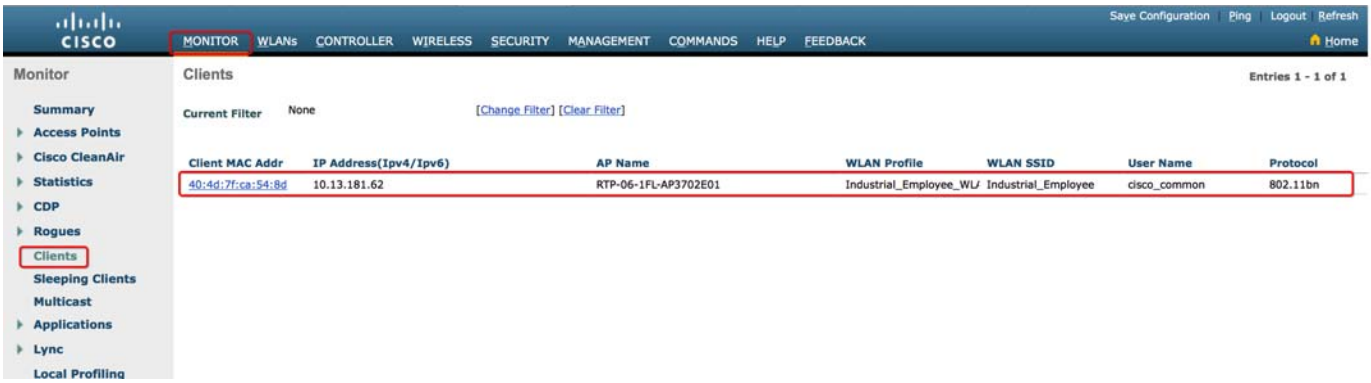
Note For complete information on Cisco WLC monitoring and troubleshooting, refer to the following URLs:

- *Debugging on Cisco Wireless Controllers*
  https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-4/config-guide/b_cg84/debugging_on_cisco_wireless_controllers.html
- *Monitoring Cisco WLC*
  https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-4/config-guide/b_cg84/monitoring_cisco_wlc.html
- *Cisco Wireless LAN Controller System Message Guide*
  https://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-system-message-guides-list.html

Troubleshooting Client Connections

To see active client connections on the WLC and the SSID to which the endpoint connects, from **Monitor** > **Clients**, click the MAC address of the client.

Figure 4-9 Monitor Client Page



From this page, you can see details such as WLAN SSID, status, and the AP to which the clients is connecting. In the **Security Information** section, you can see the ACL and URL of the web portal for BYOD redirection.

Figure 4-10 Client Details

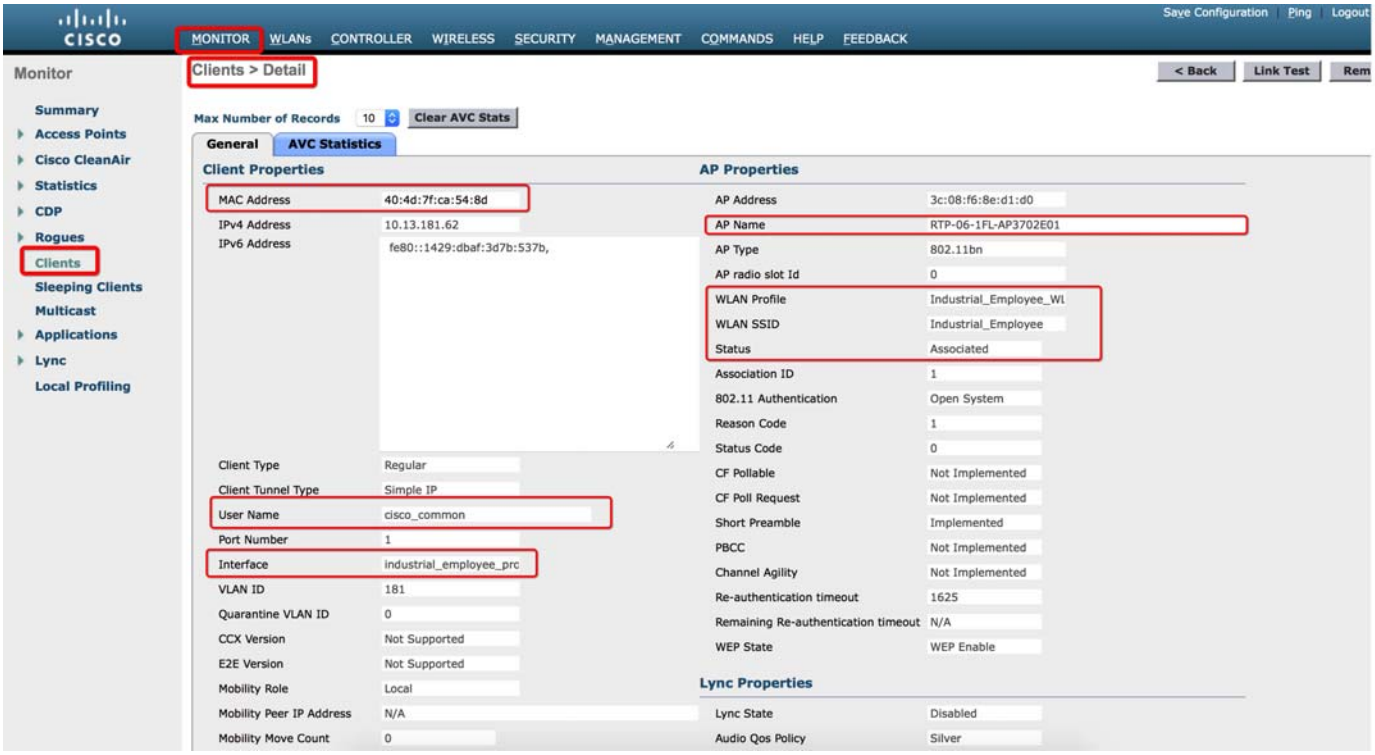
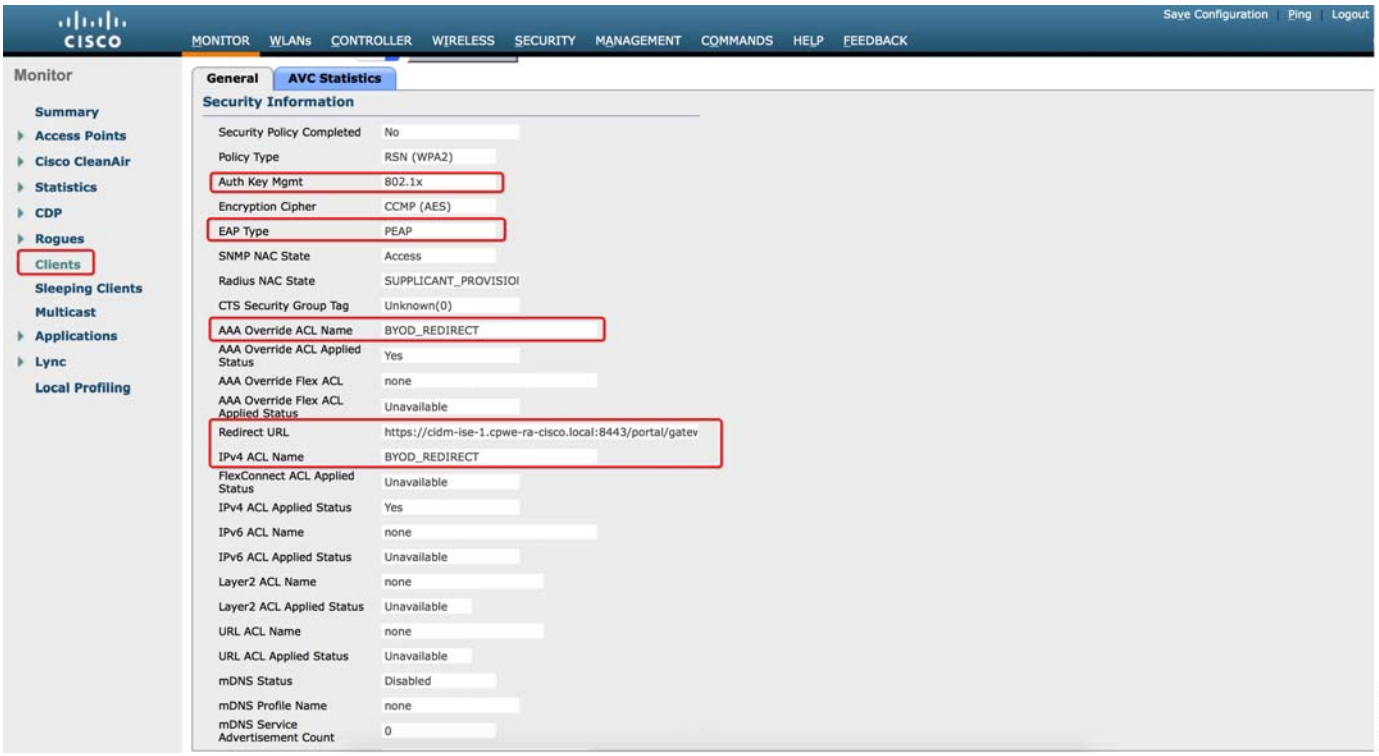


Figure 4-11 Client Security Information



Detailed control plane messages for the client can be obtained by running a debug command in the CLI:

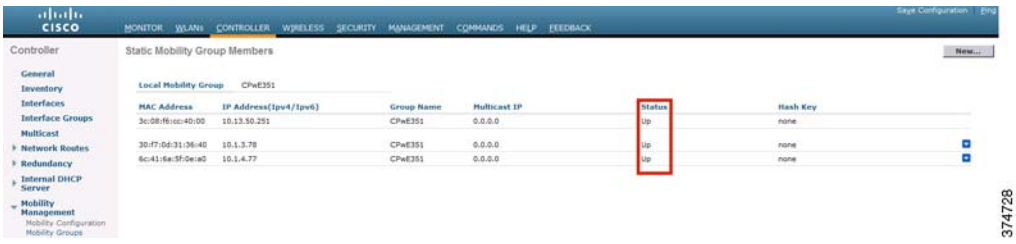
```
debug client <MAC address>
```

Verifying Mobility (EoIP) Tunnel Status

To check if the mobility tunnel is up between the Industrial WLC and the anchor WLC:

Step 1 From **Controller** > **Mobility Management** > **Mobility Groups**, check the status of the group members.

Figure 4-12 Mobility Group Status



If the status is not up, follow these troubleshooting steps:

Step 2 Check whether the group member information is correct (group name, MAC address, and IP address).

Step 3 Check if the IDMZ or Guest DMZ firewall is blocking EoIP (IP protocol 97) and CAPWAP (UDP ports 16666, 16667).

Step 4 Test the mobility UDP control packet communication between two controllers with this command:

```
mping <mobility_peer_IP_address>
```

Step 5 Test the mobility EoIP data packet communication between two controllers with this command:

```
eping <mobility_peer_IP_address>
```

Debugging AAA, RADIUS and 802.1X

The following commands can be used to debug RADIUS and 802.1X operation on the WLC.

```
debug aaa all enable
debug dot1x aaa enable
debug dot1x all enable
```

Caution Because debugging output is assigned high priority in the CPU, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems. Moreover, use debug commands only during periods of lower network traffic and reduced users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.

APPENDIX A

References

This appendix includes the following reference sections:

Converged Plantwide Ethernet (CPwE)

- Design Zone for Manufacturing-Converged Plantwide Ethernet
  http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html
- Industrial Network Architectures-Converged Plantwide Ethernet
  http://www.rockwellautomation.com/global/capabilities/industrial-networks/overview.page?pagetitle=Network-Architectures
- Converged Plantwide Ethernet (CPwE) Design and Implementation Guide (CPwE):
  - Rockwell Automation site:
    http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf
  - Cisco site:
    https://www.cisco.com/c/dam/en/us/td/docs/solutions/Verticals/CPwE/CPwE-CVD-Sept-2011.pdf
- Deploying 802.11 Wireless LAN Technology within a Converged Plantwide Ethernet Architecture Design and Implementation Guide:
  - Rockwell Automation site:
    http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td006_-en-p.pdf
  - Cisco site:
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/NovCVD/CPwE_WLAN_CVD.html
- Deploying Network Address Translation within a Converged Plantwide Ethernet Architecture Design and Implementation Guide:
  - Rockwell Automation site:
    http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td007_-en-p.pdf

  - Cisco site:
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/NAT/DIG/CPwE_NAT_CVD.html

- Deploying A Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide:
  - Rockwell Automation site:
    http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf
  - Cisco site:
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/4-0/Resiliency/DIG/CPwE_resil_CVD.html
- Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture Design and Implementation Guide:
  - Rockwell Automation site:
    http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td002_-en-p.pdf
  - Cisco site:
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-0/Firewalls/DIG/CPwE-5-IFS-DIG.html
- Securely Traversing IACS Data Across the Industrial Demilitarized Zone Design and Implementation Guide:
  - Rockwell Automation site:
    http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td009_-en-p.pdf
  - Cisco site:
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/IDMZ/DIG/CPwE_IDMZ_CVD.html

Cisco Wireless and Mobility

- Cisco Wireless and Mobility web page:
  https://www.cisco.com/c/en/us/products/wireless/index.html
- Enterprise Mobility Design Guide
  https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/Enterprise-Mobility-8-1-Design-Guide/Enterprise_Mobility_8-1_Deployment_Guide.html
- Bring your own device (BYOD)
  https://www.cisco.com/c/en/us/solutions/byod-smart-solution/overview.html
- 802.11ac Solution
  https://www.cisco.com/c/en/us/solutions/enterprise-networks/802-11ac-solution/index.html

Cisco Security

- Cisco Security web page:
  https://www.cisco.com/c/en/us/products/security/index.html
- Cisco Identity Service Engine
  https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html

- Cisco Identity Services Engine Administrator Guide
  http://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_010.html
- Cisco Identity Services Engine Installation Guide
  http://www.cisco.com/c/en/us/td/docs/security/ise/2-2/install_guide/b_ise_InstallationGuide22.html
- Cisco Web Security Appliance
  https://www.cisco.com/c/en/us/products/security/web-security-appliance/index.html
- Advanced Malware Protection (AMP)
  https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html
- Cisco Umbrella
  https://umbrella.cisco.com
- Next-Generation Firewalls
  https://www.cisco.com/c/en/us/products/security/firewalls/index.html
- Cisco Stealthwatch
  https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html

APPENDIX B

Test Hardware and Software

The components listed in Table B-1 were used in CPwE Identity and Mobility Services testing.

Table B-1 Test Hardware and Software

Role	Product	SW Version	Notes
IES Access Switches	Cisco IE 2000, Cisco IE 4000	15.2(5)E1(ED)	
	Allen-Bradley Stratix 5700, Allen-Bradley Stratix 5400	15.2(5)EA	
Distribution Switch	Cisco Catalyst 3850	16.3.2 Denali	Switch stack
Core Switches	Catalyst 6800	15.2(1)SY1a	Virtual Switching System (VSS)
	Catalyst 4500-X	3.6.2E	Virtual Switching System (VSS)
Lightweight Access Point	Cisco IW3700	15.3(3)JE	
Autonomous Access Point	Allen-Bradley Stratix 5100	15.3(3)JC1	
Workgroup Bridge (WGB)	Allen-Bradley Stratix 5100, Cisco 2700	15.3(3)JC1	
Wireless LAN Controller	Cisco 5508	8.4.100.0	Active and standby
Mobility Services Engine	Cisco MSE	8.0	
IDMZ Firewall	Cisco ASA 5525-X	9.4(3)6, ASDM 7.4(3)	Active and standby
	FireSIGHT Management Center	5.4.1.8	
Policy Servers	Cisco ISE VM, ISE 3415, ISE 3495	2.2	Distributed Cisco ISE
	Microsoft Network Policy Server	Windows Server 2012 R2	
Mobile Clients—Windows	Microsoft Windows Laptop	Windows 7 Enterprise Windows 10 Enterprise	
Mobile Clients—iOS	Apple iPhone 6S, iPad Air 2	10.3.3	
Mobile Clients—Android	Samsung Galaxy S7, Galaxy Tab S2	4.3, 6.01	
IACS Applications	FactoryTalk TeamONE	2.3.128	
	ThinManager	9.0 SP4	
	FactoryTalk View SE	9.00	
	FactoryTalk ViewPoint	9.00	
	FactoryTalk VantagePoint	8.00	

APPENDIX C

Acronyms and Initialisms

Table C-1 Acronyms and Initialisms

Term	Definition
1:1	One-to-One
AAA	Authentication, Authorization, and Accounting
AD	Microsoft Active Directory
AD CS	Active Directory Certificate Services
AD DS	Active Directory Domain Services
AES	Advanced Encryption Standard
ACL	Access Control List
AH	Authentication Header
AIA	Authority Information Access
AMP	Advanced Malware Protection
ASDM	Cisco Adaptive Security Device Manager
ASR	Cisco Aggregation Services Router
BYOD	Bring Your Own Device
CA	Certificate Authority
CDP	CRL Distribution Points
CIP	Common Industrial Protocol
CoA	Change of Authorization
CPwE	Converged Plantwide Ethernet
CRD	Cisco Reference Design
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CSSM	Cisco Smart Software Manager
CTL	Certificate Trust List
CVD	Cisco Validated Design
DIG	Design and Implementation Guide
DACL	Downloadable Access Control List
DC	Domain Controller
DHCP	Dynamic Host Configuration Protocol
DMVPN	Dynamic Multipoint Virtual Private Network

Table C-1 Acronyms and Initialisms (continued)

Term	Definition
DNS	Domain Name System
DPI	Deep Packet Inspection
DSRM	Directory Services Restoration Mode
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
EIGRP	Enhanced Interior Gateway Routing Protocol
EMI	Enterprise Manufacturing Intelligence
EoIP	Ethernet over IP
ERP	Enterprise Resource Planning
ESP	Encapsulating Security Protocol
ESR	Embedded Services Router
FIB	Forwarding Information Base
FQDN	Fully Qualified Domain Name
FVRF	Front-door Virtual Route Forwarding
GRE	Generic Routing Encapsulation
HMAC	Hash Message Authentication Code
HMI	Human-Machine Interface
IACS	Industrial Automation and Control System
ICS	Industrial Control System
IDMZ	Industrial Demilitarized Zones
IES	Industrial Ethernet Switch (Allen-Bradley Stratix, Cisco IE)
IIoT	Industrial Internet of Things
IKE	Internet Key Exchange
IoT	Internet of Things
IP	Internet Protocol
IPDT	IP Device Tracking
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
ISE	Cisco Identity Services Engine
ISR	Integrated Service Router
IT	Information Technology
LBS	Location Based Services
LWAP	Lightweight Access Point
MAB	MAC Authentication Bypass
MAC	Media Access Control
MDM	Mobile Device Management
ME	FactoryTalk View Machine Edition
mGRE	Multipoint Generic Routing Encapsulation
MMC	Microsoft Management Console
MnT	Monitoring Node
MPLS	Multiprotocol Label Switching
MSE	Mobile Service Engine
MSS	Maximum Segment Size
MTTR	Mean Time to Repair

Table C-1 Acronyms and Initialisms (continued)

Term	Definition
MTU	Maximum Transmission Unit
NAC	Network Access Control
NAT	Network Address Translation
NDES	Network Device Enrollment Service
NHRP	Next Hop Routing Protocol
NOC	Network Operation Center
NPS	Microsoft Network Policy Server
NSP	Native Supplicant Profile
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OEE	Overall Equipment Effectiveness
OT	Operational Technology
OTA	Over-the-Air
OU	Organizational Unit
PAN	Policy Administration Node
PAT	Port Address Translation
PCS	Process Control System
PEAP	Protected Extensible Authentication Protocol
PKI	Public Key Infrastructure
PSK	Pre-Shared Key
PSN	Policy Service Node
RA	Registration Authority
RADIUS	Remote Authentication Dial-In User Service
RAS	Remote Access Server
RD	Route Descriptor
RDG	Remote Desktop Gateway
RDP	Remote Desktop Protocol
RDS	Remote Desktop Services
RTT	Round Trip Time
SA	Security Association
SaaS	Software-as-a-Service
SCEP	Simple Certificate Enrollment Protocol
SE	FactoryTalk View Site Edition
SHA	Secure Hash Standard
SIG	Secure Internet Gateway
SPW	Software Provisioning Wizard
SSID	Service Set Identifier
SYN	Synchronization
TCP	Transmission Control Protocol
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNC	Virtual Network Computing
VPN	Virtual Private Network

Table C-1 Acronyms and Initialisms (continued)

Term	Definition
VRF	Virtual Route Forwarding
WAN	Wide Area Network
wIPS	wireless Intrusion Prevention Service
WLAN	Wireless LAN
WLC	Cisco Wireless LAN Controller
WSA	Cisco Web Security Appliance
ZFW	Zone-Based Policy Firewall

APPENDIX D

About the Cisco Validated Design (CVD) Program

Converged Plantwide Ethernet (CPwE) is a collection of tested and validated architectures developed by subject matter authorities at Cisco and Rockwell Automation which follows the Cisco Validated Design (CVD) program.

CVDs provide the foundation for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Each one has been comprehensively tested and documented by engineers to help achieve faster, more reliable, and fully predictable deployment.

The CVD process is comprehensive and focuses on solving business problems for customers and documenting these solutions. The process consists of the following steps:

- Requirements are gathered from a broad base of customers to devise a set of use cases that will fulfill these business needs.
- Network architectures are designed or extended to provide the functionality necessary to enable these use cases, and any missing functionality is relayed back to the appropriate product development team(s).
- Detailed test plans are developed based on the architecture designs to validate the proposed solution, with an emphasis on feature and platform interaction across the system. These tests generally consist of functionality, resiliency, scale, and performance characterization.
- All parties contribute to the development of the CVD guide, which covers both design recommendations and implementation of the solution based on the testing outcomes.

Within the CVD program, Cisco also provides Cisco Reference Designs (CRDs) that follow the CVD process but focus on reference designs developed around specific set of priority use cases. The scope of CRD testing typically focuses on solution functional verification with limited scale.

For more information about the CVD program, please see the Cisco Validated Designs at the following URL::

https://www.cisco.com/c/en/us/solutions/enterprise/validated-design-program/index.html

Publication ENET-TD008B-EN-P February 2018